Atmic Networks

CERTIFICATION EXAM SUPPORT

EXAM PREPARATION MATERIAL

Practice files designed to help you understand exam patterns, question styles and the overall assessment format.

IMPORTANT NOTE

Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns.

Stay connected with our support team
for the latest file updates and exam-related information.

www.atmicnetworks.com

Knowledge that moves beyond memorization.

www.atmicnetworks.com

Question: 1

[Security Concepts]
In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

A. Smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit

Answer: C

Explanation:

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.
Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.
For example the code below is written in hex: <a
href=javascript:alert&#
x28'XSS')>Click Here
is equivalent to:
Click Here
Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

Question: 2

[Security Concepts]
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

A. user input validation in a web page or web application
B. Linux and Windows operating systems
C. database
D. web page images

www.atmicnetworks.com

Answer: A

Explanation:

SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives ("injects") you an SQL statement that you will unknowingly run on your database. For example: Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):

txtUserId = getRequestString("UserId");

txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;

If user enter something like this: "100 OR 1=1" then the SzQL statement will look like this:

SELECT * FROM Users WHERE UserId = 100 OR 1=1;

The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE. A hacker might get access to all the user names and passwords in this database.

Question: 3

[Security Concepts]

Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two)

A. Check integer, float, or Boolean string parameters to ensure accurate values.
B. Use prepared statements and parameterized queries.
C. Secure the connection between the web and the app tier.
D. Write SQL code instead of using object-relational mapping libraries.
E. Block SQL code execution in the web application database login.

Answer: B,E

Explanation:

SQL injection attacks are a type of code injection technique that exploit the use of dynamic SQL queries in web applications. Attackers can inject malicious SQL statements into user input fields, such as login forms, search boxes, or URLs, and execute them on the underlying database. This can result in unauthorized access, data theft, data corruption, or denial of service.

To prevent SQL injection attacks, web developers should use the following techniques:

Use prepared statements and parameterized queries: Prepared statements are SQL queries that are precompiled and executed with user-supplied parameters. Parameterized queries are SQL queries that use placeholders for user input and bind them to actual values at runtime. Both techniques separate the SQL code from the user input, making it impossible for attackers to inject SQL commands into the query. For example, in Java, PreparedStatement is a class that implements parameterized queries. In PHP, PDO and mysqli are extensions that support prepared statements. Block SQL code execution in the web application database login: Web applications should use a dedicated database user account with limited privileges to connect to the database. This account should only have the permissions

necessary to perform the required operations, such as select, insert, update, or delete. It should not have the permissions to execute arbitrary SQL commands, such as create, drop, alter, grant, or revoke. This way, even if an attacker manages to inject SQL code into the query, the database will reject it due to insufficient privileges.

Reference:

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 5: Securing the Cloud, Lesson 5.2: Cloud Application Security, Topic 5.2.2: SQL Injection

SQL Injection Prevention - OWASP Cheat Sheet Series

How to Prevent SQL Injection: 5 Key Prevention Methods - eSecurityPlanet

How to Protect Against SQL Injection Attacks

Question: 4

[Content Security]

Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program

Answer: D,E

Explanation:

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

Question: 5

[Content Security]

Which two mechanisms are used to control phishing attacks? (Choose two)

A. Enable browser alerts for fraudulent websites.
B. Define security group memberships.
C. Revoke expired CRL of the websites.
D. Use antispyware software.
E. Implement email filtering techniques.

Answer: A,E

Explanation:

Phishing attacks are a type of social engineering that aim to trick users into revealing their personal or financial information, or installing malware on their devices. To control phishing attacks, users and organizations need to implement various preventive and reactive measures, such as:

Enable browser alerts for fraudulent websites. Most modern browsers have built-in features that can warn users when they visit a website that is suspected of being malicious or impersonating a legitimate entity. These alerts can help users avoid falling for phishing scams that use fake web pages to capture their credentials or other sensitive data. For example, Google Chrome has a Safe Browsing feature that displays a red warning page when users try to access a deceptive site. Users should always pay attention to these alerts and avoid proceeding to untrusted sites.

Implement email filtering techniques. Email is one of the most common channels for phishing attacks, as attackers can send spoofed messages that appear to come from trusted sources, such as banks, government agencies, or colleagues. Email filtering techniques can help block or flag suspicious emails based on various criteria, such as the sender's address, the subject line, the content, or the attachments. For example, Microsoft Outlook has a Junk Email Filter that can move potential phishing emails to a separate folder or delete them automatically. Users should also be careful not to open or reply to any unsolicited or unexpected emails, especially those that ask for personal or financial information, or contain links or attachments.

Other mechanisms that can help control phishing attacks include:

Use strong passwords and enable two-factor authentication. Even if users fall victim to phishing attacks and reveal their passwords, they can still protect their accounts by using strong and unique passwords for each service, and enabling two-factor authentication (2FA) whenever possible. 2FA adds an extra layer of security by requiring users to enter a code or a token that is sent to their phone or email, or generated by an app, in addition to their password. This way, even if attackers obtain the password, they cannot access the account without the second factor.

Don't ignore update messages. Users should always keep their operating systems, browsers, and applications updated with the latest security patches and fixes. These updates can help prevent phishing attacks that exploit known vulnerabilities or bugs in the software. Users should also use antivirus and antispyware software that can detect and remove malware that may be installed by phishing attacks.

Exercise caution when opening emails or clicking on links. Users should always be skeptical and vigilant when they receive emails or messages that ask them to take urgent or unusual actions, such as verifying their account, updating their payment information, or downloading a file. Users should also check the sender's address, the spelling and grammar, and the URL of any links before clicking on them. Users can hover over the link to see the actual destination, or use a link scanner tool, such as VirusTotal, to check if the link is malicious or not.

Reference :=

1: https://safebrowsing.google.com/ 2: https://support.microsoft.com/en-us/office/overview-of-the- junk-email-filter-5ae3ea8e-cf41-4fa0-b02a-3b96e21de089 3: https://www.virustotal.com/gui/home/url

www.atmicnetworks.com

Question: 6

[Security Concepts]
Which two behavioral patterns characterize a ping of death attack? (Choose two)

A. The attack is fragmented into groups of 16 octets before transmission.
B. The attack is fragmented into groups of 8 octets before transmission.
C. Short synchronized bursts of traffic are used to disrupt TCP connections.
D. Malformed packets are used to crash systems.
E. Publicly accessible DNS servers are typically used to execute the attack.

Answer: B,D

Explanation:

Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

A correctly-formed ping packet is typically 56 bytes in size, or 64 bytes when the ICMP header is considered, and 84 including Internet Protocol version 4 header. However, any IPv4 packet (including pings) may be as large as 65,535 bytes. Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

Question: 7

[Security Concepts]
Which two preventive measures are used to control cross-site scripting? (Choose two)

A. Enable client-side scripts on a per-domain basis.
B. Incorporate contextual output encoding/escaping.
C. Disable cookie inspection in the HTML inspection engine.
D. Run untrusted HTML input through an HTML sanitization engine.
E. Same Site cookie attribute should not be used.

Answer: B,D

Explanation:

Cross-site scripting (XSS) is a web security vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can compromise the user's interaction with the web application, steal sensitive data, perform unauthorized actions, and more. To prevent XSS, web developers need to apply various defensive techniques to ensure that user-supplied data is not interpreted as code by the browser. Two of these techniques are:

Incorporate contextual output encoding/escaping: This means that any user-supplied data that is displayed on the web page should be properly encoded or escaped according to the context where it appears. For example, if the data is inserted into an HTML attribute, it should be HTML attribute encoded; if the data is inserted into a JavaScript string, it should be JavaScript string encoded; and so on. This prevents the data from breaking out of its intended context and being executed as code by the browser. Output encoding should be done by using a reliable library or framework that supports different contexts and encodings.

Run untrusted HTML input through an HTML sanitization engine: This means that any user-supplied data that is intended to contain HTML markup should be filtered and validated by a sanitization engine that removes or escapes any potentially dangerous elements, attributes, or scripts. This prevents the attacker from injecting malicious HTML code that can execute scripts, load external resources, redirect the user, or perform other malicious actions. HTML sanitization should be done by using a well-tested and maintained library or framework that follows the best practices and standards for HTML filtering.

Reference :=

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 5: Securing the Cloud, Lesson 5.2: Web Application Security, Topic 5.2.2: Cross-Site Scripting (XSS) Cross Site Scripting Prevention Cheat Sheet - OWASP
What is cross-site scripting (XSS) and how to prevent it? - Web Security Academy

Question: 8

[Content Security]
What is the difference between deceptive phishing and spear phishing?

A. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.
B. A spear phishing campaign is aimed at a specific person versus a group of people.
C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Answer: B

Explanation:

In deceptive phishing, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials.

www.atmicnetworks.com

Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.
Spear phishing is carefully designed to get a single recipient to respond. Criminals select an individual target within an organization, using social media and other public information – and craft a fake email tailored for that person.

Question: 9

[Security Concepts]
Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting
B. water holing
C. DDoS
D. buffer overflow

Answer: D

Explanation:

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.
Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's alloted memory space. This happens quite frequently in the case of arrays.

Question: 10

[Security Concepts]
What is a language format designed to exchange threat intelligence that can be transported over the
TAXII
protocol?

A. STIX
B. XMPP
C. pxGrid
D. SMTP

www.atmicnetworks.com

Answer: A

Explanation:

TAXII (Trusted Automated Exchange of Indicator Information) is a standard that provides a transport

Question: 11

[Security Concepts]
Which two capabilities does TAXII support? (Choose two)

A. Exchange
B. Pull messaging
C. Binding
D. Correlation
E. Mitigating

Answer: A,B

Explanation:

The Trusted Automated eXchangeof Indicator Information (TAXII) specifies mechanisms for exchanging structured cyber threat information between parties over the network.

TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information.

TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that this version of TAXII supports: push messaging, pull messaging, and discovery.

Although there is no “binding” capability in the list but it is the best answer here.

Question: 12

[Security Concepts]
Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two)

A. exploits

www.atmicnetworks.com

B. ARP spoofing
C. denial-of-service attacks
D. malware
E. eavesdropping

Answer: A,D

Explanation:

Malware means “malicious software”, is any software intentionally designed to cause damage to a computer, server, client, or computer network. The most popular types of malware includes viruses, ransomware and spyware. Virus Possibly the most common type of malware, viruses attach their malicious code to clean code and wait to be run.
Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again.
Spyware is spying software that can secretly record everything you enter, upload, download, and store on your computers or mobile devices. Spyware always tries to keep itself hidden.
An exploit is a code that takes advantage of a software vulnerability or security flaw.
Exploits and malware are two risks for endpoints that are not up to date. ARP spoofing and eavesdropping are attacks against the network while denial-of-service attack is based on the flooding of IP packets.

Question: 13

[Secure Network Access, Visibility, and Enforcement]
Which PKI enrollment method allows the user to separate authentication and enrollment actions and

also
provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

A. url
B. terminal
C. profile
D. selfsigned

Answer: C

Explanation:

A trustpoint enrollment mode, which also defines the trustpoint authentication mode, can be performed via 3 main methods:

1. Terminal Enrollment – manual method of performing trustpoint authentication and certificate enrolment using copy-paste in the CLI terminal.
2. SCEP Enrollment – Trustpoint authentication and enrollment using SCEP over HTTP.
3. Enrollment Profile – Here, authentication and enrollment methods are defined separately. Along with terminal and SCEP enrollment methods, enrollment profiles provide an option to specify HTTP/TFTP commands to perform file retrieval from the Server, which is defined using an authentication or enrollment url under the profile.

Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure- pki/211333-IOSPKI-Deployment-Guide-Initial-Design.html

Question: 14

[Security Concepts]
What are two rootkit types? (Choose two)

A. registry
B. virtual
C. bootloader
D. user mode
E. buffer mode

Answer: C,D

Explanation:

The term 'rootkit' originally comes from the Unix world, where the word 'root' is used to describe a user with the highest possible level of access privileges, similar to an 'Administrator' in Windows. The word 'kit' refers to the software that grants root-level access to the machine. Put the two together and you get 'rootkit', a program that gives someone – with legitimate or malicious intentions – privileged access to a computer.
There are four main types of rootkits: Kernel rootkits, User mode rootkits, Bootloader rootkits, Memory rootkits

Question: 15

[Security Concepts]
Which form of attack is launched using botnets?

A. EIDDOS
B. virus

www.atmicnetworks.com

C. DDOS
D. TCP flood

Answer: C

Explanation:

A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them. Cyber criminals use botnets to instigate botnet attacks, which include malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks.

Question: 16

[Security Concepts]
Which threat involves software being used to gain unauthorized access to a computer system?

A. virus
B. NTP amplification
C. ping of death
D. HTTP flood

Answer: A

Explanation:

A virus is a type of malware that infects a computer system by attaching itself to another program or file. Once executed, the virus can replicate itself and spread to other files or systems. A virus can be used to gain unauthorized access to a computer system by exploiting software vulnerabilities, stealing credentials, or installing backdoors. A virus can also cause damage to the system by deleting, modifying, or encrypting data, or consuming system resources. According to the Implementing and Operating Cisco Security Core Technologies (SCOR) course, viruses are one of the most common forms of malware and can be classified into different types based on their behavior, such as boot sector viruses, file infectors, macro viruses, or polymorphic viruses1. Reference: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) course, Module 1: Malware Analysis, Lesson 1: Malware Types and Characteristics, Topic: Virus.

www.atmicnetworks.com

Question: 17

[Security Concepts]
Which type of attack is social engineering?

A. trojan
B. phishing
C. malware
D. MITM

Answer: B

Explanation:
Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem.

Question: 18

[Security Concepts]
Which two key and block sizes are valid for AES? (Choose two)

A. 64-bit block size, 112-bit key length
B. 64-bit block size, 168-bit key length
C. 128-bit block size, 192-bit key length
D. 128-bit block size, 256-bit key length
E. 192-bit block size, 256-bit key length

Answer: C,D

Explanation:

The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits (block size). It can do this using 128-bit, 192-bit, or 256-bit keys

www.atmicnetworks.com

Question: 19

[Security Concepts]
Which two descriptions of AES encryption are true? (Choose two)

A. AES is less secure than 3DES.
B. AES is more secure than 3DES.
C. AES can use a 168-bit key for encryption.
D. AES can use a 256-bit key for encryption.
E. AES encrypts and decrypts a key three times in sequence.

Answer: B,D

Explanation:

AES encryption is a symmetric block cipher algorithm that uses a single key to encrypt and decrypt data. It is more secure than 3DES, which is an older and slower algorithm that encrypts and decrypts a key three times in sequence. AES can use different key sizes, such as 128, 192, or 256 bits, depending on the security level required. The longer the key, the more rounds of encryption and decryption are performed, making it harder to break. AES encryption is based on a substitutionpermutation network, which consists of a series of operations that transform the input data into the output data using the key. Reference :=
https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Question: 20

[Secure Network Access, Visibility, and Enforcement]
Which algorithm provides encryption and authentication for data plane communication?

A. AES-GCM
B. SHA-96
C. AES-256
D. SHA-384

www.atmicnetworks.com

Answer: A

Explanation:

The data plane of any network is responsible for handling data packets that are transported across the network.
(The data plane is also sometimes called the forwarding plane.)

Maybe this Qwants to ask about the encryption and authentication in the data plane of a SD-WAN network (but SD-WAN is not a topic of the SCOR 350-701 exam?).
In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a

symmetrickey algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates.

Reference:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security- book/ security-overview.html

Question: 21

[Security Concepts]
Elliptic curve cryptography is a stronger more efficient cryptography method meant to replace which current encryption technology?

A. 3DES
B. RSA
C. DES
D. AES

Answer: B

Explanation:

Compared to RSA, the prevalent public-key cryptography of the Internet today, Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation,as well as memory, energy and bandwidth savings and is thus better suited forsmall devices.

www.atmicnetworks.com

Question: 22

[Security Concepts]
What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

Answer: C

Explanation:

Configure a Crypto ISAKMP Key
In order to configure a preshared authentication key, enter the crypto isakmp key command in global configuration mode:
crypto isakmp key cisco123 address 172.16.1.1

https://community.cisco.com/t5/vpn/isakmp-with-0-0-0-0-dmvpn/td-p/4312380
It is a bad practice but it is valid. 172.16.0.0/16 the full range will be accepted as possible PEER
https://www.examtopics.com/discussions/cisco/view/46191-exam-350-701-topic-1-question-71-discussion/#:~:text=Command%20reference%20is%20not%20decisive,172.16.1.128%20cisco123%0A CSR%2D1(config)%23
Testing without a netmask shows that command interpretation has a preference for /16 and /24.
CSR-1(config)#crypto isakmp key cisco123 address 172.16.0.0
CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.0.0
[255.255.0.0] cisco123
CSR-1(config)#no crypto isakmp key cisco123 address 172.16.0.0
CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.0
CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.1.0
[255.255.255.0] cisco123
CSR-1(config)#no crypto isakmp key cisco123 address 172.16.1.0
CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.128
CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.1.128 cisco123
CSR-1(config)#

Question: 23

[Network Security]
Which technology must be used to implement secure VPN connectivity among company branches over a

www.atmicnetworks.com

private IP cloud with any-to-any scalable connectivity?

A. DMVPN
B. FlexVPN
C. IPsec DVTI
D. GET VPN

Answer: D

Explanation:

Cisco's Group Encrypted Transport VPN (GETVPN) introduces the concept of a trusted group to eliminate point-to-point tunnels and their associated overlay routing. All group members (GMs) share a common security association (SA), also known as a group SA. This enables GMs to decrypt traffic that was encrypted by any other GM.

GETVPN provides instantaneous large-scale any-to-any IP connectivity using a group IPsec security paradigm.
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_version_2_0_External.pdf

Question: 24

[Network Security]
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two)

A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; theIPsec configuration is copied automatically
B. The active and standby devices can run different versions of the Cisco IOS software but must be the sametype of device.
C. The IPsec configuration that is set up on the active device must be duplicated on the standby device
D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device;the IKE configuration is copied automatically.
E. The active and standby devices must run the same version of the Cisco IOS software and must be thesame type of device

Answer: C,E

Explanation:

Stateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This failover process is transparent to users and does not require adjustment or reconfiguration of any remote peer. Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.

Prerequisites for Stateful Failover for IPsec

Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices

This document assumes that you have a complete IKE and IPsec configuration.

The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device.

That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on crypto map sets, all AAA configurations used for crypto, client configuration groups, IP local pools used for crypto, and ISAKMP profiles.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15- mt/sec-vpnavailability-15-mt-book/sec-state-fail-ipsec.htmlAlthough the prerequisites only stated that “Both routers should be the same type of device” but in the“Restrictions for Stateful Failover for IPsec” section of the link above, it requires “Both the active and standby devices must run the identical version of the Cisco IOS software” so answer E is better than answer B.

Question: 25

[Network Security]

Which VPN technology can support a multivendor environment and secure traffic between sites?

A. SSL VPN
B. GET VPN
C. FlexVPN
D. DMVPN

Answer: C

Explanation:

FlexVPN is an IKEv2-based VPN technology that provides several benefits beyond traditional site-to- site VPN implementations. FlexVPN is a standards-based solution that can interoperate with nonCisco IKEv2 implementations. Therefore FlexVPN can support a multivendor environment. All of the three VPN technologies support traffic between sites (site-to-site or spoke-to-spoke).

Question: 26

[Network Security]

A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 0.0.0.0 command on host A. The tunnel is not being established to hostB. What action is needed to authenticate the VPN?

A. Change isakmp to ikev2 in the command on hostA.
B. Enter the command with a different password on hostB.
C. Enter the same command on hostB.
D. Change the password on hostA to the default password.

Answer: C

Explanation:

The crypto isakmp key command is used to configure a preshared key for ISAKMP authentication between two peers. The address 0.0.0.0 indicates that the key is valid for any peer address. Therefore, the same command must be entered on hostB with the same password in order to establish the tunnel with hostA. Changing the protocol to ikev2, using a different password, or changing the password to the default will not solve the problem, as they will create a mismatch in the authentication parameters. Reference:

Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T, section "Prerequisites for Dynamic Multipoint VPN (DMVPN)"

DMVPN - Concepts & Configuration, section "DMVPN - What is it?"

DMVPN Hub as the CA Server for the DMVPN Network Configuration Example, section "Prerequisites"

Question: 27

[Network Security] Refer to the exhibit.

'- in jo 16r52:33.795: ISAKMP:(10o2): retrannmisnion skipped for phase i (tine amen lone tranxmaaioh 504)
Rl I
•Jun JU 16:52:4<.l i: ISAKMP:(lul)(purging A., ?.«•*.'jCEE05h, Jrlm- cP^ECSO
Fl*
•Jiin 30 16:52:43.291: ISAKMP!<lvU2): retrace; tung phanc . MH KEY EXCH...
•Jun 30 16:52:43.291; ISAKMP IJ 02): ;n,7r< m.-nr ;n ; r-rr u oouhte: on no, attn-pt 5 of 5: retransmit phaac I
•Jun 30 16:52:4 3.295: ISAKMP; < 1002): retransmitting phase 1 MM_KE¥_EXC11
•Jun 3G 16:52:43.295: ISAKMP;(1002): sending packet to 10.10.12.2 rsy_p?it 500 peer port SOU (Il MM KEY.EXCH
•Jun 30 16:52:4 3,295: ISAKMP: < 1 u02) (Ending an IKE IPv4 Packet. Pl»
•Jun 30 16:52:53,299: ISAKMP:(1002): retransmitting phase 1 MM KEY EXCH...
•Jun 30 16:52:5 3.2 99: ISAKMP:(1'62):peer does not I- paranoid keepa lives.

•Jun 30 16:52:53.299; ISAKMP:{1002)ideleting SA reason "Death by retransmission
Pl" State (11 MN EEY EXCH (peer id.10.12,21
•Jun JO 16:52:53.303: ISAKMP: (1"2) idelrUng SA t - • • >n "Dvath by retransmission
Pl" state III MH..KEY_EXCH (per 10.10.12,2)
•Jun 30 16:52:517307" ISAKMP: Unlocking peer struct 0x68207318 for
isadb mark sa deletedG, count [1]
•Jun 30 16:52:53.307: ISAKMP: Deleting peer node by peer reap for 10.Id.12.2: 68287319
•Jun 30 16:52:53.311: ISAKMP; {1002) rlelet mg node 79875537 error FALSE reason "IKE <Jr leted'
Hl*
•Jun 30 16:52:53.311: ISAKMP:(1302)(deleting node -484575753 error FALSE reason "IKE deleted"
•Jun 30 16:52:53.315: ISAKMP:(1002){Input IKE_MESG_IhTERNAL, IKE PHASE1_DEL
•Jun 30 > :5.':S'. m: ISAKMPMl -02):O)| Stat- IKE 1 HM5 Hew Sr.v- - iKE DEST SA

A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status. What is the problem

www.atmicnetworks.com

according to this command output?

A. hashing algorithm mismatch
B. encryption algorithm mismatch
C. authentication key mismatch
D. interesting traffic was not applied

Answer: C

Explanation:

The debug crypto isakmp sa command shows the status of the Internet Security Association and Key Management Protocol (ISAKMP) security associations (SAs). The output of this command indicates that the ISAKMP negotiation failed after several retransmissions. The most likely cause of this failure is a mismatch in the authentication key between the two peers. The authentication key is specified by the crypto isakmp key command and must be the same on both routers. If the authentication key is different, the ISAKMP messages cannot be decrypted and verified by the peers, resulting in an error. To fix this problem, the network administrator should verify and correct the authentication key on both routers and clear the existing ISAKMP SAs with the clear crypto isakmp sa command. Reference: 1, 2, 3, 4

Question: 28

[Network Security]
What is a difference between FlexVPN and DMVPN?

A. DMVPN uses IKEv1 or IKEv2, FlexVPN only uses IKEv1
B. DMVPN uses only IKEv1 FlexVPN uses only IKEv2
C. FlexVPN uses IKEv2, DMVPN uses IKEv1 or IKEv2
D. FlexVPN uses IKEv1 or IKEv2, DMVPN uses only IKEv2

Answer: C

Explanation:

FlexVPN and DMVPN are both Cisco technologies that use point-to-point GRE tunnels to create dynamic VPN networks. However, they differ in some aspects, such as:

FlexVPN is a newer solution that requires newer hardware and IOS versions, while DMVPN is more widely supported on older devices1.

FlexVPN is based on IKEv2, which is a more robust and efficient protocol than IKEv1, which is used by DMVPN (although DMVPN can also use IKEv2)2.

FlexVPN uses static or virtual access interfaces for GRE tunnels, while DMVPN uses a single multipoint GRE interface. This allows more flexibility and visibility for FlexVPN tunnels2.

FlexVPN does not require NHRP registration for spokes to communicate with the hub, while DMVPN does. This simplifies the configuration and reduces the overhead of NHRP3.

FlexVPN has only one standard mode of operation, while DMVPN has three phases with different characteristics and configurations2.

Reference := 1: what is the difference between dmvpn and flexvpn 2: Cisco FlexVPN DMVPN, Part 1 -

www.atmicnetworks.com

Overview and Design 3: DMVPN to FlexVPN Soft Migration Configuration Example

Question: 29

[Network Security]
Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

A. TLSv1.2
B. TLSv1.1
C. BJTLSv1
D. DTLSv1

Answer: D

Explanation:

DTLS is used for delay sensitive applications (voice and video) as its UDP based while TLS is TCP based.
Therefore DTLS offers strongest throughput performance. The throughput of DTLS at the time of AnyConnect connection can be expected to have processing performance close to VPN throughput.

Question: 30

[Network Security]
What is a commonality between DMVPN and FlexVPN technologies?

A. FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes
B. FlexVPN and DMVPN use the new key management protocol
C. FlexVPN and DMVPN use the same hashing algorithms
D. IOS routers run the same NHRP code for DMVPN and FlexVPN

Answer: D

Explanation:

In its essence, FlexVPN is the same as DMVPN. Connections between devices are still point-to-point GRE tunnels, spoke-to-spoke connectivity is still achieved with NHRP redirect message, IOS routers even run the same NHRP code for both DMVPN and FlexVPN, which also means that both are Cisco's proprietary technologies.
Reference: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/

www.atmicnetworks.com

Question: 31

[Security Concepts]
The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

A. SDN controller and the cloud
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the management solution

Answer: D

Explanation:

Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability1. The management solution is an example of an application that can use the northbound APIs to interact with the SDN controller and configure, monitor, and troubleshoot the network devices and services2. Therefore, the main function of northbound APIs in the SDN architecture is to enable communication between the SDN controller and the management solution. Reference: 1: What are SDN Northbound APIs (and SDN Rest APIs)? - SDxCentral 2: Software-Defined Networking Security and Network Programmability

Question: 32

[Security Concepts]
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two)

A. accounting
B. assurance
C. automation
D. authentication
E. encryption

Answer: B,C

Explanation:

What Cisco DNA Center enables you to do
Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours.
Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent.

Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere,

providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes.

Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco® solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices.

Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna- center/nb-06- cisco-dna-center-aag-cte-en.html

Question: 33

[Security Concepts]

Which functions of an SDN architecture require southbound APIs to enable communication?

A. SDN controller and the network elements
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the cloud

Answer: A

Explanation:

The Southbound API is used to communicate between Controllers and network devices

Question: 34

[Security Concepts]

Which API is used for Content Security?

A. NX-OS API
B. IOS XR API
C. OpenVuln API
D. AsyncOS API

www.atmicnetworks.com

Answer: D

Explanation:

Content Security is a term that encompasses various security features and solutions that protect the data and applications from threats such as malware, ransomware, phishing, data loss, and unauthorized access. Content Security includes products such as Cisco Email Security, Cisco Web Security, Cisco Cloudlock, and Cisco Umbrella. These products use the AsyncOS API, which is a RESTful API that allows administrators and developers to programmatically interact with the content security appliances and services. The AsyncOS API enables tasks such as configuration, reporting, monitoring, troubleshooting, and automation of content security policies and actions. The AsyncOS API is based on the HTTP protocol and uses JSON or XML as the data format. The AsyncOS API also supports authentication, authorization, rate limiting, and error handling mechanisms. The AsyncOS API documentation provides the details of the available resources, methods, parameters, and responses for each content security product. Reference :=
Cisco Content Security Products
AsyncOS API Overview
AsyncOS API Documentation
1: https://www.cisco.com/c/en/us/products/security/content-security/index.html 2:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13- 0/API/b_ESA_API_13_0_1/b_ESA_API_13_0_1_chapter_01.html 3:
https://developer.cisco.com/docs/email-security/#!asyncos-api-overview

Question: 35

[Security Concepts]
Which two request of REST API are valid on the Cisco ASA Platform? (Choose two)

A. put
B. options
C. get
D. push
E. connect

Answer: A,C

Explanation:

The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology.

All API requests are sent over HTTPS to the ASA, and a response is returned.
Request Structure
Available request methods are:
GET – Retrieves data from the specified object.
PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.

POST – Creates the object with the supplied information.

DELETE – Deletes the specified object

PATCH – Applies partial modifications to the specified object.

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

Question: 36

[Security Concepts] Refer to the exhibit.

```
def add_device_to_dnac(dnac_ip, device_ip, snmp_version,
    snmp_ro_community, snmp_rw_community,
    snmp_retry, snmp_timeout,
    cli_transport, username, password, enable_password):
    device_object = {
        'ipAddress': [
            device_ip
        ],
       'type': 'NETWORK_DEVICE',
        'computeDevice': False,
        'snmpVersion': snmp_version,
        'snmpROCommunity': snmp_ro_community,
        'snmpRWCommunity': snmp_rw_community,
        'snmpRetry': snmp_retry,
        'snmpTimeout': snmp_timeout,
        'cliTransport': cli_transport,
        'userName': username,
        'password': password,
        'enablePassword': enable_password
    }
    response = requests.post(
        'https://{}/dna/intent/api/v1/network-
device'.format(dnac_ip),
        data=json.dumps(device_object),
        headers={
            'X-Auth-Token': '{}'.format(token),
       "     'Content-type': 'application/json'
        },
        verify=False
    )
    return response.json()
```

What is the result of this Python script of the Cisco DNA Center API?

A. adds authentication to a switch
B. adds a switch to Cisco DNA Center
C. receives information about a switch
D. deletes a switch from Cisco DNA Center

www.atmicnetworks.com

Answer: C

Explanation:

The Python script of the Cisco DNA Center API in the exhibit uses the requests module to send a GET request to the /dna/intent/api/v1/network-device endpoint, which returns a list of network devices managed by Cisco DNA Center. The script also uses HTTPBasicAuth to provide the username and password for authentication. The script then parses the JSON response and prints the hostname, type, management IP address, and software version of each device in a table format using the prettytable module. Therefore, the result of this script is to receive information about a switch or switches from Cisco DNA Center. Reference:

Python Scripting APIs in Cisco DNA Center Let You Improve Effectiveness, Topic: Network device's script, simple and easy to create

Intro to Cisco DNA Center REST API with Python, Module 2: Using Python to Retrieve a Network Device List

Cisco DNA Center API Call Python Script Example, Topic: Cisco DNA CENTER SANDBOX Call DNA Center API Call Python Script Example

Question: 37

[Security Concepts] Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'

url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))

response_json = response.json()

for computer in response_json['data']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

What does the API do when connected to a Cisco security appliance?

A. get the process and PID information from the computers in the network
B. create an SNMP pull mechanism for managing AMP
C. gather network telemetry information from AMP for endpoints
D. gather the network interface information about the computers AMP sees

Answer: D

Explanation:

The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees.

Reference: https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1

Question: 38

[Security Concepts]

Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention System?

A. Security Intelligence
B. Impact Flags
C. Health Monitoring
D. URL Filtering

Answer: C

Explanation:

A network discovery policy is required for the health monitoring feature on the Cisco Firepower Next Generation Intrusion Prevention System (NGIPS). Health monitoring allows the system to collect and display information about the health and performance of the managed devices, such as CPU, memory, disk, and interface utilization, as well as the status of various processes and services. Health monitoring also enables the system to generate alerts and notifications when certain thresholds or conditions are met or violated.

To enable health monitoring, the system must have access to the network data from the managed devices, which is provided by the network discovery policy. The network discovery policy controls how the system collects data on the network assets and which network segments and ports are monitored. The network discovery policy also specifies the zones to which the policy is deployed, which determines the scope of the health monitoring data. Without a network discovery policy, the system cannot perform health monitoring on the NGIPS devices.

Reference :=

1: Network Discovery Policies, Cisco Firepower Management Center Configuration Guide, Version 7.0, page 1. 2: Health Monitoring, Cisco Firepower Management Center Configuration Guide, Version 7.0, page 1.

Question: 39

[Security Concepts]

Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two)

A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
B. Cisco FTDv with one management interface and two traffic interfaces configured
C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
D. Cisco FTDv with two management interfaces and one traffic interface configured
E. Cisco FTDv configured in routed mode and IPv6 configured

www.atmicnetworks.com

Answer: A,C

Explanation:

Cisco FTDv in AWS can be deployed in two different deployment models: single-instance and cluster. In both models, the FTDv can be configured in routed mode and managed by either an FMCv installed in AWS or a physical FMC appliance on premises. The FTDv can also use Geneve encapsulation for traffic interfaces to support AWS Gateway Load Balancer (GWLB) integration. The following table summarizes the supported deployment model configurations for FTDv in AWS: Table

Deployment Model
Management Mode
Traffic Mode
Geneve Encapsulation
Single-instance
FMCv in AWS
Routed
Optional
Single-instance
FMC on premises
Routed
Optional
Cluster
FMCv in AWS
Routed
Required
Cluster
FMC on premises
Routed
Required

Reference :=

Deploy the Threat Defense Virtual on AWS - Cisco
Deploy a Threat Defense Virtual Cluster on AWS - Cisco
Configure Geneve Interfaces in Secure FTDv - Cisco
Deployment of Cisco Secure FTDv and FMCv instances in AWS - Terraform
Solved: FTD virtual appliance in AWS - Cisco Community

Question: 40

[Security Concepts]

Which option is the main function of Cisco Firepower impact flags?

A. They alert administrators when critical events occur.
B. They highlight known and suspected malicious IP addresses in reports.
C. They correlate data about intrusions and vulnerability.
D. They identify data that the ASA sends to the Firepower module.

Answer: C

Explanation:

Cisco Firepower impact flags are indicators that help you evaluate the impact an intrusion has on your network by correlating intrusion data, network discovery data, and vulnerability information1. Impact flags are assigned to intrusion events based on the following criteria:
The operating system and application protocol of the target host
The exploitability of the target host by the attacker
The relevance of the intrusion rule to the target host
The severity of the intrusion rule Impact flags can have four values: unknown, neutral, affected, or vulnerable. Unknown means that the system does not have enough information to assess the impact. Neutral means that the system knows the target host is not affected by the intrusion. Affected means that the system knows the target host is affected by the intrusion, but not necessarily exploitable. Vulnerable means that the system knows the target host is exploitable by the intrusion1. Impact flags can help you prioritize your response to intrusion events, as well as generate reports and alerts based on the impact level. You can also use impact flags to filter and search for intrusion events in the Firepower Management Center1. Reference: 1: Firepower Management Center Configuration Guide, Version 6.1 - External Alerting with Alert Responses.

Question: 41

[Security Concepts]
On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?

A. health policy
B. system policy
C. correlation policy
D. access control policy
E. health awareness policy

Answer: A

Explanation:

On Cisco Firepower Management Center, a health policy is used to collect health modules alerts from managed devices. A health policy is a collection of tests, or health modules, that monitor the health status of the hardware and software in the system. You can apply a health policy to one or more appliances and configure the frequency and conditions for running the health modules and generating alerts. The health monitor on the Firepower Management Center tracks the health events based on the health policy settings and displays them on the Health Monitor page and the event views. You can also use external alerting mechanisms, such as SNMP traps or syslog messages, to notify you of health events. Reference := https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Health_Monitoring.htmlhttps://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/710/management-center-admin-71/health-health.html

www.atmicnetworks.com

Question: 42

[Security Concepts]
Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion Prevention System?

A. control
B. malware
C. URL filtering
D. protect

Answer: D

Explanation:

Cisco Security Intelligence is a feature that allows you to block or monitor traffic based on IP addresses or domain names that are known to be malicious or suspicious. Cisco Security Intelligence requires a Protect license on the Cisco Next Generation Intrusion Prevention System (NGIPS), which is part of the Firepower Threat Defense (FTD) software. A Protect license allows you to perform intrusion detection and prevention, file control, and Security Intelligence filtering1. The other license options (control, malware, and URL filtering) do not enable Cisco Security Intelligence on the NGIPS.

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, section "Security Intelligence"
Firepower Management Center Configuration Guide, Version 6.0, section "Licensing the Firepower System"

Question: 43

[Security Concepts]
Which two are valid suppression types on a Cisco Next Generation Intrusion Prevention System? (Choose two)

A. Port
B. Rule
C. Source
D. Application
E. Protocol

Answer: A,B

Explanation:

Suppression is a feature of Cisco Next Generation Intrusion Prevention System (NGIPS) that allows you to reduce false positives and unwanted alerts by filtering out specific traffic from the intrusion detection and prevention process. You can

www.atmicnetworks.com

configure suppression based on different criteria, such as port, rule, source, destination, and network. The two valid suppression types for this question are port and rule. Port suppression allows you to exclude traffic based on the source or destination port number, or both. For example, you can suppress alerts for port 80 (HTTP) traffic if you are not interested in web-based attacks. Rule suppression allows you to exclude traffic based on the rule ID (SID) or the rule category. For example, you can suppress alerts for rules that belong to the policyviolations category if you are not concerned about them. You can also suppress alerts for specific rules that are not relevant to your network or generate too many false positives. Reference

Question: 44

[Security Concepts]
Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

A. quality of service
B. time synchronization
C. network address translations
D. intrusion policy

Answer: B

Explanation:

Time synchronization is one of the features that can be configured for managed devices in the device platform settings of the Firepower Management Center (FMC). Time synchronization ensures that the FMC and its managed devices have the same date and time settings, which is important for accurate event logging and reporting. The FMC can act as a Network Time Protocol (NTP) server for its managed devices, or it can use an external NTP server as a time source1. The FMC can also synchronize its time with the system clock of the device where it is installed2. Reference := 1: Firepower Management Center Device Configuration Guide, 7.1 - Platform Settings 2: Firepower Management Center Configuration Guide, Version 6.6 - Device Management Basics

Question: 45

[Security Concepts]
Which information is required when adding a device to Firepower Management Center?

A. username and password
B. encryption method
C. device serial number
D. registration key

www.atmicnetworks.com

Answer: D

Explanation:

When adding a device to Firepower Management Center, you need to provide a registration key, which is a unique alphanumeric string that you create and enter on both the device and the Firepower Management Center. The registration key is used to authenticate the device and the Firepower Management Center to each other. You do not need to provide the username and password, encryption method, or device serial number when adding a device to Firepower Management Center1. Reference: 1: How to Manage a Device with the Firepower Management Center - Configure the Managed Device

Question: 46

[Security Concepts]
Which two deployment modes does the Cisco ASA FirePower module support? (Choose two)

A. transparent mode
B. routed mode
C. inline mode
D. active mode
E. passive monitor-only mode

Answer: C,D

Explanation:

You can configure your ASA FirePOWER module using one of the following deployment models:
You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa- firewall-asdm/modules-sfr.html

Question: 47

[Security Concepts]
The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?

A. Certificate Trust List
B. Endpoint Trust List
C. Enterprise Proxy Service
D. Secured Collaboration Proxy

Answer: A

Explanation:

The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. This means that the ASA acts as a proxy between the Cisco IP Phone and the Cisco Unified Communications Manager (UCM), decrypting, inspecting, and re-encrypting the voice signaling traffic. To do this, the ASA needs to have the certificates of the devices that the phone trusts, such as the UCM servers and the TFTP servers. These certificates are stored in a Certificate Trust List (CTL) file that the phone downloads from the UCM before registration. Therefore, the ASA must be added to the CTL file on the UCM platform, so that the phone can verify the identity of the ASA as a proxy. The other options are not relevant for this scenario. The Endpoint Trust List is a list of certificates that the UCM trusts for encrypted endpoints. The Enterprise Proxy Service is a feature that allows the UCM to route calls to and from the public switched telephone network (PSTN) through a SIP proxy server. The Secured Collaboration Proxy is a feature that allows the UCM to encrypt the media streams between endpoints using Secure Real-Time Transport Protocol (SRTP). Reference := Cisco Secure Firewall ASA Unified Communications Guide - TLS Proxy for Encrypted Voice Inspection TLS Proxy for Encrypted Voice Inspection - Cisco

Where must the ASA be added on the Cisco UC Manager platform?

Question: 48

[Security Operations]

Which statement about the configuration of Cisco ASA NetFlow v9 Secure Event Logging is true?

A. To view bandwidth usage for NetFlow records, the QoS feature must be enabled.
B. A sysopt command can be used to enable NSEL on a specific interface.
C. NSEL can be used without a collector configured.
D. A flow-export event type must be defined under a policy

Answer: D

Explanation:

Cisco ASA NetFlow v9 Secure Event Logging (NSEL) is a security logging mechanism that is built on NetFlow Version 9 technology and provides stateful, IP flow tracking for significant events in a flow. NSEL requires a collector to receive and process the exported data records. To configure NSEL, you need to define a flow-export event type under a policy using the Modular Policy Framework (MPF). The event type specifies which events to export, such as flow-create, flow-denied, flow-teardown, flow-update, or all. You also need to configure the NSEL collectors, the template timeout intervals, and the flow-update interval. Optionally, you can disable the redundant syslog messages and reset the runtime counters.

The other statements are false because:

To view bandwidth usage for NetFlow records, the QoS feature is not required. You can use a NetFlow collector or analyzer to view the bandwidth usage and other statistics from the exported data records.

A sysopt command cannot be used to enable NSEL on a specific interface. NSEL is enabled globally on all interfaces by default when you configure a flow-export event type under a policy.

NSEL cannot be used without a collector configured. NSEL exports data records to the configured collectors using NetFlow over UDP. If no collector is configured, the data records are discarded. Reference:

NetFlow Secure Event Logging (NSEL) - Cisco, Topic: Configuring NSEL, page 48-5

Cisco Secure Firewall ASA NetFlow Implementation Guide, Topic: Configure NSEL Collectors (CLI), Configure Flow-Export

Actions Through Modular Policy Framework, Configure Template Timeout Intervals, Change the Time Interval for Sending Flow-Update Events to a Collector, Disable and Reenable NetFlow-related Syslog Messages, Reset Runtime Counters Configuring NetFlow on ASA with ASDM - Cisco Community, Topic: Enable NetFlow (ASDM)

Question: 49

[Securing the Cloud]
Which feature is supported when deploying Cisco ASAv within AWS public cloud?

A. multiple context mode
B. user deployment of Layer 3 networks
C. IPv6
D. clustering

Answer: B

Explanation:

The ASAv on AWS supports the following features:

+ Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instance family.
+ Deployment in the Virtual Private Cloud (VPC)
+ Enhanced networking (SR-IOV) where available
+ Deployment from Amazon Marketplace
+ Maximum of four vCPUs per instance
+ User deployment of L3 networks
+ Routed mode (default)

Note: The Cisco Adaptive Security Virtual Appliance (ASAv) runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public AWS cloud.
It can then be configured to protect virtual and physical data center workloads that expand, contract, or shift their location over time. Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96 qsg/asavaws.html

Question: 50

[Security Concepts]
Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

A. It allows traffic if it does not meet the profile.
B. It defines a traffic baseline for traffic anomaly deduction.
C. It inspects hosts that meet the profile with more intrusion rules.
D. It blocks traffic if it does not meet the profile.

Answer: B

Explanation:

A traffic profile is a graph of network traffic based on connection data collected over a profiling time window (PTW). This measurement presumably represents normal network traffic. After the learning period, you can detect abnormal network traffic by evaluating new traffic against your profile. You
can also set up inactive periods in traffic profile to exclude data that does not reflect normal network behavior. You can use traffic profiles to write correlation rules that trigger when the traffic deviates from the profile by a certain threshold or standard deviation. This way, you can identify and respond to potential attacks or security policy violations that cause traffic anomalies. Reference := Some possible references are:
Firepower Management Center Configuration Guide, Version 6.0 - Traffic Profiling
Cisco Next-Generation Intrusion Prevention System (NGIPS)
Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

Question: 51

[Network Security]
Which statement about IOS zone-based firewalls is true?

A. An unassigned interface can communicate with assigned interfaces
B. Only one interface can be assigned to a zone.
C. An interface can be assigned to multiple zones.
D. An interface can be assigned only to one zone.

Answer: D

Explanation:

IOS zone-based firewalls (ZBFW) are a feature that provides stateful firewall policies between groups of interfaces known as zones. A zone is a logical grouping of one or more interfaces that have similar security requirements. A zone can be applied to physical interfaces, subinterfaces, port channels, VLAN interfaces, or tunnel interfaces. However, an interface can be assigned only to one zone, and it cannot be shared between zones. This is because the ZBFW policy is applied between zones, not interfaces, and it controls the bidirectional traffic flow between them. Therefore, an interface can belong to only one zone at a time, and it must be removed from one zone before it can be added to another zone. This ensures that the firewall policy is consistent and unambiguous for each interface. Reference := Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS XE Gibraltar 16.12.x, Configuring Zones
Understand the Zone-Based Policy Firewall Design, Zone-Based Policy Overview
IOS Zone Based Firewall Step-by-Step Basic Configuration, Zone Based Firewall Vs CBAC

Question: 52

[Security Operations]

What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

A. It tracks flow-create, flow-teardown, and flow-denied events.
B. It provides stateless IP flow tracking that exports all records of a specific flow.
C. It tracks the flow continuously and provides updates every 10 seconds.
D. Its events match all traffic classes in parallel.

Answer: A

Explanation:

The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs).
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa- general-cli/ monitor-nsel.html

Question: 53

[Security Concepts]
Which CLI command is used to register a Cisco FirePower sensor to Firepower Management Center?

A. configure system add <host><key>
B. configure manager <key> add host
C. configure manager delete
D. configure manager add <host><key

Answer: D

Explanation:

a Cisco FirePower sensor to Firepower Management Center is configure manager add <host><key>. This command establishes a secure connection between the sensor and the FMC using a registration key. The <host> parameter can be either the IP address or the hostname of the FMC.
The <key> parameter can be any alphanumeric string that matches the one configured on the FMC. This command is executed on the sensor's CLI in the privileged EXEC mode12. Reference: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) course, Module 2: Network Security, Lesson 2: Deploying Cisco Firepower Next-Generation Firewall, Topic: Registering the Cisco Firepower NGFW to the FMC2: Firepower Management Center Configuration Guide, Version 6.6 - Device Management Basics [Cisco Secure Firewall Management Center] - Cisco.

Question: 54

[Security Concepts]

Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

A. Correlation
B. Intrusion
C. Access Control
D. Network Discovery

Answer: D

Explanation:

The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible.
You can configure your network discovery policy to perform host and application detection.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html

Question: 55

[Security Concepts]
Which ASA deployment mode can provide separation of management on a shared appliance?

A. DMZ multiple zone mode
B. transparent firewall mode
C. multiple context mode
D. routed mode

Answer: C

Explanation:

Question: 56

[Security Concepts] Refer to the exhibit.

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*   0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C        1.1.1.0 255.255.255.0 is directly connect, outside
S        172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C        192.168.100.0 255.255.255.0 is directly connected, inside
C        172.16.10.0 255.255.255.0 is directly connected, dmz
S          10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz
```

```
access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
 sfr fail-open

service-policy inside-policy global
```

What is a result of the configuration?

A. Traffic from the DMZ network is redirected
B. Traffic from the inside network is redirected
C. All TCP traffic is redirected
D. Traffic from the inside and DMZ networks is redirected

Answer: D

Explanation:

The purpose of above commands is to redirect traffic that matches the ACL “redirect-acl” to the Cisco FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission.

The command “service-policy global_policy global” applies the policy to all of the interfaces.

Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-

configurefirepower-00.html

Question: 57

[Security Concepts]
Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

A. Group Policy
B. Access Control Policy
C. Device Management Policy
D. Platform Service Policy

Answer: D

Explanation:

Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features.
A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device. For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc- configguide-v62/platform_settings_policies_for_managed_devices.htmlTherefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the bestanswer here so we have to choose it.

Question: 58

[Network Security]
Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two)

A. Enable NetFlow Version 9.
B. Create an ACL to allow UDP traffic on port 9996.
C. Apply NetFlow Exporter to the outside interface in the inbound direction.
D. Create a class map to match interesting traffic.
E. Define a NetFlow collector by using the flow-export command

www.atmicnetworks.com

Answer: A,E

Explanation:

NetFlow is a protocol that collects and exports information about network traffic flows. NetFlow Version 9 is the latest version supported by the Cisco ASA 5500 Series firewall. To enable NetFlow on the ASA, you need to perform two main tasks: define a NetFlow collector and apply NetFlow exporter to an interface. A NetFlow collector is a device or application that receives and processes the NetFlow records sent by the ASA. You can define a NetFlow collector by using the flow-export command, which specifies the IP address, port number, and interface of the collector. A NetFlow exporter is a configuration that determines which traffic flows are monitored and exported by the ASA. You can apply NetFlow exporter to an interface by using the Modular Policy Framework (MPF), which allows you to create class maps and policy maps to match and act on interesting traffic. You can use the flow-export event-type option in the policy map to select the NetFlow events that you want to export. The other options (B, C, and D) are not required or correct for enabling NetFlow on the ASA. You do not need to create an ACL to allow UDP traffic on port 9996, because the ASA uses a random high port number to send NetFlow records to the collector. You do not need to apply NetFlow exporter to the outside interface in the inbound direction, because you can apply it to any interface and direction that you want to monitor. You do not need to create a class map to match interesting traffic, because the ASA monitors all traffic flows by default, unless you filter them by using the flow-export filters command. Reference:

Cisco Secure Firewall ASA NetFlow Implementation Guide, section “About NSEL”

Cisco Secure Firewall ASA NetFlow Implementation Guide, section “Configure NSEL Collectors (CLI)” Cisco Secure Firewall ASA NetFlow Implementation Guide, section “Configure Flow-Export Actions Through Modular Policy Framework”

Configuring NetFlow on ASA with ASDM, section “Enabling NetFlow on ASA”

Question: 59

[Security Concepts]

A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?

A. routed mode
B. transparent mode
C. multiple context mode
D. multiple zone mode

Answer: C

Explanation:

Multiple context mode allows you to partition a single ASA into multiple virtual firewalls, each with its own security policy, interfaces, and management IP address. This mode is useful for providing security services to different customers or tenants on a shared appliance, while maintaining separation of management and configuration. Each context acts as an independent device and can be in either routed or transparent mode. You can also assign different administrators to each context and limit their access to specific commands and features. Multiple context mode is supported in Cisco ACI with the ASA device package version 1.2 or later. Reference:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/L4-

www.atmicnetworks.com

L7_Service_Graph_Deployment_Guide/b_L4L7_Service_Graph_Deploy_ver122g/b_L4L7_Service_Graph_Deploy_ver122x_chapter_0110.pdf

https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config/intro-fw.html

Question: 60

[Security Concepts]

What is a characteristic of Firepower NGIPS inline deployment mode?

A. ASA with Firepower module cannot be deployed.
B. It cannot take actions such as blocking traffic.
C. It is out-of-band from traffic.
D. It must have inline interface pairs configured.

Answer: D

Explanation:

Firepower NGIPS inline deployment mode is a mode where the NGIPS device is placed in the traffic path and can take actions such as blocking, modifying, or redirecting traffic based on the policies and rules. In this mode, the NGIPS device must have inline interface pairs configured, which are pairs of physical or logical interfaces that act as a single logical interface. The inline interface pairs are connected to the network devices on both sides of the NGIPS device, and the traffic flows through the NGIPS device from one interface to the other. The NGIPS device can inspect and modify the traffic as it passes through the inline interface pairs12. Reference := 1: Firepower Management Center Configuration Guide, Version 6.6 - Device Management Basics 2: Configure FTD Interfaces in Inline-Pair Mode

Question: 61

[Security Operations]

An engineer wants to generate NetFlow records on traffic traversing the Cisco AS A. Which Cisco ASA command must be used?

A. flow-export destination inside 1.1.1.1 2055
B. ip flow monitor input
C. ip flow-export destination 1.1.1.1 2055
D. flow exporter

Answer: A

Explanation:

www.atmicnetworks.com

The syntax of this command is: flow-export destination interface-name ipv4-address | hostname udp-port

This command is used on Cisco ASA to configure Network Secure Event Logging (NSEL) collector to which NetFlow packets are sent. The destination keyword indicates that a NSEL collector is being configured.

+ The interface-name argument is the name of the ASA and ASA Services Module interface through which the collector is reached.
+ The ipv4-address argument is the IP address of the machine running the collector application.
+ The hostname argument is the destination IP address or name of the collector.
+ The udp-port argument is the UDP port number to which NetFlow packets are sent.

You can configure a maximum of five collectors. After a collector is configured, template records are automatically sent to all configured NSEL collectors.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.html

Question: 62

[Security Concepts]
How many interfaces per bridge group does an ASA bridge group deployment support?

A. up to 2
B. up to 4
C. up to 8
D. up to 16

Answer: B

Explanation:

Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router.

As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces.

Up to 4 interfaces are permitted per bridge–group (inside, outside, DMZ1, DMZ2)

Question: 63

[Security Concepts]
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two)

A. packet decoder
B. SIP

C. modbus
D. inline normalization
E. SSL

Answer: B,E

Explanation:

Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080cFirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

Question: 64

[Security Concepts]
Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)

A. Time-based one-time passwords
B. Data loss prevention
C. Heuristic-based filtering
D. Geolocation-based filtering
E. NetFlow

Answer: B,D

Explanation:

Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution.

Cisco Email Security appliance can now handle incoming mail connections and incoming messages from specific geolocations and perform appropriate actions on them, for example:
– Prevent email threats coming from specific geographic regions.
– Allow or disallow emails coming from specific geographic regions.

Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.html

www.atmicnetworks.com

Question: 65

[Content Security]
Why would a user choose an on-premises ESA versus the CES solution?

A. Sensitive data must remain onsite.
B. Demand is unpredictable.
C. The server team wants to outsource this service.
D. ESA is deployed inline.

Answer: A

Explanation:

One of the main reasons why a user would choose an on-premises ESA versus the CES solution is to have more control over the sensitive data that flows through the email system. With an on-premises ESA, the user can ensure that the data is stored and processed within their own network and data center, and that they comply with any regulatory or organizational requirements for data security and privacy. With a CES solution, the user would have to trust Cisco to handle the data in their cloud infrastructure, and to adhere to the service level agreements and security policies that are agreed upon. Some users may not be comfortable with this level of outsourcing, especially if they have strict data governance or compliance needs12. Reference: 1: Physical ESA vs Cloud ESA - Cisco Community 2: Cisco Email Security Appliance - Data Sheet

Question: 66

[Content Security]
Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two)

A. Sophos engine
B. white list
C. RAT
D. outbreak filters
E. DLP

Answer: A,D

Explanation:

Cisco ESA uses a multilayer approach to fight viruses and malware. The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. Outbreak filters use global threat intelligence and behavioral analysis to identify and block emerging threats before they reach the network. The second layer of defense consists of antivirus engines, which scan the message body and attachments for known viruses and malware. Cisco ESA supports multiple antivirus engines, such as Sophos, McAfee, and Cisco AMP. The Sophos engine is one of the default engines that Cisco ESA uses, along with McAfee. The Sophos engine provides fast and accurate detection of viruses and malware, and updates its signatures frequently. The other options are not features that are used to configure Cisco ESA with a

multilayer approach to fight viruses and malware. A white list is a list of trusted senders or recipients that are exempt from spam or virus filtering. RAT is the Recipient Access Table, which is used to determine whether the appliance accepts or rejects messages to a recipient address. DLP is Data Loss Prevention, which is used to prevent sensitive or confidential data from leaving the network. Reference :=

Email Security Using Cisco ESA
Demystifying Cisco ESA HAT, RAT Tables and Deployment Types
Email Security Deployment Guide - Cisco

Question: 67

[Content Security]
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

A. It decrypts HTTPS application traffic for unauthenticated users.
B. It alerts users when the WSA decrypts their traffic.
C. It decrypts HTTPS application traffic for authenticated users.
D. It provides enhanced HTTPS application detection for AsyncOS.

Answer: D

Explanation:

The Decrypt for Application Detection feature within the WSA Decryption options enhances the ability of AsyncOS to detect HTTPS applications. The HTTPS Proxy can decrypt HTTPS connections to web applications. This allows the Application Visibility and Control (AVC) engine to more accurately detect and block web applications that use HTTPS. This feature can help improve the security and performance of the network by identifying and controlling the usage of web applications that may consume bandwidth, pose security risks, or violate compliance policies.
Reference:
WSA decryption options - Cisco Community, Topic: Decrypt for Application Detection
User Guide for AsyncOS 11.7 for Cisco Web Security Appliances - GD (General Deployment) - Create Decryption Policies to Control HTTPS Traffic, Topic: Overview of Create Decryption Policies to Control HTTPS Traffic, Decryption for Application Detection

Question: 68

[Content Security]
Which two statements about a Cisco WSA configured in Transparent mode are true? (Choose two)

A. It can handle explicit HTTP requests.
B. It requires a PAC file for the client web browser.
C. It requires a proxy for the client web browser.
D. WCCP v2-enabled devices can automatically redirect traffic destined to port 80.
E. Layer 4 switches can automatically redirect traffic destined to port 80.

www.atmicnetworks.com

Answer: A,D

Explanation:

In transparent mode, the WSA can handle both explicit and transparent HTTP requests, depending on how the client browser is configured. The WSA must pretend to be the origin content server for transparent requests, since the client is unaware of the existence of a proxy1. WCCP v2 is a protocol that allows a WCCP-enabled device (such as a router or a switch) to redirect traffic to the WSA based on certain criteria, such as destination port 802. This way, the client does not need to configure a proxy or a PAC file in the browser. The other options are false because they are either required for explicit mode or not supported by the WSA. Reference :=
What is the difference between transparent and forward proxy mode?
Configure Transparent Redirection With WCCP in Order to Support HTTP, HTTPS, and Native FTP Traffic

Question: 69

[Content Security]
Which action controls the amount of URI text that is stored in Cisco WSA logs files?

A. Configure the datasecurityconfig command
B. Configure the advancedproxyconfig command with the HTTPS subcommand
C. Configure a small log-entry size.
D. Configure a maximum packet size.

Answer: C

Explanation:

The amount of URI text that is stored in Cisco WSA log files is controlled by the log-entry size parameter, which can be configured using the advancedproxyconfig command. The log-entry size parameter specifies the maximum number of bytes of the URI that will be logged for each request. The default value is 1024 bytes, but it can be changed to any value between 1 and 4096 bytes. If the URI is longer than the log-entry size, it will be truncated and a plus sign (+) will be appended to indicate that the URI was cut off. Configuring a small log-entry size can reduce the disk space and bandwidth consumption of the log files, but it can also limit the visibility and analysis of the requests. Reference :=
User Guide for AsyncOS 11.0 for Cisco Web Security Appliances, Customizing Access Logs Cisco WSA CLI Reference Guide for AsyncOS 11.0, advancedproxyconfig Command WSA FAQ: How can I view the logs on the Cisco WSA? - Cisco

Question: 70

[Content Security]
An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

A. SAT
B. BAT
C. HAT
D. RAT

Answer: D

Explanation:

The RAT (Recipient Access Table) is the list that contains the allowed recipient addresses on the Cisco ESA. The RAT controls whether the ESA accepts or rejects messages to a recipient address based on the sender group and the mail policy. The RAT can be configured to allow, relay, or reject messages to specific recipients or domains. The RAT can also be used to apply different message filters or content filters to different recipient groups12. Reference: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) course, Module 2: Network Security, Lesson 3: Deploying Cisco Email Security Appliance, Topic: Configuring Mail Policies2: Cisco Email Security Appliance User Guide, Release 13.5 - Configuring Mail Policies [Cisco Secure Email Gateway] - Cisco.

Question: 71

[Secure Network Access, Visibility, and Enforcement]
Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two)

A. DDoS
B. antispam
C. antivirus
D. encryption
E. DLP

Answer: D,E

Explanation:

Cisco Hybrid Email Security is a unique service offering that combines a cloud-based email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control – protecting sensitive information with data loss prevention (DLP) and encryption technologies.
Reference:
https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

www.atmicnetworks.com

Question: 72

[Security Concepts]
Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?

A. IP Blacklist Center
B. File Reputation Center
C. AMP Reputation Center
D. IP and Domain Reputation Center

Answer: D

Explanation:

The Talos IP and Domain Reputation Center is the world's most comprehensive real-time threat detection network. It collects and analyzes data from millions of web requests, emails, malware samples, open-source data sets, endpoint intelligence, and network intrusions. It assigns a reputation score to IP addresses and domains based on their observed malicious activity and behavior. The reputation score can range from -10 (very malicious) to +10 (very benign). The reputation score can be used to block or allow traffic, or to trigger further inspection or analysis. The Talos IP and Domain Reputation Center allows you to track the reputation of IP addresses for email and web traffic, as well as to look up the category, volume, and history of any IP address or domain. You can also submit feedback or request a change of reputation for any IP address or domain. Reference
https://talosintelligence.com/reputation_center/
https://bing.com/search?q=Talos+reputation+center+IP+addresses+email+web+traffic

Question: 73

[Content Security]
Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

A. transparent
B. redirection
C. forward
D. proxy gateway

Answer: A

Explanation:

There are two possible methods to accomplish the redirection of traffic to Cisco WSA: transparent proxy mode and explicit proxy mode.
In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who

manage Cisco WSA.

Reference:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCisco WSADesignGuide-AUG13.pdf

Question: 74

[Content Security]
After deploying a Cisco ESA on your network, you notice that some messages fail to reach their destinations. Which task can you perform to determine where each message was lost?

A. Configure the trackingconfig command to enable message tracking.
B. Generate a system report.
C. Review the log files.
D. Perform a trace.

Answer: A

Explanation:
Message tracking helps resolve help desk calls by giving a detailed view of message flow. For example, if a message was not delivered as expected, you can determine if it was found to contain a virus or placed in a spam quarantine — or if it is located somewhere else in the mail stream.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011110.html

Question: 75

[Content Security]
What is the primary benefit of deploying an ESA in hybrid mode?

A. You can fine-tune its settings to provide the optimum balance between security and performance for your environment
B. It provides the lowest total cost of ownership by reducing the need for physical appliances
C. It provides maximum protection and control of outbound messages
D. It provides email security while supporting the transition to the cloud

Answer: D

Explanation:

Cisco Hybrid Email Security is a unique service offering that facilitates the deployment of your email security

infrastructure both on premises and in the cloud. You can change the number of on-premises versus cloud users at any time throughout the term of your contract, assuming the total number of users does not change. This allows for deployment flexibility as your organization's needs change.

Question: 76

[Security Concepts]
What is the primary role of the Cisco Email Security Appliance?

A. Mail Submission Agent
B. Mail Transfer Agent
C. Mail Delivery Agent
D. Mail User Agent

Answer: B

Explanation:

Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay.

Reference:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf

Question: 77

[Security Concepts]
Which technology is used to improve web traffic performance by proxy caching?

A. WSA
B. Firepower
C. FireSIGHT
D. ASA

Answer: A

Explanation:

Proxy caching is a method that enables a proxy server to save recent and frequent website/webpage requests and data requested by one or more client machines. It reduces latency, eases bandwidth consumption, and ensures content is served more swiftly to the end-user12. WSA (Web Security Appliance) is a Cisco product that provides proxy caching functionality, along with other web security features such as malware protection, URL filtering, and data loss prevention3. Firepower, FireSIGHT, and ASA are other Cisco products that do not provide proxy caching, but rather focus on different aspects of network security, such as threat detection, management, and firewall . Reference: What is Proxy Caching? | StackPath

What Is Proxy Caching? | Definition & Overview | NinjaOne

Cisco Web Security Appliance Data Sheet

[Cisco Firepower NGFW Data Sheet]

[Cisco FireSIGHT Management Center Data Sheet]

[Cisco ASA 5500-X Series Firewalls Data Sheet]

Question: 78

[Content Security]

In which two ways does a system administrator send web traffic transparently to the Web Security Appliance? (Choose two)

A. configure Active Directory Group Policies to push proxy settings
B. configure policy-based routing on the network infrastructure
C. reference a Proxy Auto Config file
D. configure the proxy IP address in the web-browser settings
E. use Web Cache Communication Protocol

Answer: B,E

Explanation:

In order to send web traffic transparently to the Web Security Appliance (WSA), the system administrator can use one of these two methods:

Policy-based routing (PBR) on the network infrastructure: This method allows the administrator to define routing policies based on the source or destination IP address, port number, protocol, or other criteria of the web traffic. The administrator can then apply these policies to the network interfaces or subinterfaces and redirect the matching traffic to the WSA. This method does not require any configuration on the client side and can be applied to any type of web traffic, including HTTPS and FTP. However, this method may require additional network resources and maintenance, as well as coordination with other network administrators.

Web Cache Communication Protocol (WCCP) on the WSA and the network device: This method allows the administrator to configure the WSA and the network device (such as a router, switch, or firewall) to communicate with each other using WCCP, a Cisco proprietary protocol. The network device acts as a WCCP router and redirects the web traffic to the WSA, which acts as a WCCP client. The WSA then processes the traffic and returns it to the network device, which forwards it to the original destination. This method does not require any configuration on the client side and can be applied to HTTP,

HTTPS, and native FTP traffic. However, this method requires that the network device supports WCCP and that the WSA and the network device are in the same Layer 2 domain.

Question: 79

[Security Concepts]
Which technology reduces data loss by identifying sensitive information stored in public computing environments?

A. Cisco SDA
B. Cisco Firepower
C. Cisco HyperFlex
D. Cisco Cloudlock

Answer: D

Explanation:

Cisco Cloudlock is a cloud-native security platform that provides data loss prevention (DLP) capabilities for public cloud environments, such as SaaS, IaaS, and PaaS. Cisco Cloudlock can discover, classify, and protect sensitive data stored in cloud applications, such as Office 365, Google Workspace, Salesforce, Dropbox, and AWS. Cisco Cloudlock uses advanced techniques, such as regular expressions, keywords, dictionaries, and machine learning, to identify and monitor data based on predefined or custom policies. Cisco Cloudlock can also enforce actions, such as encryption, quarantine, deletion, or notification, to prevent data leakage or exposure12. Reference := 1: Cisco Cloudlock Data Sheet 2: Cloud Data Loss Prevention (Cloud DLP) Overview

Question: 80

[Security Concepts]
Which deployment model is the most secure when considering risks to cloud adoption?

A. Public Cloud
B. Hybrid Cloud
C. Community Cloud
D. Private Cloud

Answer: D

Explanation:

A private cloud is a cloud deployment model that is dedicated to a single organization and provides exclusive access to its resources and services. A private cloud can be hosted on-premises or off- premises by a third-party provider, but in either case, the organization has full control and visibility over the security, privacy, and compliance of its data and applications. A private cloud can also leverage the security features and best practices of the public cloud service provider, if applicable, while maintaining a higher degree of isolation and customization. A private cloud is the most secure deployment model when considering risks to cloud adoption, as it minimizes the exposure of sensitive data to external threats, reduces the dependency on the security posture of the cloud service provider, and enables the organization to meet its specific security and regulatory

requirements123. Reference: 1: Best Practices to Manage Risks in the Cloud - ISACA 2: Security in the Microsoft Cloud Adoption Framework for Azure 3: Five challenges to cloud adoption and how to overcome them - PwC Middle East

Question: 81

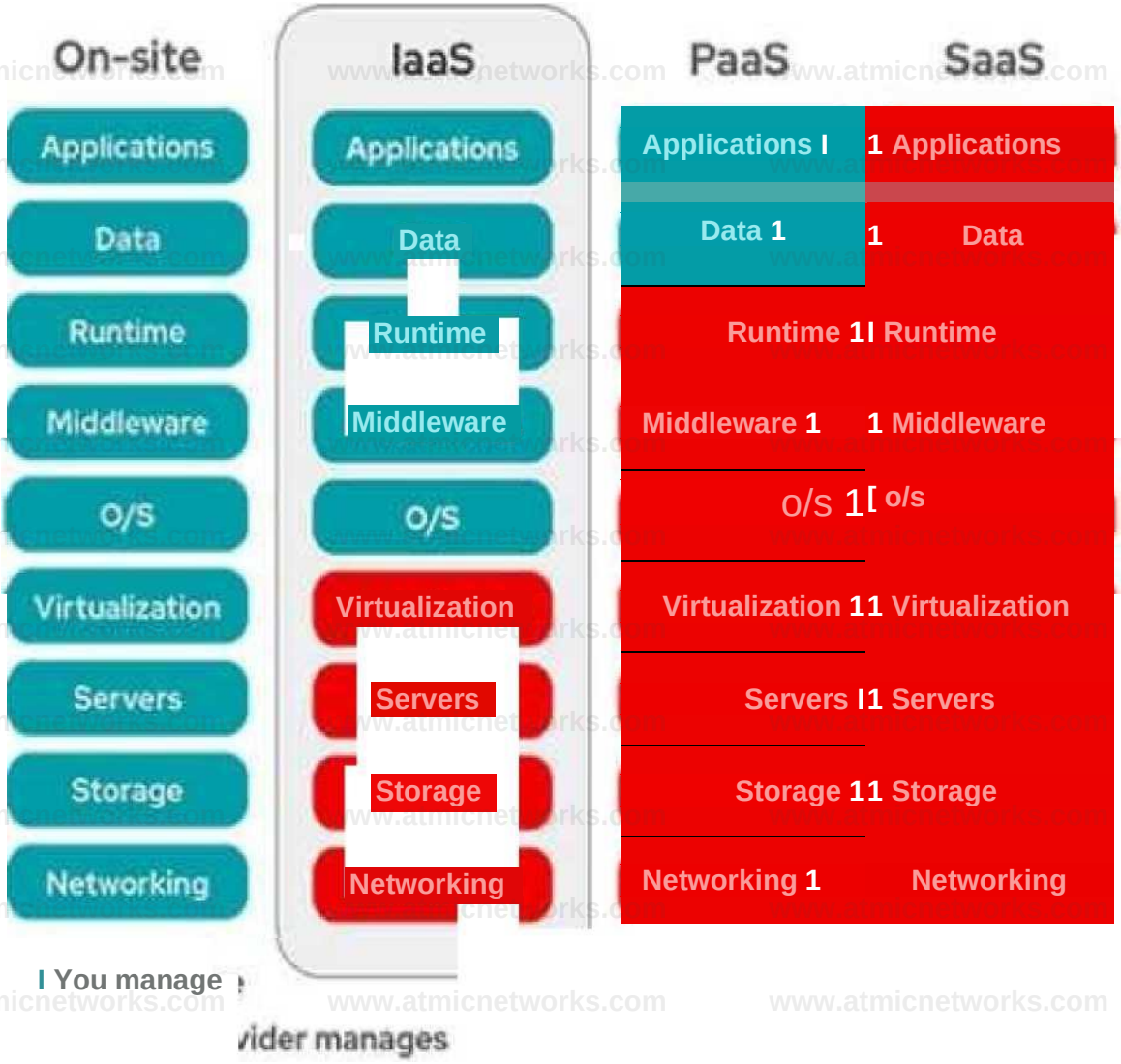
[Endpoint Protection and Detection]
In which cloud services model is the tenant responsible for virtual machine OS patching?

A. IaaS
B. UCaaS
C. PaaS
D. SaaS

Answer: A

Explanation:

Only in On-site (on-premises) and IaaS we (tenant) manage O/S (Operating System).



Question:
82

[Security Concepts]

Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

A. PaaS
B. XaaS
C. IaaS
D. SaaS

Answer:
A

Explanation:

Cloud computing can be broken into the following three basic models:
+ Infrastructure as a Service (IaaS): IaaS describes a cloud solution where you are renting infrastructure. You purchase virtual power to execute your software as needed. This is much like running a virtual server on your own equipment, except you are now running a virtual server on a virtual disk. This model is similar to a utility company model because you pay for what you use. + Platform as a Service (PaaS): PaaS provides everything except applications. Services provided by this
model include all phases of the system development life cycle (SDLC) and can use application programming interfaces (APIs), website portals, or gateway software. These solutions tend to be proprietary, which can cause problems if the customer moves away from the provider's platform. + Software as a Service (SaaS): SaaS is designed to provide a complete packaged solution. The software is rented out to the user. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a peruse fee.
Reference: CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide

Question: 83

[Network Security]
What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

A. It allows the administrator to quarantine malicious files so that the application can function, just notmaliciously.
B. It discovers and controls cloud apps that are connected to a company's corporate environment.
C. It deletes any application that does not belong in the network.
D. It sends the application information to an administrator to act on.

Answer: B

Explanation:

The Cloudlock Apps Firewall is a feature of Cisco Cloudlock, which is a cloud-native cloud access security broker (CASB) that helps organizations move to the cloud safely. The Cloudlock Apps Firewall mitigates security concerns from an application perspective by discovering and controlling cloud apps that are connected to a company's corporate environment, such as Google G Suite or Microsoft Azure Active Directory (AD). These cloud apps are authorized through OAuth to access corporate data and resources via APIs, and may pose risks such as data exfiltration, account compromise, or malicious behavior. The Cloudlock Apps Firewall provides visibility into the app ecosystem, including the app name, category, risk level, access scopes, and number of users. It also allows administrators to ban or allowlist apps based on their risk profile and compliance requirements. Additionally, the Cloudlock Apps Firewall leverages a crowd-sourced Community Trust Rating for each app, which reflects the feedback from other Cloudlock customers on the app's security and

functionality. Reference :=
Cisco Content Security Products
Cisco Cloudlock - Cisco

Question: 84

[Security Concepts]
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

A. Nexus
B. Stealthwatch
C. Firepower
D. Tetration

Answer: D

Explanation:

Tetration is the solution that protects hybrid cloud deployment workloads with application visibility and segmentation. Tetration enables a zero-trust model using segmentation, which allows you to identify security incidents faster, contain lateral movement, and reduce your attack surface. Tetration supports both on-premises and public cloud workloads and provides real-time telemetry data, behavior analysis, software inventory, and policy enforcement. Tetration is part of the Cisco Zero Trust portfolio, which also includes solutions for securing the workforce and workplace. Reference: Cisco Tetration Platform - Cisco, Topic: Cisco Tetration offers holistic workload protection for multicloud data centers by enabling a zero-trust model using segmentation.

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 5: Securing the Cloud, Lesson 5.3: Cloud Workload Security, Topic 5.3.1: Tetration
Cisco Zero Trust Tetration, Topic: Tetration provides zero-trust security for workloads as part of the Cisco Zero Trust portfolio.

Question: 85

[Securing the Cloud]
In a PaaS model, which layer is the tenant responsible for maintaining and patching?

A. hypervisor
B. virtual machine
C. network
D. application

Answer: D

Explanation:

In a PaaS model, the cloud provider is responsible for managing and maintaining the underlying infrastructure, such as the hypervisor, the virtual machine, and the network. The tenant only needs to focus on developing and deploying the application, which runs on the cloud platform. The tenant is responsible for ensuring the security and availability of the application, as well as applying any patches or updates to the application code or configuration12. Reference := Shared responsibility in the cloud
Best practices for secure PaaS deployments

Question: 86

[Security Concepts]
On which part of the IT environment does DevSecOps focus?

A. application development
B. wireless network
C. data center
D. perimeter network

Answer: A

Explanation:

DevSecOps is a development practice that integrates security into all phases of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery. DevSecOps focuses on application development, as it aims to deliver secure and robust applications that meet the customers' needs and expectations. DevSecOps also makes security a shared responsibility of development, security, and operations teams, rather than a separate silo. DevSecOps enables faster and safer software delivery by automating security processes and tools, and addressing security issues as they emerge, rather than at the end of the cycle.

Reference :=
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 6: Securing the Data Center, Lesson 6.2: DevSecOps
What Is DevSecOps? Definition and Best Practices | Microsoft Security
What is DevSecOps? | IBM
What is DevSecOps? | DevSecOps vs. DevOps | VMware

Question: 87

[Securing the Cloud]
What is the function of Cisco Cloudlock for data security?

A. data loss prevention
B. controls malicious cloud apps

C. detects anomalies
D. user and entity behavior analytics

Answer: A

Explanation:

The function of Cisco Cloudlock for data security is data loss prevention (DLP). Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cloudlock's simple, open, and automated approach uses APIs to manage the risks in your cloud app ecosystem1. One of the key features of Cloudlock is its DLP technology, which continuously monitors cloud environments to detect and secure sensitive information. It provides countless out-of-the-box policies as well as highly tunable custom policies. You can use Cloudlock's DLP to prevent data breaches, comply with regulations, and enforce data governance across SaaS, PaaS, and IaaS platforms2. Reference: 1: Cisco Cloudlock - Cisco2: Cloudlock: Cloud User Security - Cisco Umbrella.

Question: 88

[Content Security]
An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the
latest build of Windows 10.
What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

A. Cisco Identity Services Engine and AnyConnect Posture module
B. Cisco Stealthwatch and Cisco Identity Services Engine integration
C. Cisco ASA firewall with Dynamic Access Policies configured
D. Cisco Identity Services Engine with PxGrid services enabled

Answer: A

Explanation:

Cisco Identity Services Engine (ISE) and AnyConnect Posture module are the best solution to ensure that all endpoints are compliant before users are allowed access on the corporate network. ISE is a policy-based platform that provides secure network access, identity management, and endpoint compliance. AnyConnect Posture module is a component of the AnyConnect Secure Mobility Client that performs posture assessment and remediation on the endpoints. Together, they can enforce policies based on the endpoint's compliance status, such as the presence and update of the corporate antivirus application and the Windows 10 build version. The administrator can configure posture requirements, profiles, and policies on ISE, and deploy them to the endpoints through AnyConnect. The endpoints will then report their posture status to ISE, which will grant or deny network access accordingly, or redirect them to a remediation portal if needed. Reference :

Question: 89

[Endpoint Protection and Detection]

An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the
endpoint to apply a new or updated policy from ISE. Which CoA type achieves this goal?

A. Port Bounce
B. CoA Terminate
C. CoA Reauth
D. CoA Session Query

Answer: C

Explanation:

CoA (Change of Authorization) is a feature that allows ISE to dynamically change the authorization attributes of an endpoint after it has been authenticated. CoA can be triggered by various events, such as posture assessment, profiling, or manual intervention1. There are different types of CoA that ISE can send to the network access device (NAD) to perform different actions on the endpoint session. The CoA type that achieves the goal of forcing an endpoint to re-authenticate without disrupting its session is CoA Reauth. CoA Reauth instructs the NAD to initiate a new RADIUS authentication for the endpoint, which allows ISE to apply a new or updated policy based on the latest attributes of the endpoint2. The other CoA types do not achieve this goal, as they either disconnect the endpoint session or do not change the authorization attributes. Port Bounce causes the NAD to shut down and bring up the port where the endpoint is connected, which effectively disconnects and reconnects the endpoint session2. CoA Terminate causes the NAD to terminate the endpoint session and send an Accounting-Stop message to ISE2. CoA Session Query causes the NAD to send an Accounting-Request message to ISE with the current session information, but does not

change the authorization attributes of the endpoint2. Reference:
Cisco Content Hub - Manage Network Devices, section “CoA Types”
Solved: COA and ISE Clarification - Cisco Community, answer by Tarik Admani
Configuring Profiler Policies
[Cisco Identity Services Engine] - Cisco …, section “Change of Authorization”

Question: 90

[Endpoint Protection and Detection]

Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two)

A. RADIUS
B. TACACS+
C. DHCP

D. sFlow
E. SMTP

Answer: A,C

Explanation:

Cisco Identity Services Engine (ISE) uses various probes to collect attributes of connected endpoints, such as device type, operating system, IP address, MAC address, and so on. These attributes are used to profile the endpoints and assign them to appropriate identity groups and policies. Two of the probes that can be configured to gather attributes of connected endpoints using Cisco ISE are RADIUS and DHCP.
RADIUS probe: The RADIUS probe collects attributes from the RADIUS packets that are exchanged between the network access devices (NADs) and the ISE Policy Service Nodes (PSNs) during the authentication and authorization process. The RADIUS probe can extract attributes such as username, calling-station-ID, NAS-IP-address, NAS-port-type, service-type, and so on. The RADIUS probe can also collect attributes from the RADIUS accounting packets that are sent by the NADs to the ISE PSNs after the session is established. The RADIUS probe can extract attributes such as session-ID, framed-IP-address, acct-session-time, and so on. The RADIUS probe is enabled by default and does not require any additional configuration on the NADs or the ISE PSNs.
DHCP probe: The DHCP probe collects attributes from the DHCP packets that are exchanged between the endpoints and the DHCP server during the IP address assignment process. The DHCP probe can extract attributes such as hostname, vendor-class-identifier, client-identifier, parameter-request-list, and so on. The DHCP probe can also collect attributes from the DHCP relay packets that are forwarded by the NADs to the ISE PSNs. The DHCP probe can extract attributes such as relay-agent- information and subscriber-ID. The DHCP probe requires some configuration on the NADs and the ISE PSNs. The NADs must be configured to relay or copy the DHCP packets to the ISE PSNs, and the ISE PSNs must be configured to receive the DHCP packets on a specific interface.
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_assetvisibility_endpointprofiler.html
https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_00.html

Question: 91

[Secure Network Access, Visibility, and Enforcement]
Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

A. RSA SecureID
B. Internal Database
C. Active Directory
D. LDAP

www.atmicnetworks.com

Answer: C

Explanation:

Active Directory (AD) is an ID store that requires that a shadow user be created on Cisco ISE for the admin login to work. A shadow user is a user account that is defined in the ISE internal database, but has the password set to external. This means that the user authentication is performed against an external identity source, such as AD, while the user authorization is based on the ISE admin group membership. A shadow user is useful when the admin wants to assign different roles or permissions to specific AD users, rather than using AD groups. To create a shadow user, the admin must check the External checkbox in the ISE admin user configuration, and make sure that the username matches the AD username. The shadow user must also be assigned to an ISE admin group that has the Type set to External123. Reference := 1: ISE Admin User Shadow AD Account Issue 2: ISE Admin user authentication from AD 3: Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

Question: 92

[Security Concepts]
An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17- 010 patch
was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate
the risk of this ransom ware infection? (Choose two)

A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowingaccess on the network.

B. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowingaccess on the network.

C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is metbefore allowing access on the network.

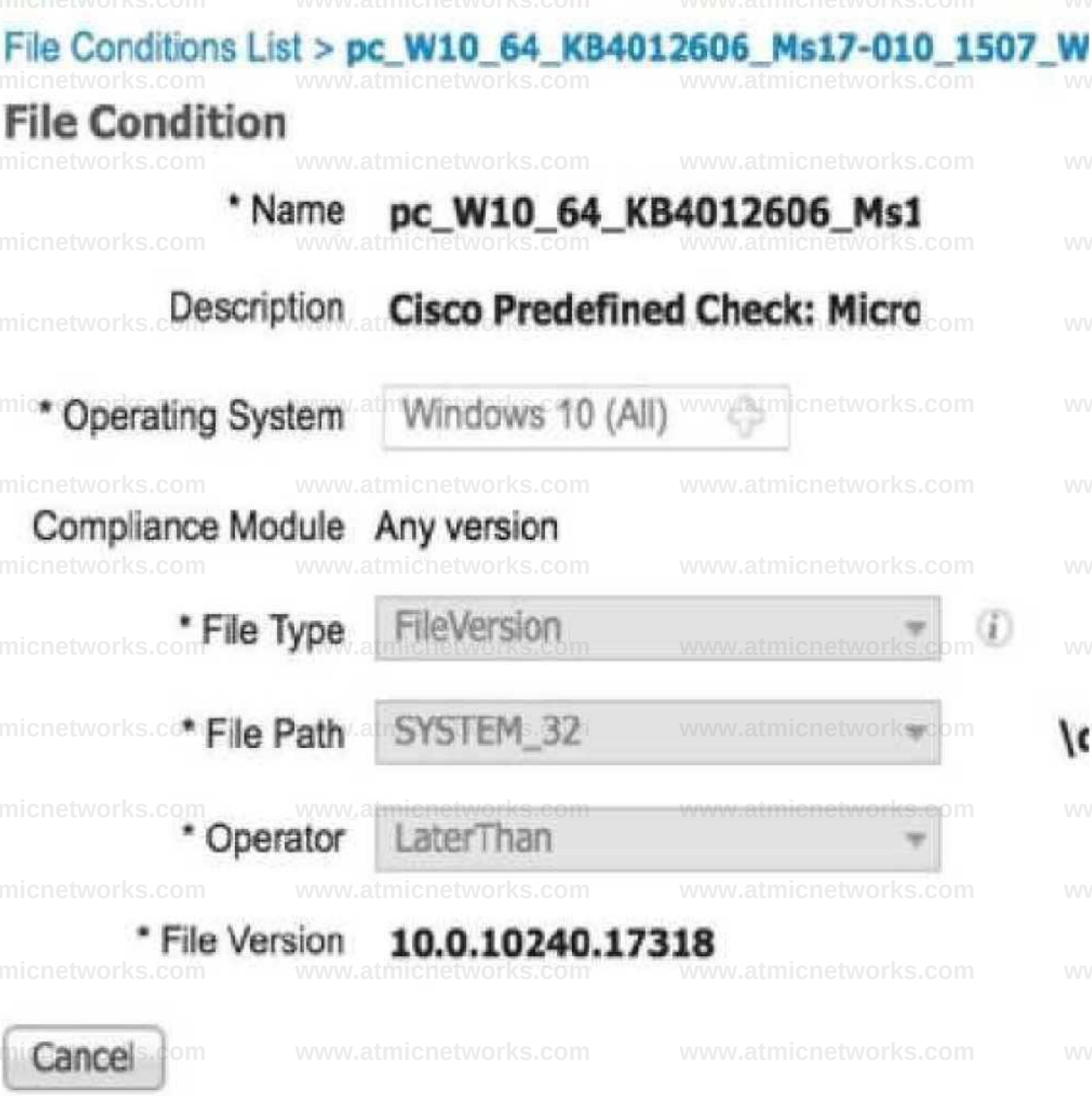
D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicatethroughout the network.

E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Answer: A,C

Explanation:

A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. We can configure ISE to check for the Windows patch at Work Centers > Posture > Posture Elements > Conditions > File.
In this example, we are going to use the predefined file check to ensure that our Windows 10 clients have the critical security patch installed to prevent the Wanna Cry malware.



Question: 93

[Network Security]

Which feature of Cisco ASA allows VPN users to be postured against Cisco ISE without requiring an inline posture node?

A. RADIUS Change of Authorization
B. device tracking
C. DHCP snooping
D. VLAN hopping

www.atmicnetworks.com

Answer: A

Explanation:

RADIUS Change of Authorization (CoA) is a feature of Cisco ASA that allows VPN users to be postured against Cisco ISE without requiring an inline posture node. RADIUS CoA enables the ISE to send a message to the ASA to change the authorization attributes of an existing VPN session, such as the assigned IP address, ACL, or group policy. This way, the ISE can dynamically adjust the access level of the VPN user based on the posture assessment results, without the need for an intermediate device to enforce the policy change12. RADIUS CoA is supported by the ASA since version 9.2.13. Reference: 1: ASA Version 9.2.1 VPN Posture with ISE Configuration Example - Cisco 2: How To: ISE and ASA Integration using CoA for Posture - Cisco Community 3: How To Configure Posture with AnyConnect Compliance … - Cisco Community

Question: 94

What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two)

A. multiple factor auth
B. local web auth
C. single sign-on
D. central web auth
E. TACACS+

Answer: B, D

Explanation:

Local web authentication (LWA) and central web authentication (CWA) are two mechanisms that are used to redirect users to a web portal to authenticate to ISE for guest services. Both methods involve the use of a redirect access control list (ACL) that allows the user to access only the web portal URL and blocks all other traffic until the user is authenticated. The difference between LWA and CWA is where the web portal and the authentication logic are hosted.

LWA: The web portal and the authentication logic are hosted on the wireless LAN controller (WLC). The WLC sends a RADIUS access-accept message to the network access device (NAD) along with the redirect ACL and the web portal URL. The NAD then redirects the user to the web portal on the WLC, where the user enters their credentials. The WLC verifies the credentials with the ISE and grants or denies access to the user. The advantage of LWA is that it does not require any configuration on the ISE, but the disadvantage is that it does not support advanced features such as posture assessment, profiling, or authorization policies.

CWA: The web portal and the authentication logic are hosted on the ISE. The WLC sends a RADIUS access-challenge message to the NAD along with the redirect ACL and the web portal URL. The NAD then redirects the user to the web portal on the ISE, where the user enters their credentials. The ISE verifies the credentials and sends a RADIUS access-accept message to the WLC with the authorization profile and the final ACL. The WLC then applies the authorization profile and the final

ACL to the user session. The advantage of CWA is that it supports advanced features such as posture assessment, profiling, or authorization policies, but the disadvantage is that it requires more configuration on the ISE.

Reference :=

Configure Guest Access

Web Authentication Redirection to Original URL

Configure Local Web Authentication with External Authentication

Question: 95

[Endpoint Protection and Detection]

For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two)

A. Windows service
B. computer identity
C. user identity
D. Windows firewall
E. default browser

Answer: A,D

Explanation:

ISE posture assessment allows you to inspect the security "health" of your PC and MAC clients. This includes checking for the installation, running state, and last update for security software, such as anti-virus, anti-malware, personal firewall, and so on1. Windows service and Windows firewall are examples of such security software that can be checked by ISE posture assessment. Computer identity and user identity are not conditions that can be checked by ISE posture assessment, as they are related to authentication and authorization, not security posture. Default browser is also not a condition that can be checked by ISE posture assessment, as it is not a security software or a security risk. Reference: 1: Chapter 15. Device Posture Assessment - Cisco ISE for BYOD and Secure Unified Access, 3

Question: 96

[Security Concepts]

Which compliance status is shown when a configured posture policy requirement is not met?

A. compliant
B. unknown
C. authorized
D. noncompliant

Answer: D

Explanation:

Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security
policies.
A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems.
Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies.
+ If a mandatory requirement fails, the user will be moved to Non-Compliant state
+ If an optional requirement fails, the user is allowed to skip the specified optional requirements and the user
is moved to Compliant state
This Qdid not clearly specify the type of posture policy requirement (mandatory or optional) is not met so the
user can be in Non-compliant or compliant state. But "noncompliant" is the best answer here.
Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010111.html

Question: 97

[Endpoint Protection and Detection]
Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

A. It allows the endpoint to authenticate with 802.1x or MAB.
B. It verifies that the endpoint has the latest Microsoft security patches installed.
C. It adds endpoints to identity groups dynamically.
D. It allows CoA to be applied if the endpoint status is compliant.

Answer: D

Explanation:

Posture is a service in Cisco ISE that checks the compliance of endpoints with corporate security policies before allowing them to connect to the network. Posture policies define the requirements that endpoints must meet to be compliant, such as having antivirus software installed and updated, or having a specific registry key value. If an endpoint is compliant, Cisco ISE can apply a Change of Authorization (CoA) to grant it access to the network resources. CoA is a mechanism that allows Cisco ISE to dynamically change the authorization attributes of an existing session, such as VLAN, dACL, or SGT, without requiring the user to reauthenticate. CoA can be triggered by various events, such as posture assessment results, profiling changes, or manual actions by the administrator. CoA can also be used to quarantine or disconnect non-compliant endpoints. Therefore, ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE provides the benefit of allowing CoA to be applied if the endpoint status is compliant. Reference :=
Cisco Identity Services Engine Administrator Guide, Release 2.2 - Configure Client Posture Policies Cisco Identity Services Engine Administrator Guide, Release 2.2 - Change of Authorization

www.atmicnetworks.com

Question: 98

[Security Concepts]
Which IPS engine detects ARP spoofing?

A. Atomic ARP Engine
B. Service Generic Engine
C. ARP Inspection Engine
D. AIC Engine

Answer: A

Explanation:

The Atomic ARP engine is a signature engine that defines basic Layer 2 ARP signatures and provides more advanced detection of the ARP spoof tools dsniff and ettercap. ARP spoofing is an attack that involves sending spoofed ARP messages over a local area network to associate the attacker's MAC address with the IP address of the target. The Atomic ARP engine inspects the Layer 2 ARP protocol and compares the ARP requests and replies with the MAC address table to detect any anomalies or inconsistencies. The Atomic ARP engine can also detect gratuitous ARP messages, which are unsolicited ARP replies that can be used to poison the ARP cache of other hosts. The Atomic ARP engine is different from other IPS engines because most engines are based on Layer 3 IP protocol. Reference :=
https://www.cisco.com/c/en/us/td/docs/security/ips/6-1/configuration/guide/cli/cliguide/cli_signature_engines.htmlhttps://security.stackexchange.com/questions/71023/can-suricata-ips-detect-and-prevent-arp- poisoning-attacks

Question: 99

[Security Concepts]

What is a characteristic of Dynamic ARP Inspection?

A. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCPsnooping binding database.
B. In a typical network, make all ports as trusted except for the ports connecting to switches, which areuntrusted
C. DAI associates a trust state with each switch.
D. DAI intercepts all ARP requests and responses on trusted ports only.

Answer: A

Explanation:

Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address

bindings. This capability protects the network from certain “man-in-the-middle” attacks. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database. DAI also supports static ARP ACLs for hosts with static IP addresses. DAI checks all ARP packets on untrusted interfaces, and only forwards the packets that have valid bindings. DAI can also rate-limit the ARP packets on untrusted interfaces to prevent DoS attacks. The other options are incorrect because:
B . In a typical network, DAI should be configured to make all ports as untrusted except for the ports connecting to trusted hosts or switches, which are trusted.
C . DAI does not associate a trust state with each switch, but with each interface on the switch.
D . DAI intercepts all ARP requests and responses on untrusted ports only, not on trusted ports. Reference :=

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html https://study-ccna.com/dynamic-arp-inspection-dai/

Question: 100

[Security Concepts]
What is a characteristic of traffic storm control behavior?

A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level withinthe interval.
B. Traffic storm control cannot determine if the packet is unicast or broadcast.
C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet isunicast or broadcast.

Answer: D

Explanation:

Traffic storm control is a feature that prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces. Traffic storm control monitors the level of each traffic type for which it is enabled in 1-second intervals and compares it with the configured threshold, which is a percentage of the total available bandwidth of the port. When the ingress traffic reaches the threshold, traffic storm control drops the traffic until the end of the interval. Traffic storm control uses the Individual/Group bit in the packet destination address to determine if the packet is unicast or broadcast. This bit is set to 0 for unicast addresses and 1 for multicast or broadcast addresses. Traffic storm control does not use the source address to classify the traffic type. Reference := Configuring Traffic Storm Control - Cisco, Understanding Cisco Traffic Storm Control - NetCraftsmen

Question: 101

[Security Concepts]
A malicious user gained network access by spoofing printer connections that were authorized using MAB on

four different switch ports at the same time. What two catalyst switch security features will prevent further violations? (Choose two)

A. DHCP Snooping
B. 802.1AE MacSec
C. Port security
D. IP Device track
E. Dynamic ARP inspection
F. Private VLANs

Answer: B,C

Explanation:

MAB is a fallback mechanism for IEEE 802.1X that allows network access based on the MAC address of the endpoint. However, MAB does not prevent MAC address spoofing, which is a technique used by attackers to impersonate authorized devices and bypass authentication. To mitigate this risk, two catalyst switch security features can be used in conjunction with MAB: 802.1AE MacSec and port security.

802.1 AE MacSec is a standard that provides encryption and integrity protection for data frames between two MACsec-capable devices. MacSec also uses a secure key exchange protocol called MKA (MACsec Key Agreement) to establish and maintain cryptographic keys between the peers. By enabling MacSec on the switch ports, the switch can verify the identity and authenticity of the

endpoints and prevent unauthorized access or tampering with the data frames.

Port security is a feature that allows the switch to limit the number and type of MAC addresses that can access a port. Port security can be configured to allow only a specific MAC address or a maximum number of MAC addresses per port. Port security can also be configured to take an action when a violation occurs, such as shutting down the port, sending a trap, or dropping packets. By enabling port security on the switch ports, the switch can prevent multiple devices from accessing the same port or deny access to devices with spoofed MAC addresses.

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 2: Network Security, Lesson 2.2: Implementing Network Access Control

MAC Authentication Bypass Deployment Guide, MAB Benefits and Limitations, MAB Feature Interaction

Question: 102

[Secure Network Access, Visibility, and Enforcement]
Which command enables 802.1X globally on a Cisco switch?

A. dot1x system-auth-control
B. dot1x pae authenticator
C. authentication port-control aut
D. aaa new-model

Answer: A

Explanation:

The dot1x system-auth-control command enables 802.1X globally on a Cisco switch. This command allows the switch to act as an authenticator for 802.1X clients connected to the switch ports. The switch will then communicate with a RADIUS server to authenticate the clients and grant or deny access to the network. The other commands are not related to enabling 802.1X globally. The dot1x pae authenticator command enables 802.1X authentication on a specific interface. The authentication port-control aut command enables automatic port-based authentication on an interface. The aaa new-model command enables the AAA framework for authentication, authorization, and accounting. Reference := https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series- managed-switches/smb5635-configure-global-802-1x-properties-on-a-switch-through-the-c.htmlhttps://www.cisco.com/c/en/us/td/docs/routers/nfvis/switch_command/b-nfvis-switch-command-reference/802_1x_commands.html

Question: 103

[Secure Network Access, Visibility, and Enforcement]
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?

A. 1
B. 2
C. 6
D. 31

Answer: C

Explanation:

Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential. Cisco switches uniquely identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB AccessRequest message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server.
Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_guide_c17-663759.html

Question: 104

[Security Concepts]
A network administrator configures Dynamic ARP Inspection on a switch. After Dynamic ARP Inspection is applied, all users on that switch are unable to communicate with any destination. The network administrator

checks the interface status of all interfaces, and there is no err-disabled interface. What is causing this problem?

A. DHCP snooping has not been enabled on all VLANs.
B. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users.
C. Dynamic ARP Inspection has not been enabled on all VLANs
D. The no ip arp inspection trust command is applied on all user host interfaces

Answer: D

Explanation:

Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. It

intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. After enabling DAI, all ports become untrusted ports.

Question: 105

[Secure Network Access, Visibility, and Enforcement] Refer to the exhibit.

```
SwitchA(config)#interface gigabitethernet1/0/1
SwitchA(config-if)#dot1x host-mode multi-host
SwitchA(config-if)#dot1x timeout quiet-period 3
SwitchA(config-if)#dot1x timeout tx-period 15
SwitchA(config-if)#authentication port-control
auto
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 12
```

An engineer configured wired 802.1x on the network and is unable to get a laptop to authenticate. Which port configuration is missing?

A. authentication open
B. dotlx reauthentication
C. cisp enable
D. dot1x pae authenticator

Answer: D

Explanation:

The dot1x pae authenticator command enables 802.1x authentication on the port and configures the port as an authenticator. This command is required for the port to initiate the authentication process with the connected client. Without this command, the port will not send EAPOL packets to the client and will not receive the client credentials. Therefore, the client will not be authenticated and will remain in the unauthorized state. The other options are not mandatory for 802.1x authentication, although they can be used to modify the default behavior of the port. For example, authentication open allows the port to grant access to the client before authentication, dot1x reauthentication enables periodic reauthentication of the client, and cisp enable enables Cisco Identity Services Protocol (CISP) on the port. Reference: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 5: Secure Network Access, Lesson 5.1: Implementing 802.1X Authentication, Topic 5.1.2: Configuring 802.1X Authentication, Page 5-9.

www.atmicnetworks.com

Question: 106

[Security Concepts]
Which SNMPv3 configuration must be used to support the strongest security possible?

A. asa-host(config)#snmp-server group myv3 v3 privasa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXXasa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
B. asa-host(config)#snmp-server group myv3 v3 noauthasa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXasa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
C. asa-host(config)#snmpserver group myv3 v3 noauthasa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXXasa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
D. asa-host(config)#snmp-server group myv3 v3 privasa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXasa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

Answer: D

Explanation:

The strongest security possible for SNMPv3 requires both authentication and encryption, which is achieved by using the priv security level. Authentication ensures that the message is from a valid source, and encryption scrambles the content of the packet to prevent it from being learned by an unauthorized source. The auth sha and priv aes 256 parameters specify the algorithms used for authentication and encryption, respectively. SHA is more secure than MD5, and AES 256 is more secure than DES or 3DES. Therefore, option D is the correct answer, as it uses the priv security level, the SHA algorithm for authentication, and the AES 256 algorithm for encryption. The other options either use a lower security level (noauth or authNoPriv), a weaker encryption algorithm (des or 3des), or no encryption at all. Reference :=
SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) - SNMP Version 3 Configuration Template for SNMPv3 - Cisco Community
SNMP Version 3 - Cisco

Question: 107

[Security Concepts] Refer to the exhibit.

Interface	MAC Address	Methoc	1 Domain	Status	Fg	Session I
G14/15	0050.b6d4.8a60	dot lx	DATA	Au th		0A021982000
Gi8/43	0024.c4fe.1832	dotlx	VOICE	Au th		0A021982000
GilO/25	0026.7391.bbdl	dot lx	DATA	Au th		0A021982000
Gi8/2B	0026.0b5e.51d5	dotlx	VOICE	Auth		0A021982000
Gi4/13	0025.4593.e575	dotlx	VOICE	Auth		0A021982000
GilO/23	0025.8418.217f	dotlx	VOICE	Auth		0A021982OOO
Gi7/4	0025.8418.Ibc7	dotlx	VOICE	Auth		0A021982000
Gi7/7	0026.0b5e.50fb	dotlx	VOICE	Auth		0A021982000
Ci8/14	c85b.7604.fald	dotlx	DATA	Auth		0A021982000
GilO/29	0026.0b5e.528a	dotlx	VOICE	Auth		OA021982OOO
Gi4/2	0026.0b5e.4f9f	dotlx	VOICE	Auth		0A021982000
Gil0/30	0025.4593.e5ac	dotlx	VOICE	Auth		OA021982OOO
Gi8/29	68bd.aba5.2e44	dotlx	VOICE	Auth		0A021982000
Gi7/4	54ee.75db.d766	dotlx	DATA	Auth		0A021982000
Gi2/34	e804.62eb.a658	dotlx	VOICE	Auth		0A021982000
GilO/22	482a.e307.d9c8	dotlx	DATA	Auth		0A021932OOO
Gi9/22	0007.b00c.8c35	mab	DATA	Auth		0A021982000

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

A. show authentication registrations
B. show authentication method
C. show dot1x all
D. show authentication sessions

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137
Displaying the Summary of All Auth Manager Sessions on the Switch
Enter the following:

Switch# show authentication sessions
Interface MAC Address Method Domain Status Session ID
Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C
Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58
Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

Question: 108

[Secure Network Access, Visibility, and Enforcement]
What Cisco command shows you the status of an 802.1X connection on interface gi0/1?

A. show authorization status
B. show authen sess int gi0/1
C. show connection status gi0/1
D. show ver gi0/1

Answer: B

Explanation:

The command show authen sess int gi0/1 displays the authentication session information for the interface gi0/1, such as the MAC address, the authentication method, the authentication state, the session timeout, and the VLAN assignment. This command is useful for verifying the status of an 802.1X connection on a specific interface. The other commands are not related to 802.1X authentication. The command show authorization status displays the authorization status for the current user. The command show connection status gi0/1 is not a valid Cisco command. The command show ver gi0/1 displays the version information for the interface gi0/1. Reference: 802.1X Authentication Commands, Configuring IEEE 802.1x Port-Based Authentication, What Cisco command shows you the status of an 802.1X connection on interface gi0/1?

Question: 109

[Security Concepts] Refer to the exhibit.

samp-server group SNMP v3 auth access 15

What does the number 15 represent in this configuration?

A. privilege level for an authorized user to this router
B. access list that identifies the SNMP devices that can access the router
C. interval in seconds between SNMPv3 authentication attempts
D. number of possible failed attempts until the SNMPv3 user is locked out

Answer: B

Explanation:

The syntax of this command is shown below:

snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write write-view] [notify notify-view] [access access-list]

The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just

www.atmicnetworks.com

happened to be passing through on their way to some other destination device.

Question: 110

[Security Concepts]
Under which two circumstances is a CoA issued? (Choose two)

A. A new authentication rule was added to the policy on the Policy Service node.
B. An endpoint is deleted on the Identity Service Engine server.
C. A new Identity Source Sequence is created and referenced in the authentication policy.
D. An endpoint is profiled for the first time.
E. A new Identity Service Engine server is added to the deployment with the Administration persona

Answer: B,D

Explanation:

The profiling service issues the change of authorization in the following cases:

– Endpoint deleted—When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network.

An exception action is configured—If you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the corresponding static profile by issuing a CoA.

– An endpoint is profiled for the first time—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.

+ An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.

The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:

++ The endpoint identity group changes for endpoints when they are dynamically profiled

++ The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint – An endpoint profiling policy has changed and the policy is used in an authorization policy—When an endpoint profiling policy changes, and the policy is included in a logical profile that is used in an authorization policy. The endpoint profiling policy may change due to the profiling policy match or when an endpoint is statically assigned to an endpoint profiling policy, which is associated to a logical profile. In both the cases, the profiling service issues a CoA, only when the endpoint profiling policy is used in an authorization policy.

Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html

Question: 111

[Secure Network Access, Visibility, and Enforcement] Refer to the exhibit.

```
HQ_Router(config)#username admin5 privilege 5
HQ_Router(config)#privilege interface level 5
shutdown
HQ_Router(config)#privilege interface level 5 ip
HQ_Router(config)#privilege interface level 5
description
```

A network administrator configures command authorization for the admin5 user. What is the admin5 user able to do on HQ_Router after this configuration?

A. set the IP address of an interface
B. complete no configurations
C. complete all configurations
D. add subinterfaces

Answer: B

Explanation:

The user "admin5" was configured with privilege level 5. In order to allow configuration (enter global configuration mode), we must type this command:
(config)#privilege exec level 5 configure terminal
Without this command, this user cannot do any configuration.
Note: Cisco IOS supports privilege levels from 0 to 15, but the privilege levels which are used by default are privilege level 1 (user EXEC) and level privilege 15 (privilege EXEC)

Question: 112

[Security Concepts]
A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0380739941 command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?

A. snmp-server host inside 10.255.254.1 version 3 andy
B. snmp-server host inside 10.255.254.1 version 3 myv3
C. snmp-server host inside 10.255.254.1 snmpv3 andy
D. snmp-server host inside 10.255.254.1 snmpv3 myv3

Answer: A

Explanation:

The command “snmp-server user user-name group-name
[remote ip-address
[udp-port port]] {v1 | v2c | v3
[encrypted]
[auth {md5 | sha} auth-password]}
[access access-list]” adds a new user (in this case “andy”) to an SNMPv3 group (in this case group name “myv3”) and configures a password for the user.
In the “snmp-server host” command, we need to:
+ Specify the SNMP version with key word “version {1 | 2 | 3}”
+ Specify the username (“andy”), not group name (“myv3”).
Note: In “snmp-server host inside …” command, “inside” is the interface name of the ASA interface through which the NMS (located at 10.255.254.1) can be reached.

Question: 113

[Security Concepts]
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?

A. interpacket variation
B. software package variation
C. flow insight variation
D. process details variation

Answer: A

Explanation:

The telemetry information consists of three types of data:
+ Flow information: This information contains details about endpoints, protocols, ports, when the flow started, how long the flow was active, etc.
+ Interpacket variation: This information captures any interpacket variations within the flow. Examples include variation in Time To Live (TTL), IP and TCP flags, payload length, etc
+ Context details: Context information is derived outside the packet header. It includes details about variation in buffer utilization, packet drops within a flow, association with tunnel endpoints, etc. Reference:
https://www.cisco.com/c/dam/global/en_uk/products/switches/cisco_nexus_9300_ex_platform_swi
tches_white_paper_uki.pdf

www.atmicnetworks.com

Question: 114

[Security Concepts]
How is ICMP used an exfiltration technique?

A. by flooding the destination host with unreachable packets
B. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address
C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
D. by overwhelming a targeted host with ICMP echo-request packets

Answer: C

Explanation:

ICMP is a protocol that is used to send diagnostic messages between hosts on a network. It is not designed to carry any data, but it can be abused by attackers to exfiltrate data from a compromised host. By encrypting the payload in an ICMP packet, the attacker can hide the data from network monitoring tools and firewalls that may not inspect ICMP traffic. The attacker can then use another
tool to decrypt the data from the ICMP packets on a remote host. This technique is known as ICMP tunneling and it is a form of protocol tunneling (MITRE T1572: Protocol Tunneling1). Reference:
1: https://attack.mitre.org/techniques/T1572/
2: https://www.cynet.com/attack-techniques-hands-on/how-hackers-use-icmp-tunneling-to-own- your-network/
3: https://digital-security.quodagis.fr/ressources/ressource/exfiltration-de-donnees-les-techniques- icmp-et-dns-tunneling-855

Question: 115

[Security Concepts]
Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?

A. DNS tunneling
B. DNSCrypt
C. DNS security
D. DNSSEC

Answer: A

Explanation:

DNS Tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses. DNS tunneling often includes data payloads that can be added to an attacked DNS server and used to control a remote server and applications.

Question: 116

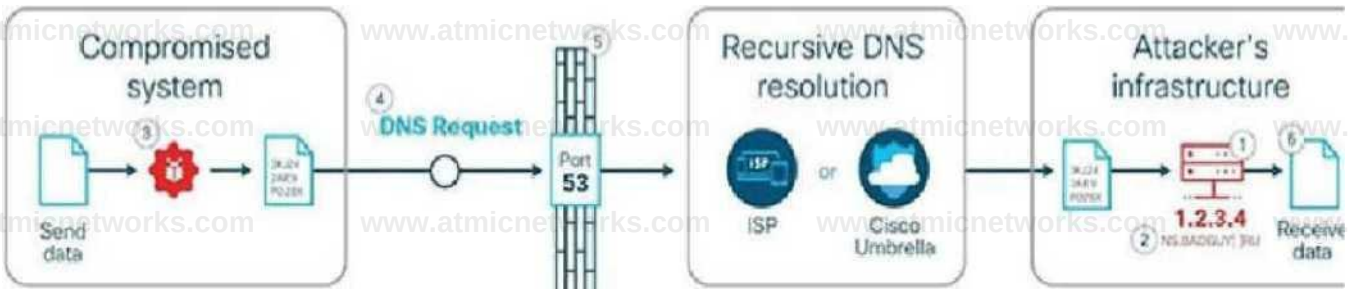
[Security Concepts]
How is DNS tunneling used to exfiltrate data out of a corporate network?

A. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
B. It encodes the payload with random characters that are broken into short strings and the DNS serverrebuilds the exfiltrated data.
C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damageand theft on the network.
D. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.

Answer: B

Explanation:

Domain name system (DNS) is the protocol that translates human-friendly URLs, such as securitytut.com, into IP addresses, such as 183.33.24.13. Because DNS messages are only used as the beginning of each communication and they are not intended for data transfer, many organizations do not monitor their DNS traffic for malicious activity. As a result, DNS-based attacks can be effective if launched against their networks. DNS tunneling is one such attack.
An example of DNS Tunneling is shown below:



The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNSnameserver (NS) and malicious payload.2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.43. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,…).4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as
Reference: https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0

Question: 117

[Security Concepts]
Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent?
(Choose two)

www.atmicnetworks.com

A. Outgoing traffic is allowed so users can communicate with outside organizations.
B. Malware infects the messenger application on the user endpoint to send company data.
C. Traffic is encrypted, which prevents visibility on firewalls and IPS systems.
D. An exposed API for the messaging platform is used to send large amounts of data.
E. Messenger applications cannot be segmented with standard network controls

Answer: C,E

Explanation:

Question: 118

[Endpoint Protection and Detection] Which Cisco AMP file disposition valid?

A. pristine
B. malware
C. dirty
D. non malicious

Answer: B

Explanation:

Question: 119

[Endpoint Protection and Detection]
When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?

A. Spero analysis
B. dynamic analysis
C. sandbox analysis
D. malware analysis

Answer: A

Explanation:

Spero analysis is a feature of Cisco AMP for Networks that examines structural characteristics such as metadata and header

www.atmicnetworks.com

information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud for analysis1. Spero analysis can detect malware based on the file's structure and behavior, without requiring a full file upload2. Spero analysis is different from dynamic analysis, sandbox analysis, and malware analysis, which are other features of Cisco AMP for

Networks that perform different types of file inspection and analysis3. Reference: 1: How to configure Firepower AMP to not upload files to … - Cisco Community 2: File Policies - Network Direction 3: Cisco AMP for Networks - Cisco

Question: 120

[Endpoint Protection and Detection]

Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?

A. cloud web services
B. network AMP
C. private cloud
D. public cloud

Answer: C

Explanation:

Cisco Advanced Malware Protection (AMP) for Endpoints is a cloud-based solution that provides endpoint protection against malware and advanced threats. It can be deployed in different architectures depending on the customer's needs and preferences. One of the deployment options is the private cloud, which is designed to keep data within a network perimeter. In this option, the customer hosts the AMP for Endpoints console and the AMP cloud on their own infrastructure, and the endpoints connect to the private cloud for analysis and policy enforcement. This option provides more control and privacy over the data, but also requires more resources and maintenance from the customer. The other deployment options are the public cloud, which uses the Cisco-hosted AMP cloud and console, and the hybrid cloud, which uses a combination of the public and private clouds123 Reference: 1: Protecting Against Malware Threats with Cisco AMP for Endpoints (SSFAMP) course overview 2: Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco 3: Cisco Advanced Malware Protection for Endpoints - Zones

Question: 121

[Securing the Cloud]

Which capability is exclusive to a Cisco AMP public cloud instance as compared to a private cloud instance?

A. RBAC
B. ETHOS detection engine

C. SPERO detection engine D. TETRA detection engine

Answer: B

Explanation:

ETHOS is one of the many detection engines that AMP uses to continuously protect you from malware. It is only available in the public cloud, as it requires a large amount of data and processing power to operate. ETHOS uses machine learning to analyze the behavior and characteristics of files and determine their maliciousness. It can detect both known and unknown threats, as well as polymorphic and metamorphic malware that can change their appearance or code. ETHOS is part of the AMP cloud's dynamic analysis capabilities, which also include SPERO and Threat Grid12.

The private cloud instance of AMP does not have ETHOS, as it is meant to be an on-premises, selfcontained solution that satisfies stringent privacy requirements. The private cloud instance also does not have SPERO or Threat Grid, unless they are deployed separately as additional appliances. The private cloud instance relies on the TETRA detection engine, which is a signature-based engine that can identify known malware. TETRA is updated regularly with new signatures from the AMP cloud, but it cannot detect unknown or zero-day threats as effectively as ETHOS34.

Therefore, the capability that is exclusive to the AMP public cloud instance as compared to the private cloud instance is the ETHOS detection engine. Reference: 1: Cisco Advanced Malware Protection Private Cloud Appliance Data Sheet 2: What is AMP Private Cloud 3: Deploy Cisco AMP Private Cloud on Cisco HyperFlex Systems 4: AMP Private Cloud vs Public Cloud Dashboard different

Question: 122

[Endpoint Protection and Detection]

An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?

A. device flow correlation
B. simple detections
C. application blocking list
D. advanced custom detections

Answer: C

Explanation:

The application blocking list is an outbreak control method that allows the administrator to block certain files from executing on the endpoints based on their SHA values. This can prevent malware from running on the endpoints and causing damage. The other options are not outbreak control

methods, but rather different features of AMP for endpoints. Device flow correlation is a network analysis feature that monitors connections and detects malicious activity. Simple detections and advanced custom detections are custom rules that can be created by the administrator to detect and block files based on signatures or other criteria.

Reference:

Configure Windows Policy in AMP for Endpoints - Cisco
Prevent, Detect and Respond with Cisco AMP for Endpoints

Question: 123

[Security Concepts]
Which function is the primary function of Cisco AMP threat Grid?

A. automated email encryption
B. applying a real-time URI blacklist
C. automated malware analysis
D. monitoring network traffic

Answer: C

Explanation:

Cisco AMP Threat Grid is a cloud-based or on-premises solution that provides advanced malware analysis and threat intelligence. It combines static and dynamic analysis techniques to examine the behavior of malware samples and correlate them with global and historical context. It also produces detailed reports, threat scores, and behavioral indicators that help security teams prioritize and respond to threats faster and more effectively12. Reference: 1: Cisco Secure Malware Analytics (Threat Grid) - Cisco 2: Products - Cisco Threat Grid Cloud Data Sheet - Cisco

Question: 124

[Endpoint Protection and Detection]
What are two list types within AMP for Endpoints Outbreak Control? (Choose two)

A. blocked ports
B. simple custom detections
C. command and control
D. allowed applications
E. URL

Answer: B,D

Explanation:

Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists.

A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine.
Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by

a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf

Question: 125

[Endpoint Protection and Detection]
What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?

A. Enable IP Layer enforcement.
B. Activate the Advanced Malware Protection license
C. Activate SSL decryption.
D. Enable Intelligent Proxy.

Answer: D

Explanation:

To enable malware file scanning for the Secure Internet Gateway (SIG), you need to enable Intelligent Proxy, which is a feature of Cisco Umbrella that provides selective proxying of web requests based on the risk level of the domain1. Intelligent Proxy allows SIG to inspect the content of potentially malicious web requests and block or allow them based on the configured policies2. Intelligent Proxy also enables SSL decryption, which is necessary to scan encrypted web traffic for malware3. Enabling IP Layer enforcement, activating the Advanced Malware Protection license, and activating SSL decryption are not required prerequisites to enable malware file scanning for the SIG, although they may provide additional security benefits45. Reference: 1: Intelligent Proxy - Cisco Umbrella 2: Cisco Umbrella SIG Advantage - Cisco Umbrella 3:
[SSL Decryption - Cisco Umbrella] 4:
[IP Layer Enforcement - Cisco Umbrella] 5:
[Advanced Malware Protection - Cisco Umbrella]

Question: 126

[Secure Network Access, Visibility, and Enforcement]
When wired 802.1X authentication is implemented, which two components are required? (Choose two)

A. authentication server: Cisco Identity Service Engine
B. supplicant: Cisco AnyConnect ISE Posture module
C. authenticator: Cisco Catalyst switch
D. authenticator: Cisco Identity Services Engine
E. authentication server: Cisco Prime Infrastructure

Answer: A,C

Explanation:

Wired 802.1X authentication is a port-based network access control that uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port1. Wired 802.1X authentication requires three components: a supplicant, an authenticator, and an authentication server2. The supplicant is the client device that requests access to the network. The authenticator is the switch port that controls the access to the network based on the authentication result. The authentication server is the server that validates the credentials of the supplicant and sends the authentication result to the authenticator3.

In this question, option A is correct because Cisco Identity Service Engine (ISE) is an example of an authentication server that supports wired 802.1X authentication4. Option C is correct because Cisco Catalyst switch is an example of an authenticator that supports wired 802.1X authentication5. Option B is incorrect because Cisco AnyConnect ISE Posture module is not a supplicant, but a software component that checks the compliance status of the supplicant. Option D is incorrect because Cisco ISE is not an authenticator, but an authentication server. Option E is incorrect because Cisco Prime Infrastructure is not an authentication server, but a network management tool.

: 1: Wired 802.1X Deployment Guide - Cisco 2: 802.1X Authenticated Wired Access Overview | Microsoft Learn 3: About 802.1X Authentication - Aruba 4: Cisco Identity Services Engine - Products & Services - Cisco 5: Cisco Catalyst 2960-X Series Switches - Products & Services - Cisco : Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9 - Configure Posture [Cisco AnyConnect Secure Mobility Client] - Cisco : Cisco Prime Infrastructure - Products & Services - Cisco

Question: 127

[Security Concepts] Refer to the exhibit.

```
Sysauthcontrol              Enabled
Dotlx Protocol Version        3

Dotlx Info for GigabitEthernet1/0/12

PAE                    = AUTHENTICATOR
Portcontrol            = FORCE_AUTHORIZED
ControlDirection =    Both
HostMode               = SINGLE_HOST
QuietPeriod            = 60
ServerTimeout          = 0
```

```
SuppTimeout          = 30
ReAuthMax            = 2
MaxReq               = 2
TxPeriod             = 30
```

Which command was used to display this output?

A. show dot1x all
B. show dot1x
C. show dot1x all summary
D. show dot1x interface gi1/0/12

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec- user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

Question: 128

[Secure Network Access, Visibility, and Enforcement]
Refer to the exhibit.

```
aaa new-model
radius-server host 10.0.0.12 key
secret 12
```

Which statement about the authentication protocol used in the configuration is true?

A. The authentication request contains only a password
B. The authentication request contains only a username
C. The authentication and authorization requests are grouped in a single packet
D. There are separate authentication and authorization request packets

Answer: C

Explanation:

This command uses RADIUS which combines authentication and authorization in one function (packet).

Question: 129

[Endpoint Protection and Detection]

An engineer needs a solution for TACACS+ authentication and authorization for device administration. The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth. Which product meets all of these requirements?

A. Cisco Prime Infrastructure
B. Cisco Identity Services Engine
C. Cisco Stealthwatch
D. Cisco AMP for Endpoints

Answer: B

Explanation:

Cisco Identity Services Engine (ISE) is a product that provides comprehensive and scalable access policy enforcement for wired and wireless networks. ISE supports TACACS+ for device administration, which allows for granular control over the commands and actions that network administrators can perform on network devices. ISE also supports 802.1X, MAB, and WebAuth for network access, which enables authentication and authorization of users and endpoints based on various attributes, such as identity, device type, posture, location, and time. ISE can also integrate with other Cisco security products, such as Cisco Stealthwatch and Cisco AMP for Endpoints, to provide enhanced visibility and threat detection. Therefore, ISE is the product that meets all of the requirements stated in the question. Reference := Some possible references are:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Secure Network Access, Identity Management, and Secure Access

TACACS+ Configuration Guide, Configuring TACACS

Cisco Identity Services Engine Administrator Guide, Release 2.7, Device Administration

Cisco Identity Services Engine Administrator Guide, Release 2.7, Network Access Devices Cisco Identity Services Engine Administrator Guide, Release 2.7, Policy Sets

Question: 130

[Secure Network Access, Visibility, and Enforcement]

Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?

A. aaa server radius dynamic-author
B. aaa new-model
C. auth-type all
D. ip device-tracking

Answer: A

Explanation:

The aaa server radius dynamic-author command enables authentication, authorization, and accounting (AAA) globally on the device so that Change of Authorization (CoA) is supported. CoA is a feature that allows an external AAA server to dynamically change the attributes of a user session after it is authenticated. For example, the AAA server can send a CoA request to reauthenticate a user, terminate a session, or apply a new policy. The aaa server radius dynamic-author command specifies the IP address and port number of the device that listens for CoA requests from the AAA server. The command also configures the shared secret key that is used to encrypt the communication between the device and the AAA server12. Reference := 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Securing Networks with Cisco Firepower Next Generation Firewall, Lesson 3.2: Deploying Cisco Firepower Next-Generation Firewall, Topic 3.2.2: Cisco Firepower NGFW Device Management 2: Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15SY - RADIUS Change of Authorization

[Support] - Cisco3

Question: 131

[Security Concepts]
An MDM provides which two advantages to an organization with regards to device management? (Choose two)

A. asset inventory management
B. allowed application management
C. Active Directory group policy management
D. network device management
E. critical device management

Answer: A,B

Explanation:

Mobile Device Management (MDM) is a solution that allows an organization to manage, monitor, and secure mobile devices such as smartphones, tablets, and laptops. MDM provides two main advantages to an organization with regards to device management:
Asset inventory management: MDM helps an organization keep track of all the mobile devices that are connected to its network, including their location, status, configuration, and usage. MDM also enables an organization to remotely wipe or lock devices that are lost, stolen, or compromised, preventing data loss and unauthorized access. Asset inventory management helps an organization optimize its resources, reduce costs, and comply with regulations12.
Allowed application management: MDM allows an organization to control what applications can be installed and run on the mobile devices, as well as how they can access and share data. MDM can also push updates and patches to the devices, ensuring that they are always running the latest and most secure versions of the applications. Allowed application management helps an organization enhance security, productivity, and performance of the mobile devices34.
: 1: 7 Advantages and Disadvantages of Mobile Device Management

www.atmicnetworks.com

[2024] 2: 5 Benefits of Mobile Device Management - ESET 3: Top 10 Benefits of Mobile Device Management (MDM) - TechFunnel 4: Benefits of Mobile Device Management (MDM) for Businesses

Question: 132

[Endpoint Protection and Detection]

Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

A. NGFW
B. AMP
C. WSA
D. ESA

Answer: B

Explanation:

Cisco AMP (Advanced Malware Protection) is a product that provides proactive endpoint protection and allows administrators to centrally manage the deployment. AMP uses cloud-based intelligence, sandboxing, and continuous analysis to detect and block advanced threats before they reach the endpoints. AMP also provides retrospective security, which means that it can alert and remediate endpoints if a file that was previously deemed benign is later found to be malicious. AMP can be integrated with other Cisco products, such as Firepower, Meraki, and Email Security Appliance, to provide comprehensive security across the network. AMP is available for Windows, Mac, Linux, Android, and iOS devices. Reference := Some possible references are:
Endpoint Protection Platform (EPP) Definition - Cisco: This page defines what an endpoint protection platform (EPP) is and how it differs from traditional antivirus solutions. It also explains the benefits of using Cisco Secure Endpoint, formerly known as AMP for Endpoints.
Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco: This page provides an overview of the features and capabilities of Cisco Secure Endpoint, such as cloud-based intelligence, endpoint isolation, file trajectory, device flow correlation, and more. It also offers resources for getting started, deploying, and managing Cisco Secure Endpoint.
SCOR 350-701 Flashcards | Quizlet: This page contains flashcards for the SCOR 350-701 exam, which covers the topics of implementing and operating Cisco security core technologies. One of the flashcards is the same question as the one asked by the user, and it provides the correct answer and a brief .

Question: 133

[Endpoint Protection and Detection]

Which benefit does endpoint security provide the overall security posture of an organization?

A. It streamlines the incident response process to automatically perform digital forensics on the endpoint.
B. It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
C. It allows the organization to detect and respond to threats at the edge of the network.

www.atmicnetworks.com

D. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.

Answer: D

Explanation:

Endpoint security is the process of protecting devices like workstations, servers, and other devices from malicious threats and cyberattacks. Endpoint security enables businesses to secure endpoints that employees use for work purposes or servers that are either on a network or in the cloud. Endpoint security is important because every device that connects to the corporate network is a potential vulnerability, providing a possible entry point for cyber criminals. Therefore, every device an employee uses to connect to any business system or resource carries the risk of becoming the chosen route for hacking into an organization. These devices can be exploited by malware that could leak or steal sensitive data from the business12.

One of the benefits of endpoint security is that it allows the organization to detect and mitigate threats that the perimeter security devices do not detect. Perimeter security devices, such as firewalls and intrusion prevention systems, are designed to protect the network from external attacks. However, they may not be able to prevent or detect attacks that originate from within the network, such as insider threats, compromised devices, or lateral movement. Endpoint security solutions can provide visibility and control over the devices that connect to the network, and can monitor, analyze, and respond to suspicious or malicious activities on the endpoints. Endpoint security solutions can also leverage threat intelligence and advanced analytics to identify and block known and unknown threats, such as ransomware, zero-day exploits, and targeted attacks13. Reference := 1: What is Endpoint Security? How Does It Work? | Fortinet 2: Microsoft Defender for Endpoint | Microsoft Security 3: Endpoint Security - Check Point Software

Question: 134

[Secure Network Access, Visibility, and Enforcement]

What are the two most commonly used authentication factors in multifactor authentication? (Choose two)

A. biometric factor
B. time factor
C. confidentiality factor
D. knowledge factor
E. encryption factor

Answer: A,D

Explanation:

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource. MFA requires means of verification that unauthorized

users

won't have.

Proper multi-factor authentication uses factors from at least two different categories.

MFA methods:

+ Knowledge – usually a password – is the most commonly used tool in MFA solutions. However, despite their simplicity, passwords have become a security problem and slow down productivity.

+ Physical factors – also called possession factors–use tokens, such as a USB dongle or a portable device, that generate a temporary QR (quick response) code. Mobile phones are commonly used, as they have the advantage of being readily available in most situations.

+ Inherent – This category includes biometrics like fingerprint, face, and retina scans. As technology advances, it may also include voice ID or other behavioral inputs like keystroke metrics. Because inherent factors are reliably unique, always present, and secure, this category shows promise.

+ Location-based and time-based – Authentication systems can use GPS coordinates, network parameters, and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these data points with historical or contextual user data.

A time factor in conjunction with a location factor could detect an attacker attempting to authenticate in Europe when the user was last authenticated in California an hour prior, for example.

+ Time-based one-time password (TOTP) – This is generally used in 2FA but could apply to any MFA method where a second step is introduced dynamically at login upon completing a first step. The wait for a second step–in which temporary passcodes are sent by SMS or email–is usually brief, and the process is easy to use for a wide range of users and devices. This method is currently widely used.

+ Social media – In this case a user grants permission for a website to use their social media username and password for login. This provide an easy login process, and one generally available to all users.

+ Risk-based authentication – Sometimes called adaptive multi-factor authentication, this method combines adaptive authentication and algorithms that calculate risk and observe the context of specific login requests. The goal of this method is to reduce redundant logins and provide a more user-friendly workflow.

+ Push-based 2FA – Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security while improving ease of use. It confirms a user's identity with multiple factors of authentication that other methods cannot. Because push-based 2FA sends notifications through data networks like cellular or Wi-Fi, users must have data access on their mobile devices to use the 2FA functionality.

Reference: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.htmlThe two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint,face, and retina scans. Biometrics is used commonly in mobile devices).

Question: 135

[Secure Network Access, Visibility, and Enforcement]

Which two kinds of attacks are prevented by multifactor authentication? (Choose two)

A. phishing
B. brute force
C. man-in-the-middle
D. DDOS
E. teardrop

Answer: A,B

Explanation:

Multi-factor authentication (MFA) is a method of verifying a user's identity by requiring two or more factors, such as something the user knows (e.g. password), something the user has (e.g. token), or something the user is (e.g. biometric). MFA can prevent or mitigate some common types of cyberattacks that rely on stealing or guessing a user's credentials, such as phishing and brute force attacks12

Phishing is an attack where an attacker sends a fraudulent email or message that appears to come from a legitimate source, such as a bank or a government agency, and tries to trick the user into clicking on a malicious link or attachment, or providing their credentials or personal information34 MFA can prevent phishing attacks by requiring an additional factor of authentication that the attacker cannot obtain from the phishing email or message, such as a one-time password (OTP) sent to the user's phone or email, or a biometric verification such as a fingerprint or face scan56
Brute force is an attack where an attacker tries to guess a user's password by systematically trying different combinations of characters, words, or phrases until they find the correct one. MFA can prevent brute force attacks by requiring an additional factor of authentication that the attacker cannot guess, such as a physical token or a push notification that the user has to approve.
: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 course overview 2: What Type of Attacks Does MFA Prevent? | OneLogin 3: 5 Multi-Factor Authentication Vulnerabilities and How to Resolve Them 4: FBI warns about attacks that bypass multi-factor authentication (MFA) 5: Defend your users from MFA fatigue attacks - Microsoft Community Hub 6: What type of attacks does Multi-Factor Authentication prevent? : How to Prevent Brute Force Attacks | Cloudflare : Brute Force Attack - an overview | ScienceDirect Topics : Multi-factor authentication - Wikipedia : Multi-factor authentication fatigue attacks are on the rise: How to defend against them | CSO Online

Question: 136

[Endpoint Protection and Detection]

What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.
B. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.
C. EPP focuses on network security, and EDR focuses on device security.
D. EDR focuses on network security, and EPP focuses on device security.

Answer: A

Explanation:

Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) are both important components of an endpoint security strategy, but they have different goals and capabilities. EPP is designed to act as a preventive security measure, blocking known and unknown malware and malicious activity on endpoint devices using various techniques such as antivirus, data encryption, and data loss prevention. EPP solutions are mainly cloud-managed and assisted by cloud data, and use multiple detection engines such as signature-based, machine learning, and behavioral analysis. EPP solutions

prevent breaches by leveraging threat intelligence and sandboxing capabilities to continuously protect endpoints from emerging threats12.

EDR, on the other hand, focuses on detecting and responding to advanced threats that have already evaded the front-line defenses and infiltrated the environment. EDR solutions provide continuous and comprehensive visibility into endpoint activity in real time, allowing security teams to quickly and effectively identify and remediate cyberattacks such as ransomware and fileless malware. EDR solutions offer advanced threat detection, investigation, and response capabilities, including incident data search and investigation, alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment. EDR solutions serve as a safety net to capture threats that go undetected by traditional antivirus software and uncover incidents that would otherwise remain invisible34.

Therefore, the primary difference between an EPP and an EDR is that EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses. Reference: 1: Endpoint Protection Platform (EPP) Definition - Cisco 2: EPP vs. EDR: Why You Need Both - CrowdStrike 3: Endpoint Detection and Response (EDR) Definition - Cisco 4: EDR vs EPP: Why Should You Have to Choose? - Check Point Software

Question: 137

[Endpoint Protection and Detection]

An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group. Which probe must be enabled for this type of profiling to work?

A. NetFlow
B. NMAP
C. SNMP
D. DHCP

Answer: B

Explanation:

Cisco ISE can determine the type of device or endpoint connecting to the network by performing "profiling."

Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint.

NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address.

Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes:

+ EndPointPolicy
+ LastNmapScanCount
+ NmapScanCount
+ OUI
+ Operating-system

Reference: http://www.network-node.com/blog/2016/1/2/ise-20-profiling

Question: 138

[Secure Network Access, Visibility, and Enforcement]

What are two reasons for implementing a multifactor authentication solution such as Duo Security provide to an organization? (Choose two)

A. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes, and push notifications
B. single sign-on access to on-premises and cloud applications
C. integration with 802.1x security using native Microsoft Windows supplicant
D. secure access to on-premises and cloud applications
E. identification and correction of application vulnerabilities before allowing access to resources

Answer: A,D

Explanation:

Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.

Note: Single sign-on (SSO) is a property of identity and access management that enables users to securely authenticate with multiple applications and websites by logging in only once with just one set of credentials (username and password). With SSO, the application or website that the user is trying to access relies on a trusted third party to verify that users are who they say they are.

Question: 139

[Security Concepts]

An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network. Which action tests the routing?

A. Ensure that the client computers are pointing to the on-premises DNS servers.
B. Enable the Intelligent Proxy to validate that traffic is being routed correctly.
C. Add the public IP address that the client computers are behind to a Core Identity.
D. Browse to http://welcome.umbrella.com/ to validate that the new identity is working.

Answer: D

Explanation:

the routing of traffic through the Cisco Umbrella network is to browse
to http://welcome.umbrella.com/. This URL will display a message that confirms whether the new network identity is working or not. If the message says “You’re protected by Cisco Umbrella”, then the traffic is being routed correctly. If the message says “You’re not using Cisco Umbrella”, then the traffic is not being routed correctly and the configuration needs to

be checked. The other options are not valid actions to test the routing. Option A is incorrect because the client computers should point to the Cisco Umbrella DNS servers, not the on-premises DNS servers. Option B is incorrect because the Intelligent Proxy is a feature that selectively intercepts and proxies web requests for deeper inspection, not a tool to test the routing. Option C is incorrect because adding the public IP address to a Core Identity is a way to identify the network, not a way to test the routing. Reference: How To: Successfully test to ensure you're running Umbrella correctly Add a Network Identity

Question: 140

[Security Concepts]
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

A. File Analysis
B. SafeSearch
C. SSL Decryption
D. Destination Lists

Answer: C

Explanation:

SSL Decryption is an important part of the Umbrella Intelligent Proxy. he feature allows the Intelligent Proxy to go beyond simply inspecting normal URLs and actually proxy and inspect traffic that's sent over HTTPS. The SSL Decryption feature does require the root certificate be installed. Reference: https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the- IntelligentProxy

Question: 141

[Security Operations]
How is Cisco Umbrella configured to log only security events?

A. per policy
B. in the Reporting settings
C. in the Security Settings section
D. per network in the Deployments section

Answer: A

Explanation:

The logging of your identities' activities is set per-policy when you first create a policy. By default, logging is on and set to log all requests an identity makes to reach destinations. At any time after you create a policy, you can change what level of identity activity Umbrella logs.

From the Policy wizard, log settings are:

Log All Requests—For full logging, whether for content, security or otherwise

Log Only Security Events—For security logging only, which gives your users more privacy—a good setting for people with the roaming client installed on personal devices

Don't Log Any Requests—Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on.

Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

Question: 142

[Secure Network Access, Visibility, and Enforcement]

How does Cisco Umbrella archive logs to an enterprise owned storage?

A. by using the Application Programming Interface to fetch the logs
B. by sending logs via syslog to an on-premises or cloud-based syslog server
C. by the system administrator downloading the logs from the Cisco Umbrella web portal
D. by being configured to send logs to a self-managed AWS S3 bucket

Answer: D

Explanation:

The Cisco Umbrella Multi-Org console has the ability to upload, store, and archive traffic activity logs from your organizations' Umbrella dashboards to the cloud through Amazon S3. CSV formatted Umbrella logs are compressed (gzip) and uploaded every ten minutes so that there's a minimum of delay between traffic from the organization's Umbrella dashboard being logged and then being available to download from an S3 bucket.

By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage.

Reference: https://docs.umbrella.com/deployment-umbrella/docs/manage-logs

Question: 143

[Security Concepts]

When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

A. Application Control
B. Security Category Blocking
C. Content Category Blocking
D. File Analysis

Answer: B

Explanation:

Cisco Umbrella groups harmful destinations into categories of security threat, such as Malware, Command Control Callbacks, Phishing Attacks, Dynamic DNS, Potentially Harmful Domains, DNS Tunneling VPN, and Cryptomining1. When web policies are configured in Cisco Umbrella, the security category blocking provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats. By enabling or disabling these categories, the administrator can control the identity access to these destinations and protect the network from malicious traffic2.
Reference: 1: Security Categories - Umbrella User Guide 2: Manage Security Settings - Umbrella User Guide

Question: 144

[Security Concepts]
Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

A. AMP
B. AnyConnect
C. DynDNS
D. Talos

Answer: D

Explanation:

When Umbrella receives a DNS request, it uses intelligence to determine if the request is safe, malicious or risky — meaning the domain contains both malicious and legitimate content. Safe and malicious requests are routed as usual or blocked, respectively. Risky requests are routed to our cloud-based proxy for deeper inspection. The Umbrella proxy uses Cisco Talos web reputation and other third-party feeds to determine if a URL is malicious.

Question: 145

[Security Concepts]
Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings
B. content categories
C. security settings
D. destination lists

Answer: D

Explanation:

A destination list is a list of internet destinations that can be blocked or allowed based on the administrative preferences for the policies applied to the identities within your organization. A destination is an IP address (IPv4), URL, or fully qualified domain name. You can add a destination list to Umbrella at any time; however, a destination list does not come into use until it is added to a policy.
Reference: https://docs.umbrella.com/deployment-umbrella/docs/working-with-destination-lists

Question: 146

[Network Security]
Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?

A. Cisco Stealthwatch
B. Cisco Umbrella
C. Cisco Firepower
D. NGIPS

Answer: B

Explanation:

Cisco Umbrella protects users from accessing malicious domains by proactively analyzing and blocking unsafe destinations – before a connection is ever made. Thus it can protect from phishing attacks by blocking suspicious domains when users click on the given links that an attacker sent.

Cisco Umbrella roaming protects your employees even when they are off the VPN.

Question: 147

[Security Concepts]
How does Cisco Stealthwatch Cloud provide security for cloud environments?

A. It delivers visibility and threat detection.
B. It prevents exfiltration of sensitive data.
C. It assigns Internet-based DNS protection for clients and servers.
D. It facilitates secure connectivity between public and private networks.

Answer: A

Explanation:

Cisco Stealthwatch Cloud: Available as an SaaS product offer to provide visibility and threat detection within public cloud infrastructures such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Question: 148

[Security Concepts]
What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two)

A. data exfiltration
B. command and control communication
C. intelligent proxy
D. snort
E. URL categorization

Answer: A,B

Explanation:

Cisco Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution automatically identifies and investigates suspicious or malicious webbased traffic. It identifies both potential and confirmed threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign

that has spread across multiple organizations or a unique threat you've never seen before. Detection and analytics features provided in Cognitive Threat Analytics are shown below: + Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content + Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats

Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat- analytics/at-aglance-c45-736555.pdf

Question: 149

[Security Operations]
Which network monitoring solution uses streams and pushes operational data to provide a near real time view of activity?

A. SNMP
B. SMTP
C. syslog
D. model-driven telemetry

Answer: D

Explanation:

The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data. Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc. Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming.
Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide

Question: 150

[Security Concepts]
What provides visibility and awareness into what is currently occurring on the network?

A. CMX
B. WMI
C. Prime Infrastructure
D. Telemetry

Answer: D

Explanation:

Telemetry – Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the

device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks.

Reference:

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/active threat-analytics-premier.pdf

Question: 151

[Security Concepts]

What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?

A. Cisco Umbrella
B. External Threat Feeds
C. Cisco Threat Grid
D. Cisco Stealthwatch

Answer: C

Explanation:

Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically.

Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat- intelligencedirector

Question: 152

[Security Concepts]

Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?

A. Cisco Security Intelligence
B. Cisco Application Visibility and Control
C. Cisco Model Driven Telemetry
D. Cisco DNA Center

Answer: B

Explanation:

The Cisco Application Visibility and Control (AVC) solution leverages multiple technologies to recognize, analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. AVC combines several Cisco IOS/IOS XE components, as well as communicating with external tools, to integrate the following functions into a powerful solution… Reference: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/avc_tech_overview.html

Question: 153

[Security Concepts]
Which two activities can be done using Cisco DNA Center? (Choose two)

A. DHCP
B. Design
C. Accounting
D. DNS
E. Provision

Answer: B,E

Explanation:

Cisco DNA Center has four general sections aligned to IT workflows:
Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site.
Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need.
Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and- drop task.
The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity—greatly facilitating remote office setups.
Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows

detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work.
The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks.
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna- center/nb-06- dna-center-so-cte-en.html

Question: 154

[Security Concepts]
What must be used to share data between multiple security products?

A. Cisco Rapid Threat Containment
B. Cisco Platform Exchange Grid
C. Cisco Advanced Malware Protection
D. Cisco Stealthwatch Cloud

Answer: B

Explanation:

To share data between multiple security products, you must use Cisco Platform Exchange Grid (pxGrid). pxGrid is an open and scalable framework that allows for bi-directional any-to-any partner platform integrations. pxGrid uses REST and WebSocket interfaces to exchange intelligence and obtain contextual information from Cisco Identity Services Engine (ISE) and other security products. pxGrid can also direct ISE to contain threats by setting network policies. pxGrid enables crossplatform network system collaboration across your IT infrastructure and helps you monitor security, detect threats, and manage assets, configuration, identity, and access. Reference: Introduction to the Cisco Platform Exchange Grid (pxGrid) in ISE, Cisco Identity Services Engine Administrator Guide, Release 3.3

Question: 155

[Security Concepts]
Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?

A. Advanced Malware Protection
B. Platform Exchange Grid
C. Multifactor Platform Integration
D. Firepower Threat Defense

Answer: B

Explanation:

With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

Question: 156

[Security Concepts]
What is a feature of the open platform capabilities of Cisco DNA Center?

A. intent-based APIs
B. automation adapters
C. domain integration
D. application adapters

Answer: A

Explanation:

Cisco DNA Center is an open and extensible platform that allows third-party applications and processes to exchange data and intelligence with Cisco DNA Center1. One of the features of the open platform capabilities of Cisco DNA Center is the intent-based APIs, which enable DNA Center to provide automation to applications2. Intent-based APIs allow applications to express their intent or desired outcome, and let DNA Center translate that intent into network configurations and policies3. Intent-based APIs simplify the interaction between applications and the network, and enable faster and more consistent service delivery.
: 1: Cisco DNA Center 2.3.5 Data Sheet - Cisco 2: Intent-Based Networking's Next Evolution: The DNA Center Platform - Cisco Blogs 3: Unlocking the Power of Open Platforms with Cisco DNA Center Platform

Question: 157

[Security Concepts]
What is the function of the Context Directory Agent?

A. maintains users' group memberships
B. relays user authentication requests from Web Security Appliance to Active Directory
C. reads the Active Directory logs to map IP addresses to usernames
D. accepts user authentication requests on behalf of Web Security Appliance for user identification

Answer: C

Explanation:

Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to). CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_ovevi w.html

Question: 158

[Network Security]
What is a characteristic of a bridge group in ASA Firewall transparent mode?

A. It includes multiple interfaces and access rules between interfaces are customizable
B. It is a Layer 3 segment and includes one port and customizable access rules
C. It allows ARP traffic with a single access rule
D. It has an IP address on its BVI interface and is used for management traffic

Answer: A

Explanation:

A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.

Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.

You can include multiple interfaces per bridge group. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not

want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired.

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa- 95-generalconfig/intro-fw.htmlNote: BVI interface is not used for management purpose. But we can add a separate Management slot/port interface

www.atmicnetworks.com

that is not part of any bridge group, and that allows only management traffic to the ASA.

Question: 159

[Security Concepts]

When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?

A. Common Security Exploits
B. Common Vulnerabilities and Exposures
C. Common Exploits and Vulnerabilities
D. Common Vulnerabilities, Exploits and Threats

Answer: B

Explanation:

Vendors, security researchers, and vulnerability coordination centers typically assign vulnerabilities an identifier that's disclosed to the public. This identifier is known as the Common Vulnerabilities and Exposures (CVE).

CVE is an industry-wide standard. CVE is sponsored by US-CERT, the office of Cybersecurity and Communications at the U.S. Department of Homeland Security.

The goal of CVE is to make it's easier to share data across tools, vulnerability repositories, and security services.

Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide

Question: 160

[Security Operations]

Which two fields are defined in the NetFlow flow? (Choose two)

A. type of service byte
B. class of service bits
C. Layer 4 protocol type
D. destination port
E. output logical interface

Answer: A,D

Explanation:

Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow:

+ Ingress interface (SNMP ifIndex)

+ Source IP address
+ Destination IP address
+ IP protocol
+ Source port for UDP or TCP, 0 for other protocols
+ Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
+ IP Type of Service

Note: A flow is a unidirectional series of packets between a given source and destination.

Question: 161

[Security Concepts]

What provides the ability to program and monitor networks from somewhere other than the DNAC GUI?

A. NetFlow
B. desktop client
C. ASDM
D. API

Answer: D

Explanation:

The Cisco DNA Center API provides the ability to program and monitor networks from somewhere other than the DNAC GUI. The API is a set of RESTful web services that allow users to interact with Cisco DNA Center programmatically. The API can be used to automate tasks, integrate with third- party applications, or create custom applications. The API exposes the same functionality as the DNAC GUI, such as design, provision, policy, assurance, and platform1. The API also provides documentation, examples, and testing tools for each API call1. Reference := Cisco DNA Center User Guide, Release 2.3.3 Cisco DNA Center User Guide, Release 2.2.2
DNAC Tour Part 1: Introduction to Cisco DNA Center
Cisco DNA Center Platform User Guide, Release 2.2.2

Question: 162

[Security Concepts]

An organization has two machines hosting web applications. Machine 1 is vulnerable to SQL injection while machine 2 is vulnerable to buffer overflows. What action would allow the attacker to gain access to machine 1 but not machine 2?

A. sniffing the packets between the two hosts
B. sending continuous pings
C. overflowing the buffer's memory
D. inserting malicious commands into the database

Answer: D

Explanation:

A SQL injection attack is a type of attack that exploits a vulnerability in a web application that uses user-supplied data to construct SQL statements that interact with a database. By inserting malicious commands into the database, an attacker can execute arbitrary SQL queries or commands on the database server, which may result in data theft, data manipulation, or command execution. Machine 1 is vulnerable to SQL injection because it does not properly validate or sanitize the user input before using it in a SQL statement. Therefore, inserting malicious commands into the database would allow the attacker to gain access to machine 1.

A buffer overflow attack is a type of attack that exploits a vulnerability in a program that does not check the boundaries of a buffer (a temporary storage area for data) before copying data into it. By overflowing the buffer's memory, an attacker can overwrite adjacent memory locations, which may result in corrupting data, crashing the program, or executing malicious code. Machine 2 is vulnerable to buffer overflow because it does not properly handle the size or length of the data that it receives from the user or another source. Therefore, overflowing the buffer's memory would allow the attacker to gain access to machine 2.

Sniffing the packets between the two hosts is a passive attack that involves capturing and analyzing the network traffic that flows between the two machines. This attack may reveal sensitive information, such as credentials, session tokens, or database queries, but it does not directly allow the attacker to gain access to either machine. Sending continuous pings is a type of denial-of-service attack that involves flooding the target machine with ICMP echo request packets, which may consume its network bandwidth or processing resources, but it does not directly allow the attacker to gain access to either machine. Therefore, neither sniffing the packets nor sending continuous pings would allow the attacker to gain access to machine 1 but not machine 2. Reference := Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Web Security, SQL Injection Attacks

Understanding SQL Injection - Cisco, SQL Injection Explained

Buffer Overflow and SQL Injection: To Remotely Attack and … - Springer, Buffer Overflow and SQL Injection Attacks

Question: 163

[Security Concepts]

An organization is trying to improve their Defense in Depth by blocking malicious destinations prior to a connection being established. The solution must be able to block certain applications from being used within the network. Which product should be used to accomplish this goal?

A. Cisco Firepower
B. Cisco Umbrella
C. ISE
D. AMP

Answer: B

Explanation:

Cisco Umbrella protects users from accessing malicious domains by proactively analyzing and blocking unsafe destinations –

before a connection is ever made. Thus it can protect from phishing attacks by blocking suspicious domains when users click on the given links that an attacker sent.

Question: 164

[Secure Network Access, Visibility, and Enforcement]
A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment. Which tool should be used to accomplish this goal?

A. Security Manager
B. Cloudlock
C. Web Security Appliance
D. Cisco ISE

Answer: B

Explanation:
Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

Question: 165

[Security Concepts]
An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used. However, the connection is failing. Which action should be taken to accomplish this goal?

A. Disable telnet using the no ip telnet command.
B. Enable the SSH server using the ip ssh server command.
C. Configure the port using the ip ssh port 22 command.
D. Generate the RSA key using the crypto key generate rsa command.

Answer: D

Explanation:

In this question, the engineer was trying to secure the connection so maybe he was trying to allow SSH to the device. But maybe something went wrong so the connection was failing (the connection used to be good). So maybe he was

missing the “crypto key generate rsa” command.

Question: 166

[Content Security]
A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?

A. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.
B. The file is queued for upload when connectivity is restored.
C. The file upload is abandoned.
D. The ESA immediately makes another attempt to upload the file.

Answer: C

Explanation:

The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796- technoteesa-00.htmlIn this question, it stated “the network is congested” (not the file analysis server was overloaded) so theappliance will not try to upload the file again.

Question: 167

[Security Concepts]
Which type of algorithm provides the highest level of protection against brute-force attacks?

A. PFS
B. HMAC
C. MD5
D. SHA

Answer: A

Explanation:

PFS stands for Perfect Forward Secrecy, which is a property of some cryptographic protocols that ensures that the compromise of a long-term key does not affect the security of past or future sessions. PFS provides the highest level of protection against brute-force attacks, because even if an attacker manages to break the long-term key, they cannot decrypt the previous or subsequent communications that use different session keys. PFS is achieved by using ephemeral or temporary keys that are derived from a Diffie-Hellman key exchange, and are not based on the long-term key. Therefore, each session has a unique and independent key that is not stored or reused. PFS is supported by some protocols such as TLS, SSH, and IPsec123. Reference := 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Securing Networks with Cisco Firepower Next Generation IPS, Lesson 4.1: Deploying Cisco Firepower Next-Generation IPS, Topic 4.1.2: Cisco Firepower NGIPS Device Management 2: What is Perfect Forward Secrecy? | Baeldung on Computer Science4 3: Perfect Forward Secrecy - an overview | ScienceDirect Topics5

Question: 168

[Endpoint Protection and Detection]
What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?

A. posture assessment
B. CoA
C. external identity source
D. SNMP probe

Answer: B

Explanation:

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.
One of the settings to configure the CoA type is “Reauth”. This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.
Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010101.html

Question: 169

[Security Concepts]
A network administrator is configuring a rule in an access control policy to block certain URLs and selects the “Chat and Instant Messaging” category. Which reputation score should be selected to accomplish this goal?

A. 1
B. 3
C. 5

www.atmicnetworks.com

D. 10

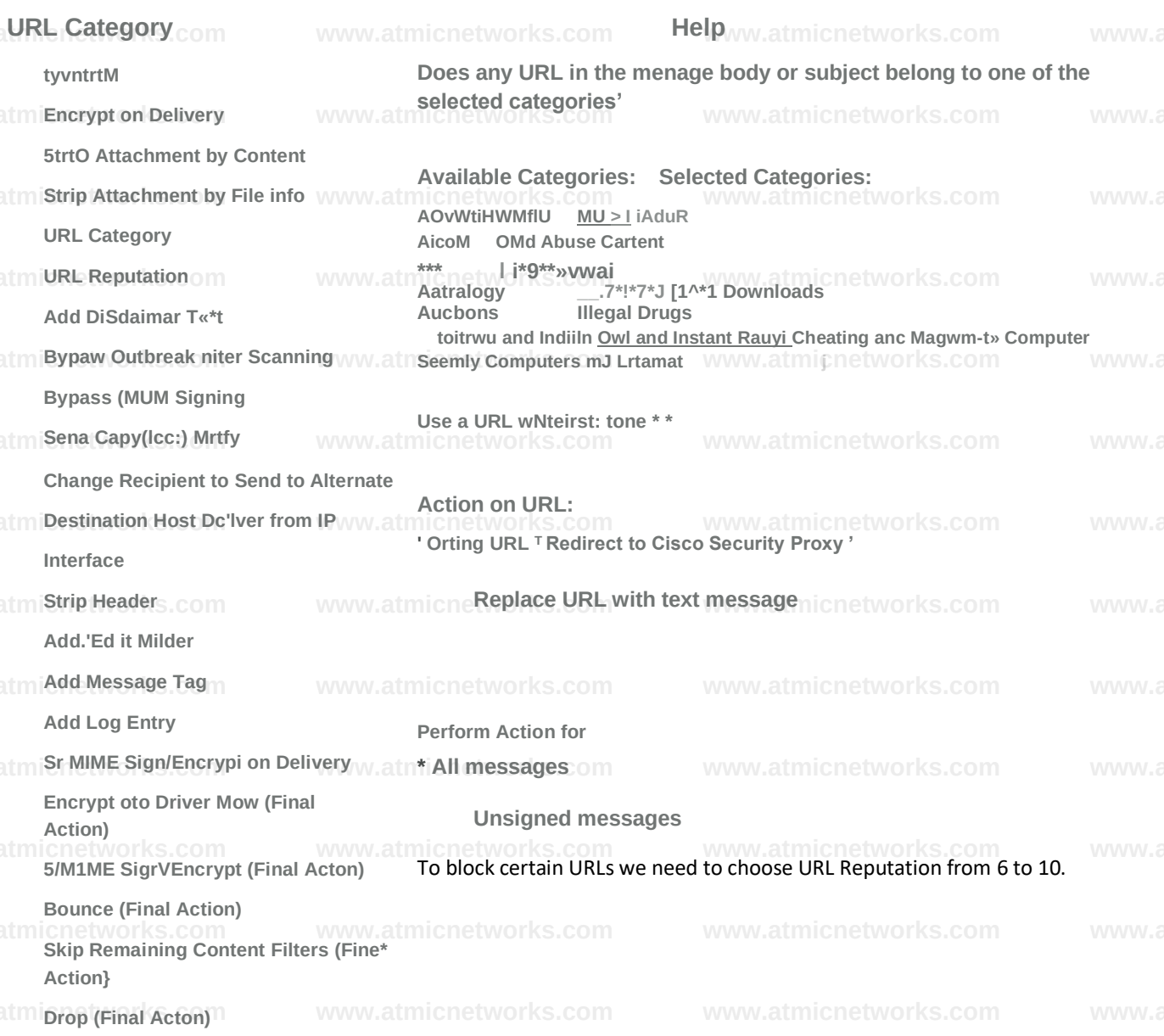
Answer: D

Explanation:

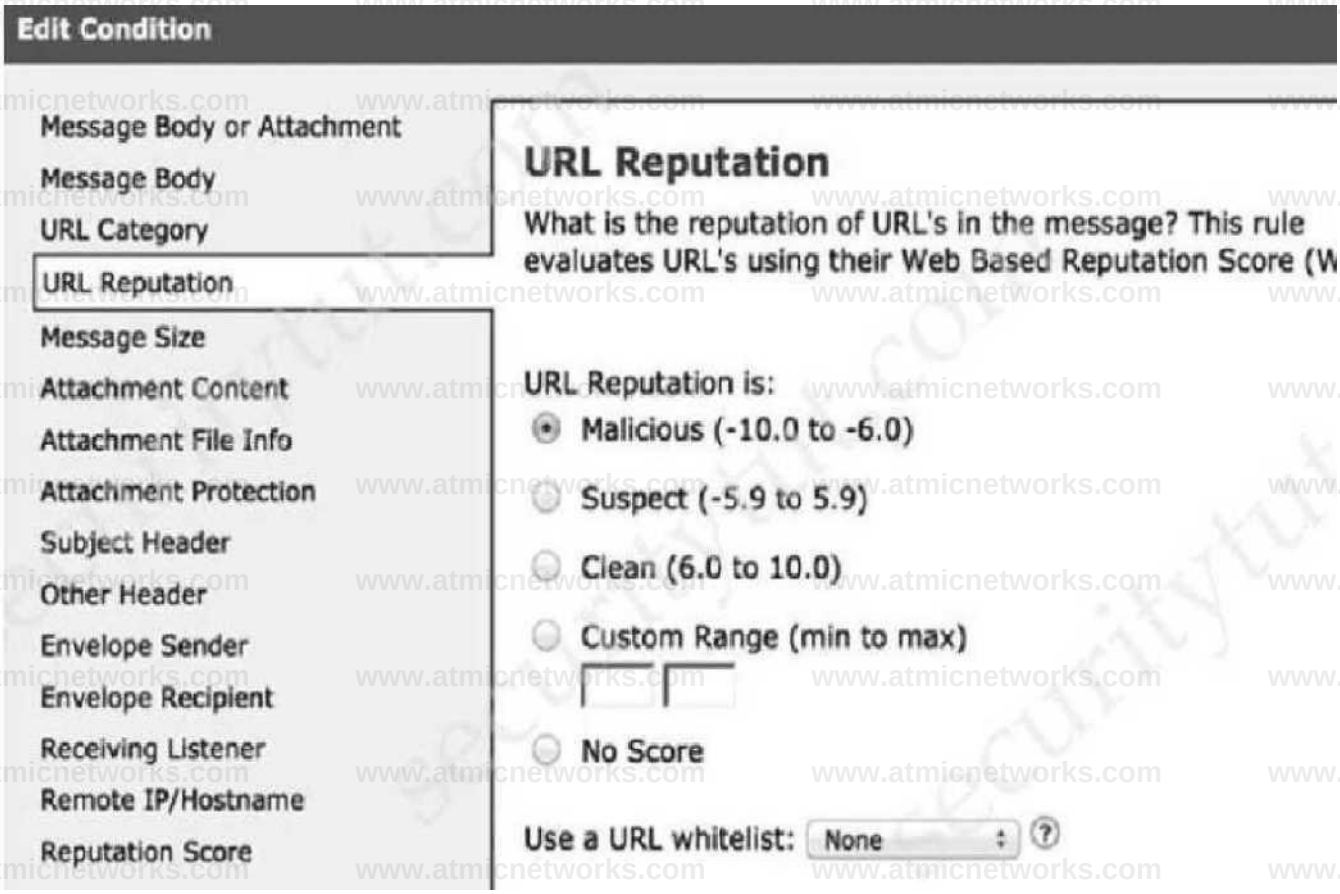
www.atmicnetworks.com

We choose “Chat and Instant Messaging” category in “URL Category”:





To block certain URLs we need to choose URL Reputation from 6 to 10.



Question: 170

[Security Concepts]

Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?

A. PSIRT
B. Talos
C. CSIRT
D. DEVNET

Answer: B

Explanation:

Talos Threat Source is a regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news.

Reference: https://talosintelligence.com/newsletters

Question: 171

[Security Concepts]
What are the two types of managed Intercloud Fabric deployment models? (Choose two.)

A. Public managed
B. Service Provider managed
C. Enterprise managed
D. User managed
E. Hybrid managed

Answer: B,C

Explanation:

Many enterprises prefer to deploy development workloads in the public cloud, primarily for convenience and faster deployment. This approach can cause concern for IT administrators, who must control the flow of IT traffic and spending and help ensure the security of data and intellectual property. Without the proper controls, data and intellectual property can escape this oversight. The Cisco Intercloud Fabric solution helps control this shadow IT, discovering resources deployed in the public cloud outside IT control and placing these resources under Cisco Intercloud Fabric control.

Cisco Intercloud Fabric addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed (an enterprise manages its own cloud environments) and Service
Provider Managed (the service provider administers and controls all cloud resources).

Reference:
https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_2.html

Question: 172

[Security Concepts]
What are two DDoS attack categories? (Choose two)

A. sequential
B. protocol
C. database
D. volume-based
E. screen-based

www.atmicnetworks.com

Answer: B,D

Explanation:

There are three basic categories of attack:
+ volume-based attacks, which use high traffic to inundate the network bandwidth
+ protocol attacks, which focus on exploiting server resources
+ application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks
Reference: https://www.esecurityplanet.com/networks/types-of-ddos- attacks/

Question: 173

[Secure Network Access, Visibility, and Enforcement] Refer to the exhibit.

```
info: New SMTP ICID 30 interface Management (132.168.0.100) address
  10.128.128.200 reverse dns host unknown verified no
info: ICID 30 ACCEPT SG SUSPECTLIST match stars[none] SBRS None
Info: ICID 30 TLS success protocol TLSv1 cipher
  □HE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using AUTH
  mechanism: LOGIN with profile: ldap_smtp
info: MID 80 matched all recipients for per-recipient policy DEFAULT
  in the outbound table
```

Which type of authentication is in use?

A. LDAP authentication for Microsoft Outlook
B. POP3 authentication
C. SMTP relay server authentication
D. external user and relay mail authentication

Answer: A

Explanation:

The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If

a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844- technoteesa-00.htmlThe exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

Question: 174

[Content Security]
An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically.
What must be configured to accomplish this?

A. Configure the Cisco WSA to modify policies based on the traffic seen
B. Configure the Cisco ESA to receive real-time updates from Talos
C. Configure the Cisco WSA to receive real-time updates from Talos
D. Configure the Cisco ESA to modify policies based on the traffic seen

Answer: D

Explanation:

The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.



Question: 175

[Security Concepts]

Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

A. Encrypted Traffic Analytics
B. Threat Intelligence Director
C. Cognitive Threat Analytics
D. Cisco Talos Intelligence

Answer: B

Explanation:

The product that allows Cisco FMC to push security intelligence observable to its sensors from other products is Threat Intelligence Director (TID). TID is a feature of Cisco FMC that enables you to integrate third-party threat intelligence feeds

into your security policies. TID collects, aggregates, and correlates observables from multiple sources, such as Cisco Talos Intelligence, Cisco Umbrella, and other external providers. TID then pushes the observables to the sensors that are managed by FMC, such as Firepower Threat Defense (FTD) devices, Firepower appliances, and Cisco Secure Firewall Cloud Native. The sensors can then use the observables to block or monitor traffic based on the reputation and threat level of the IP addresses, URLs, and domains12.

: 1: Firepower Management Center Configuration Guide, Version 6.6 - Threat Intelligence Director [Cisco Secure Firewall Management Center] - Cisco 2: Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.6 - Threat Intelligence Director [Cisco Firepower NGFW] - Cisco

Question: 176

[Content Security]

What are two differences between a Cisco WSA that is running in transparent mode and one running in explicit mode? (Choose two)

A. The Cisco WSA responds with its own IP address only if it is running in explicit mode.
B. The Cisco WSA is configured in a web browser only if it is running in transparent mode.
C. The Cisco WSA responds with its own IP address only if it is running in transparent mode.
D. The Cisco WSA uses a Layer 3 device to redirect traffic only if it is running in transparent mode.
E. When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request destination.

Answer: A,D

Explanation:

In explicit proxy mode, users are configured to use a web proxy and the web traffic is sent directly to the Cisco WSA. In contrast, in transparent proxy mode the Cisco WSA intercepts user's web traffic redirected from other network devices, such as switches, routers, or firewalls.

Question: 177

[Content Security]

After a recent breach, an organization determined that phishing was used to gain initial access to the network before regaining persistence. The information gained from the phishing attack was a result of users visiting known malicious websites. What must be done in order to prevent this from

happening in the future?

A. Modify an access policy
B. Modify identification profiles

C. Modify outbound malware scanning policies
D. Modify web proxy settings

Answer: D

Explanation:

URL conditions in access control rules allow you to limit the websites that users on your network can access. This feature is called URL filtering. There are two ways you can use access control to specify URLs you want to block (or, conversely, allow):

– With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic.

– With a URL Filtering license, you can also control access to websites based on the URL's general classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details.

Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules URL_Filtering.html

Question: 178

[Security Concepts]
What is the function of SDN southbound API protocols?

A. to allow for the dynamic configuration of control plane applications
B. to enable the controller to make changes
C. to enable the controller to use REST
D. to allow for the static configuration of control plane applications

Answer: B

Explanation:

Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs.
Reference: https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2

Note: Southbound APIs helps us communicate with data plane (not control plane) applications

Question: 179

[Security Concepts]
Refer to the exhibit.

```
> show crypto ipsec sa interface: Outside
      Crypto map tag: CSM Outside map, seq num: 1, local addr: 209.165.200.225

         access-list CSMIPSECACLl extended permit ip 10.0.11.0
255.255.255.0 10.0.10.0 255.255.255.0
         local ident (addr/mask/prot/port): (10.0.11.0/255.255.255.0/0/0)
         remote ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0)
         current peer: 209.165.202.129

         Dpkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
         *pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
         Hpkts compressed: 0, #pkts decompressed: 0
         Mpkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
         #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
         #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
         #TFC rcvd: 0, #TFC sent: 0
         (♦Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
         *send errors: 0, #recv errors: 0

         local crypto endpt.: 209,165,200.225/500, remote crypto endpt.:
209.165.202.129/500
         path mtu 1500, ipsec overhead 55(36), media mtu 1500
         PMTU time remaining (sec): 0, DF policy: copy-df
         ICMP error validation: disabled, TFC packets: disabled
         current outbound spi: B6F5EA53
         current inbound spi : 84348DEE
```

Traffic is not passing through IPsec site-to-site VPN on the Firepower Threat Defense appliance. What is causing this issue?

A. No split-tunnel policy is defined on the Firepower Threat Defense appliance.
B. The access control policy is not allowing VPN traffic in.
C. Site-to-site VPN peers are using different encryption algorithms.
D. Site-to-site VPN preshared keys are mismatched.

Answer: A

Explanation:

If sysopt permit-vpn is not enabled then an access control policy must be created to allow the VPN traffic through the FTD device. If sysopt permit-vpn is enabled skip creating an access control policy. Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike- protocols/215470- site-to-site-vpn-

www.atmicnetworks.com

configuration-on-ftd-ma.html

Question: 180

[Security Concepts]

An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which vulnerability allows the attacker to see the passwords being transmitted in clear text?

A. weak passwords for authentication
B. unencrypted links for traffic
C. software bugs on applications
D. improper file security

Answer: B

Explanation:

The vulnerability that allows the attacker to see the passwords being transmitted in clear text is the lack of encryption on the VPN links. Encryption is a process of transforming data into an unreadable form, so that only authorized parties can access it. VPN (Virtual Private Network) is a technology that creates a secure tunnel between two or more devices over a public network, such as the Internet. VPN links should be encrypted to prevent eavesdropping, tampering, or spoofing of the data that passes through them. If the VPN links are not encrypted, an attacker can use a packet sniffer to intercept and read the data, including the passwords, that are sent over the network. This is called a sniffing attack, and it can lead to credential theft, identity spoofing, or data manipulation. Therefore, VPN links should always use strong encryption protocols, such as IPsec or SSL/TLS, to protect the

confidentiality and integrity of the data. Reference :=

Some possible references are:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 - Cisco: This is the official course page for the SCOR 350-701 exam, which covers the topics of implementing and operating Cisco security core technologies. It provides the course objectives, outline, duration, and prerequisites. It also offers various learning options, such as instructor-led training, e-learning, and practice exams.

SCOR 350-701 Official Cert Guide - Cisco Press: This is the official study guide for the SCOR 350-701 exam, written by Omar Santos, a principal engineer at Cisco's Security Research and Operations group. It covers all the exam topics in depth, with s, examples, exercises, and practice questions. It also includes a companion website with online resources, such as videos, quizzes, flashcards, and more.

Cleartext submission of password - PortSwigger: This is a web security article that explains the vulnerability of transmitting passwords over unencrypted connections, and how to exploit it using Burp Suite, a web application testing tool. It also provides some remediation advice, such as using HTTPS and HSTS to enforce encryption.

What Are Sniffing Attacks, and How Can You Protect Yourself? - EC-Council: This is a blog post that describes what sniffing attacks are, how they work, and what are the common types and tools of sniffing attacks. It also provides some tips on how to prevent or detect sniffing attacks, such as using encryption, VPN, firewall, IDS, and anti-sniffing software.

OWASP Application Security FAQ | OWASP Foundation: This is a frequently asked questions page about application security, maintained by the Open Web Application Security Project (OWASP), a non-profit organization that promotes web security awareness and best practices. It covers various topics, such as authentication, authorization, session management, input

validation, output encoding, cryptography, error handling, logging, and more.

Question: 181

[Security Concepts]
Using Cisco Firepower's Security Intelligence policies, upon which two criteria is Firepower block based? (Choose two)

A. URLs
B. protocol IDs
C. IP addresses
D. MAC addresses
E. port numbers

Answer: A,C

Explanation:

Security Intelligence Sources

Custom Block lists or feeds (or objects or groups)
Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.)
For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed, add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-configguide-v623/security_intelligence_blacklisting.html

Question: 182

[Content Security]
Which Cisco platform ensures that machines that connect to organizational networks have the recommended antivirus definitions and patches to help prevent an organizational malware outbreak?

A. Cisco WiSM
B. Cisco ESA
C. Cisco ISE
D. Cisco Prime Infrastructure

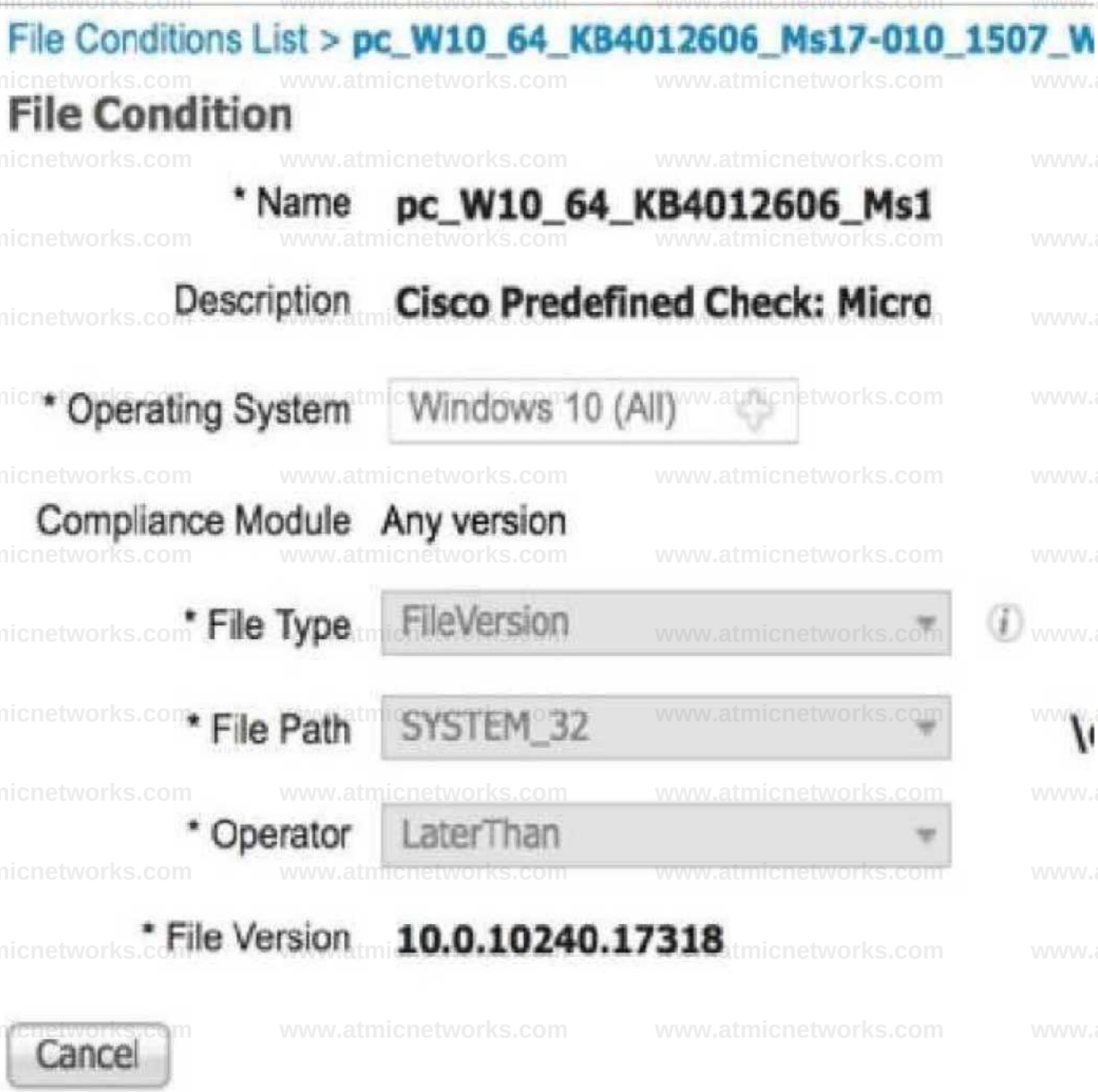
www.atmicnetworks.com

Answer: C

Explanation:

A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. We can configure ISE to check for the Windows patch at Work Centers > Posture > Posture Elements > Conditions > File.

In this example, we are going to use the predefined file check to ensure that our Windows 10 clients have the critical security patch installed to prevent the Wanna Cry malware; and we can also configure ISE to update the client with this patch.



Question: 183

[Security Operations]
What are two benefits of Flexible NetFlow records? (Choose two)

A. They allow the user to configure flow information to perform customized traffic identification
B. They provide attack prevention by dropping the traffic
C. They provide accounting and billing enhancements
D. They converge multiple accounting technologies into one accounting mechanism
E. They provide monitoring of a wider range of IP packet information from Layer 2 to 4

Answer: A,D

Explanation:

NetFlow is typically used for several key customer applications, including the following:

Billing and accounting. NetFlow data provides fine-grained metering (for instance, flow data includes details such as IP addresses, packet and byte counts, time stamps, type of service (ToS), and application ports) for highly flexible and detailed resource utilization accounting. Service providers may use the information for billing based on time of day, bandwidth usage, application usage, quality of service, and so on. Enterprise customers may use the information for departmental charge back or cost allocation for resource utilization.

Reference:
https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon_extern al_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyond theselayers.

Question: 184

[Security Concepts]
How does DNS Tunneling exfiltrate data?

A. An attacker registers a domain that a client connects to based on DNS records and sends malware throughthat connection.
B. An attacker opens a reverse DNS shell to get into the client's system and install malware on it.
C. An attacker uses a non-standard DNS port to gain access to the organization's DNS servers in order topoison the resolutions.
D. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a maliciousdomain.

Answer: A

Explanation:

DNS tunneling is a technique that exploits the DNS protocol to tunnel malware and other data through a client-server model. DNS tunneling can be used for data exfiltration, command and control, or IP-over-DNS tunneling. DNS tunneling works by encoding the information of other protocols or programs in DNS queries and responses. An attacker registers a domain, such as badsite.com, and sets up a malicious DNS server that can interpret the encoded data. The attacker then infects a client with malware that can send and receive DNS queries to the attacker's domain. The malware can use DNS queries to request commands from the attacker, or to send sensitive data

to the attacker. The DNS queries and responses look like normal DNS traffic, but they contain hidden data that can bypass network defenses123. Reference := 1: What Is DNS Tunneling? - Palo Alto Networks 2: What is DNS Tunneling? - Check Point Software 3: What Is DNS Tunneling and How to Detect and Prevent Attacks

Question: 185

[Security Concepts]
A user has a device in the network that is receiving too many connection requests from multiple machines.
Which type of attack is the device undergoing?

A. phishing
B. slowloris
C. pharming
D. SYN flood

Answer: D

Explanation:

A SYN flood is a type of denial-of-service (DoS) attack that exploits the TCP three-way handshake process to exhaust the resources of a target server. The attacker sends a large number of SYN packets to the target server, each with a spoofed source IP address. The target server allocates resources for each incoming SYN packet and responds with a SYN-ACK packet to the spoofed address. However, the spoofed address never sends back the final ACK packet to complete the connection, leaving the target server with many half-open connections that eventually fill up its connection table. This prevents the target server from accepting new legitimate connections and causes service disruption123 Reference: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 course overview 2: SYN Flood Explained. How to Prevent this Attack from Taking over your … 3: What is a SYN flood attack? | Cloudflare

Question: 186

[Content Security]
An organization is receiving SPAM emails from a known malicious domain. What must be configured in order to prevent the session during the initial TCP communication?

A. Configure the Cisco ESA to drop the malicious emails
B. Configure policies to quarantine malicious emails

C. Configure policies to stop and reject communication D. Configure the Cisco ESA to reset the TCP connection

Answer: C

Explanation:

The best way to prevent the session during the initial TCP communication is to configure policies to stop and reject communication from the known malicious domain. This will prevent the ESA from accepting any messages from that domain

and send a negative SMTP response code back to the sender. This will also save the ESA's resources and bandwidth, as it will not have to process or store the malicious emails. This can be done by creating a sender group in the Host Access Table (HAT) that matches the malicious domain and setting the mail flow policy to "Reject" or "Throttle". Alternatively, a message filter can be created that checks the envelope sender against the malicious domain and applies the "stop_connection" or "reject_connection" action12.

The other options are not as effective as stopping and rejecting the communication at the TCP level. Configuring the Cisco ESA to drop the malicious emails (option A) will still allow the ESA to accept the messages and then silently discard them, which will consume the ESA's resources and bandwidth, and also not notify the sender of the rejection. Configuring policies to quarantine malicious emails (option B) will also require the ESA to accept and store the messages, which will take up disk space and require manual or automated management of the quarantine. Configuring the Cisco ESA to reset the TCP connection (option D) will abruptly terminate the connection without sending a proper SMTP response code, which may cause the sender to retry the delivery and generate more traffic. Resetting the TCP connection is also considered a less polite and less compliant way of rejecting messages than sending a negative SMTP response code34. Reference: 1: How to Block a Sender Domain on the Email Security Appliance 2: Message Filters on the Cisco Email Security Appliance 3: How to Configure the Cisco Email Security Appliance to Reject or Drop Messages 4: Cisco Email Security Appliance User Guide - Configuring Mail Policies

Question: 187

[Security Concepts]

A Cisco Firepower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose two)

A. permit
B. trust
C. reset
D. allow
E. monitor

Answer: B,E

Explanation:

Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic.

Note: With action "trust", Firepower does not do any more inspection on the traffic. There will be no intrusion protection and also no file-policy on this traffic.

www.atmicnetworks.com

Question: 188

[Securing the Cloud]

An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization's public cloud to send telemetry using the cloud provider's mechanisms to a security device. Which mechanism should the engineer configure to accomplish this goal?

A. mirror port
B. Flow
C. NetFlow
D. VPC flow logs

Answer: D

Explanation:

The mechanism that the engineer should configure to accomplish the goal of sending telemetry using the cloud provider's mechanisms to a security device is VPC flow logs. VPC flow logs are a feature of Google Cloud that capture and record information about the network flows sent from and received by the virtual machines (VMs) inside a VPC network1. VPC flow logs can provide network telemetry data such as source and destination IP addresses, ports, protocols, bytes sent and received, and connection state1. VPC flow logs can be exported to Cloud Logging, Pub/Sub, or Cloud Storage for further analysis by security devices or tools1. VPC flow logs can help the engineer to perform behavioral analysis to detect malicious activity on the hosts, such as network scans, port sweeps, brute force attacks, data exfiltration, or lateral movement2.

The other options are not correct mechanisms to send telemetry using the cloud provider's mechanisms to a security device. Option A is incorrect because mirror port is not a feature of Google

Cloud, but rather a network device configuration that copies traffic from one port to another for monitoring purposes3. Option B is incorrect because flow is not a specific mechanism, but rather a generic term that refers to a sequence of packets between a source and a destination4. Option C is incorrect because NetFlow is not a feature of Google Cloud, but rather a network protocol developed by Cisco that collects and aggregates information about network flows5. NetFlow is not compatible with VPC flow logs, which use a different format6. Reference:

VPC flow logs overview

When to use 5 telemetry types in security threat monitoring

What is a Mirror Port?

What is a Network Flow?

What is NetFlow?

Exporting VPC flow logs to Pub/Sub

Question: 189

[Content Security]

An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly

identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?

A. Configure incoming content filters
B. Use Bounce Verification
C. Configure Directory Harvest Attack Prevention
D. Bypass LDAP access queries in the recipient access table

Answer: C

Explanation:

A Directory Harvest Attack (DHA) is a technique used by spammers to find valid/existent email addresses at a domain either by using Brute force or by guessing valid e-mail addresses at a domain using different permutations of common username. Its easy for attackers to get hold of a valid email address if your organization uses standard format for official e-mail alias (for example: jsmith@example.com). We can configure DHA Prevention to prevent malicious actors from quickly identifying valid recipients.
Note: Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email programs use to look up contact information from a server, such as ClickMail Central Directory. For example, here's an LDAP search translated into plain English: "Search for all people located in Chicago who's name contains "Fred" that have an email address. Please return their full name, email, title, and description.

Question: 190

[Security Operations]
What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

A. Multiple NetFlow collectors are supported
B. Advanced NetFlow v9 templates and legacy v5 formatting are supported
C. Secure NetFlow connections are optimized for Cisco Prime Infrastructure
D. Flow-create events are delayed

Answer: B

Explanation:

The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions:

– Delays the export of flow-create events.

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa- general-cli/ monitor-nsel.pdf

www.atmicnetworks.com

Question: 191

[Network Security]
An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?

A. TCP 6514
B. UDP 1700
C. TCP 49
D. UDP 1812

Answer: B

Explanation:

CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port 1700, while the actual RFC calls out using UDP port 3799.

Question: 192

[Network Security]
Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

A. Google Cloud Platform
B. Red Hat Enterprise Visualization
C. VMware ESXi
D. Amazon Web Services

Answer: D

Explanation:

Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall.
The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure.
In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.
In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions.

www.atmicnetworks.com

Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual- appliance-asav/ white-paper-c11-740505.html

Question: 193

[Secure Network Access, Visibility, and Enforcement]
What is the purpose of the My Devices Portal in a Cisco ISE environment?

A. to register new laptops and mobile devices
B. to request a newly provisioned mobile device
C. to provision userless and agentless systems
D. to manage and deploy antivirus definitions and patches on systems owned by the end user

Answer: A

Explanation:

Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network.
Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html

Question: 194

[Security Concepts]
Refer to the exhibit.

```
ip dhcp snooping
ip dhcp snooping vlan 41,44

interface GigabitEthernet1/0/1
 description    Uplink_To_Distro_Switch_g1/0/11
 switchport trunk native vlan 999 switchport
 trunk allowed vlan 40,41,44 switchport mode
 trunk
```

An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?

A. ip dhcp snooping verify mac-address
B. ip dhcp snooping limit 41
C. ip dhcp snooping vlan 41
D. ip dhcp snooping trust

Answer: D

Explanation:

To understand DHCP snooping we need to learn about DHCP spoofing attack first.

DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle". The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.

DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.

Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.

The port connected to a DHCP server should be configured as trusted port with the "ip dhcp snooping trust" command. Other ports connecting to hosts are untrusted ports by default. In this question, we need to configure the uplink to "trust" (under interface Gi1/0/1) as shown below.

Question: 195

[Security Concepts]

What is the purpose of the certificate signing request when adding a new certificate for a server?

A. It is the password for the certificate that is needed to install it with.
B. It provides the server information so a certificate can be created and signed
C. It provides the certificate client information so the server can authenticate against it when installing
D. It is the certificate that will be loaded onto the server

www.atmicnetworks.com

Answer: B

Explanation:

A certificate signing request (CSR) is one of the first steps towards getting your own SSL Certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) that the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key

Question: 196

[Security Concepts]
What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

A. Cisco Cloudlock
B. Cisco Umbrella
C. Cisco AMP
D. Cisco App Dynamics

Answer: A

Explanation:

Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely.
It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

Question: 197

[Security Concepts]
What is managed by Cisco Security Manager?

A. access point
B. WSA
C. ASA
D. ESA

Answer: C

Explanation:

Cisco Security Manager provides a comprehensive management solution for:
– Cisco ASA 5500 Series Adaptive Security Appliances
– Cisco intrusion prevention systems 4200 and 4500 Series Sensors
– Cisco AnyConnect Secure Mobility Client
Reference: https://www.cisco.com/c/en/us/products/security/security-manager/index.html

Question: 198

[Content Security]
How does Cisco Advanced Phishing Protection protect users?

A. It validates the sender by using DKIM.
B. It determines which identities are perceived by the sender
C. It utilizes sensors that send messages securely.
D. It uses machine learning and real-time behavior analytics.

Answer: B

Explanation:

Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats.
Reference: https://docs.ces.cisco.com/docs/advanced-phishing-protection

Question: 199

[Security Concepts]
What is a benefit of using Cisco FMC over Cisco ASDM?

A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
B. Cisco FMC provides centralized management while Cisco ASDM does not.
C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices

Answer: B

Explanation:

Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by

the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct
Reference: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheetc78-736775.html

Question: 200

[Security Concepts]
What is a key difference between Cisco Firepower and Cisco ASA?

A. Cisco ASA provides access control while Cisco Firepower does not.
B. Cisco Firepower provides identity-based access control while Cisco ASA does not.
C. Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.
D. Cisco ASA provides SSL inspection while Cisco Firepower does not.

Answer: C

Explanation:

Cisco Firepower is a unified security solution that combines firewall, intrusion prevention system (IPS), advanced malware protection (AMP), and threat intelligence features. Cisco ASA is a traditional firewall that focuses on network traffic control based on packet filtering and stateful inspection. One of the key differences between Cisco Firepower and Cisco ASA is that Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not. Intrusion prevention is the process of detecting and blocking malicious network traffic before it reaches the intended target. Cisco Firepower uses a combination of signature-based and behavior-based detection methods to identify and stop known and unknown attacks. Cisco ASA, on the other hand, does not have built-in intrusion prevention capabilities. It can only perform basic packet inspection and filtering based on predefined rules. To enable intrusion prevention on Cisco ASA, an additional module called FirePOWER Services is required. This module integrates Cisco Firepower features into Cisco ASA, but

it is not the same as Cisco Firepower itself. Cisco Firepower offers more advanced and integrated security features than Cisco ASA with FirePOWER Services123. Reference: 1: Cisco ASA vs Cisco Firepower | What are the differences? - StackShare 2: Cisco FTD vs ASA: Difference and Comparison 3: CISCO FIREPOWER VS. ASA - Critical Design

Question: 201

[Security Concepts]
An organization is implementing URL blocking using Cisco Umbrell
a. The users are able to go to some sites
but other sites are not accessible due to an error. Why is the error occurring?
A. Client computers do not have the Cisco Umbrella Root CA certificate installed.
B. IP-Layer Enforcement is not configured.
C. Client computers do not have an SSL certificate deployed from an internal CA server.
D. Intelligent proxy and SSL decryption is disabled in the policy

Answer: A

Explanation:

Other features are dependent on SSL Decryption functionality, which requires the Cisco Umbrella root certificate. Having the SSL Decryption feature improves:
Custom URL Blocking—Required to block the HTTPS version of a URL.

Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed.
Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing.
To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users—if you're a network admin.
Reference: https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import- information

Question: 202

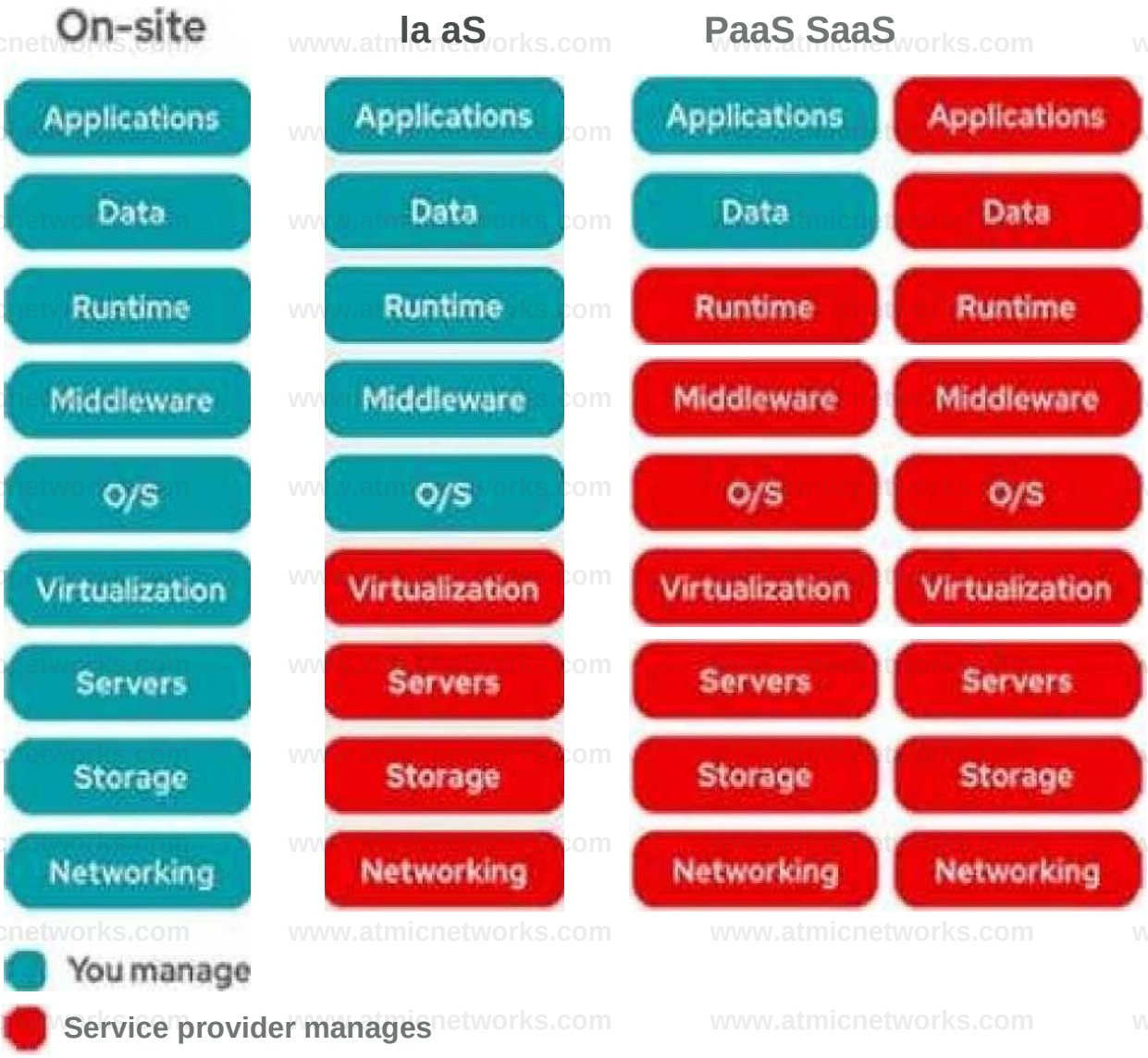
[Securing the Cloud]
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)

A. virtualization
B. middleware
C. operating systems
D. applications
E. data

Answer: D,E

Explanation:

Customers must manage applications and data in PaaS.



Question: 203

[Security Concepts]
What is an attribute of the DevSecOps process?

A. mandated security controls and check lists
B. security scanning and theoretical vulnerabilities
C. development security
D. isolated security team

Answer: C

Explanation:

DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move
security activities to the start of the development life cycle and have built-in security practices in the continuous
integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer
to IT and business objectives.
Three key things make a real DevSecOps environment:
+ Security testing is done by the development team.
+ Issues found during that testing is managed by the development team.
+ Fixing those issues stays within the development team.

Question: 204

[Security Concepts]
An engineer notices traffic interruption on the network. Upon further investigation, it is learned that broadcast
packets have been flooding the network. What must be configured, based on a predefined threshold, to address this issue?

A. Bridge Protocol Data Unit guard
B. embedded event monitoring
C. storm control
D. access control lists

Answer: C

Explanation:

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm. By using the "storm-control broadcast level [falling-threshold]" we can limit the broadcast traffic on the switch.

Question: 205

[Network Security]
Which two cryptographic algorithms are used with IPsec? (Choose two)

A. AES-BAC

www.atmicnetworks.com

B. AES-ABC
C. HMAC-SHA1/SHA2
D. Triple AMC-CBC
E. AES-CBC

Answer: C,E

Explanation:

Cryptographic algorithms defined for use with IPsec include:
+ HMAC-SHA1/SHA2 for integrity protection and authenticity.
+ TripleDES-CBC for confidentiality
+ AES-CBC and AES-CTR for confidentiality.
+ AES-GCM and ChaCha20-Poly1305 providing confidentiality and authentication together efficiently.

Question: 206

[Security Concepts]
In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?

A. LDAP injection
B. man-in-the-middle
C. cross-site scripting
D. insecure API

Answer: B

Explanation:

In a man-in-the-middle (MITM) attack, the attacker inserts their machine between two hosts that are communicating with each other, and secretly relays and possibly alters the messages between them. The attacker can intercept, modify, or spoof the data, and the hosts are unaware that their communication is compromised. A MITM attack can target any communication channel that uses

weak or no encryption, such as email, web, or wireless networks. A MITM attack can break the confidentiality, integrity, and authenticity of the communication, and can have various goals, such as eavesdropping, stealing credentials, impersonating a legitimate party, or redirecting traffic. A MITM attack can be prevented by using strong encryption protocols, such as TLS, IPSec, or SSH, and verifying the identity of the communication endpoints using certificates or other
means. Reference: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Man- in-the-

Question: 207

[Security Concepts]
Which Dos attack uses fragmented packets to crash a target machine?

A. smurf
B. MITM
C. teardrop
D. LAND

Answer: C

Explanation:

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

Question: 208

[Security Concepts]
Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?

A. to prevent theft of the endpoints
B. because defense-in-depth stops at the network
C. to expose the endpoint to more threats
D. because human error or insider threats will still exist

Answer: D

Explanation:

www.atmicnetworks.com

Question: 209

[Security Concepts]
Which type of API is being used when a security application notifies a controller within a software- defined network architecture about a specific security threat?

A. westbound API
B. southbound API
C. northbound API
D. eastbound API

Answer: C

Explanation:

A security application that notifies a controller within a software-defined network architecture about a specific security threat is using a northbound API. A northbound API is an interface that enables communication between the SDN controller and the applications or management systems that use the network services1. A security application can use a northbound API to send alerts, requests, or commands to the SDN controller, which can then take appropriate actions on the network devices or policies2. For example, a security application can use a northbound API to inform the SDN controller about a malicious traffic pattern, and the SDN controller can then block or redirect the traffic using a southbound API3.
: 1: What is Software-Defined Networking (SDN)? | VMware Glossary 2: Intent-Based Networking's Next Evolution: The DNA Center Platform - Cisco Blogs 3: Cisco SDN Security: Securing the Software Defined Network - Cisco

Question: 210

[Network Security]
When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?

A. Multiple routers or VRFs are required.
B. Traffic is distributed statically by default.
C. Floating static routes are required.
D. HSRP is used for faliover.

Answer: A

Explanation:

An active/active FlexVPN configuration allows for multiple routers or VRFs to act as hubs for different VPN

groups, providing load balancing and redundancy1. This is useful when the VPN deployment has a large number of spokes or different security policies for different groups of spokes. DMVPN, on the other hand, only supports a single hub or a pair of hubs in active/standby mode for each VPN group2. This limits the scalability and flexibility of DMVPN deployments. Therefore, an engineer would opt for an active/active FlexVPN configuration as opposed to DMVPN when multiple routers or VRFs are required. Reference :=
Cisco FlexVPN: Benefits and Best Practices
Cisco DMVPN Design Guide

Question: 211

[Security Concepts]
Which algorithm provides asymmetric encryption?

A. RC4
B. AES
C. RSA
D. 3DES

Answer: C

Explanation:

Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner. In asymmetric encryption, the sender uses the recipient's public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key. RSA is one of the most commonly used asymmetric encryption algorithms. It is based on the mathematical problem of factoring large numbers, which is believed to be hard to solve. RSA stands for Rivest-Shamir-Adleman, the names of the three inventors of the algorithm. RSA can be used for both encryption and digital signatures. To generate an RSA key pair, the following steps are performed:

Choose two large prime numbers, p and q, and compute their product, n = pq. This is called the modulus.
Choose a small number, e, that is relatively prime to (p-1)(q-1). This is called the public exponent. Compute a number, d, that satisfies the equation ed ≡ 1 (mod (p-1)(q-1)). This is called the private exponent.
The public key is (n, e) and the private key is (n, d).
To encrypt a message, m, with the public key (n, e), the following formula is used: c = m^e mod n
To decrypt a ciphertext, c, with the private key (n, d), the following formula is used: m = c^d mod n
Reference :=

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 3: VPN

Technologies, Lesson 3.1: Site-to-Site VPNs, Topic 3.1.2: IPsec VPNs
What is Asymmetric Encryption? - GeeksforGeeks
What is asymmetric encryption? | Asymmetric vs. symmetric … - Cloudflare

Question: 212

[Security Concepts]
What are two functions of secret key cryptography? (Choose two)

A. key selection without integer factorization
B. utilization of different keys for encryption and decryption
C. utilization of large prime number iterations
D. provides the capability to only know the key on one side
E. utilization of less memory

Answer: A,E

Explanation:

Secret key cryptography, also known as symmetric key cryptography, is a type of encryption where a single secret key is used for both encryption and decryption of a message. The cryptographic key is kept secret between the sender and receiver, making it difficult for anyone else to decipher the message. Some of the functions of secret key cryptography are:

Key selection without integer factorization: Secret key cryptography does not rely on complex mathematical problems such as integer factorization or discrete logarithms to generate keys. Instead, the keys are chosen randomly or derived from a passphrase or a shared secret. This makes the key generation process faster and simpler than in public key cryptography.

Utilization of less memory: Secret key cryptography uses less memory than public key cryptography, as it only requires one key to be stored and managed. Public key cryptography, on the other hand, requires two keys (public and private) for each user, which increases the memory overhead and complexity of key management.

The other options are not functions of secret key cryptography, but rather characteristics of public key cryptography or asymmetric cryptography, which is a different type of encryption where different keys are used for encryption and decryption. Public key cryptography has the following features: Utilization of different keys for encryption and decryption: Public key cryptography uses a pair of keys, one public and one private, for each user. The public key can be shared with anyone, while the private key must be kept secret. The public key is used to encrypt messages, while the private key is used to decrypt them. This allows users to communicate securely without having to exchange a secret key beforehand.

Utilization of large prime number iterations: Public key cryptography relies on hard mathematical problems such as integer factorization or discrete logarithms to generate keys. These problems involve finding the prime factors of large numbers or finding the discrete logarithms of numbers in a finite field. These problems are easy to solve in one direction, but hard to solve in the reverse direction. For example, it is easy to multiply two large prime numbers, but hard to find the prime factors of the product. This makes the keys hard to break by brute force or other methods.

Provides the capability to only know the key on one side: Public key cryptography enables users to encrypt

www.atmicnetworks.com

messages without knowing the recipient's key, and vice versa. This is possible because the encryption and decryption keys are different and mathematically related. For example, Alice can encrypt a message with Bob's public key, and only Bob can decrypt it with his private key. Alice does not need to know Bob's private key, and Bob does not need to know Alice's key. This also enables public key cryptography to support digital signatures, which are a way of verifying the identity and integrity of a message.

Reference :=

What Is Secret Key Cryptography? A Complete Guide - Helenix

Definition of Secret-key Cryptography - Gartner

Question: 213

[Security Concepts]

For Cisco IOS PKI, which two types of Servers are used as a distribution point for CRLs? (Choose two)

A. SDP
B. LDAP
C. subordinate CA
D. SCP
E. HTTP

Answer: B,E

Explanation:

Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.

A PKI is composed of the following entities: …

– A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pki-overview.html

Question: 214

[Security Concepts]

Which attack type attempts to shut down a machine or network so that users are not able to access it?

A. smurf

www.atmicnetworks.com

B. bluesnarfing
C. MAC spoofing
D. IP spoofing

Answer: A

Explanation:

Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to its intended users.
The Smurf attack is a DDoS attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.

Question: 215

[Network Security]
What is a difference between DMVPN and sVTI?

A. DMVPN supports tunnel encryption, whereas sVTI does not.
B. DMVPN supports dynamic tunnel establishment, whereas sVTI does not.
C. DMVPN supports static tunnel establishment, whereas sVTI does not.
D. DMVPN provides interoperability with other vendors, whereas sVTI does not.

Answer: B

Explanation:

DMVPN and sVTI are both VPN technologies that use IPsec to secure the tunnel traffic. However, they differ in how they establish and manage the tunnels. DMVPN supports dynamic tunnel establishment, which means that the VPN endpoints can create and delete tunnels on demand, based on the routing information. This allows for a scalable and flexible VPN topology, where the endpoints can communicate directly with each other without going through a central hub. sVTI, on the other hand, supports static tunnel establishment, which means that the VPN endpoints have to manually configure the tunnel source and destination addresses. This requires a one-to-one mapping between the endpoints, and limits the VPN topology to a hub-and-spoke model, where the endpoints can only communicate with the hub. Therefore, DMVPN is more suitable for large and dynamic VPN networks, while sVTI is more suitable for small and stable VPN networks. Reference:

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 5: Secure Connectivity, Lesson 5.2: Implementing Site-to-Site VPNs, Topic 5.2.3: Dynamic Multipoint VPN (DMVPN)
what is difference between svti and DVTI? - Cisco Community

www.atmicnetworks.com

Question: 216

[Security Concepts]

What features does Cisco FTDv provide over ASAv?

A. Cisco FTDv runs on VMWare while ASAv does not
B. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not
C. Cisco FTDv runs on AWS while ASAv does not
D. Cisco FTDv supports URL filtering while ASAv does not

Answer: D

Explanation:

Cisco FTDv is a virtual appliance that combines the features of Cisco ASA and Cisco Firepower NGIPS. It provides stateful firewall, IPS, URL filtering, malware protection, and other advanced security functions. Cisco ASAv is a virtual appliance that only provides stateful firewall and VPN features. It does not support URL filtering or other Firepower functions. Therefore, Cisco FTDv provides more features than ASAv, especially for next-generation firewall capabilities. Reference := Cisco Firewall in AWS - Should i use ASAv or FTDv/FMCv?

Difference between Cisco ASAv, NGIPSv and FTDv…?

Are there any differences in features between Cisco ASA hardware …

Question: 217

[Endpoint Protection and Detection]

In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

A. when there is a need for traditional anti-malware detection
B. when there is no need to have the solution centrally managed
C. when there is no firewall on the network
D. when there is a need to have more advanced detection capabilities

Answer: D

Explanation:

Endpoint protection platforms (EPP) prevent endpoint security threats like known and unknown malware. Endpoint detection and response (EDR) solutions can detect and respond to threats that your EPP and other

www.atmicnetworks.com

security tools did not catch.

EDR and EPP have similar goals but are designed to fulfill different purposes. EPP is designed to provide device-level protection by identifying malicious files, detecting potentially malicious activity, and providing tools for incident investigation and response.

The preventative nature of EPP complements proactive EDR. EPP acts as the first line of defense, filtering out attacks that can be detected by the organization's deployed security solutions. EDR acts as a second layer of protection, enabling security analysts to perform threat hunting and identify more subtle threats to the endpoint.

Effective endpoint defense requires a solution that integrates the capabilities of both EDR and EPP to provide protection against cyber threats without overwhelming an organization's security team.

Question: 218

[Security Concepts]

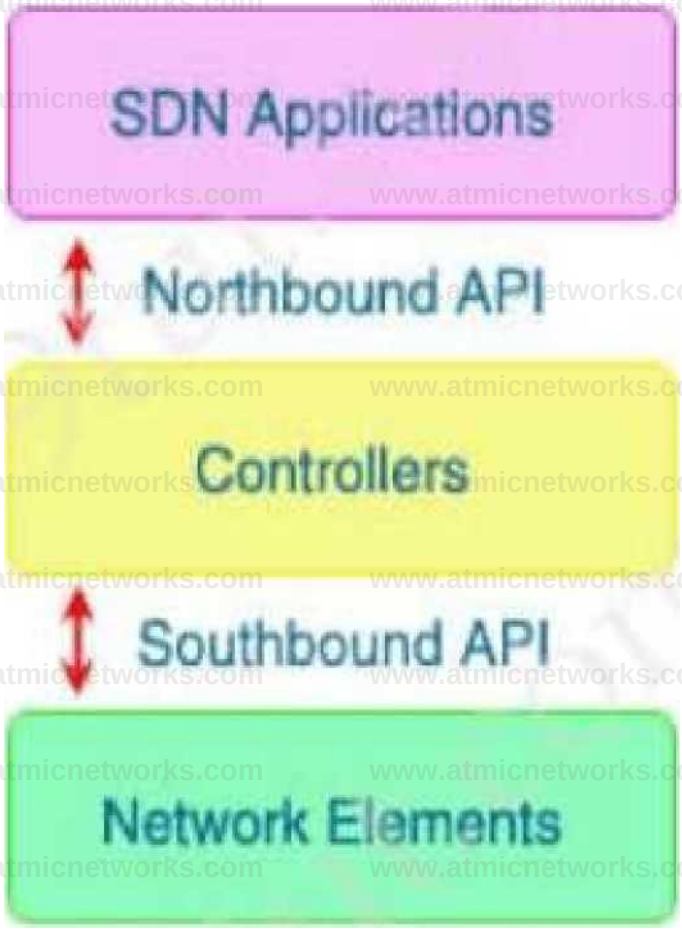
Which type of API is being used when a controller within a software-defined network architecture dynamically makes configuration changes on switches within the network?

A. westbound AP
B. southbound API
C. northbound API
D. eastbound API

Answer: B

Explanation:

Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs.



Question: 219

[Security Concepts]
An organization has two systems in their DMZ that have an unencrypted link between them for communication.
The organization does not have a defined password policy and uses several default accounts on the systems.
The application used on those systems also have not gone through stringent code reviews. Which vulnerability
would help an attacker brute force their way into the systems?

A. weak passwords
B. lack of input validation
C. missing encryption
D. lack of file permission

Answer: C

Explanation:

www.atmicnetworks.com

The version 9 export format uses templates to provide access to observations of IP packet flows in a flexible and extensible manner. A template defines a collection of fields, with corresponding descriptions of structure and semantics.
Reference: https://tools.ietf.org/html/rfc3954

Question: 220

[Network Security]
What is provided by the Secure Hash Algorithm in a VPN?

A. integrity
B. key exchange
C. encryption
D. authentication

Answer: A

Explanation:

The HMAC-SHA-1-96 (also known as HMAC-SHA-1) encryption technique is used by IPSec to ensure that a message has not been altered. (-> Therefore answer "integrity" is the best choice). HMAC- SHA-1 uses the SHA-1 specified in FIPS-190-1, combined with HMAC (as per RFC 2104), and is described in RFC 2404.
Reference: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4

Question: 221

[Security Concepts]
A network engineer is deciding whether to use stateful or stateless failover when configuring two ASAs for high availability. What is the connection status in both cases?

A. need to be reestablished with stateful failover and preserved with stateless failover
B. preserved with stateful failover and need to be reestablished with stateless failover
C. preserved with both stateful and stateless failover
D. need to be reestablished with both stateful and stateless failover

Answer: B

Explanation:

Stateful failover means that the connection state information is replicated from the active ASA to the standby ASA, so that in the event of a failover, the connections are preserved and do not need to be reestablished. Stateless failover means that the connection state information is not replicated, so that in the event of a failover, the connections are dropped and need to be reestablished by the end hosts. Stateful failover

provides a smoother transition and less disruption to the network traffic, while stateless failover is simpler and less resource-intensive. Reference:
Failover for High Availability - Cisco
Failover Types / ASA Failover Addresses / Failover Requirements | Cisco …

Question: 222

[Security Concepts]
Which type of protection encrypts RSA keys when they are exported and imported?

A. file
B. passphrase
C. NGE
D. nonexportable

Answer: B

Explanation:

A passphrase is a type of protection that encrypts RSA keys when they are exported and imported. A passphrase is a sequence of characters that the user enters to decrypt the key. The passphrase acts as a symmetric key that is used to encrypt and decrypt the RSA key with a symmetric algorithm, such as AES. This way, the RSA key is protected from unauthorized access or tampering when it is transferred or stored. A passphrase can also provide additional security by adding entropy to the RSA key generation process. A file, NGE, and nonexportable are not types of protection that encrypt RSA keys when they are exported and imported. A file is a container that stores the RSA key, but does not

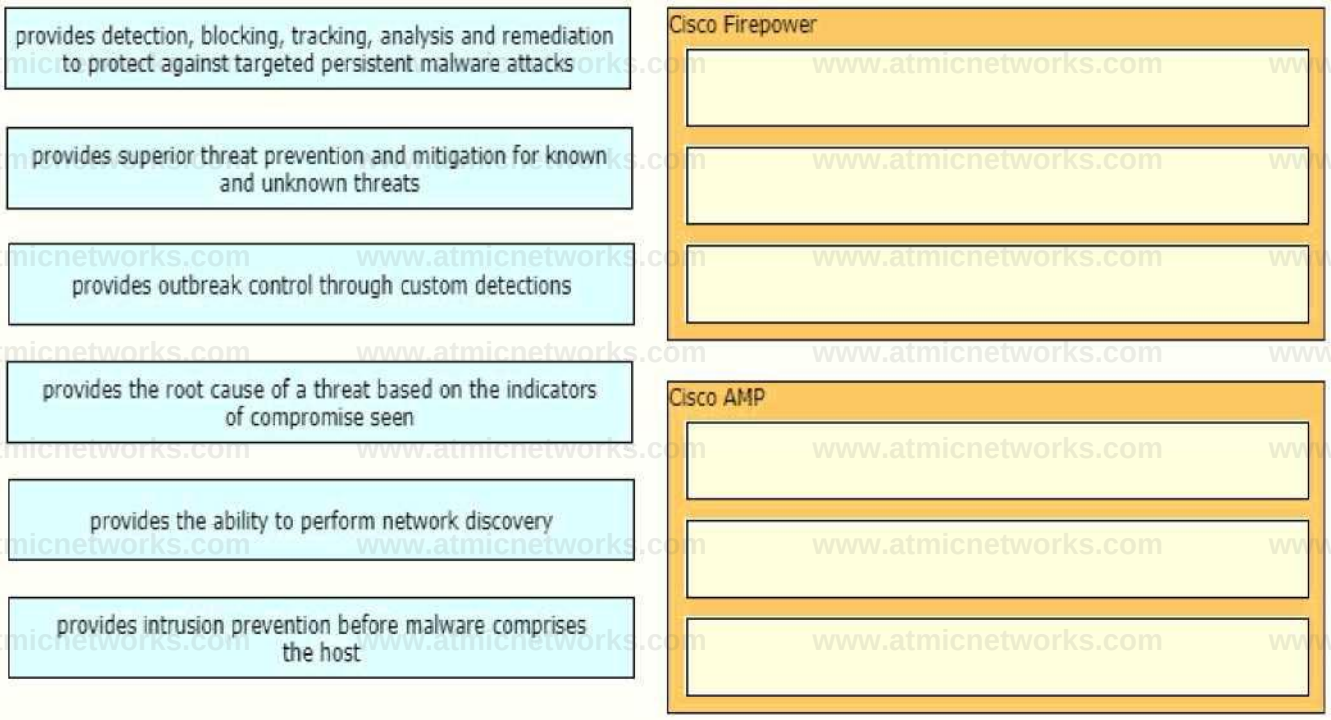
encrypt it. NGE stands for Next Generation Encryption, which is a set of cryptographic standards and algorithms that Cisco recommends, but it is not a specific type of protection. Nonexportable is a property that prevents the RSA key from being exported at all, but it does not encrypt it. Reference: RSA/Schannel Key BLOBs, Common Encryption Types, Protocols and Algorithms Explained, Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 (Module 5: Implementing Secure Communications with VPNs, Lesson 5.1: Implementing Site-to-Site VPNs, Topic 5.1.2: Implementing Site-to-Site VPNs with Pre-Shared Keys)

Question: 223

DRAG DROP

[Endpoint Protection and Detection]

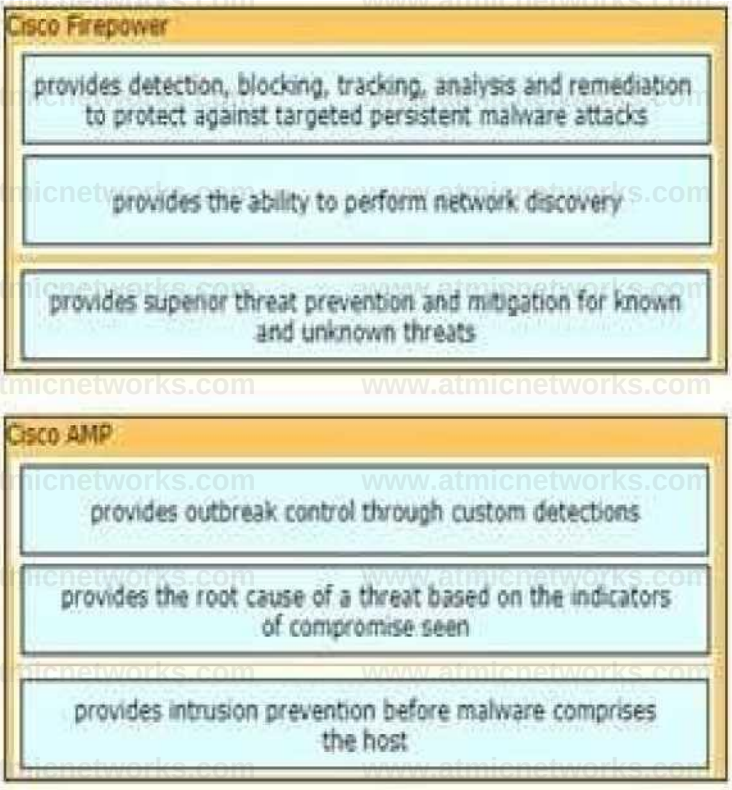
Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate



category on the right.

Answer:

Explanation:



The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible.

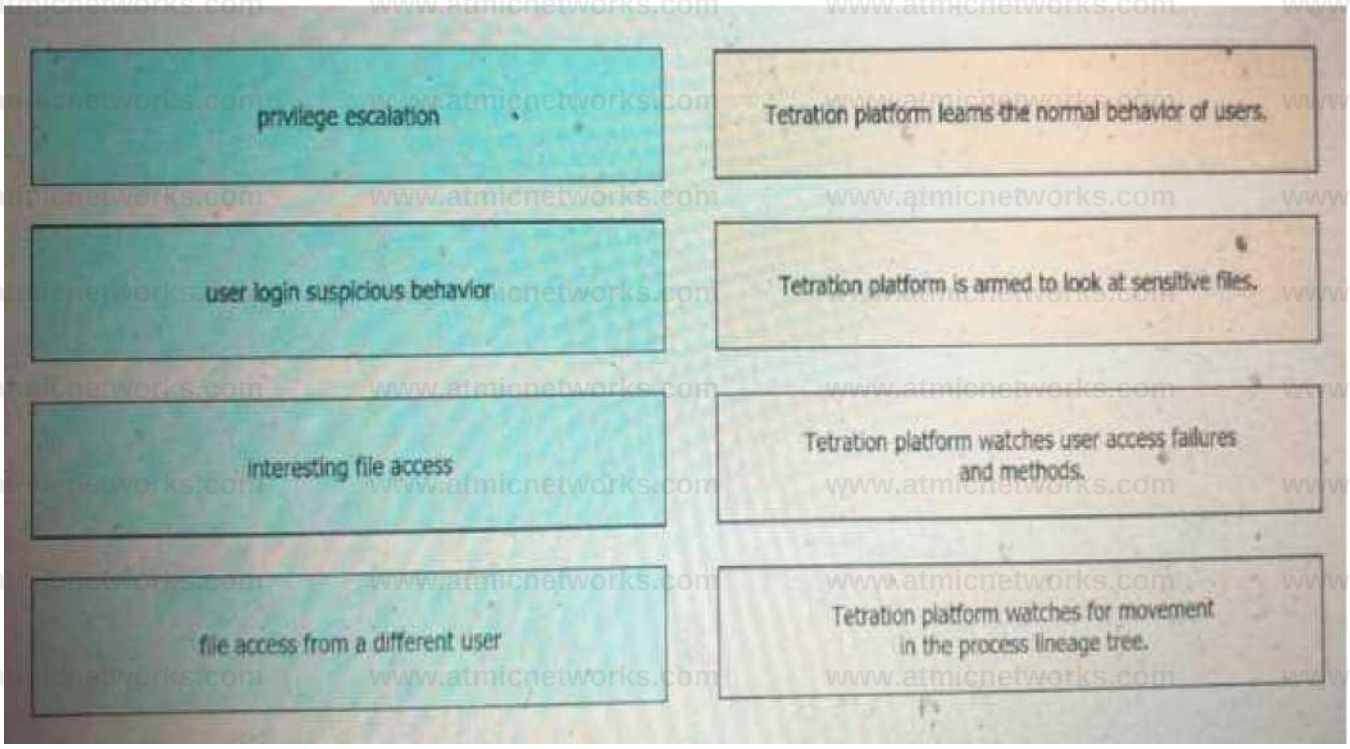
The Cisco Advanced Malware Protection (AMP) solution enables you to detect and block malware, continuously analyze for malware, and get retrospective alerts. AMP for Networks delivers networkbased advanced malware protection that goes beyond point-in-time detection to protect your organization across the entire attack continuum – before, during, and after an attack. Designed for Cisco Firepower® network threat appliances, AMP for Networks detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system. It also provides the visibility and control necessary to protect your organization against highly sophisticated, targeted, zero-day, and persistent advanced malware threats.

Question: 224

DRAG DROP

[Security Concepts]

Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.



Explanation:

Answer:

interesting file access

privilege escalation

user login suspicious behavior

file access from a different user

Cisco Tetration platform studies the behavior of the various processes and applications in the workload, measuring them against known bad behavior sequences. It also factors in the process hashes it collects. By studying various sets of malwares, the Tetration Analytics engineering team deconstructed it back into its

www.atmicnetworks.com

basic

building blocks. Therefore, the platform understands clear and crisp definitions of these building blocks and watches for them.

The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:

+ Shell code execution: Looks for the patterns used by shell code.

+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.

+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.

+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).

+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.

+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.

+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.

+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage

of each command over time. Any new command or command with a different lineage triggers the interest of the

Tetration Analytics platform.

Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

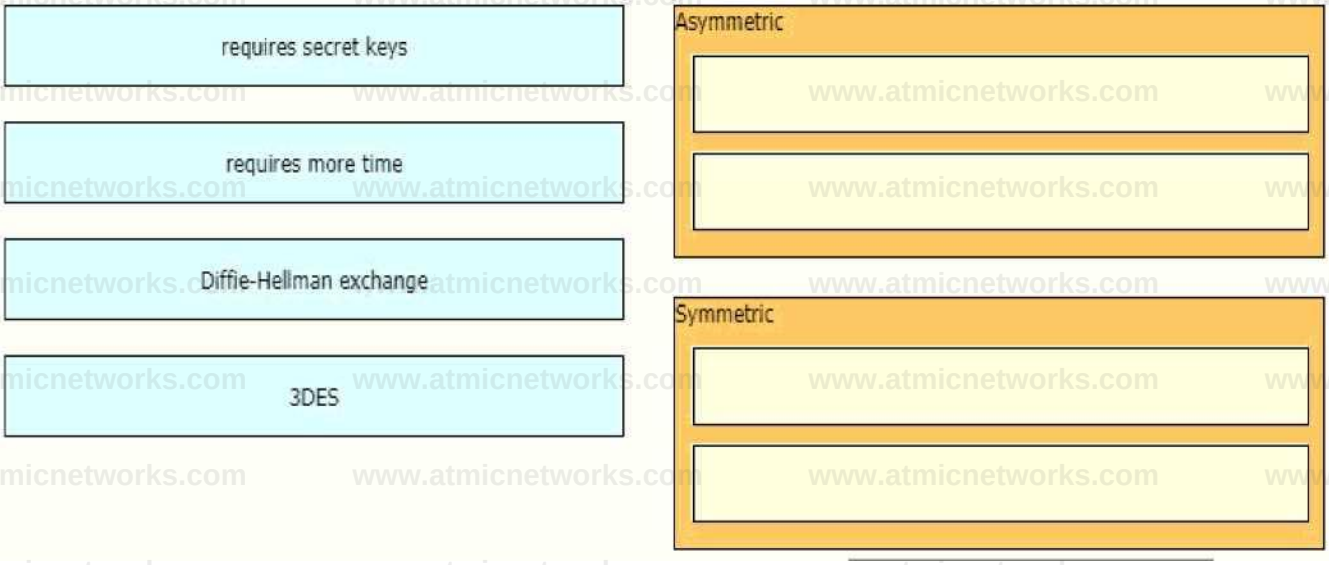
Question: 225

DRAG DROP

[Security Concepts]

Drag and drop the descriptions from the left onto the encryption algorithms on the right.

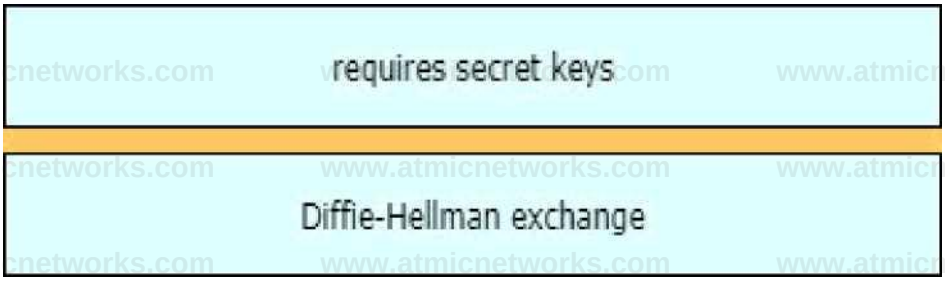
www.atmicnetworks.com



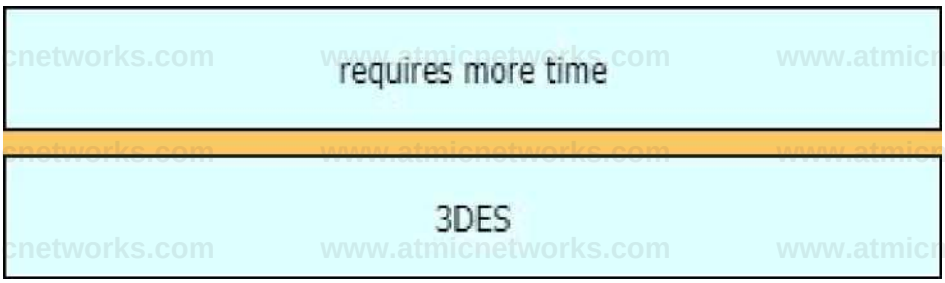
Answer:

Explanation:

Asymmetric



Symmetric



Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetric encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.

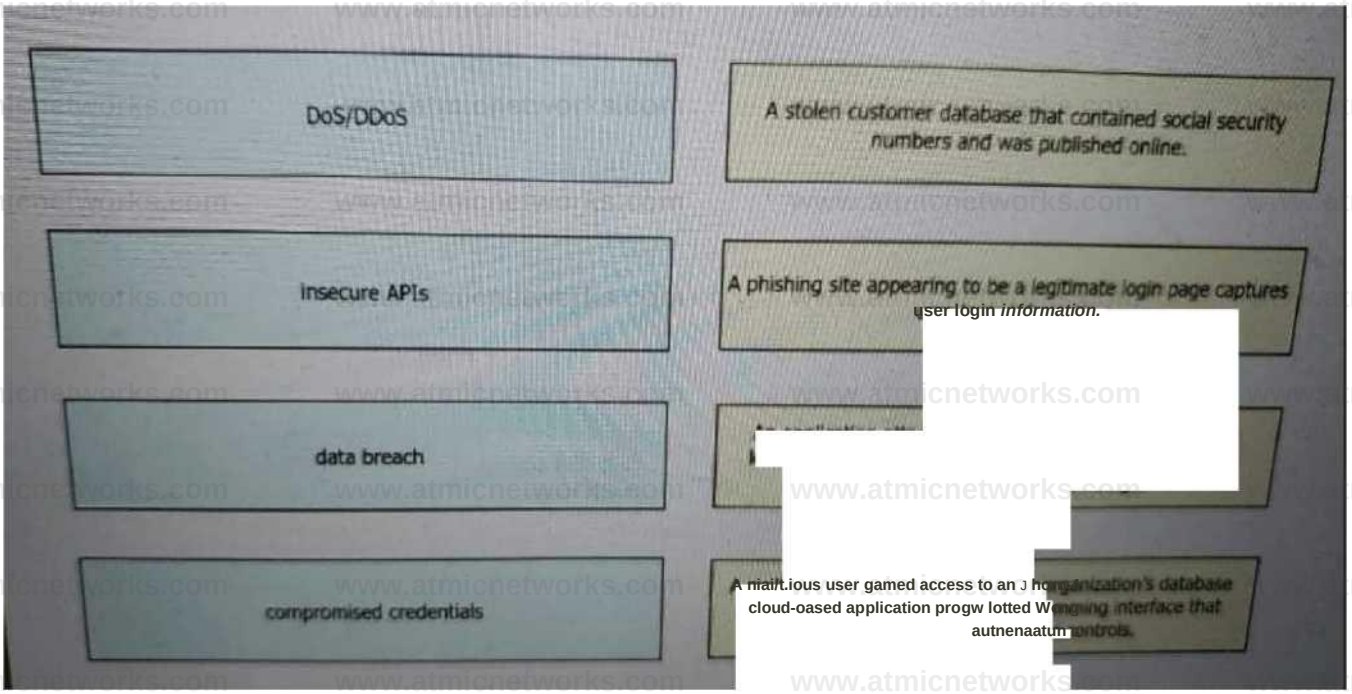
Asymmetric encryption takes relatively more time than the symmetric encryption.

Diffie Hellman algorithm is an asymmetric algorithm used to establish a shared secret for a

symmetric key
algorithm. Nowadays most of the people uses hybrid crypto system i.e, combination of symmetric and asymmetric encryption. Asymmetric Encryption is used as a technique in key exchange mechanism to share secret key and after the key is shared between sender and receiver, the communication will take place using symmetric encryption. The shared secret key will be used to encrypt the communication.
Triple DES (3DES), a symmetric-key algorithm for the encryption of electronic data, is the successor of DES (Data Encryption Standard) and provides more secure encryption then DES.
Note: Although "requires secret keys" option in this question is a bit unclear but it can only be assigned to Symmetric algorithm.

Question: 226

DRAG DROP
[Security Concepts]
Drag and drop the threats from the left onto examples of that threat on the right



Answer:

Explanation:

Correct Answer:



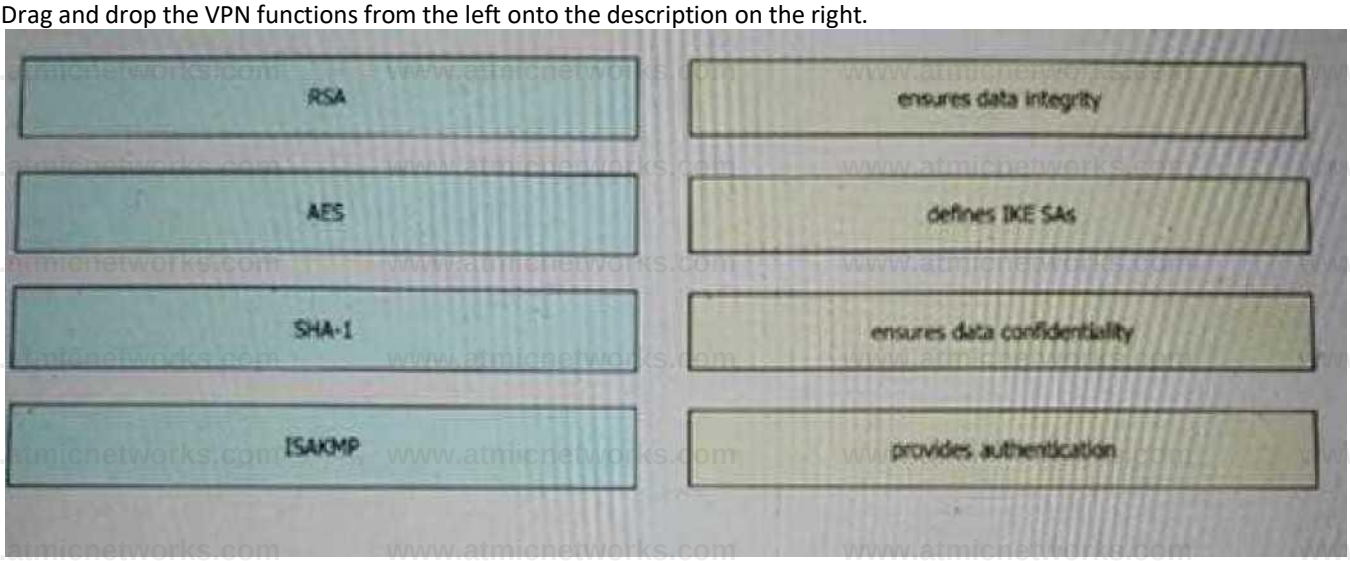
A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment.

When your credentials have been compromised, it means someone other than you may be in possession of your account information, such as your username and/or password.

Question: 227

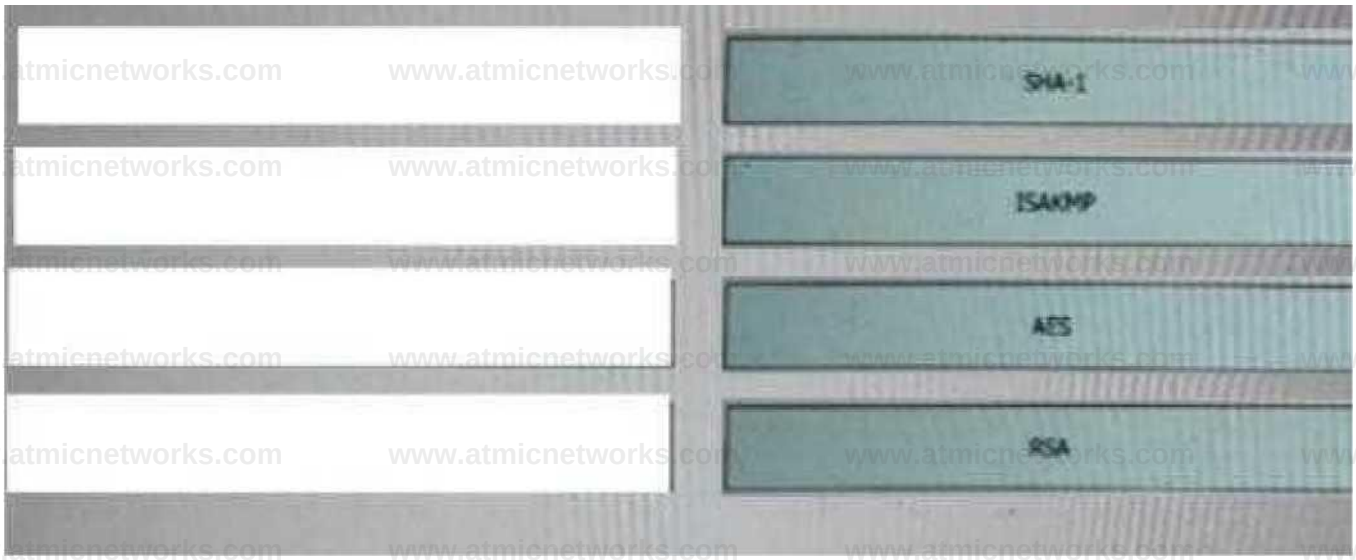
DRAG DROP [Network Security]

Drag and drop the VPN functions from the left onto the description on the right.



Answer:

Explanation:



Question: 228

DRAG DROP

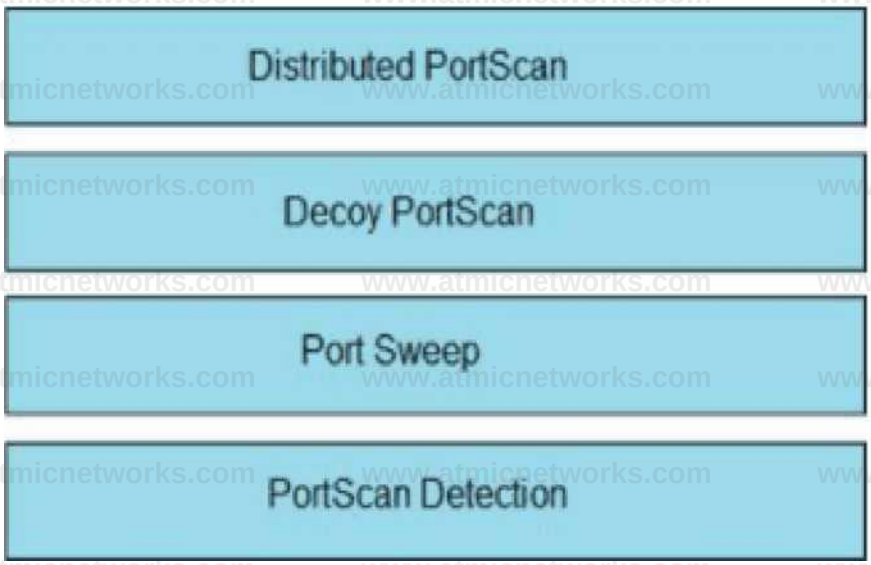
[Security Concepts]

Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

PortScan Detection	many to-one PortScan in which multiple hosts query a single host tor open ports
Port Sweep	one to one PortScan attacker mixes spooled source IP addresses with the actual scanning IP address
Decoy PortScan	one to many port sweep, an attacker against one or a few hosts to scan a si ogle port on multiple tar get hosts
Distributed PortScan	one to one PortScan an attacker against one or a lew hosts Io scan one or multiple ports

Answer:

Explanation:



Question: 229

DRAG DROP

[Security Concepts]

Drag and drop the capabilities from the left onto the correct technologies on the right.

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs combined	application control and URL filtering
integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

Answer:

Explanation:

www.atmicnetworks.com

superior threat prevention and mitigation for known and unknown threats

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

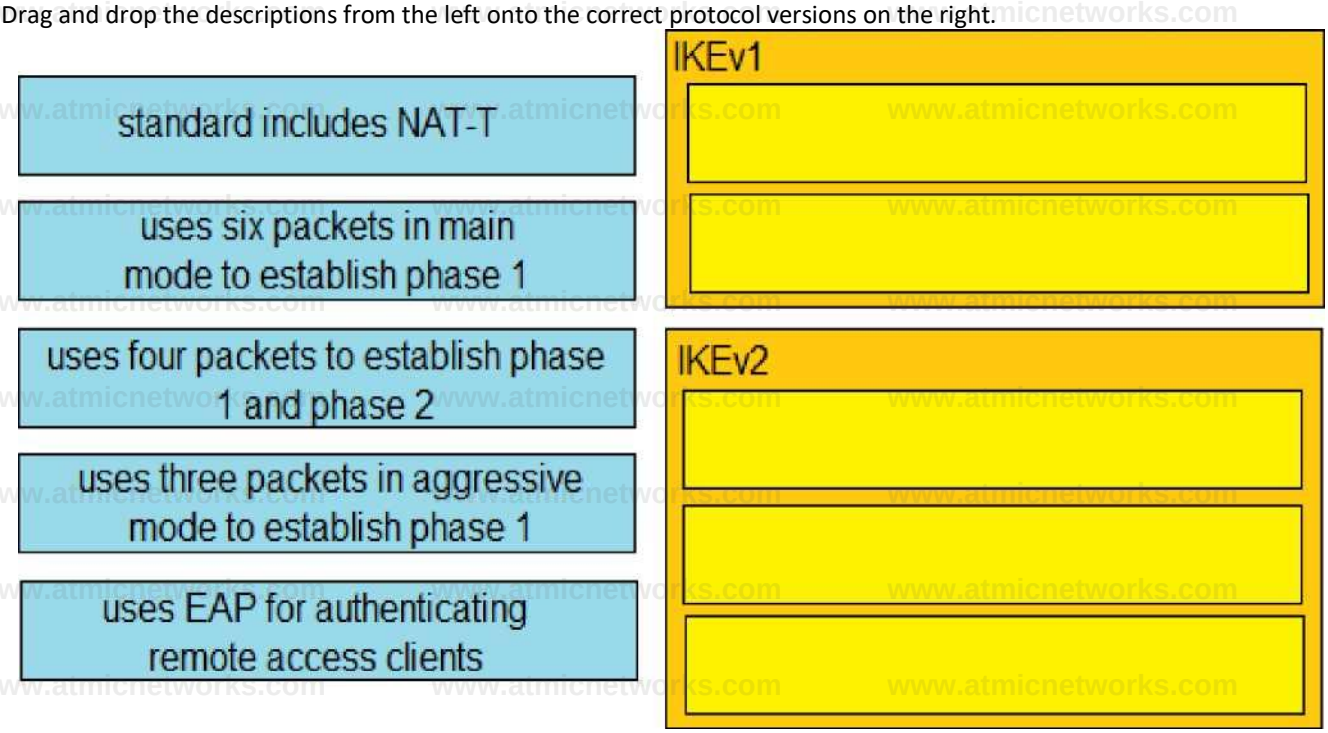
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs combined integrated solution of strong defense and web protection, visibility, and controlling solutions

Question: 230

DRAG DROP

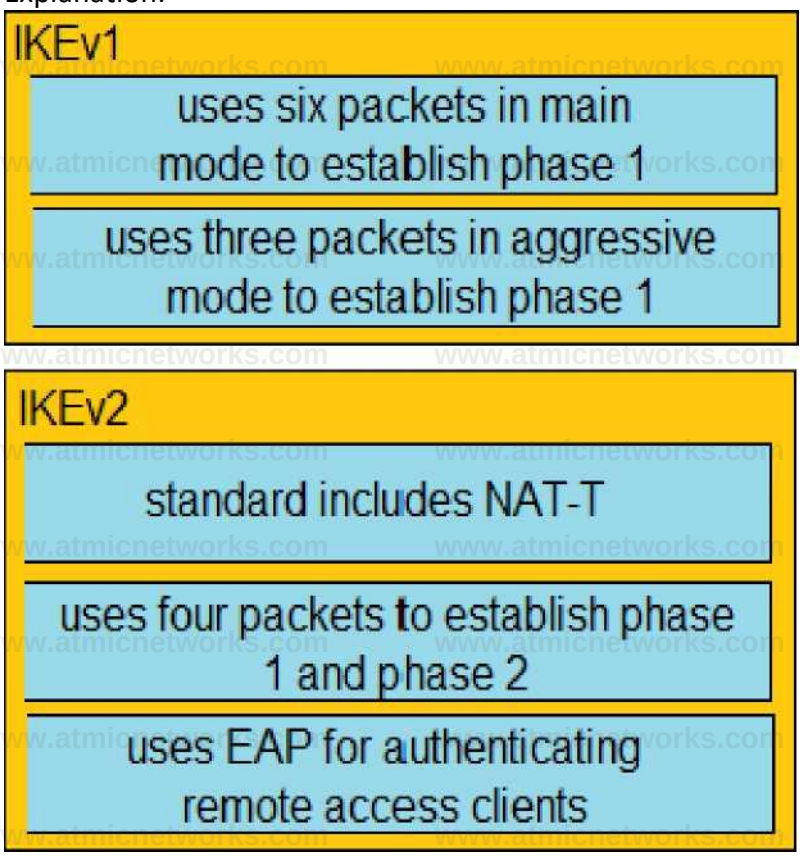
[Security Concepts]

Drag and drop the descriptions from the left onto the correct protocol versions on the right.



Answer:

Explanation:



Question: 231

DRAG DROP [Security Concepts]

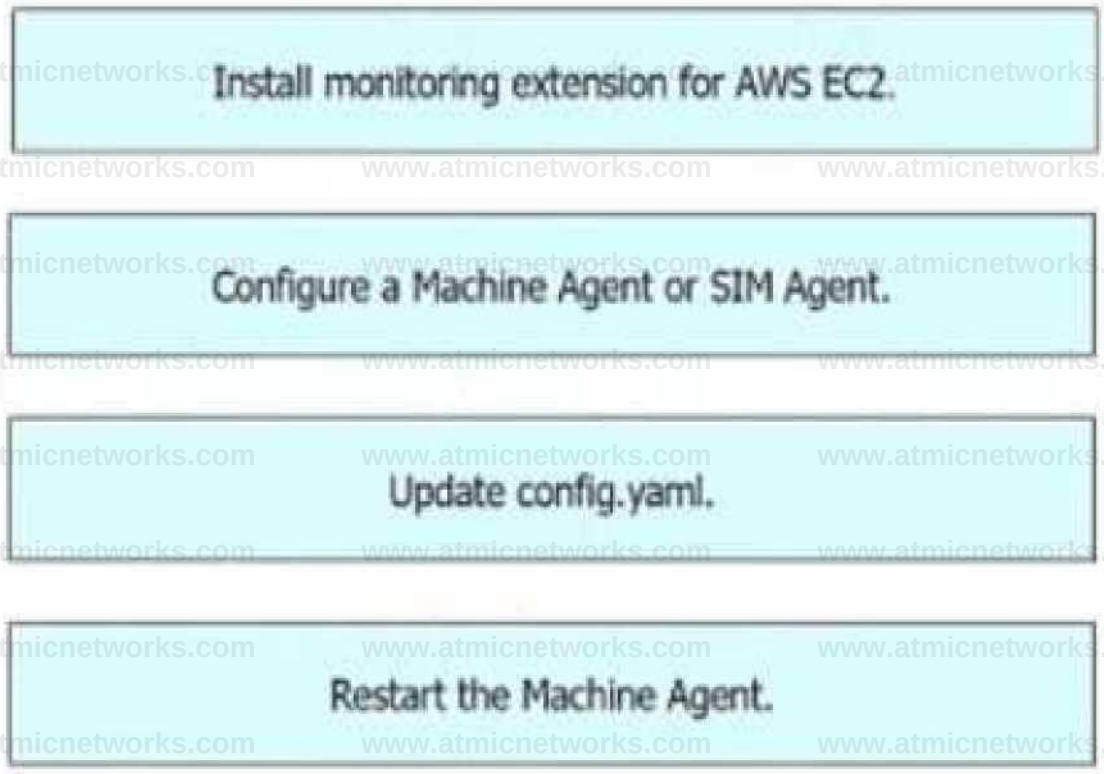
Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

Install monitoring extension for AWS EC2.	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent.	step 4

Answer:

Explanation:

www.atmicnetworks.com

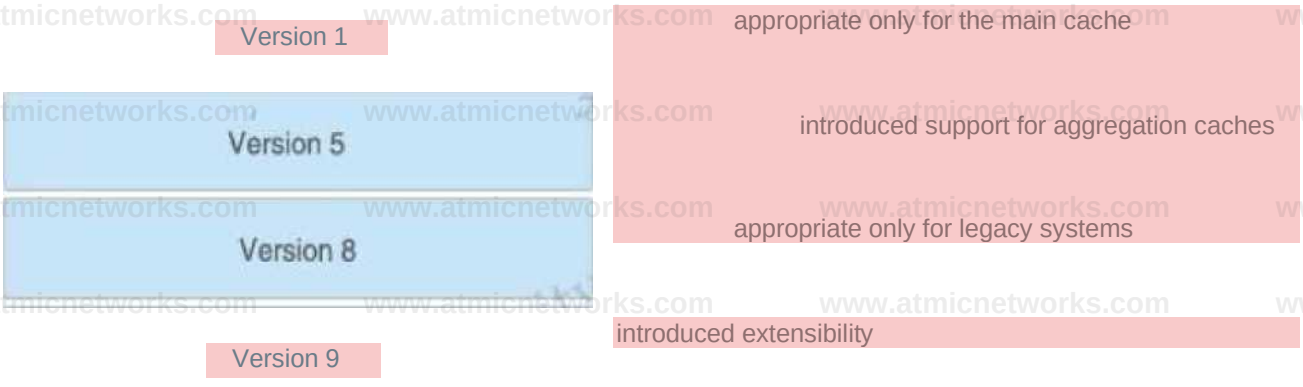


Question: 232

DRAG DROP

[Security Operations]

Drag and drop the NetFlow export formats from the left onto the descriptions on the right.



Answer:

Explanation:



The Version 1 format was the initially released version. Do not use the Version 1 format unless you are using a legacy collection system that requires it. Use Version 9 or Version 5 export format. Version 5 export format is suitable only for the main cache; it cannot be expanded to support new features.

Version 8 export format is available only for aggregation caches; it cannot be expanded to support new features.

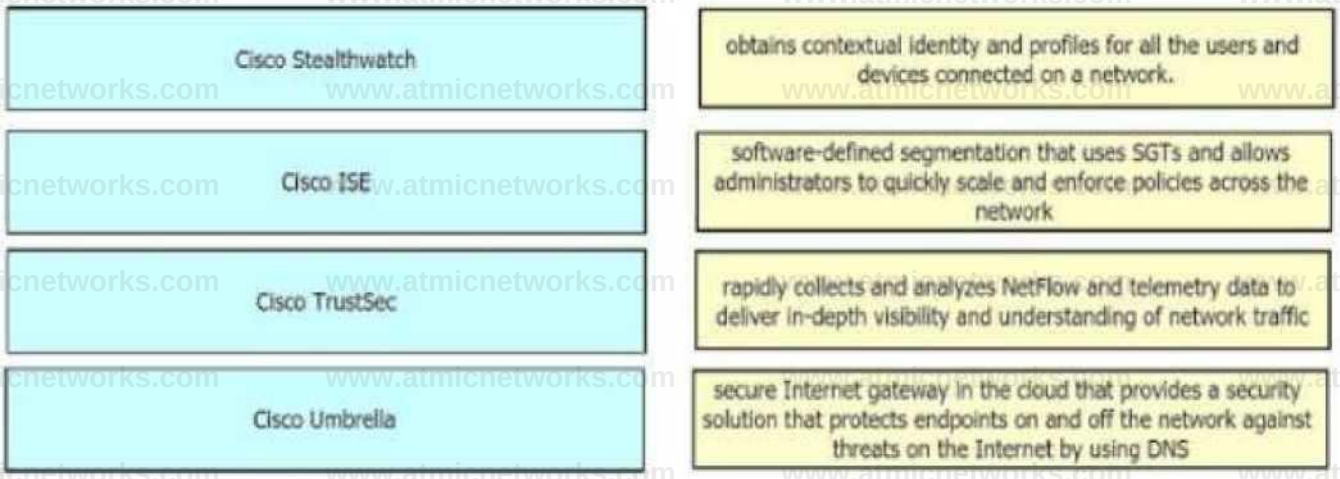
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgnflow-data-expt.html

Question: 233

DRAG DROP

[Security Concepts]

Drag and drop the solutions from the left onto the solution's benefits on the right.



Answer:

Explanation:

Cisco Stealthwatch - rapidly collects and analyzes netflow and telementy data to deliver in-depth visibility and understanding of network traffic

Cisco ISE – obtains contextual identity and profiles for all users and device

Cisco TrustSec – software defined segmentation that uses SGTs

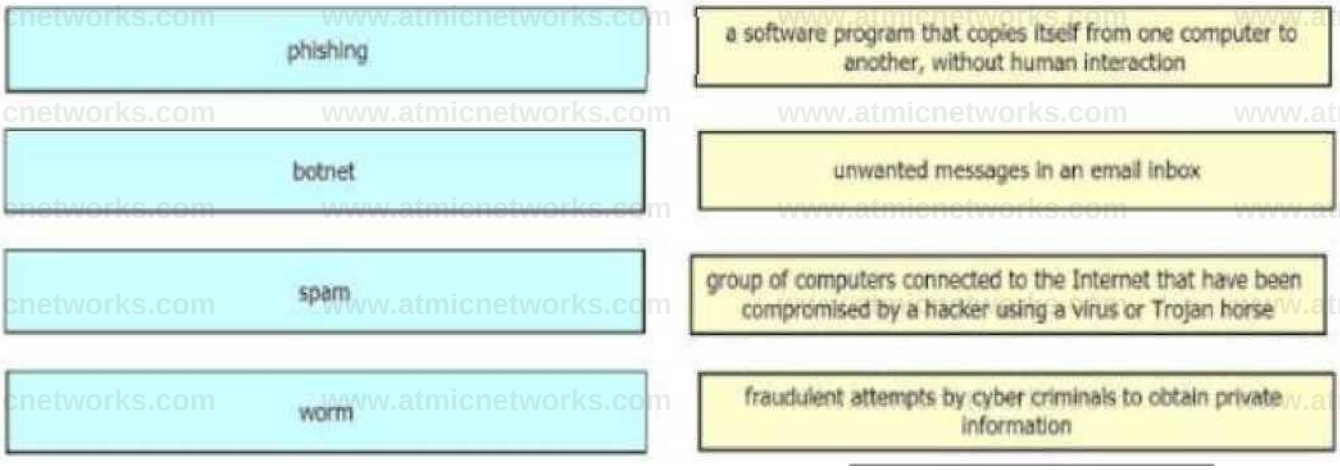
Cisco Umbrella – secure internet gateway ion the cloud that provides a security solution

Question: 234

DRAG DROP

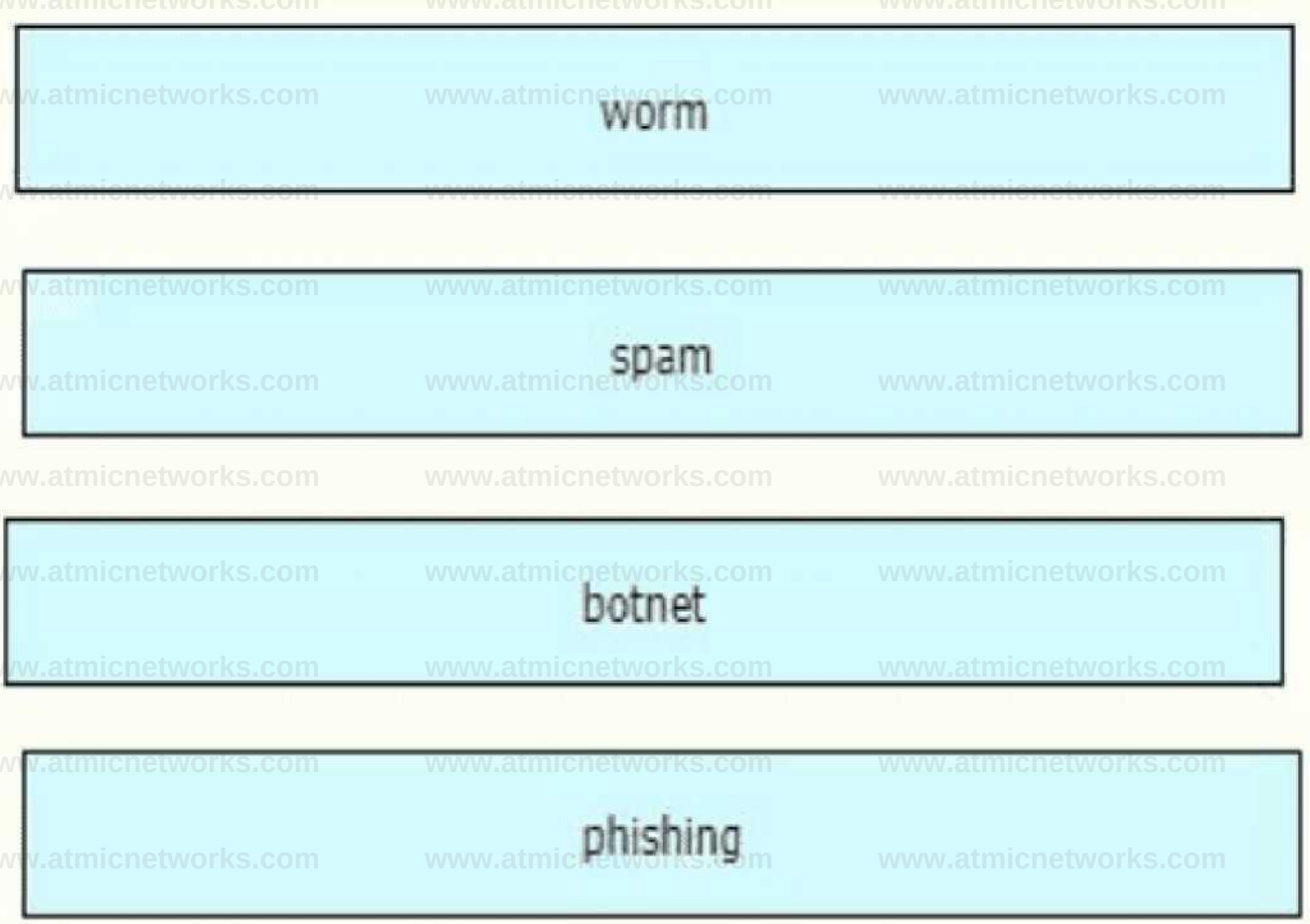
[Security Concepts]

Drag and drop the common security threats from the left onto the definitions on the right.



Explanation:

Answer:



Question: 235

[Content Security]

A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?

A. The policy was created to send a message to quarantine instead of drop
B. The file has a reputation score that is above the threshold
C. The file has a reputation score that is below the threshold
D. The policy was created to disable file analysis

Answer: B

Explanation:

The Cisco ESA uses the Sender Domain Reputation (SDR) service to assign a reputation verdict to

each message based on the sender's domain and other attributes. The SDR verdicts range from Awful to Good, and each verdict has a corresponding reputation score. The administrator can configure a message or content filter to take action on messages based on their SDR verdict or score. For example, the administrator can set a threshold score to drop messages that have a poor or awful reputation. However, if the SDR service cannot determine a verdict for a message, it assigns an undetermined verdict with a score of -1. This means that the message will not be dropped by the filter unless the administrator explicitly sets the threshold to -1 or lower. Therefore, the reason why the Cisco ESA is not dropping files that have an undetermined verdict is because the file has a reputation score that is above the threshold. Reference := Some possible references are:

Configure Sender Domain Reputation for ESA

Sender Domain Reputation Filtering

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 (source book)

Question: 236

[Security Concepts]

An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

A. NetFlow
B. Packet Tracer
C. Network Discovery
D. Access Control

Answer: A

Explanation:

NetFlow is a network protocol developed by Cisco for the collection and monitoring of network traffic flow data generated by NetFlow-enabled routers and switches. The flows do not contain actual packet data, but rather the metadata for communications. It is a standard form of session data that details who, what, when, and where of network traffic -> Answer A is not correct.

Reference: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.html

Question: 237

[Content Security]

Which attack is preventable by Cisco ESA but not by the Cisco WSA?

A. buffer overflow
B. DoS
C. SQL injection
D. phishing

Answer: D

Explanation:

The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway:
Prevents the following:
+ Attacks that use compromised accounts and social engineering.
+ Phishing, ransomware, zero-day attacks and spoofing.
+ BEC with no malicious payload or URL.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

Question: 238

[Content Security]
A Cisco ESA administrator has been tasked with configuring the Cisco ESA to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two)

A. Use outbreak filters from SenderBase
B. Enable a message tracking service
C. Configure a recipient access table
D. Deploy the Cisco ESA in the DMZ
E. Scan quarantined emails using AntiVirus signatures

Answer: A,E

Explanation:
We should scan emails using AntiVirus signatures to make sure there are no viruses attached in emails.
Note: A virus signature is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified. Antivirus software uses a virus signature to find a virus in a computer file system, allowing to detect, quarantine, and remove the virus.
SenderBase is an email reputation service designed to help email administrators research senders, identify legitimate sources of email, and block spammers. When the Cisco ESA receives messages from known or highly reputable senders, it delivers them directly to the end user without any content scanning. However, when the Cisco ESA receives email messages from unknown or less reputable senders, it performs antispam and antivirus scanning.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html-> Therefore Outbreak filters can be used to block emails from bad mail servers.Web servers and email gateways are generally located in the DMZ soNote: The recipient access table (RAT), not to be confused with remote-access Trojan (also RAT), is a Cisco ESA term that defines which recipients are accepted by a public listener.

www.atmicnetworks.com

Question: 239

[Security Concepts]
Which type of dashboard does Cisco DNA Center provide for complete control of the network?

A. service management
B. centralized management
C. application management
D. distributed management

Answer: B

Explanation:

Cisco's DNA Center is the only centralized network management system to bring all of this functionality into a single pane of glass.
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna- center/nb-06- dna-center-faq-cte-en.html

Question: 240

[Securing the Cloud]
In an IaaS cloud services model, which security function is the provider responsible for managing?

A. Internet proxy
B. firewalling virtual machines
C. CASB
D. hypervisor OS hardening

Answer: B

Explanation:

In this IaaS model, cloud providers offer resources to users/machines that include computers as virtual machines, raw (block) storage, firewalls, load balancers, and network devices.
Note: Cloud access security broker (CASB) provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware such as ransomware.

www.atmicnetworks.com

Question: 241

[Secure Network Access, Visibility, and Enforcement]

A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

A. Use MAB with profiling
B. Use MAB with posture assessment.
C. Use 802.1X with posture assessment.
D. Use 802.1X with profiling.

Answer: A

Explanation:

As the new device does not have a supplicant, we cannot use 802.1X.
MAC Authentication Bypass (MAB) is a fallback option for devices that don't support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device's MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or AccessReject just like it would with 802.1x.

Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles.

Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone.

Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta- p/3739456

Question: 242

[Secure Network Access, Visibility, and Enforcement]

An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command ntp authentication-key 1 md5 Cisc392368270. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so.
Which command is required to enable the client to accept the server's authentication key?

A. ntp peer 1.1.1.1 key 1
B. ntp server 1.1.1.1 key 1
C. ntp server 1.1.1.2 key 1
D. ntp peer 1.1.1.2 key 1

Answer: B

Explanation:
To configure an NTP enabled router to require authentication when other devices connect to it, use the following commands:
NTP_Server(config)#ntp authentication-key 2 md5 securitytut
NTP_Server(config)#ntp authenticate
NTP_Server(config)#ntp trusted-key 2
Then you must configure the same authentication-key on the client router:
NTP_Client(config)#ntp authentication-key 2 md5 securitytut
NTP_Client(config)#ntp authenticate
NTP_Client(config)#ntp trusted-key 2
NTP_Client(config)#ntp server 10.10.10.1 key 2
Note: To configure a Cisco device as a NTP client, use the command ntp server <IP address>. For example:
Router(config)#ntp server 10.10.10.1. This command will instruct the router to query 10.10.10.1 for the time.

Question: 243

[Content Security]
What is the role of an endpoint in protecting a user from a phishing attack?

A. Use Cisco Stealthwatch and Cisco ISE Integration.
B. Utilize 802.1X network security to ensure unauthorized access to resources.
C. Use machine learning models to help identify anomalies and determine expected sending behavior.
D. Ensure that antivirus and anti malware software is up to date

Answer: D

Explanation:

One of the key capabilities of endpoint security is to prevent phishing attacks by ensuring that antivirus and anti malware software is up to date. This helps to detect and block malicious attachments or links that may be embedded in phishing emails. Antivirus and anti malware software can also scan the endpoint for any signs of compromise or infection that may have resulted from a successful phishing attack. Additionally, endpoint security can provide data loss prevention (DLP)

features that can prevent sensitive data from being exfiltrated by attackers who have gained access to the endpoint through phishing. Reference := Some possible references are:

Endpoint Security and Phishing: What to Know

Protect Against Spear Phishing with Endpoint Security

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 (source book)

Question: 244

[Security Concepts]

An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic. Which action will accomplish this task?

A. Set content settings to High
B. Configure the intelligent proxy.
C. Use destination block lists.
D. Configure application block lists.

Answer: B

Explanation:

Obviously, if you allow all traffic to these risky domains, users might access malicious content, resulting in an infection or data leak. But if you block traffic, you can expect false positives, an increase in support inquiries, and thus, more headaches. By only proxying risky domains, the intelligent proxy delivers more granular visibility and control. The intelligent proxy bridges the gap by allowing access to most known good sites without being proxied and only proxying those that pose a potential risk. The proxy then filters and blocks against specific URLs hosting malware while allowing access to everything else.

Reference: https://docs.umbrella.com/deployment-umbrella/docs/what-is-the-intelligent-proxy

Question: 245

[Security Concepts]

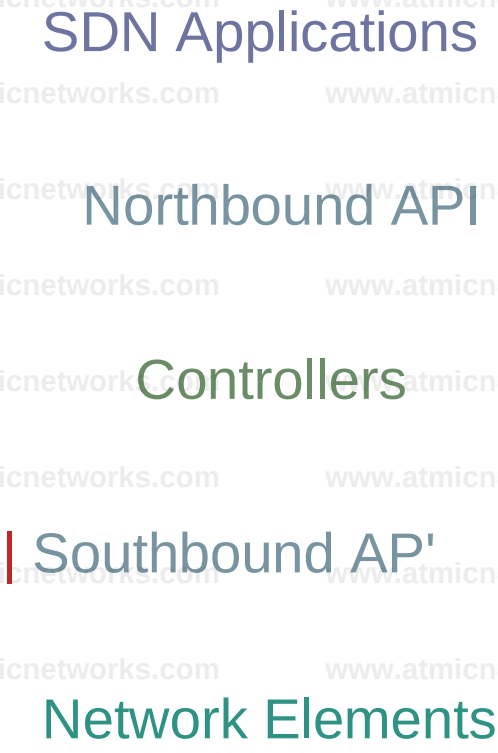
With which components does a southbound API within a software-defined network architecture communicate?

A. controllers within the network
B. applications
C. appliances
D. devices such as routers and switches

Answer: D

Explanation:

www.atmicnetworks.com



The Southbound API is used to communicate between Controllers and network devices.

Question: 246

[Security Concepts]
A network administrator needs to find out what assets currently exist on the network. Third-party systems need to be able to feed host data into Cisco Firepower. What must be configured to accomplish this?

A. a Network Discovery policy to receive data from the host
B. a Threat Intelligence policy to download the data from the host
C. a File Analysis policy to send file data into Cisco Firepower
D. a Network Analysis policy to receive NetFlow data from the host

Answer: A

Explanation:

You can configure discovery rules to tailor the discovery of host and application data to your needs.
The Firepower System can use data from NetFlow exporters to generate connection and discovery events, and to add host and application data to the network map.
A network analysis policy governs how traffic is decoded and preprocessed so it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt -> Answer D is not correct.

www.atmicnetworks.com

Question: 247

[Security Concepts]
When configuring ISAKMP for IKEv1 Phase1 on a Cisco IOS router, an administrator needs to input the command crypto isakmp key cisco address 0.0.0.0. The administrator is not sure what the IP addressing in this command issued for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?

A. The key server that is managing the keys for the connection will be at 1.2.3.4
B. The remote connection will only be allowed from 1.2.3.4
C. The address that will be used as the crypto validation authority
D. All IP addresses other than 1.2.3.4 will be allowed

Answer: B

Explanation:

The command crypto isakmp key cisco address 1.2.3.4 authenticates the IP address of the 1.2.3.4 peer by using the key cisco. The address of "0.0.0.0" will authenticate any address with this key

Question: 248

[Security Concepts]
Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

A. file access from a different user
B. interesting file access
C. user login suspicious behavior
D. privilege escalation

Answer: C

Explanation:

The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:
+ Shell code execution: Looks for the patterns used by shell code.
+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.
+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.
+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).
+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.
+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.
+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by

www.atmicnetworks.com

which user.

+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform.

Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

Question: 249

[Security Concepts]

Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps. Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)

A. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the preconfigured interval.
B. Use EEM to have the ports return to service automatically in less than 300 seconds.
C. Enter the shutdown and no shutdown commands on the interfaces.
D. Enable the snmp-server enable traps command and wait 300 seconds
E. Ensure that interfaces are configured with the error-disable detection and recovery feature

Answer: C,E

Explanation:

You can also bring up the port by using these commands:

+ The “shutdown” interface configuration command followed by the “no shutdown” interface configuration command restarts the disabled port.
+ The “errdisable recovery cause …” global configuration command enables the timer to automatically recover error-disabled state, and the “errdisable recovery interval interval” global configuration command specifies the time to recover error-disabled state.

Question: 250

[Security Concepts]
What is the difference between Cross-site Scripting and SQL Injection, attacks?

A. Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.
B. Cross-site Scripting is a brute force attack targeting remote sites, whereas SQL Injection is a socialengineering attack.
C. Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when adatabase is manipulated.
D. Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.

Answer: A

Explanation:

Answer B is not correct because Cross-site Scripting (XSS) is not a brute force attack.
Answer C is not correct because the statement “Cross-site Scripting is when executives in a corporation are attacked” is not true. XSS is a client-side vulnerability that targets other application users.
Answer D is not correct because the statement “Cross-site Scripting is an attack where code is executed from the server side”. In fact, XSS is a method that exploits website vulnerability by injecting scripts that will run at client’s side.
Therefore only answer A is left. In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters.
Note: The main difference between a SQL and XSS injection attack is that SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

Question: 251

[Endpoint Protection and Detection]
A network administrator is configuring a switch to use Cisco ISE for 802.1X. An endpoint is failing authentication and is unable to access the network. Where should the administrator begin troubleshooting to verify the authentication details?

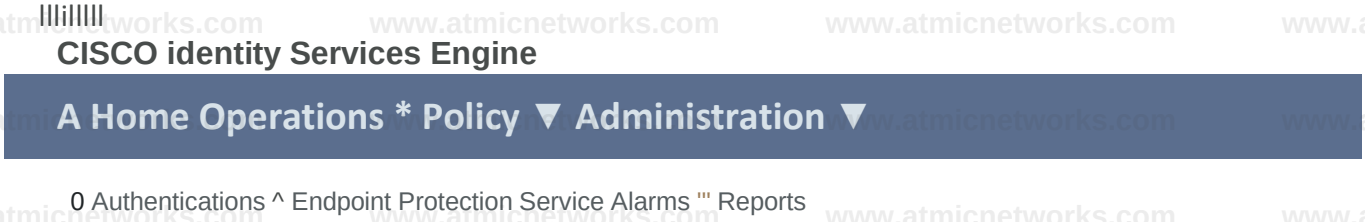
A. Adaptive Network Control Policy List

B. Context Visibility
C. Accounting Reports
D. RADIUS Live Logs

Answer: D

Explanation:

How To Troubleshoot ISE Failed Authentications & Authorizations
Check the ISE Live Logs
Login to the primary ISE Policy Administration Node (PAN).
Go to Operations > RADIUS > Live Logs
(Optional) If the event is not present in the RADIUS Live Logs, go to Operations > Reports > Reports > Endpoints and Users > RADIUS Authentications
Check for Any Failed Authentication Attempts in the Log



Reference: https://community.cisco.com/t5/security-documents/how-to-troubleshoot-ise-failed-authenticationsamp/ta-p/3630960

Question: 252

[Secure Network Access, Visibility, and Enforcement]
What is a prerequisite when integrating a Cisco ISE server and an AD domain?

A. Place the Cisco ISE server and the AD server in the same subnet
B. Configure a common administrator account
C. Configure a common DNS server

D. Synchronize the clocks of the Cisco ISE server and the AD server

Answer: D

Explanation:

The following are the prerequisites to integrate Active Directory with Cisco ISE.

+ Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI.

+ If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation.

+ You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE.

Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

Question: 253

[Content Security]

An organization recently installed a Cisco WSA and would like to take advantage of the AVC engine to allow the organization to create a policy to control application specific activity. After enabling the AVC engine, what must be done to implement this?

A. Use security services to configure the traffic monitor, .
B. Use URL categorization to prevent the application traffic.
C. Use an access policy group to configure application control settings.
D. Use web security reporting to validate engine functionality

Answer: C

Explanation:

The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

www.atmicnetworks.com

Question: 254

[Security Concepts]

Which method is used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources?

A. BYOD on boarding
B. Simple Certificate Enrollment Protocol
C. Client provisioning
D. MAC authentication bypass

Answer: A

Explanation:

When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.

Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal.

Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices.

Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html

Question: 255

[Security Concepts]

Refer to the exhibit.

```
import requests
url = https://api.amp.cisco.com/v1/computers
headers = {
    'accept' : application/json
    'content-type' : application/json
    'authorization' : Basic API Credentials
    'cache-control' : "no cache"

response = requests.request ("GET", url, headers = headers)
print (response.txt)
```

What will happen when this Python script is run?

A. The compromised computers and malware trajectories will be received from Cisco AMP
B. The list of computers and their current vulnerabilities will be received from Cisco AMP
C. The compromised computers and what compromised them will be received from Cisco AMP
D. The list of computers, policies, and connector statuses will be received from Cisco AMP

Answer: D

Explanation:

The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees Reference: https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1

Question: 256

[Security Concepts]
An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

A. Cisco Umbrella
B. Cisco AMP
C. Cisco Stealthwatch
D. Cisco Tetration

Answer: D

Explanation:

Micro-segmentation secures applications by expressly allowing particular application traffic and, by default, denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for application workloads in the data center and cloud.

Cisco Tetration is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation policy generation and enforcement. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies.

To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to discover the relationships between different application tiers and infrastructure services. In addition, the platform supports "what-if" policy analysis using real-time data or historical data to assist in the validation and risk

assessment of policy application pre-enforcement to ensure ongoing application availability. The normalized microsegmentation policy can be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any data center. Once the microsegmentation policy is enforced, Cisco Tetration continues to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior change.
Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf

Question: 257

[Secure Network Access, Visibility, and Enforcement]
Which factor must be considered when choosing the on-premise solution over the cloud-based one?

A. With an on-premise solution, the provider is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the customer is responsible for it
B. With a cloud-based solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
C. With an on-premise solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
D. With an on-premise solution, the customer is responsible for the installation and maintenance of theproduct, whereas with a cloud-based solution, the provider is responsible for it.

Answer: D

Explanation:

The main difference between an on-premise solution and a cloud-based solution is the distribution of responsibilities between the customer and the provider. With an on-premise solution, the customer has full control over the installation, configuration, maintenance, and security of the product, but also bears the costs and risks associated with it. With a cloud-based solution, the provider takes care of most of these aspects, while the customer pays a subscription fee and accesses the product over the internet. Therefore, when choosing between the two options, the customer must consider factors such as cost, scalability, performance, availability, security, compliance, and customization. For example, an on-premise solution may be preferred if the customer has strict security or regulatory requirements, or needs a high level of customization. A cloud-based solution may be preferred if the customer wants to reduce capital expenditure, or needs a flexible and scalable solution that can adapt to changing demands. Reference := Some possible references are: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Security Concepts, Lesson 1: Describing Information Security Concepts, Topic: Cloud Security 350-701 SCOR - Cisco, Exam Topics, 1.0 Security Concepts, 1.6 Compare and contrast the characteristics of a data center and the cloud
Cloud vs. On-Premise Software Comparison

Question: 258

[Security Concepts]
Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?

A. consumption

B. sharing
C. analysis
D. authoring

Answer: A

Explanation:

… we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat- intelligencedirector

Question: 259

[Secure Network Access, Visibility, and Enforcement]
An organization has a Cisco Stealthwatch Cloud deployment in their environment. Cloud logging is working as expected, but logs are not being received from the on-premise network, what action will resolve this issue?

A. Configure security appliances to send syslogs to Cisco Stealthwatch Cloud
B. Configure security appliances to send NetFlow to Cisco Stealthwatch Cloud
C. Deploy a Cisco FTD sensor to send events to Cisco Stealthwatch Cloud
D. Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud

Answer: D

Explanation:

You can also monitor on-premises networks in your organizations using Cisco Stealthwatch Cloud. In order to do so, you need to deploy at least one Cisco Stealthwatch Cloud Sensor appliance (virtual or physical appliance).
Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide

Question: 260

[Endpoint Protection and Detection]
What does Cisco AMP for Endpoints use to help an organization detect different families of malware?

A. Ethos Engine to perform fuzzy fingerprinting
B. Tetra Engine to detect malware when me endpoint is connected to the cloud

C. Clam AV Engine to perform email scanning
D. Spero Engine with machine learning to perform dynamic analysis

Answer: A

Explanation:

ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.
Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdfETHOS = Fuzzy Fingerprinting using static/passive heuristics
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/BRKSEC-2139.pdf

Question: 261

[Security Concepts]
What are two characteristics of Cisco DNA Center APIs? (Choose two)

A. Postman is required to utilize Cisco DNA Center API calls.
B. They do not support Python scripts.
C. They are Cisco proprietary.
D. They quickly provision new devices.
E. They view the overall health of the network

Answer: D,E

Explanation:

Cisco DNA Center APIs are RESTful APIs that allow you to automate and operate your network at scale, using Python scripts or other tools. They are not Cisco proprietary, as they follow the OpenAPI

specification and can be accessed by any client that supports HTTP requests. They do not require Postman, although Postman is a useful tool to test and explore the API endpoints. They can quickly provision new devices by applying predefined templates and workflows, and they can view the overall health of the network by retrieving metrics and alerts from various sources. Reference := Cisco DNA Center Platform - Cisco DevNet
Introduction to Cisco DNA Center REST APIs - Cisco DevNet Learning Labs
Cisco DNA Center Platform User Guide, Release 2.3.4

www.atmicnetworks.com

Question: 262

[Security Concepts]
What is a benefit of conducting device compliance checks?

A. It indicates what type of operating system is connecting to the network.
B. It validates if anti-virus software is installed.
C. It scans endpoints to determine if malicious activity is taking place.
D. It detects email phishing attacks.

Answer: D

Explanation:

Device compliance checks are a feature of Cisco Identity Services Engine (ISE) that allows you to verify the posture of endpoints before allowing them to access your network. Posture is the state of the endpoint in terms of security, such as the presence of anti-virus software, firewall, patches, and so on. A posture agent, such as the AnyConnect ISE Posture Agent, runs on the endpoint and collects posture information, which is then sent to the ISE server for evaluation. Based on the posture policy, the ISE server can grant or deny network access, or apply remediation actions to the endpoint. One of the benefits of conducting device compliance checks is that it validates if anti-virus software is installed on the endpoint, which can prevent malware infections and protect your network from threats. The other options are not benefits of device compliance checks, as they are not related to the posture of the endpoint. Reference:
Compliance - Cisco
Device Compliance - Cisco

Question: 263

[Secure Network Access, Visibility, and Enforcement]
In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two)

A. It allows multiple security products to share information and work together to enhance security posture in the network.
B. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.
C. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.
D. It integrates with third-party products to provide better visibility throughout the network.
E. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

Answer: C,E

Explanation:

Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity.
Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-witheasy-connect-configuration-guide.pdf

Question: 264

[Endpoint Protection and Detection]
What is the benefit of installing Cisco AMP for Endpoints on a network?

A. It provides operating system patches on the endpoints for security.
B. It provides flow-based visibility for the endpoints network connections.
C. It enables behavioral analysis to be used for the endpoints.
D. It protects endpoint systems through application control and real-time scanning

Answer: D

Explanation:

Cisco AMP for Endpoints is a cloud-based endpoint security solution that provides advanced malware protection, threat detection and response, and endpoint isolation. It protects endpoint systems through application control and real-time scanning, which are two of its multifaceted prevention techniques. Application control allows administrators to define and enforce policies on which applications can run on the endpoints, while real-time scanning continuously monitors files and processes for malicious activity. These features help stop threats from compromising the endpoints and reduce the attack surface. Cisco Secure Endpoint (Formerly AMP for Endpoints) - CiscoMalware Protection - Cisco AMP Advanced Malware Protection Reference:
Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco
Malware Protection - Cisco AMP Advanced Malware Protection
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.1: Cisco AMP for Endpoints, Topic 3.1.1: Introduction to Cisco AMP for Endpoints
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.1: Cisco AMP for Endpoints, Topic 3.1.2: Cisco AMP for Endpoints Architecture
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.1: Cisco AMP for Endpoints, Topic 3.1.3: Cisco AMP for Endpoints Features

Question: 265

[Security Concepts]
An administrator is configuring a DHCP server to better secure their environment. They need to be able to ratelimit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?

A. Set a trusted interface for the DHCP server
B. Set the DHCP snooping bit to 1

www.atmicnetworks.com

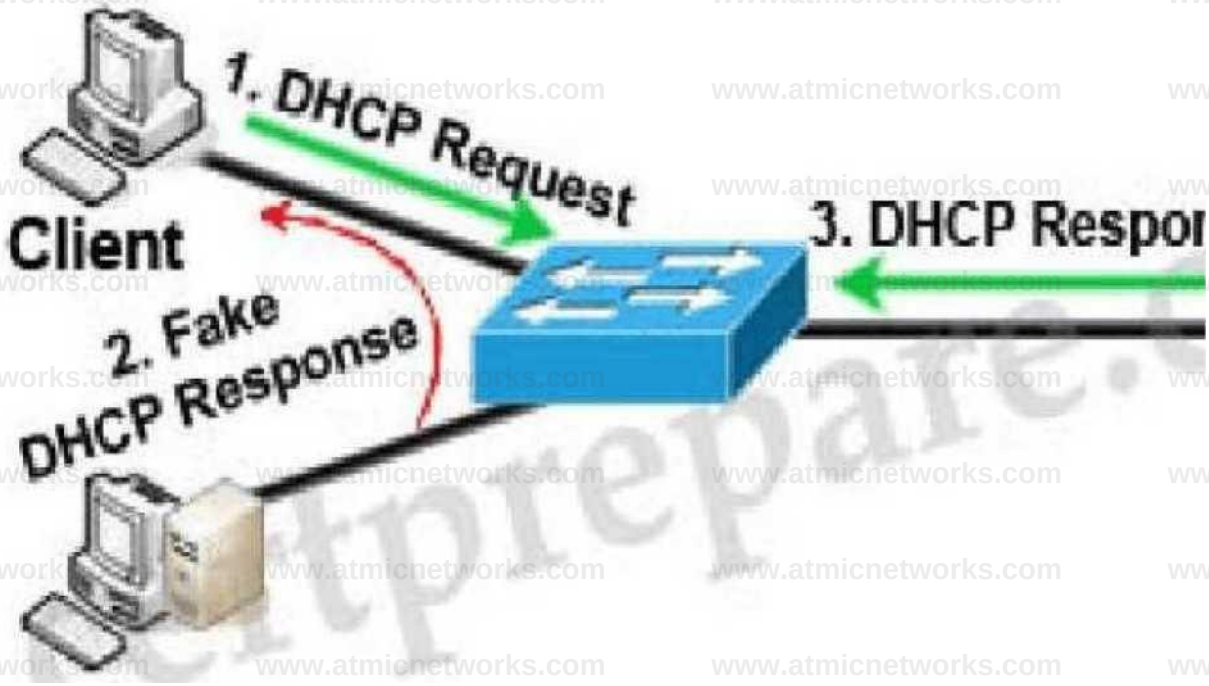
C. Add entries in the DHCP snooping database

D. Enable ARP inspection for the required VLAN

Answer: A

Explanation:

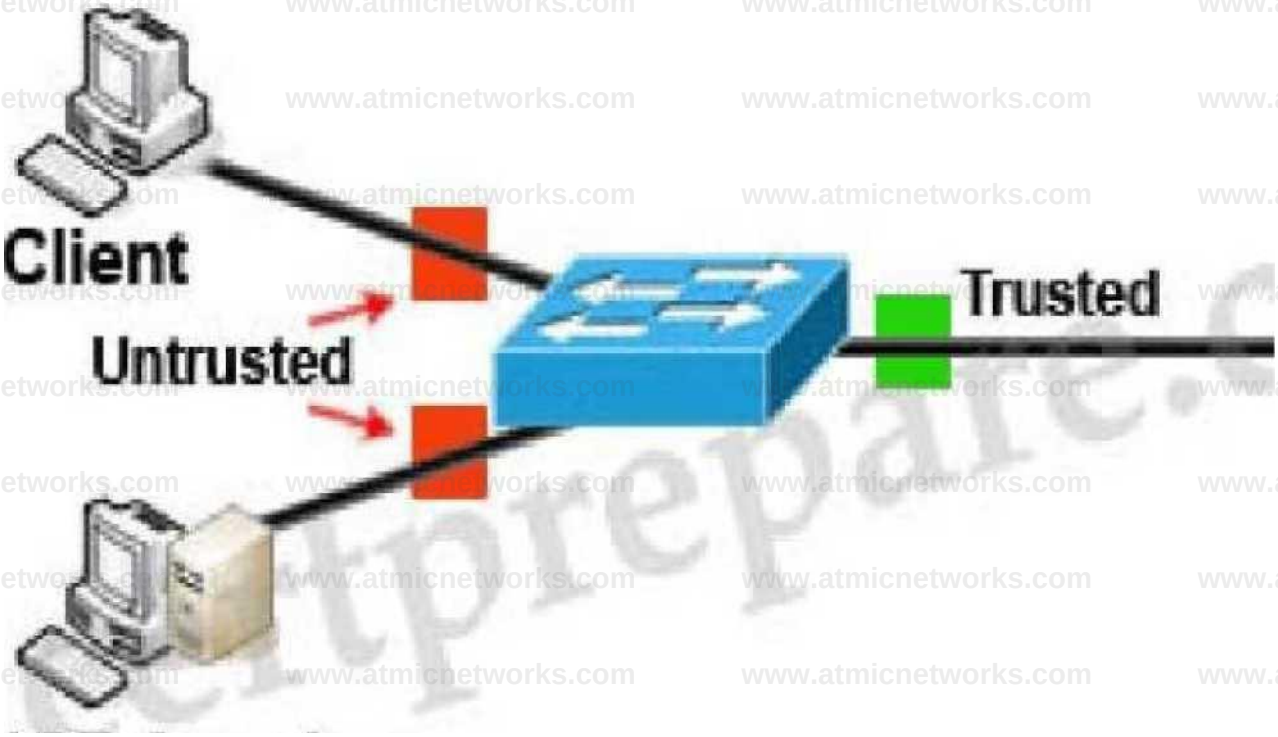
To understand DHCP snooping we need to learn about DHCP spoofing attack first.



DHCP Attacker

DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a “man-in-the-middle”. The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is “closer” than the DHCP Server then he doesn’t need to do anything. Or he can DoS the DHCP Server so that it can’t send the DHCP Response.

DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.



DHCP Attacker

Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.

Question: 266

[Security Concepts]
Refer to the exhibit.

```
import requests
client_id = '<Client id>'
api_key = '<API Key>'
url = 'https://api.amp.cisco.com/v1/computers'
response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()
for computer in response_json['data'] hostname =
    computer['hostname'] print(hostname)
```

What will happen when the Python script is executed?

A. The hostname will be translated to an IP address and printed.
B. The hostname will be printed for the client in the client ID field.
C. The script will pull all computer hostnames and print them.
D. The script will translate the IP address to FODN and print it

www.atmicnetworks.com

Answer: C

Explanation:

The Python script in the exhibit uses the Cisco AMP for Endpoints API to get information about the computers in the deployment. It imports the requests library, which allows it to make HTTP requests. It then defines three variables: client_id, api_key, and url. These are used to authenticate and access the API endpoint. The url is set to '1', which returns a list of computers in JSON format. The script then makes a GET request using the requests.get() method, passing the url and the authentication details as parameters. The response from the API is stored in the response variable, and converted to JSON using the response.json() method. The script then loops over each computer in the 'data' field of the JSON response, using a for loop. Inside the loop, it extracts the hostname of each computer using the 'hostname' key, and prints it using the print() function. Therefore, the script will pull all computer hostnames and print them, which is option C. Reference:

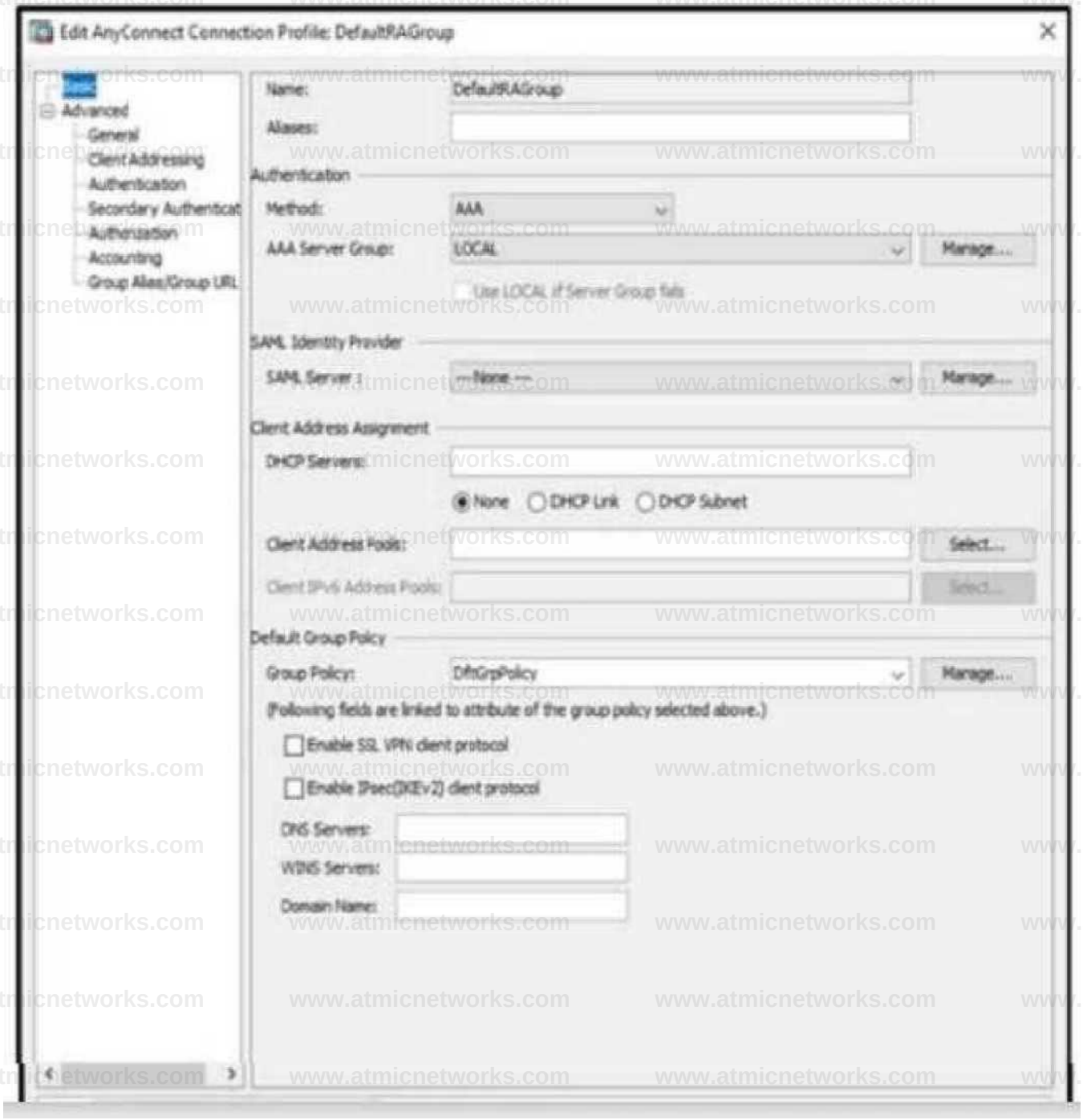
Overview of the Cisco AMP for Endpoints API

Secure Endpoint API - Cisco DevNet

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Question: 267

[Network Security] Refer to the exhibit.



When configuring a remote access VPN solution terminating on the Cisco ASA, an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates. Which configuration item must be modified to allow this?

A. Group Policy
B. Method
C. SAML Server
D. DHCP Servers

Answer:

B

www.atmicnetworks.com

Explanation:

In order to use AAA along with an external token authentication mechanism, set the "Method" as "Both" in the Authentication.

Question: 268

[Securing the Cloud]

An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?

A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock

Answer: D

Explanation:

Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform.

Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web- security/at-a-glance-c45-738565.pdf

Question: 269

[Security Concepts]

An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?

A. SIEM
B. CASB
C. Adaptive MFA
D. Cisco Cloudlock

Answer: D

Explanation:

+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy.
+ Cloudlock is API-based.
+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).
Reference: https://docs.umbrella.com/cloudlock-documentation/docs/endpointsNote:+ Security information and event management (SIEM) platforms collect log and event data from securitysystems, networks and computers, and turn it into actionable security insights.+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when acondition of an alerting policy has been met.

Question: 270

[Security Concepts]
Why is it important to implement MFA inside of an organization?

A. To prevent man-the-middle attacks from being successful.
B. To prevent DoS attacks from being successful.
C. To prevent brute force attacks from being successful.
D. To prevent phishing attacks from being successful.

Answer: C

Explanation:

Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy1. MFA is important to implement inside of an organization because it can prevent brute force attacks from

being successful. A brute force attack is a type of cyberattack that tries to guess the user's password or PIN by trying different combinations until it finds the correct one. This can be done manually or with automated tools. MFA can stop brute force attacks by requiring an additional factor of authentication that the attacker does not have, such as a phone, a token, a biometric, or a location. MFA can also reduce the risk of other types of attacks that rely on stealing or compromising the user's credentials, such as phishing, keylogging, or credential stuffing. Reference := 1: What is Multi-Factor Authentication (MFA)? | OneLogin

Question: 271

[Security Concepts]
A network administrator is configuring SNMPv3 on a new router. The users have already been created; however, an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this?

A. map SNMPv3 users to SNMP views
B. set the password to be used for SNMPv3 authentication
C. define the encryption algorithm to be used by SNMPv3
D. specify the UDP port used by SNMP

Answer: A

Explanation:

SNMPv3 is a security model that uses authentication and encryption to provide secure access to devices. SNMPv3 requires the configuration of SNMP groups, users, and views. SNMP groups define the security model, security level, and access rights for a set of users. SNMP users are members of SNMP groups and have passwords for authentication and encryption. SNMP views define the subset of the MIB tree that a group of users can access. To facilitate access to the SNMP views, the network administrator must map the SNMPv3 users to the SNMP views using the snmp-server group command with the v3 and view keywords. This command assigns a view to a group of users and specifies the security model and level for that group. For example, the following command maps the SNMPv3 users in the group admin to the view all using the authPriv security level: snmp-server group admin v3 authPriv read all write all
This command allows the users in the group admin to access all the MIB objects in the view all using authentication and encryption. The other options are not correct because they are not related to the SNMP views. Option B is incorrect because the password for SNMPv3 authentication is configured for each user using the snmp-server user command with the auth keyword. Option C is incorrect because the encryption algorithm for SNMPv3 is also configured for each user using the snmp-server user command with the priv keyword. Option D is incorrect because the UDP port used by SNMP is not configurable and is always 161 for queries and 162 for traps. Reference :=
Some possible references for this question are:
SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) - SNMP Version 3 Configuration Template for SNMPv3 - Cisco Community
Configure ESXi for SNMP v3 - VMware Docs
How to Configure SNMPv3 and How It Works - CBT Nuggets

Question: 272

[Security Concepts]
An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

A. Cisco Defense Orchestrator
B. Cisco Secureworks

C. Cisco DNA Center
D. Cisco Configuration Professional

Answer: A

Explanation:

Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms. Cisco Defense Orchestrator features:

Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.
Reference: https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html

Question: 273

[Security Concepts]
What is a function of 3DES in reference to cryptography?

A. It hashes files.
B. It creates one-time use passwords.
C. It encrypts traffic.
D. It generates private keys.

Answer: C

Explanation:

3DES is a symmetric-key block cipher that applies the DES algorithm three times to each data block. It was developed to improve the security of DES, which has a small key size and is vulnerable to brute-force attacks. 3DES encrypts traffic by using three different keys, each 56 bits long, to perform three rounds of encryption on the plaintext. The encryption process can be described as follows: Encrypt the plaintext with the first key (K1).
Decrypt the result with the second key (K2).
Encrypt the result again with the third key (K3).
The final ciphertext is the output of the third encryption. The decryption process is the reverse of the encryption process, using the same keys in reverse order:
Decrypt the ciphertext with the third key (K3).
Encrypt the result with the second key (K2).
Decrypt the result again with the first key (K1).
The final plaintext is the output of the third decryption. 3DES is more secure than DES because it uses a longer effective key length of 168 bits (56 x 3), which makes brute-force attacks more difficult. However, 3DES is also slower than DES because it requires three times more computations.

Moreover, 3DES has some weaknesses, such as the meet-in-the-middle attack, which can reduce the effective key length to 112 bits. Therefore, 3DES is not recommended for new applications and has been deprecated by NIST since 201712
Reference := 1: NIST Special Publication 800-67 Revision 2 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher 2: What is 3DES encryption and how does DES work? | Comparitech

Question: 274

[Security Concepts]
Which risk is created when using an Internet browser to access cloud-based service?

A. misconfiguration of infrastructure, which allows unauthorized access
B. intermittent connection to the cloud connectors
C. vulnerabilities within protocol
D. insecure implementation of API

Answer: D

Explanation:

Using an Internet browser to access cloud-based service creates the risk of insecure implementation of API. API stands for Application Programming Interface, which is a set of rules and protocols that
allow different applications or services to communicate and exchange data. API is often used to access cloud-based service, such as software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS). However, if the API is not implemented securely, it can expose sensitive data or allow unauthorized access to the cloud service. For example, an API may not use encryption, authentication, or authorization mechanisms to protect the data in transit or at rest. An API may also have vulnerabilities such as injection, broken authentication, or insufficient logging and monitoring, which can be exploited by attackers to compromise the cloud service or the user's browser. Therefore, it is important to follow the best practices and standards for secure API development and testing, such as OWASP API Security Top 10.
Reference:
1: Implementing and Operating Cisco Security Core Technologies (SCOR) - Cisco
2: 350-701 SCOR - Cisco
3: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0
4: 12 Cloud Security Issues: Risks, Threats & Challenges - CrowdStrike
5: 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud - SEI Blog
6: Remote Browser Isolation Protects Users from Threats - Cisco Umbrella
7: Which risk is created when using an Internet browser to access cloud-based service?
8: Browser in the Cloud: The Evolution of Secure Browsing - Leostream
[9]: OWASP API Security Top 10 2023

Question: 275

[Content Security]

www.atmicnetworks.com

An organization has a Cisco ESA set up with policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?

A. deliver and send copies to other recipients
B. quarantine and send a DLP violation notification
C. quarantine and alter the subject header with a DLP violation
D. deliver and add disclaimer text

Answer: D

Explanation:

You specify primary and secondary actions that the appliance will take when it detects a possible DLP violation in an outgoing message. Different actions can be assigned for different violation types and severities. Primary actions include:

– Deliver
– Drop
– Quarantine

Secondary actions include:

– Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message. – Encrypting messages. The appliance only encrypts the message body. It does not encrypt the message headers.
– Altering the subject header of messages containing a DLP violation.
– Adding disclaimer text to messages.
– Sending messages to an alternate destination mailhost.
– Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination.)
– Sending a DLP violation notification message to the sender or other contacts, such as a manager or DLP compliance officer.

Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html

Question: 276

[Security Concepts] Refer to the exhibit.



An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC. The Cisco FTD is not behind a NAT device. Which command is needed to enable this on the Cisco FTD?

A. configure manager add DONTRESOLVE kregistration key>
B. configure manager add <FMC IP address> <registration key> 16
C. configure manager add DONTRESOLVE <registration key> FTD123
D. configure manager add <FMC IP address> <registration key>

Answer: D

Explanation:

To let FMC manages FTD, first we need to add manager from the FTD and assign a register key of your choice. The command configure manager add 1.1.1.2 the_registration_key_you_want, where 1.1.1.2 is the IP address of the FMC, you need to use the same registration key in FMC when adding this FTD as a managed device.

Reference: https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/

www.atmicnetworks.com

Question: 277

[Security Concepts]
A switch with Dynamic ARP Inspection enabled has received a spoofed ARP response on a trusted interface. How does the switch behave in this situation?

A. It forwards the packet after validation by using the MAC Binding Table.
B. It drops the packet after validation by using the IP & MAC Binding Table.
C. It forwards the packet without validation.
D. It drops the packet without validation.

Answer: B

Explanation:

Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets on untrusted interfaces by comparing the MAC address to IP address bindings in the DHCP snooping database or an ARP access-list. If the ARP packet contains invalid or spoofed information, it is dropped and logged. DAI also inspects ARP packets on trusted interfaces, but it does not drop them if they are invalid. Instead, it forwards them to the destination without validation. This allows the switch to support devices that use static IP addresses or have legitimate reasons to send ARP packets with different MAC address to IP address bindings. However, this also means that if a spoofed ARP packet is received on a trusted interface, it will bypass the DAI validation and be forwarded to the destination. This could allow an attacker to poison the ARP cache of other devices and perform a man-in-the-middle attack.
Therefore, the correct answer is option B. The switch drops the packet after validation by using the IP & MAC Binding Table. Reference:
Understanding and Configuring Dynamic ARP Inspection
DAI (Dynamic ARP Inspection)
Dynamic ARP Inspection (DAI) & Configuration
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Question: 278

[Network Security]
What is a functional difference between a Cisco ASA and a Cisco IOS router with Zone-based policy firewall?

A. The Cisco ASA denies all traffic by default whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces
B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot
C. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas the Cisco ASA starts out by allowing all traffic until rules are added
D. The Cisco ASA can be configured for high availability whereas the Cisco IOS router with ZoneBased Policy Firewall cannot

Answer: A

Explanation:

The Cisco ASA and the Cisco IOS router with Zone-Based Policy Firewall (ZFW) have different default behaviors when it comes to traffic filtering. The Cisco ASA follows a default deny-all policy that prohibits traffic between firewall security zones until an explicit policy is applied to allow desirable traffic1. The Cisco IOS router with ZFW, on the other hand, starts out by allowing all traffic, even on untrusted interfaces, until a zone-pair policy is applied to restrict or inspect traffic2. This means that the Cisco ASA provides a higher level of security by default, while the Cisco IOS router with ZFW requires more configuration to harden the router. However, the Cisco IOS router with ZFW also offers more flexibility and granularity in defining firewall policies, as well as more advanced features such as DMVPN, GET VPN, and Policy-Based Routing, which are not supported by the Cisco
ASA23. Reference:

2: IOS Firewall vs. ASA - Cisco Community
1: Understand the Zone-Based Policy Firewall Design - Cisco
4: What is a functional difference between a Cisco ASA and a Cisco IOS router with Zone-based policy firewall?
5: What is a functional difference between a Cisco ASA and Cisco IOS router with Zone-based policy firewall?
3: Cisco Zone-Based Firewall Reporting – Plixer

Question: 279

[Security Concepts]
What is a benefit of performing device compliance?

A. Verification of the latest OS patches
B. Device classification and authorization
C. Providing multi-factor authentication
D. Providing attribute-driven policies

Answer: D

Explanation:

Device compliance is the state of devices meeting the standards and regulations for the industry or organization. Device compliance policies define the rules and settings that users and devices must meet to be compliant, such as minimum operating systems, disk encryption, or Secure Boot. Device compliance policies can also include actions that apply to devices that are noncompliant, such as alerting users, blocking access, or wiping data. Device compliance policies can be integrated with Conditional Access, which can enforce attribute-driven policies based on the compliance status of the device. Attribute-driven policies are policies that use attributes of the device, user, or resource to determine the level of access or protection. For example, a policy can allow access to a resource only if the device is compliant, the user is in a certain group, and the resource is in a certain location. Attribute-driven policies provide more granular and flexible control over access and security than traditional policies based on roles or permissions. Therefore, the benefit of performing device compliance is providing attribute-driven policies, which is option D. Reference:
Device compliance policies in Microsoft Intune
Device Compliance settings for Windows 10/11 in Intune
Device Compliance: What it is and why you should use it
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Question: 280

[Security Concepts]
Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group?

A. Hybrid
B. Community
C. Private
D. Public

Answer: B

Explanation:

Community Cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally by organizations or by the third-party.

Question: 281

[Secure Network Access, Visibility, and Enforcement]
Which cryptographic process provides origin confidentiality, integrity, and origin authentication for packets?

A. IKEv1
B. AH
C. ESP
D. IKEv2

Answer: C

Explanation:

ESP (Encapsulating Security Payload) is a cryptographic process that provides origin confidentiality, integrity, and origin authentication for packets. ESP encrypts the payload of an IP packet with a symmetric key, and adds a header and a trailer to the packet. The header contains a security parameter index (SPI) and a sequence number, which are used to identify the security association (SA) and prevent replay attacks. The trailer contains padding and a next header field, which are used to align the packet and indicate the type of the original payload. ESP also adds an authentication data field at the end of the packet, which contains a message authentication code (MAC) that is computed over the entire ESP packet (except for the authentication data field itself) using a secret key and a hash function. The MAC provides data integrity and origin authentication for the packet. ESP can operate in two modes: tunnel mode and transport mode. In tunnel mode, ESP encapsulates the entire original IP packet, including the IP header, and adds a new IP header. This mode provides protection for the entire packet, but adds more overhead. In transport mode, ESP only encapsulates the payload of the original IP

packet, and leaves the IP header intact. This mode provides protection only for the payload, but preserves the original IP header information. ESP is one of the two main protocols of IPsec, along with AH (Authentication Header). AH only provides data integrity and origin authentication, but not confidentiality. AH adds a header to the IP packet, which contains a MAC that is computed over the immutable fields of the IP header and the entire payload. AH does not encrypt the payload, and therefore does not protect it from eavesdropping. AH can also operate in tunnel mode or transport mode, but it is incompatible with NAT devices, which modify the IP header fields. IKE (Internet Key Exchange) is a protocol that is used to establish and manage SAs for IPsec. IKE negotiates the security parameters, such as the encryption and authentication algorithms, the keys, and the SPIs, for the IPsec protocols. IKE also performs mutual authentication between the IPsec peers, and establishes a secure channel for exchanging keying material. IKE has two versions: IKEv1 and IKEv2. IKEv1 consists of two phases: phase 1 and phase 2. In phase 1, IKEv1 establishes an IKE SA, which is a secure channel for phase 2. In phase 2, IKEv1 negotiates one or more IPsec SAs, which are used to protect the IPsec traffic. IKEv2 simplifies the IKE protocol by combining the two phases of IKEv1 into a single exchange. IKEv2 also supports more features, such as NAT traversal, EAP authentication, and MOBIKE. Reference :=

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: VPN Technologies, Lesson 3.1: Site-to-Site VPNs, Topic 3.1.1: IPsec VPNs

IPsec - Wikipedia

AH and ESP protocols - IBM

How TLS provides identification, authentication, confidentiality, and integrity - IBM

Question: 282

[Securing the Cloud]

An organization wants to secure users, data, and applications in the cloud. The solution must be APIbased and operate as a cloud-native CASB. Which solution must be used for this implementation?

A. Cisco Cloudlock
B. Cisco Cloud Email Security
C. Cisco Firepower Next-Generation Firewall
D. Cisco Umbrella

Answer: A

Explanation:

Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform.

Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf

Question: 283

[Endpoint Protection and Detection]

What are two Trojan malware attacks? (Choose two)

A. Frontdoor

B. Rootkit
C. Smurf
D. Backdoor
E. Sync

Answer: B,D

Explanation:

A Trojan malware attack is a type of malicious code or software that disguises itself as a legitimate program or file to trick users into executing it. Once executed, the Trojan can perform various harmful actions on the infected system or network, such as stealing data, deleting files, or installing

other malware. There are different types of Trojan malware attacks, depending on their purpose and behavior. Two common types are:

Rootkit: A rootkit is a type of Trojan that hides itself and other malware from detection and removal by antivirus software or system tools. A rootkit can modify the operating system or the firmware of the device to gain persistent and privileged access to the system. A rootkit can also intercept and manipulate system calls, network traffic, or user input to conceal its activities or redirect them to malicious servers.

Backdoor: A backdoor is a type of Trojan that creates a secret or unauthorized access point to the infected system or network. A backdoor can allow an attacker to remotely control the system, execute commands, upload or download files, or monitor the system activity. A backdoor can also be used to install other malware or launch further attacks on other systems or networks.

Reference:

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 1: Malware Threats, Lesson 1: Identifying Malware Threats, Topic: Trojan Horse

What is a Trojan? Is it a virus or is it malware? - Norton™

Trojan Horse Examples (2024): The 6 Worst Attacks Ever - SoftwareLab

Question: 284

[Endpoint Protection and Detection]

What is the role of Cisco Umbrella Roaming when it is installed on an endpoint?

A. To protect the endpoint against malicious file transfers
B. To ensure that assets are secure from malicious links on and off the corporate network
C. To establish secure VPN connectivity to the corporate network
D. To enforce posture compliance and mandatory software

Answer: B

Explanation:

Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are off the VPN.

Question: 285

[Security Operations]
What is a capability of Cisco ASA Netflow?

A. It filters NSEL events based on traffic

B. It generates NSEL events even if the MPF is not configured
C. It logs all event types only to the same collector
D. It sends NetFlow data records from active and standby ASAs in an active standby failover pair

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01101.html Policy Order The order in which policies are listed in a policy table determines the priority with which they are applied to Web requests. Web requests are checked against policies beginning at the top of the table and ending at the first policy matched. Any policies below that point in the table are not processed. If no user- defined policy is matched against a Web request, then the global policy for that policy type is applied. Global policies are always positioned last in Policy tables and cannot be re-ordered.

Question: 286

[Security Concepts]
Which component of Cisco umbrella architecture increases reliability of the service?

A. Anycast IP
B. AMP Threat grid
C. Cisco Talos
D. BGP route reflector

Answer: A

Explanation:

Anycast IP is a component of Cisco umbrella architecture that increases reliability of the service by allowing the same IP address to exist on multiple servers around the world. This way, the user's request is automatically routed to the nearest and fastest data center, and failover is seamless in case of an outage. Anycast IP also reduces latency and improves performance by using BGP to select the shortest path to the destination12. Reference := 1: Why Cisco Umbrella uses anycast routing - Cisco Umbrella 2: Cisco Umbrella At a Glance

Question: 287

[Secure Network Access, Visibility, and Enforcement]
What is the benefit of integrating Cisco ISE with a MDM solution?

A. It provides compliance checks for access to the network
B. It provides the ability to update other applications on the mobile device
C. It provides the ability to add applications to the mobile device through Cisco ISE
D. It provides network device administration access

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperability_mdm.html

Question: 288

[Security Concepts]
An administrator configures a new destination list in Cisco Umbrella so that the organization can block specific domains for its devices. What should be done to ensure that all subdomains of domain.com are blocked?

A. Configure the *.com address in the block list.
B. Configure the *.domain.com address in the block list
C. Configure the *.domain.com address in the block list
D. Configure the domain.com address in the block list

Answer: D

Explanation:

To block all subdomains of domain.com, the administrator should configure the domain.com address in the block list. This is because Umbrella automatically applies a left side and right side wildcard to every domain in a block or allow destination list. Therefore, adding domain.com to a block list will result in requests to domain.com or its subdomains, such as www.domain.com, being blocked. Adding a wildcard character (*) is not supported and will not work. Adding the *.com address in the block list will block all domains that end with .com, which is not the desired outcome. Reference: Understanding Destination lists supported entries and error messages Wildcards and Destination Lists

Question: 289

[Security Concepts]
An organization wants to provide visibility and to identify active threats in its network using a VM. The

organization wants to extract metadata from network packet flow while ensuring that payloads are not retained or transferred outside the network. Which solution meets these requirements?

A. Cisco Umbrella Cloud
B. Cisco Stealthwatch Cloud PNM
C. Cisco Stealthwatch Cloud PCM
D. Cisco Umbrella On-Premises

Answer: B

Explanation:

Private Network Monitoring (PNM) provides visibility and threat detection for the on-premises network, delivered from the cloud as a SaaS solution. It is the perfect solution for organizations who prefer SaaS products and desire better awareness and security in their on-premises environments while reducing capital expenditure and operational overhead. It works by deploying lightweight software in a virtual machine or server that can consume a variety of native sources of telemetry or extract metadata from network packet flow. It encrypts this metadata and sends it to the Stealthwatch Cloud analytics platform for analysis. Stealthwatch Cloud consumes metadata only. The packet payloads are never retained or transferred outside the network.
This lab focuses on how to configure a Stealthwatch Cloud Private Network Monitoring (PNM) Sensor, in order to provide visibility and effectively identify active threats, and monitors user and device behavior within onpremises networks.
The Stealthwatch Cloud PNM Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. –VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC- 2240-LG2.pdf

Question: 290

[Security Concepts]
An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution. The organization does not have a local VM but does have existing Cisco ASAs that must migrate over to Cisco FTDs. Which solution meets the needs of the organization?

A. Cisco FMC
B. CSM
C. Cisco FDM
D. CDO

Answer: A

Explanation:

Cisco FMC is the centralized management solution for Cisco FTD appliances. It provides configuration, monitoring, analysis, and reporting capabilities for FTD devices. Cisco FMC can also manage Cisco ASAs that have been converted to FTD devices. Cisco FMC can be deployed as a physical or virtual appliance, or as a cloud service (CDO). However, since the organization does not have a local VM, CDO is not an option. Cisco FDM is the on-box management solution for FTD devices, which does not support centralized management or ASA migration. CSM is the legacy management solution for Cisco ASAs, which does not support FTD devices. Reference := Some possible references are:
Cisco Firepower Management Center Configuration Guide, Version 6.7
Install and Upgrade FTD on Firepower Appliances
Firepower Threat Defense simplifies application security

Question: 291

[Security Concepts]
An organization wants to secure data in a cloud environment. Its security model requires that all users be authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and dat
a. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?

A. Virtual routing and forwarding
B. Microsegmentation
C. Access control policy
D. Virtual LAN

Answer: C

Explanation:

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.
The Zero Trust model uses microsegmentation — a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network — to contain attacks.

Question: 292

[Network Security]
A Cisco FTD engineer is creating a new IKEv2 policy called s2s00123456789 for their organization to allow for additional protocols to terminate network devices with. They currently only have one policy established and need the new policy to be

a backup in case some devices cannot support the stronger algorithms listed in the primary policy. What should be done in order to support this?

A. Change the integrity algorithms to SHA* to support all SHA algorithms in the primary policy
B. Make the priority for the new policy 5 and the primary policy 1
C. Change the encryption to AES* to support all AES algorithms in the primary policy
D. Make the priority for the primary policy 10 and the new policy 1

Answer: B

Explanation:

All IKE policies on the device are sent to the remote peer regardless of what is in the selected policy section.
The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first.
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike- protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html

Question: 293

[Security Concepts]

Which type of encryption uses a public key and private key?

A. Asymmetric
B. Symmetric
C. Linear
D. Nonlinear

Answer: A

Explanation:

Asymmetric encryption, also known as public key cryptography, uses two different keys for encryption and decryption: a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret. Data encrypted with the public key can only be decrypted with the private key, and vice versa. This ensures that only the intended recipient can access the encrypted data, and that the sender can prove their identity with a digital signature. Asymmetric encryption is widely used for securing Internet communications, such as TLS/SSL, which enables HTTPS. Some examples of asymmetric encryption algorithms are RSA, Diffie-Hellman, and Elliptic Curve Cryptography. The other options are not correct because they do not use a public key and private key. Symmetric encryption uses the same key for encryption and decryption, and is faster and more efficient than asymmetric encryption. However, symmetric encryption requires a secure way to exchange the key between the sender and the receiver, which can be facilitated by asymmetric encryption. Linear and nonlinear encryption are not types of encryption, but rather properties of encryption algorithms. A linear encryption

www.atmicnetworks.com

algorithm is one that can be expressed as a linear function, such as XOR. A nonlinear encryption algorithm is one that involves more complex mathematical operations, such as modular arithmetic or S-boxes. Nonlinear encryption algorithms are generally more secure and resistant to cryptanalysis than linear encryption algorithms. Reference :=

Public-key cryptography - Wikipedia

How does public key cryptography work? - Cloudflare

Public and private encryption keys | PreVeil

AES encryption, what are public and private keys?

Question: 294

[Security Operations]

What are two features of NetFlow flow monitoring? (Choose two)

A. Can track ingress and egress information
B. Include the flow record and the flow importer
C. Copies all ingress flow information to an interface
D. Does not required packet sampling on interfaces
E. Can be used to track multicast, MPLS, or bridged traffic

Answer: A,E

Explanation:

The following are restrictions for Flexible NetFlow:

+ Traditional NetFlow (TNF) accounting is not supported.
+ Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported.
+ Both ingress and egress NetFlow accounting is supported.
+ Microflow policing feature shares the NetFlow hardware resource with FNF.
+ Only one flow monitor per interface and per direction is supported.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15- mt-book/cfgmpls-netflow.html

Question: 295

[Security Concepts]

A customer has various external HTTP resources available including Intranet Extranet and Internet, with a proxy configuration running in explicit mode. Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?

A. Transport mode
B. Forward file
C. PAC file
D. Bridge mode

Answer: C

Explanation:

A Proxy Auto-Configuration (PAC) file is a JavaScript function definition that determines whether web browser requests (HTTP, HTTPS, and FTP) go direct to the destination or are forwarded to a web proxy server. PAC files are used to support explicit proxy deployments in which client browsers are explicitly configured to send traffic to the web proxy. The big advantage of PAC files is that they are usually relatively easy to create and maintain.

Question: 296

[Security Concepts]
Which Talos reputation center allows for tracking the reputation of IP addresses for email and web traffic?

A. IP and Domain Reputation Center
B. File Reputation Center
C. IP Slock List Center
D. AMP Reputation Center

Answer: A

Explanation:

The IP and Domain Reputation Center is a service provided by Talos, Cisco's Security Intelligence and Research Group, that tracks the reputation of IP addresses and domains for email and web traffic. The IP and Domain Reputation Center collects and analyzes data from millions of deployed web, email, firewall and IPS appliances, as well as open-source data sets, endpoint intelligence, and network intrusions. The IP and Domain Reputation Center transforms this data into actionable threat intelligence and tools to improve security posture. The IP and Domain Reputation Center allows users to look up websites, URLs and IP addresses and the information Talos has about them, such as their reputation score, category, volume, and threat level. The IP and Domain Reputation Center also provides threat data overviews, such as the top email and spam senders by country, and the standard categories used to classify website content and attack types123. Reference := 1: Reputation Center - A Real Time Threat Detection Service || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence 2: IP & Domain Reputation Center - Talos Intelligence 3: Talos Reputation Center overview | Talos Support Documents

Question: 297

[Network Security]
An engineer is configuring IPsec VPN and needs an authentication protocol that is reliable and supports ACK and sequence. Which protocol accomplishes this goal?

A. AES-192
B. IKEv1

C. AES-256

D. ESP

Answer: B

Explanation:

IKEv1 is the authentication protocol that is reliable and supports ACK and sequence for IPsec VPN. IKEv1 is a key management protocol that is used in conjunction with IPsec to establish secure and authenticated connections between IPsec peers. IKEv1 uses UDP port 500 and consists of two phases: phase 1 and phase 2. In phase 1, the peers authenticate each other and negotiate a shared secret key that is used to encrypt the subsequent messages. In phase 2, the peers negotiate the security parameters for the IPsec tunnel, such as the encryption and authentication algorithms, the lifetime, and the mode (transport or tunnel). IKEv1 uses ACK and sequence numbers to ensure the reliability and integrity of the messages exchanged between the peers. ACK is an acknowledgment message that confirms the receipt of a previous message. Sequence number is a unique identifier that is assigned to each message to prevent replay attacks and to detect missing or out-of-order messages. IKEv1 also supports various authentication methods, such as pre-shared keys, digital certificates, and extended authentication (XAUTH). Reference : Internet Key Exchange for IPsec VPNs Configuration Guide, Security for VPNs with IPsec Configuration Guide, IPSec Architecture

Question: 298

[Network Security]

An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of 172.19.20.24. Which command on the hub will allow the administrator to accomplish this?

A. crypto ca identity 172.19.20.24

B. crypto isakmp key Cisco0123456789 172.19.20.24

C. crypto enrollment peer address 172.19.20.24

D. crypto isakmp identity address 172.19.20.24

Answer: B

Explanation:

The command “crypto isakmp identity address 172.19.20.24” is not valid. We can only use “crypto isakmp identity {address | hostname}. The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address.

At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified: crypto isakmp identity address

crypto isakmp key sharedkeystring address 192.168.1.33

www.atmicnetworks.com

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified:
crypto isakmp identity address
crypto isakmp key sharedkeystring address 10.0.0.1
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp3880782430The command “crypto enrollment peer address” is not valid either.The command “crypto ca identity …” is only used to declare a trusted CA for the router and puts you in the caidentity configuration mode. Also it should be followed by a name, not an IP address. For example: “crypto caidentity CA-Server” -> Answer A is not correct.Only answer B is the best choice left.

Question: 299

[Security Concepts]
What is a difference between an XSS attack and an SQL injection attack?

A. SQL injection is a hacking method used to attack SQL databases, whereas XSS attacks can exist in many different types of applications
B. XSS is a hacking method used to attack SQL databases, whereas SQL injection attacks can exist in many different types of applications
C. SQL injection attacks are used to steal information from databases whereas XSS attacks are used toredirect users to websites where attackers can steal data from them
D. XSS attacks are used to steal information from databases whereas SQL injection attacks are used toredirect users to websites where attackers can steal data from them

Answer: C

Explanation:

In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters.

Question: 300

[Security Concepts]
An engineer has been tasked with configuring a Cisco FTD to analyze protocol fields and detect anomalies in the traffic from industrial systems. What must be done to meet these requirements?

A. Implement pre-filter policies for the CIP preprocessor
B. Enable traffic analysis in the Cisco FTD
C. Configure intrusion rules for the DNP3 preprocessor
D. Modify the access control policy to trust the industrial traffic

Answer: C

Explanation:

"configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically:
"If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules."
"If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy."

[1] https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.html

Question: 301

[Security Concepts]
Which posture assessment requirement provides options to the client for remediation and requires the remediation within a certain timeframe?

A. Audit
B. Mandatory
C. Optional
D. Visibility

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_policies.html#:~:text=Policy%20Require ment%20Types-,Mandatory%20Requirements,the%20requirements%20within%20the%20time%20specified%20in%20the%20remediation%20timer%20settings.,-For%20example%2C%20you

Mandatory Requirements During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings

Question: 302

[Secure Network Access, Visibility, and Enforcement]
Which attribute has the ability to change during the RADIUS CoA?

A. NTP
B. Authorization
C. Accessibility
D. Membership

Answer: B

Explanation:

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html

Question: 303

[Endpoint Protection and Detection]
With Cisco AMP for Endpoints, which option shows a list of all files that have been executed in your environment?

A. Prevalence
B. File analysis
C. Detections
D. Vulnerable software
E. Threat root cause

Answer: A

Explanation:

Prevalence allows you to view files that have been executed in your deployment.
Note: Threat Root Cause shows how malware is getting onto your computers.
Reference: https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf

Question: 304

[Endpoint Protection and Detection]

A company discovered an attack propagating through their network via a file. A custom file policy was created in order to track this in the future and ensure no other endpoints execute the infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the created is functioning as it should?

A. Create an IP block list for the website from which the file was downloaded
B. Block the application that the file was using to open
C. Upload the hash for the file into the policy
D. Send the file to Cisco Threat Grid for dynamic analysis

Answer: D

Explanation:

the file to Cisco Threat Grid for dynamic analysis. Cisco Threat Grid is a cloud-based service that provides malware analysis and threat intelligence. It can analyze suspicious files and URLs, and provide detailed reports on the behavior, indicators, and severity of the threat1. By sending the file to Cisco Threat Grid, the custom file policy can leverage the dynamic analysis results to detect the file as an indicator of compromise, and prevent other endpoints from executing the infected file. The other options are not correct because they do not address the root cause of the problem, which is the lack of detection by the custom file policy. Creating an IP block list, blocking the application, or uploading the hash for the file may help to mitigate the attack, but they do not ensure that the custom file policy is functioning as it should. Reference:

2: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 - Module 5: Endpoint Protection and Detection

3: Cisco AMP for Endpoints User Guide - Custom Detection Lists

4: Cisco AMP for Endpoints User Guide - File Analysis and Cisco Threat Grid

1: Cisco Threat Grid - Overview

Question: 305

[Network Security]

A network engineer is trying to figure out whether FlexVPN or DMVPN would fit better in their environment. They have a requirement for more stringent security multiple security associations for the connections, more efficient VPN establishment as well consuming less bandwidth. Which solution would be best for this and why?

A. DMVPN because it supports IKEv2 and FlexVPN does not
B. FlexVPN because it supports IKEv2 and DMVPN does not
C. FlexVPN because it uses multiple SAs and DMVPN does not
D. DMVPN because it uses multiple SAs and FlexVPN does not

Answer: C

Explanation:

FlexVPN supports IKEv2 -> Answer A is not correct.
DMVPN supports both IKEv1 & IKEv2 -> Answer B is not correct.
FlexVPN support multiple SAs -> Answer D is not correct.

Question: 306

[Security Concepts]
How does Cisco Workload Optimization Manager help mitigate application performance issues?

A. It deploys an AWS Lambda system
B. It automates resource resizing
C. It optimizes a flow path
D. It sets up a workload forensic score

Answer: B

Explanation:

Cisco Workload Optimization Manager provides specific real-time actions that ensure workloads get the resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software).
Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf

Question: 307

[Endpoint Protection and Detection]
An organization configures Cisco Umbrella to be used for its DNS services. The organization must be able to block traffic based on the subnet that the endpoint is on but it sees only the requests from its public IP address instead of each internal IP address. What must be done to resolve this issue?

A. Set up a Cisco Umbrella virtual appliance to internally field the requests and see the traffic of each IP address
B. Use the tenant control features to identify each subnet being used and track the connections within theCisco Umbrella dashboard
C. Install the Microsoft Active Directory Connector to give IP address information stitched to the requests in the Cisco Umbrella dashboard
D. Configure an internal domain within Cisco Umbrella to help identify each address and create policy from the domains

Answer: A

Explanation:

A Cisco Umbrella virtual appliance (VA) is a lightweight virtual machine that acts as a DNS forwarder in your network. It forwards internal DNS queries to Umbrella and provides Umbrella with the internal IP address and hostname of the device that made the request. This allows Umbrella to apply policies and report on traffic based on the subnet, hostname, or user identity of the device1. The other options are not relevant for this scenario. Tenant control features are used to limit access to specific instances of cloud applications, such as Microsoft 365 or Google G Suite2. The Microsoft Active Directory Connector is used to provision users and groups from Active Directory to Umbrella, not to provide IP address information3. An internal domain is a domain that is resolved by your own DNS server, not by Umbrella, and is used to bypass Umbrella for domains that are only accessible within your network4. Reference:

1: Deploy Virtual Appliances - Umbrella User Guide

2: Manage Tenant Controls - Umbrella SIG User Guide

3: Connect Active Directory to Umbrella to Provision User and Groups

4: Domain Management - Umbrella User Guide

Question: 308

[Security Concepts]

What is a difference between a DoS attack and a DDoS attack?

A. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a

DDoS attack is where multiple systems target a single system with a DoS attack

B. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN C. A DoS attack is where a computer is used to flood a server with UDP packets whereas a DDoS attack is where a computer is used to flood a server with TCP packets

D. A DoS attack is where a computer is used to flood a server with TCP packets whereas a DDoS attack is where a computer is used to flood a server with UDP packets

Answer: A

Explanation:

A DoS (Denial of Service) attack is a type of cyberattack that aims to disrupt the normal functioning of a server, service, or network by overwhelming it with a large amount of traffic or requests. A DoS attack typically uses a single computer or device to launch the attack, sending TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) packets to the target server. TCP and UDP are two common protocols used to send data over the internet. TCP packets require a connection to be established between the sender and the receiver, and ensure that the data is delivered reliably and in order. UDP packets do not require a connection, and do not guarantee the delivery or order of the data. Both TCP and UDP packets can be used to flood a server with requests, consuming its resources and bandwidth, and preventing legitimate users from accessing the service.

A DDoS (Distributed Denial of Service) attack is a type of DoS attack that uses multiple computers or devices to launch the

attack, creating a large network of attackers that can generate more traffic or requests than a single source. A DDoS attack often involves a botnet, which is a network of compromised computers or devices that are controlled by a malicious actor, usually through malware or hacking. The botnet can send TCP or UDP packets to the target server from different locations and IP addresses, making it harder to trace and block the attack. A DDoS attack can also target multiple servers or services that are distributed over a LAN (Local Area Network), such as a web hosting service or a cloud computing platform, affecting the availability and performance of the entire network.

The main difference between a DoS attack and a DDoS attack is the number and diversity of the sources that are involved in the attack. A DoS attack comes from a single source, while a DDoS attack comes from multiple sources. This makes a DDoS attack more powerful, faster, and harder to stop than a DoS attack.

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Malware Threats, Lesson 2: Identifying Network Attacks, Topic: DoS and DDoS Attacks

DoS Attack vs. DDoS Attack: Key Differences? | Fortinet

What's the Difference Between a DOS and DDoS Attack? - How-To Geek

Question: 309

[Security Concepts]

Which two capabilities of Integration APIs are utilized with Cisco DNA center? (Choose two)

A. Upgrade software on switches and routers
B. Third party reporting
C. Connect to ITSM platforms
D. Create new SSIDs on a wireless LAN controller
E. Automatically deploy new virtual routers

Answer: B,C

Explanation:

Reference: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/integration-api-westbound

Question: 310

[Security Concepts]

Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?

A. Integration
B. Intent
C. Event
D. Multivendor

Answer: B

Explanation:

The kind of API that is used with Cisco DNA Center to provision SSIDs, QoS policies, and update software versions on switches is the Intent API. The Intent API is a category of APIs that allows users to express their desired network outcomes or intents, such as creating a site, adding a device, or deploying a network profile. The Intent API then translates these intents into specific network configurations and commands, and applies them to the relevant network devices and services. The Intent API simplifies and automates the network provisioning and management process, and enables users to focus on the business objectives rather than the technical details. Some examples of Intent APIs are:

Site Management API: This API allows users to create, update, delete, and retrieve sites and buildings in Cisco DNA Center. A site is a logical grouping of network devices and services that share common characteristics, such as location, policies, or functions. A site can have one or more buildings, and a building can have one or more floors. Sites are used to organize and manage the network hierarchy and topology.

Network Settings API: This API allows users to configure and manage network-wide settings, such as global credentials, network discovery, IP address pools, DHCP and DNS servers, and SNMP settings.

These settings are applied to all network devices and services that are managed by Cisco DNA Center. Network Profile API: This API allows users to create, update, delete, and retrieve network profiles in Cisco DNA Center. A network profile is a collection of network settings and policies that define how a network segment or service should operate, such as SSIDs, QoS policies, security policies, and device roles. Network profiles are used to standardize and simplify the network configuration and deployment process, and to ensure consistency and compliance across the network.

Software Image Management API: This API allows users to manage the software images and versions of network devices that are managed by Cisco DNA Center. Users can import, export, delete, and retrieve software images, as well as assign them to network devices or device groups. Users can also schedule and monitor software image updates, and view the software image compliance status of network devices.

Reference:

Cisco DNA Center Platform User Guide, Release 2.3.7.0 and 2.3.7.3, Chapter 1: Introduction to Cisco DNA Center Platform, Topic: Intent APIs

Introduction to Cisco DNA Center REST APIs, Learning Lab: Cisco DNA Center Platform - Network Devices

Cisco DNA Center Platform - Cisco DevNet, APIs: Intent APIs

Question: 311

[Security Concepts]

What is the purpose of CA in a PKI?

A. To issue and revoke digital certificates
B. To validate the authenticity of a digital certificate
C. To create the private key for a digital certificate
D. To certify the ownership of a public key by the named subject

Answer: A

Explanation:

A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues.

Reference: https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in- pki/

Question: 312

[Security Concepts]

Which DevSecOps implementation process gives a weekly or daily update instead of monthly or quarterly in the applications?

A. Orchestration
B. CI/CD pipeline
C. Container
D. Security

Answer: B

Explanation:

Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly.

Reference: https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/

Question: 313

[Security Operations]

Which parameter is required when configuring a Netflow exporter on a Cisco Router?

A. DSCP value
B. Source interface
C. Exporter name
D. Exporter description

Answer: C

Explanation:

www.atmicnetworks.com

An example of configuring a NetFlow exporter is shown below: flow exporter Exporter destination 192.168.100.22 transport udp 2055

Question: 314

[Security Concepts]
Which category includes DoS Attacks?

A. Virus attacks
B. Trojan attacks
C. Flood attacks
D. Phishing attacks

Answer: C

Explanation:

Flood attacks are a type of denial-of-service (DoS) attacks that aim to saturate the bandwidth or resources of a target by sending a large number of packets or requests. Flood attacks can be classified into different categories based on the protocol or layer they target, such as ICMP, UDP, TCP SYN, HTTP, DNS, etc. Flood attacks can also be distributed (DDoS) if they involve multiple sources of attack traffic, such as compromised devices or servers123. Reference := 1: Denial of Service - OWASP Cheat Sheet Series 2: What is a denial-of-service (DoS) attack? | Cloudflare 3: Types of DOS attacks - GeeksforGeeks

Question: 315

[Network Security]
What are two advantages of using Cisco Any connect over DMVPN? (Choose two)

A. It provides spoke-to-spoke communications without traversing the hub
B. It allows different routing protocols to work over the tunnel
C. It allows customization of access policies based on user identity
D. It allows multiple sites to connect to the data center
E. It enables VPN access for individual users from their machines

Answer: C,E

Explanation:

Cisco AnyConnect is a client-based VPN solution that provides secure remote access for individual users from their machines. It allows customization of access policies based on user identity, such as group membership, device posture, or location. This enables granular control over who can access what resources on the network. Cisco AnyConnect also supports various authentication methods, such as certificates, multifactor authentication, or single sign-on. Cisco AnyConnect can be deployed

with Cisco Adaptive Security Appliance (ASA) or Cisco Firepower Threat Defense (FTD) as the VPN headend.
Cisco DMVPN is a network-based VPN solution that provides dynamic, on-demand, and scalable connectivity for branch offices, teleworkers, and business partners. It uses multipoint GRE (mGRE) tunnels and Next Hop Resolution Protocol (NHRP) to establish direct spoke-to-spoke communications without traversing the hub. It also supports IPsec encryption and various routing protocols over the tunnel. Cisco DMVPN can be deployed with Cisco IOS routers as the VPN headend.
The advantages of using Cisco AnyConnect over DMVPN are:
It enables VPN access for individual users from their machines, which is useful for mobile workers or telecommuters who need to connect to the network from anywhere.
It allows customization of access policies based on user identity, which is useful for enforcing security and compliance requirements for different types of users or devices.
The advantages of using DMVPN over Cisco AnyConnect are:
It provides spoke-to-spoke communications without traversing the hub, which reduces latency and bandwidth consumption for traffic between remote sites.
It allows different routing protocols to work over the tunnel, which provides flexibility and scalability for network design and management.
Reference:
Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications Data Sheet

[Cisco AnyConnect Secure Mobility Client Data Sheet]
Cisco Get VPN vs DMVPN: Difference and Comparison
Comparing Cisco SD-WAN to DMVPN
What are two advantages of using Cisco AnyConnect over DMVPN?

Question: 316

[Security Concepts]
When choosing an algorithm to us, what should be considered about Diffie Hellman and RSA for key establishment?

A. RSA is an asymmetric key establishment algorithm intended to output symmetric keys
B. RSA is a symmetric key establishment algorithm intended to output asymmetric keys
C. DH is a symmetric key establishment algorithm intended to output asymmetric keys
D. DH is an asymmetric key establishment algorithm intended to output symmetric keys

Answer: D

Explanation:

GETVPN and IPsec are both VPN technologies that use ESP (Encapsulating Security Payload) to encrypt and authenticate data packets. However, they differ in the following aspects:
GETVPN uses a group IPSec security paradigm, which means that all group members share the same IPSec SA (Security Association) and can communicate with each other without having to establish point-to-point tunnels. IPsec, on the other hand, uses a pair-wise IPSec security paradigm, which
requires each pair of devices to negotiate and maintain their own IPSec SAs and tunnels.
GETVPN uses GDOI (Group Domain of Interpretation) as a key management protocol, which allows a Key Server (KS) to

distribute the encryption keys and policies to all group members. IPsec uses IKE (Internet Key Exchange) as a key management protocol, which involves two phases of negotiation between each pair of devices to establish the IPSec SAs.

GETVPN supports multicast traffic without the need for GRE (Generic Routing Encapsulation) tunneling, as it preserves the original IP header of the packet. IPsec does not support multicast traffic natively, and requires GRE tunneling to encapsulate the multicast packets with a new IP header.

GETVPN relies on the underlying WAN routing to deliver the encrypted packets to the destination, as it does not create any overlay routing. IPsec creates an overlay routing, which may introduce additional latency and complexity.

Reference :=

Some possible references are:

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 6: Secure Connectivity, Lesson 6.2: Implementing Site-to-Site VPNs, Topic 6.2.2: Group Encrypted Transport VPN

Group Encrypted Transport VPN (GETVPN)

GETVPN - Cisco Community

Cisco Get VPN vs DMVPN: Difference and Comparison

What is a difference between GETVPN and IPsec?

Diffie Hellman (DH) uses a private-public key pair to establish a shared secret, typically a symmetric key. DH is not a symmetric algorithm – it is an asymmetric algorithm used to establish a shared secret for a symmetric key algorithm.

Question: 317

[Security Concepts]

Which type of DNS abuse exchanges data between two computers even when there is no direct connection?

A. Malware installation
B. Command-and-control communication
C. Network footprinting
D. Data exfiltration

Answer: D

Explanation:

Malware installation: This may be done by hijacking DNS queries and responding with malicious IP addresses.

Command & Control communication: As part of lateral movement, after an initial compromise, DNS communications is abused to communicate with a C2 server. This typically involves making periodic DNS queries from a computer in the target network for a domain controlled by the adversary. The responses contain encoded messages that may be used to perform unauthorized actions in the target network.

Network footprinting: Adversaries use DNS queries to build a map of the network. Attackers live off the terrain so developing a map is important to them.

Data theft (exfiltration): Abuse of DNS to transfer data; this may be performed by tunneling other protocols like FTP, SSH through DNS queries and responses. Attackers make multiple DNS queries from a compromised computer to a domain owned by the adversary. DNS tunneling can also be used for executing commands and transferring malware into the target network.
Reference: https://www.netsurion.com/articles/5-types-of-dns-attacks-and-how-to-detect-them

Question: 318

[Network Security]
What is a difference between GETVPN and IPsec?

A. GETVPN reduces latency and provides encryption over MPLS without the use of a central hub
B. GETVPN provides key management and security association management
C. GETVPN is based on IKEv2 and does not support IKEv1
D. GETVPN is used to build a VPN network with multiple sites without having to statically configure all devices

Answer: C

Explanation:

Question: 319

[Security Operations]
What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

A. Telemetry uses a pull mehod, which makes it more reliable than SNMP
B. Telemetry uses push and pull, which makes it more scalable than SNMP
C. Telemetry uses push and pull which makes it more secure than SNMP
D. Telemetry uses a push method which makes it faster than SNMP

Answer: D

Explanation:

SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.
The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data.
Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.

Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Referfence: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start- guide/streaming telemetry

Question: 320

[Network Security]

An organization wants to use Cisco FTD or Cisco ASA devices. Specific URLs must be blocked from being accessed via the firewall which requires that the administrator input the bad URL categories that the organization wants blocked into the access policy. Which solution should be used to meet this requirement?

A. Cisco ASA because it enables URL filtering and blocks malicious URLs by default, whereas Cisco FTDdoes not
B. Cisco ASA because it includes URL filtering in the access control policy capabilities, whereas Cisco FTD does not
C. Cisco FTD because it includes URL filtering in the access control policy capabilities, whereas Cisco ASA does not
D. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not

Answer: C

Explanation:

Cisco FTD is the recommended solution for this requirement because it allows the administrator to configure URL filtering as part of the access control policy. URL filtering in FTD can block or allow traffic based on the destination URL of a web request, the generalized category of the URL, or the public reputation of the target site. FTD can also use HTTPS URL filtering to inspect encrypted web traffic and block malicious or unwanted sites. FTD supports both local URL lists and external URL filtering servers such as Cisco Talos Intelligence Group (TIG), Websense, or SmartFilter12.

Cisco ASA does not include URL filtering in the access control policy capabilities. ASA can only enable URL filtering for web traffic using external filtering servers such as Websense or SmartFilter. ASA cannot block HTTPS or FTP traffic based on URLs, nor can it use local URL lists or categories. ASA also does not block malicious URLs by default, but relies on the filtering server's configuration34.

Therefore, option C is the correct answer, and the other options are incorrect. Reference :=

FTD URL Filtering - How it works? - Cisco Community

Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2.3 - Access Control

Configuring Filtering Services - Cisco

Configuring URL Filtering - Cisco

Question: 321

[Content Security]

An administrator configures a Cisco WSA to receive redirected traffic over ports 80 and 443. The organization requires that a network device with specific WSA integration capabilities be configured to send the traffic to the WSA to proxy the requests and increase visibility, while making this invisible to the users. What must be done on the Cisco WSA to support these requirements?

A. Configure transparent traffic redirection using WCCP in the Cisco WSA and on the network device B. Configure active traffic redirection using WPAD in the Cisco WSA and on the network device C. Use the Layer 4 setting in the Cisco WSA to receive explicit forward requests from the network device
D. Use PAC keys to allow only the required network devices to send the traffic to the Cisco WSA

Answer: A

Explanation:

Transparent traffic redirection using WCCP is a deployment mode for the Cisco WSA that allows it to intercept and proxy web requests from client applications without requiring any configuration on the clients. This mode increases the visibility and control of web traffic, while making the proxy function invisible to the users. To support this mode, the Cisco WSA must be configured to use the transparent proxy mode, which enables it to listen on ports 80 and 443 for HTTP and HTTPS traffic, respectively. The Cisco WSA must also be configured to use WCCP service IDs, which are numerical identifiers that specify the type and range of ports to be redirected. For example, service ID 0 (web-cache) redirects port 80, service ID 70 (https-cache) redirects port 443, and service ID 60 (ftp-native) redirects port 21 and a range of passive FTP ports. The Cisco WSA must also be configured to join a WCCP group, which is a set of WCCP routers or switches that cooperate to redirect traffic to the WSA. The WCCP group can be specified by a group list, which is an access list that defines the IP addresses of the WCCP routers or switches, or by a password, which is a shared secret that authenticates the WCCP communication. The WCCP group must also be configured on the network device that performs the traffic redirection, such as a Cisco router, switch, or ASA firewall. The network device must support WCCPv2, which is the latest version of the protocol that allows for advanced features such as load balancing, encryption, and GRE encapsulation. The network device must also be configured to use the same WCCP service IDs and group list or password as the Cisco WSA. The network device must also be configured to apply the WCCP redirection to the appropriate interface and direction, such as

the inside interface and inbound direction for traffic originating from the internal network. The network device must also be configured to use an access list that defines the traffic to be redirected or bypassed, such as the source and destination IP addresses, ports, and protocols. The access list can also be used to exclude certain traffic from WCCP redirection, such as traffic to private or internal destinations, or traffic from specific hosts123 Reference := 1: Configure Transparent Redirection With WCCP in Order to Redirect Native FTP Traffic - Cisco 2: Solved: Transparent Redirection - Cisco Community 3: Cisco WSA : Is it possible to use web proxy in transparent mode without WCCP - Cisco Community

Question: 322

[Secure Network Access, Visibility, and Enforcement]
An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices. Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen however the attributes for CDP or DHCP are not. What should the administrator do to address this issue?

A. Configure the ip dhcp snooping trust command on the DHCP interfaces to get the information to Cisco ISE
B. Configure the authentication port-control auto feature within Cisco ISE to identify the devices that are trying to connect
C. Configure a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE

D. Configure the device sensor feature within the switch to send the appropriate protocol information

Answer: D

Explanation:

Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols: + Cisco Discovery Protocol (CDP) + Link Layer Discovery Protocol (LLDP)
+ Dynamic Host Configuration Protocol (DHCP)

Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292- ConfigureDevice-Sensor-for-ISE-Profilin.html

Question: 323

[Secure Network Access, Visibility, and Enforcement]

A network engineer must monitor user and device behavior within the on-premises network. This data must be sent to the Cisco Stealthwatch Cloud analytics platform for analysis. What must be done to meet this requirement using the Ubuntu-based VM appliance deployed in a VMware-based hypervisor?

A. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud
B. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud
C. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud
D. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud

Answer: B

Explanation:

The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. –VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC- 2240-LG2.pdf

Question: 324

[Security Concepts]

An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management

port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?

A. Manually change the management port on Cisco FMC and all managed Cisco FTD devices
B. Set the tunnel to go through the Cisco FTD
C. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTDdevices
D. Set the tunnel port to 8305

Answer: A

Explanation:

The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305.

Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other.

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc- ftd-mgmtnw.html

Question: 325

[Security Concepts]

Which service allows a user export application usage and performance statistics with Cisco Application Visibility and control?

A. SNORT
B. NetFlow
C. SNMP
D. 802.1X

Answer: B

Explanation:

Application Visibility and control (AVC) supports NetFlow to export application usage and performance statistics. This data can be used for analytics, billing, and security policies.

www.atmicnetworks.com

Question: 326

[Endpoint Protection and Detection]

An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the configuration. The simple detection mechanism is configured, but the dashboard indicates that the hash is not 64 characters and is non-zero. What is the issue?

A. The engineer is attempting to upload a hash created using MD5 instead of SHA-256
B. The file being uploaded is incompatible with simple detections and must use advanced detections
C. The hash being uploaded is part of a set in an incorrect format
D. The engineer is attempting to upload a file instead of a hash

Answer: A

Explanation:

The issue is that the engineer is using the wrong hashing algorithm to generate the hash for the custom detection policy. Cisco AMP for Endpoints requires the use of SHA-256 hashes for simple custom detections, as stated in the Configure a Simple Custom Detection List on the AMP for Endpoints Portal document. SHA-256 hashes are 64 hexadecimal characters long, while MD5 hashes are 32 hexadecimal characters long. Therefore, if the engineer tries to upload a hash created using MD5, the dashboard will indicate that the hash is not 64 characters and is non-zero, as shown in the image below:

To resolve the issue, the engineer should use a tool or a website that can generate SHA-256 hashes from files, such as this one, and upload the correct hash to the custom detection list. Reference : Configure a Simple Custom Detection List on the AMP for Endpoints Portal, Create an Advanced Custom Detection List in Cisco Secure Endpoint, Working with Advanced Malware Protection (AMP) for Endpoints

Question: 327

[Endpoint Protection and Detection] Refer to the exhibit.

www.atmicnetworks.com

```
interface GigabitEthernet1/0/18
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device-tracking attach-policy IPDT_MAX_10
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
dot1x pae authenticator
dot1x timeout tx-period 7
dot1x max-reauth-req 3
spanning-tree portfast
```

Refer to the exhibit. A Cisco ISE administrator adds a new switch to an 802.1X deployment and has difficulty with some endpoints gaining access.

Most PCs and IP phones can connect and authenticate using their machine certificate credentials. However printer and video cameras cannot base d on the interface configuration provided, what must be to get these devices on to the network using Cisco ISE for authentication and authorization while maintaining security controls?

A. Change the default policy in Cisco ISE to allow all devices not using machine authentication .
B. Enable insecure protocols within Cisco ISE in the allowed protocols configuration.
C. Configure authentication event fail retry 2 action authorize vlan 41 on the interface
D. Add mab to the interface configuration.

Answer: D

Explanation:

the interface configuration. MAB stands for MAC Authentication Bypass, which is a feature that allows devices that do not support 802.1X, such as printers and video cameras, to bypass the authentication process and gain network access based on their MAC addresses1. By adding mab to the interface configuration, the Cisco ISE administrator can enable MAB as a fallback method after 802.1X fails or times out. This way, the devices that support 802.1X can use their machine certificate credentials, while the devices that do not support 802.1X can use their MAC addresses to authenticate with Cisco ISE2. The other options are not correct because they either compromise the security controls or do not address the problem. Changing the default policy in Cisco ISE to allow all devices not using machine authentication would weaken the security posture and expose the network to unauthorized access. Enabling insecure protocols within Cisco ISE in the allowed

protocols configuration would also reduce the security level and increase the risk of attacks. Configuring authentication event fail retry 2 action authorize vlan 41 on the interface would only apply to the devices that fail authentication twice, and would not solve the issue for the devices that do not support 802.1X at

www.atmicnetworks.com

all3. Reference:

1: MAC Authentication Bypass Deployment Guide

2: Configuring MAC Authentication Bypass

3: Cisco Identity Services Engine Administrator Guide, Release 3.1 - Segmentation

Question: 328

[Secure Network Access, Visibility, and Enforcement]

An administrator is adding a new switch onto the network and has configured AAA for network access control. When testing the configuration, the RADIUS authenticates to Cisco ISE but is being rejected. Why is the ip radius source-interface command needed for this configuration?

A. Only requests that originate from a configured NAS IP are accepted by a RADIUS server

B. The RADIUS authentication key is transmitted only from the defined RADIUS source interface

C. RADIUS requests are generated only by a router if a RADIUS source interface is defined.

D. Encrypted RADIUS authentication requires the RADIUS source interface be defined

Answer: A

Explanation:

The ip radius source-interface command is needed for this configuration because it forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets. This ensures that the RADIUS server can identify the source of the requests and apply the appropriate policies. If this command is not used, RADIUS will use the IP address of the interface that is closest to the destination, which may not match the configured NAS IP on the RADIUS server. This can cause the RADIUS server to reject the requests as unauthorized12. Reference:

1: RADIUS source interface - Cisco Community

2: RADIUS Commands - Cisco

Question: 329

[Security Concepts]

A customer has various external HTTP resources available including Intranet. Extranet, and Internet, with a proxy configuration running in explicit mode Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?

A. Transparent mode

B. Forward file

C. PAC file

D. Bridge mode

www.atmicnetworks.com

Answer: C

Explanation:

A PAC file is a Proxy Auto-Configuration file that contains a JavaScript function that determines whether web browser requests go directly to the destination or are forwarded to a web proxy server. A PAC file allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy based on the URL and the host name. A PAC file can be downloaded from a web server or a local file. A PAC file is more suitable for complex proxy configurations or multiple proxy servers12

A transparent mode is a proxy configuration where the client browsers do not need to be configured to use the proxy. The proxy intercepts the traffic and forwards it to the destination. A transparent mode does not allow the client browsers to select when to connect direct or when to use the proxy34

A forward file is not a valid proxy configuration method.

A bridge mode is a network configuration where a device connects two or more network segments and forwards traffic between them. A bridge mode is not a proxy configuration method5 Reference := 1: Proxy Auto-Configuration (PAC) file - HTTP | MDN 2: Proxy auto-config - Wikipedia 3: Explicit and Transparent Proxy - techdocs.broadcom.com 4: Configure Explicit Proxy - Palo Alto Networks | TechDocs 5: config web-proxy explicit | FortiGate / FortiOS 7.4.0

Question: 330

[Security Concepts]

```
import http client
import base64
import ssl
import sys

host = sys.argv[1] # "10.10 10.240"
user = sys argv[2] # "ersad"
password - sys argv(3] # "Passwordl"

conn = http client HTTPSConnection("{}:9060" format(host),
contexts! SSL Contexts! PROTOCOL_TLSv1_2))

creds = str encodef' join((user, password)))
encodedAuth = bytes decode(base64.b64encode(creds))

headers - {
    'accept' "application/json",
    'authorization' " " |oin(rBasic",encodedAuth)),
    'cache-control' "no-cache",
    }

conn roquest("GET', "/ers/config/internaluser/", headers-headers)

res = conn getresponsef)
data - res read()

pnntf'Status 0".format(res.status))
printf'Header An{}" tormat(res head
nnntCBodyVi(rfprr^^
```

Refer to the exhibit. What does this Python script accomplish?

A. It allows authentication with TLSv1 SSL protocol
B. It authenticates to a Cisco ISE with an SSH connection.
C. lt authenticates to a Cisco ISE server using the username of ersad
D. It lists the LDAP users from the external identity store configured on Cisco ISE

Answer: C

Explanation:

The Python script accomplishes the following tasks:
It imports the required libraries for HTTP, base64, SSL, and sys modules.
It takes the host, user, and password information from the command line arguments and assigns them to variables.
It creates an HTTPS connection object using the host and port 9060, and specifies the SSL protocol as TLSv1_2.
It encodes the user and password information in base64 format for basic HTTP authentication.
It sets the headers for the HTTP request, including the accept, authorization, and cache-control fields. It sends a GET request to the Cisco ISE server to retrieve information from the "/ers/config/internaluser/" endpoint, which returns the list of internal users configured on Cisco ISE.
It reads the response from the server and prints the status, headers, and body in a human-readable format.
The script authenticates to the Cisco ISE server using the username of ersad and the password of Password1, and

retrieves the internal user information from the server.

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 5: Secure Network Access, Lesson 2: Cisco Identity Services Engine, Topic: Cisco ISE REST API Cisco Identity Services Engine API Reference Guide, Release 2.7 - Cisco ISE ERS API Overview [Cisco Identity Services Engine]

Python 3 - HTTP Client - Tutorialspoint

Question: 331

[Security Concepts]

Which system facilitates deploying microsegmentation and multi-tenancy services with a policybased container?

A. SDLC
B. Docker
C. Lambda
D. Contiv

Answer: D

Explanation:

Contiv is an open source container networking fabric that supports heterogeneous container deployments across virtual machines, bare-metal, and public or private clouds. Contiv facilitates deploying microsegmentation and multi-tenancy services with a policy-based container by allowing cloud architects and IT admins to create, manage, and enforce operational policies such as traffic isolation, bandwidth prioritization, latency requirements, and policies for L4-L7 network services. Contiv also integrates natively with Cisco infrastructure and provides consistent networking across any platform (Docker Swarm, Kubernetes, or OpenShift) and any networking backend (Layer 2, Layer 3, Overlays, or ACI mode)123. Reference := 1: Introducing Contiv 1.0 - The Most Powerful Container Networking Fabric 2: contivpp 3: Contiv · GitHub

Question: 332

[Endpoint Protection and Detection]

Which feature is leveraged by advanced antimalware capabilities to be an effective endpomt protection platform?

A. big data
B. storm centers
C. sandboxing
D. blocklisting

Answer: C

Explanation:

Sandboxing is a feature that is leveraged by advanced antimalware capabilities to be an effective endpoint protection platform. Sandboxing allows an endpoint protection platform to isolate suspect files in a safe environment and analyze their behavior and impact without affecting the rest of the system. Sandboxing can help detect and prevent unknown or zero-day malware that may evade traditional signature-based detection methods. Sandboxing can also provide valuable threat intelligence and forensic data for further investigation and response.

Big data, storm centers, and blocklisting are not features that are leveraged by advanced antimalware capabilities to be an effective endpoint protection platform. Big data refers to the large volume, variety, and velocity of data that can be used for various purposes, such as analytics, machine learning, or business intelligence. Storm centers are centralized hubs that monitor and respond to cyber incidents and threats. Blocklisting is a method of preventing access to malicious or unwanted domains, IP addresses, or files by adding them to a list of blocked entities. Reference: Endpoint Protection Platform (EPP) Definition

Cisco Advanced Malware Protection (AMP) for Endpoints

Cisco AMP for Endpoints: Sandboxing

Question: 333

[Security Concepts]

An organization wants to implement a cloud-delivered and SaaS-based solution to provide visibility and threat detection across the AWS network. The solution must be deployed without software agents and rely on AWS VPC flow logs instead. Which solution meets these requirements?

A. Cisco Stealthwatch Cloud
B. Cisco Umbrella
C. NetFlow collectors
D. Cisco Cloudlock

Answer: A

Explanation:

Cisco Stealthwatch Cloud is a cloud-delivered and SaaS-based solution that provides visibility and threat detection across the AWS network. It does not require any software agents to be installed on the AWS instances, and it relies on AWS VPC flow logs to collect network traffic metadata. Cisco Stealthwatch Cloud analyzes the flow logs using machine learning and behavioral modeling to detect anomalies and threats, such as data exfiltration, lateral movement, reconnaissance, and compromised instances. Cisco Stealthwatch Cloud also provides contextual information and actionable alerts to help users respond to incidents and remediate issues.

Cisco Umbrella is a cloud-delivered and SaaS-based solution that provides DNS-layer security and web filtering for internet traffic. It does not provide visibility and threat detection for internal AWS network traffic, and it requires software agents to be installed on the endpoints or network devices to enforce policies and redirect DNS requests.

NetFlow collectors are devices or software applications that collect and analyze NetFlow records, which are generated by network devices to capture information about IP traffic flows. NetFlow collectors can provide visibility and threat detection for network traffic, but they are not cloud- delivered or SaaS-based solutions. They also require NetFlow exporters to be

configured on the network devices, which may not be supported by AWS.
Cisco Cloudlock is a cloud-delivered and SaaS-based solution that provides cloud security posture management (CSPM) and cloud access security broker (CASB) capabilities for cloud applications and environments. It does not provide visibility and threat detection for AWS network traffic, and it does not rely on AWS VPC flow logs. It focuses on protecting cloud data, users, and configurations from misconfigurations, compliance violations, and malicious activities. Reference := Cisco Stealthwatch Cloud for AWS
Cisco Umbrella
NetFlow

[Cisco Cloudlock]

Question: 334

[Security Concepts]
What is the difference between a vulnerability and an exploit?

A. A vulnerability is a hypothetical event for an attacker to exploit
B. A vulnerability is a weakness that can be exploited by an attacker
C. An exploit is a weakness that can cause a vulnerability in the network
D. An exploit is a hypothetical event that causes a vulnerability in the network

Answer: B

Explanation:

vulnerability is a flaw or gap in the security of a system or network that can be exploited by an attacker to compromise its functionality, integrity, confidentiality, or availability. A vulnerability can

exist in the design, implementation, configuration, or operation of a system or network, and can be caused by human errors, software bugs, hardware defects, or environmental factors. A vulnerability can be exploited by an attacker using various methods, such as malware, phishing, brute force, denial-of-service, or injection attacks. A vulnerability can also be exploited by an insider who has legitimate access to the system or network, but abuses their privileges for malicious purposes. A vulnerability can be discovered by security researchers, ethical hackers, or malicious hackers, and can be reported to the vendor or the public for remediation or exploitation. A vulnerability can be mitigated by applying patches, updates, or configuration changes, or by using security tools such as firewalls, antivirus, or encryption.
An exploit is a piece of code, data, or technique that takes advantage of a vulnerability to perform unauthorized or malicious actions on a system or network. An exploit can be used to gain access, escalate privileges, execute commands, steal data, disrupt services, or damage resources. An exploit can be delivered by various means, such as email attachments, web links, removable media, or network packets. An exploit can be developed by security researchers, ethical hackers, or malicious hackers, and can be shared or sold on the dark web or other platforms for testing or attacking purposes. An exploit can be detected by security tools such as intrusion detection systems, antivirus, or anti-exploit software.
The difference between a vulnerability and an exploit is that a vulnerability is a potential weakness that can be exploited, while an exploit is an actual attack that uses a vulnerability. A vulnerability can exist without being exploited, but an exploit cannot exist without a vulnerability. A vulnerability can be fixed or prevented, but an exploit can only be blocked or stopped. Reference := Exploit vs Vulnerability: What's the Difference? - InfoSec Insights Difference Between Vulnerability and Exploit - GeeksforGeeks Exploit vs. Vulnerability: What Is the Difference? - Coralogix

Question: 335

[Security Concepts]
Cisco SensorBase gaihers threat information from a variety of Cisco products and services and performs analytics to find patterns on threats Which term describes this process?

A. deployment
B. consumption
C. authoring
D. sharing

Answer: B

Explanation:

Cisco SensorBase gathers threat information from a variety of Cisco products and services, such as Cisco IPS, Cisco ASA, Cisco IronPort, Cisco Umbrella, and Cisco Talos, and performs analytics to find patterns on threats. This process is called consumption, which is one of the four phases of the Cisco Security Intelligence Operations (SIO) framework. The consumption phase involves collecting,

aggregating, and analyzing threat data from multiple sources and providing actionable intelligence and tools to customers and partners. The consumption phase also leverages the Cisco SensorBase Network, which is the world's largest threat monitoring network that tracks millions of domains and IP addresses around the world and maintains a global watch list for Internet traffic. SensorBase provides Cisco with an assessment of reliability for known Internet domains and IP addresses, based on their reputation score, category, volume, and threat level. SensorBase also provides threat data overviews, such as the top email and spam senders by country, and the standard categories used to classify website content and attack types1234. Reference := 1: How Cisco's SensorBase works | Network World 2: What is Cisco SensorBase? - networklore.com 3: User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - GD … 4: Cisco Security Intelligence Operations At-A-Glance

Question: 336

[Security Concepts]
An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea!thwatch406397954 command Which additional command is required to complete the flow record?

A. transport udp 2055
B. match ipv4 ttl
C. cache timeout active 60
D. destination 1.1.1.1

Answer: D

Explanation:

The destination command is required to complete the flow record and specify the IP address of the Stealthwatch collector that will receive the NetFlow data. The transport udp 2055 command is also needed, but it is part of the flow exporter configuration, not the flow record. The match ipv4 ttl and cache timeout active 60 commands are optional and can be used to customize the flow record, but they are not mandatory. The flow record defines the fields that are collected and exported for each flow, such as source and destination IP addresses, ports, protocols, etc. The flow exporter defines the destination, source, transport protocol, and port for sending the NetFlow data. The flow monitor binds the flow record and the flow exporter together and applies them to an interface. The following is an example of a complete NetFlow configuration for sending data to Stealthwatch:
flow exporter EXPORTER description Export NetFlow to Stealthwatch destination 1.1.1.1 exportprotocol netflow-v9 source Vlan100 transport udp 2055 ! flow record RECORD description NetFlow record match datalink mac source address input match datalink mac destination address input match datalink vlan input match ipv4 ttl match ipv4 tos match ipv4 protocol match ipv4 source address match ipv4 destination address match transport source-port match transport destination-port match interface input collect interface output collect counter bytes long collect counter packets long collect timestamp absolute first collect timestamp absolute last ! flow monitor IPv4_NETFLOW record RECORD exporter EXPORTER cache timeout active 60 ! interface <> ip flow monitor IPv4_NETFLOW input ! Reference : Configuring and Troubleshooting NetFlow for Stealthwatch, Cisco NetFlow

Configuration, Building a Better Monitoring Solution with Flexible Netflow

Question: 337

[Security Concepts]
Which Cisco platform processes behavior baselines, monitors for deviations, and reviews for malicious processes in data center traffic and servers while performing software vulnerability detection?

A. Cisco Tetration
B. Cisco ISE
C. Cisco AMP for Network
D. Cisco AnyConnect

Answer: A

Explanation:

Cisco Tetration, which is a hybrid-cloud workload protection platform that uses machine learning, behavior analysis, and algorithmic approaches to secure compute instances in both the on-premises data center and the public cloud1. Cisco Tetration can process behavior baselines, monitor for deviations, and review for malicious processes in data center traffic and servers while performing software vulnerability detection. It can also provide zero-trust microsegmentation, proactive identification of security incidents, and reduction of the attack surface1. The other options are not correct because they do not offer the same level of workload protection as Cisco Tetration. Cisco ISE is an identity and access control platform that provides secure network access, endpoint compliance, and device administration2. Cisco AMP for Network is a network-based

www.atmicnetworks.com

malware prevention solution that detects and blocks malicious files and URLs before they reach the endpoints3. Cisco AnyConnect is a VPN client that provides secure remote access, endpoint visibility, and posture enforcement4. Reference:

1: Cisco Secure Workload Platform Data Sheet
2: Cisco Identity Services Engine Data Sheet
3: Cisco Advanced Malware Protection for Networks Data Sheet
4: Cisco AnyConnect Secure Mobility Client Data Sheet

Question: 338

[Security Concepts]
How is data sent out to the attacker during a DNS tunneling attack?

A. as part of the UDP/53 packet payload

B. as part of the domain name
C. as part of the TCP/53 packet header
D. as part of the DNS response packet

Answer: B

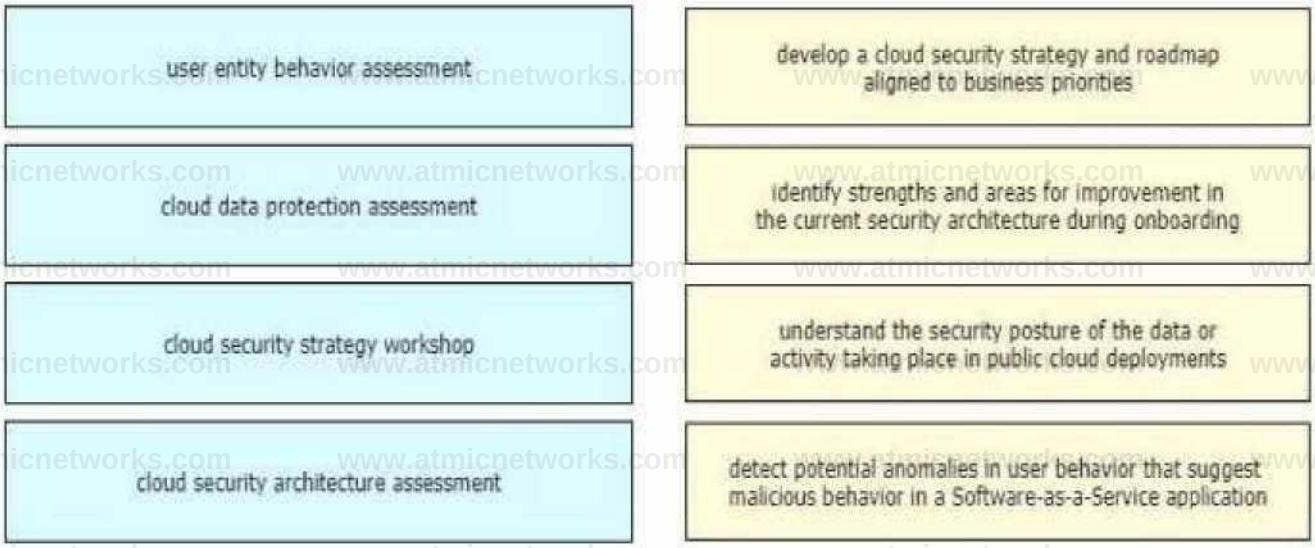
Explanation:

Data is sent out to the attacker during a DNS tunneling attack as part of the domain name. DNS tunneling is a technique that encodes the data of other protocols or programs in DNS queries and responses. The attacker registers a domain, such as badsite.com, and points it to a server under their control, where a tunneling program is installed. The attacker infects a device with malware, which sends DNS queries to the attacker's server, using subdomains of badsite.com to encode the data. For example, the malware could send a query for 1234.badsite.com, where 1234 is the encoded data. The attacker's server decodes the data from the subdomain and sends back a DNS response, which may also contain encoded data in the answer section12. The other options are not correct, because they do not use the domain name to encode the data. The UDP/53 and TCP/53 packet payload and header are used to transport the DNS query and response, but they are not modified by the tunneling technique. The DNS response packet contains the answer to the query, but it is not the only way to send data to the attacker3. Reference:

1: DNS Tunneling attack - What is it, and how to protect ourselves?
2: What Is DNS Tunneling? - Palo Alto Networks
3: What Are DNS Attacks? - Palo Alto Networks

Question: 339

DRAG DROP
[Securing the Cloud]
Drag and drop the cloud security assessment components from the left onto the definitions on the right.



Answer:

Explanation:



Question: 340

[Secure Network Access, Visibility, and Enforcement]

An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?

A. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within

Cisco ISE.

B. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE

C. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.

D. Modify the current policy with the condition MFASourceSequence DUO=true in the authorization conditions within Cisco ISE

Answer: B

Explanation:

accomplish the task is to install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE. This will allow the engineer to integrate Cisco ISE with Cisco DUO for TACACS+ device administration using Active Directory as the primary authentication source and Cisco DUO as the secondary authentication source for multi-factor authentication (MFA). The steps to configure this solution are as follows12:

Install and configure the Cisco DUO Authentication Proxy on a Windows or Linux machine. The proxy will act as a RADIUS server that communicates with Cisco ISE and a RADIUS client that communicates with Cisco DUO cloud. The proxy will also connect to Active Directory for the primary authentication of the users.

Configure the proxy by editing the authproxy.cfg file. The file should include the following sections:

[ad_client]: This section defines the connection parameters to Active Directory, such as the host, service_account_username, service_account_password, and search_dn.

[radius_server_auto]: This section defines the RADIUS server parameters for the proxy, such as the ikey, skey, api_host, radius_ip_1, radius_secret_1, and client parameters. The ikey, skey, and api_host are obtained from the Cisco DUO web portal when creating a RADIUS application. The radius_ip_1 and radius_secret_1 are the IP address and shared secret of the Cisco ISE node that will send authentication requests to the proxy. The client parameter specifies the authentication method for Cisco DUO, such as auto, push, phone, or passcode.

[main]: This section defines the global settings for the proxy, such as the debug, log_max_size, and log_max_files parameters.

Restart the proxy service after saving the authproxy.cfg file.

Configure Cisco ISE as a TACACS+ server and add the proxy as an external RADIUS server. The steps are as follows:

Navigate to Administration > System > Deployment and enable the Device Administration Service on the appropriate node.

Navigate to Work Centers > Device Administration > Network Resources and add the network devices that will use TACACS+ for device administration. Specify the device name, IP address, device type, and shared secret.

Navigate to Work Centers > Device Administration > Network Access and add the proxy as an external RADIUS server. Specify the server name, IP address, port, shared secret, and timeout. Optionally, enable the Continue for additional authorization policy option to allow Cisco ISE to perform authorization based on the user's Active Directory attributes after successful authentication by Cisco DUO.

Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles and create a TACACS profile for device administration. Specify the profile name, type, and custom attributes, such as the shell:roles and shell:priv-lvl attributes.

Navigate to Work Centers > Device Administration > Policy Sets and create a policy set for device administration. Specify the policy set name, conditions, and results. The conditions can be based on the device type, the protocol, or the identity source sequence. The results can be the TACACS profile and the external RADIUS server (the proxy).

Configure the network devices to use TACACS+ for device administration and specify Cisco ISE as the TACACS+ server and

the proxy as the RADIUS server. The configuration commands may vary depending on the device type and model, but the general syntax is as follows: aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local aaa accounting exec default start-stop group tacacs+ tacacs server ISE
address ipv4 <ISE IP address>
key <ISE shared secret>
radius server DUO
address ipv4 <proxy IP address> auth-port <proxy port> key <proxy shared secret>
Test the solution by logging into the network devices using Active Directory credentials. The user should receive a Cisco DUO prompt for the second factor authentication, such as a push notification, a phone call, or a passcode. After approving the second factor authentication, the user should be granted access to the device with the appropriate privileges based on the TACACS profile and the Active Directory attributes.
Reference := 1: Duo MFA Integration with ISE for TACACS+ Device Administration with Microsoft Active Directory Users - Cisco Community 2: Protecting Access to Network devices with ISE TACACS+ and DUO MFA - Cisco Community

Question: 341

[Endpoint Protection and Detection]
A Cisco AMP for Endpoints administrator configures a custom detection policy to add specific MD5 signatures The configuration is created in the simple detection policy section, but it does not work What is the reason for this failure?

A. The administrator must upload the file instead of the hash for Cisco AMP to use.
B. The MD5 hash uploaded to the simple detection policy is in the incorrect format
C. The APK must be uploaded for the application that the detection is intended
D. Detections for MD5 signatures must be configured in the advanced custom detection policies

Answer: D

Explanation:
The reason for the failure is that detections for MD5 signatures must be configured in the advanced custom detection policies, not in the simple detection policy section. The simple detection policy section allows users to create a list of SHA-256 hashes of files that they want to block or quarantine on the endpoints. The SHA-256 hash is a more secure and unique identifier of a file than the MD5 hash, which can have collisions or duplicates. The advanced custom detection policy section allows users to create more complex and flexible rules to detect and block files based on various criteria, such as file name, size, type, signature, or MD5 hash. The advanced custom detection policy section also supports wildcards and regular expressions to match multiple files or patterns. Therefore, if the administrator wants to add specific MD5 signatures to the custom detection policy, they should use the advanced custom detection policy section instead of the simple detection policy section. Reference:
Configure a Simple Custom Detection List on the AMP for Endpoints Portal - Cisco, Step 4: On the Add SHA-256 option, paste the SHA-256 code previously collected from the specific file you want to block, as shown in the image.
Create an Advanced Custom Detection List in Cisco Secure Endpoint - Cisco, Step 3: Next, Edit that new Signature Set, and Add Signature.
Win.Exploit.CVE_2020_0601:1::06072A8648CE3D02010606072A8648CE3D020130.

Question: 342

[Endpoint Protection and Detection]

An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?

A. Platform as a Service because the customer manages the operating system
B. Infrastructure as a Service because the customer manages the operating system
C. Platform as a Service because the service provider manages the operating system
D. Infrastructure as a Service because the service provider manages the operating system

Answer: C

Explanation:

Platform as a Service (PaaS) is a cloud service model that delivers and manages all the hardware and software resources to develop applications through the cloud. The service provider is responsible for the infrastructure, middleware, runtime, and operating system, while the customer only has to focus on the application and data. PaaS enables the customer to avoid the hassle of patching, updating, or maintaining the operating system, as well as the underlying hardware and network12. Infrastructure as a Service (IaaS) is a cloud service model that delivers on-demand infrastructure resources, such as compute, storage, networking, and virtualization, to the customer via the cloud. The service provider hosts and manages the infrastructure, but the customer is responsible for the operating system, middleware, virtual machines, and any apps or data. IaaS requires the customer to handle the patch management of the operating system, as well as the security and configuration of the virtual machines34. Reference := 1: Use platform as a service (PaaS) options - Azure Architecture Center 2:

What is Platform-as-a-Service (PaaS)? - Cloudflare 3: PaaS vs IaaS vs SaaS: What's the difference? | Google Cloud 4: SaaS vs PaaS vs IaaS: What's The Difference & How To Choose – BMC Software | Blogs

Question: 343

[Secure Network Access, Visibility, and Enforcement]

An administrator is adding a new Cisco ISE node to an existing deployment. What must be done to ensure that the addition of the node will be successful when inputting the FQDN?

A. Change the IP address of the new Cisco ISE node to the same network as the others.
B. Make the new Cisco ISE node a secondary PAN before registering it with the primary.
C. Open port 8905 on the firewall between the Cisco ISE nodes
D. Add the DNS entry for the new Cisco ISE node into the DNS server

Answer: D

Explanation:

Add the DNS entry for the new Cisco ISE node into the DNS server. This is because the fully qualified domain name (FQDN) of the new Cisco ISE node, for example, ise1.cisco.com, must be DNS- resolvable from the primary Administration ISE node. Otherwise, node registration will fail. The DNS server must contain the IP addresses and FQDNs of the ISE nodes that are part of the distributed deployment1.

The other options are incorrect because:

Changing the IP address of the new Cisco ISE node to the same network as the others is not necessary, as long as the nodes can communicate with each other over the network.

Making the new Cisco ISE node a secondary PAN before registering it with the primary is not possible, as the node must be registered first before changing its persona or role.

Opening port 8905 on the firewall between the Cisco ISE nodes is not required, as this port is used for communication between the primary and secondary Monitoring ISE nodes, not for node registration.

Reference:

Setting Up Cisco ISE in a Distributed Environment

ISE node registering after change domain-name

FQDN IN ISE

Question: 344

[Security Concepts] Refer to the exhibit.

```
interface GigabitEthernet1/0/18
 description ISE dot1x Port
 switchport access vlan 41
 switchport mode access
 switchport voice vlan 44
 device-tracking attach-policy IPDT_MAX_10
 authentication periodic
 authentication timer reauthenticate server
 access-session host-mode multi-domain
 access-session port-control auto
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 spanning-tree portfast
 service-policy type control subscriber POLICY_Gi1/0/18
```

What will occur when this device tries to connect to the port?

A. 802.1X will not work, but MAB will start and allow the device on the network.
B. 802.1X will not work and the device will not be allowed network access
C. 802 1X will work and the device will be allowed on the network
D. 802 1X and MAB will both be used and ISE can use policy to determine the access level

Answer: D

Explanation:

Based on the configuration script in the image, the interface GigabitEthernet0/0/18 is configured for both 802.1X and MAB authentication. The command authentication port-control auto enables 802.1X authentication on the port, while the command dot1x pae authenticator enables the port to act as an authenticator. The command authentication host-mode multi-domain enables MAB authentication on the port, and allows two devices to be authenticated, one in the voice VLAN and one in the data VLAN. Therefore, when a device tries to connect to the port, the switch will first attempt 802.1X authentication, and if it fails, it will fall back to MAB authentication using the device's MAC address. The switch will then contact the ISE server, which is configured as the RADIUS server group ise-group, to verify the device's credentials and assign the appropriate access level based on the ISE policy. The ISE policy can also dynamically assign VLANs, ACLs, or service policies to the device based on its identity and posture. Reference :=
Some possible references are:

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 6: Secure Connectivity, Lesson 6.2: Implementing Site-to-Site VPNs, Topic 6.2.2: Group Encrypted Transport VPN

Cisco IOS Security Configuration Guide, Release 15M&T - Configuring IEEE 802.1x Port-Based Authentication
Cisco IOS Security Configuration Guide, Release 15M&T - Configuring MAC Authentication Bypass
Cisco Identity Services Engine Administrator Guide, Release 2.7 - Configure Wired 802.1X and MAB

Question: 345

[Content Security]
A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access The Cisco ESA must also join a cluster machine using preshared keys What must be configured to meet these requirements?

A. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA CLI.
B. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA GUI
C. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA GUI.
D. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA CLI

Answer: A

Explanation:

Two-factor authentication is a security feature that requires users to provide two forms of information before gaining access to the Cisco ESA. The two factors are usually something the user knows, such as a password, and something the user has, such as a token or a code. Two-factor authentication can be enabled for specific user roles on the Cisco ESA through a RADIUS server, which is an external authentication server that supports the Remote Authentication Dial-In User Service (RADIUS) protocol. The RADIUS server can generate and validate the second factor for the users, such as

a one-time password (OTP) or a time-based one-time password (TOTP). To enable two- factor authentication through a RADIUS server, the network engineer must configure the RADIUS server settings on the Cisco ESA, and assign the user roles that require two-factor authentication to use the RADIUS server as the authentication source. This can be done on the System Administration > Users page in the web interface, or by using the userconfig command in the CLI12.
A cluster is a group of Cisco ESAs that share the same configuration information and can be managed centrally. A cluster can provide increased reliability, flexibility, and scalability for the email security system. To join a cluster, a Cisco ESA must have the same AsyncOS version as the other cluster members, and must use a pre-shared key to authenticate with the cluster leader. The pre-shared key is a secret passphrase that is configured on the cluster leader and must be entered on the joining appliance. To join a cluster by using the Cisco ESA CLI, the network engineer must use the clusterconfig command, which allows the engineer to create a new cluster, join an existing cluster, or leave a cluster. The clusterconfig command also allows the engineer to specify the communication

port and the hostname or IP address of the cluster leader. If the Cisco ESA has enabled two-factor authentication, the network engineer must also use the clusterconfig > prepjoin command to configure the pre-shared key before joining the cluster34.
Therefore, option A is the correct answer, and the other options are incorrect. Option B is incorrect because the cluster configuration options must be done via the CLI on the Cisco ESA and cannot be created or joined in the GUI. Option C is incorrect because the Cisco ESA does not support TACACS+ as an external authentication source, only LDAP and RADIUS. Option D is incorrect because it also uses TACACS+, which is not supported by the Cisco ESA. Reference := User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) - Distributing Administrative Tasks
User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) - External Authentication
Configure an Email Security Appliance (ESA) Cluster
User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) - Centralized Management

Question: 346

[Endpoint Protection and Detection]
Which portion of the network do EPP solutions solely focus on and EDR solutions do not?

A. server farm
B. perimeter
C. core
D. East-West gateways

Answer: B

Explanation:

EPP solutions solely focus on the perimeter of the network, which is the boundary between the internal and external networks. The perimeter is where most of the endpoints, such as laptops, desktops, mobile devices, and IoT devices, are located and connected to the network. EPP solutions aim to prevent, detect, and remediate security threats on these endpoints by using technologies such as antivirus, data encryption, and data loss prevention. EPP solutions rely on signatures and other indicators of intrusion by known threats to block malicious activity and malware on the endpoints12.
EDR solutions do not focus on the perimeter, but rather on the entire network, including the core and the East-West

gateways. The core is the central part of the network that connects different segments and provides high-speed data transmission. The East-West gateways are the points of communication between different segments within the network, such as between different data centers or cloud environments. EDR solutions provide continuous and comprehensive visibility into endpoint activities across the network by using threat hunting tools for behavior-based endpoint threat detection. EDR solutions monitor and record endpoint data, detect anomalies and malicious behavior, and respond to threats that EPP and other security tools did not catch. EDR solutions also

enable security teams to proactively investigate and contain incidents by using incident data search, alert triage, threat validation, and malicious activity blocking134.

Reference := 1: EPP vs. EDR: Why You Need Both - CrowdStrike 2: Comparing endpoint security: EPP vs. EDR vs. XDR | Infosec 3: EDR vs EPP: What is the Difference? - Exabeam 4: EDR vs EPP: Key Features, Differences, and How They Work Together

Question: 347

[Network Security] Refer to the exhibit.

```
crypto ikev2 name-mangier MANGLER dn
  organization-unit
```

An engineer is implementing a certificate based VPN. What is the result of the existing configuration?

A. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.
B. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully
C. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER
D. The OU of the IKEv2 peer certificate is set to MANGLER

Answer: B

Explanation:

The configuration snippet in the image is a part of IKEv2 configuration where the name mangler is associated with the organizational unit (OU) “MANGLER”. In Cisco’s IKEv2 implementation, this specific configuration means that only an IKEv2 peer whose certificate has an OU attribute set to “MANGLER” can establish an IKEv2 Security Association successfully. This is a method of ensuring that only peers with certificates issued to a specific organizational unit can connect, enhancing security by limiting unauthorized access. The name mangler is a feature that allows the administrator to specify a string that must be present in the peer’s certificate for authentication. The name mangler can be applied to any certificate field, such as common name (CN), organization (O), or OU. The name mangler can also be used to modify the peer’s identity based on the certificate field, such as appending or prepending a string to the identity. The name mangler is configured under the IKEv2 profile using the command crypto ikev2 profile profile-name identity name-mangler name-mangler- name dn field-name. In this case, the name mangler is applied to the OU field of the peer’s certificate. The other options are incorrect because they do not describe the effect of the name mangler configuration. Option A is incorrect because the name mangler does not affect the identity matching for the IKEv2 authorization policy. The identity matching is based on

the peer's identity

type and value, which can be different from the certificate field. Option C is incorrect because the name mangler does not encrypt the OU field of the peer's certificate. The OU field is part of the certificate's subject, which is not encrypted in the IKEv2 messages. Option D is incorrect because the name mangler does not set the OU field of the peer's certificate. The OU field is determined by the certificate authority (CA) that issues the certificate, and the name mangler only verifies or modifies the peer's identity based on the OU field. Reference : Configuring Internet Key Exchange Version 2, Internet Key Exchange Version 2 CLI Constructs, Tutorial: Setting up a certificate-based IKEv2 VPN connection (RSA)

Question: 348

[Content Security]
What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

A. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not
B. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.
C. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA
D. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA

Answer: A

Explanation:

Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not. Cisco CWS is a cloud-based web security service that provides comprehensive protection against web-based threats for users anywhere, on any device1. Cisco WSA is an onpremises web security appliance that provides web filtering, malware scanning, data loss prevention, and other features for users within the network perimeter2. One of the benefits of using Cisco CWS over Cisco WSA is that it eliminates the need to backhaul traffic through headquarters for remote workers, which can reduce bandwidth costs, latency, and complexity3. Remote workers can connect directly to the nearest Cisco CWS data center and receive the same level of web security as if they were in the office. Cisco WSA, on the other hand, requires remote workers to use a VPN or proxy to route their web traffic through the headquarters, which can affect their performance and user experience. Reference:
1: Cisco Cloud Web Security Data Sheet
2: Cisco Secure Web Appliance Data Sheet
3: Cisco Cloud Web Security: Comprehensive Defense, Advanced Threat Protection, and Superior Flexibility for Your Business
: Cisco Cloud Web Security: How It Works
: Cisco Cloud Web Security: FAQ

Question: 349

[Security Concepts]
What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?

A. trusted automated exchange
B. Indicators of Compromise
C. The Exploit Database
D. threat intelligence

Answer: D

Explanation:

Threat intelligence is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems. Threat intelligence is the result of collecting, analyzing, and contextualizing data from various sources, such as network traffic, logs, feeds, reports, etc. Threat intelligence provides insights into the tactics, techniques, and procedures (TTPs) of adversaries, as well as their motivations, intentions, and capabilities. Threat intelligence can help organizations to detect, prevent, and respond to cyberattacks, as well as to improve their security posture and resilience12. The other options are not correct, because they are not terms for having information about threats and threat actors. Trusted automated exchange is a concept that refers to the sharing of threat intelligence among trusted entities in a timely and secure manner3. Indicators of Compromise (IoCs) are pieces of forensic data, such as IP addresses, domains, hashes, etc., that indicate a potential intrusion or compromise of a system or network. The Exploit Database is a public repository of exploits and vulnerable software, maintained by Offensive Security.

Reference:

1: What is Cyber Threat Intelligence? - Cisco
2: Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
3: Trusted Automated Exchange of Intelligence Information (TAXII™) Version 2.0
[4] : What Are Indicators of Compromise (IOCs)? - Cisco
[5] : The Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers

Question: 350

[Security Concepts]
An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services They want to use this information for behavior analytics and statistics Which two actions must be taken to implement this requirement? (Choose two.)

A. Configure Cisco ACI to ingest AWS information.
B. Configure Cisco Thousand Eyes to ingest AWS information.
C. Send syslog from AWS to Cisco Stealthwatch Cloud.
D. Send VPC Flow Logs to Cisco Stealthwatch Cloud.
E. Configure Cisco Stealthwatch Cloud to ingest AWS information

Answer: D,E

Explanation:

To collect full metadata information about the traffic going through their AWS cloud services, the organization needs to send VPC Flow Logs to Cisco Stealthwatch Cloud and configure Cisco Stealthwatch Cloud to ingest AWS information. VPC Flow Logs is a feature that enables the organization to capture information about the IP traffic going to and from network interfaces in their VPC. Flow log data can be published to Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose1. Cisco Stealthwatch Cloud is a SaaS-based network and cloud security solution that provides behavioral analytics across the network to help the organization improve threat detection and achieve a stronger security posture2. By sending VPC Flow Logs to Cisco Stealthwatch Cloud, the organization can leverage the rich network flow metadata to perform various types of flow analysis, such as troubleshooting connectivity issues, monitoring the traffic patterns, detecting anomalous or malicious activity, and verifying compliance3. To send VPC Flow Logs to Cisco Stealthwatch Cloud, the organization needs to create a flow log for their VPC, subnet, or network interface, and specify Cisco Stealthwatch Cloud as the destination4. To configure Cisco Stealthwatch Cloud to ingest AWS information, the organization needs to add their AWS account as a data source in the Cisco Stealthwatch Cloud portal, and grant the necessary permissions for Cisco Stealthwatch Cloud to access their VPC Flow Logs5. By doing so, the organization can view and analyze the flow log data in the Cisco Stealthwatch Cloud dashboard, and receive valuable security alerts and insights based on the network behavior6.

Reference := 1: Logging IP traffic using VPC Flow Logs - Amazon Virtual Private Cloud 2: Cisco Secure Cloud Analytics (Stealthwatch Cloud) - Cisco 3: Cisco Secure Cloud Analytics - AWS VPC Flow Logs: A New Tool for Your … 4: Publish flow logs to Cisco Stealthwatch Cloud - Amazon Virtual Private Cloud 5: AWS Data Source Setup - Cisco Stealthwatch Cloud 6: AWS Workload Protection - Cisco Stealthwatch Cloud

Question: 351

[Network Security]

What is the function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?

A. It defines what data is going to be encrypted via the VPN
B. It configures the pre-shared authentication key
C. It prevents all IP addresses from connecting to the VPN server.
D. It configures the local address for the VPN server.

Answer: B

Explanation:

The function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel is to configure the pre-shared authentication key. This command specifies the key that will be used to authenticate the Internet Key Exchange (IKE) phase 1 negotiation between the IPsec peers. The key is associated with the address 0.0.0.0 0.0.0.0, which means that it will apply to any peer that initiates or responds to the IKE negotiation. This is a common configuration for dynamic IPsec VPN scenarios, such as Dynamic Multipoint VPN (DMVPN) or Easy VPN, where the IP addresses of the peers are not known in advance. However, this is also a less secure configuration, as it exposes the VPN server to potential brute-force attacks from any source. A more secure configuration would be to specify the exact IP address or subnet of the peer, or to use certificates instead of pre-shared keys.

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Securing the Cloud, Lesson 2: Site-to-Site VPNs, Topic: IPsec VPN Configuration

Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4 - Configuring Internet Key Exchange for

IPsec VPNs
[Support] - Cisco, Configuring IKE Policies, Step 3: crypto isakmp key keystring [address | hostname] [mask | no-xauth] [netmask mask]

Question: 352

[Security Concepts]
An organization wants to improve its cybersecurity processes and to add intelligence to its data The organization wants to utilize the most current intelligence data for URL filtering, reputations, and vulnerability information that can be integrated with the Cisco FTD and Cisco WSA What must be done to accomplish these objectives?

A. Create a Cisco pxGrid connection to NIST to import this information into the security products for policy use
B. Create an automated download of the Internet Storm Center intelligence feed into the Cisco FTD and Cisco WSA databases to tie to the dynamic access control policies.
C. Download the threat intelligence feed from the IETF and import it into the Cisco FTD and Cisco WSA databases
D. Configure the integrations with Talos Intelligence to take advantage of the threat intelligence that it provides.

Answer: D

Explanation:

Talos Intelligence is a comprehensive threat intelligence service that provides up-to-date information on URL filtering, reputations, and vulnerability information. Talos Intelligence can be integrated with Cisco FTD and Cisco WSA to enhance the security and visibility of the network. Cisco FTD and Cisco WSA can leverage the Talos Intelligence feeds to perform Security Intelligence filtering, which allows the devices to block or allow traffic based on the reputation of the source or destination IP addresses, URLs, or DNS requests. Talos Intelligence feeds are updated regularly and can be configured to download automatically or manually on the FTD and WSA devices12345. Reference := 1: Cisco Talos Intelligence Group - Comprehensive Threat Intelligence 2: Threat Intelligence on Cisco Stealthwatch - Cisco Community 3: Third-Party Integration of Security Feeds with FMC (Cisco Threat … - Cisco Community 4: Cisco Firepower Threat Defense Configuration Guide for Firepower Device … 5: Cisco Firepower Threat Defense Configuration Guide for Firepower Device ...

Question: 353

[Secure Network Access, Visibility, and Enforcement] Refer to the exhibit.

```
ntp anthentlcat ion-key 10 tl5 ciseals 3
dtp trnjted-key 10
```

A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced What is the cause of this issue?

A. The key was configured in plain text.
B. NTP authentication is not enabled.
C. The hashing algorithm that was used was MD5. which is unsupported.

D. The router was not rebooted after the NTP configuration updated.

Answer: B

Explanation:

The cause of this issue is that NTP authentication is not enabled on the router. The commands shown in the exhibit only define the authentication key and mark it as trusted, but they do not enable NTP authentication globally or on a per-peer basis. To enable NTP authentication globally, the command ntp authenticate must be used. To enable NTP authentication on a per-peer basis, the command ntp server ip-address key key-id or ntp peer ip-address key key-id must be used, where key-id is the same as the one defined by the ntp authentication-key command. Without enabling NTP authentication, any device can synchronize time with this router, regardless of whether it has the same authentication key or not.

The other options are incorrect because:

The key was configured in plain text, but this is not the cause of the issue. Although it is recommended to use the ntp authentication-key key-id md5 key [encrypted] command to encrypt the key, using plain text does not prevent NTP authentication from working, as long as the same key is configured on both the router and the peer.

The hashing algorithm that was used was MD5, which is supported by NTP. MD5 is the default algorithm for NTP authentication and it can be used with any key length from 1 to 16 characters. Other algorithms, such as SHA and SHA1, are also supported by NTP if the OpenSSL library is installed, but they are not required for NTP authentication to work.

The router was not rebooted after the NTP configuration updated, but this is not necessary for NTP authentication to take effect. NTP authentication is applied immediately after the configuration commands are entered, and no reboot is required.

Reference:

Configuring NTP

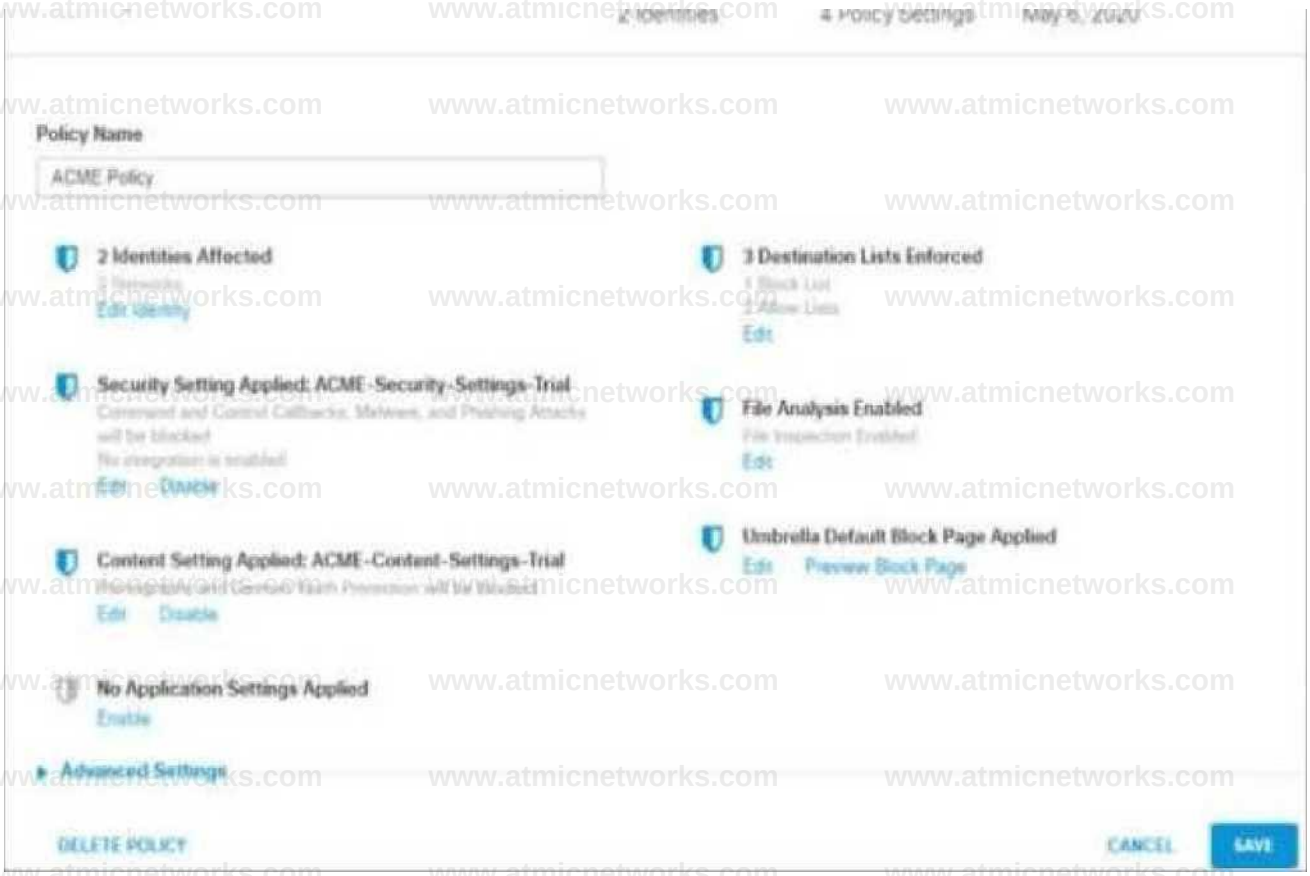
Authentication Support

NTP Authentication Explained

Question: 354

[Security Concepts]

Refer to the exhibit.



How does Cisco Umbrella manage traffic that is directed toward risky domains?

A. Traffic is proximed through the intelligent proxy.
B. Traffic is managed by the security settings and blocked.
C. Traffic is managed by the application settings, unhandled and allowed.
D. Traffic is allowed but logged.

Answer: A

Explanation:

Cisco Umbrella is a cloud-delivered and SaaS-based solution that provides DNS-layer security and web filtering for internet traffic. It blocks requests to malicious domains or IPs before a connection is even established, and logs and inspects all web traffic for greater transparency, control, and protection1.

However, not all domains or IPs are clearly malicious or benign. Some of them may be risky, meaning that they host both legitimate and malicious content, or that they have a low reputation score based on various factors. For these domains or IPs, Cisco Umbrella offers the option to proxy the traffic through the intelligent proxy, which is a selective web proxy that performs deeper inspection and analysis of the web content2.

The intelligent proxy can apply URL filtering, file inspection, and file type control to the proxied traffic, and block or allow it based on the policy settings. The intelligent proxy can also leverage Cisco Advanced Malware Protection (AMP) and antivirus engines to scan files for malware and threats3. Therefore, by using the intelligent proxy, Cisco Umbrella can manage traffic that is directed toward risky domains more effectively, and provide an additional layer of security and visibility for the organization.

Reference :=
Manage the Intelligent Proxy
Manage File Inspection

www.atmicnetworks.com

Cisco Umbrella At a Glance

Question: 355

[Security Concepts]

An engineer needs to add protection for data in transit and have headers in the email message Which configuration is needed to accomplish this goal?

A. Provision the email appliance
B. Deploy an encryption appliance.
C. Map sender !P addresses to a host interface.
D. Enable flagged message handling

Answer: B

Explanation:

The configuration that is needed to accomplish the goal of adding protection for data in transit and having headers in the email message is to deploy an encryption appliance. An encryption appliance is a device that encrypts and decrypts email messages using various encryption standards, such as S/MIME, PGP, or Cisco Registered Envelope Service (CRES). An encryption appliance can also add headers to the email message to indicate the encryption status, the encryption key, or the encryption policy. An encryption appliance can be integrated with an email appliance, such as Cisco Email Security Appliance (ESA), to provide end-to-end email security and encryption.

The other options are incorrect because:

Provisioning the email appliance is not enough to add protection for data in transit and have headers in the email message. An email appliance can provide various email security features, such as spam filtering, virus scanning, content filtering, or data loss prevention, but it does not encrypt or decrypt email messages by itself. An email appliance needs to work with an encryption appliance to provide email encryption and decryption.

Mapping sender IP addresses to a host interface is not related to adding protection for data in transit and having headers in the email message. This is a configuration option for an email appliance that allows it to accept email messages from specific IP addresses or ranges and assign them to a specific host interface. This can be useful for load balancing, traffic management, or policy enforcement, but it does not affect email encryption or decryption.

Enabling flagged message handling is not relevant to adding protection for data in transit and having headers in the email message. This is a configuration option for an email appliance that allows it to handle email messages that have a specific flag or tag in the subject line or the body. This can be useful for testing, troubleshooting, or applying special policies, but it does not affect email encryption or decryption.

Reference:

Cisco Email Encryption

Cisco Email Encryption Appliance

Cisco Email Security Appliance Configuration Guide

Question: 356

[Security Concepts]
How does a cloud access security broker function?

A. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution
B. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution
C. It acts as a security information and event management solution and receives syslog from other cloud solutions.
D. It scans other cloud solutions being used within the network and identifies vulnerabilities

Answer: B

Explanation:

A cloud access security broker (CASB) is a security solution that helps protect cloud-hosted services and applications from cyberattacks and data breaches. A CASB acts as an intermediary between cloud users and cloud providers, and enforces the organization's security policies and compliance requirements. A CASB integrates with other cloud solutions via APIs and monitors the cloud activity and data across multiple platforms and devices. A CASB can also create incidents based on events from the cloud solution, such as unauthorized access, data leakage, malware infection, or policy violation. A CASB can then alert the administrators, block the malicious actions, or remediate the issues. A CASB provides visibility, control, and protection for the organization's cloud environment12. Reference :=
What Is a Cloud Access Security Broker (CASB)? | Microsoft
What is a CASB Cloud Access Security Broker? - CrowdStrike

Question: 357

[Secure Network Access, Visibility, and Enforcement]
An engineer integrates Cisco FMC and Cisco ISE using pxGrid Which role is assigned for Cisco FMC?

A. client
B. server
C. controller
D. publisher

Answer: A

Explanation:

Cisco FMC is assigned the role of a client in the pxGrid ecosystem. A client is a partner that subscribes to the contextual data published by other partners or by ISE. A client can also publish its own data, but it does not have to. A client can use the contextual data to enforce security policies, perform threat analysis, or provide visibility. Cisco FMC can subscribe to various topics from ISE or other partners, such as user identity, session directory, endpoint profile, SGT

mapping, threat events, or vulnerability assessment. Cisco FMC can also publish its own threat events to ISE or other partners. Cisco FMC can use the contextual data to apply access control rules, correlation policies, or network discovery policies based on the attributes of the users, endpoints, or sessions12.

The other options are not correct because they are not the roles assigned for Cisco FMC. A server is a partner that publishes contextual data to other partners or to ISE. A server can also subscribe to data, but it does not have to. A server can provide valuable information about the network, such as device inventory, configuration, or compliance. An example of a server is Cisco Prime Infrastructure3. A controller is the core component of the pxGrid ecosystem that manages the communication, authentication, and authorization between the partners. The controller is always ISE, and it is responsible for creating and maintaining the pxGrid domain, distributing the certificates, and

facilitating the data exchange4. A publisher is a partner that publishes contextual data to other partners or to ISE, but does not subscribe to any data. A publisher can provide useful information about the network, such as security events, alerts, or incidents. An example of a publisher is Cisco Stealthwatch. Reference :=

Integrate FMC with ISE using pxGrid | Blue Network Security

How To: Integrate Firepower Management Center (FMC) 6 … - Cisco Community

Cisco Prime Infrastructure and ISE pxGrid Integration - Cisco

pxGrid Overview - Cisco

[Cisco Stealthwatch and ISE pxGrid Integration - Cisco]

Question: 358

[Security Concepts]

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https://<FMC IP>/capure/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

A. Disable the proxy setting on the browser
B. Disable the HTTPS server and use HTTP instead
C. Use the Cisco FTD IP address as the proxy server setting on the browser
D. Enable the HTTPS server for the device platform policy

Answer: D

Explanation:

The error 403: Forbidden indicates that the web server denied access to the requested resource, which in this case is the PCAP file. One possible reason for this error is that the HTTPS server is not enabled for the device platform policy, which is a configuration that applies to the FTD devices managed by the FMC. The device platform policy defines the settings for the management interface, the SSH access, the SNMP, the NTP, the DNS, and the HTTPS server. The HTTPS server allows the FMC to access the FTD devices via HTTPS and perform tasks such as packet capture, packet tracer, and file transfer. If the HTTPS server is not enabled for the device platform policy, the FMC cannot access the PCAP file from the FTD device via HTTPS. Therefore, the engineer must enable the HTTPS server for the device platform policy in order to

resolve this issue. To enable the HTTPS server for the device platform policy, the engineer must follow these steps:

Log in to the FMC web interface and navigate to Devices > Platform Settings.

Select the device platform policy that applies to the FTD device and click Edit. In the General tab, check the Enable HTTPS Server checkbox and click Save. Deploy the policy changes to the FTD device and wait for the deployment to complete. Try to access the PCAP file again from the FMC web browser using the same address.

Alternatively, the engineer can also enable the HTTPS server for the FTD device from the FTD CLI

using the command configure network https-server enable. However, this method is not recommended because it may cause a configuration conflict with the FMC123

Reference := 1: Use Firepower Threat Defense Captures and Packet Tracer - Cisco 2: Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.6 - Device Management Basics

[Cisco Firepower NGFW] - Cisco 3: Cisco Firepower Threat Defense Command Reference - C through D Commands

[Cisco Firepower NGFW] - Cisco

Question: 359

[Security Concepts]

What is a description of microsegmentation?

A. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate

B. Environments deploy a container orchestration platform, such as Kubernetes, to manage the application delivery

C. Environments implement private VLAN segmentation to group servers with similar applications.

D. Environments deploy centrally managed host-based firewall rules on each server or container

Answer: A

Explanation:

Microsegmentation is a network security technique that enables security architects to logically divide the data center or cloud environment into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment. Microsegmentation software with network virtualization technology is used to create zones in cloud deployments. These granular secure zones isolate workloads, securing them individually with custom, workload-specific policies. Microsegmentation uses a zero-trust model, which means that no traffic is allowed by default, and only explicitly authorized traffic is permitted based on the principle of least privilege. Microsegmentation helps to reduce the attack surface, prevent the lateral movement of threats, and strengthen regulatory compliance. The other options are incorrect because they do not describe microsegmentation accurately. Option B is incorrect because container orchestration platforms, such as Kubernetes, are used to automate the deployment, scaling, and management of containerized applications, but they do not provide microsegmentation by themselves. Option C is incorrect because private VLAN segmentation is a network security technique that isolates hosts within the same VLAN, but it does not provide granular security controls at the workload level. Option D is incorrect because host-based firewall rules are one of the components of microsegmentation, but they are not sufficient to implement microsegmentation without network virtualization and policy automation. Reference : What Is Microsegmentation? - Palo Alto Networks, What Is Micro-

Segmentation? - Cisco, What is Micro-Segmentation? | VMware Glossary

Question: 360

[Securing the Cloud]
What must be enabled to secure SaaS-based applications?

A. modular policy framework
B. two-factor authentication
C. application security gateway
D. end-to-end encryption

Answer: B

Explanation:

two-factor authentication. Two-factor authentication (2FA) is a security measure that requires users to provide two pieces of evidence to verify their identity before accessing SaaS-based applications1. These pieces of evidence can be something the user knows (such as a password or a PIN), something the user has (such as a smartphone or a token), or something the user is (such as a fingerprint or a face scan)1. 2FA enhances the security of SaaS-based applications by making it harder for attackers to compromise login credentials and gain unauthorized access to sensitive data and resources2. The other options are not correct because they are not sufficient to secure SaaS-based applications. Modular policy framework (MPF) is a feature of Cisco ASA that allows administrators to create and apply security policies to traffic flows3. However, MPF alone cannot protect SaaS-based applications from web-based threats or data breaches. Application security gateway (ASG) is a device that provides firewall, intrusion prevention, and content filtering services for web applications4. However, ASG cannot prevent credential theft or account takeover attacks that target SaaS-based applications. End-to-end encryption (E2EE) is a method of encrypting data in transit and at rest, so that only the sender and the receiver can decrypt it. However, E2EE cannot prevent unauthorized access to SaaS-based applications if the encryption keys are compromised or stolen. Reference: 1: What is Two-Factor Authentication (2FA)?
2: How to Secure Your SaaS Applications
3: Modular Policy Framework Overview
4: What is an Application Security Gateway? : What is End-to-End Encryption?

Question: 361

[Content Security]
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.

A. Create NTLM or Kerberos authentication realm and enable transparent user identification B. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
C. Create an LDAP authentication realm and disable transparent user identification.
D. Deploy a separate eDirectory server: the client IP address is recorded in this server

Answer: A,B

Explanation:

Transparently identify users with authentication realms – This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers: Active Directory – Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory. LDAP – Create an LDAP authentication realm configured as an eDirectory, and enable transparent user identification. For more information, see Transparent User Identification with LDAP.

Details:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01001.html#:~:text=Transparently%20identify%20users%20with%20authentication,User%20Identification%20with%20LDAP.

Question: 362

[Security Concepts]
Which method of attack is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code?

A. buffer overflow
B. browser WGET
C. SQL injection
D. cross-site scripting

Answer: D

Explanation:

Cross-site scripting (XSS) is the method of attack that is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code. XSS is a type of injection attack that exploits the lack of input validation or output encoding

in a web application. An attacker can craft a malicious script and embed it in a web page or a URL that is sent to the user. When the user visits the web page or clicks the URL, the script is executed by the user's browser, which may not be able to distinguish it from legitimate code. The script can then perform various actions, such as stealing cookies, session tokens, or other sensitive information, redirecting the user to a malicious site, or performing actions on behalf of the user12. The other options are not correct, because they are not methods of attack that use web applications to execute malicious code on the user's browser. Buffer overflow is a type of attack that exploits a memory vulnerability in a program or system, where an attacker can overwrite the memory beyond the allocated buffer and execute arbitrary code3. Browser WGET is a command-line tool that can be used to download files from the web, but it is not an attack method by itself4.

SQL injection is a type of attack that exploits a database vulnerability in a web application, where an attacker can inject malicious SQL statements into a user input field and execute them on the database server5. Reference:

1: What is Cross-Site Scripting (XSS)? - Cisco
2: Cross-Site Scripting (XSS) - OWASP
3: What is a Buffer Overflow? - Cisco
4: GNU Wget 1.21.1 Manual
5: What is SQL Injection (SQLi)? - Cisco

Question: 363

[Security Concepts]

An administrator enables Cisco Threat Intelligence Director on a Cisco FMC. Which process uses STIX and allows uploads and downloads of block lists?

A. consumption
B. sharing
C. editing
D. authoring

Answer: B

Explanation:

The process that uses STIX and allows uploads and downloads of block lists is sharing. STIX (Structured Threat Information Expression) is a standard language and format for exchanging cyber threat intelligence data. Block lists are collections of observables, such as IP addresses, URLs, or domains, that are associated with malicious activity and can be used to block or monitor network traffic. Cisco Threat Intelligence Director (TID) is a feature that operationalizes threat intelligence data by consuming, normalizing, publishing, and correlating data from various sources, including third-party STIX feeds. TID enables the administrator to upload STIX files from local or remote sources, or download STIX files from the Firepower Management Center (FMC) to share with other systems. TID also allows the administrator to configure actions (such as block or monitor) based on the indicators and observables in the STIX files, and generate incidents and observations when the system detects traffic that matches the threat intelligence data123

Reference := 1: Firepower Management Center Configuration Guide, Version 6.2.3 - Threat Intelligence Director 2 2: Introduction to STIX - GitHub Pages 4 3: Third-Party Integration of Security Feeds with FMC (Cisco Threat Intelligence Director) - Cisco Community 3

Question: 364

[Security Concepts]

Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

A. OpenC2
B. OpenIOC
C. CybOX
D. STIX

Answer: D

Explanation:

The open standard that creates a framework for sharing threat intelligence in a machine-digestible format is STIX (Structured Threat Information Expression). STIX is a language and serialization format that enables the exchange of cyber threat information across organizations, tools, and platforms. STIX defines a common vocabulary and data model for representing various types of threat intelligence, such as indicators, observables, incidents, campaigns, threat actors, courses of action, and more. STIX also supports the expression of context, relationships, confidence, and handling of the threat information. STIX aims to improve the speed, accuracy, and efficiency of threat detection, analysis, and response.

STIX is often used in conjunction with TAXII (Trusted Automated Exchange of Indicator Information), which is a protocol and transport mechanism that enables the secure and automated communication of STIX data. TAXII defines how to request, send, receive, and store STIX data using standard methods and formats, such as HTTPS, JSON, and XML. TAXII supports various exchange models, such as hub- and-spoke, peer-to-peer, or subscription-based. TAXII enables the interoperability and scalability of threat intelligence sharing among different systems and organizations.

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Malware Threats, Lesson 3: Identifying Advanced Threats, Topic: Threat Intelligence Sharing What is STIX/TAXII? | Cloudflare

STIX 2.1 Specification Documents

Question: 365

[Security Concepts]

What are two functionalities of SDN Northbound APIs? (Choose two.)

A. Northbound APIs provide a programmable interface for applications to dynamically configure the network.
B. Northbound APIs form the interface between the SDN controller and business applications.
C. OpenFlow is a standardized northbound API protocol.
D. Northbound APIs use the NETCONF protocol to communicate with applications.
E. Northbound APIs form the interface between the SDN controller and the network switches or routers.

Answer: A,B

Explanation:

Northbound APIs are the link between the applications and the SDN controller. The applications can tell the network what they need (data, storage, bandwidth, and so on) and the network can deliver those resources, or communicate what it has.

www.atmicnetworks.com

These APIs support a wide variety of applications, such as load balancers, firewalls, orchestration platforms, and automation stacks. Northbound APIs also enable the applications to use the controller's capabilities to program flows into the network devices using the southbound interface. Northbound APIs are usually RESTful APIs that use HTTP methods to exchange data in JSON or XML formats12.

OpenFlow is not a northbound API protocol, but a southbound API protocol that defines the communication between the SDN controller and the network switches or routers. OpenFlow allows the controller to manipulate the forwarding behavior of the switches or routers by sending commands and receiving events3 .

NETCONF is not a northbound API protocol, but a network management protocol that can be used as a southbound API protocol to configure and monitor network devices. NETCONF uses XML to encode data and remote procedure calls (RPCs) to exchange messages between the controller and the network devices . Reference := 1: What are SDN Northbound APIs (and SDN Rest APIs)? - SDxCentral 2: SDN North-bound and South-bound APIs and Interfaces 3: OpenFlow - Wikipedia : OpenFlow - SDxCentral : NETCONF - Wikipedia : NETCONF Protocol - Cisco

1sdxcentral.com2computernetworkingnotes.com3examguides.com

Question: 366

[Security Concepts]

What is an advantage of network telemetry over SNMP pulls?

A. accuracy
B. encapsulation
C. security
D. scalability

Answer: D

Explanation:

Network telemetry is a technology that allows network devices to push data to a collector in real time, rather than waiting for the collector to pull data from them. This improves the efficiency and accuracy of data collection, and enables the monitoring of a large number of network devices. SNMP, on the other hand, is a protocol that uses a pull model, where the collector requests data from the devices periodically. This can cause delays, gaps, and overhead in data collection, and limit the scalability of network monitoring. Therefore, network telemetry has an advantage over SNMP pulls in terms of scalability. Reference:

What Is Telemetry? Telemetry vs. SNMP - Huawei

Streaming telemetry challenges SNMP in large, complex networks

Network streaming telemetry: Monitoring in "real-time" - Paessler

An Overview of Network Telemetry - Geek Speak - Resources - THWACK

Question: 367

[Security Concepts]

What are two functions of TAXII in threat intelligence sharing? (Choose two.)

A. determines the "what" of threat intelligence

B. Supports STIX information
C. allows users to describe threat motivations and abilities
D. exchanges trusted anomaly intelligence information
E. determines how threat intelligence information is relayed

Answer: B,E

Explanation:

TAXII, short for Trusted Automated eXchange of Intelligence Information, is a protocol that defines how cyber threat information can be shared via services and message exchanges. It is designed specifically to support STIX information, which is a standardized language for expressing and exchanging cyber threat information. TAXII enables organizations to share STIX information by defining an API that aligns with common sharing models, such as hub and spoke, source/subscriber, and peer-to-peer. TAXII also defines four services that allow users to discover, manage, receive, and request STIX information. Therefore, TAXII supports STIX information and determines how threat intelligence information is relayed. TAXII does not determine the "what" of threat intelligence, as that is the role of STIX. TAXII does not allow users to describe threat motivations and abilities, as that is also part of STIX. TAXII does not exchange trusted anomaly intelligence information, as that is a specific type of threat intelligence that may or may not be represented in STIX. Reference: What are STIX/TAXII Standards I Resources I Anomali
Cyber Threat Intelligence Technical Committee - GitHub Pages

Question: 368

[Content Security]
A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion. What is a requirement for both physical hosts?

A. The hosts must run Cisco AsyncOS 10.0 or greater.
B. The hosts must run different versions of Cisco AsyncOS.
C. The hosts must have access to the same defined network.
D. The hosts must use a different datastore than the virtual appliance.

Answer: C

Explanation:

To migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion, both hosts must have access to the same defined network. This is because vMotion preserves the network identity and connections of the virtual machine, and requires that the source and destination hosts have compatible CPUs and shared storage1. The hosts do not need to run the same or different versions of Cisco AsyncOS, as long as they meet the minimum requirements for the virtual appliance2. The hosts do not need to use a different datastore than the virtual appliance, as vMotion can migrate virtual machines across datastores as well3. Reference: 1: VMware vMotion: Live Migration of Virtual Machines and Storage 2: Cisco Secure Web Appliance Virtual - Cisco 3: Migrating to Virtual SMA from Physical - Cisco Community

Question: 369

[Endpoint Protection and Detection]
What is a difference between Cisco AMP for Endpoints and Cisco Umbrella?

A. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.
B. Cisco AMP for Endpoints prevents connections to malicious destinations, and C malware.
C. Cisco AMP for Endpoints automatically researches indicators of compromise ..
D. Cisco AMP for Endpoints prevents, detects, and responds to attacks before and against Internet threats.

Answer: D

Explanation:

https://learn-umbrella.cisco.com/i/802005-umbrella-security-report/3?

https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html#:~:text=Powerful%20EDR%20capabilities,from%20Kenna%20Security.
Cisco Advanced Malware Protection (AMP) for endpoints can be seen as a replacement for the traditional antivirus solution. It is a next generation, cloud delivered endpoint protection platform (EPP), and advanced endpoint detection and response (EDR). Providing Protection – Detection Response
While Cisco Umbrella can enforce security at the DNS-, IP-, and HTTP/S-layer, this report does not require that blocking is enabled and only monitors your DNS activity. Any malicious domains requested and IPs resolved are indicators of compromise (IOC).
Any malicious domains requested and IPs resolved are indicators of compromise (IOC)

Question: 370

[Security Concepts]
What is the result of the ACME-Router(config)#login block-for 100 attempts 4 within 60 command on a Cisco IOS router?

A. If four log in attempts fail in 100 seconds, wait for 60 seconds to next log in prompt.
B. After four unsuccessful log in attempts, the line is blocked for 100 seconds and only permit IP addresses are permitted in ACL
C. After four unsuccessful log in attempts, the line is blocked for 60 seconds and only permit IP addresses are permitted in ACL1
D. If four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds.

Answer: D

Explanation:

The login block-for command sets a limit on the maximum number of failed login attempts allowed within a defined period of time. If this limit is exceeded, no further logins are allowed for the specified period of time. This feature is designed to

www.atmicnetworks.com

protect the router from denial-of-service and dictionary attacks. The syntax of the command is as follows: login block-for <block-time-period> attempts <fail-attempts> within <login-attempt-time-period> The <block-time-period> parameter specifies the duration of the quiet period in seconds. The <failattempts> parameter specifies the number of failed attempts that trigger the quiet period.

The <login-attempt-time-period> parameter specifies the time window in seconds for counting the failed attempts. In this question, the command login block-for 100 attempts 4 within 60 means that if four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds. During the quiet period, no login attempts are accepted, and the router responds with the message "Login disabled for <block-time- period> seconds due to too many failed login attempts." After the quiet period expires, the router resumes normal login operations.

The other options are incorrect because they do not match the command syntax or the expected behavior of the login block-for feature.

Reference :=

Some possible references for this question are:

User Security Configuration Guide - Cisco IOS Login Enhancements-Login Block

Configuring Login Block

Restrict login attempts : login block-for command

When applied to a router, which command would help mitigate brute-force password attacks against the router?

Question: 371

[Security Concepts]

An engineer is implementing Cisco CES in an existing Microsoft Office 365 environment and must route inbound email to Cisco CE.. record must be modified to accomplish this task?

A. CNAME
B. MX
C. SPF
D. DKIM

Answer: B

Explanation:

To route inbound email to Cisco Cloud Email Security (CES), the engineer must modify the MX record of the domain to point to the CES hostname or IP address. The MX record is a DNS record that specifies the mail server responsible for accepting email messages on behalf of a domain name. By changing the MX record, the engineer can direct all incoming email traffic to the CES gateway, where it can be filtered and scanned for threats before being delivered to the Microsoft Office 365 mailboxes. The other options are not relevant for this task. A CNAME record is a DNS record that maps an alias name to a canonical name. An SPF record is a DNS record that identifies the authorized senders of email for a domain. A DKIM record is a DNS record that contains a public key for verifying the digital signature of email messages sent from a domain. Reference := Some possible references for this question are: Configure Microsoft 365 with Secure Email Configure Microsoft 365 with Secure Email - More

[Cisco Cloud Email Security - Configuration Guide]

Question: 372

[Security Concepts]
What are two functionalities of northbound and southbound APIs within Cisco SDN architecture?

(Choose two.)

A. Southbound APIs are used to define how SDN controllers integrate with applications.
B. Southbound interfaces utilize device configurations such as VLANs and IP addresses.
C. Northbound APIs utilize RESTful API methods such as GET, POST, and DELETE.
D. Southbound APIs utilize CLI, SNMP, and RESTCONF.
E. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices.

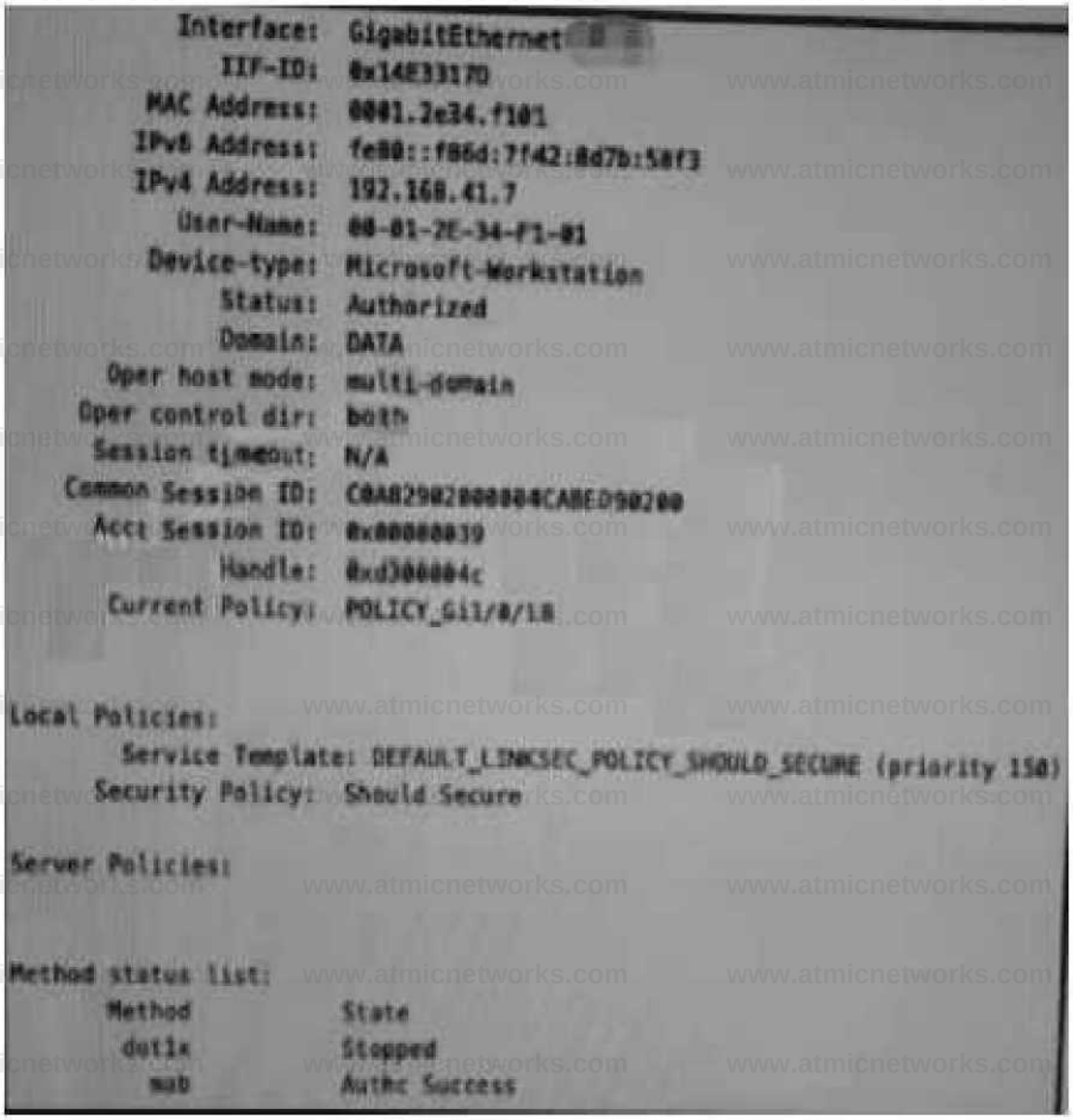
Answer: C,D

Explanation:

Northbound and southbound APIs are two types of interfaces that enable communication between different layers of the SDN architecture. Northbound APIs relay information between the controller and the applications or policy engines, while southbound APIs relay information between the controller and the network devices.
Northbound APIs allow applications to request network services or resources from the controller, such as bandwidth, latency, security, or routing. The controller then translates these requests into network configurations and applies them to the network devices via the southbound APIs.
Northbound APIs typically use RESTful API methods such as GET, POST, and DELETE to communicate with the controller.
Southbound APIs allow the controller to program the network devices to perform forwarding and other functions. The controller can use different protocols or standards to communicate with the network devices, depending on their capabilities and vendor-specific features. Some common examples of southbound APIs are CLI, SNMP, RESTCONF, NETCONF, OpenFlow, and OpFlex. Reference:
Software-Defined Networking (SDN) Definition - Cisco
Software-Defined Networking Security and Network … - Cisco Press
Cisco SDN – Software Defined Networking Explained - Study-CCNA
SDN Network - Cisco Community

Question: 373

[Security Concepts] Refer to the exhibit.



Which configuration item makes it possible to have the AAA session on the network?

A. aaa authentication login console ise
B. aaa authentication enable default enable
C. aaa authorization network default group ise
D. aaa authorization exec default ise

Answer: C

Explanation:

AAA stands for Authentication, Authorization, and Accounting. It is a framework that provides security to network resources by controlling who can access them (authentication), what they can do (authorization), and what actions they perform (accounting). AAA can be implemented by using the local database of the device or by using an external server such as Cisco ISE (Identity Services Engine).

The question asks which configuration item makes it possible to have the AAA session on the network. A session is a logical

connection between a user and a network device. A session can be initiated by various methods, such as console, telnet, SSH, PPP, etc. Each session can have different AAA policies applied to it, depending on the method list configured for that session.

A method list is a set of rules that define the authentication, authorization, and accounting methods to be used for a particular session. A method list can be named or default. A named method list is applied to a specific session by using the login, authorization, or accounting keyword followed by the name of the method list. A default method list is applied to all sessions that do not have a named method list configured.

The configuration item that makes it possible to have the AAA session on the network is the aaa authorization network default group ise command. This command configures a default method list for network authorization, which is the process of determining the network services and attributes that a user is allowed to access after authentication. The command specifies that the network authorization method is group, which means that the device will use an external server (such as Cisco ISE) to obtain the authorization information for the user. The command also specifies that the name of the server group is ise, which means that the device will use the server group defined by the aaa group server radius ise command.

The other options are incorrect because they do not configure a default method list for network authorization. Option A configures a named method list for login authentication, which is the process of verifying the identity of the user. Option B configures a default method list for enable authentication, which is the process of verifying the identity of the user who wants to enter the privileged EXEC mode. Option D configures a default method list for exec authorization, which is the process of determining the commands and features that a user can access in the EXEC mode. Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Security Concepts, Lesson 1: Describing Information Security Concepts

Configure Basic AAA on an Access Server, General AAA Configuration, Authentication Configuration, Authorization Configuration

AAA (Authentication, Authorization and Accounting) - GeeksforGeeks, AAA implementation, ACS server

Question: 374

[Security Concepts] Refer to the exhibit.

www.atmicnetworks.com

•reman** it
"duUirtit'on^tKvico* ' Tiwi<r uwrvKind
V« . ■ dt< - .'.'l'S- -. cnte p.

■arch V

'permrt* tiueORtateo 'active* Tn#*
"povtxxf *1* 'wurteMOress** ("ToncT sotircWdfessKind \aiue* sourcaAdotess

INESEDUMPS 通过测试

req = ur*02 RequesRurt non ckaWPWOW. headers)
baseWstrmo - O^M encooesl^Ss S$ % (U$#^T< pewwMlUetfKefX ') idqadd h-i
kafAuWKxe^KJtr *Hws< %< %turtofttannq) t^
I - uM2 ur)opv<X<<M>
5Mu$_oote ■ I gefcocfei)

pr! *SUM Wie ir'Mf($!«1u5_COW)
rf ^rtuS-Ctrie - - 201
pririul "OpQttf «X1 six.i.uWuT
QHWl uilit'2 HTTPEnqf, on
pruH'lnoe toccMMl Hom MIW HTTP State coto "•'.ti(wT coku
kF
ponjror = pon kMMtRerr NMdQ)
rtponjMMr
pnnt pOfl dunx^V^ «r<X$_4$50/1 kn>*,= True «i>3^ VX***^'-C,' Tl oxcop! Valua&rw
pass fm^Hy ill tdowo

EDUMPS 通过测试

What is the function of the Python script code snippet for the Cisco ASA REST API?

A. adds a global rule into policies
B. changes the hostname of the Cisco ASA
C. deletes a global rule from policies
D. obtains the saved configuration of the Cisco ASA firewall

Answer: A

Explanation:

The Python script code snippet for the Cisco ASA REST API is used to add a global rule into policies. The script uses the urllib2 module to create an HTTP request with the URL, headers, and post_data. The post_data is a JSON object that contains the parameters for the global rule, such as the destination service, the source address, the permit value, and the position. The script also uses the base64 module to encode the username and password for authentication. The script then sends the request to the ASA REST API and prints the status code and the response. If the status code is 201, it means the operation was successful and the global rule was added. If the status code is not 201, it means there was an error and the script prints the JSON error message. The script also handles any HTTP errors and value errors that might occur during the execution. Reference: Cisco ASA REST API Quick Start Guide Configure Secure Access to Use REST API with Python

GitHub - timwukp/Cisco-ASA-REST-API

Question: 375

[Security Concepts]
An engineer must modify a policy to block specific addresses using Cisco Umbrell
a. The policy is created already and is actively u: of the default policy elements. What else must be done to accomplish this task?

A. Add the specified addresses to the identities list and create a block action.
B. Create a destination list for addresses to be allowed or blocked.
C. Use content categories to block or allow specific addresses.
D. Modify the application settings to allow only applications to connect to required addresses.

Answer: B

Explanation:

Cisco Umbrella allows you to create custom destination lists that contain specific domains or IP addresses that you want to allow or block. You can then apply these destination lists to your policies to override the default behavior of Umbrella. For example, if you want to block specific addresses using Cisco Umbrella, you can create a destination list with those addresses and set the action to block. Then, you can assign this destination list to the policy that you want to modify. This way, any request to those addresses will be blocked by Umbrella, regardless of the content category or application settings12 Reference := 1: Manage Policies - Umbrella User Guide 2: Understanding Destination lists supported entries and error messages - Cisco Umbrella

Question: 376

[Network Security]
An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?

A. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol.
B. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.
C. GRE over IPsec adds its own header, and L2TP does not.
D. GRE over IPsec cannot be used as a standalone protocol, and L2TP can.

Answer: C

Explanation:

L2TP and GRE are both tunneling protocols that can be used to create site-to-site VPNs. However, they have some differences in how they encapsulate and transport data. L2TP is a layer 2 protocol that uses IP packet encapsulation to carry PPP frames over an IP network. L2TP does not add any additional header to the IP packet, but relies on IPsec to provide encryption and authentication. GRE is a layer 3 protocol that adds its own header to the IP packet, which contains information such as the protocol type, checksum, and key. GRE can be used to carry any type of payload over an IP network, not just PPP frames. GRE also requires IPsec to provide security for the tunnel. Therefore, the correct answer is C, because GRE over IPsec adds its own header, and L2TP does not1234 Reference := 1: Implementing and Operating Cisco

Security Core Technologies (SCOR) v1.0 - Module 5: Secure Connectivity 2: What is the difference between L2TP vs GRE 3: GRE over IPSec vs L2TP over IPSEC 4: difference between L2TP/GRE/MPLS

Question: 377

[Secure Network Access, Visibility, and Enforcement]
What is a benefit of using a multifactor authentication strategy?

A. It provides visibility into devices to establish device trust.
B. It provides secure remote access for applications.
C. It provides an easy, single sign-on experience against multiple applications
D. It protects data by enabling the use of a second validation of identity.

Answer: D

Explanation:

Multifactor authentication (MFA) is a security measure that requires two or more proofs of identity to grant access to network resources. These proofs can be something the user knows (such as a password or a PIN), something the user has (such as a token or a card), or something the user is (such as a fingerprint or a face scan). The benefit of using MFA is that it adds an extra layer of

protection against unauthorized access, especially if the first factor (such as a password) is compromised or stolen. By requiring a second validation of identity, MFA reduces the risk of data breaches and identity theft. MFA can also help comply with regulatory and industry standards that mandate strong authentication for sensitive data and systems.
Reference := Some possible references are:
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Security Concepts, Lesson 1.3: Identity and Access Management
Multi-factor authentication best practices & strategy, NordLayer Blog
How to implement Multi-Factor Authentication (MFA), Microsoft Security Blog
Multi-factor authentication, Cyber.gov.au
What is Multi-Factor Authentication?, IBM

Question: 378

[Endpoint Protection and Detection]
A Cisco ISE engineer configures Central Web Authentication (CWA) for wireless guest access and must have the guest endpoints redirect to the guest portal for authentication and authorization. While testing the policy, the engineer notices that the device is not redirected and instead gets full guest access. What must be done for the redirect to work?

A. Tag the guest portal in the CWA part of the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.

B. Use the track movement option within the authorization profile for the authorization policy line that the unauthenticated devices hit.

C. Create an advanced attribute setting of Cisco:cisco-gateway-id=guest within the authorization profile for the authorization policy line that the unauthenticated devices hit.

D. Add the DACL name for the Airespace ACL configured on the WLC in the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.

Answer: D

Explanation:

To enable CWA for wireless guest access, the ISE engineer needs to configure the following steps on the ISE server:
Create a guest portal with the desired settings and appearance.
Create an authorization profile that references the guest portal and the DACL name for the Airespace ACL configured on the WLC. The DACL name must match the name of the ACL on the WLC exactly. The authorization profile also needs to have the common tasks of Web Redirection and Web Authentication enabled.
Create an authorization policy that matches the unauthenticated devices based on the MAC address or other criteria and applies the authorization profile created in the previous step.
The DACL name is required for the WLC to apply the correct ACL to the guest endpoints and redirect them to the guest portal. Without the DACL name, the WLC will not know which ACL to use and may grant full guest access to the endpoints. Therefore, the correct answer is D.

Reference :=
Some possible references are:
Central Web Authentication (CWA) for guests with ISE
Understand And Troubleshoot Central Web-Authentication (CWA) In Guest Anchor Set-Up
Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Release 17.3.0 - Guest Access

Question: 379

[Content Security]
Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

A. Cisco Umbrella
B. Cisco ISE
C. Cisco DNA Center
D. Cisco TrustSec
E. Cisco Duo Security

Answer: A,E

Explanation:

Cisco Umbrella and Cisco Duo Security are two solutions that help combat social engineering and phishing at the endpoint level. Cisco Umbrella is a cloud-based security platform that provides DNS- layer security, web filtering, and threat

intelligence to protect users from malicious websites and domains. Cisco Duo Security is a multi-factor authentication (MFA) solution that verifies the identity of users and the health of their devices before granting access to applications. Both solutions help prevent attackers from compromising endpoints and stealing credentials or data through phishing or other social engineering techniques. Reference:

Cisco Umbrella

Cisco Duo Security

Implementing and Operating Cisco Security Core Technologies (SCOR) - Module 3: Cloud and Content Security

Question: 380

[Secure Network Access, Visibility, and Enforcement] Which role is a default guest type in Cisco ISE?

A. Monthly
B. Yearly
C. Contractor
D. Full-Time

Answer: C,D

Explanation:

To add switches into the fabric, administrators can use PowerOn Auto Provisioning (POAP) or Seed IP methods. POAP is a feature that automates the process of upgrading software images and installing configuration files on Cisco switches that are being deployed in the network for the first time. Seed IP is a method that allows administrators to specify the IP address of a switch that is already part of the fabric, and then use it to discover and add other switches that are connected to it. Both methods enable administrators to control how switches are added into DCNM for private cloud management. Reference:

POAP, section "PowerOn Auto Provisioning (POAP)".

Seed IP, section "Add Switches".

https://www.cisco.com/c/en/us/td/docs/security/ise/1-4-1/admin_guide/b_ise_admin_guide_141/b_ise_admin_guide_141_chapter_01110.html

Question: 381

[Securing the Cloud]

Which two methods must be used to add switches into the fabric so that administrators can control how switches are added into DCNM for private cloud management? (Choose two.)

A. Cisco Cloud Director
B. Cisco Prime Infrastructure

www.atmicnetworks.com

C. PowerOn Auto Provisioning

D. Seed IP

E. CDP AutoDiscovery

Answer: C,D

Explanation:

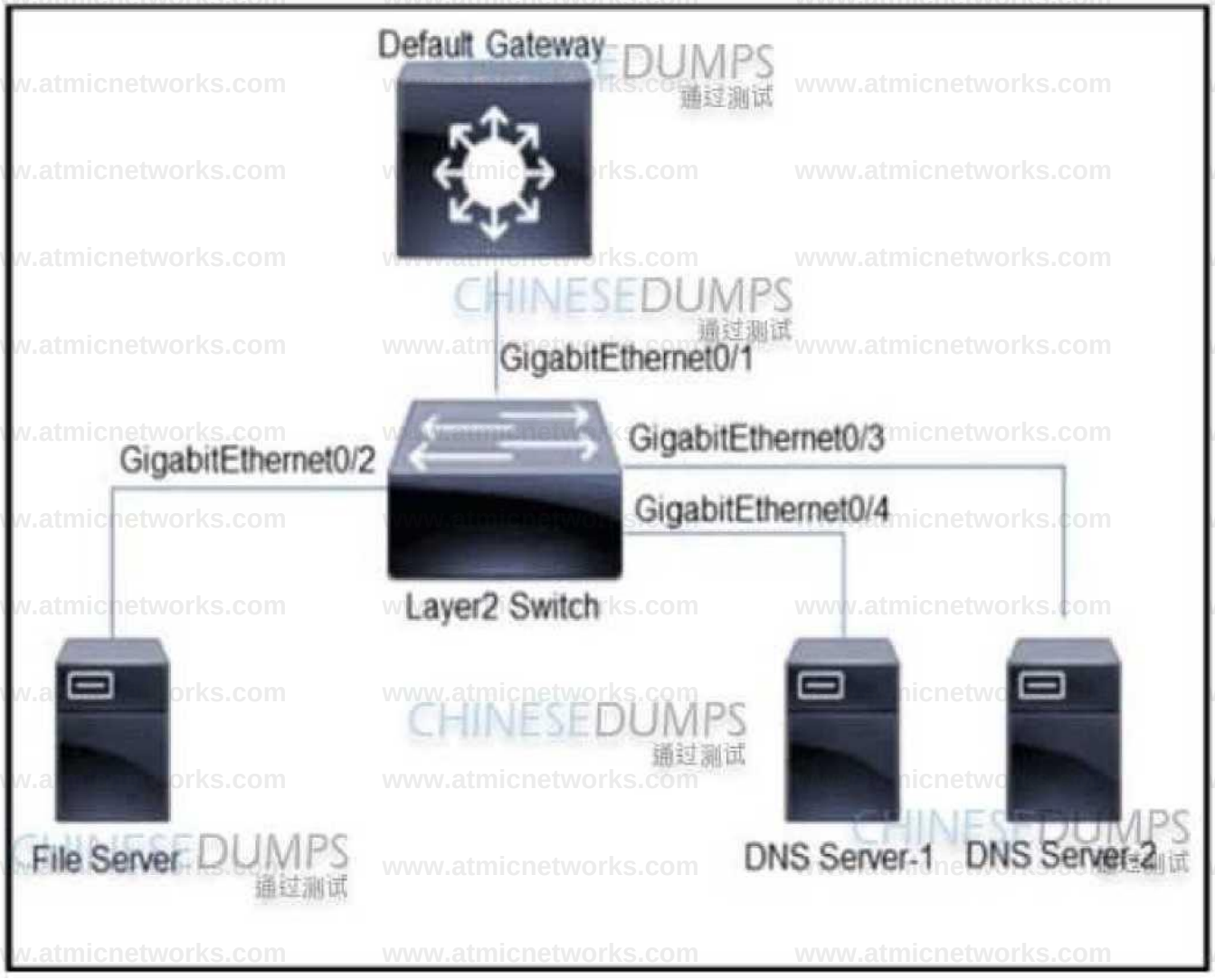
To add switches into the fabric for private cloud management, administrators can use the following two methods:
PowerOn Auto Provisioning (POAP): This method allows the switches to be automatically discovered and provisioned by DCNM using a POAP configuration file. The switches are assigned an IP address and a startup configuration based on the fabric settings and policies. The switches are then added to the fabric and deployed with the VXLAN EVPN configuration. This method is suitable for greenfield

deployments or adding new switches to an existing fabric12.

Seed IP: This method allows the administrators to manually specify the IP address of the switches that they want to add to the fabric. The switches must have a reachable IP address and a username and password that match the fabric settings. The switches are then added to the fabric and deployed with the VXLAN EVPN configuration. This method is suitable for brownfield deployments or transitioning existing switches to DCNM management12. Reference: Cisco NDFC Fabric Controller Configuration Guide, Release 12.0.x, Cisco DCNM LAN Fabric Configuration Guide, Release 11.5(x).

Question: 382

[Security Concepts]



Refer to the exhibit. All servers are in the same VLAN/Subnet. DNS Server-1 and DNS Server-2 must communicate with each other, and all servers must communicate with default gateway multilayer switch. Which type of private VLAN ports should be configured to prevent communication between DNS servers and the file server?

A. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet0/4 as promiscuous ports.

B. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as promiscuous port, Gigabit Ethernet0/3 and

GigabitEthernet0/4 as isolated ports C. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as isolated port and GigabitEthernet0/3 and

GrgabitEthernet0/4 as community ports

C. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as community port, and

GigabitEthernet0/3 and GrgabitEthernet0/4 as isolated ports.

Answer: C

Explanation:

to configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as isolated port and GigabitEthernet0/3 and GrgabitEthernet0/4 as community ports. This way, the default gateway can communicate with all servers, the isolated port can only communicate with the promiscuous port, and the community ports can communicate with each other and the promiscuous port. This prevents the file server from communicating with the DNS servers, as required by the question.

To understand the concept of private VLANs and port types, you can refer to the following sections of the source book:

Section 1.1.2: Describe the concepts of network security

Section 1.1.2.1: Describe the concepts of private VLANs

Section 1.1.2.2: Describe the concepts of port types

Section 1.1.2.3: Describe the concepts of PVLAN edge

Section 1.1.2.4: Describe the concepts of protected ports

Section 1.1.2.5: Describe the concepts of PVLAN configuration

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Private VLAN - GeeksforGeeks

A quick summarized view to Private VLAN (PVLAN) - Cisco Learning Network

Question: 383

[Security Concepts]

Refer to the exhibit. When creating an access rule for URL filtering, a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?

A. Only URLs for botnets with reputation scores of 1-3 will be blocked.

B. Only URLs for botnets with a reputation score of 3 will be blocked.

C. Only URLs for botnets with reputation scores of 3-5 will be blocked.

D. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.

Answer: B

Explanation:

The exhibit shows an access rule for URL filtering that has the following conditions:

The action is Block

The URL category is Botnets

The URL reputation is 3
The URL list is empty
This means that the rule will block any URL that matches the category and reputation criteria, regardless of the individual URL. According to the Cisco documentation1, the URL reputation is a score from 1 to 5 that indicates the risk level of a URL, where 1 is the most risky and 5 is the least risky. Therefore, a reputation score of 3 means a moderate risk level. The rule will not block URLs for botnets with reputation scores of 1, 2, 4, or 5, nor will it block any other URL category or list. The rule will also not allow any URL, as the action is Block, not Allow.
Reference := 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Securing the Cloud, Lesson 4.3: Cloud Application Security, Topic 4.3.2: Cisco Umbrella, page 4-58.

Question: 384

[Endpoint Protection and Detection]
Why is it important to have a patching strategy for endpoints?

A. to take advantage of new features released with patches
B. so that functionality is increased on a faster scale when it is used
C. so that known vulnerabilities are targeted and having a regular patch cycle reduces risks
D. so that patching strategies can assist with disabling nonsecure protocols in applications

Answer: C

Explanation:

Patching is important for security, compliance, stability, and reputation reasons. Patches are released to fix security vulnerabilities in software and systems, which can be exploited by cybercriminals to cause data breaches, data loss, or other damage. Failure to patch these vulnerabilities leaves the company's systems exposed to potential security risks. Patch management helps to minimize these risks by ensuring that all software and systems are up-to-date with the latest security patches. Patch management also helps to comply with regulatory and industry standards that require a certain level of security, and to avoid legal consequences for non-compliance. Additionally, patches provide bug fixes and other updates that improve the stability and performance of software and systems, and prevent system crashes, downtime, and other issues that can negatively impact the business operations. Finally, patch management helps to maintain a positive reputation for the company, as a

security breach or downtime caused by unpatched vulnerabilities can damage the customer trust and loyalty, and result in revenue loss. Reference:
5 Patch Management Best Practices for Success in 2023 - TechRepublic
Six Patch Management Best Practices [Updated 2024] - Heimdal Security

Question: 385

[Security Concepts]

www.atmicnetworks.com

An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the policy that the identity must use takes precedence over the second one?

A. Configure the default policy to redirect the requests to the correct policy
B. Place the policy with the most-specific configuration last in the policy order
C. Configure only the policy with the most recently changed timestamp
D. Make the correct policy first in the policy order

Answer: D

Explanation:

Cisco Umbrella evaluates policies from the top down and looks for a matching identity and destination. Once a match is found, Umbrella applies that policy's settings to the identity and destination and stops evaluating all other DNS policies. Therefore, to ensure that the policy that the identity must use takes precedence over the second one, the engineer should make the correct policy first in the policy order. This way, Umbrella will match the identity to the correct policy before checking the second policy. The other options are not correct because they do not guarantee that the identity will use the correct policy. Configuring the default policy to redirect the requests to the correct policy will not work if the identity matches another policy before the default one. Placing the policy with the most-specific configuration last in the policy order will not work if the identity matches a less-specific policy before the last one. Configuring only the policy with the most recently changed timestamp will not work if the identity matches an older policy before the newer one. Reference := Some possible references are:
Policy Precedence - Umbrella User Guide1
Manage Policies - Umbrella User Guide2
Umbrella Policy order - Cisco Community3

Question: 386

[Security Concepts]

Which security product enables administrators to deploy Kubernetes clusters in air-gapped sites without needing Internet access?

A. Cisco Content Platform
B. Cisco Container Controller
C. Cisco Container Platform
D. Cisco Cloud Platform

Answer: C

Explanation:

Cisco Container Platform (CCP) is a security product that enables administrators to deploy Kubernetes clusters in air-gapped sites without needing Internet access. CCP tenant images contain all the necessary binaries and don't need internet access to function. CCP also supports ofline installation and updates of the platform

components. CCP is designed to simplify the deployment and management of containerized applications across hybrid cloud environments, while ensuring security and compliance. CCP integrates with Cisco security solutions such as Cisco Tetration and Cisco Stealthwatch Cloud to provide visibility and protection for Kubernetes clusters and workloads. CCP also leverages Cisco Intersight, a cloud-based management platform, to provide centralized monitoring and automation for CCP clusters. Reference:
Cisco Container Platform
350-701 SCOR Cisco CCNP Security Updated Questions in April

Question: 387

[Security Concepts]
What is the intent of a basic SYN flood attack?

A. to solicit DNS responses
B. to exceed the threshold limit of the connection queue
C. to flush the register stack to re-initiate the buffers
D. to cause the buffer to overflow

Answer: B

Explanation:

A basic SYN flood attack is a type of denial-of-service (DoS) attack that aims to exhaust the resources of a server by sending a large number of SYN packets and not completing the TCP three-way handshake. The intent of this attack is to exceed the threshold limit of the connection queue, which is the data structure that stores the information about the pending connections. By doing so, the attacker prevents legitimate clients from establishing connections with the server, as the server

cannot accept any more SYN requests. A SYN flood attack can be performed with spoofed IP addresses or without IP spoofing, depending on the attacker's strategy and the server's configuration. Reference:
[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 3: Securing Networks with Firewalls, Lesson 3.2: Firewall Technologies, Topic 3.2.1: Firewall Technologies Overview, Page 8. SYN flood DDoS attack | Cloudflare. How to Perform TCP SYN Flood DoS Attack & Detect it with Wireshark - Kali Linux hping3. SYN flood - Wikipedia. SYN Flood Attack | SpringerLink. What Is a SYN Flood Attack? | F5.

Question: 388

[Security Concepts]
An engineer configures new features within the Cisco Umbrella dashboard and wants to identify and proxy traffic that is categorized as risky domains and may contain safe and malicious content. Which action accomplishes these objectives?

A. Configure URL filtering within Cisco Umbrella to track the URLs and proxy the requests for those categories and below.

B. Configure intelligent proxy within Cisco Umbrella to intercept and proxy the requests for only those categories.

C. Upload the threat intelligence database to Cisco Umbrella for the most current information on reputations and to have the destination lists block them.

D. Create a new site within Cisco Umbrella to block requests from those categories so they can be sent to the proxy device.

Answer: D

Explanation:

The intelligent proxy is a feature of Cisco Umbrella that allows it to selectively inspect and proxy web requests for domains that are classified as risky or potentially malicious. These domains may contain both safe and harmful content, and the intelligent proxy can filter out the malicious files or URLs while allowing the benign ones to pass through. The intelligent proxy can also apply SSL decryption to inspect encrypted traffic and enforce policies based on the content or destination of the web requests. To enable the intelligent proxy, an engineer needs to configure it within the Cisco Umbrella dashboard and select the categories of domains that should be proxied. The categories are based on the domain reputation and security risk, and range from High Risk to Low Risk. The engineer can also customize the list of domains to include or exclude from the intelligent proxy. By configuring the intelligent proxy, the engineer can achieve the objectives of identifying and proxying traffic that is categorized as risky domains and may contain safe and malicious content.

Reference := Some possible references are:

Enable the Intelligent Proxy - Umbrella User Guide, Cisco

Manage the Intelligent Proxy - Umbrella User Guide, Cisco

Intelligent Proxy in Cisco Umbrella how it works, Cisco Learning Network What is the Intelligent Proxy? - MSP User Guide, Cisco

Cisco Umbrella Intelligent Proxy and SSL Decryption implementation, Cisco Community

Question: 389

[Content Security]

Which endpoint solution protects a user from a phishing attack?

A. Cisco Identity Services Engine

B. Cisco AnyConnect with ISE Posture module

C. Cisco AnyConnect with Network Access Manager module

D. Cisco AnyConnect with Umbrella Roaming Security module

Answer: D

Explanation:

Cisco AnyConnect with Umbrella Roaming Security module protects a user from a phishing attack by enforcing security at

the DNS layer and blocking malicious domains that are used for phishing campaigns. The Umbrella Roaming Security module integrates with the Cisco AnyConnect client and provides always-on security even when no VPN is active. The Umbrella Roaming Security module can replace the existing Cisco Umbrella roaming client or be part of a new AnyConnect deployment12. Cisco Identity Services Engine (ISE) is not an endpoint solution, but a network access control and policy enforcement platform that can integrate with AnyConnect for posture assessment and compliance3. Cisco AnyConnect with ISE Posture module is used to check the compliance status of the endpoint device and apply the appropriate network access policy based on the posture result4. Cisco AnyConnect with Network Access Manager module is used to manage the network connections and profiles of the endpoint device and support various authentication methods5. Neither of these modules directly protect the user from a phishing attack.

Reference :=

Roaming Client: Umbrella Roaming Security (Integration with AnyConnect)

Secure Umbrella Roaming: Cisco Secure Client (Formerly AnyConnect)

Cisco Identity Services Engine

[Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9 - Posture Module]

[Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9 - Network Access Manager Module]

Question: 390

[Security Concepts]

Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?

A. Cisco Identity Services Engine (ISE)
B. Cisco Enterprise Security Appliance (ESA)
C. Cisco Web Security Appliance (WSA)
D. Cisco Advanced Stealthwatch Appliance (ASA)

Answer: C

Explanation:

Cisco Web Security Appliance (WSA) is the platform that automatically blocks risky sites, and tests unknown sites for hidden advanced threats before allowing users to click them, using Cisco Cognitive Threat Analytics. Cisco Cognitive Threat Analytics is a cloud-based solution that reduces the time to discovery of threats operating inside the network by analyzing web traffic and detecting anomalous behavior. Cisco WSA integrates with Cisco Cognitive Threat Analytics to provide enhanced web security and breach detection. Cisco WSA can also leverage other Cisco security solutions, such as Cisco Umbrella, Cisco Advanced Malware Protection (AMP), and Cisco Talos Intelligence Group, to provide comprehensive web security. Reference:

Cisco Web Security Appliance (WSA)

Cisco Cognitive Threat Analytics At-a-Glance

Introducing Cisco Cognitive Threat Analytics

Question: 391

[Content Security]
What are two things to consider when using PAC files with the Cisco WSA? (Choose two.)

A. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.
B. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.
C. The WSA hosts PAC files on port 9001 by default.
D. The WSA hosts PAC files on port 6001 by default.
E. By default, they direct traffic through a proxy when the PC and the host are on the same subnet.

Answer: B,C

Explanation:

PAC files are scripts that tell web browsers how to use proxies on the network. They use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host, based on criteria such as the destination URL, the source IP address, or the network subnet12. The WSA can host PAC files on port 9001 by default, and this port can be changed in the PAC file hosting settings2. If the WSA host port is changed, the default port does not redirect web traffic to the correct port automatically; the browser needs to point to the new port in the PAC file URL2. The WSA does not host PAC files on port 6001 by default2. PAC files do not direct traffic through a proxy when the PC and the host are on the same subnet by default; this behavior depends on the PAC file logic12. Reference:
PAC file format
PAC file hosting on WSA

Question: 392

[Secure Network Access, Visibility, and Enforcement]

Which IETF attribute is supported for the RADIUS CoA feature?

A. 24 State
B. 30 Calling-Station-ID
C. 42 Acct-Session-ID
D. 81 Message-Authenticator

www.atmicnetworks.com

Answer: A

Explanation:

The RADIUS CoA feature supports the IETF attribute 24 State, which is used to identify the session for which the CoA request is intended. The State attribute is sent by the device in the Access-Accept message and must be echoed back by the RADIUS server in the CoA-Request message. The other attributes are not supported for the RADIUS CoA feature.

To understand the concept of RADIUS CoA and the supported attributes, you can refer to the following sections of the source book:

Section 1.1.2: Describe the concepts of network security

Section 1.1.2.6: Describe the concepts of RADIUS CoA

Section 1.1.2.7: Describe the concepts of supported IETF attributes

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

RADIUS Change of Authorization - Cisco

RADIUS attribute for change of authorization - Ruckus Networks

Question: 393

[Content Security]

When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

A. guest
B. limited Internet
C. blocked
D. full Internet

Answer: C

Explanation:

When a transparent authentication fails on the Web Security Appliance (WSA), the end user gets blocked access. This means that the user cannot access any web resources until they successfully authenticate. The WSA can use different methods to authenticate users transparently, such as Transparent User Identification (TUI), Transparent Identification, or Kerberos1. If none of these methods work, the WSA will send a block page to the user with a message explaining why the authentication failed and how to resolve the issue2. The block page can be customized by the administrator to provide more information or instructions to the user3.

Reference := 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Securing the Cloud, Lesson 4.3: Cloud Application Security, Topic 4.3.2: Cisco Umbrella, page 459. 2: User Guide for AsyncOS 12.5 for Cisco Web Security Appliances - GD (General Deployment), Chapter: Acquire End-User Credentials, Topic: Failed Authentication Credentials, page 4-67. 3: User Guide for AsyncOS 12.5 for Cisco Web Security Appliances - GD (General Deployment), Chapter: Customize End-User Notifications, Topic: Customize Block Pages, page 5-1.

www.atmicnetworks.com

Question: 394

[Security Concepts]
What are two ways that Cisco Container Platform provides value to customers who utilize cloud service providers? (Choose two.)

A. Allows developers to create code once and deploy to multiple clouds
B. helps maintain source code for cloud deployments
C. manages Docker containers
D. manages Kubernetes clusters
E. Creates complex tasks for managing code

Answer: A,D

Explanation:

Cisco Container Platform (CCP) is a solution that simplifies the deployment and management of containerized applications across multiple clouds. It provides the following benefits to customers who utilize cloud service providers12:
Allows developers to create code once and deploy to multiple clouds. CCP is based on open source components, such as Kubernetes and Docker, that are compatible with various cloud platforms. This enables developers to write code once and run it anywhere, without worrying about the underlying infrastructure or vendor lock-in. CCP also supports hybrid and multicloud scenarios, allowing customers to leverage the best features of different cloud providers and optimize their costs and performance.
Manages Kubernetes clusters. CCP automates the installation, configuration, and maintenance of Kubernetes clusters, which are groups of nodes that run containerized applications. CCP provides a simple GUI-driven menu system to deploy clusters, as well as automated monthly updates for bug fixes, feature enhancements, and security patches. CCP also offers a choice of networking solutions, such as Cisco ACI, Calico, or Contiv, to connect and secure the clusters. CCP also integrates with Cisco AppDynamics and Prometheus for visibility and monitoring of the clusters and applications.
Reference:
Cisco Container Platform - Cisco
Cisco Container Platform - At-a-Glance - Cisco

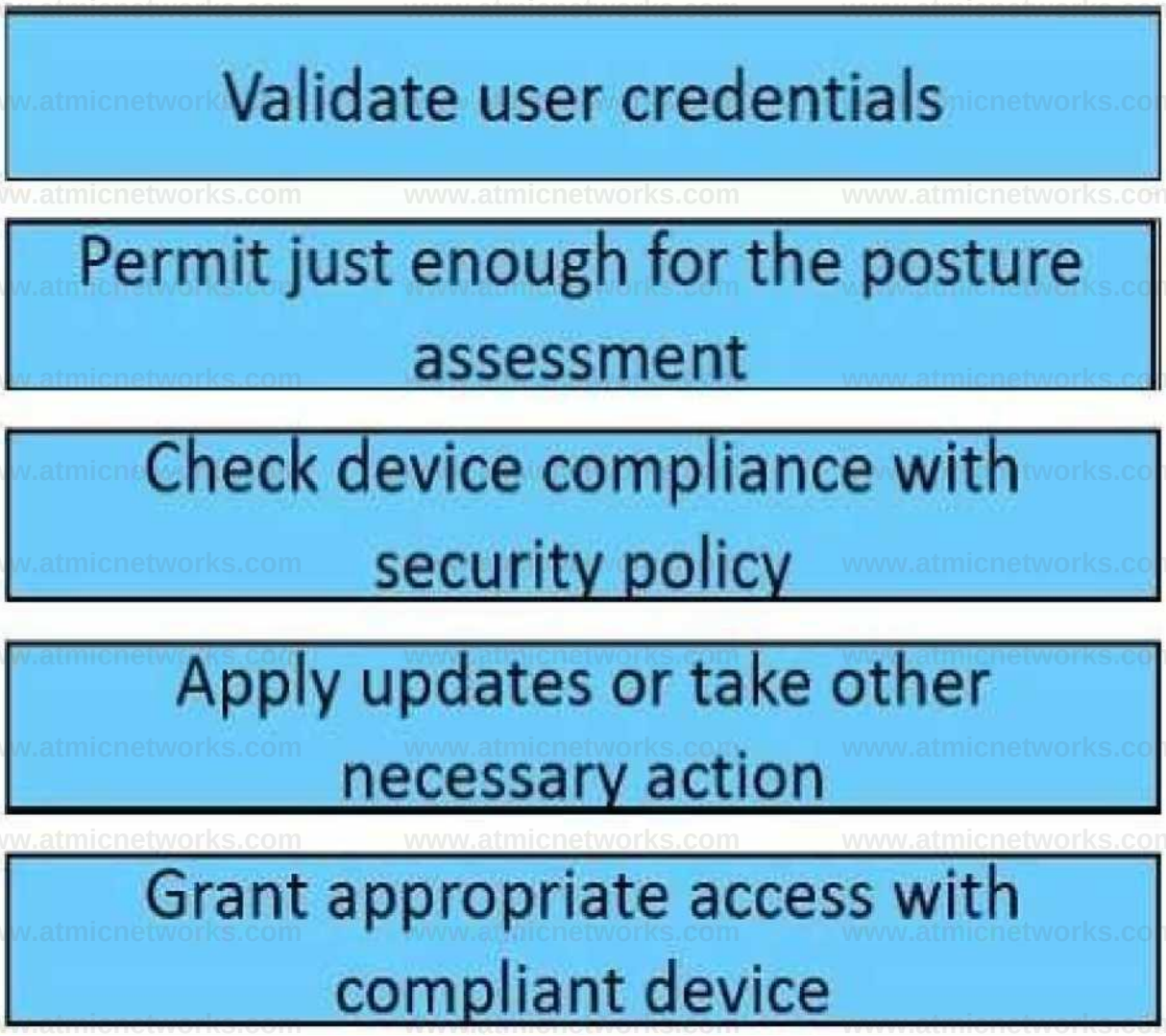
Question: 395

DRAG DROP
[Security Concepts]
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

Validate user credentials	step 1
Check device compliance with security policy	step 2
Grant appropriate access with compliant device Apply updates or take other necessary action Permit just enough for the posture assessment	step 3 step 4 step 5

Answer:

Explanation:



Question: 396

[Endpoint Protection and Detection] Refer to the exhibit.

www.atmicnetworks.com

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'
```

What does the API key do while working with https://api.amp.cisco.com/v1/computers?

A. displays client ID
B. HTTP authorization
C. Imports requests
D. HTTP authentication

Answer: D

Explanation:

The API key is used for HTTP authentication when working with APIs, including https://api.amp.cisco.com/v1/computers. It ensures that the user or system making the API request is authenticated and authorized to access the resources requested. The image you sent shows a Python code snippet that imports the requests module, assigns a client ID and an API key to variables, and uses them to make an API call. The API key is passed as a header parameter in the requests.get() function, which is a common way of implementing HTTP authentication. The other options are not correct because they do not describe the role of the API key. The client ID is a different parameter that identifies the user or system making the request, but it does not authenticate them. HTTP authorization is a process of granting or denying access to resources based on the user's identity and permissions, but it is not the same as authentication. Importing requests is a Python statement that loads the requests module, which is a library for making HTTP requests, but it has nothing to do with the API key.

Reference :=

Some possible references are:

Cisco AMP for Endpoints API requests - HTTP for Humans HTTP authentication - MDN Web Docs

Question: 397

[Security Concepts]

Which statement describes a serverless application?

A. The application delivery controller in front of the server farm designates on which server the application runs each time.

B. The application runs from an ephemeral, event-triggered, and stateless container that is fully managed by a cloud provider.
C. The application is installed on network equipment and not on physical servers.
D. The application runs from a containerized environment that is managed by Kubernetes or Docker Swarm.

Answer: B

Explanation:

A serverless application is one that does not require the developer to manage the underlying infrastructure or servers. Instead, the application code is executed by a cloud provider in response to events or triggers, such as HTTP requests, database changes, or messages. The cloud provider automatically provisions, scales, and manages the resources needed to run the code, and charges only for the time and resources consumed by the execution. A serverless application runs from an ephemeral, event-triggered, and stateless container that is fully managed by a cloud provider. This means that the container is created on demand when an event occurs, and is destroyed when the execution is completed. The container does not store any persistent state or data, and is isolated from other containers. The cloud provider handles the load balancing, fault tolerance, security, and monitoring of the container. A serverless application can leverage various cloud services, such as databases, storage, messaging, analytics, and machine learning, to perform complex tasks and functionalities. Serverless computing is a cloud-native development model that enables developers to focus on the business logic and deliver faster and more scalable applications. Reference: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 8: Cloud and Virtual Network Security, Lesson 8.1: Cloud Computing Concepts
What is serverless? - Red Hat
Serverless computing and applications | Microsoft Azure

Question: 398

[Security Concepts]
What is a description of microsegmentation?

A. Environments deploy a container orchestration platform, such as Kubernetes, to manage the application delivery.
B. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate.
C. Environments deploy centrally managed host-based firewall rules on each server or container.
D. Environments implement private VLAN segmentation to group servers with similar applications.

Answer: B

Explanation:

Microsegmentation is a network security strategy that breaks a network into smaller network “segments” to boost security and control over data traffic1. Unlike traditional network security, which primarily defends the network’s outer boundaries, microsegmentation focuses on securing individual workloads and devices within the network2. Microsegmentation uses an allow-list model to significantly reduce the attack surface across different workload types and environments3. Microsegmentation is also referred to as application segmentation or east-west segmentation in a

multicloud data center4.

Option B is the correct description of microsegmentation, as it captures the essence of applying a zero-trust model and specifying how applications on different servers or containers can communicate. Option A is incorrect, as deploying a container orchestration platform is not a sufficient condition for microsegmentation. Option C is incorrect, as deploying host-based firewall rules is not a necessary condition for microsegmentation. Option D is incorrect, as implementing private VLAN segmentation is a different technique from microsegmentation. Reference: An Introduction to Microsegmentation in Network Security. What Is Micro-Segmentation? - Cisco. What Is Microsegmentation? - Palo Alto Networks. What Is Microsegmentation in Networking? Beginner's Guide.

Question: 399

[Content Security]

Which Cisco WSA feature supports access control using URL categories?

A. transparent user identification
B. SOCKS proxy services
C. web usage controls
D. user session restrictions

Answer: C

Explanation:

Web usage controls are a feature of Cisco Web Security Appliance (WSA) that allow administrators to define and enforce policies for web access based on URL categories. URL categories are groups of websites that share a common theme or content, such as news, sports, entertainment, etc. Cisco WSA uses the Cisco Dynamic Content Analysis Engine and the Talos Security Intelligence and Research Group to provide accurate and up-to-date URL categorization. Administrators can use the web usage controls to allow, block, warn, or monitor web requests based on the URL category of the

destination website. They can also create custom URL categories to include or exclude specific domains or URLs from the predefined categories. Web usage controls help administrators to control web traffic, enhance security, improve productivity, and comply with regulatory and organizational requirements. Reference := Some possible references are:

Web Usage Controls - Cisco Web Security Appliance User Guide, Cisco

Cisco Web Usage Control Filtering Categories Data Sheet, Cisco

Define Custom URL Categories in WSA, Cisco

Question: 400

[Security Concepts]

Which technology limits communication between nodes on the same network segment to individual applications?

www.atmicnetworks.com

A. serverless infrastructure
B. microsegmentation
C. SaaS deployment
D. machine-to-machine firewalling

Answer: B

Explanation:

Microsegmentation is a technology that limits communication between nodes on the same network segment to individual applications by creating secure zones across cloud and data center environments. Microsegmentation isolates application workloads from one another and secures them individually with granular firewall policies based on a zero-trust security approach1. Microsegmentation can reduce the attack surface, prevent the lateral movement of threats, and strengthen regulatory compliance1.

Serverless infrastructure is a technology that allows developers to run code without provisioning or managing servers2. Serverless infrastructure does not limit communication between nodes on the same network segment to individual applications, but rather abstracts away the underlying infrastructure from the application logic.

SaaS deployment is a technology that delivers software applications over the internet as a service3. SaaS deployment does not limit communication between nodes on the same network segment to individual applications, but rather provides access to software applications from any device and location.

Machine-to-machine firewalling is a technology that controls the communication between machines or devices on a network. Machine-to-machine firewalling does not limit communication between nodes on the same network segment to individual applications, but rather applies rules to the traffic between machines or devices based on their IP addresses, ports, protocols, or other criteria. Reference :=

What Is Micro-Segmentation? - Cisco

What is serverless?

What is SaaS?

[Machine-to-Machine Firewalling]

Question: 401

[Security Concepts]

An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users. Which action accomplishes this goal?

A. Restrict access to only websites with trusted third-party signed certificates.
B. Modify the user's browser settings to suppress errors from Cisco Umbrella.
C. Upload the organization root CA to Cisco Umbrella.
D. Install the Cisco Umbrella root CA onto the user's device.

Answer: D

Explanation:

Installing the Cisco Umbrella root CA onto the user's device is the action that accomplishes the goal of inspecting traffic without alerting end-users. This is because the root CA allows the user's device to trust the certificates issued by the Cisco Umbrella intelligent proxy, which acts as a man-in-the- middle for SSL sites on Umbrella's grey list. Without the root CA, the user's browser would raise errors when accessing those sites, as it would detect an untrusted certificate. By installing the root CA, the user's browser would accept the certificate and allow the traffic to be proxied and inspected by the intelligent proxy. Reference:

Enable SSL Decryption - Umbrella User Guide

SSL Decryption in the Intelligent Proxy – Cisco Umbrella

Cisco Umbrella Intelligent Proxy and SSL Decryption

Intelligent Proxy and SSL Decryption with Cisco Umbrella

Question: 402

[Content Security]

What is the purpose of joining Cisco WSAs to an appliance group?

A. All WSAs in the group can view file analysis results.
B. The group supports improved redundancy
C. It supports cluster operations to expedite the malware analysis process.
D. It simplifies the task of patching multiple appliances.

Answer: D

Explanation:

Joining Cisco WSAs to an appliance group simplifies the task of patching multiple appliances. An appliance group is a collection of WSAs that share the same configuration settings and software versions. Administrators can use appliance groups to apply configuration changes and software updates to multiple WSAs at once, instead of performing these tasks individually for each appliance12. This reduces the administrative overhead and ensures consistency across the WSAs.

Reference:

Appliance groups, section "Appliance Groups".

What is the purpose of joining Cisco WSAs to an appliance group?

Question: 403

[Secure Network Access, Visibility, and Enforcement]

Why should organizations migrate to an MFA strategy for authentication?

A. Single methods of authentication can be compromised more easily than MFA.
B. Biometrics authentication leads to the need for MFA due to its ability to be hacked easily.

C. MFA methods of authentication are never compromised.
D. MFA does not require any piece of evidence for an authentication mechanism.

Answer: A

Explanation:

single methods of authentication can be compromised more easily than MFA. MFA, or multi-factor authentication, is a security process that requires users to provide two or more factors to verify their identity and access resources. MFA reduces the risk of unauthorized access by making it harder for attackers to compromise all the factors needed, especially if they are different in nature, such as something you know (password), something you have (token), and something you are (biometric). To understand the concept of MFA and why it is important for authentication security, you can refer to the following sections of the source book:
Section 1.1.1: Describe the concepts of identity and access management
Section 1.1.1.1: Describe the concepts of identity principles
Section 1.1.1.2: Describe the concepts of authentication
Section 1.1.1.3: Describe the concepts of authorization
Section 1.1.1.4: Describe the concepts of accounting
Section 1.1.1.5: Describe the concepts of identity stores
Section 1.1.1.6: Describe the concepts of MFA
Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0
What is Multi-Factor Authentication? | IBM
How to implement Multi-Factor Authentication (MFA) | Microsoft Security Blog

Question: 404

[Security Concepts]
Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?

A. RADIUS-based REAP
B. fingerprinting
C. Dynamic ARP Inspection
D. multifactor authentication

Answer: D

Explanation:

Multifactor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN1. MFA is a core component of a strong identity and access management (IAM) policy. MFA can help prevent an attacker from stealing usernames and

passwords of users within an organization by adding an extra layer of security beyond the traditional username and password. For example, a user may need to enter a one-time code sent to their phone or email, scan their fingerprint, or use a hardware token to prove their identity. This way, even if an attacker obtains the user's credentials, they cannot access the resource without the second factor2.

The other options are not technologies that can help prevent an attacker from stealing usernames and passwords of users within an organization. RADIUS-based REAP is a protocol that allows wireless clients to authenticate with a RADIUS server, but it does not provide MFA3. Fingerprinting is a technique that identifies the operating system or application of a device based on its network characteristics, but it does not provide MFA4. Dynamic ARP Inspection is a security feature that prevents ARP spoofing attacks by validating ARP packets, but it does not provide MFA5.

Reference := 1: What is Multi-Factor Authentication (MFA)? | OneLogin(https://www.onelogin.com/learn/what-is-mfa) 2: What is: Multifactor Authentication - Microsoft Support(https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication- e5e39437-121c-be60-d123-eda06bddf661) 3: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Securing the Network, Lesson 3.3: Secure Wireless Connectivity, Topic 3.3.1: Wireless Security Protocols, page 3-40. 4: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 2: Securing the Cloud, Lesson 2.2: Cloud Security Assessment, Topic 2.2.1: Cloud Security Concepts, page 2-13. 5: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Securing the Network, Lesson 3.2: Secure Network Access, Topic 3.2.2: Layer 2 Security Features, page 3-19.

Question: 405

[Security Concepts]
Which type of attack is MFA an effective deterrent for?

A. ping of death
B. phishing
C. teardrop
D. syn flood

Answer: B

Explanation:

MFA, or multi-factor authentication, is a method of verifying a user's identity by requiring two or more factors, such as something the user knows (e.g. password), something the user has (e.g. phone), or something the user is (e.g. fingerprint). MFA is an effective deterrent for phishing attacks, which are attempts to trick users into revealing their credentials or other sensitive information by sending them fraudulent emails or websites that impersonate legitimate entities. MFA can prevent phishing attacks by adding an extra layer of security that is not easily compromised by the attackers, even if they manage to obtain the user's password. For example, if the user receives a phishing email that asks them to log in to their bank account, and they enter their password on the fake website, the attacker will not be able to access the account unless they also have the user's phone or fingerprint. MFA can also alert the user of a phishing attempt if they receive an unexpected authentication request on their phone or other device. Reference:

What Type of Attacks Does MFA Prevent? | OneLogin
Multi-Factor Authentication and Cyberattacks - NYU

www.atmicnetworks.com

Question: 406

[Security Concepts]
Which solution for remote workers enables protection, detection, and response on the endpoint against known and unknown threats?

A. Cisco AMP for Endpoints
B. Cisco AnyConnect
C. Cisco Umbrella
D. Cisco Duo

Answer: A

Explanation:

Cisco AMP for Endpoints is a solution that enables protection, detection, and response on the endpoint against known and unknown threats. It provides continuous visibility and analysis of endpoint activity, as well as automated threat prevention and response capabilities. It leverages cloud-based intelligence, sandboxing, and machine learning to block malware, fileless attacks, ransomware, and other advanced threats. It also allows security teams to quickly investigate and remediate incidents, as well as hunt for indicators of compromise across all endpoints. Cisco AMP for Endpoints is part of the Cisco SecureX platform, which integrates with other Cisco security solutions to provide a unified and simplified security experience. The other options are not correct because they do not offer the same level of endpoint protection, detection, and response as Cisco AMP for Endpoints. Cisco AnyConnect is a VPN solution that provides secure access to the network for remote workers, but it does not monitor or respond to endpoint threats. Cisco Umbrella is a DNS security solution that blocks malicious domains, IPs, and URLs, but it does not analyze or remediate endpoint activity. Cisco Duo is a multi-factor authentication solution that verifies the identity of users and devices, but it does not protect or detect endpoint attacks. Reference := Some possible references are:
Cisco AMP for Endpoints
Cisco SecureX
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 - Module 5: Endpoint Protection and Detection

Question: 407

[Endpoint Protection and Detection]
Which Cisco platform provides an agentless solution to provide visibility across the network including encrypted traffic analytics to detect malware in encrypted traffic without the need for decryption?

A. Cisco Advanced Malware Protection
B. Cisco Stealthwatch
C. Cisco Identity Services Engine
D. Cisco AnyConnect

Answer: B

Explanation:

Cisco Stealthwatch is a network security and visibility platform that provides an agentless solution to monitor network traffic and detect threats, including those in encrypted traffic. Stealthwatch uses Encrypted Traffic Analytics (ETA), a technology that leverages network telemetry and machine learning to identify malicious patterns and behaviors in encrypted traffic without decryption. ETA can also assess the cryptographic strength and compliance of the encryption protocols used in the network. Stealthwatch integrates with other Cisco security products, such as Cisco Identity Services Engine (ISE) and Cisco Advanced Malware Protection (AMP), to provide contextual information and threat intelligence for faster and more effective response. Stealthwatch is the only Cisco platform that offers ETA as a solution to provide visibility across the network, including encrypted traffic analytics, to detect malware in encrypted traffic without the need for decryption. Reference :=

Some possible references are:
Cisco Secure Network Analytics (Stealthwatch) - Cisco, Cisco
Encrypted Traffic Analytics > Security | Cisco Press, Cisco Press
Solutions - Encrypted Traffic Analytics with the New Cisco Network and Secure Network Analytics Ata-Glance - Cisco, Cisco
Cisco Encrypted Traffic Analytics White Paper, Cisco

Question: 408

[Secure Network Access, Visibility, and Enforcement]
Which two Cisco ISE components must be configured for BYOD? (Choose two.)

A. local WebAuth
B. central WebAuth
C. null WebAuth
D. guest
E. dual

Answer: B,D

Explanation:

Cisco ISE supports two types of WebAuth for BYOD: central WebAuth and local WebAuth. Central WebAuth is the default method and it uses the ISE portal to authenticate the users and redirect them to the BYOD portal. Local WebAuth is an alternative method that uses the network access device (NAD) portal to authenticate the users and then redirects them to the ISE BYOD portal. Both methods require the configuration of a guest component on ISE, which is used to create the BYOD portal and the guest user accounts. The guest component also provides the self-service onboarding and registration features for the BYOD users. The dual component is not related to BYOD, but rather to the dual-SSID method, which uses two separate SSIDs for provisioning and access. The null WebAuth component is not a valid option for BYOD.
Reference :=
Some possible references are:
Cisco ISE BYOD Prescriptive Deployment Guide

Configure Single SSID Wireless BYOD on Windows and ISE
Cisco ISE for BYOD and Secure Unified Access, 2nd Edition

Question: 409

[Security Concepts]
Which system performs compliance checks and remote wiping?

A. MDM
B. ISE
C. AMP
D. OTP

Answer: A

Explanation:

MDM stands for Mobile Device Management, which is a system that performs compliance checks and remote wiping on mobile devices. MDM allows administrators to enforce security policies, monitor device status, and remotely manage devices in case of loss, theft, or compromise. MDM can also integrate with other Cisco security solutions, such as ISE, AMP, and Umbrella, to provide enhanced protection and visibility for mobile devices. Reference:
Mobile Device Management (MDM) - Cisco
Implementing and Operating Cisco Security Core Technologies (SCOR) - Module 5: Secure Network Access

Question: 410

[Content Security]
An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?

A. single interface
B. multi-context
C. transparent
D. two-interface

Answer: D

Explanation:

To enable a separated email transfer flow from the Internet and from the LAN, the engineer must use the two-interface deployment mode on the Cisco WSA. This mode allows the WSA to have two separate network interfaces, one for the Internet traffic and one for the LAN traffic. This way, the WSA can apply different policies and settings for each interface,

and isolate the email flows from each other. The two-interface mode also provides better performance and security than the singleinterface mode, which uses only one network interface for both Internet and LAN traffic12. The other deployment modes, such as multi-context, transparent, or single-interface, do not support a separated email transfer flow from the Internet and from the LAN. Reference: Two-interface mode, section “Deployment”. WSA network configuration, section “Interfaces”.

Question: 411

[Secure Network Access, Visibility, and Enforcement]

A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)

A. RADIUS communication must be permitted between the ISE server and the domain controller.
B. The ISE account must be a domain administrator in Active Directory to perform JOIN operations.
C. Active Directory only supports user authentication by using MSCHAPv2.
D. LDAP communication must be permitted between the ISE server and the domain controller.
E. Active Directory supports user and machine authentication by using MSCHAPv2.

Answer: A,D

Explanation:

To implement external authentication against Active Directory, the Cisco ISE server needs to communicate with the domain controller using either RADIUS or LDAP protocols. RADIUS is used for network access control, while LDAP is used for identity management and directory services. Both protocols require the appropriate ports to be opened and firewall rules to be configured to allow the traffic between the ISE server and the domain controller.
The ISE account does not need to be a domain administrator in Active Directory to perform JOIN operations. It only needs to have the permissions to create computer objects and reset passwords in the domain. This can be achieved by delegating the rights to a specific OU or using a service account with limited privileges.
Active Directory supports user and machine authentication by using various methods, not only MSCHAPv2. MSCHAPv2 is a challenge-response authentication protocol that is commonly used with RADIUS and VPN connections. However, Active Directory also supports other protocols such as Kerberos, NTLM, EAP, and PEAP, depending on the scenario and the client capabilities.

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0
Cisco ISE Integration with Microsoft Active Directory RADIUS vs. LDAP: What’s the Difference?
MS-CHAP v2 Authentication

Question: 412

[Endpoint Protection and Detection]

Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or

Microsoft vSwitch?

A. inter-EPG isolation
B. inter-VLAN security
C. intra-EPG isolation
D. placement in separate EPGs

Answer: C

Explanation:

Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another.

Question: 413

[Content Security]
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)

A. Create an LDAP authentication realm and disable transparent user identification.
B. Create NTLM or Kerberos authentication realm and enable transparent user identification.
C. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
D. The eDirectory client must be installed on each client workstation.
E. Deploy a separate eDirectory server; the dent IP address is recorded in this server.

Answer: B,C

Explanation:

A network administrator can transparently identify users using Active Directory on the Cisco WSA in two ways:
Create NTLM or Kerberos authentication realm and enable transparent user identification. This option allows the WSA to use the NTLM or Kerberos protocol to authenticate users without prompting them for credentials. The WSA must join the Active Directory domain and have a valid service principal name (SPN) for this option to work1.
Deploy a separate Active Directory agent such as Cisco Context Directory Agent (CDA). This option allows the WSA to receive user-to-IP mappings from the CDA, which monitors the Active Directory domain controllers for user logon events. The CDA must be installed on a Windows server and have access to the domain controllers and the WSA2.
The other options are not ways to transparently identify users using Active Directory on the Cisco WSA. Creating an LDAP authentication realm and disabling transparent user identification will require users to enter their credentials manually. Installing the eDirectory client on each client workstation or deploying a separate eDirectory server are not related to Active Directory, but to

Novell eDirectory, which is a different directory service3.
Reference := 1: User Guide for AsyncOS 11.0 for Cisco Web Security Appliances, Chapter: Acquire End-User Credentials, Topic: Active Directory/Kerberos, page 4-3. 2: User Guide for AsyncOS 11.0 for Cisco Web Security Appliances, Chapter:

Acquire End-User Credentials, Topic: Active Directory Agent, page 4-5. 3: User Guide for AsyncOS 11.0 for Cisco Web Security Appliances, Chapter: Acquire EndUser Credentials, Topic: eDirectory, page 4-8.

Question: 414

[Security Concepts]
Which baseline form of telemetry is recommended for network infrastructure devices?

A. SDNS
B. NetFlow
C. passive taps
D. SNMP

Answer: B

Explanation:

NetFlow is a baseline form of telemetry that is recommended for network infrastructure devices. NetFlow is a technology that collects and exports information about IP traffic flows on enabled interfaces. NetFlow can provide valuable insight into the network performance, utilization, behavior, and security. NetFlow can help identify anomalies, such as DDoS attacks, malware, or misconfigurations, by comparing the current traffic patterns with the normal or baseline ones. NetFlow can also help with capacity planning, troubleshooting, and forensic analysis. NetFlow is supported on various Cisco platforms, such as routers, switches, firewalls, and IPS sensors. NetFlow can export data to different collectors and analyzers, such as Cisco Security Monitoring, Analysis and Response System (CS-MARS), Cisco Traffic Anomaly Detectors and Cisco Guard DDoS Mitigation Appliances, Cisco Network Analysis Module (NAM), and other third-party tools.
Reference:

Question: 415

[Endpoint Protection and Detection]
In which scenario is endpoint-based security the solution?

A. inspecting encrypted traffic
B. device profiling and authorization
C. performing signature-based application control
D. inspecting a password-protected archive

Answer: C

Explanation:

Endpoint-based security is the solution for performing signature-based application control, which is a method of identifying and blocking malicious applications based on their signatures or hashes. Signature-based application control is one of the features of endpoint security solutions, such as Cisco AMP for Endpoints1, that protect endpoints from known

and unknown threats. Endpoint security solutions can also perform other functions, such as behavioral analysis, sandboxing, machine learning, and threat hunting, to provide comprehensive protection, detection, and response on the endpoint2. The other options are not scenarios where endpoint-based security is the solution. Inspecting encrypted traffic requires a network-based security solution, such as Cisco SSL Appliance3, that can decrypt and inspect the traffic for malicious content. Device profiling and authorization requires a network access control solution, such as Cisco Identity Services Engine4, that can identify and authenticate devices and users and enforce policies based on their roles and contexts. Inspecting a password-protected archive requires a file analysis solution, such as Cisco Threat Grid5, that can extract and analyze the contents of the archive for malware and indicators of compromise. Reference :=

Cisco AMP for Endpoints

What is Endpoint Security? How Does It Work?

Cisco SSL Appliance

Cisco Identity Services Engine

Cisco Threat Grid

Question: 416

[Security Concepts]

```
def dnac_login(host, username, password):
    url = "https://{}/api/system/v1/auth/token".format(host)
    response = requests.request("POST", url,
auth=HTTPBasicAuth(username, password),
                                headers=headers, verify=False)
    return response.json() ["Token"]
```

Refer to the exhibit. What is the result of the Python script?

A. It uses the POST HTTP method to obtain a username and password to be used for authentication.
B. It uses the POST HTTP method to obtain a token to be used for authentication.
C. It uses the GET HTTP method to obtain a token to be used for authentication.
D. It uses the GET HTTP method to obtain a username and password to be used for authentication

Answer: B

Explanation:

The Python script is using the dnac_login function to authenticate to a Cisco DNA Center server and obtain a token that can be used for subsequent API calls. The function takes three parameters: host, username, and password. It constructs a URL for the authentication endpoint, which
is https://{}/api/system/v1/auth/token. It then uses the requests library to send a POST HTTP request to the URL, passing the username and password as HTTP Basic Authentication credentials, and setting the headers to indicate the expected content type and response format. The function also disables the SSL verification by setting the verify parameter to False. This is not recommended for production environments, as it exposes the script to potential security risks. The function then returns the token value from the JSON response, which is accessed by using the response.json() ["Token"] syntax.

The token can then be used as a bearer token for subsequent API calls to the Cisco DNA Center server. Reference: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 9: Content Security, Lesson 9.3: Cisco DNA Center APIs
Cisco DNA Center Platform API Reference, Authentication API
Refer to the exhibit. What will happen when the Python script is executed?

Question: 417

[Endpoint Protection and Detection]
Why is it important to patch endpoints consistently?

A. Patching reduces the attack surface of the infrastructure.
B. Patching helps to mitigate vulnerabilities.
C. Patching is required per the vendor contract.
D. Patching allows for creating a honeypot.

Answer: B

Explanation:

Patching helps to mitigate vulnerabilities by applying fixes or updates to software or firmware that have known security flaws. Vulnerabilities can be exploited by cybercriminals to compromise the confidentiality, integrity, or availability of the IT systems and data. Patching endpoints consistently reduces the risk of cyberattacks and data breaches by closing the gaps that attackers can use to gain unauthorized access or cause damage. Patching also improves the performance and functionality of the IT systems by addressing bugs or errors12.
Option B is the correct answer, as it explains the main benefit of patching endpoints consistently. Option A is incorrect, as patching does not necessarily reduce the attack surface of the infrastructure, which is the total number of possible entry points for an attacker. Patching only addresses the
existing vulnerabilities in the software or firmware, but does not eliminate the attack surface itself. Option C is incorrect, as patching is not always required per the vendor contract, although some vendors may provide support or incentives for patching. Option D is incorrect, as patching does not allow for creating a honeypot, which is a decoy system that is intentionally left vulnerable to lure and trap attackers. Reference: Patch Management Overview, Challenges, and Recommendations. Patch Management Explained: Challenges, Best Practices & Steps.

Question: 418

[Security Concepts]
Which two parameters are used for device compliance checks? (Choose two.)

A. endpoint protection software version
B. Windows registry values
C. DHCP snooping checks
D. DNS integrity checks
E. device operating system version

Answer: A,E

Explanation:

Device compliance checks are used to verify that the devices managed by Intune meet the security and configuration requirements defined by the organization. Device compliance checks can use various parameters to evaluate the device state, such as:

Endpoint protection software version: This parameter checks if the device has a valid and up-to-date antivirus or antimalware software installed and running. This parameter helps to protect the device from malicious software and network attacks.

Device operating system version: This parameter checks if the device has the minimum or maximum operating system version supported by the organization. This parameter helps to ensure that the device has the latest security patches and features available.

Windows registry values: This parameter checks if the device has specific registry values configured or not. This parameter helps to enforce custom settings or policies on the device that are not covered by other parameters.

DHCP snooping checks: This parameter checks if the device is connected to a trusted network that uses DHCP snooping to prevent rogue DHCP servers from assigning IP addresses to the device. This parameter helps to prevent man-in-the-middle attacks and network spoofing.

DNS integrity checks: This parameter checks if the device is using a secure and reliable DNS server that can resolve domain names correctly and prevent DNS hijacking or poisoning. This parameter helps to prevent phishing and redirection attacks.

Reference :=

Some possible references are:

Device compliance policies in Microsoft Intune | Microsoft Learn, Microsoft

Monitor results of your device compliance policies in Microsoft Intune | Microsoft Learn, Microsoft

Check device access | Microsoft Learn, Microsoft

Ensure device compliance - Configuration Manager | Microsoft Learn, Microsoft

Question: 419

[Securing the Cloud]

Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?

A. Cisco Defense Orchestrator
B. Cisco Configuration Professional
C. Cisco Secureworks
D. Cisco DNAC

Answer: A

Explanation:

Cisco Defense Orchestrator (CDO) is a cloud-based management solution that allows you to manage security policies and

www.atmicnetworks.com

device configurations with ease across multiple Cisco and cloud-native security platforms. CDO centrally manages elements of policy and configuration across Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS1. CDO also provides visibility, automation, and orchestration capabilities to simplify and unify security operations2. The other options are not cloud security software that can centrally manage policies on multiple platforms. Cisco Configuration Professional is a device management tool for Cisco routers and switches. Cisco Secureworks is a security services provider that offers threat intelligence and incident response. Cisco DNAC is a network controller that automates and assures services across campus, branch, and edge networks. Reference := Cisco Defense Orchestrator Data Sheet
Cisco Defense Orchestrator

Question: 420

[Endpoint Protection and Detection]
Which Cisco security solution determines if an endpoint has the latest OS updates and patches installed on the system?

A. Cisco Endpoint Security Analytics
B. Cisco AMP for Endpoints
C. Endpoint Compliance Scanner
D. Security Posture Assessment Service

Answer: B

Explanation:

Cisco AMP for Endpoints is the Cisco security solution that determines if an endpoint has the latest OS updates and patches installed on the system. Cisco AMP for Endpoints is a cloud-based endpoint protection platform that provides advanced malware prevention, detection, and response capabilities. One of the features of Cisco AMP for Endpoints is the Endpoint Compliance Scanner, which allows administrators to create and enforce policies that check the compliance status of endpoints based on various criteria, such as OS version, patch level, antivirus status, firewall status, and more. The Endpoint Compliance Scanner can also remediate non-compliant endpoints by applying patches, updating antivirus signatures, enabling firewall, and so on. By using the Endpoint Compliance Scanner, administrators can ensure that all endpoints are up to date and secure against known vulnerabilities and threats. Reference:
Cisco AMP for Endpoints
Endpoint Compliance Scanner
Implementing and Operating Cisco Security Core Technologies (SCOR) - Module 4: Endpoint Protection and Detection

Question: 421

[Security Concepts]
A network administrator is configuring a role in an access control policy to block certain URLs and selects the "Chat and instant Messaging" category. which reputation score should be selected to accomplish this goal?

A. 3

B. 5

C. 10

D. 1

Answer: B

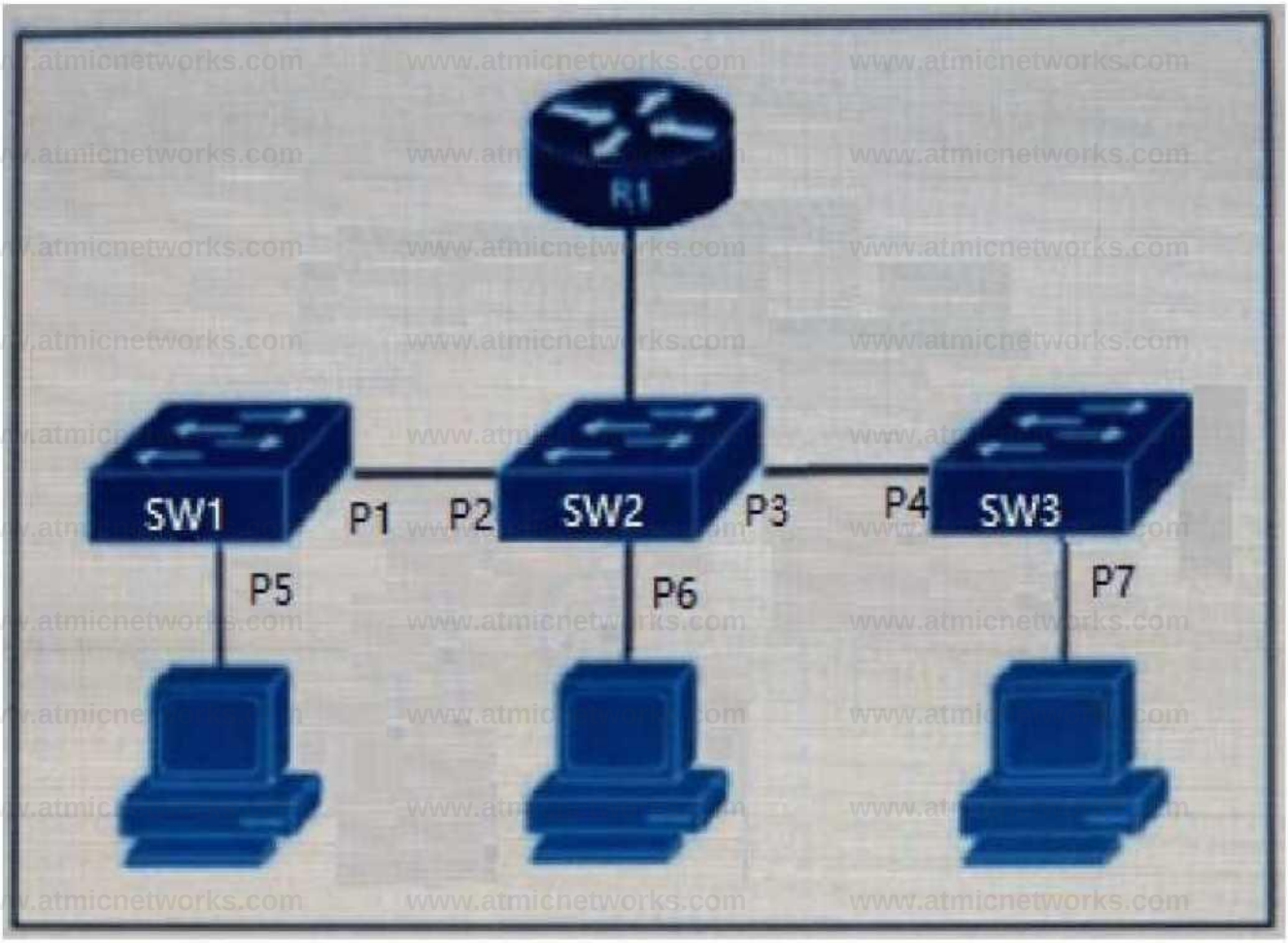
Explanation:

To block certain URLs based on the “Chat and Instant Messaging” category, the network administrator should select a reputation score of 5. A reputation score is a numerical value that indicates the likelihood of a URL being malicious or unwanted. The lower the score, the higher the risk. A score of 5 means that the URL is suspicious or potentially harmful, and should be blocked or inspected12. A score of 3 means that the URL is unknown or unverified, and may be allowed or blocked depending on the policy settings12. A score of 10 means that the URL is trustworthy or benign, and should be allowed12. A score of 1 means that the URL is malicious or high-risk, and

should be blocked12. Therefore, a score of 5 is the most appropriate to block the "Chat and Instant Messaging" category, which may contain unwanted or problematic websites. Reference: Reputation score, section "Reputation score". Web content filtering, section "What is web content filtering?".

Question: 422

[Security Concepts] Refer to the exhibit.



The DHCP snooping database resides on router R1, and dynamic ARP inspection is configured only on switch SW2. Which ports must be configured as untrusted so that dynamic ARP inspection operates normally?

A. P2 and P3 only
B. P5, P6, and P7 only
C. P1, P2, P3, and P4 only
D. P2, P3, and P6 only

Answer: D

Explanation:

P2, P3, and P6 only. Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network and

prevents ARP spoofing attacks. DAI relies on the DHCP snooping database to verify the IP-to-MAC bindings of hosts on the network. DAI operates on untrusted ports, which are ports that connect to hosts or devices that generate ARP traffic. Trusted ports are ports that connect to other switches or routers that do not generate ARP traffic.

In this scenario, the DHCP snooping database resides on router R1, which means that switch SW2 needs to trust the port P3 that connects to R1. This way, SW2 can receive the DHCP snooping information from R1 and populate its own database. The port P4 that connects to switch SW3 also needs to be trusted, because SW3 does not generate ARP traffic. The ports P2 and P6 that connect to hosts P6 and P7 need to be untrusted, because they generate ARP traffic and need to be validated by DAI. The port P1 that connects to host P5 does not need to be configured as untrusted, because DAI is not enabled on switch SW1.

To understand the concept of DAI and how to configure it, you can refer to the following sections of the source book:

Section 1.1.2: Describe the concepts of network security

Section 1.1.2.8: Describe the concepts of DAI

Section 1.1.2.9: Describe the concepts of DHCP snooping

Section 1.1.2.10: Describe the concepts of trusted and untrusted ports

Section 1.1.2.11: Describe the concepts of DAI configuration

Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Understanding and Configuring Dynamic ARP Inspection

DHCP Snooping and Dynamic ARP Inspection

Question: 423

[Secure Network Access, Visibility, and Enforcement]

An engineer is configuring device-hardening on a router in order to prevent credentials from being seen if the router configuration was compromised. Which command should be used?

A. service password-encryption
B. username <username> privilege 15 password <password>
C. service password-recovery
D. username < username> password <password>

Answer: A

Explanation:

The service password-encryption command is used to encrypt all passwords in the router configuration file, such as the enable password, the console password, the vty password, and the username password. This command prevents credentials from being seen if the router configuration was compromised, for example, by an attacker who gained access to the router or the backup files. The encryption used by this command is a weak algorithm that can be easily reversed, but it provides some level of protection against casual observers1.

The other commands are not used to encrypt passwords in the router configuration file. The username <username> privilege 15 password <password> and the username <username> password <password> commands are used to create local user accounts with or without administrative privileges, respectively. These commands store the passwords in clear text unless the service password-encryption command is enabled2. The service password-recovery command is used to enable or disable the password recovery mechanism on the router. This command does not affect the encryption of passwords in the configuration file3.

Reference := 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Security Concepts, Lesson 1.2: Securing Network Devices, Topic 1.2.1: Device Hardening, page 114. 2: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Security Concepts, Lesson 1.2: Securing Network Devices, Topic 1.2.2: Management Plane Security, page 117. 3: Cisco IOS Configuration Fundamentals Command Reference, Release 12.2, Chapter: service password-recovery, page 1.

Question: 424

[Security Concepts]

Which security solution protects users leveraging DNS-layer security?

A. Cisco ISE
B. Cisco FTD
C. Cisco Umbrella
D. Cisco ASA

Answer: C

Explanation:

DNS-layer security is a method of protecting users from cyberthreats by blocking malicious or risky domains before a connection is established. Cisco Umbrella is a cloud-based service that provides DNS-layer security by using Cisco Talos threat intelligence to filter DNS requests and prevent access to malicious domains. Cisco Umbrella also offers other security features, such as web filtering, cloud- delivered firewall, secure web gateway, and cloud access security broker. Cisco Umbrella can protect users on and off the corporate network, regardless of their location or device. Cisco Umbrella is compatible with other Cisco security solutions, such as Cisco ISE, Cisco FTD, and Cisco ASA, but it is the only one that offers DNS-layer security as a core capability. Reference:

What Is DNS Security? How Does It Work? - Cisco Umbrella

Why Umbrella DNS Security? - Cisco Umbrella

Question: 425

[Secure Network Access, Visibility, and Enforcement]

Which CoA response code is sent if an authorization state is changed successfully on a Cisco IOS device?

A. CoA-NCL B. CoA-NAK C. CoA-MAB D. CoA-ACK

Answer: D

Explanation:

CoA-ACK is the CoA response code that is sent if an authorization state is changed successfully on a Cisco IOS device. CoA-ACK stands for CoA acknowledgment, which indicates that the device has received and processed the CoA request from

the server and applied the new authorization settings to the session. The attributes returned within a CoA-ACK can vary based on the CoA request, such as session reauthentication, session termination, or session modification. The other options are not correct because they are not valid CoA response codes. CoA-NCL, CoA-NAK, and CoA-MAV are not defined in RFC 5176, which specifies the CoA protocol. CoA-NAK is the closest option, but it stands for CoA non-acknowledgment, which indicates that the device has rejected the CoA request from the server due to some error or inconsistency.

Reference := Some possible references are:

RADIUS Change of Authorization - Cisco

Security and VPN Configuration Guide, Cisco IOS XE 17.x

RFC 5176 - Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

Question: 426

[Security Operations]

Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

A. Cisco CTA
B. Cisco Stealthwatch
C. Cisco Encrypted Traffic Analytics
D. Cisco Umbrella

Answer: B

Explanation:

Cisco Stealthwatch is a security solution that uses NetFlow to provide visibility across the network, data center, branch offices, and cloud. NetFlow is a protocol that collects and exports statistics on network traffic flows from routers, switches, firewalls, and other devices. NetFlow data can be used to monitor network performance, troubleshoot issues, detect anomalies, and identify security threats. Cisco Stealthwatch analyzes NetFlow data from various sources and correlates it with other contextual information, such as identity, device, location, and threat intelligence. Cisco Stealthwatch then applies advanced behavioral analytics and machine learning to detect and respond to malicious activities, such as data exfiltration, malware infection, insider threats, and denial-of-service attacks. Cisco Stealthwatch also provides comprehensive network visibility and security across hybrid environments, including public cloud, private cloud, and on-premises networks. Cisco Stealthwatch can integrate with other Cisco security solutions, such as Cisco Identity Services Engine (ISE), Cisco Firepower, Cisco Umbrella, and Cisco Advanced Malware Protection (AMP), to enhance network security and incident response capabilities. Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 8: Cloud and Virtual Network Security, Lesson 8.2: Cisco Stealthwatch Cloud

Cisco Stealthwatch

NetFlow for Cybersecurity and Incident Response B

Question: 427

[Content Security]
How does a WCCP-configured router identify if the Cisco WSA is functional?

A. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the router.
B. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longertransmitted to the WSA.
C. The WSA sends a Here-I-Am message every 10 seconds, and the router acknowledges with an ISee-You message.
D. The router sends a Here-I-Am message every 10 seconds, and the WSA acknowledges with an ISee-You message.

Answer: D

Explanation:

The WCCP-configured router identifies if the Cisco WSA is functional by exchanging periodic messages with the WSA. The WSA sends a Here-I-Am message every 10 seconds to the router, which contains information such as the WSA's IP address, service group, and hash assignment. The router responds with an I-See-You message, which acknowledges the receipt of the Here-I-Am message and provides information such as the router's IP address, service group, and view of the WCCP topology. These messages allow the router and the WSA to maintain a bidirectional communication and to detect any changes or failures in the WCCP network12.
Option C is the correct answer, as it describes the correct message exchange between the WCCP- configured router and the Cisco WSA. Option A is incorrect, as the router does not use ICMP ping to check the WSA's functionality, and the traffic is not transmitted to the router, but redirected by the router. Option B is incorrect, as the router does not use ICMP ping to check the WSA's functionality, and the traffic is not transmitted to the WSA, but redirected by the WSA. Option D is incorrect, as the router does not send a Here-I-Am message, but an I-See-You message, and the WSA does not acknowledge with an I-See-You message, but a Here-I-Am message. Reference: WCCP Router Configuration Example - Cisco. Cisco ASA WCCP Traffic Redirection Guide - Cisco.

Question: 428

[Security Concepts]
Which solution supports high availability in routed or transparent mode as well as in northbound and southbound deployments?

A. Cisco FTD with Cisco ASDM
B. Cisco FTD with Cisco FMC
C. Cisco Firepower NGFW physical appliance with Cisco. FMC
D. Cisco Firepower NGFW Virtual appliance with Cisco FMC

Answer: B

Explanation:

Question: 429

[Security Concepts]
Which Cisco ASA Platform mode disables the threat detection features except for Advanced Threat Statistics?

A. cluster
B. transparent
C. routed
D. multiple context

Answer: B

Explanation:

Question: 430

[Network Security]
Which benefit does DMVPN provide over GETVPN?

A. DMVPN supports QoS, multicast, and routing, and GETVPN supports only QoS.
B. DMVPN is a tunnel-less VPN, and GETVPN is tunnel-based.
C. DMVPN supports non-IP protocols, and GETVPN supports only IP protocols.
D. DMVPN can be used over the public Internet, and GETVPN requires a private network.

Answer: D

Explanation:

Question: 431

[Endpoint Protection and Detection]
An organization has DHCP servers set up to allocate IP addresses to clients on the LAN. What must be done to ensure the LAN switches prevent malicious DHCP traffic while also distributing IP addresses to the correct endpoints?

www.atmicnetworks.com

A. Configure Dynamic ARP inspection and add entries in the DHCP snooping database.
B. Configure DHCP snooping and set trusted interfaces for all client connections.
C. Configure Dynamic ARP inspection and antispoofing ACLs in the DHCP snooping database.
D. Configure DHCP snooping and set a trusted interface for the DHCP server.

Answer: B

Explanation:
Reference:
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multiboo
k/configuration_guide/b_consolidated_config_guide_3850_chapter_0110101.html

Question: 432

[Security Concepts]
Which two parameters are used to prevent a data breach in the cloud? (Choose two.)

A. DLP solutions
B. strong user authentication
C. encryption
D. complex cloud-based web proxies
E. antispoofing programs

Answer: A,B

Explanation:

Question: 433

[Security Concepts]
Which technology enables integration between Cisco ISE and other platforms to gather and share network and vulnerability data and SIEM and location information?

A. pxGrid
B. NetFlow
C. SNMP
D. Cisco Talos

Answer: A

Explanation:

Question: 434

[Security Concepts]

Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DNA Center?

A. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device/count

B. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device

C. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/networkdevice?parameter1=value&param eter2=value& .....

D. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v 1/networkdevice/startIndex/recordsToReturn

Answer: A

Explanation:

Question: 435

[Network Security]

An organization must add new firewalls to its infrastructure and wants to use Cisco ASA or Cisco FTD. The chosen firewalls must provide methods of blocking traffic that include offering the user the option to bypass the block for certain sites after displaying a warning page and to reset the connection. Which solution should the organization choose?

A. Cisco FTD because it supports system rate level traffic blocking, whereas Cisco ASA does not

B. Cisco ASA because it allows for interactive blocking and blocking with reset to be configured via the GUI, whereas Cisco FTD does not.

C. Cisco FTD because it enables interactive blocking and blocking with reset natively, whereas Cisco ASA does not

D. Cisco ASA because it has an additional module that can be installed to provide multiple blocking capabilities, whereas Cisco FTD does not.

Answer: C

Explanation:

Question: 436

[Security Concepts]

www.atmicnetworks.com

An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway. The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?

A. third-party
B. self-signed
C. organization owned root
D. SubCA

Answer: C

Explanation:

Question: 437

[Security Concepts]
An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?

A. monitor
B. allow
C. block
D. trust

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/access_control_using_intrusion_and_file_policies.html#:~:text=File%20Policies-,Access%20Control%20Traffic%20Handling%20with%20Intrusion%20and%20File%20Policies,-The%20following%20diagram

the first three access control rules in the policy—Monitor, Trust, and Block—cannot inspect matching traffic. Monitor rules track and log but do not inspect network traffic, so the system continues to match traffic against additional rules to determine whether to permit or deny it

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/access_control_rules.html#:~:text=Rule%20Blocking%20Actions-,Access%20Control%20Rule%20Allow%20Action,network%20discovery%20policy%3B%20additionally%2C%20application%20discovery%20is%20limited%20for%20encrypted%20sessions.,-Related%20Concepts

www.atmicnetworks.com

Question: 438

[Security Operations]
When NetFlow is applied to an interface, which component creates the flow monitor cache that is used to collect traffic based on the key and nonkey fields in the configured record?

A. records
B. flow exporter
C. flow sampler
D. flow monitor

Answer: D

Explanation:

A flow monitor is a component of Flexible NetFlow that is used to store and export flow data. A flow monitor consists of a record, an optional exporter, and a cache. The cache is a section of memory that stores flow entries before they are exported to an external collector. The cache is created by the flow monitor when NetFlow is applied to an interface. The cache collects traffic based on the key and nonkey fields in the configured record. The key fields are used to identify a flow uniquely, while the nonkey fields are used to provide additional information about the flow. The cache can be configured with various parameters, such as the number of entries, the timeout values, and the type of cache. The cache can also be viewed and cleared using show and clear commands. Reference := Some possible references are:
Flexible Netflow Configuration Guide, Cisco IOS Release 15M&T
ASR9000/XR Netflow Architecture and overview
Cisco IOS Flexible NetFlow Command Reference - cache (Flexible NetFlow) through match flow

Question: 439

[Network Security]
Which encryption algorithm provides highly secure VPN communications?

A. 3DES
B. AES 256
C. AES 128
D. DES

Answer: B

Explanation:

AES (Advanced Encryption Standard) is a symmetric encryption algorithm that uses the same key to encrypt and decrypt data. It turns plain text into a code that only the intended recipient can read. AES has different key sizes, such as 128, 192, and 256 bits. The larger the key size, the more secure and complex the encryption is. AES 256 is the most secure encryption algorithm for VPN communications, as it uses a 256-bit key that would take an enormous amount of time and

computing power to crack. AES 256 is widely used by VPN providers, as it offers a high level of security and performance for VPN tunnels. AES 256 is also recommended by the U.S. government for protecting classified information. Reference :=

How Does a VPN Securely Encrypt Your Connection?

What Is VPN Encryption, Types, Protocols And Algorithms Explained

What is AES (Advanced Encryption Standard)?

What is VPN Encryption & How Does it Work?

Question: 440

[Security Concepts]

An administrator needs to configure the Cisco ASA via ASDM such that the network management system can actively monitor the host using SNMPv3. Which two tasks must be performed for this configuration? (Choose two.)

A. Specify the SNMP manager and UDP port.
B. Specify an SNMP user group
C. Specify a community string.
D. Add an SNMP USM entry
E. Add an SNMP host access entry

Answer: B,D

Explanation:

To configure the Cisco ASA via ASDM for SNMPv3, the administrator needs to perform two main tasks: specify an SNMP user group and add an SNMP USM entry. An SNMP user group defines the access level and security model for a group of SNMP users. An SNMP USM entry defines the authentication and encryption parameters for a specific SNMP user. These two tasks are required for SNMPv3 because it uses a user-based security model (USM) that provides secure access to the MIB objects. SNMPv3 does not use a community string, which is a shared password used by SNMPv1 and SNMPv2c. The SNMP manager and UDP port are optional parameters that can be specified to customize the SNMP communication. The SNMP host access entry is also optional and can be used to restrict the access of SNMP hosts to specific interfaces or networks. Reference :=

Some possible references are:

SNMP Configuration, Verification and Troubleshooting on ASA

How to configure SNMP v3 on Cisco Switch, Router, ASA, Nexus

SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

Question: 441

[Security Concepts]

Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?

A. routed mode
B. transparent mode
C. single context mode
D. multiple context mode

Answer: B

Explanation:

Transparent mode is a Cisco ASA deployment model that allows the ASA to act as a bump in the wire, or a stealth firewall. In this mode, the ASA does not have an IP address on the network, and it does not participate in routing. Instead, it filters traffic between hosts in the same IP subnet using higher-level protocols such as TCP, UDP, and ICMP. Transparent mode is useful when you want to apply security policies without readdressing the network or changing the default gateway of the hosts. Some of the benefits of transparent mode are:

It preserves the original source and destination IP addresses of the packets, which can be useful for logging and auditing purposes.

It simplifies the configuration of the ASA, as you do not need to configure routing protocols, NAT, or DHCP.

It allows the ASA to inspect non-IP traffic, such as ARP, STP, and CDP.

It supports multiple contexts, which can provide logical separation of traffic for different tenants or customers.

Some of the limitations of transparent mode are:

It does not support VPN, dynamic routing, multicast routing, or QoS.

It requires the use of EtherType ACLs to filter non-IP traffic, which can be complex and cumbersome. It requires the use of bridge groups and bridge domains to define the interfaces and VLANs that belong to the same broadcast domain.

It requires the use of MAC address learning and aging to maintain a MAC address table for each bridge group.

Reference :=

Some possible references are:

Cisco ASA Series Firewall CLI Configuration Guide, 9.10 - Transparent Firewall Mode Deploying ASA - Cisco

Cisco ASA 5500-X Series Firewalls - Configuration Guides - Cisco

Question: 442

[Security Concepts]

Which function is performed by certificate authorities but is a limitation of registration authorities?

A. accepts enrollment requests
B. certificate re-enrollment
C. verifying user identity
D. CRL publishing

Answer: D

Explanation:

Certificate authorities (CAs) are responsible for issuing, renewing, revoking, and publishing digital certificates. They also maintain a certificate revocation list (CRL), which is a database of revoked certificates that can be checked by relying parties to verify the validity of a certificate. Registration authorities (RAs) are entities that assist CAs with the verification of user identities and enrollment requests. They do not issue certificates themselves, nor do they have access to the CRL. Therefore, CRL publishing is a function that is performed by CAs but is a limitation of RAs. Reference := Some possible references are:
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Secure Connectivity, Lesson 4.1: VPN Fundamentals, Topic 4.1.1: Public Key Infrastructure (PKI) Easy guide to SSL certificate authorities, Namecheap
How exactly are registration authorities related to certificate authorities?, Information Security Stack Exchange

Question: 443

[Content Security]
Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)

A. blocks malicious websites and adds them to a block list
B. does a real-time user web browsing behavior analysis
C. provides a defense for on-premises email deployments
D. uses a static algorithm to determine malicious
E. determines if the email messages are malicious

Answer: B,E

Explanation:

Cisco Advanced Phishing Protection (AAP) is a solution that helps organizations protect against fraudulent senders and identity deception-based attacks, such as business email compromise (BEC) and spear phishing. AAP uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to perform two main functions12:
It determines if the email messages are malicious by assessing the threat posture of the sender and the content of the message. It also validates the reputation and authenticity of the sender by checking various indicators, such as the domain, the IP address, the SPF, DKIM, and DMARC records, the display name, the reply-to address, and the header information. AAP assigns a risk score to each email message and provides a verdict of clean, malicious, or suspicious. It also adds a banner to the email message to inform the recipient of the risk level and the recommended action.
It does a real-time user web browsing behavior analysis by monitoring the user's interaction with the email message and the links embedded in it. It tracks the user's clicks, mouse movements, dwell time, and other indicators to detect any signs of hesitation, confusion, or curiosity. It also analyzes the destination URL of the links and compares it with the known malicious websites. If AAP detects any anomalous or risky behavior, it intervenes with a warning message or a redirect page to educate the user and prevent them from falling victim to the phishing attack. Reference := 1: Cisco's Security Innovations to Protect the Endpoint and Email 2: Cisco Advanced Phishing Protection - Cisco Video Portal

www.atmicnetworks.com

Question: 444

[Security Operations]
What is a feature of NetFlow Secure Event Logging?

A. It exports only records that indicate significant events in a flow.
B. It filters NSEL events based on the traffic and event type through RSVP.
C. It delivers data records to NSEL collectors through NetFlow over TCP only.
D. It supports v5 and v8 templates.

Answer: A

Explanation:

NetFlow Secure Event Logging (NSEL) is a security logging mechanism that is built on NetFlow Version 9 technology. It provides a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow, such as flow-create, flow-teardown, and flow-denied. NSEL events are triggered by the event that caused the state change in the flow. This reduces the amount of data that is exported and provides more relevant information for security analysis. NSEL also

supports periodic flow-update events, which provide byte counters over the duration of the flow. These events are usually time-driven, but may also be triggered by state changes in the flow. NSEL uses templates to describe the format of the data records that are exported through NetFlow. Each event has several record formats or templates associated with it. NSEL delivers templates and data records to configured NSEL collectors through NetFlow over UDP only. NSEL also allows filtering of NSEL events based on the traffic and event type through Modular Policy Framework, and then sends records to different collectors. The supported event types are flow-create, flow-denied, flowteardown, flow-update, and all.

Reference :=
Some possible references are:
NetFlow Secure Event Logging (NSEL) - Cisco
NetFlow Secure Event Logging (NSEL) - Cisco
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 (source book)

Question: 445

[Security Concepts]
A hacker initiated a social engineering attack and stole username and passwords of some users within a company. Which product should be used as a solution to this problem?

A. Cisco NGFW
B. Cisco AnyConnect
C. Cisco AMP for Endpoints
D. Cisco Duo

Answer: D

Explanation:

Cisco Duo is a cloud-based solution that provides multi-factor authentication (MFA) and device trust for secure access to applications and data. MFA adds an extra layer of security by requiring users to verify their identity with something they know (such as a password) and something they have (such as a phone or a hardware token). Device trust ensures that only trusted devices can access sensitive resources by checking the device health and compliance. Cisco Duo can help prevent social engineering attacks by making it harder for hackers to impersonate legitimate users or compromise their credentials. Cisco Duo can also integrate with other Cisco security products, such as Cisco AnyConnect, Cisco AMP for Endpoints, and Cisco Umbrella, to provide a comprehensive security solution. Reference :=

Cisco Duo Security

Cisco Duo: Multi-Factor Authentication

Cisco Duo: Device Trust

Cisco Security Core Technologies SCOR

Question: 446

[Security Concepts]

Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?

A. Cisco NBAR2
B. Cisco ASAV
C. Account on Resolution
D. Cisco Prime Infrastructure

Answer: A

Explanation:

Cisco NBAR2 is a classification engine that recognizes and classifies a wide variety of protocols and applications based on their deep packet inspection (DPI) signatures. NBAR2 enables the platform to identify and output various applications within the network traffic flows, such as web, email, voice, video, and so on. NBAR2 also supports custom protocols and applications, allowing the platform to classify traffic based on user-defined criteria. NBAR2 helps the platform to apply the appropriate quality of service (QoS), security, and policy for each application or protocol. Reference := Some possible references are:

Cisco NBAR2

Classifying Network Traffic Using NBAR

Next Generation NBAR (NBAR2)

Question: 447

[Secure Network Access, Visibility, and Enforcement]

Which RADIUS feature provides a mechanism to change the AAA attributes of a session after it is authenticated?

A. Authorization
B. Accounting
C. Authentication
D. CoA

Answer: D

Explanation:

CoA stands for Change of Authorization, which is a feature that allows a RADIUS server to adjust an active client session after it is authenticated. For example, CoA can be used to reauthenticate a

client, terminate a client session, or change the VLAN or group policy of a client. CoA is supported by several RADIUS vendors, including Cisco ISE. CoA is defined in RFC 5176 and uses a pushed model, where the request originates from the RADIUS server and is sent to the network device that acts as a listener. CoA requests can have two possible response codes: CoA-ACK (acknowledgment) or CoA- NAK (non-acknowledgment). Reference :=
Some possible references are:
RADIUS Change of Authorization
Change of Authorization with RADIUS (CoA) on MR Access Points
Change of Authorization with RADIUS (CoA) on MS Switches
Technical Tip: Radius COA behavior

Question: 448

[Security Concepts]
Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers and can be stopped by Cisco Umbrella?

A. DNS tunneling
B. DNS flood attack
C. cache poisoning
D. DNS hijacking

Answer: A

Explanation:

Question: 449

[Network Security]

A large organization wants to deploy a security appliance in the public cloud to form a site-to-site VPN and link the public cloud environment to the private cloud in the headquarters data center. Which Cisco security appliance meets these requirements?

A. Cisco Cloud Orchestrator
B. Cisco ASAV
C. Cisco WSAV
D. Cisco Stealthwatch Cloud

Answer: B

Explanation:

Question: 450

[Content Security]
Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco ESA?

A. webadvancedconfig
B. websecurity advancedconfig
C. outbreakconfig
D. websecurity config

Answer: B

Explanation:

Question: 451

[Security Concepts]
Which standard is used to automate exchanging cyber threat information?

A. TAXII
B. MITRE
C. IoC
D. STIX

www.atmicnetworks.com

Answer: A

Explanation:

Question: 452

[Content Security]
What is a function of the Layer 4 Traffic Monitor on a Cisco WSA?

A. blocks traffic from URL categories that are known to contain malicious content
B. decrypts SSL traffic to monitor for malicious content
C. monitors suspicious traffic across all the TCP/UDP ports
D. prevents data exfiltration by searching all the network traffic for specified sensitive information

Answer: C

Explanation:

Question: 453

[Security Concepts]
A network engineer entered the snmp-server user asmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxx command and needs to send SNMP information to a host at 10.255.255.1. Which command achieves this goal?

A. snmp-server host inside 10.255.255.1 version 3 myv7
B. snmp-server host inside 10.255.255.1 snmpv3 myv7
C. snmp-server host inside 10.255.255.1 version 3 asmith
D. snmp-server host inside 10.255.255.1 snmpv3 asmith

Answer: C

Explanation:

Question: 454

[Security Concepts] Refer to the exhibit.

```
ASA# show service-policy str

Global policy:
  Service-policy: global_policy
    Class-map: SFR
      SFR: card status Up, mode fail-open monito
                                                r-only
        Packet input 0, packet output
                                                drop 0, reset-drop 0
```

What are two indications of the Cisco Firepower Services Module configuration? (Choose two.)

A. The module is operating in IDS mode.
B. Traffic is blocked if the module fails.
C. The module fails to receive redirected traffic.
D. The module is operating in IPS mode.
E. Traffic continues to flow if the module fails.

Answer: A,E

Explanation:

sfr {fail-open | fail-close
[monitor-only]} <- There's a couple different options here. The first one is fail-open which means that if the Firepower software module is unavailable, the ASA will continue to forward traffic. fail-close means that if the Firepower module fails, the traffic will stop flowing. While this doesn't seem ideal, there might be a use case for it when securing highly regulated environments. The monitor-only switch can be used with both and basically puts the Firepower services into IDS-mode only. This might be useful for initial testing or setup.

Question: 455

[Endpoint Protection and Detection]
Why is it important for the organization to have an endpoint patching strategy?

A. so the organization can identify endpoint vulnerabilities
B. so the internal PSIRT organization is aware of the latest bugs
C. so the network administrator is notified when an existing bug is encountered
D. so the latest security fixes are installed on the endpoints

Answer: D

Explanation:

www.atmicnetworks.com

Question: 456

[Network Security]
An email administrator is setting up a new Cisco ES

A. The administrator wants to enable the blocking of greymail for the end user. Which feature must the administrator enable first?

A. File Analysis
B. IP Reputation Filtering
C. Intelligent Multi-Scan
D. Anti-Virus Filtering

Answer: C

Explanation:

Intelligent Multi-Scan (IMS) is a feature that enables the Cisco ESA to perform multiple anti-spam scans on each message and apply different actions based on the results. IMS also includes the Graymail Detection and Safe Unsubscribe services, which allow the ESA to identify and filter messages that are not strictly spam, but are low-priority or unwanted by the end user, such as newsletters, social media notifications, or marketing emails. The Graymail Detection service can classify messages into different categories, such as bulk, mass, or subscription, and assign different scores and verdicts to them. The Safe Unsubscribe service can provide a link for the end user to safely unsubscribe from the sender's mailing list, without revealing their email address or opening a malicious URL. To enable the blocking of greymail for the end user, the administrator must first enable the IMS feature globally and then configure the Graymail and Safe Unsubscribe settings in the mail policies. The administrator can also enable the centralized spam quarantine and the end-user quarantine interface to allow the end user to manage their own quarantined messages. Reference := Best Practice Guide for Anti-Spam, Anti-Virus, Graymail and Outbreak Filters
Graymail Detection and Safe Unsubscribing Functionality

Question: 457

[Security Concepts]
What limits communication between applications or containers on the same node?

A. microsegmentation
B. container orchestration
C. microservicing
D. Software-Defined Access

Answer: A

Explanation:

Microsegmentation is a technique that divides a network into smaller segments or zones, each with its own security policies and controls. This helps to isolate and protect workloads and applications from each other, and limit the lateral movement of threats within the network. Microsegmentation can be applied to different platforms and environments, such as virtual machines, containers, cloud services, and endpoints. Microsegmentation can also improve the visibility and enforcement of network traffic, as well as the performance and scalability of security solutions.

In the context of applications or containers on the same node, microsegmentation can limit the communication between them by enforcing granular policies based on attributes such as identity, context, and behavior. For example, microsegmentation can restrict which ports, protocols, or services are allowed for each application or container, and block any unauthorized or malicious traffic. Microsegmentation can also prevent the exposure of sensitive data or resources to other applications or containers on the same node, or to external attackers who may compromise one of them.

Container orchestration, microservicing, and Software-Defined Access are not directly related to limiting the communication between applications or containers on the same node. Container orchestration is a process of managing the lifecycle, deployment, and scaling of containers across a cluster of nodes. Microservicing is an architectural style of developing applications as a collection of loosely coupled, independent, and modular services. Software-Defined Access is a network architecture that abstracts the network infrastructure from the network policies, and enables consistent and secure access to any application or service across any domain. Reference: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 5: Securing the Cloud, Lesson 5.1: Describing Cloud Computing and Deployment Models, Topic 5.1.4: Microsegmentation

What Is Micro-Segmentation? - Cisco

Communicating With Docker Containers on the Same Machine - Baeldung on Ops

Question: 458

[Security Concepts]

Which open source tool does Cisco use to create graphical visualizations of network telemetry on Cisco IOS XE devices?

A. InfluxDB
B. Splunk
C. SNMP
D. Grafana

Answer: D

Explanation:

Grafana is an open source tool that displays graphs and counters for data streamed from network devices. Cisco uses Grafana to create graphical visualizations of network telemetry on Cisco IOS XE devices, which support model-driven telemetry. Model-driven telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming. Grafana uses the data from InfluxDB database to build dashboards and graphs. InfluxDB is a time-series database that stores the telemetry data received from the network devices. Telegraf is an agent that collects the telemetry data from the network devices and pushes it to InfluxDB. The TIG software stack refers to the three open-source software components that enable receiving, storing, and visualization the telemetry data:

Telegraf, InfluxDB, and Grafana. Reference :=

Enterprise Streaming Telemetry and You: Getting Started with Model Driven Telemetry - Cisco Blogs Explore Model-Driven Telemetry - Cisco Blogs

Telemetry Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.8.x - Dial-Out Telemetry Session from Router to Destination

Free 350-701 Implementing and Operating Cisco Security Core Technologies Practice Test Questions

Question: 459

[Content Security]

How does the Cisco WSA enforce bandwidth restrictions for web applications?

A. It implements a policy route to redirect application traffic to a lower-bandwidth link.
B. It dynamically creates a scavenger class QoS policy and applies it to each client that connects through the WSA.
C. It sends commands to the uplink router to apply traffic policing to the application traffic.
D. It simulates a slower link by introducing latency into application traffic.

Answer: D

Explanation:

The Cisco WSA can enforce bandwidth restrictions for web applications by using the Application Visibility and Control (AVC) engine. The AVC engine allows the WSA to identify and control application activity on the network, and to apply bandwidth limits to certain application types or individual applications. The WSA dynamically creates a scavenger class QoS policy and applies it to

each client that connects through the WSA. The scavenger class QoS policy assigns a low priority to the application traffic and limits the bandwidth usage based on the configured settings. This way, the WSA can prevent congestion and ensure fair allocation of bandwidth among different applications and users. Reference:

User Guide for AsyncOS 11.8 for Cisco Web Security Appliances - GD (General Deployment) - Managing Access to Web Applications

WSA - limit bandwidth - Cisco Community

Question: 460

[Security Concepts]

Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)

A. services running over the network
B. OpenFlow

C. external application APIs
D. applications running over the network
E. OpFlex

Answer: B,E

Explanation:

Southbound APIs are used to communicate between the SDN Controller and the switches and routers of the network. They can be open-source or proprietary. They facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs. OpenFlow and OpFlex are two examples of southbound APIs. OpenFlow, which was developed by the Open Networking Foundation (ONF), is the first and probably most well-known southbound interface. OpenFlow defines the way the SDN Controller should interact with the forwarding plane to make adjustments to the network, so it can better adapt to changing business requirements. With OpenFlow, entries can be added and removed to the internal flow-table of switches and routers to make the network more responsive to real-time traffic demands. OpFlex, which was proposed by Cisco, is another southbound interface that uses a declarative model to communicate policies and state between the controller and the network devices. OpFlex allows the network devices to retain some intelligence and autonomy, while still being managed by the controller. OpFlex is designed to be flexible and extensible, and can support different types of network devices and services. Services running over the network, external application APIs, and applications running over the network are not southbound APIs, as they do not directly communicate between the controller and the network devices. Therefore, the correct answer is B and E. Reference :=

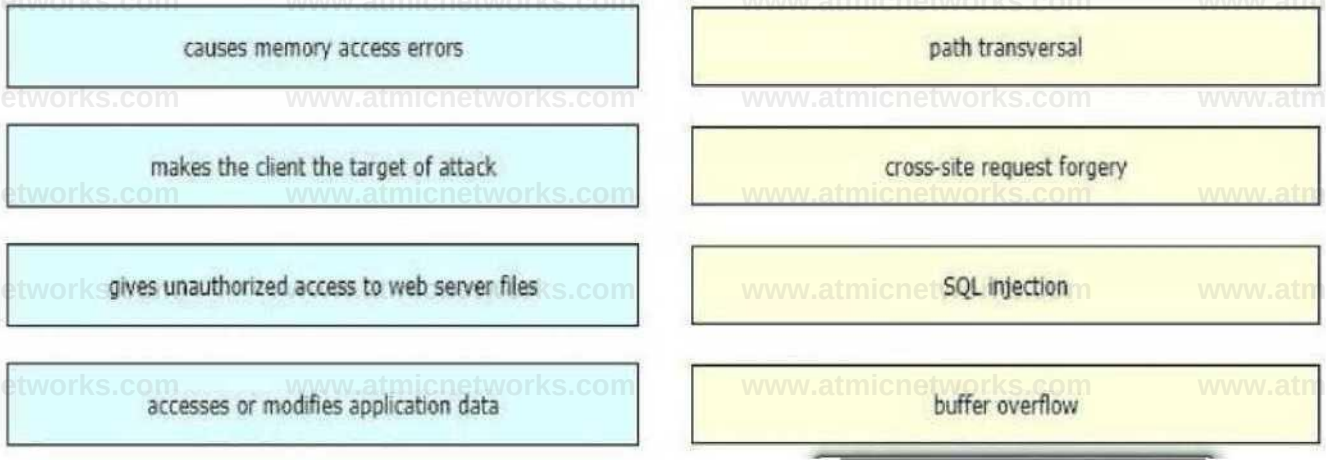
Some possible references are:

What are SDN Southbound APIs? - Where they are used. - SDxCentral

SDN North-bound and South-bound APIs and Interfaces

Question: 461

DRAG DROP
[Security Concepts]
Drag and drop the exploits from the left onto the type of security vulnerability on the right.



Explanation:

Answer:

gives unauthorized access to web server files

makes the client the target of attack

accesses or modifies application data

causes memory access errors

Question: 462

[Endpoint Protection and Detection]

What is the term for when an endpoint is associated to a provisioning WLAN that is shared with guest access, and the same guest portal is used as the BYOD portal?

A. single-SSID BYOD
B. multichannel GUI
C. dual-SSID BYOD
D. streamlined access

Answer: C

Explanation:

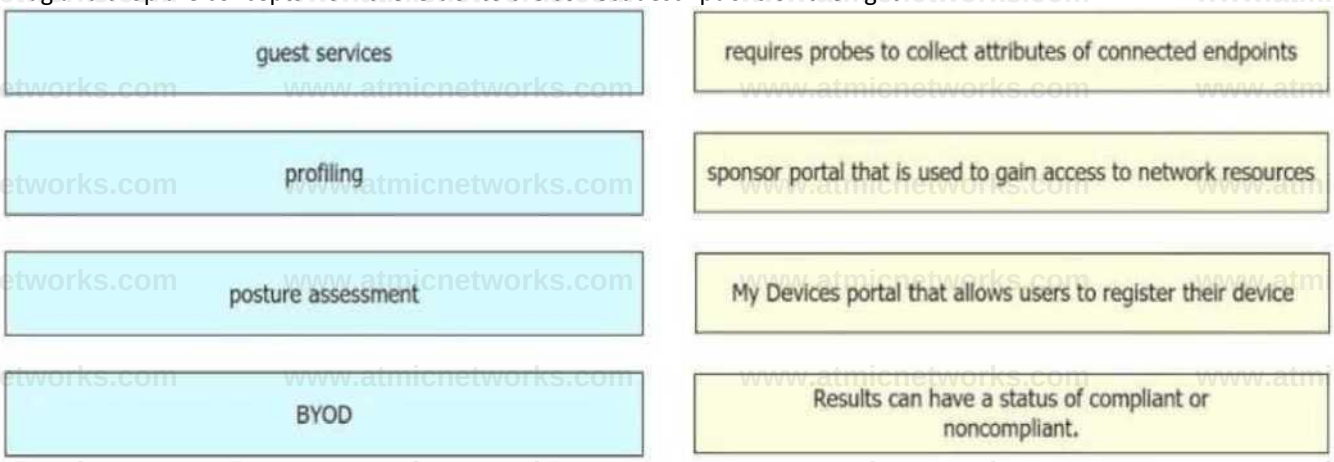
Dual-SSID BYOD is the term for when an endpoint is associated to a provisioning WLAN that is shared with guest access, and the same guest portal is used as the BYOD portal. This flow is a unique capability of ISE where the user does not have to log in twice, as ISE can take the user information from the 802.1X session and direct the user to the BYOD flow. Once the endpoint is onboarded, it is reconnected to the secured WLAN for full network access. This flow is different from single-SSID BYOD, where the endpoint associates to a secure WLAN, gets onboarded, and then reconnects to the same WLAN12. Reference: 1: ISE BYOD: Dual vs. Single SSID Onboarding - Cisco Community 2: Cisco ISE BYOD Prescriptive Deployment Guide - Cisco Community

Question: 463

DRAG DROP

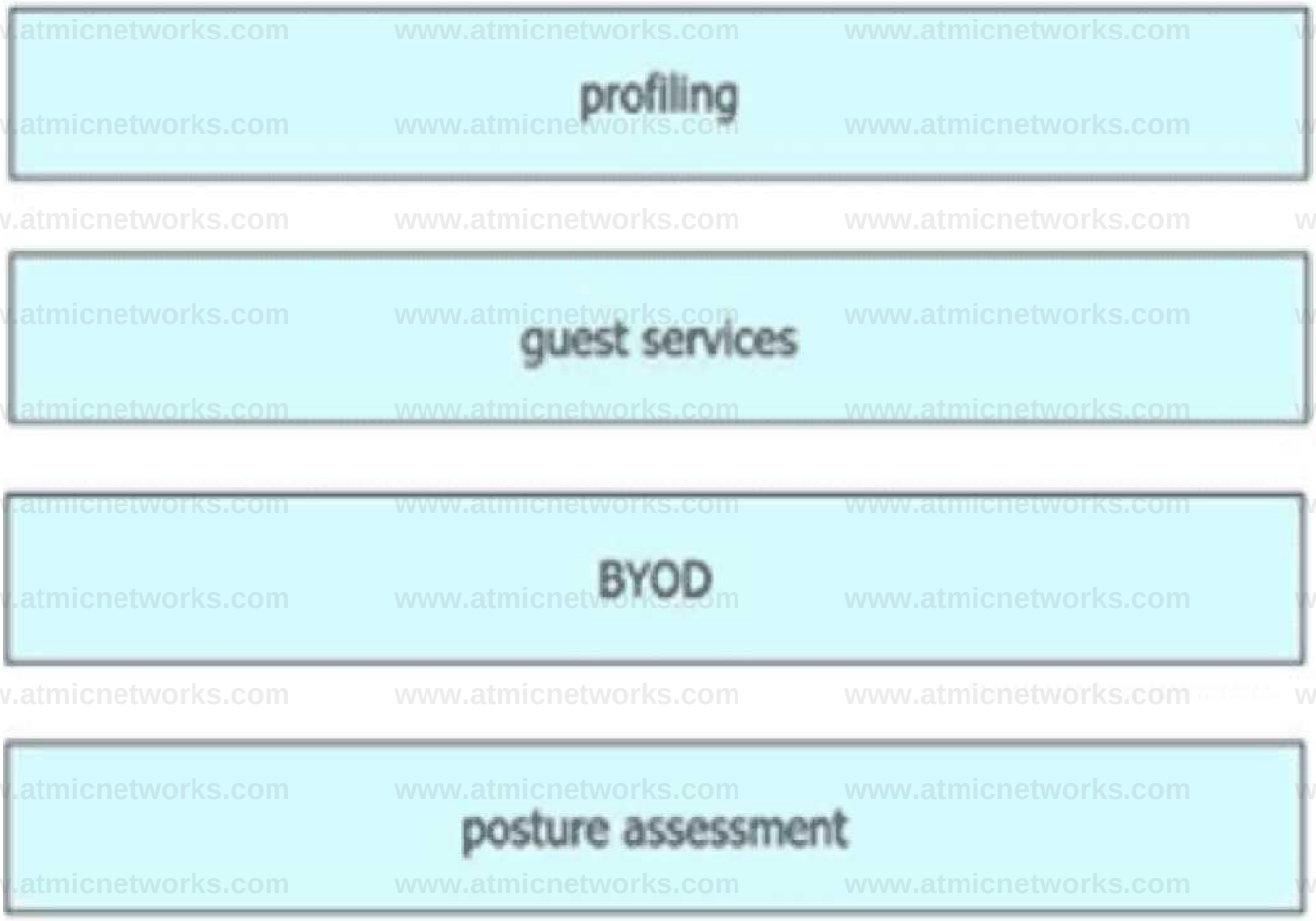
[Security Concepts]

Drag and drop the concepts from the left onto the correct descriptions on the right



Answer:

Explanation:



Question: 464

[Endpoint Protection and Detection]

Which feature within Cisco ISE verifies the compliance of an endpoint before providing access to the network?

A. Posture
B. Profiling
C. pxGrid
D. MAB

Answer: A

Explanation:

Posture is a feature within Cisco ISE that verifies the compliance of an endpoint before providing access to the network. Posture assessment checks the state of the endpoint, such as the operating

system, antivirus, firewall, patches, and so on, against the predefined policies. If the endpoint does not meet the policy requirements, it can be remediated by installing or updating the necessary software or configuration. Posture assessment can be done for both wired and wireless endpoints, as well as VPN clients. Posture assessment requires the installation of a posture agent on the endpoint, which communicates with the posture service on the ISE server. The posture agent can be either a persistent agent, which runs in the background and provides continuous assessment, or a temporal agent, which runs on-demand and is removed after the assessment is complete. Posture assessment can be integrated with 802.1X or web authentication methods for network access control. Reference :=
Some possible references are:
ISE Posture Prescriptive Deployment Guide
ISE Posture Deployment Best Practices and Considerations Understanding ISE Posture Services

Question: 465

[Security Concepts]
Which MDM configuration provides scalability?

A. pushing WPA2-Enterprise settings automatically to devices
B. enabling use of device features such as camera use
C. BYOD support without extra appliance or licenses
D. automatic device classification with level 7 fingerprinting

Answer: C

Explanation:

Mobile device management (MDM) is a solution that allows organizations to manage and secure mobile devices such as smartphones and tablets. MDM can provide scalability by supporting BYOD (bring your own device) scenarios without requiring extra appliance or licenses. BYOD allows employees to use their personal devices for work purposes, which can reduce costs and increase productivity. However, BYOD also introduces security and compliance risks, which MDM can mitigate by enforcing policies, monitoring device status, and performing remote actions. MDM can also integrate with other Cisco security solutions such as Identity Services Engine (ISE) and Umbrella to provide additional protection and visibility. According to the Cisco SCOR course, MDM can provide the following benefits for BYOD1:
Simplify device enrollment and configuration
Automate device compliance checks and remediation
Apply granular policies based on device type, user role, location, and network
Enable secure access to corporate resources and applications
Protect data at rest and in transit with encryption and VPN Detect and respond to device threats and vulnerabilities Wipe or lock devices in case of loss or theft
: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 - Module 4: Secure Connectivity - Lesson 4.3: Mobile Device Management (MDM)

Question: 466

[Endpoint Protection and Detection]
Which Cisco ISE service checks the compliance of endpoints before allowing the endpoints to connect to the network?

A. posture
B. profiler
C. Cisco TrustSec
D. Threat Centric NAC

Answer: A

Explanation:

Posture is a service in Cisco ISE that allows you to check the compliance, also known as posture, of endpoints, before allowing them to connect to your network. A posture agent, such as the AnyConnect ISE Posture Agent or Network Admission Control (NAC) Agent, runs on the endpoint and collects information about the endpoint's security posture, such as antivirus, antispyware, firewall, and patch status. The posture agent then communicates with the ISE server, which evaluates the posture information against the posture policy and determines the compliance state of the endpoint. Based on the compliance state, the ISE server can grant or deny network access to the endpoint, or apply remediation actions to bring the endpoint into compliance. Posture service is part of the ISE solution for network access control (NAC), which aims to secure the network from unauthorized or compromised endpoints. Reference: Cisco Identity Services Engine Administrator Guide, Release 2.2 - Configure Client Posture Policies Configuring posture services with the Cisco Identity Services Engine - Cisco Community Cisco Content Hub - Configure Client Posture Policies

Question: 467

[Endpoint Protection and Detection]
Which endpoint protection and detection feature performs correlation of telemetry, files, and intrusion events that are flagged as possible active breaches?

A. retrospective detection
B. indication of compromise
C. file trajectory
D. elastic search

Answer: A

Explanation:

Retrospective detection is a feature of Cisco Advanced Malware Protection (AMP) for Endpoints that performs correlation of telemetry, files, and intrusion events that are flagged as possible active breaches. Retrospective detection allows AMP to continuously analyze file activity across the network and identify malicious behavior that was previously undetected. Retrospective detection can also trigger alerts and remediation actions when a file's disposition changes from clean to malicious12. Reference: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Endpoint Protection and Detection, Lesson 4.1: Cisco AMP for Endpoints Overview, Topic 4.1.3: Retrospective Detection 2: Cisco AMP for Endpoints User Guide, Chapter: Retrospective Detection, URL: 3

Question: 468

[Security Concepts]
Which feature enables a Cisco ISR to use the default bypass list automatically for web filtering?

A. filters
B. group key
C. company key
D. connector

Answer: D

Explanation:

A connector is a feature that enables a Cisco ISR to use the default bypass list automatically for web filtering. A connector is a software component that runs on the ISR and communicates with the Cloud Web Security service. The connector intercepts the web traffic from the branch users and redirects it to the Cloud Web Security service for scanning and policy enforcement. The connector also maintains a default bypass list, which contains the domains and URLs that are not redirected to the Cloud Web Security service. The default bypass list is updated automatically by the Cloud Web Security service and can be customized by the administrator. The default bypass list helps to improve the performance and reliability of the web filtering solution by avoiding unnecessary redirections of trusted or sensitive web traffic12.
Reference: 1: Security Configuration Guide: Cloud Web Security, Cisco IOS Release 15M&T - Cisco Integrated Services Routers Generation 2 with Cisco Cloud Web Security Solution
[Support] - Cisco 2: Security Configuration Guide: Cloud Web Security, Cisco IOS Release 15M&T - Configuring Cloud Web Security on Integrated Services Routers Generation 2
[Support] - Cisco

Question: 469

[Security Concepts]
A network engineer has configured a NTP server on a Cisco AS
A. The Cisco ASA has IP reachability to the
NTP server and is not filtering any traffic. The show ntp association detail command indicates that the configured NTP server is unsynchronized and has a stratum of 16. What is the cause of this issue?

A. Resynchronization of NTP is not forced
B. NTP is not configured to use a working server.
C. An access list entry for UDP port 123 on the inside interface is missing.
D. An access list entry for UDP port 123 on the outside interface is missing.

Answer: B

Explanation:

NTP uses UDP port 123 to communicate with its servers and peers. If the Cisco ASA has IP reachability

to the NTP server and is not filtering any traffic, then the most likely cause of the unsynchronized state and the stratum of 16 is that the NTP server is not working properly or is not configured to provide NTP service. A stratum of 16 means that the NTP server is unreachable or is not considered a viable candidate1. The value.INIT. in the refid column indicates that NTP is initializing, and the server has not yet been reached1. To resolve this issue, the network engineer should verify the status and configuration of the NTP server, and use a different server if needed. Alternatively, the network engineer can use the ntp server command with the prefer keyword to specify a preferred NTP server, or use the ntp update-calendar command to force a resynchronization of NTP2. Reference:

1: NTP server is unsynchronized or unreachable, a Wireshark perspective.

2: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Network Security, Lesson 1.3: Configuring Network Time Protocol.

Question: 470

[Endpoint Protection and Detection]

When a next-generation endpoint security solution is selected for a company, what are two key deliverables that help justify the implementation? (Choose two.)

A. signature-based endpoint protection on company endpoints
B. macro-based protection to keep connected endpoints safe
C. continuous monitoring of all files that are located on connected endpoints
D. email integration to protect endpoints from malicious content that is located in email
E. real-time feeds from global threat intelligence centers

Answer: C,E

Explanation:

A next-generation endpoint security solution is a modern approach of combining user and system behavior analytics with AI and machine learning to provide endpoint security12. These solutions are specifically designed to detect unknown malware and zero-day threats, which other non-nextgeneration solutions might fail to detect3. Two key deliverables that help justify the implementation of a next-generation endpoint security solution are:

Continuous monitoring of all files that are located on connected endpoints. This feature allows the solution to scan and analyze all files on the endpoints, regardless of their origin or type, and identify any malicious or suspicious behavior. This helps to prevent malware from infecting the endpoints or spreading to other devices on the network4.

Real-time feeds from global threat intelligence centers. This feature enables the solution to leverage the latest information and insights from various sources, such as security researchers, vendors, and customers, to detect and block new and emerging threats. This helps to keep the endpoints updated and protected from the most advanced and sophisticated attacks5.

Reference := 1: Overview of next-generation protection in Microsoft Defender for Endpoint 2: What Is Next-Generation Endpoint Security? 2024 Ultimate Guide - SelectHub 3:

[Next

www.atmicnetworks.com

Question: 471

[Security Concepts]
What is the process of performing automated static and dynamic analysis of files against preloaded behavioral indicators for threat analysis?

A. deep visibility scan
B. point-in-time checks
C. advanced sandboxing
D. advanced scanning

Answer: C

Explanation:

The process of performing automated static and dynamic analysis of files against preloaded behavioral indicators for threat analysis is called advanced sandboxing. Advanced sandboxing is a feature of Cisco Secure Malware Analytics (Threat Grid), which is a cloud-based or on-premises solution that analyzes the behavior of suspicious files and URLs. Advanced sandboxing uses a combination of static and dynamic analysis techniques to examine the files against more than 700

behavioral indicators, such as registry changes, network connections, file modifications, and process injections. These indicators help to uncover stealthy and sophisticated threats, and provide the security team with detailed reports and actionable intelligence. Advanced sandboxing also integrates with other Cisco security products, such as AMP, Firepower, and Email Security, to provide comprehensive malware protection across the network. Advanced sandboxing is different from other options, such as deep visibility scan, point-in-time checks, and advanced scanning, which are not specific processes or features of Cisco Secure Malware Analytics. Deep visibility scan is a generic term that refers to the ability to inspect network traffic and files for malicious activity. Point-in-time checks are periodic scans that detect malware at a specific moment, but do not provide continuous analysis or retrospective security. Advanced scanning is also a generic term that can refer to any scanning technique that goes beyond basic signature-based detection, such as heuristic analysis, machine learning, or behavioral analysis. Reference := Some possible references are:
Cisco Secure Malware Analytics (Threat Grid)
Malware Protection - Cisco AMP Advanced Malware Protection
Cisco Secure Malware Analytics Data Sheet

Question: 472

[Security Concepts]
Which solution is made from a collection of secure development practices and guidelines that developers must follow to build secure applications?

A. AFL
B. Fuzzing Framework
C. Radamsa

D. OWASP

Answer: D

Explanation:

OWASP stands for Open Web Application Security Project, a non-profit organization that provides resources for web application security. OWASP has developed a number of standards, projects, events, and news on topics such as web application security, supply chain security, and cyber risk mitigation1. One of the most widely recognized OWASP resources is the OWASP Top 10, a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications, such as broken access control, cryptographic failures, injection, and insecure design2. The OWASP Top 10 is updated periodically based on data analysis and community feedback. The latest edition was released in 20213. By following the OWASP Top 10 and other OWASP resources, developers can build more secure applications that minimize these risks. Reference := 1: OWASP Foundation, the Open Source Foundation for Application Security 2: OWASP Top Ten | OWASP Foundation 3: OWASP Top 10:2021

Question: 473

[Security Concepts]
What do tools like Jenkins, Octopus Deploy, and Azure DevOps provide in terms of application and infrastructure automation?

A. continuous integration and continuous deployment
B. cloud application security broker
C. compile-time instrumentation
D. container orchestration

Answer: A

Explanation:

Tools like Jenkins, Octopus Deploy, and Azure DevOps provide continuous integration and continuous deployment (CI/CD) capabilities for application and infrastructure automation. CI/CD is a process that enables developers to deliver code changes more frequently and reliably by automating the building, testing, and deployment stages. CI/CD tools help to integrate various components of the software delivery pipeline, such as source control, testing frameworks, configuration management, security scanning, and deployment platforms. By using CI/CD tools, developers can achieve faster feedback loops, improved quality, reduced errors, and increased efficiency123.
According to the Cisco course on Implementing and Operating Cisco Security Core Technologies (SCOR), CI/CD is one of the key concepts of DevSecOps, which is a culture and practice that aims to embed security into every stage of the software development lifecycle. DevSecOps requires collaboration and communication between development, security, and operations teams, as well as the use of automation tools and techniques to ensure security is integrated throughout the process45. Reference: 1: Configuring Jenkins in Azure and deploying with Octopus 2: Octopus Deploy vs. Azure DevOps (VSTS/TFS) 3: Building .NET Core Apps in Azure DevOps and integrating Octopus Deploy 4: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 5: 350-701 SCOR - Cisco

www.atmicnetworks.com

Question: 474

[Security Concepts]
Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?

A. inbound
B. north-south
C. east-west
D. outbound

Answer: D

Explanation:

DNS tunneling is a technique that encodes data of other programs and protocols in DNS queries, including data payloads that can be used to control a remote server and applications1. DNS exfiltration is a form of DNS tunneling that allows attackers to extract data from a compromised system by sending encoded DNS requests to a domain under their control2. The direction of the data transfer in DNS exfiltration is outbound, meaning from the victim's network to the attacker's network. This is different from inbound, which means from the attacker's network to the victim's network, or north-south and east-west, which are terms used to describe the traffic flow between different network segments or zones3. Outbound DNS requests are often allowed by default in many firewalls and network devices, making them an attractive channel for data exfiltration4. However, DNS exfiltration can be detected and prevented by using security solutions that monitor and analyze DNS traffic for anomalies and malicious patterns5.
: 1: Improvements to DNS Tunneling & Exfiltration Detection - Cisco Umbrella 2: DNS Exfiltration & Tunneling: How it Works & DNSteal Demo Setup 3: What Is DNS Tunneling? - Palo Alto Networks 4: DNS Data Exfiltration and DNS Tunneling | Vercara 5: DNS Exfiltration: The Light at the End of the DNS Tunnel - site

Question: 475

[Endpoint Protection and Detection]
Which technology provides a combination of endpoint protection endpoint detection, and response?

A. Cisco AMP
B. Cisco Talos
C. Cisco Threat Grid
D. Cisco Umbrella

Answer: A

Explanation:

Cisco AMP (Advanced Malware Protection) is a technology that provides a combination of endpoint protection, endpoint detection, and response. Cisco AMP protects endpoints from malware and other threats by using multiple prevention engines, including signatures, machine learning, and file reputation. Cisco AMP also continuously monitors and analyzes endpoint activity to detect malicious behavior and indicators of compromise. Cisco AMP can respond to threats by

blocking, isolating, or removing malicious files, processes, or devices across the network. Cisco AMP leverages the cloud-based intelligence of Cisco Talos and Cisco Threat Grid to provide global threat visibility and analysis. Cisco AMP can also integrate with Cisco Umbrella and other security solutions to provide a comprehensive and unified approach to endpoint security. Reference:

Cisco Secure Endpoint (Formerly AMP for Endpoints)

Prevent, Detect and Respond with Cisco AMP for Endpoints

Provide State-of-the-Art Endpoint Protection as a Managed Service

Question: 476

[Security Concepts]

What is a feature of container orchestration?

A. ability to deploy Amazon ECS clusters by using the Cisco Container Platform data plane B. ability to deploy Amazon EKS clusters by using the Cisco Container Platform data plane C. ability to deploy Kubernetes clusters in air-gapped sites D. automated daily updates

Answer: C

Explanation:

Container orchestration is the automated process of organizing the functions of modular, containerized components that create the infrastructure of an application1. Container orchestration tools, such as Kubernetes, provide a framework for managing containers and microservices architecture at scale2. A feature of container orchestration is the ability to deploy Kubernetes clusters in air-gapped sites, which are isolated from the internet and other networks for security reasons3. Cisco Container Platform (CCP) is a solution that simplifies the deployment and management of Kubernetes clusters in any environment, including air-gapped sites4. CCP provides a data plane that runs on the Kubernetes nodes and handles the container networking, storage, and security. CCP also provides a control plane that runs on a separate management cluster and provides a web-based user interface and API for cluster operations. CCP supports the deployment of Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS) clusters on the data plane, but not on air-gapped sites. Reference: 1: What Is Container Orchestration? | AppDynamics 2: What is container orchestration? - Red Hat 3: Container orchestration for microservices - Azure Architecture Center 4: Cisco Container Platform Data Sheet : Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 5: Cloud and Network Security, Lesson 5.3: Cisco Cloud Security Solutions, Topic 5.3.2: Cisco Container Platform : Cisco Container Platform User Guide, Release 5.1, Chapter: Deploying Amazon ECS Clusters

Question: 477

[Security Concepts]

What are two security benefits of an MDM deployment? (Choose two.)

A. robust security policy enforcement
B. privacy control checks
C. on-device content management
D. distributed software upgrade

www.atmicnetworks.com

E. distributed dashboard

Answer: A,B

Explanation:

Mobile device management (MDM) is a solution that allows organizations to manage and secure mobile devices such as smartphones and tablets. MDM can provide two security benefits: Robust security policy enforcement: MDM can enforce strong security practices and hygiene by defining unified settings that can be applied across your fleet. This centralized software ensures all devices are continuously staying in compliance. For example, MDM can configure settings like full-disk encryption, screen locks, password policies, device restrictions, VPN, firewall, antivirus, and more. MDM can also prevent unwanted or risky software from being installed, and remotely lock or wipe devices if they are lost, stolen, or compromised1.

Privacy control checks: MDM can help organizations stay compliant with privacy regulations and protect sensitive data from unauthorized access. MDM can segment personal and corporate data on devices, and selectively wipe only corporate data when needed. MDM can also monitor device usage and location, and alert administrators of any suspicious or anomalous behavior. MDM can also provide secure containers for sensitive documents and content, and encrypt data in transit and at rest23.

Reference:

1: 5 benefits of implementing a Mobile Device Management (MDM) platform - CyberOne

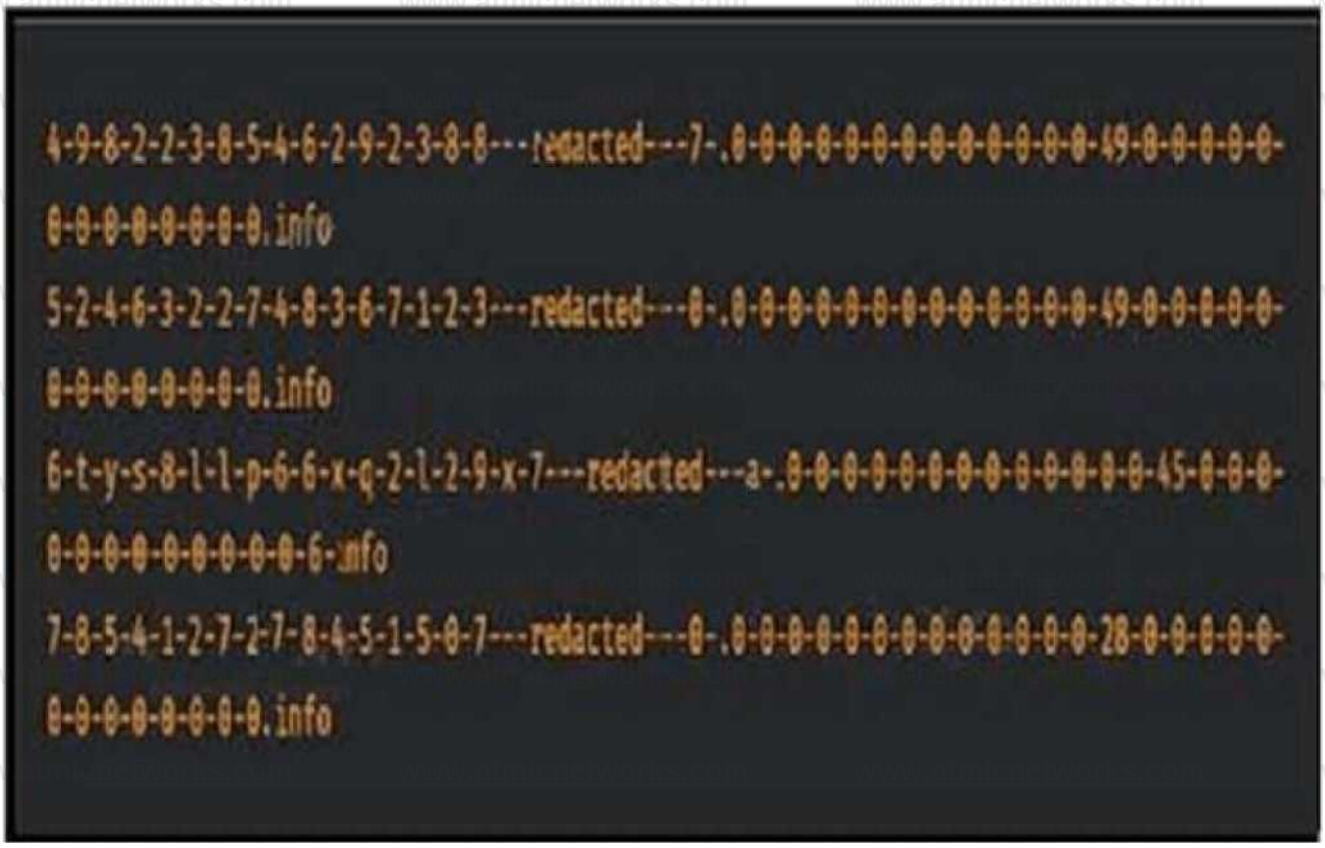
2: Top Six Benefits of Mobile Device Management - N-able

3: Mobile device management 101: Why it matters and how to deploy - Vanta

4: MDM and security: here is everything you should know - Blog Appaloosa

Question: 478

[Security Concepts] Refer to the exhibit.



Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?

A. Spectre Worm
B. Eternal Blue Windows
C. Heartbleed SSL Bug
D. W32/AutoRun worm

Answer: D

Explanation:

The W32/AutoRun worm is a type of malware that spreads through removable drives, such as USB flash drives, and modifies the autorun.inf file to execute itself when the drive is inserted. The worm also attempts to connect to a remote server and download additional malicious files. One of the features of this worm is that it generates random domain names based on the current date and time, and sends DNS requests to these domains. This is a technique to evade detection and analysis, as well as to communicate with the command and control server. The DNS requests generated by the worm have a distinctive pattern, such as the length of the domain name, the number of subdomains, and the use of redacted characters. By comparing these features to the expected behavior of normal DNS requests, security analysts can identify the presence of the worm and block its traffic. Reference :=
Some possible references are:
W32/AutoRun worm

DNS requests malicious attack
Four major DNS attack types and how to mitigate them

www.atmicnetworks.com

Question: 479

[Security Concepts]

What is the recommendation in a zero-trust model before granting access to corporate applications and resources?

A. to use multifactor authentication
B. to use strong passwords
C. to use a wired network, not wireless
D. to disconnect from the network when inactive

Answer: A

Explanation:

The zero-trust model is a modern security strategy that assumes breach and verifies each request as though it originates from an open network. The main concept behind the zero-trust model is "never trust, always verify", which means that users and devices should not be trusted by default, even if they are connected to a permissioned network such as a corporate LAN and even if they were previously verified12

One of the principles of the zero-trust model is to verify explicitly, which means to always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies13 To achieve this, the zero-trust model recommends using multifactor authentication (MFA), which is a method of verifying a user's identity by requiring two or more pieces of evidence, such as something the user knows (e.g., password, PIN), something the user has (e.g., token, smart card), or something the user is (e.g., fingerprint, face scan). MFA provides a higher level of security than using only a single factor, such as a password, which can be easily compromised or guessed. MFA also reduces the risk of unauthorized access to corporate applications and resources, which may contain sensitive or confidential information.

Therefore, the recommendation in a zero-trust model before granting access to corporate applications and resources is to use multifactor authentication, as it ensures that only verified and authorized users and devices can access the data they need, and nothing more13 Reference := 1: Zero Trust Model - Modern Security Architecture | Microsoft Security 2: Zero trust security model - Wikipedia 3: What is Zero Trust? | Microsoft Learn : Multifactor Authentication (MFA) | Cisco

Question: 480

[Endpoint Protection and Detection]

Which Cisco AMP feature allows an engineer to look back to trace past activities, such as file and process activity on an endpoint?

A. endpoint isolation
B. advanced search
C. advanced investigation
D. retrospective security

Answer: D

Explanation:

Retrospective security is a feature of Cisco AMP that enables continuous analysis and alerting of files and network activity, even after the initial point of inspection. It allows an engineer to look back in time and trace the processes, file activities, and communications of an endpoint that was infected by malware. This helps to understand the full extent of an infection, establish root causes, and perform remediation. Retrospective security is different from endpoint isolation, advanced search, and advanced investigation, which are other features of Cisco AMP that provide different capabilities. Endpoint isolation allows an engineer to isolate an endpoint from the network to prevent further spread of malware. Advanced search allows an engineer to query the AMP cloud database for information about files, endpoints, events, and trajectories. Advanced investigation allows an engineer to perform deep analysis of files and endpoints using Cisco Secure Malware Analytics (formerly Threat Grid). Reference :=

Some possible references are:

Malware Defense with Cisco Secure Firewall Data Sheet

Best Practice Guide for Advanced Malware Protection (AMP) on Cisco Email Security Malware Protection - Cisco AMP Advanced Malware Protection

Question: 481

[Secure Network Access, Visibility, and Enforcement]

Which solution stops unauthorized access to the system if a user's password is compromised?

A. VPN
B. MFA
C. AMP
D. SSL

Answer: B

Explanation:

MFA stands for multi-factor authentication, which is a security method that requires users to provide two or more pieces of evidence to verify their identity before accessing a system. MFA can prevent unauthorized access to the system if a user's password is compromised, because the attacker would also need to obtain the other factors, such as a one-time code, a biometric scan, or a physical token. MFA can be implemented using various technologies, such as SMS, email, phone call, mobile app, or hardware device. According to Microsoft, adopting MFA can prevent approximately 99.9% of compromised user accounts, significantly bolstering security measures against unauthorized access12. Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 6: Secure Network Access and Visibility, Lesson 6.1: Implementing Secure Network Access 350-701 SCOR - Cisco, Exam Topics, 6.1 Implement secure network access

What Is Unauthorized Access? 5 Key Prevention Best Practices - Cynet, Best Practice #3: Implement multi-factor authentication

Unauthorized Access: Top 8 Practices for Detecting and Responding - Ekran System, Best Practice #3: Use multi-factor authentication

Question: 482

[Security Concepts]
What is a benefit of using Cisco Tetration?

A. It collects telemetry data from servers and then uses software sensors to analyze flowinformation.
B. It collects policy compliance data and process details.
C. It collects enforcement data from servers and collects interpacket variation.
D. It collects near-real time data from servers and inventories the software packages that exist onservers.

Answer: A

Explanation:

Cisco Tetration is a hybrid-cloud workload protection platform that secures compute instances in both the on-premises data center and the public cloud1. One of the benefits of using Cisco Tetration is that it collects telemetry data from servers and then uses software sensors to analyze flow information2. This allows Cisco Tetration to provide comprehensive visibility into every workload interaction and powerful AI/ML driven automation2. By analyzing the flow information, Cisco Tetration can also generate microsegmentation policies, detect workload behavior anomalies, identify software vulnerabilities, and monitor policy compliance23. Reference: 1: Cisco Secure Workload (formerly Tetration) FAQ 2: Cisco Secure Workload Platform Data Sheet 3: Cisco Tetration Platform - Cisco

Question: 483

[Security Concepts]
How does Cisco Umbrella protect clients when they operate outside of the corporate network?

A. by modifying the registry for DNS lookups
B. by using Active Directory group policies to enforce Cisco Umbrella DNS servers
C. by using the Cisco Umbrella roaming client
D. by forcing DNS queries to the corporate name servers

Answer: C

Explanation:

Cisco Umbrella is a cloud-delivered security service that protects users from malicious domains and IPs, regardless of their location or network. When users are off the corporate network, they can use the Cisco Umbrella roaming client, which is embedded in the Cisco AnyConnect client, to enforce Umbrella DNS servers for all DNS queries. This way, Umbrella can block requests to malicious or unwanted domains before a connection is ever made, and provide visibility and protection for users anywhere they go. The Umbrella roaming client does not require any additional agents or end user action, and it can work with or without a VPN connection. Reference := Cisco Umbrella Roaming, Umbrella Roaming Client – How it Works on Your Company Network

Question: 484

[Secure Network Access, Visibility, and Enforcement]

Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other interoperable security platforms?

A. IEEE
B. IETF
C. NIST
D. ANSI

Answer: B

Explanation:

Cisco ISE and pxGrid use the IETF (Internet Engineering Task Force) standards to integrate with each other and with other interoperable security platforms. IETF is an open, international community of network designers, operators, vendors, and researchers who produce voluntary standards for the Internet. Cisco pxGrid is based on the IETF standards-track XMPP (Extensible Messaging and

Presence Protocol) and RESTCONF (Representational State Transfer Configuration Protocol) technologies. These standards enable Cisco pxGrid to provide a scalable, secure, and open data- sharing platform that supports multiple security products and services. Cisco ISE uses the IETF standards-track RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) protocols to provide network access control and policy enforcement. Cisco ISE also supports the IETF standards-track SXP (Security Group Tag eXchange Protocol) to propagate security group tags across the network. By using the IETF standards, Cisco ISE and pxGrid can interoperate with other security platforms that support the same standards, such as Infoblox, Splunk, Rapid7, and more. Reference:

Cisco pxGrid - Cisco

ISE pxGrid General Information & FAQ - Cisco Community

How To: Integrate Cisco WSA using ISE and TrustSec via pxGrid

Infoblox DDI, Cisco ISE, and the pxGrid Solution Platform

Question: 485

[Content Security]

What are two facts about WSA HTTP proxy configuration with a PAC file? (Choose two.)

A. It is defined as a Transparent proxy deployment.
B. In a dual-NIC configuration, the PAC file directs traffic through the two NICs to the proxy.
C. The PAC file, which references the proxy, is deployed to the client web browser.
D. It is defined as an Explicit proxy deployment.
E. It is defined as a Bridge proxy deployment.

www.atmicnetworks.com

Answer: C,D

Explanation:

A PAC file, or proxy auto-configuration file, is a script that tells the web browser how to use a proxy server for different URLs. A PAC file can be hosted on a web server or on the WSA itself, and can be deployed to the client web browser manually or automatically. A WSA HTTP proxy configuration with a PAC file is defined as an explicit proxy deployment, because the client web browser is aware of the proxy and sends requests to it directly. This is different from a transparent proxy deployment, where the client web browser is unaware of the proxy and the requests are redirected to it by a network device such as a router or a firewall. A bridge proxy deployment is a type of transparent proxy deployment where the WSA acts as a layer 2 bridge between two network segments and intercepts the traffic passing through it. A PAC file is not used in a bridge proxy deployment. In a dual-NIC configuration, the WSA has two network interfaces, one for the client-side network and one for the server-side network. The PAC file does not direct traffic through the two NICs to the proxy, but rather tells the client web browser to send requests to the proxy's IP address and port number. The WSA then forwards the requests to the server-side network through the other NIC. Therefore, option B is incorrect. Reference :=
Some possible references are:

1: What is a Proxy Pac file and are there any examples? - Cisco
2: What is a PAC file and where is it located on WSA? - Cisco
3: [WSA Training Series] How to configure the HTTPS Proxy on the Cisco Web Security Appliance
4: Proxy Auto-Configuration (PAC) file
5: Use proxy auto-configuration (.pac) files with IEAK 11

Question: 486

[Security Concepts]
Which solution should be leveraged for secure access of a CI/CD pipeline?

A. Duo Network Gateway
B. remote access client
C. SSL WebVPN
D. Cisco FTD network gateway

Answer: A

Explanation:

A CI/CD pipeline is a process of automating the development, testing, and deployment of software applications. A CI/CD pipeline typically involves multiple tools and stages, such as source code management, build automation, testing, security scanning, and deployment. To secure a CI/CD pipeline, one of the best practices is to avoid hardcoding secrets in config files and CI/CD build tools, and instead use a secure access solution that can authenticate and authorize the access to the pipeline resources.

Duo Network Gateway is a cloud-based solution that provides secure access to internal web applications without requiring a VPN or modifying firewall rules. Duo Network Gateway integrates with Duo's two-factor authentication (2FA) service to verify the identity of users and devices before granting access to the web applications. Duo Network Gateway also supports single sign-on (SSO) and identity federation with various identity providers, such as Active Directory, Azure AD, Google, and Okta.

By using Duo Network Gateway, you can leverage a CI/CD pipeline without exposing your internal web applications to the internet or compromising security. Duo Network Gateway can protect access to your source code repositories, build servers, testing tools, and deployment platforms. You can also enforce granular access policies based on user roles, device health, location, and time. Duo Network Gateway can help you achieve compliance with industry standards and regulations, such as PCI DSS, HIPAA, and GDPR.

The other options are not as suitable for securing access to a CI/CD pipeline as Duo Network Gateway. A remote access client is a software that allows users to connect to a remote network or server, such as a VPN client. However, a VPN client may not provide sufficient security for a CI/CD pipeline, as it may expose the entire network to potential attacks, or require complex firewall configurations and network segmentation. A VPN client may also introduce performance and reliability issues, as it depends on the quality and availability of the network connection.

SSL WebVPN is a feature of Cisco Adaptive Security Appliance (ASA) that allows users to access web based resources securely over SSL/TLS. SSL WebVPN can provide secure access to web applications, email, file shares, and other network services. However, SSL WebVPN may not be able to support all the tools and stages of a CI/CD pipeline, as some of them may require non-web protocols, such as SSH, RDP, or VNC. SSL WebVPN may also require additional licenses and hardware resources to support a large number of concurrent users and connections.

Cisco FTD network gateway is a unified platform that combines the features of Cisco ASA and Cisco Firepower. Cisco FTD network gateway can provide firewall, intrusion prevention, malware protection, and VPN services. Cisco FTD network gateway can also integrate with Cisco Identity Services Engine (ISE) to provide identity-based access control and visibility. However, Cisco FTD network gateway may not be the best solution for securing access to a CI/CD pipeline, as it may require complex network design and deployment, and may not support all the CI/CD tools and protocols. Cisco FTD network gateway may also incur additional costs and maintenance efforts. Reference := : Secure CI/CD Pipelines: Best Practices for Managing CI/CD Secrets : Duo Network Gateway | Duo Security : VPN vs. Duo Network Gateway | Duo Security : SSL VPN Deployment Guide for Cisco ASA - Cisco : Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.7 - VPN Overview [Cisco Firepower NGFW]

Question: 487

[Endpoint Protection and Detection]

Which function is included when Cisco AMP is added to web security?

A. multifactor, authentication-based user identity
B. detailed analytics of the unknown file's behavior
C. phishing detection on emails
D. threat prevention on an infected endpoint

Answer: B

Explanation:

Cisco Advanced Malware Protection (AMP) for Web Security is a solution that provides protection against web-related threats before, during, and after an attack. One of the functions that AMP for Web Security includes is detailed analytics

of the unknown file's behavior. This means that AMP can continuously monitor and analyze the activity of files that cross the web gateway, even after they have been initially scanned and allowed. This allows AMP to detect and block any malicious behavior that may emerge later, and provide retrospective security alerts and remediation actions12. Reference: 1: Cisco Advanced Malware Protection for Web Security 2: Cisco Adds Advanced Malware Protection to Web and Email Security Appliances and Cloud Services

Question: 488

[Network Security]
A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to ensure that bandwidth is available for VPN users needing access to corporate resources on the10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the network?

A. Use split tunneling to tunnel traffic for the 10.0.0.0/24 network only.
B. Configure VPN load balancing to distribute traffic for the 10.0.0.0/24 network,
C. Configure VPN load balancing to send non-corporate traffic straight to the internet.
D. Use split tunneling to tunnel all traffic except for the 10.0.0.0/24 network.

Answer: A

Explanation:

Split tunneling is a feature that allows VPN users to access both the corporate network and the internet at the same time. By using split tunneling, only the traffic destined for the 10.0.0.0/24 network will be encrypted and sent through the VPN tunnel, while the rest of the traffic will be sent directly to the internet. This reduces the VPN bandwidth load on the headend Cisco ASA and ensures that bandwidth is available for VPN users needing access to corporate resources. Split tunneling can be configured on the ASA by using the split-tunnel-network-list value command under the group- policy attributes. The network list should include the 10.0.0.0/24 network as the only entry. Reference: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 5: Secure Connectivity, Lesson 5.1: Implementing Site-to-Site VPNs on Cisco Routers and ASA Firewalls, Topic 5.1.3: Configuring Site-to-Site VPNs on Cisco ASA Firewalls, Subtopic 5.1.3.2: Configuring Split Tunneling.

Question: 489

[Security Concepts]
Which solution detects threats across a private network, public clouds, and encrypted traffic?

A. Cisco Stealthwatch
B. Cisco CTA
C. Cisco Encrypted Traffic Analytics
D. Cisco Umbrella

Answer: A

Explanation:

Cisco Stealthwatch is the only solution that detects threats across your private network, public

clouds, and encrypted traffic. It uses network telemetry and advanced behavioral analytics to monitor network activity and identify anomalies that indicate potential threats. It also leverages Cisco Encrypted Traffic Analytics (ETA) to detect malware in encrypted traffic without decryption. Cisco Stealthwatch provides visibility, threat detection, and response across your entire network and cloud environment1234 Reference := 1: Cisco Stealthwatch detects threats across private networks, public clouds, and encrypted traffic - Cisco Blogs 2: The XDR Solution to the Ransomware Problem - Cisco Blogs 3: Network Threat Detection and Response with Cisco Stealthwatch - Locuz 4: Cisco Secure Network Analytics (Stealthwatch) - Cisco

Question: 490

[Security Concepts]

Which Cisco security solution integrates with cloud applications like Dropbox and Office 365 while protecting data from being exfiltrated?

A. Cisco Tajos
B. Cisco Steaithwatch Cloud
C. Cisco Cloudlock
D. Cisco Umbrella Investigate

Answer: C

Explanation:

Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cloudlock's simple, open, and automated approach uses APIs to manage the risks in your cloud app ecosystem. Cloudlock integrates with cloud applications like Dropbox and Office 365 by providing visibility, compliance, threat protection, and data security. Cloudlock can detect and prevent data exfiltration by applying data loss prevention (DLP) policies, encrypting sensitive data, and alerting or blocking unauthorized activities. Cloudlock also supports cloud app discovery and risk assessment, user and entity behavior analytics (UEBA), and cloud app firewall12. Reference: 1: Cisco Cloudlock - Cisco 2: Cisco Cloudlock Privacy Data Sheet

Question: 491

[Endpoint Protection and Detection]

Which two actions does the Cisco identity Services Engine posture module provide that ensures endpoint security?(Choose two.)

A. The latest antivirus updates are applied before access is allowed.
B. Assignments to endpoint groups are made dynamically, based on endpoint attributes.

C. Patch management remediation is performed.
D. A centralized management solution is deployed.
E. Endpoint supplicant configuration is deployed.

Answer: A,C

Explanation:

The Cisco Identity Services Engine (ISE) posture module provides a service that allows you to check the compliance of endpoints with corporate security policies. This service consists of three main components: client provisioning, posture policy, and authorization policy. Client provisioning ensures that the endpoints receive the appropriate posture agent, such as the AnyConnect ISE Posture Agent or the Network Admission Control (NAC) Agent. Posture policy defines the conditions and requirements that the endpoints must meet to be considered compliant, such as having the latest antivirus updates or patches installed. Authorization policy determines the level of network access granted to the endpoints based on their posture assessment results, such as allowing full access, limited access, or quarantine.
The two actions that the Cisco ISE posture module provides that ensure endpoint security are: The latest antivirus updates are applied before access is allowed. This action prevents malware infections and protects the network from potential threats. The posture policy can include predefined or custom conditions that check the antivirus status of the endpoints, such as the product name, version, definition date, and scan result. If the endpoint does not meet the antivirus requirement, the posture agent can trigger a remediation action, such as launching the antivirus update or scan, before allowing network access.
Patch management remediation is performed. This action ensures that the endpoints have the latest security patches installed and are not vulnerable to known exploits. The posture policy can include predefined or custom conditions that check the patch status of the endpoints, such as the operating system, service pack, hotfix, or update. If the endpoint does not meet the patch requirement, the posture agent can trigger a remediation action, such as redirecting the endpoint to a patch management server or launching the patch installation, before allowing network access. Reference :=
Cisco Identity Services Engine Administrator Guide, Release 2.2 - Configure Client Posture Policies Configuring posture services with the Cisco Identity Services Engine
Cisco Identity Services Engine Administrator Guide, Release 2.0 - Posture Policy

Question: 492

[Content Security]
Which two authentication protocols are supported by the Cisco WSA? (Choose two.)

A. WCCP
B. NTLM
C. TLS
D. SSL
E. LDAP

Answer: B,E

Explanation:

The Cisco WSA supports two main authentication protocols: LDAP and NTLM. LDAP is a protocol for accessing and managing directory information over a network. NTLM is a Windows proprietary protocol that uses a challenge-response mechanism for authentication. The Cisco WSA can use both LDAP and NTLM to authenticate users and apply policies based on their identity. The Cisco WSA does not support WCCP, TLS, or SSL as authentication protocols, although it can use them for other purposes, such as traffic redirection or encryption. Reference:
User Guide for AsyncOS 11.0 for Cisco Web Security Appliances, Chapter: Acquire End-User Credentials
Cisco Web Security Appliance Best Practices Guidelines, Section: Active authentication
Cisco WSA Authentication, Blog post by Kareem CCIE
Authentication and Authorization, PDF document by Cisco

Question: 493

[Content Security]
When a Cisco WSA checks a web request, what occurs if it is unable to match a user-defined policy?

A. It blocks the request.
B. It applies the global policy.
C. It applies the next identification profile policy.
D. It applies the advanced policy.

Answer: B

Explanation:

When a Cisco WSA receives a web request, it evaluates it against the policies in the policy table. Each policy type has a predefined, global policy, which maintains default actions for that policy type. If the web request does not match any user-defined policy, the WSA applies the global policy. The global policy can be configured to allow, block, or redirect the web request based on various criteria. The global policy acts as a catch-all policy for any web request that is not explicitly handled by a user- defined policy. Reference :=
User Guide for AsyncOS 11.0 for Cisco Web Security Appliances - Create Policies to Control Internet Requests
User Guide for AsyncOS 12.7 for Cisco Web Security Appliances - LD (Limited Deployment) - Acquire End-User Credentials

Question: 494

[Security Concepts]
Which Cisco solution extends network visibility, threat detection, and analytics to public cloud environments?

A. Cisco Umbrella
B. Cisco Stealthwatch Cloud
C. Cisco Appdynamics

D. Cisco CloudLock

Answer: B

Explanation:

Cisco Stealthwatch Cloud is a network detection and response (NDR) solution that leverages preexisting infrastructure to offer enterprise-wide, contextual visibility of network traffic from the private network to the public cloud1. It uses advanced analytics and machine learning to detect threats and anomalies across on-premises and cloud environments, and provides actionable alerts and recommendations to remediate them2. Cisco Stealthwatch Cloud is part of Cisco's XDR strategy, which converges its deep expertise and visibility across the network and endpoints into one turnkey, risk-based solution3. Reference: 3: Cisco Unveils New Solution to Rapidly Detect Advanced Cyber Threats and Automate Response 2: Cisco Secure Network Analytics - Cisco 1: Cisco Stealthwatch and Cisco Tetration Workload Security

Question: 495

[Security Operations]

Which metric is used by the monitoring agent to collect and output packet loss and jitter information?

A. WSAv performance
B. AVC performance
C. OTCP performance
D. RTP performance

Answer: D

Explanation:

The monitoring agent uses the RTP (Real-time Transport Protocol) performance metric to collect and output packet loss and jitter information. RTP is a network protocol used for delivering audio and video over IP networks. It provides mechanisms for timestamping, sequence numbering, and delivery monitoring, which allow for the measurement of packet loss and jitter. RTP is specifically designed for real-time multimedia streaming applications, which are more sensitive to changes in the transmission characteristics of data networks than other applications. Therefore, RTP performance is a suitable metric for monitoring and collecting packet loss and jitter information. The other options are not directly related to measuring packet loss and jitter. TCP (Transmission Control Protocol) is a transport protocol that ensures reliable and ordered delivery of data, but it is not typically used for real-time multimedia applications. WSAv (Web Security Virtual Appliance) is a Cisco solution for web security, but it does not measure packet loss and jitter. AVC (Application Visibility and Control) is a technology that monitors and controls network applications, but it does not focus on packet loss and jitter. Reference :=
Measuring Delay, Jitter, and Packet Loss with Cisco IOS SAA and RTTMON1 Implementing and Operating Cisco Security Core Technologies (SCOR) v1.02 Cisco 350-701: Which metric used by monitoring agent to collect and output packet loss and jitter information?

www.atmicnetworks.com

Question: 496

[Content Security]

Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

A. It must include the current date.
B. It must reside in the trusted store of the WSA.
C. It must reside in the trusted store of the endpoint.
D. It must have been signed by an internal CA.
E. it must contain a SAN.

Answer: B,E

Explanation:

The WSA uses a root certificate and a private key to decrypt HTTPS traffic. The root certificate must reside in the trusted store of the WSA, and it must be able to sign server certificates on the fly. The

server certificates that the WSA generates must contain a SAN (Subject Alternative Name) field, which specifies the hostnames or IP addresses that the certificate is valid for. The SAN field is required by modern browsers and applications to verify the identity of the server. If the WSA does not include a SAN field in the server certificate, the browser or application may reject the connection or display a warning message.

The other options are not correct because:

A . The current date is not a criterion for the WSA to use a certificate to decrypt application traffic. The WSA checks the validity period of the certificate, which includes the start date and the end date. The current date must be within the validity period, but it does not have to be the same as the start date or the end date.

C . The root certificate that the WSA uses to decrypt HTTPS traffic does not have to reside in the trusted store of the endpoint. However, the endpoint must trust the root certificate in order to accept the server certificate that the WSA generates. This can be achieved by manually installing the root certificate on the endpoint, or by using a group policy or a certificate management system to distribute the root certificate to the endpoints.

D . The root certificate that the WSA uses to decrypt HTTPS traffic does not have to be signed by an internal CA. The WSA can generate its own self-signed root certificate, or it can use a root certificate that is signed by an external CA. However, the root certificate must be trusted by the endpoints, as explained in option C.

Reference := : WSA Certificate Usage for HTTPS Decryption :

[User Guide for AsyncOS 12.0 for Cisco Web Security Appliances - GD (General Deployment) - Create Decryption Policies to Control HTTPS Traffic]

Question: 497

DRAG DROP

[Security Concepts]

Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.



Answer:

Explanation:

Full Context Awareness - policy enforcement
NGIPS - threat prevention
AMP - real-time
Collective Sec Intel - Detection, blocking an remediation

Question: 498

[Security Concepts]
What are two benefits of using Cisco Duo as an MFA solution? (Choose two.)

A. grants administrators a way to remotely wipe a lost or stolen device
B. provides simple and streamlined login experience for multiple applications and users
C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
D. encrypts data that is stored on endpoints
E. allows for centralized management of endpoint device applications and configurations

Answer: B,C

Explanation:

Cisco Duo is a multi-factor authentication (MFA) solution that verifies the identity of all users with Duo's easy, one-tap-approval MFA app. It also provides device visibility and adaptive policies to ensure that only trusted devices can access corporate applications and networks. Some of the benefits of using Cisco Duo as an MFA solution are:
It provides a simple and streamlined login experience for multiple applications and users. Users can access all their applications from a single dashboard, and authenticate with a simple push notification or other convenient methods. Duo also supports single sign-on (SSO) for integrated applications, reducing the need for multiple passwords and logins12.
It offers native integration that helps secure applications across multiple cloud platforms or onpremises environments. Duo can be easily integrated with most major apps and custom applications, enabling a secure access solution that can be implemented with minimal IT involvement. Duo also supports various protocols and standards, such as SAML, RADIUS, LDAP, and WebAuthn, to enable seamless integration with different environments13.
: 1: Multi-Factor Authentication (MFA) | Duo Security 2: Multi-Factor Authentication (MFA) | Duo Security - Cisco 3: What Is Duo? Two-Factor Authentication From Cisco - Cisco

Question: 499

[Security Concepts]
How does Cisco Workload Optimization portion of the network do EPP solutions solely performance issues?

A. It deploys an AWS Lambda system
B. It automates resource resizing
C. It optimizes a flow path
D. It sets up a workload forensic score

Answer: B

Explanation:

Cisco Workload Optimization Manager (CWOM) is a decision-automation engine that provides workloads with the exact resources they need at the right time in accordance with business policies, freeing IT teams to focus on innovation rather than the maintenance of their IT environment1. CWOM is part of the Cisco SecureX platform, which integrates various security solutions, including endpoint protection platforms (EPPs), to provide a unified and simplified security experience2. CWOM does not deploy an AWS Lambda system, optimize a flow path, or set up a workload forensic score. These are not related to CWOM's functionality or EPP solutions. CWOM automates resource resizing, which means it can dynamically adjust the CPU, memory, disk, and network resources allocated to each workload based on real-time demand and performance metrics1. This helps EPP solutions to solely address performance issues by ensuring that workloads

have the optimal resources to run efficiently and securely, without overprovisioning or underutilizing resources3.

www.atmicnetworks.com

Reference: 1: Cisco Workload Optimization Manager (CWOM) - Cisco, 2: Endpoint Protection Platform (EPP) Definition - Cisco, 3: Cisco Intersight Workload Optimizer Data Sheet

Question: 500

[Security Concepts]

What are two benefits of using an MDM solution? (Choose two.)

A. grants administrators a way to remotely wipe a lost or stolen device
B. provides simple and streamlined login experience for multiple applications and users
C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
D. encrypts data that is stored on endpoints
E. allows for centralized management of endpoint device applications and configurations

Answer: A,E

Explanation:

A mobile device management (MDM) solution is a software tool that helps organizations manage, secure, and monitor mobile devices such as smartphones, tablets, and laptops. Some of the benefits of using an MDM solution are:
A . grants administrators a way to remotely wipe a lost or stolen device: This feature allows administrators to erase all the data and settings on a device that is lost or stolen, preventing unauthorized access to sensitive information. This can also help comply with data protection regulations and policies12
E . allows for centralized management of endpoint device applications and configurations: This feature enables administrators to control the applications and settings on the devices, such as enforcing security policies, installing or updating software, configuring network access, and restricting device features. This can help improve productivity, performance, and compliance of the devices13
Other benefits of using an MDM solution are:
B . provides simple and streamlined login experience for multiple applications and users: This feature allows users to access multiple applications and services with a single sign-on (SSO) or multi-factor authentication (MFA) mechanism, reducing the hassle of remembering and entering multiple credentials. This can also enhance security and user satisfaction4
C . native integration that helps secure applications across multiple cloud platforms or on-premises environments: This feature allows applications to leverage the native security features of the devices, such as encryption, biometric authentication, and device attestation. This can also help protect the applications from malware, tampering, and data breaches across different environments. D . encrypts data that is stored on endpoints: This feature allows data to be encrypted at rest and in

transit on the devices, preventing unauthorized access or interception of the data. This can also help comply with data protection regulations and policies.
Reference := 1: Mobile Device Management (MDM): What is MDM & why do Businesses need it? - Business Tech Weekly 2: Top 10 Benefits of Mobile Device Management (MDM) - TechFunnel 3: What are the Benefits of Mobile Device

Management? - knowledgenile 4: Mobile Device Management (MDM) - Cisco : Mobile Application Management (MAM) - Cisco : Mobile Device Security - Cisco

Question: 501

[Endpoint Protection and Detection]

A company has 5000 Windows users on its campus. Which two precautions should IT take to prevent WannaCry ransomware from spreading to all clients? (Choose two.)

A. Segment different departments to different IP blocks and enable Dynamic ARp inspection on all VLANs
B. Ensure that noncompliant endpoints are segmented off to contain any potential damage.
C. Ensure that a user cannot enter the network of another department.
D. Perform a posture check to allow only network access to (hose Windows devices that are already patched.
E. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGFW. ni

Answer: B,D

Explanation:

WannaCry ransomware is a type of malware that encrypts the files on the infected devices and demands a ransom for their decryption. It exploits a vulnerability in the Windows SMB protocol that allows remote code execution. To prevent WannaCry ransomware from spreading to all clients, IT should take the following precautions:
Ensure that noncompliant endpoints are segmented off to contain any potential damage. This means that any device that is not patched, managed, or compliant with the security policies should be isolated from the rest of the network and given limited access to resources. This can be done using Cisco Identity Services Engine (ISE) and Cisco TrustSec, which can enforce dynamic segmentation based on the device's identity, posture, and context. This way, IT can prevent the ransomware from infecting other devices and reduce the impact of the attack12
Perform a posture check to allow only network access to those Windows devices that are already patched. This means that IT should verify that the devices have installed the latest security updates from Microsoft that fix the SMB vulnerability. This can be done using Cisco AnyConnect Secure Mobility Client, which offers a VPN Posture/HostScan Module and an ISE Posture Module. Both

modules can assess the endpoint's compliance for things like operating system, patches, antivirus, antispyware, and firewall software. If the device is not patched, it can be denied access to the network or redirected to a remediation portal13
: 1: Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.0 - Configure
Posture 2: Can We Trust Your Device? Checking Security Posture - Cisco 3: Cisco AnyConnect Secure Mobility Client

www.atmicnetworks.com

Administrator Guide, Release 4.10 - Configure Posture

Question: 502

[Security Concepts]
What provides total management for mobile and PC including managing inventory and device tracking, remote view, and live troubleshooting using the included native remote desktop support?

A. mobile device management
B. mobile content management
C. mobile application management
D. mobile access management

Answer: A

Explanation:

Mobile device management (MDM) is a solution that allows organizations to monitor and manage mobile devices such as smartphones, tablets, and laptops. MDM provides features such as inventory and device tracking, remote view, live troubleshooting, remote device locking, device wipe, application management, certificate management, and self-service PIN changes. MDM can help organizations secure their devices, control access to corporate data, and enforce security policies on mobile endpoints. Cisco offers MDM solutions such as Cisco Meraki Systems Manager and Cisco Business Mobile app, which are cloud-based and integrated with other Cisco security products. Reference:
Cisco Meraki Systems Manager
Mobile Device Management in the Meraki Cloud
What Is Endpoint Management?
Device Management using Cisco Business Mobile App

Question: 503

[Security Concepts]
What is the process In DevSecOps where all changes In the central code repository are merged and

synchronized?

A. CD
B. EP
C. CI
D. QA

Answer: C

Explanation:

The process in DevSecOps where all changes in the central code repository are merged and synchronized is called Continuous Integration (CI). CI is a practice that aims to improve the quality and speed of software development by automating the building, testing, and integration of code changes. CI enables developers to collaborate more effectively and detect errors early in the development cycle. CI also helps to ensure that the code in the repository is always in a deployable state and conforms to the security and quality standards123. Reference: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) course, Module 5: Secure Network Access, Identity Management, and Visibility, Lesson 5.1: Introducing DevSecOps 2: DevSecOps code process - AT&T4 3: Building a DevSecOps Culture - from a Technical Perspective5

Question: 504

[Secure Network Access, Visibility, and Enforcement]

Based on the NIST 800-145 guide, which cloud architecture may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises?

A. hybrid cloud
B. private cloud
C. public cloud
D. community cloud

Answer: D

Explanation:

According to the NIST 800-145 guide1, a community cloud is a cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. A community cloud is different from a hybrid cloud, which is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). A private cloud is a cloud infrastructure that is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. A public cloud is a cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Reference :=

Some possible references are:

1: NIST SP 800-145, The NIST Definition of Cloud Computing, 1 2: Evaluation of Cloud Computing Services Based on NIST SP 800-145, 3 3: What Is Community Cloud? Definition, Architecture, Examples, and Best Practices, 6

Question: 505

[Network Security]

Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?

A. NTP
B. syslog
C. SNMP
D. NetFlow

Answer: D

Explanation:

The Cisco Stealthwatch system collects and analyzes network telemetry such as flow (NetFlow, sFlow, JFlow, IPFIX, etc.) from routers, switches, and firewalls to monitor network and user behavior. The system conducts sophisticated, proprietary analytics on network data to automatically detect abnormal behaviors that may signify an attack1. NetFlow is a protocol that provides information about network traffic flows, such as source and destination IP addresses, ports, protocols, bytes, packets, and timestamps. NetFlow data can be used to identify network anomalies, bandwidth

usage, application performance, and security incidents2. Reference :=

Some possible references are:

1: Cisco Stealthwatch Improves Threat Defense with Network Visibility and Security Analytics, Zones, 3 2: What is NetFlow? Definition and Benefits, Cisco, 7

Question: 506

[Security Concepts]

What is the most common type of data exfiltration that organizations currently experience?

A. HTTPS file upload site
B. Microsoft Windows network shares
C. SQL database injections
D. encrypted SMTP

Answer: B

Explanation:
Reference: https://blogs.cisco.com/security/sensitive-data-exfiltration-and-the-insider

Question: 507

[Endpoint Protection and Detection]

Which security solution is used for posture assessment of the endpoints in a BYOD solution?

A. Cisco FTD
B. Cisco ASA
C. Cisco Umbrella
D. Cisco ISE

Answer: D

Explanation:

Cisco ISE is the security solution that is used for posture assessment of the endpoints in a BYOD solution. Posture assessment allows Cisco ISE to inspect the security health of the endpoints, such as their operating system, software applications, network settings, and security software. Cisco ISE can then enforce posture policies based on the compliance status of the endpoints and grant or deny them access to the network resources. Cisco ISE supports different types of posture agents, such as AnyConnect, AnyConnect Stealth, and Temporal Agent, to monitor and remediate the endpoints. Cisco ISE also supports agentless posture for devices that cannot run an agent, such as printers, cameras, and IoT devices. Cisco ISE integrates with various third-party vendors to provide posture assessment for different endpoint platforms, such as Windows, Mac, Linux, Android, and iOS. Reference :=
Some possible references are:
Cisco Identity Services Engine Administrator Guide, Release 3.0 - Compliance
Chapter 15. Device Posture Assessment - Cisco ISE for BYOD and Secure Unified Access Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

www.atmicnetworks.com

Question: 508

[Securing the Cloud]

An engineer is configuring Dropbox integration with Cisco Cloudlock. Which action must be taken before granting API access in the Dropbox admin console?

A. Authorize Dropbox within the Platform settings in the Cisco Cloudlock portal.
B. Add Dropbox to the Cisco Cloudlock Authentication and API section in the Cisco Cloudlock portal.
C. Send an API request to Cisco Cloudlock from Dropbox admin portal.
D. Add Cisco Cloudlock to the Dropbox admin portal.

Answer: B

Explanation:

Cisco AMP for Endpoints provides next-generation protection by leveraging an endpoint protection platform (EPP) and endpoint detection and response (EDR) capabilities. EPP is a set of multifaceted prevention techniques that stop threats from compromising endpoints, such as behavioral analytics, machine learning, and signature-based methods. EDR is a set of powerful features that reduce the attack surface and remediate faster, such as advanced threat hunting, endpoint isolation, and dynamic malware analysis. Cisco AMP for Endpoints also integrates with SecureX, a built-in platform that offers extended detection and response (XDR) capabilities across multiple control points, such as network, cloud, email, and web. By combining EPP, EDR, and XDR, Cisco AMP for Endpoints delivers

a comprehensive and resilient endpoint security solution that can detect, respond, and recover from sophisticated attacks. Reference:

Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco
Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco
Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco

Question: 509

[Endpoint Protection and Detection]

How does Cisco AMP for Endpoints provide next-generation protection?

A. It encrypts data on user endpoints to protect against ransomware.
B. It leverages an endpoint protection platform and endpoint detection and response.
C. It utilizes Cisco pxGrid, which allows Cisco AMP to pull threat feeds from threat intelligence centers.

D. It integrates with Cisco FTD devices.

Answer: B

Explanation:

Cisco AMP for Endpoints provides next-generation protection by leveraging an endpoint protection platform (EPP) and endpoint detection and response (EDR) capabilities. EPP is a set of multifaceted prevention techniques that stop threats from compromising endpoints, such as behavioral analytics, machine learning, and signature-based methods. EDR is a set of powerful features that reduce the attack surface and remediate faster, such as advanced threat hunting, endpoint isolation, and dynamic malware analysis. Cisco AMP for Endpoints also integrates with SecureX, a built-in platform that offers extended detection and response (XDR) capabilities across multiple control points, such as network, cloud, email, and web. By combining EPP, EDR, and XDR, Cisco AMP for Endpoints delivers a comprehensive and resilient endpoint security solution that can detect, respond, and recover from sophisticated attacks. Reference:
Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco
Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco
Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco

Question: 510

[Content Security]

Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)

A. NTLMSSP
B. Kerberos
C. CHAP
D. TACACS+
E. RADIUS

Answer: A,B

Explanation:

The Web Security Appliance (WSA) supports different authentication protocols and schemes to acquire end-user credentials. The most common protocols are NTLMSSP and Kerberos, which are both supported by Active Directory realms. NTLMSSP is a challenge-response authentication protocol that uses a hash of the user's password to authenticate. Kerberos is a ticket-based authentication protocol that uses a trusted third-party (the Key Distribution Center) to issue tickets to the user and the service. Both protocols are more secure and widely supported than Basic authentication, which sends the user's credentials in clear text. CHAP, TACACS+, and RADIUS are not supported by the WSA for end-user authentication, although they can be used for external authentication of administrators or for credential encryption. Reference: 1, 2, 3

https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/guide-c07- 742373.html

https://frontegg.com/blog/authentication

Question: 511

[Security Concepts]
Which API method and required attribute are used to add a device into Cisco DNA Center with the native API?

A. GET and serialNumber
B. userSudiSerlalNos and deviceInfo

C. POST and name
D. lastSyncTime and pid

Answer: C

Explanation:

To add a device into Cisco DNA Center with the native API, the POST method and the name attribute are required. The POST method is used to create a new resource on the server, such as a device. The name attribute is used to specify the hostname or IP address of the device to be added. The POST method requires a JSON body that contains the device information, such as the name, type, role, credentials, and other optional parameters. The Cisco DNA Center API documentation provides an example of the JSON body and the response for adding a device1. The Cisco DNA Center Platform User Guide also explains how to use the native API to add devices2. Reference := 1: Cisco DNA Center API Documentation - Add Device 2: Cisco DNA Center Platform User Guide, Release 2.3.5 - Manage Devices Using the Native API

Question: 512

[Security Concepts]

What is a benefit of using Cisco Umbrella?

A. DNS queries are resolved faster.
B. Attacks can be mitigated before the application connection occurs.
C. Files are scanned for viruses before they are allowed to run.
D. It prevents malicious inbound traffic.

Answer: B

Explanation:

Cisco Umbrella is a cloud-delivered security service that provides DNS-layer security, secure web gateway, firewall, cloud access security broker, and threat intelligence functions. It helps improve security visibility, detect compromised systems, and protect your users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints1. One of the benefits of using Cisco Umbrella is that it can block threats before they launch, reducing response times, and delivering safe, secure internet with Umbrella's cloud tools2. By intercepting DNS requests and applying security policies, Umbrella can prevent malicious connections from being established, and mitigate attacks before the application connection occurs3. This can also reduce

bandwidth costs and improve performance by filtering out unwanted traffic1. Reference: 1: The Essential Benefits of Cisco Umbrella 2: 5 Reasons to Try Cisco Umbrella Now 3: Why choose Cisco Umbrella for cybersecurity protection

Question: 513

[Security Concepts]

Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

A. Cisco Umbrella
B. Cisco AMP for Endpoints
C. Cisco ISE
D. Cisco Stealthwatch

Answer: C

Explanation:

Cisco ISE is a solution that allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard. Cisco ISE integrates with Mobile Device Management (MDM) servers to provide necessary insight into the posture of mobile devices and enforce network access policies. Cisco ISE can also perform device registration, remediation, and periodic compliance checks on mobile devices. Cisco ISE can also issue remote actions on the device through the MDM server, such as full wipe, corporate wipe, and PIN lock. Cisco ISE can also augment endpoint data with information from the MDM server that cannot be gathered using the Cisco ISE profiling services. Reference:

Integrate XenMobile Mobile Device Management (MDM) with Cisco Identity Services Engine (ISE) Cisco Identity Services Engine Administrator Guide, Release 2.4 - Mobile Device Manager Interoperability with Cisco ISE

Cisco ISE Integration with Mobile Device Management (MDM)

Question: 514

[Security Concepts]

What is the term for the concept of limiting communication between applications or containers on the same node?

A. container orchestration B. software-defined access C. microservicing
D. microsegmentation

Answer: D

Explanation:

Microsegmentation is a method of securing multi cloud data centers using granular segmentation rules for the individual workload or application, reducing the risk of an attacker moving from one compromised workload or application to another1. Microsegmentation with Cisco ACI enables you to automatically assign endpoints to logical security zones called endpoint groups (EPGs). These EPGs are based on various network-based or virtual machine (VM)-based
attributes2. Microsegmentation is also referred to as application segmentation or east-west segmentation in a multicloud data center1. Reference: 1: What Is Micro-Segmentation? - Cisco 2: Microsegmentation with Cisco ACI

Question: 515

[Endpoint Protection and Detection]

Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?

A. Cisco ISE
B. Cisco NAC
C. Cisco TACACS+
D. Cisco WSA

Answer: A

Explanation:

Cisco ISE is a platform that can onboard the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing

the endpoint to gain network access. Cisco ISE has an internal CA service that can validate and sign certificate requests from endpoints, generate and store keys and certificates, and provide an OCSP responder to check the validity of certificates. Cisco ISE also supports Enrollment over Secure Transport (EST), which is a protocol that allows endpoints to securely enroll with a CA and obtain certificates. Cisco ISE can use EST to provision certificates to endpoints and configure their network settings to use EAP-TLS authentication. Cisco ISE can also use BYOD workflows to onboard endpoints and issue certificates to them. Reference:

Understand ISE Internal Certificate Authority Services

Endpoint On-boarding using Internal ISE CA

Cisco ISE BYOD Prescriptive Deployment Guide

Question: 516

[Security Concepts]

What are two characteristics of the RESTful architecture used within Cisco DNA Center? (Choose two.)

A. REST uses methods such as GET, PUT, POST, and DELETE.
B. REST codes can be compiled with any programming language.
C. REST is a Linux platform-based architecture.
D. The POST action replaces existing data at the URL path.
E. REST uses HTTP to send a request to a web service.

Answer: A,E

Explanation:

REST stands for Representational State Transfer, which is an architectural style for designing web services. RESTful web services use HTTP as the application protocol and support the standard HTTP methods, such as GET, PUT, POST, and DELETE, to perform CRUD (Create, Read, Update, Delete) operations on resources. Cisco DNA Center exposes its functionality through a set of RESTful APIs that allow external applications to interact with the network controller and automate various tasks. The RESTful architecture used within Cisco DNA Center has the following characteristics12: It is simple, extensible, and secure to use. The APIs are based on open standards and use JSON as the data format. The APIs also support HTTPS for secure communication and authentication.

It is stateless, meaning that each request contains all the information necessary to process it, and the server does not store any session or client state. This improves scalability and performance of the web services.

It is resource-oriented, meaning that each API endpoint represents a logical entity or a resource that can be manipulated by the HTTP methods. For example, the /dna/intent/api/v1/network-

device endpoint represents the network devices resource, and the GET method can be used to retrieve the list of network devices from Cisco DNA Center.

It is uniform, meaning that the same interface and conventions are used across all the APIs. For example, the APIs use the same authentication mechanism, error handling, pagination, filtering, and sorting parameters. Reference:

1: Introduction to Cisco DNA Center REST APIs - Cisco DevNet Learning Labs

2: Cisco DNA Center Platform User Guide, Release 2.2.3

Question: 517

[Security Concepts]

Which cloud service offering allows customers to access a web application that is being hosted, managed, and maintained by a cloud service provider?

A. IaC
B. SaaS
C. IaaS
D. PaaS

Answer: B

Explanation:

SaaS stands for Software as a Service, which is a cloud service offering that allows customers to access a web application that is being hosted, managed, and maintained by a cloud service provider. SaaS applications are typically accessed through a web browser or a mobile app, and the customers do not need to install, update, or maintain any software or hardware on their own. SaaS applications can provide various benefits, such as lower upfront costs, faster deployment, scalability, and automatic updates. Some examples of SaaS applications are Gmail, Salesforce, Zoom, and Netflix123. IaC stands for Infrastructure as Code, which is a method of provisioning and managing cloud resources using code or scripts, rather than manual processes or graphical user interfaces. IaC can help automate and standardize the deployment and configuration of cloud infrastructure, as well as improve consistency, reliability, and security. IaC is not a cloud service offering, but rather a technique or practice that can be used with different cloud service models, such as IaaS or PaaS45. IaaS stands for Infrastructure as a Service, which is a cloud service offering that provides customers with access to virtualized computing resources, such as servers, storage, networks, and operating systems. IaaS customers can rent or lease these resources from a cloud service provider, and have full control over their configuration and management. IaaS customers are responsible for installing, updating, and maintaining their own applications and middleware on top of the cloud infrastructure. IaaS can provide various benefits, such as flexibility, scalability, cost-effectiveness, and security. Some examples of IaaS providers are Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform . PaaS stands for Platform as a Service, which is a cloud service offering that provides customers with

access to a cloud-based platform that includes the infrastructure, operating system, middleware, and development tools needed to build, deploy, and run applications. PaaS customers can focus on developing and running their own applications, without worrying about the underlying cloud infrastructure or software. PaaS can provide various benefits, such as faster development, scalability, compatibility, and security. Some examples of PaaS providers are Heroku, AWS Elastic Beanstalk, and Google App Engine .

Reference := 1: IaaS vs. PaaS vs. SaaS | IBM 2: What is SaaS? Software as a service explained | InfoWorld 3: SaaS - Software as a Service | Oracle 4: What is Infrastructure as Code (IaC)? | Red Hat 5: Infrastructure as

Code (IaC) | AWS : What is IaaS? Infrastructure as a service explained | InfoWorld : IaaS - Infrastructure as a Service | Oracle : Cloud Computing Services | Google Cloud : What is PaaS? Platform as a service explained | InfoWorld : PaaS - Platform as a Service | Oracle : Cloud Services - Deploy Cloud Apps & APIs | Microsoft Azure

Question: 518

[Content Security]
Which characteristic is unique to a Cisco WSAv as compared to a physical appliance?

A. supports VMware vMotion on VMware ESXi
B. requires an additional license
C. performs transparent redirection
D. supports SSL decryption

Answer: C,D

Explanation:

To prevent rogue NTP servers from inserting themselves as the authoritative time source, the administrator needs to configure NTP authentication and specify the interface for syncing to the NTP server. NTP authentication allows the ASA to verify the identity and integrity of the NTP packets received from the server, using a shared secret key. Specifying the interface for syncing to the NTP server ensures that the ASA uses the correct source address for sending and receiving NTP packets, and avoids potential routing issues. The other options are not required or relevant for this task. Specifying the NTP version is optional and does not affect security. Configuring the NTP stratum is only applicable for NTP servers, not clients. The ASA can only act as an NTP client, not a server. Setting the NTP DNS hostname is not recommended, as it introduces a dependency on DNS resolution and may cause synchronization problems if the DNS server changes the IP address of the NTP server. Reference :=
Some possible references are:
Configure NTP Authentication on Secure Network Analytics
CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.6 - Basic Settings Cisco ASA NTP and Clock Configuration with Examples

Question: 519

[Security Concepts]

An administrator is configuring N I P on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)

A. Specify the NTP version
B. Configure the NTP stratum

C. Set the authentication key
D. Choose the interface for syncing to the NTP server
E. Set the NTP DNS hostname

Answer: C,D

Explanation:

To prevent rogue NTP servers from inserting themselves as the authoritative time source, the administrator needs to configure NTP authentication and specify the interface for syncing to the NTP server. NTP authentication allows the ASA to verify the identity and integrity of the NTP packets received from the server, using a shared secret key. Specifying the interface for syncing to the NTP server ensures that the ASA uses the correct source address for sending and receiving NTP packets, and avoids potential routing issues. The other options are not required or relevant for this task. Specifying the NTP version is optional and does not affect security. Configuring the NTP stratum is only applicable for NTP servers, not clients. The ASA can only act as an NTP client, not a server. Setting the NTP DNS hostname is not recommended, as it introduces a dependency on DNS resolution and may cause synchronization problems if the DNS server changes the IP address of the NTP server. Reference :=
Some possible references are:
Configure NTP Authentication on Secure Network Analytics
CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.6 - Basic Settings Cisco ASA NTP and Clock Configuration with Examples

Question: 520

[Endpoint Protection and Detection]

What is a characteristic of an EDR solution and not of an EPP solution?

A. stops all ransomware attacks
B. retrospective analysis
C. decrypts SSL traffic for better visibility
D. performs signature-based detection

Answer: B

Explanation:

EDR stands for endpoint detection and response, while EPP stands for endpoint protection platform. EDR and EPP are two types of endpoint security solutions that have different capabilities and objectives. EDR provides real-time visibility into endpoint activities, detects malicious behavior and anomalies, and enables security teams to investigate and respond to threats. EPP prevents, detects, and remediates security threats on endpoints, such as known and unknown malware, ransomware, and zero-day vulnerabilities. EPP solutions may also include EDR capabilities, but not all EDR

solutions include EPP capabilities.

One of the key features of EDR is retrospective analysis, which means the ability to look back at historical endpoint data and identify the root cause, scope, and impact of a security incident. Retrospective analysis helps security teams understand how the threat entered the network, what actions it performed, and how to prevent it from happening again. EPP solutions, on the other hand, do not provide retrospective analysis, as they are mainly focused on preventing and remediating threats, rather than investigating and responding to them.

Therefore, the correct answer is B. Retrospective analysis is a characteristic of an EDR solution and not of an EPP solution.

Reference:

EPP vs. EDR: Why You Need Both - CrowdStrike

EDR vs EPP: What is the Difference? - Exabeam

Understanding MDR, EDR, EPP, and XDR | Netsurion

EDR vs EPP: Key Features, Differences, and How They Work Together

Endpoint Security Tools: EPP vs EDR | Prey Blog

Question: 521

[Content Security]

Email security has become a high priority task for a security engineer at a large multi-national organization due to ongoing phishing campaigns. To help control this, the engineer has deployed an

Incoming Content Filter with a URL reputation of (-10 00 to -6 00) on the Cisco ESA Which action will the system perform to disable any links in messages that match the filter?

A. Defang
B. Quarantine
C. FilterAction
D. ScreenAction

Answer: A

Explanation:

Defanging is the process of modifying a URL in a message to prevent it from being clickable. This can help protect users from malicious links that have a low URL reputation score. Defanging is one of the actions that can be configured in the Incoming Content Filter on the Cisco ESA. The other actions are Quarantine, FilterAction, and ScreenAction. Quarantine sends the message to a quarantine area for further inspection. FilterAction applies a predefined action such as drop, bounce, or deliver. ScreenAction displays a warning message to the user before allowing them to access the URL. Defanging is the only action that disables the links in the message without affecting the delivery or visibility of the

message12. Reference: 1: URL Filtering on the Cisco IronPort ESA – Mikail's Blog 2: Configure URL Filtering for Secure Email Gateway and Cloud Gateway - Cisco
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-content-filters.pdf

Question: 522

[Security Concepts]

What are two workloaded security models? (Choose two)

A. SaaS
B. IaaS
C. on-premises
D. off-premises
E. PaaS

Answer: B,C

Explanation:

Workloaded security models are ways of protecting applications, services, and capabilities that run

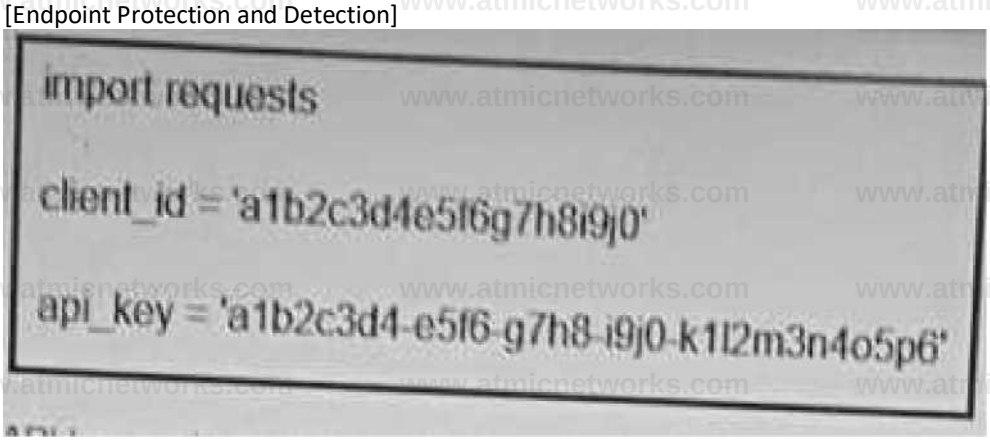
on a cloud resource. Virtual machines, databases, containers, and applications are all considered cloud workloads. There are different types of cloud deployment models, such as public, private, hybrid, and multicloud. Depending on the deployment model, the cloud workload security can vary in terms of responsibility, visibility, and control.
Infrastructure as a service (IaaS) is a cloud deployment model where the cloud provider offers the basic computing infrastructure, such as servers, storage, and networking, as a service. The customer is responsible for installing, configuring, and managing the operating systems, applications, and security of the workloads that run on the cloud infrastructure. IaaS provides the customer with more flexibility and control over the workload security, but also more complexity and overhead.
On-premises is a deployment model where the customer owns and operates the entire IT infrastructure, including the hardware, software, and security. The customer has full responsibility and control over the workload security, but also the highest cost and maintenance. On-premises deployment can offer more security and compliance than cloud deployment, depending on the customer's security posture and practices.

https://www.cisco.com/site/us/en/products/security/secure-workload/index.htmlhttps://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-workload-security/

www.atmicnetworks.com

Question: 523

[Endpoint Protection and Detection]



Refer to the exhibit. What function does the API key perform while working with https://api.amp.cisco.com/v1/computers?

A. imports requests
B. HTTP authorization
C. HTTP authentication
D. plays dent ID

Answer: C

Explanation:

The API key is a secret token that is used to authenticate the client to the server. It is functionally equivalent to a username and password, and should be treated as such. The API key is passed as part of the HTTP header in the request, using the Authorization: Basic scheme. The API key is combined with the client ID and encoded in base64 format. For example, if the client ID is d16aff14860af496e848 and the API key is d01ed435-b00d-4a4d-a299-1806ac117e72, the HTTP header would look like this:

Authorization: Basic ZDE2YWZmMTQ4NjBhZjQ5NmU4NDg6ZDAxZWQ0MzUtYjAwZC00YTRkLWEyOTktMTgwNmFjMTE3ZT cy

The server then decodes the header and verifies the credentials. If the credentials are valid, the server grants access to the requested resource. If the credentials are invalid, the server returns an HTTP 401 Unauthorized error.

The API key performs the function of HTTP authentication, which is the process of verifying the identity of the client. HTTP authentication is different from HTTP authorization, which is the process of determining the permissions of the client. HTTP authorization is based on the scope of the API credential, which can be either read-only or read & write. The scope determines what actions the client can perform on the Cisco AMP for Endpoints data.

Importing requests is not a function of the API key, but rather a Python module that allows sending HTTP requests. Playing dent ID is not a meaningful term in this context. Therefore, the correct answer is C. Reference:

Secure Endpoint API - Cisco DevNet

Overview of the Cisco AMP for Endpoints API - Cisco

Configure AMP for Endpoints Event Stream Feature - Cisco

www.atmicnetworks.com

Question: 524

[Network Security]
What is a benefit of using GET VPN over FlexVPN within a VPN deployment?

A. GET VPN supports Remote Access VPNs
B. GET VPN natively supports MPLS and private IP networks
C. GET VPN uses multiple security associations for connections
D. GET VPN interoperates with non-Cisco devices

Answer: B

Explanation:

GET VPN (Group Encrypted Transport VPN) is a tunnel-less VPN technology that uses a single security association (SA) for all routers in a group. This allows GET VPN to natively support MPLS and private IP networks, without requiring any additional encapsulation or tunneling protocols. GET VPN also supports multicast traffic without GRE, which reduces overhead and improves performance. FlexVPN is a newer VPN solution that covers all VPN types, such as site-to-site, hub and spoke, and remote access. FlexVPN uses IKEv2 for all VPN types, which offers some advantages over IKEv1, such as resiliency and fewer messages. However, FlexVPN requires newer hardware and software versions to support its features. FlexVPN also relies on GRE or static and dynamic point-to-point interfaces to support MPLS and private IP networks, which adds complexity and overhead. Therefore, a benefit of using GET VPN over FlexVPN within a VPN deployment is that GET VPN natively supports MPLS and private IP networks, without requiring any additional encapsulation or tunneling protocols. Reference:
Group Encrypted Transport VPN (GETVPN)
Introduction to FlexVPN
what is the difference between dmvpn and flexvpn

Question: 525

[Security Concepts]

An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users.

A. Upload the organization root CA to the Umbrella admin portal
B. Modify the user's browser settings to suppress errors from Umbrella.
C. Restrict access to only websites with trusted third-party signed certificates.
D. Import the Umbrella root CA into the trusted root store on the user's device.

www.atmicnetworks.com

Answer: D

Explanation:

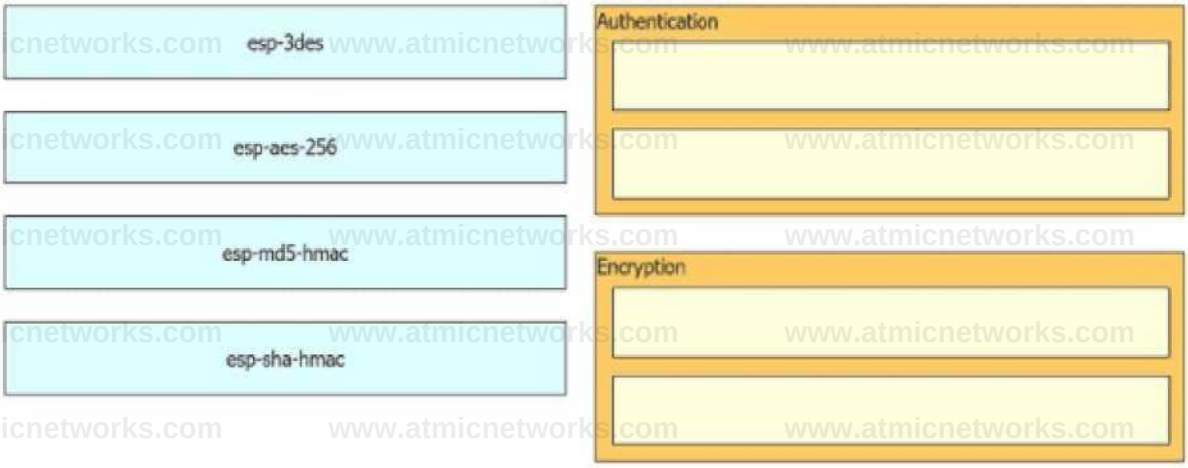
SSL decryption allows the intelligent proxy to inspect traffic over HTTPS. Some websites may use selfsigned certificates or certificates that are not trusted by the user's device. This may cause the browser to display a warning or an error message when accessing those websites through the intelligent proxy. To avoid this, the user's device needs to trust the Umbrella root CA, which is the certificate authority that signs the certificates for the websites that are proxied by Umbrella. By importing the Umbrella root CA into the trusted root store on the user's device, the browser will recognize the certificates as valid and will not alert the end-users12. Reference: 1: Enable SSL

Question: 526

DRAG DROP

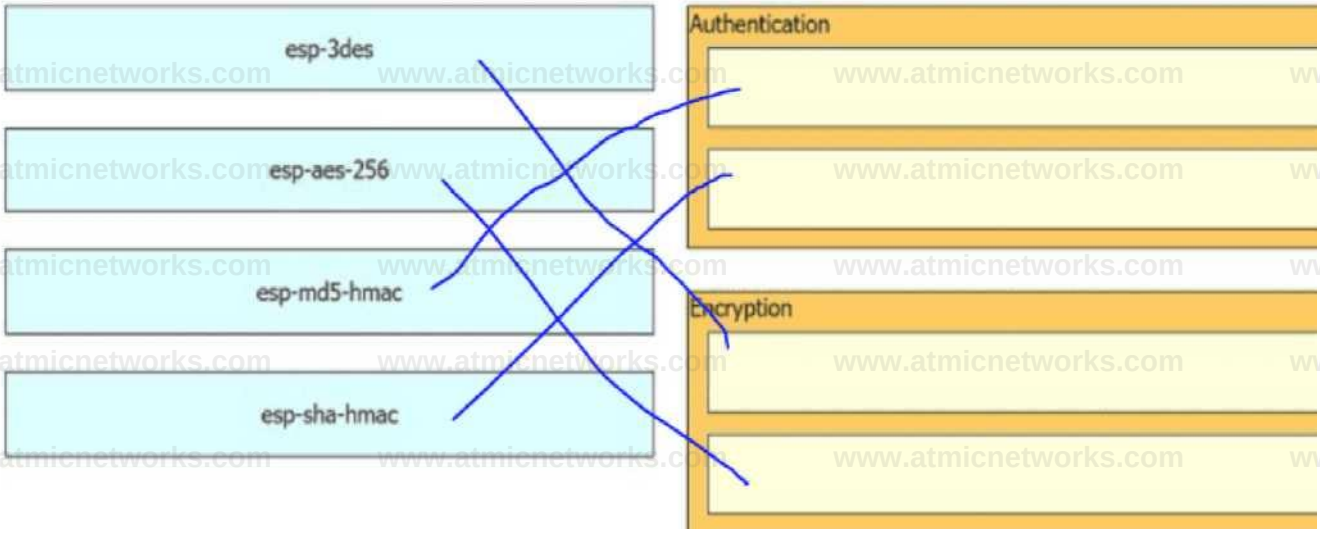
[Network Security]

Drag and drop the cryptographic algorithms for IPsec from the left onto the cryptographic processes on the right.



Answer:

Explanation:

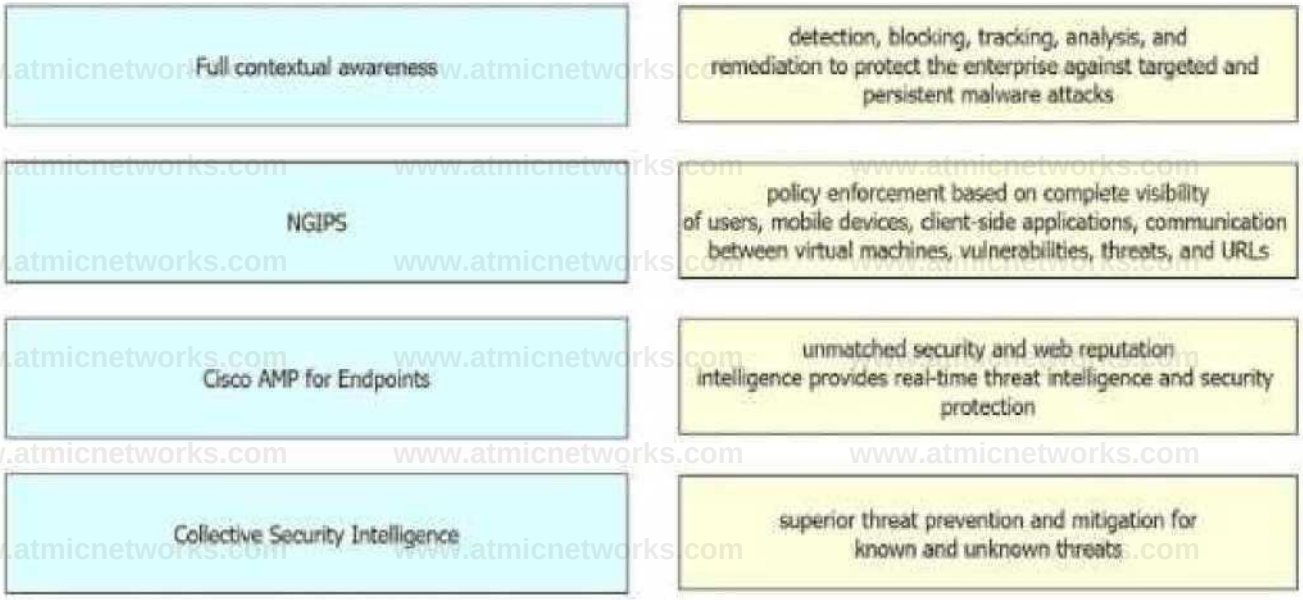


Question: 527

DRAG DROP

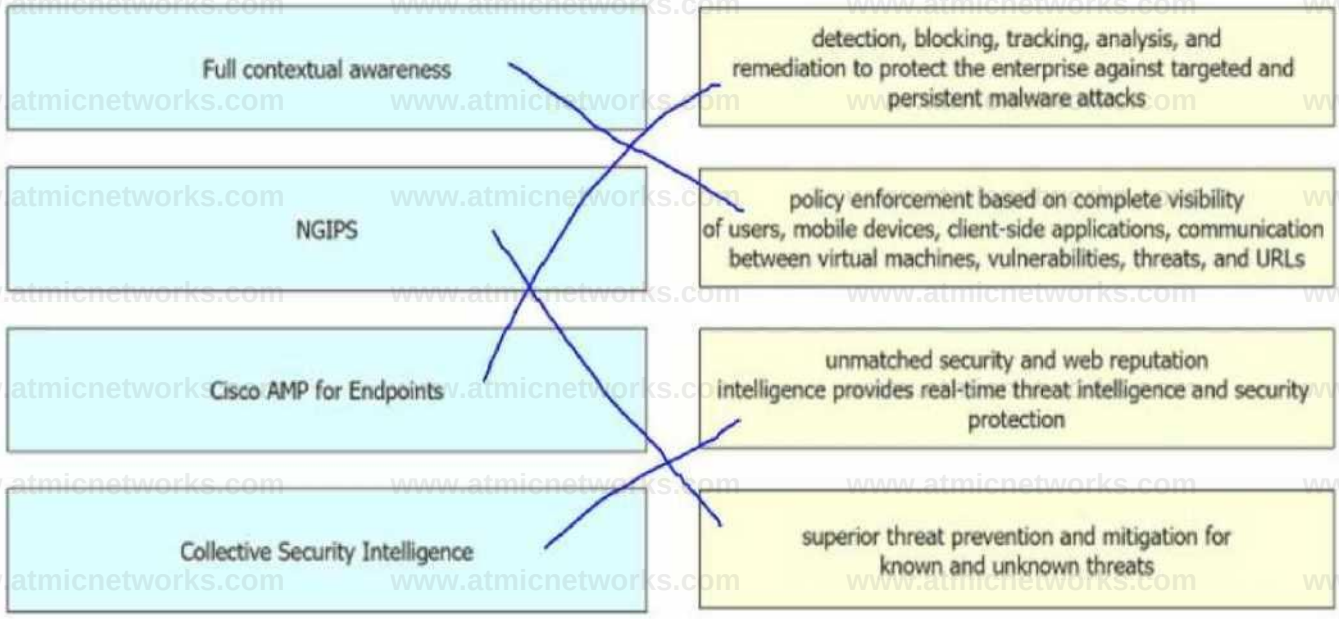
[Security Concepts]

Drag and drop the security solutions from the left onto the benefits they provide on the right.



Answer:

Explanation:



Question: 528

[Security Concepts]

DoS attacks are categorized as what?

A. phishing attacks
B. flood attacks
C. virus attacks

D. trojan attacks

Answer: B

Explanation:

DoS attacks are categorized as flood attacks or crash attacks. Flood attacks are the more common form of DoS attacks. They occur when the attacked system is overwhelmed by large amounts of traffic that the server is unable to handle. The system eventually stops. Some examples of flood attacks are ICMP flood, SYN flood, and UDP flood. Crash attacks are less frequent and they exploit flaws in the targeted system. The result is that the system crashes. Some examples of crash attacks are Ping of Death, Teardrop, and Land. Reference:
What is a denial-of-service (DoS) attack? | Cloudflare
What is a Denial of Service (DoS) attack? | Norton
What is a Denial of Service (DoS) Attack? | Cobalt
What is a denial of service attack (DoS) - Palo Alto Networks

Question: 529

[Security Concepts]
Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?

A. api/v1/fie/config
B. api/v1/onboarding/pnp-device/import
C. api/v1/onboarding/pnp-device
D. api/v1/onboarding/workflow

Answer: B

Explanation:

The Cisco DNA Center RESTful PNP API allows external applications to interact with the Plug and Play (PNP) service of Cisco DNA Center, which automates the onboarding and provisioning of network devices. The PNP API has several endpoints for different operations, such as importing, claiming, updating, and deleting devices. The endpoint that adds and claims a device into a workflow is api/v1/onboarding/pnp-device/import, which takes a JSON payload with the device information and the workflow ID. This endpoint creates a new device entry in the PNP database and associates it with the specified workflow. The workflow defines the configuration template, image, and license to

be applied to the device during the provisioning process12. Reference:
1: See How to Use the Plug and Play API in DNA Center – Part 2
2: Cisco DNA Center Platform User Guide, Release 2.2.3

www.atmicnetworks.com

Question: 530

[Security Operations]
What is the purpose of a NetFlow version 9 template record?

A. It specifies the data format of NetFlow processes.
B. It provides a standardized set of information about an IP flow.
C. It defines the format of data records.
D. It serves as a unique identification number to distinguish individual data records

Answer: C

Explanation:

A NetFlow version 9 template record is a record that contains information about the fields that will be present in the data records that follow the template. A template record consists of a template ID, a field count, and a list of field types and lengths. A template record is sent periodically by the NetFlow exporter to the NetFlow collector, so that the collector can parse and interpret the data records correctly. A template record can also be requested by the collector using an options template record. The purpose of a template record is to define the format of data records, which contain the actual information about the IP flows1234.
A . It specifies the data format of NetFlow processes. - This is incorrect, because a template record does not specify the data format of NetFlow processes, but rather the data format of data records. NetFlow processes are the functions that perform flow creation, aggregation, export, and analysis on the NetFlow device or the collector. B. It provides a standardized set of information about an IP flow. - This is incorrect, because a template record does not provide any information about an IP flow, but rather the information about the fields that will be present in the data records. The data records are the ones that provide the information about an IP flow, such as source and destination IP addresses, ports, protocols, bytes, packets, timestamps, and so on. C. It defines the format of data records. - This is correct, because a template record defines the format of data records by specifying the field types and lengths that will be present in the data records. A template record allows the NetFlow collector to parse and interpret the data records correctly, and also enables the NetFlow exporter to use different formats for different types of flows. D. It serves as a unique identification number to distinguish individual data records. - This is incorrect, because a template record does not serve as a unique identification number, but rather as a description of the fields. A template record has a template ID, which is a 16-bit value that identifies the template record uniquely within an export packet, but this ID is not used to distinguish individual data records. The data records are distinguished by their position within the export packet and their association with a template record. Reference := 1: NetFlow Version 9 Flow-Record Format

[IP Application Services] - Cisco … 2: NetFlow V9 formats - IBM 3: Netflow :: Version 9 - Caligare 4: NetFlow Versions > NetFlow for Cybersecurity | Cisco Press

Question: 531

[Security Operations]

What is a benefit of flexible NetFlow records?

A. They are used for security
B. They are used for accounting
C. They monitor a packet from Layer 2 to Layer 5
D. They have customized traffic identification

Answer: D

Explanation:

https://confluence.netvizura.com/display/NVUG/Traditional+vs.+Flexible+NetFlow

Question: 532

[Endpoint Protection and Detection]

What is the purpose of the Cisco Endpoint loC feature?

A. It provides stealth threat prevention.
B. lt is a signature-based engine.
C. lt is an incident response tool
D. It provides precompromise detection.

Answer: C

Explanation:

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco Secure_Managed_Endpoint.pdf

Question: 533

[Content Security]

An engineer recently completed the system setup on a Cisco WSA Which URL information does the system send to SensorBase Network servers?

A. Summarized server-name information and MD5-hashed path information
B. complete URL,without obfuscating the path segments
C. URL information collected from clients that connect to the Cisco WSA using Cisco AnyConnect
D. none because SensorBase Network Participation is disabled by default

Answer: A

Explanation:

The Cisco WSA can participate in the Cisco SensorBase Network, which is a threat management database that collects and shares data from Cisco security products. By participating in the SensorBase Network, the WSA can receive web reputation scores and URL categories for the requested web content, and also contribute data to improve the accuracy and efficacy of the service. The data that the WSA sends to the SensorBase Network servers includes information about request attributes and how the appliance handles requests. However, to protect the privacy and confidentiality of the users and the organization, the WSA does not send the complete URL, but only the summarized server-name information and the MD5-hashed path information. The MD5 hash is a one-way encryption algorithm that converts the path information into a fixed-length string that cannot be reversed. This way, the SensorBase Network can identify the URL without revealing the actual content or parameters of the request. The WSA also does not send any personal or confidential information such as usernames and passwords, or any information about HTTPS transactions, except for the IP address, web reputation score, and URL category of the server name in the certificate. The SensorBase Network Participation is enabled by default, but it can be disabled by the administrator if desired123. Reference: 3: Web Base Network Participation (WBNP) and Sender Base Network Participation (SBNP) - Cisco 2: User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - GD (General Deployment) - Introduction 1: User Guide for AsyncOS 12.0 for Cisco Web Security Appliances - GD (General Deployment) - Introduction

Question: 534

[Endpoint Protection and Detection]
What does endpoint isolation in Cisco AMP for Endpoints security protect from?

A. an infection spreading across the network E
B. a malware spreading across the user device
C. an infection spreading across the LDAP or Active Directory domain from a user account
D. a malware spreading across the LDAP or Active Directory domain from a user account

Answer: C

Explanation:

https://community.cisco.com/t5/endpoint-security/amp-endpoint-isolation/td-p/4086674#:~:text=Isolating%20an%20endpoint%20blocks%20all,your%20IP%20isolation%20allow %20list

Question: 535

[Endpoint Protection and Detection]

www.atmicnetworks.com

An engineer is deploying Cisco Advanced Malware Protection (AMP) for Endpoints and wants to create a policy that prevents users from executing file named abc424952615.exe without quarantining that file What type of Outbreak Control list must the SHA.-256 hash value for the file be added to in order to accomplish this?

A. Advanced Custom Detection
B. Blocked Application
C. Isolation
D. Simple Custom Detection

Answer: D

Explanation:

This is a type of Outbreak Control list that allows the administrator to create a list of files based on their SHA-256 hash values that will be detected, blocked, and quarantined by the AMP for Endpoints connectors. The Simple Custom Detection list can be applied to a policy and synchronized with the devices that have the AMP connectors installed. This way, the administrator can prevent the execution of specific files without having to quarantine them on the devices.

The other options are incorrect because:

Advanced Custom Detection is a type of Outbreak Control list that allows the administrator to create custom rules based on file attributes, such as file name, size, path, or parent process. These rules can be used to detect and block files that match certain criteria, but they cannot be used to quarantine them.

Blocked Application is a type of Outbreak Control list that allows the administrator to create a list of

applications based on their SHA-256 hash values that will be blocked from running on the devices that have the AMP connectors installed. However, this list does not detect or quarantine the applications, only prevents them from executing.

Isolation is a feature of AMP for Endpoints that allows the administrator to isolate a device from the network if it is compromised by malware. This prevents the device from communicating with other devices or the internet, but does not affect the files on the device.

Reference:

https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/215176-configure-a-simple- custom-detection-list.html

https://community.cisco.com/t5/endpoint-security/block-list-data-source-in-cisco-amp/td- p/4077205

https://community.cisco.com/t5/security-videos/amp4e-outbreak-control/ba-p/4071894

Question: 536

[Security Concepts]

Which Cisco security solution stops exfiltration using HTTPS?

A. Cisco FTD
B. Cisco AnyConnect
C. Cisco CTA
D. Cisco ASA

Answer: C

Explanation:

https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a- glance-c45-736555.pdf

Question: 537

[Endpoint Protection and Detection]

What is a functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client?

A. The Umbrella Roaming client stops and tracks malicious activity on hosts, and AMP for Endpoints tracks only URL-based threats.

B. The Umbrella Roaming Client authenticates users and provides segmentation, and AMP for Endpoints allows only for VPN connectivity

C. AMP for Endpoints authenticates users and provides segmentation, and the Umbrella Roaming Client allows only for VPN connectivity.

D. AMP for Endpoints stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats.

Answer: D

Explanation:

Cisco AMP for Endpoints and Cisco Umbrella Roaming Client are both security solutions that protect mobile users from threats, but they have different functions and features. Cisco AMP for Endpoints is a cloud-managed endpoint security solution that stops and tracks malicious activity on hosts, such as malware execution, file behavior, and command-and-control callbacks. It also provides threat intelligence, sandboxing, and retrospective analysis to detect and respond to advanced threats. Cisco Umbrella Roaming Client is a lightweight DNS client that tracks only URL-based threats, such as phishing, ransomware, and botnets. It prevents connections to malicious domains and IP addresses, and provides visibility and enforcement for off-network devices. It also integrates with Cisco AnyConnect VPN client to provide seamless protection for VPN and non-VPN traffic. Therefore, the functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client is that AMP for Endpoints stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats. Reference :=
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and

Detection, Lesson 3.1: Cisco AMP for Endpoints Overview
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.2: Cisco AMP for Endpoints Architecture and Components Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.3: Cisco AMP for Endpoints Installation and Configuration Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.4: Cisco AMP for Endpoints Analysis and Response Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.5: Cisco Umbrella Overview
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.6: Cisco Umbrella Architecture and Components
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.7: Cisco Umbrella Roaming Client
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.8: Cisco Umbrella Policies and Reporting
Best Mobile Cybersecurity Solution - Cisco Umbrella

Question: 538

[Endpoint Protection and Detection]
What is the difference between EPP and EDR?

A. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.
B. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.
C. EDR focuses solely on prevention at the perimeter.
D. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.

Answer: D

Explanation:

EPP and EDR are two types of endpoint security solutions that have different goals and capabilities. EPP stands for endpoint protection platform, which is a suite of technologies that work together to prevent, detect, and remediate security threats on endpoints. EPP solutions use techniques such as antivirus, firewall, application control, and patch management to block known and unknown malware and malicious activity. EDR stands for endpoint detection and response, which is a solution that provides real-time visibility into endpoint activities and enables security teams to detect, investigate, and respond to advanced threats that may have bypassed EPP defenses. EDR solutions use techniques such as behavioral analysis, threat intelligence, and incident response to flag offending files at the first sign of malicious behavior, contain and isolate compromised endpoints, and remediate the damage caused by the attack. Therefore, the correct answer is D, as having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior. The other options are incorrect because:

A is false, as EPP focuses primarily on threats that have evaded front-line defenses that entered the environment, not EDR.
B is false, as having an EPP solution allows an engineer to detect, investigate, and remediate modern threats, not EDR.
C is false, as EDR focuses on detection and response at the endpoint level, not prevention at the perimeter.

Reference:
EPP vs. EDR: Why You Need Both - CrowdStrike
EDR vs EPP: What is the Difference? - Exabeam
EPP vs. EDR: What Matters More, Prevention or Response? - Cynet

Question: 539

[Security Concepts]
Which algorithm is an NGE hash function?

A. HMAC
B. SHA-1
C. MD5
D. SISHA-2

Answer: D

Explanation:

SHA-2 is a family of hash functions that includes SHA-256, SHA-384, and SHA-512. SHA-2 is part of the Next Generation Encryption (NGE) suite of cryptographic algorithms that Cisco recommends for strong security and good performance. SHA-2 is believed to be quantum-computer resistant, meaning that it would not be easily broken by a hypothetical quantum-computer. SHA-2 is also more secure than older hash functions such as MD5 and SHA-1, which have been shown to have weaknesses and collisions. SHA-2 is widely used in various protocols and functions, such as digital signatures, integrity verification, and key derivation. Reference: 1
https://sec.cloudapps.cisco.com/security/center/resources/next_generation_cryptography
https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/116055- technote-ios-crypto.html

Question: 540

[Security Concepts]
What are two recommended approaches to stop DNS tunneling for data exfiltration and command and control call backs? (Choose two.)

A. Use intrusion prevention system.
B. Block all TXT DNS records.
C. Enforce security over port 53.
D. Use next generation firewalls.
E. Use Cisco Umbrella.

Answer: C,E

Explanation:

DNS tunneling is a technique that uses the DNS protocol to exfiltrate data or establish command and control channels between a compromised host and an attacker-controlled server. DNS tunneling can bypass network security controls that allow outbound DNS traffic without inspection or filtering. To stop DNS tunneling, two recommended approaches are:

Enforce security over port 53. This means applying firewall rules, access control lists, or other mechanisms to restrict outbound DNS traffic to only authorized DNS servers and domains. Additionally, DNS traffic should be inspected and analyzed for anomalies, such as unusually large or frequent queries, non-standard encoding, or suspicious domains. This can help detect and block DNS tunneling attempts.

Use Cisco Umbrella. Cisco Umbrella is a cloud-based security service that provides DNS security, web filtering, and threat intelligence. Cisco Umbrella can prevent DNS tunneling by blocking malicious

domains, enforcing policies based on content categories, and applying machine learning to identify and stop emerging threats. Cisco Umbrella can also provide visibility and reporting on DNS activity and security events.

Reference :=

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 5: Securing the Cloud, Lesson 5.2: DNS Security

What Is DNS Tunneling? - Palo Alto Networks

An Introduction to DNS Tunneling Detection & Data Exfiltration via DNS - Vercara

Question: 541

[Security Concepts]

Which two capabilities does an MDM provide? (Choose two.)

A. delivery of network malware reports to an inbox in a schedule
B. unified management of mobile devices, Macs, and PCs from a centralized dashboard
C. enforcement of device security policies from a centralized dashboard
D. manual identification and classification of client devices
E. unified management of Android and Apple devices from a centralized dashboard

Answer: B,C

Explanation:

Mobile device management (MDM) is a toolset that provides a workforce with mobile productivity tools and applications while keeping corporate data secure1. One of the essential capabilities of an MDM solution is the unified management of mobile devices, Macs, and PCs from a centralized dashboard2. This allows IT and security departments to manage all of a company's devices, regardless of their operating system, and perform tasks such as provisioning, configuration, update, lock, wipe, and troubleshoot2. Another important capability of an MDM solution is the enforcement of device security policies from a centralized dashboard3. This enables IT and security departments to protect the device's applications, data, and content, and ensure compliance with organizational and regulatory standards3. For example, an MDM solution

www.atmicnetworks.com

can set minimum password strength, encrypt data, restrict access, and detect threats3.

: 1: What is Mobile Device Management (MDM)? | IBM 2: 5 Essential Capabilities of an MDM Solution | Macworld 3: What is device management? | Microsoft Learn

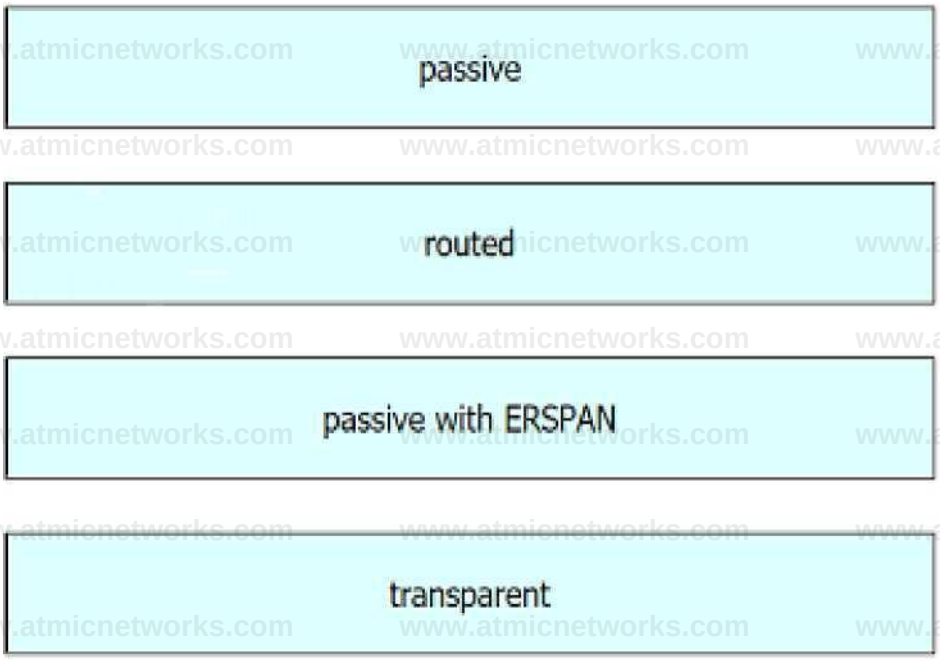
Question: 542

DRAG DROP
[Security Concepts]
Drag and drop the deployment models from the left onto the s on the right.

routed	A GRE tunnel is utilized in this solution.
passive	This solution allows inspection between hosts on the same subnet.
passive with ERSPAN	Attacks are not prevented with this solution.
transparent	This solution does not provide filtering between hosts on the same subnet.

Answer:

Explanation:



Question: 543

[Security Concepts]

Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?

A. VMware APIC
B. VMwarevRealize
C. VMware fusion
D. VMware horizons

Answer: A

Explanation:

VMware APIC is a platform that integrates with Cisco ACI to provide enhanced visibility, policy integration and deployment, and security policies with access lists. VMware APIC is a virtual appliance that runs on VMware vSphere and communicates with the Cisco APIC controller. VMware APIC allows administrators to create and manage Cisco ACI policies for VMware virtual machines and networks. VMware APIC also provides a unified view of the physical and virtual network topology, health, and statistics. VMware APIC supports the following modes of Cisco ACI and VMware integration:

VMware VDS: When integrated with Cisco ACI, the VMware vSphere Distributed Switch (VDS) enables administrators to configure VM networking in the ACI fabric.

Cisco ACI Virtual Edge: Cisco ACI Virtual Edge is a distributed service that provides Layer 4 to Layer 7 services for applications running on VMware vSphere.

Cisco Application Virtual Switch (AVS): Cisco AVS is a distributed virtual switch that provides policybased network services for VMware vSphere environments. Reference:

Cisco ACI with VMware VDS Integration

Cisco ACI and VMware NSX-T Data Center Integration

Cisco ACI and VMware: The Perfect Pair

Setting the Record Straight: Confusion about ACI on VMware Technologies

Question: 544

[Secure Network Access, Visibility, and Enforcement]

An organization is implementing AAA for their users. They need to ensure that authorization is verified for every command that is being entered by the network administrator. Which protocol must be configured in order to provide this capability?

A. EAPOL
B. SSH
C. RADIUS
D. TACACS+

Answer: D

Explanation:

TACACS+ is a protocol that provides authentication, authorization, and accounting (AAA) services for network devices. Unlike RADIUS, which only supports authorization at the user level, TACACS+ supports authorization at the command level. This means that TACACS+ can verify the permissions of the network administrator for every command that is entered, and allow or deny access accordingly. This provides more granular and secure control over network resources and operations. EAPOL, SSH, and RADIUS are not protocols that can provide command-level authorization for AAA.

Reference := Some possible references are:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Security Concepts, Lesson 1.2: Network Security Devices and Cloud Services, Topic 1.2.3: AAA

350-701 SCOR - Cisco, Exam Topics, 1.0 Security Concepts, 1.2 Compare network security solutions, 1.2.a AAA

What Is AAA Security? | Fortinet, Authentication, Authorization, and Accounting (AAA)

Question: 545

[Security Concepts]

Which capability is provided by application visibility and control?

A. reputation filtering
B. data obfuscation
C. data encryption
D. deep packet inspection

Answer: D

Explanation:

Application visibility and control (AVC) is a solution that leverages multiple technologies to recognize, analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications1. One of the key components of AVC is application recognition, which uses stateful deep packet inspection (DPI) to identify applications within the network traffic flow, using L3 to L7 data2. DPI is a technique that examines the content of packets beyond the header information, and can classify applications based on their signatures, protocols, ports, or other attributes3. DPI enables AVC to monitor and control application performance, bandwidth usage, quality of service, and security policies4. Reference := 1: Cisco Application Visibility and Control (AVC) - Cisco 2: Cisco Application Visibility and Control User Guide - Technology Overview 3: What is application visibility and control? | Juniper Networks US 4: Application visibility and control - Secure Internet Access Enterprise

Question: 546

[Security Concepts]

When network telemetry is implemented, what is important to be enabled across all network infrastructure devices to correlate different sources?

A. CDP
B. NTP
C. syslog
D. DNS

Answer: B

Explanation:

Network telemetry is the collection, measurement, and analysis of data related to the behavior and performance of a network1. It involves gathering information about routers, switches, servers, and applications to gain insights into how they function and how data moves through them. To correlate different sources of network telemetry data, it is important to enable Network Time Protocol (NTP) across all network infrastructure devices. NTP is a protocol that synchronizes the clocks of network devices to a common reference time source2. This ensures that the network telemetry data has consistent timestamps and can be compared and correlated accurately. NTP also helps with troubleshooting network issues, as it allows network administrators to pinpoint the exact time of events and anomalies. NTP is a core security technology that is covered in the Implementing and Operating Cisco Security Core Technologies (SCOR) course3, which helps you prepare for the Cisco CCNP Security and CCIE Security certifications and for senior-level security
roles. Reference: 1: Network Telemetry Explained: Frameworks, Applications & Standards - Splunk 2: [Network Time Protocol (NTP) - Cisco] 3: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Question: 547

[Content Security]
In which two ways does the Cisco Advanced Phishing Protection solution protect users? (Choose two.)

A. It prevents use of compromised accounts and social engineering.
B. It prevents all zero-day attacks coming from the Internet.
C. It automatically removes malicious emails from users' inbox.
D. It prevents trojan horse malware using sensors.
E. It secures all passwords that are shared in video conferences.

Answer: A,C

Explanation:

Cisco Advanced Phishing Protection (AAP) is a solution that adds sophisticated machine learning capabilities to Cisco Email Security to block advanced identity deception attacks for inbound email by assessing its threat posture1. It also uses both global and local telemetry data combined with analytics and modeling to validate the reputation and authenticity of senders2. AAP provides sender authentication and BEC detection capabilities, and uses advanced machine learning techniques, real-

time behavior analytics, relationship modeling and telemetry to protect against identity deception– based threats3.
In two ways, the Cisco Advanced Phishing Protection solution protects users:
It prevents use of compromised accounts and social engineering. AAP detects and blocks phishing emails that attempt to impersonate legitimate senders, such as executives, partners, or customers, and trick users into revealing sensitive information or transferring funds. AAP analyzes the sender's identity, behavior, and relationship with the recipient, and assigns a risk score to the email. If the email is deemed suspicious or malicious, AAP can quarantine it, flag it, or deliver it with a warning4. It automatically removes malicious emails from users' inbox. AAP provides retrospective analysis and

www.atmicnetworks.com

remediation capabilities, which means that it can identify and remove emails that were initially delivered but later found to be malicious. AAP leverages the Cisco Talos threat intelligence network and the Sensor-based solution to continuously monitor the threat landscape and update the email disposition accordingly. If an email is reclassified as malicious, AAP can automatically delete it from the users' inbox, or notify the administrator or the user to take action45. The other options are incorrect because they do not accurately describe the functions of AAP. AAP does not prevent all zero-day attacks coming from the Internet, as it focuses on phishing and identity deception attacks. AAP does not prevent trojan horse malware using sensors, as sensors are used to collect and analyze email data, not to block malware. AAP does not secure all passwords that are shared in video conferences, as it is not related to video conferencing security. Therefore, the correct answer is A and C. Reference:

Cisco's Security Innovations to Protect the Endpoint and Email

Cisco Advanced Phishing Protection - Cisco Video Portal

Cisco Advanced Phishing Protection At A Glance - AVANTEC

User Guide for Cisco Advanced Phishing Protection

Cisco Secure Email Threat Defense - Cisco

Integrating the Email Gateway with Cisco Advanced Phishing Protection

Question: 548

[Secure Network Access, Visibility, and Enforcement]

An engineer is adding a Cisco router to an existing environment. NTP authentication is configured on all devices in the environment with the command ntp authentication-key 1 md5 Clsc427128380. There are two routers on the network that are configured as NTP servers for redundancy, 192.168.1.110 and 192.168.1.111. 192.168.1.110 is configured as the authoritative time source. What command must be configured on the new router to use 192.168.1.110 as its primary time source without the new router attempting to offer time to existing devices?

A. ntp server 192.168.1.110 primary key 1
B. ntp peer 192.168.1.110 prefer key 1
C. ntp server 192.168.1.110 key 1 prefer
D. ntp peer 192.168.1.110 key 1 primary

Answer: C

Explanation:

The correct command to configure the new router to use 192.168.1.110 as its primary time source without the new router attempting to offer time to existing devices is ntp server 192.168.1.110 key 1 prefer. This command specifies that the new router will act as an NTP client and synchronize its time with the NTP server at 192.168.1.110, using the authentication key 1 and giving preference to this server over other possible servers. The prefer keyword indicates that this server is preferred over other servers with the same stratum number. The ntp server command is different from the ntp peer command, which configures the new router to act as an NTP peer and exchange time information with another NTP device. A peer relationship is bidirectional and symmetric, meaning that both devices can provide and receive time information from each other. A client-server relationship is unidirectional and asymmetric, meaning that the client only receives time information from the server and does not provide any time information to the server. Therefore, the ntp peer command is not suitable for the scenario, as it would make the new router attempt to offer time to existing devices, which is not desired. The primary keyword is not a valid option for either the ntp server or the ntp peer command, and it would cause a syntax error. Reference := Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Security Concepts, Lesson 1.3: Network Time Protocol

www.atmicnetworks.com

Configuring NTP - Cisco, Configuring NTP on the Switch, Configuring NTP in Client Mode NTP Commands - Cisco, ntp server, ntp peer

Question: 549

[Network Security]

Which ESA implementation method segregates inbound and outbound email?

A. one listener on a single physical Interface
B. pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address
C. pair of logical IPv4 listeners and a pair Of IPv6 listeners on two physically separate interfaces
D. one listener on one logical IPv4 address on a single logical interface

Answer: B

Explanation:

ESA stands for Email Security Appliance, which is a Cisco product that provides comprehensive email security solutions. ESA can be deployed in different modes, such as gateway, hybrid, or cloud, depending on the customer's needs and preferences. One of the key components of ESA configuration is the listener, which is a service that listens for incoming SMTP connections on a specific port and interface. A listener can be configured to handle inbound or outbound email, or both, depending on the mail flow policies and sender groups that are applied to it.

One way to segregate inbound and outbound email on ESA is to use a pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address. This method allows the ESA to have two separate listeners for inbound and outbound email, each with its own IP address and mail flow policies, while using the same physical interface and port. This can simplify the network configuration and reduce the hardware requirements for ESA deployment. The IPv6 address can be used to support dual-stack IPv4 and IPv6 environments, or to provide redundancy in case of IPv4 address exhaustion.

The other options are incorrect because:

A is false, as one listener on a single physical interface cannot segregate inbound and outbound email, unless it uses different sender groups and mail flow policies for different hosts, which is not a recommended practice.

C is false, as pair of logical IPv4 listeners and a pair of IPv6 listeners on two physically separate interfaces is an unnecessary and complex configuration that does not provide any additional benefits over option B.

D is false, as one listener on one logical IPv4 address on a single logical interface cannot segregate inbound and outbound email, unless it uses different sender groups and mail flow policies for different hosts, which is not a recommended practice.

Reference:

www.atmicnetworks.com

ESA Outbound Traffic Relay Configuration Example
How do I configure a relay host on the ESA for outbound mail?
[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0] - Module 5: Securing Email with Cisco Email Security Appliance, Lesson 5.1: Describing the Cisco Email Security Solution

Question: 550

[Network Security]
During a recent security audit a Cisco IOS router with a working IPSEC configuration using IKEv1 was flagged for using a wildcard mask with the crypto isakmp key command The VPN peer is a SOHO router with a dynamically assigned IP address Dynamic DNS has been configured on the SOHO router to map the dynamic IP address to the host name of vpn sohoroutercompany.com In addition to the command crypto isakmp key Cisc425007536 hostname vpn.sohoroutercompany.com what other two commands are now required on the Cisco IOS router for the VPN to continue to function after the wildcard command is removed? (Choose two)

A. ip host vpn.sohoroutercompany.eom <VPN Peer IP Address>
B. crypto isakmp identity hostname
C. Add the dynamic keyword to the existing crypto map command
D. fqdn vpn.sohoroutercompany.com <VPN Peer IP Address>
E. ip name-server <DNS Server IP Address>

Answer: B,E

Explanation:

The crypto isakmp identity hostname command is required to define the identity used by the router when participating in the Internet Key Exchange protocol. This command is needed when you specify preshared keys for authentication. The ip name-server <DNS Server IP Address> command is required to specify the IP address of the DNS server that can resolve the FQDN of the remote peer. This command is needed when you use the crypto isakmp key command with the hostname option instead of the address option. The other commands are not required or correct for this scenario.
Reference: 1, 2, 3

Question: 551

[Security Concepts]
Which command is used to log all events to a destination colector 209.165.201.107?

A. CiscoASA(config-pmap-c)#flow-export event-type flow-update destination 209.165.201.10
B. CiscoASA(config-cmap)# flow-export event-type all destination 209.165.201.
C. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.10
D. CiscoASA(config-cmap)#flow-export event-type flow-update destination 209.165.201.10

www.atmicnetworks.com

Answer: C

Explanation:

The correct command to log all events to a destination collector is flow-export event-type all destination 209.165.201.10. This command configures a flow-export action that sends all NSEL events to the specified IP address. NSEL events include flow-create, flow-teardown, flow-denied, and flow-update events. The command must be entered in the policy-map class configuration mode, after defining a policy-map and a class-map that match the traffic and event type. The other commands are incorrect because they either specify the wrong event type (flow-update instead of all) or the wrong destination IP address (209.165.201 instead of 209.165.201.10). Reference := Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 5: Securing the Cloud, Lesson 5.2: DNS Security

Cisco Secure Firewall ASA NetFlow Implementation Guide Configuring Cisco ASA for NetFlow Export via CLI – Plixer

Question: 552

[Security Concepts]
What is the most commonly used protocol for network telemetry?

A. SMTP
B. SNMP
C. TFTP
D. NctFlow

Answer: B

Explanation:

SNMP (Simple Network Management Protocol) is the most commonly used protocol for network telemetry. SNMP is a standard protocol that allows network devices to exchange management information1. SNMP agents run on network devices and collect data about their status, performance, configuration, and events. SNMP managers run on network management systems and query the agents for data or receive notifications from them. SNMP can also be used to configure or control network devices remotely2. SNMP is widely supported by various vendors and platforms, and it provides a simple and flexible way to monitor and manage networks3.

: 1: What is SNMP? | Cisco 2: SNMP Basics: What is SNMP and How It Works |
SolarWinds 3: Network Telemetry Explained: Frameworks, Applications & Standards | Splunk

Question: 553

[Network Security]
What are two functions of IKEv1 but not IKEv2? (Choose two)

A. NAT-T is supported in IKEv1 but rot in IKEv2.
B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext
C. With IKEv1, mode negotiates faster than main mode
D. IKEv1 uses EAP authentication
E. IKEv1 conversations are initiated by the IKE_SA_INIT message

Answer: B,C

Explanation:

IKEv1 has two modes of operation: main mode and aggressive mode. Main mode uses six messages to establish the IKE SA, while aggressive mode uses only three messages. Therefore, aggressive mode is faster than main mode, but less secure, as it exposes the identities of the peers in cleartext. This makes it vulnerable to man-in-the-middle attacks. IKEv2 does not have these modes, but uses a single four-message exchange to establish the IKE SA. IKEv2 also encrypts the identities of the peers, making it more secure than IKEv1 aggressive mode.

IKEv1 uses EAP authentication only for remote access VPNs, not for site-to-site VPNs. IKEv2 supports EAP authentication for both types of VPNs. EAP authentication allows the use of various authentication methods, such as certificates, tokens, or passwords.

IKEv1 conversations are initiated by the ISAKMP header, which contains the security parameters and the message type. IKEv2 conversations are initiated by the IKE_SA_INIT message, which contains the security parameters, the message type, and the message ID. The message ID is used to identify and order the messages in the IKEv2 exchange.

NAT-T is supported by both IKEv1 and IKEv2. NAT-T stands for Network Address Translation-Traversal, and it is a mechanism that allows IKE and IPsec traffic to pass through a NAT device. NAT-T detects the presence of NAT and encapsulates the IKE and IPsec packets in UDP headers, so that they can be translated by the NAT device.

Reference:

IKEv1 vs IKEv2 – What is the Difference?
Comparison between IKEv1 and IKEv2
IKEv2 vs IKEv1: What are the differences?

Question: 554

[Security Concepts]
Which threat intelligence standard contains malware hashes?

A. structured threat information expression
B. advanced persistent threat
C. trusted automated exchange or indicator information
D. open command and control

Answer: C

Explanation:

Trusted Automated Exchange of Indicator Information (TAXII) is a standard that defines how to exchange cyber threat intelligence (CTI) over HTTPS. CTI includes indicators of compromise (IOCs), such as malware hashes, IP addresses, URLs, and domains, that can be used to detect and respond to cyberattacks. TAXII enables the sharing of CTI in a secure, automated, and interoperable way among different organizations and tools. Structured Threat Information Expression (STIX) is a standard that defines how to represent and structure CTI in a common language. STIX and TAXII are often used together to facilitate the exchange of CTI. Advanced Persistent Threat (APT) is not a standard, but a term used to describe a sophisticated and stealthy cyberattack that persists over a long period of time, often targeting specific organizations or sectors. Open Command and Control (OpenC2) is a standard that defines how to communicate and execute cyber defense actions across different technologies and domains. OpenC2 enables the orchestration and automation of cyber defense actions, such as blocking, isolating, or redirecting malicious traffic or devices. Reference := Some possible references are:

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 4: Content Security, Lesson 4.3: Cisco Umbrella, Topic 4.3.1: Cisco Umbrella Investigate

350-701 SCOR - Cisco, Exam Topics, 4.0 Content Security, 4.3 Describe the components, capabilities, and benefits of Cisco Umbrella, 4.3.a Investigate

TAXII - OASIS Cyber Threat Intelligence Technical Committee, Overview, Introduction

STIX - OASIS Cyber Threat Intelligence Technical Committee, Overview, Introduction OpenC2 - OASIS Open Command and Control Technical Committee, Overview, Introduction What is an Advanced Persistent Threat (APT)? | Fortinet, Definition, What is an APT?

Question: 555

[Security Concepts]

A company identified a phishing vulnerability during a pentest What are two ways the company can protect employees from the attack? (Choose two.)

A. using Cisco Umbrella
B. using Cisco ESA
C. using Cisco FTD
D. using an inline IPS/IDS in the network
E. using Cisco ISE

Answer: A,B

Explanation:

Phishing is a type of cyberattack that uses fraudulent emails or other communications to trick users into providing sensitive information or installing malware on their devices1. Phishing can lead to identity theft, data breaches, ransomware infections, and financial losses. To protect employees from phishing attacks, a company can use various solutions that can detect, block, and remediate phishing threats. Two of these solutions are:

Cisco Umbrella: Cisco Umbrella is a cloud-based security platform that provides the first line of defense against threats on the internet, including phishing2. Cisco Umbrella uses DNS-layer security, which can identify and block malicious domains, IPs, and URLs before they can reach the user's device2. Cisco Umbrella also integrates with Cisco Email Security to provide additional protection against phishing emails that may bypass the email gateway3.

Cisco Email Security Appliance (ESA): Cisco ESA is an email gateway that protects inbound and outbound email traffic from spam, malware, phishing, and other threats4. Cisco ESA uses multiple layers of defense, such as reputation filtering, antivirus scanning, outbreak filters, and content filtering, to prevent malicious emails from reaching the user's inbox4. Cisco ESA also leverages Cisco Advanced Phishing Protection, which uses machine learning and threat intelligence to identify and block sophisticated phishing attacks that use identity deception techniques5.

Reference := 1: What Is Phishing? Examples and Phishing Quiz - Cisco 2: Cisco Umbrella - Cloud Delivered Enterprise Security 3: Cisco Umbrella and Cisco Email Security Integration 4: Cisco Secure Email - Cisco 5: Cisco Advanced Phishing Protection - Cisco Video Portal

Question: 556

[Endpoint Protection and Detection]
Which Cisco ISE feature helps to detect missing patches and helps with remediation?

A. posture assessment
B. profiling policy
C. authentication policy
D. enabling probes

Answer: A

Explanation:

Posture assessment is a feature of Cisco ISE that allows you to check the compliance of endpoints with corporate security policies before allowing them to access the network1. Posture assessment can detect missing patches on endpoints and help with remediation by applying the appropriate posture policy and requirement2. Posture assessment can also check for the presence and status of security software, such as antivirus, antispyware, firewall, and so on3. Posture assessment is one of the core security technologies covered in the Implementing and Operating Cisco Security Core Technologies (SCOR) course4, which prepares you for the Cisco CCNP Security and CCIE Security certifications and for senior-level

www.atmicnetworks.com

security roles. Reference: 1: Posture Service 2: Configure Posture Policies 3: Posture Conditions 4: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Question: 557

[Secure Network Access, Visibility, and Enforcement]

```
aaa new-model
radius-server host 10.0.0.12 key secret12
```

Refer to the exhibit. What is the result of using this authentication protocol in the configuration?

A. The authentication request contains only a username.
B. The authentication request contains only a password.
C. There are separate authentication and authorization request packets.
D. The authentication and authorization requests are grouped in a single packet.

Answer: D

Explanation:

The result of using this authentication protocol in the configuration is that the authentication and authorization requests are grouped in a single packet. This is because the configuration uses RADIUS as the AAA protocol, which combines both authentication and authorization functions in one process. RADIUS is facilitated through AAA and can be enabled only through AAA commands. The aaa new-model global configuration command enables AAA, and the radius-server host command specifies the IP address and the shared secret key of the RADIUS server. The aaa authentication command defines the method list for RADIUS authentication, and the aaa group server command defines the group name and the members of the group. The line and interface commands enable the defined method list to be used. When a user tries to access the router, the router sends a single Access-Request packet to the RADIUS server, which contains the user credentials and other attributes. The RADIUS server then verifies the credentials and returns either an Access-Accept packet, which grants access and may include authorization information, or an Access-Reject packet, which denies access. Therefore, the correct answer is D. Reference: Security Configuration Guide, Cisco IOS XE Everest 16.6.x (Catalyst ... Configuring Basic AAA on an Access Server - Cisco
AAA Server Priority explained with New Radius Server Command Line Configuring AAA on Cisco Devices – RADIUS and TACACS+ - Study-CCNA

Question: 558

[Security Operations]

Which feature must be configured before implementing NetFlow on a router?

A. SNMPv3
B. syslog
C. VRF
D. IP routing

Answer: D

Explanation:

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. NetFlow is based on 7 key fields that identify a flow, such as source and destination IP addresses, source and destination port numbers, layer 3 protocol type, ToS byte, and input logical interface. To enable NetFlow on a router, IP routing must be configured first, because NetFlow relies on IP addresses to classify and monitor traffic. SNMPv3, syslog, and VRF are not required for NetFlow configuration, although they can be used for other purposes such as network management, logging, and virtualization. Reference:

Getting Started with Configuring Cisco IOS NetFlow and NetFlow Data Export (Section: NetFlow Data Capture)
How to configure NetFlow on Cisco routers (Section: Enable NetFlow)
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 (Module 5.1.1)

Question: 559

[Security Concepts]

What is an advantage of the Cisco Umbrella roaming client?

A. the ability to see all traffic without requiring TLS decryption
B. visibility into IP-based threats by tunneling suspicious IP connections
C. the ability to dynamically categorize traffic to previously uncategorized sites
D. visibility into traffic that is destined to sites within the office environment

Answer: B

Explanation:

The Cisco Umbrella roaming client is a cloud-delivered security service for Cisco's next-generation firewall that protects employees when they are off the VPN. No additional agents are required. Simply enable the Umbrella functionality in the Cisco AnyConnect client. One of the advantages of the Umbrella roaming client is that it provides visibility into IP-based threats by tunneling suspicious IP connections to the Umbrella cloud for inspection and blocking. This way, the roaming client can prevent malware, phishing, and command-and-control callbacks from reaching malicious domains and IPs,

regardless of the port or protocol. The Umbrella roaming client also provides DNS-layer security when the VPN is off, and proactive blocking of emerging threats using real-time data analysis. Reference:
Cisco Umbrella Roaming
3 Benefits of Using Roaming Client with Cisco Umbrella
Secure remote workers with the Cisco Umbrella roaming client
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 (Module 5.1.1)

Question: 560

[Endpoint Protection and Detection]

What is a function of Cisco AMP for Endpoints?

A. It detects DNS attacks
B. It protects against web-based attacks
C. It blocks email-based attacks
D. It automates threat responses of an infected host

Answer: D

Explanation:

Cisco AMP for Endpoints is a next generation endpoint security solution that provides prevention, detection, and response capabilities. One of its functions is to automate threat responses of an infected host by isolating it from the network, blocking malicious files, and removing them from all endpoints. This reduces the time and effort required to contain and remediate a threat, and prevents further damage or data loss. According to the source book, Cisco AMP for Endpoints can perform the following automated responses1:
Endpoint Isolation: This feature allows you to isolate an endpoint from the network if it is compromised or infected. This prevents the endpoint from communicating with other devices or servers, and stops the spread of malware or exfiltration of data. You can isolate an endpoint manually from the console, or automatically based on a policy or a detection. You can also restore the network connectivity of an isolated endpoint when it is safe to do so.

File Blocking: This feature allows you to block a file from executing on any endpoint if it is deemed malicious or suspicious. You can block a file manually from the console, or automatically based on a policy or a detection. You can also unblock a file if it is a false positive or no longer a threat. File Removal: This feature allows you to remove a file from any endpoint if it is malicious or unwanted. You can remove a file manually from the console, or automatically based on a policy or a detection. You can also restore a file from quarantine if it is a false positive or needed for analysis. : 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 6: Endpoint Protection and Detection, Lesson 6.2: Cisco AMP for Endpoints, Topic 6.2.3: Automated Responses.

www.atmicnetworks.com

Question: 561

DRAG DROP

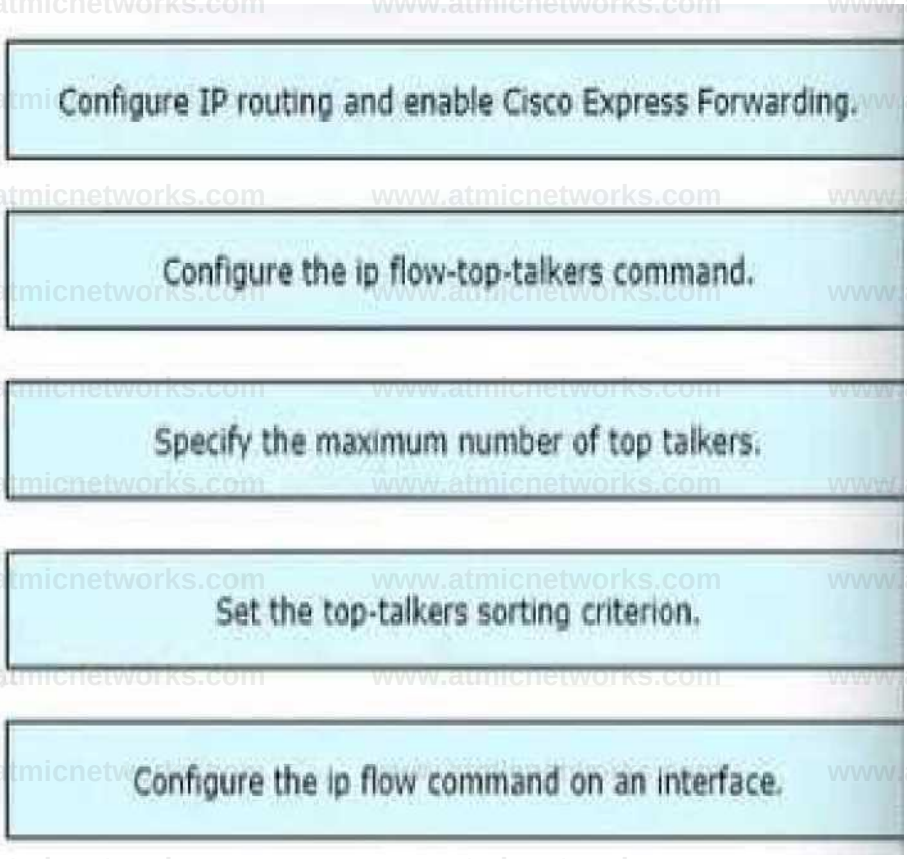
[Security Operations]

A network engineer is configuring NetFlow top talkers on a Cisco router Drag and drop the steps in the process from the left into the sequence on the right



Answer:

Explanation:



Question: 562

[Secure Network Access, Visibility, and Enforcement]

An engineer is implementing DHCP security mechanisms and needs the ability to add additional attributes to profiles that are created within Cisco ISE Which action accomplishes this task?

A. Define MAC-to-IP address mappings in the switch to ensure that rogue devices cannot get an IP address
B. Use DHCP option 82 to ensure that the request is from a legitimate endpoint and send the information to Cisco ISE
C. Modify the DHCP relay and point the IP address to Cisco ISE.
D. Configure DHCP snooping on the switch VLANs and trust the necessary interfaces

Answer: B

Explanation:

DHCP option 82 is a feature that allows the network access device (NAD) to insert additional information into the DHCP request packet from the endpoint. This information can include the switch ID, port number, VLAN ID, and other attributes that can help Cisco ISE to identify and profile the

endpoint. Cisco ISE can use DHCP option 82 to assign the endpoint to the appropriate identity group, policy, and

www.atmicnetworks.com

authorization profile. DHCP option 82 is also useful to prevent rogue DHCP servers from assigning IP addresses to endpoints, as Cisco ISE can verify the legitimacy of the DHCP request based on the option 82 data. To use DHCP option 82, the NAD must be configured to enable this feature and send the option 82 data to Cisco ISE. Cisco ISE must also be configured to accept and parse the option 82 data from the NAD. For more details on how to configure DHCP option 82 on Cisco ISE and NAD, see the references below. Reference:

Configuring the DHCP Probe

Securing Your Network From DHCP Risks

Can we use ISE as DHCP/DNS server to prevent guest traffic using …

Question: 563

[Security Concepts]

Which feature requires that network telemetry be enabled?

A. per-interface stats
B. SNMP trap notification
C. Layer 2 device discovery
D. central syslog system

Answer: C

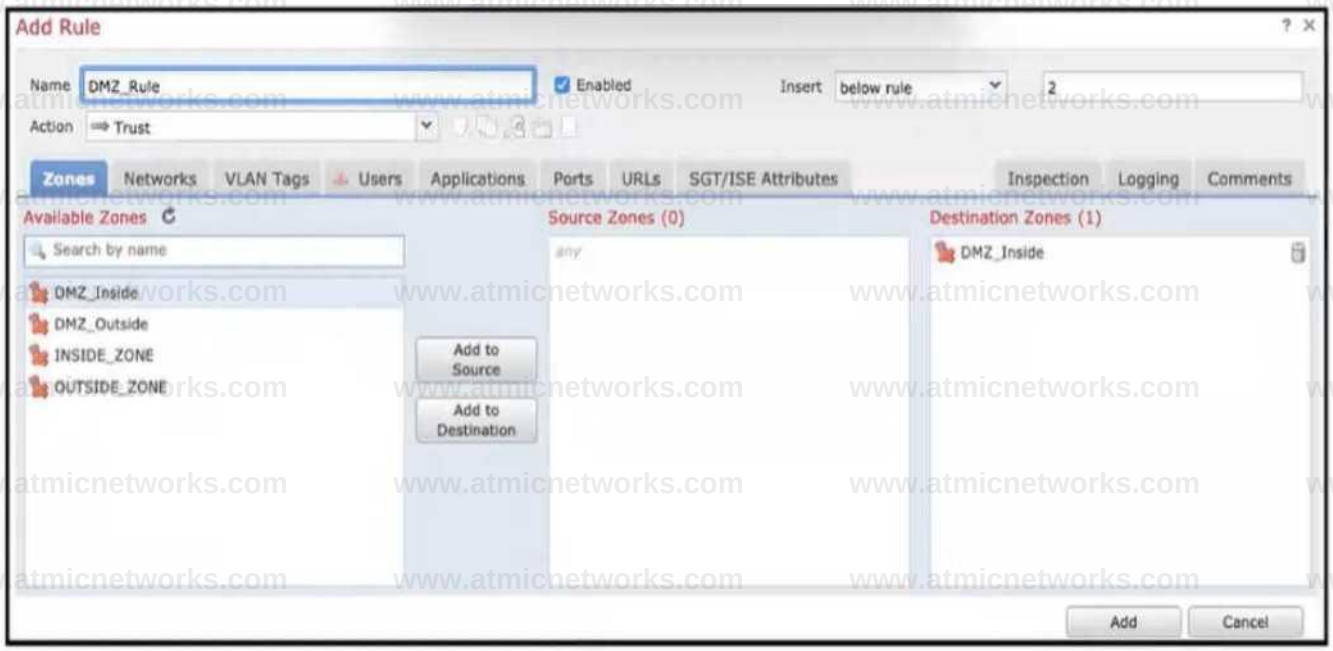
Explanation:

Network telemetry is a technology for gaining network insight and facilitating efficient and automated network management. It encompasses various techniques for remote data generation, collection, correlation, and consumption1. Network telemetry can be used for various purposes, such as network performance monitoring, security analysis, troubleshooting, and optimization. One of the applications of network telemetry is Layer 2 device discovery, which allows network operators to discover and map the physical topology of the network, including switches, routers, hosts, and links. Layer 2 device discovery can be achieved by using protocols such as Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP), which enable network devices to advertise their identity, capabilities, and neighbors to other devices on the same network segment. To enable Layer 2 device discovery, network telemetry must be enabled on the network devices, so that they can send and receive LLDP or CDP packets. This feature requires network telemetry to be enabled, because without it, the network devices would not be able to exchange information about their topology and configuration. Therefore, the correct answer is C. Layer 2 device discovery. Reference: 1: RFC 9232: Network Telemetry Framework - Internet Engineering Task Force

Question: 564

[Security Concepts]

v



Refer to the exhibit When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZjnside zone once the configuration is deployed?

A. All traffic from any zone to the DMZ_inside zone will be permitted with no further inspection B. No traffic will be allowed through to the DMZ_inside zone regardless of if it's trusted or not C. All traffic from any zone will be allowed to the DMZ_inside zone only after inspection D. No traffic will be allowed through to the DMZ_inside zone unless it's already trusted

Answer: A

Explanation:

The access control rule in the exhibit has the following characteristics:
The rule name is DMZ_Rule and it is enabled.
The action set for this rule is Trust, meaning traffic matching this rule will not be subjected to further inspection.
The source zones are not specified, meaning any zone can match this rule.
The destination zone is DMZ_Inside, meaning only traffic destined to this zone can match this rule.
Therefore, the effect of this rule is that all traffic from any zone to the DMZ_Inside zone will be permitted with no further inspection. This is the correct answer, option A.
The other options are incorrect because they do not match the configuration of the rule or the behavior of the Trust action. Option B is incorrect because traffic will be allowed through to the

DMZ_Inside zone, not blocked. Option C is incorrect because traffic will not be inspected before being allowed to the DMZ_Inside zone. Option D is incorrect because traffic does not need to be trusted to be allowed to the DMZ_Inside zone. Reference:
Firepower Management Center Configuration Guide, Version 6.6 - Access Control Rules
Firepower Management Center Device Configuration Guide, 7.1 - Access Control Policies
How to Deploy FMC/FTD part 2 – Access Control Policies

www.atmicnetworks.com

Question: 565

[Securing the Cloud]

An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration Which solution best meets these requirements?

A. Cisco CloudLock
B. Cisco AppDynamics Cloud Monitoring
C. Cisco Umbrella
D. Cisco Stealthwatch

Answer: A

Explanation:

Cisco CloudLock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. CloudLock's simple, open, and automated approach uses APIs to manage the risks in your cloud app ecosystem. With CloudLock you can more easily combat data breaches while meeting compliance regulations1.

Cisco CloudLock provides the following features that meet the requirements of visibility into data transfers as well as protection against data exfiltration:

User security: Cloudlock uses advanced machine learning algorithms to detect anomalies based on multiple factors. It also identifies activities outside allowed countries and spots actions that seem to take place at impossible speeds across distances1.

Data security: Cloudlock's data loss prevention (DLP) technology continuously monitors cloud environments to detect and secure sensitive information. It provides countless out-of-the-box policies as well as highly tunable custom policies. It also supports inline and out-of-band data inspection and blocking capabilities to protect sensitive data12.

App security: The Cloudlock Apps Firewall discovers and controls cloud apps connected to your corporate environment. You can see a crowd-sourced Community Trust Rating for individual apps, and you can ban or allowlist them based on risk1.

The other solutions do not provide the same level of visibility and protection as Cisco CloudLock: Cisco Umbrella is a cloud-delivered network security service that provides DNS-layer security, secure web gateway, cloud-delivered firewall, cloud access security broker, and threat intelligence3. It does not offer data security features such as DLP, data inspection, and data blocking4.

Cisco AppDynamics Cloud Monitoring is a cloud-native application performance management solution that helps you monitor, troubleshoot, and optimize your cloud applications. It does not offer user security, data security, or app security features as a CASB solution.

Cisco Stealthwatch is a network traffic analysis solution that provides visibility and threat detection across your network, endpoints, and cloud. It does not offer data security features such as DLP, data inspection, and data blocking.

: 3: Cisco Umbrella Packages - Cisco Umbrella 1: Cisco Cloudlock - Cisco 2: Cisco Cloudlock Cisco Cloudlock: Secure Cloud Data 4: Easy to Deploy & Simple to Manage CASB Solution - Cisco Umbrella : Cisco AppDynamics Cloud Monitoring : Cisco Stealthwatch - Cisco

www.atmicnetworks.com

Question: 566

[Endpoint Protection and Detection]

An engineer needs to detect and quarantine a file named abc424400664 zip based on the MD5 signature of the file using the Outbreak Control list feature within Cisco Advanced Malware Protection (AMP) for Endpoints The configured detection method must work on files of unknown disposition Which Outbreak Control list must be configured to provide this?

A. Blocked Application
B. Simple Custom Detection
C. Advanced Custom Detection
D. Android Custom Detection

Answer: B

Explanation:

Simple Custom Detection is a feature of Cisco AMP for Endpoints that allows administrators to block specific files based on their SHA-256 or MD5 hashes. This feature can be used to detect and quarantine files of unknown disposition, such as abc424400664.zip, by adding their hashes to a custom list in the AMP portal. The list can then be applied to a policy that is assigned to the endpoints. Simple Custom Detection works on files of any type, size, or platform, unlike the other options that are either platform-specific (Android Custom Detection), size-limited (Blocked Application), or signature-based (Advanced Custom Detection). Reference: 1, 2, 3

Question: 567

[Secure Network Access, Visibility, and Enforcement]

With regard to RFC 5176 compliance, how many IETF attributes are supported by the RADIUS CoA feature?

A. 3
B. 5
C. 10
D. 12

Answer: B

Explanation:

The RADIUS CoA feature supports five IETF attributes as defined in RFC 5176. These are: Event-Timestamp: This attribute indicates the time when the CoA request was generated by the server.

State: This attribute contains a value that is copied from the Access-Accept message that authorized the session.

Session-Timeout: This attribute specifies the maximum number of seconds of service provided to the user before termination of the session or prompt.
Idle-Timeout: This attribute specifies the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.
Filter-Id: This attribute identifies the filter list to be applied to the user session.
The RADIUS CoA feature also supports vendor-specific attributes (VSAs) that are defined by Cisco or other vendors. These VSAs can be used to perform additional actions such as port shutdown, port bounce, or security and password accounting. Reference := Some possible references are:
RFC 5176: This document describes the dynamic authorization extensions to RADIUS, including the CoA request and response codes, and the supported IETF attributes.
RADIUS Change of Authorization - Cisco: This document provides the configuration guide for the RADIUS CoA feature on Cisco IOS devices, including the supported IETF and Cisco VSAs.
Supported IETF attributes in RFC 5176 - Ruckus Networks: This document lists the supported IETF attributes and error clause values for the RADIUS CoA feature on Ruckus devices.
V

Question: 568

[Security Operations]

An engineer is configuring cloud logging using a company-managed Amazon S3 bucket for Cisco Umbrella logs. What benefit does this configuration provide for accessing log data?

A. It is included m the license cost for the multi-org console of Cisco Umbrella
B. It can grant third-party SIEM integrations write access to the S3 bucket
C. No other applications except Cisco Umbrella can write to the S3 bucket
D. Data can be stored ofline for 30 days.

Answer: B

Explanation:

Using a company-managed Amazon S3 bucket for Cisco Umbrella logs allows the administrator to have full control over the access and lifecycle of the log data. This configuration can grant third-party SIEM integrations write access to the S3 bucket, which can enable more advanced analysis and correlation of the log data with other sources. This configuration also provides more flexibility in terms of how long the data can be stored ofline, as opposed to the Cisco-managed S3 bucket, which has a fixed retention period of 30 days. Reference:
Enable Logging to Your Own S3 Bucket
Centralized Umbrella Log Management with Amazon's S3 service for MSP, MSSP, and Multi-org customers

www.atmicnetworks.com

Question: 569

[Security Concepts]

For a given policy in Cisco Umbrella, how should a customer block website based on a custom list?

A. by specifying blocked domains in me policy settings
B. by specifying the websites in a custom blocked category
C. by adding the websites to a blocked type destination list
D. by adding the website IP addresses to the Cisco Umbrella blocklist

Answer: B

Explanation:

To block a website based on a custom list, the customer should add the websites to a blocked type destination list. A destination list is a custom list of domains or URLs that the customer wants to allow or block for their identities. The customer can create destination lists through the Policy Components > Destination Lists page, or within the policy wizard when creating or editing a policy. The custom URL destination block lists feature enables Umbrella to extend a domain level block list

to encompass full and partial URLs. In turn, this allows the customer to block certain portions of a website based specifically on the full or partial URL. This feature requires the customer to enable the intelligent proxy and install a root certificate for SSL decryption. Reference: Configure Web Policies and Destination Lists - Cisco Umbrella

Control Access to Custom URLs - Umbrella SIG User Guide

Cisco 350-701: How should customer block websites based on custom list

Umbrella Dashboard: New Features—Custom blocked URLs

Understanding Destination lists supported entries and … - Cisco Umbrella

Question: 570

[Security Concepts]

||

An engineer musí set up 200 new laptops on a network and wants to prevent the users from moving their laptops around to simplify administration Which switch port MAC address security setting must be used?

A. sticky
B. static
C. aging
D. maximum

www.atmicnetworks.com

Answer: A

Explanation:

The switch port MAC address security setting that must be used is sticky. This option allows the switch to dynamically learn the MAC addresses of the devices connected to the port and add them to the running configuration. If the port is shut down or the switch is restarted, the MAC addresses remain associated with the port and are not aged out. This way, the engineer can limit the number of MAC addresses per port and prevent unauthorized devices from accessing the network. The sticky option also allows the engineer to manually configure some MAC addresses and let the switch learn the rest. Reference:

Configuring Port Security - Cisco (Section: Allowing Traffic Based on the Host MAC Address) How to configure port-security on Cisco Switch - NetworkLessons.com (Section: Sticky MAC addresses)

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 (Module 5.1.1)

Question: 571

[Network Security]

Which Cisco Firewall solution requires zone definition?

A. CBAC
B. Cisco AMP
C. ZBFW
D. Cisco ASA

Answer: C

Explanation:

ZBFW stands for Zone-Based Firewall, which is a feature that allows unidirectional application of IOS firewall policies between groups of interfaces known as zones. Interfaces are assigned to zones, and firewall rules are applied to specific types of traffic moving in one direction between the zones. ZBFW enforces a secure inter-zone policy by default, meaning traffic cannot pass between security zones until an explicit policy allowing that traffic is defined. The zone itself is an abstraction of multiple interfaces with the same or similar security requirements that can be logically grouped together. ZBFW is CBAC's replacement and offers intuitive policies for multiple-interface routers, increased granularity of firewall policy application, and a default deny-all policy that prohibits traffic between firewall security zones until an explicit policy is applied to allow desirable traffic. ZBFW is supported on IOS devices running 12.4(6)T or later, and ASR devices running 12.2(33) or later. Reference: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Securing the Cloud, Lesson 4.1: Introducing Cisco Cloud Services Router 1000V Series, Topic 4.1.2: Zone-Based Firewall

Understand the Zone-Based Policy Firewall Design

Managing Zone-based Firewall Rules

Zone Based Firewall Overview CBAC vs. Zone-based firewall

www.atmicnetworks.com

Question: 572

[Endpoint Protection and Detection]

A company recently discovered an attack propagating throughout their Windows network via a file named abc428565580xyz exe The malicious file was uploaded to a Simple Custom Detection list in the AMP for Endpoints Portal and the currently applied policy for the Windows clients was updated to reference the detection list Verification testing scans on known infected systems shows that AMP

for Endpoints is not detecting the presence of this file as an indicator of compromise What must be performed to ensure detection of the malicious file?

A. Upload the malicious file to the Blocked Application Control List
B. Use an Advanced Custom Detection List instead of a Simple Custom Detection List
C. Check the box in the policy configuration to send the file to Cisco Threat Grid for dynamic analysis
D. Upload the SHA-256 hash for the file to the Simple Custom Detection List

Answer: D

Explanation:

A Simple Custom Detection List is a feature of Cisco AMP for Endpoints that allows administrators to create a list of SHA-256 hashes of files that they want to detect, block, and quarantine on their endpoints. The list can be applied to a policy and the connectors will synchronize with the latest changes. However, the list only works with the exact SHA-256 hashes that are provided, and it does not detect any variations or modifications of the files. Therefore, if the malicious file abc428565580xyz.exe has been altered in any way, such as by changing its name, size, or content, the Simple Custom Detection List will not be able to recognize it as a threat. To ensure detection of the malicious file, the administrator must upload the SHA-256 hash of the current version of the file to the Simple Custom Detection List, or use another method that can detect file variations, such as an Advanced Custom Detection List or Cisco Threat Grid. Reference := Some possible references are:
Configure a Simple Custom Detection List on the AMP for Endpoints Portal
Create an Advanced Custom Detection List in Cisco Secure Endpoint

[Cisco AMP for Endpoints User Guide]
https://www.cisco.com/c/en/us/td/docs/security/firepower/amp/6-3/user-guide/amp-user- guide.pdf

Question: 573

[Secure Network Access, Visibility, and Enforcement]

Which two configurations must be made on Cisco ISE and on Cisco TrustSec devices to force a session to be adjusted after a policy change is made? (Choose two)

A. posture assessment
B. aaa authorization exec default local
C. tacacs-server host 10.1.1.250 key password
D. aaa server radius dynamic-author
E. CoA

Answer: D,E

Explanation:

To force a session to be adjusted after a policy change is made, two configurations are required on Cisco ISE and on Cisco TrustSec devices: Dynamic Authorization and Change of Authorization (CoA). Dynamic Authorization allows Cisco ISE to send commands to network devices to change the authorization status of a user session. CoA is a feature that enables Cisco ISE to send a RADIUS message to a network device to reauthenticate or disconnect a user session. These two configurations enable Cisco ISE to apply the updated policy to the user session without requiring the user to log out and log in again.

According to the source book, the steps to configure Dynamic Authorization and CoA are as follows1: On Cisco ISE, navigate to Administration > Network Resources > Network Devices and select the network device that supports TrustSec.

On the Edit Network Device page, select the Advanced TrustSec Settings tab and check the Support for CoA check box.

On the same tab, select the appropriate CoA type from the drop-down list. The options are RADIUS Disconnect, Port Bounce, and Reauth.

Click Submit to save the changes.

On the network device, enter the global configuration mode and issue the command aaa server radius dynamic-author to enable Dynamic Authorization.

Optionally, you can specify the source interface, authentication key, and port number for the Dynamic Authorization messages.

Exit the global configuration mode and save the configuration.

: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Secure Connectivity, Lesson 4.2: Implementing TrustSec, Topic 4.2.3: Configuring TrustSec on Cisco ISE and Network Devices, pp. 4-83 to 4-85.

Question: 574

[Content Security]

An engineer is configuring Cisco WSA and needs to deploy it in transparent mode. Which configuration component must be used to accomplish this goal?

A. MDA on the router
B. PBR on Cisco WSA
C. WCCP on switch
D. DNS resolution on Cisco WSA

Answer: C

Explanation:

To deploy Cisco WSA in transparent mode, the configuration component that must be used is WCCP on switch. WCCP stands for Web Cache Communication Protocol, which is a protocol that allows a network device (such as a switch) to redirect web traffic to a proxy server (such as Cisco WSA) transparently. This means that the client does not need to configure any proxy settings on the browser, and the proxy server can intercept and process the web requests and responses without the client's knowledge. WCCP can also provide load balancing and failover capabilities for multiple proxy servers.

The other options are incorrect because they are not required or relevant for transparent mode deployment. Option A is incorrect because MDA (Multilink PPP Dial Access) is a feature that allows multiple physical links to be aggregated into a single logical link for dial-up connections. It has nothing to do with transparent mode. Option B is incorrect because PBR (Policy-Based Routing) is a feature that allows routing decisions to be based on criteria other than the destination IP address, such as source IP address, protocol, port, etc. It is not necessary for transparent mode, as WCCP can handle the traffic redirection. Option D is incorrect because DNS resolution on Cisco WSA is not a configuration component, but a function that allows the proxy server to resolve domain names to IP addresses. It is not specific to transparent mode, as it is also used in explicit mode. Reference: What is the difference between transparent and forward proxy mode? User Guide for AsyncOS 12.7 for Cisco Web Security Appliances - LD (Limited Deployment) - Acquire End-User Credentials

Cisco WSA : Is it possible to use web proxy in transparent mode without WCCP?

Question: 575

[Secure Network Access, Visibility, and Enforcement]

Which feature is used in a push model to allow for session identification, host reauthentication, and session termination?

A. AAA attributes
B. CoA request
C. AV pair
D. carrier-grade NAT

Answer: B

Explanation:

A CoA request is a network protocol message used in the context of network access control and authentication systems. It is typically employed in scenarios where a user's access privileges or attributes need to be modified during an active network session. CoA requests are commonly used in conjunction with the RADIUS protocol, which is widely used for managing user authentication and authorization in network environments. When a CoA request is initiated, it is sent by a

network access server (NAS) to a RADIUS server to request a change in the user's authorization state or attributes. The CoA request contains information specifying the desired change, such as granting additional access privileges, revoking existing privileges, modifying session parameters, or updating user attributes. The RADIUS server processes the CoA request and applies the necessary changes to the user's session in real-time, allowing dynamic adjustments to the user's authorization and network access. CoA requests are often utilized in scenarios where an administrator needs to promptly update a user's access rights without requiring them to terminate their current session. This flexibility is particularly valuable in environments that demand fine-grained access control or where access privileges need to be adjusted based on changing circumstances or policies. Reference :=

Some possible references for this answer are:

RADIUS Change of Authorization - Cisco

What is a CoA Request? - Portnox

RADIUS Change of Authorization: Explained - Cloud RADIUS

Question: 576

[Security Concepts]

An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices The default management port conflicts with other communications on the network and must be changed What must be done to ensure that all devices can communicate together?

A. Set the sftunnel to go through the Cisco FTD
B. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices
C. Set the sftunnel port to 8305.
D. Manually change the management port on Cisco FMC and all managed Cisco FTD devices

Answer: D

Explanation:

The management port on Cisco FMC is used to establish a secure connection with the managed Cisco FTD devices. If the default management port (8305) conflicts with other communications on the network, it must be changed on both the Cisco FMC and the Cisco FTD devices. This cannot be

done automatically by the Cisco FMC, as it would lose connectivity with the devices. Therefore, the administrator must manually change the management port on the Cisco FMC and all the managed Cisco FTD devices using the command line interface (CLI). The steps to change the management port are as follows:

Log into the CLI of the Cisco FMC and the Cisco FTD devices using a console connection or SSH. Enter the configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces command to change the management port on the Cisco FMC. For example, configure network ipv4 manual 10.10.10.10 255.255.255.0 data-interfaces changes the management port to 10.10.10.10/24.

Enter the configure network {ipv4 | ipv6} manual ip_address netmask gateway management- only command to change the management port on the Cisco FTD devices. For example, configure network ipv4 manual 10.10.10.11 255.255.255.0

10.10.10.10 management-only changes the management port to 10.10.10.11/24 and sets the gateway to the Cisco FMC's management port. Save the configuration and restart the Cisco FMC and the Cisco FTD devices. Verify the connectivity between the Cisco FMC and the Cisco FTD devices using the show managers command on the Cisco FTD devices and the show devices command on the Cisco FMC. Reference :=
Firepower Management Center Device Configuration Guide, 7.1 - Device Management
Change management port fmc 1600 - Cisco Community
Solved: FMC 2120 FTD Management Only Port - Cisco Community
Change the FMC Access Interface from Management to Data

Question: 577

[Security Concepts]
What is the concept of Cl/CD pipelining?

A. The project is split into several phases where one phase cannot start before the previous phase finishes successfully.
B. The project code is centrally maintained and each code change should trigger an automated build and test sequence
C. The project is split into time-limited cycles and focuses on pair programming for continuous code review
D. Each project phase is independent from other phases to maintain adaptiveness and continual improvement

Answer: B

Explanation:

Cl/CD pipelining is a method of software development that aims to deliver software faster and more reliably by automating the process of integrating, testing, and deploying code changes. Cl stands for continuous integration, which means that every code change is merged into a shared repository and verified by automated tests. CD stands for continuous delivery, which means that the code is always

in a deployable state and can be released to production environments with minimal human intervention. Cl/CD pipelining enables developers to collaborate more effectively, detect and fix errors earlier, and deliver value to customers more frequently. Cl/CD pipelining is a key practice of DevOps, a culture and set of processes that bridge the gap between development and operations teams. Reference:
https://www.redhat.com/en/topics/devops/what-cicd-pipeline https://about.gitlab.com/topics/ci-cd/cicd-pipeline/

Question: 578

[Secure Network Access, Visibility, and Enforcement]
Why should organizations migrate to a multifactor authentication strategy?

A. Multifactor authentication methods of authentication are never compromised
B. Biometrics authentication leads to the need for multifactor authentication due to its ability to be hacked easily
C. Multifactor authentication does not require any piece of evidence for an authentication mechanism
D. Single methods of authentication can be compromised more easily than multifactor authentication

Answer: D

Explanation:

Multifactor authentication (MFA) is a security measure that requires two or more proofs of identity to grant access to a resource, such as a username and password, a one-time code, a smart card, etc.1 MFA provides stronger protection than single-factor authentication (SFA), which only requires one proof of identity, such as a password. SFA can be compromised more easily by attackers who can guess, steal, or intercept passwords, or use phishing or social engineering techniques to trick users into revealing their credentials. MFA adds an extra layer of security that makes it harder for attackers to gain access, even if they have the password. MFA can also prevent unauthorized access from lost or stolen devices, as the attacker would need another factor to authenticate. MFA can also deter attackers from targeting an organization, as they would need to invest more time and resources to bypass the security measures. Therefore, organizations should migrate to a multifactor authentication strategy to enhance their security posture and protect their data and assets. Reference := 1: What is Multi-Factor Authentication (MFA)? - Auth0

Question: 579

[Security Concepts]
Which DoS attack uses fragmented packets in an attempt to crash a target machine?

A. teardrop
B. smurf
C. LAND
D. SYN flood

Answer: A

Explanation:

A teardrop attack is a type of DoS attack that uses fragmented packets in an attempt to crash a target machine. The attacker sends IP packets that are deliberately malformed, such that the fragments overlap or have invalid offsets. When the target machine tries to reassemble the packets, it encounters an error or a buffer overflow, resulting in a system crash or a denial of service. Teardrop attacks exploit a vulnerability in the TCP/IP fragmentation reassembly process, which is responsible for splitting and recombining large packets that exceed the maximum transmission unit (MTU) size. Teardrop attacks can affect various operating systems, such as Windows, Linux, and BSD, depending on the implementation of the TCP/IP stack. Teardrop attacks are also known as IP fragmentation attacks or overlapping fragment attacks. Reference:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 5: Securing the Cloud, Lesson 5.2:

Cloud Security Threats, Topic 5.2.2: DoS Attacks
What is an IP Fragmentation Attack (Teardrop ICMP/UDP)
Teardrop Attack - Radware
What Is a Teardrop Attack? | F5

Reference: https://www.radware.com/security/ddos-knowledge-center/ddospedia/teardrop-attack/

Question: 580

[Security Concepts]
An engineer needs to configure a Cisco Secure Email Gateway (SEG) to prompt users to enter multiple forms of identification before gaining access to the SEG. The SEG must also join a cluster using the preshared key of cisc421555367. What steps must be taken to support this?

A. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG GUI.
B. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG CLI.
C. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI
D. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG GUI.

Answer: C

Explanation:

The correct answer is to enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI. Two-factor authentication is a security feature that requires users to provide two forms of identification before accessing the SEG, such as a username and password, and a onetime code or token. This adds an extra layer of protection against unauthorized access and phishing attacks. The SEG supports two-factor authentication through external RADIUS servers, which can be configured on the System Administration > Users page in the web interface, or the userconfig command in the CLI. See User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) (Section: Two-Factor Authentication) for more details.
To join a cluster, the SEG must communicate with other cluster members using either SSH or CCS (Cluster Communication Service). The cluster communication port and method can be configured on the Network > Cluster Communication page in the web interface, or the clusterconfig command in the CLI. See User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) (Section: Cluster Communication) for more details.
If two-factor authentication is enabled on the SEG, it cannot join a cluster using the web interface, because the web interface does not support two-factor authentication for cluster operations. Therefore, the SEG must join the cluster using the CLI, and provide a pre-shared key that matches the cluster's admin passphrase. The pre-shared key can be configured using the clusterconfig > prepjoin command in the CLI. See User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) (Section: Creating and Joining a Cluster) for more details.
The other options are incorrect because they either use the wrong authentication server (TACACS+ instead of RADIUS), or the wrong communication method (GUI instead of CLI). Reference: User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) Configure an Email Security Appliance (ESA) Cluster - Cisco

Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.pdf

www.atmicnetworks.com

Question: 581

[Security Concepts]
What are two workload security models? (Choose two.)

A. SaaS
B. PaaS
C. off-premises
D. on-premises
E. IaaS

Answer: C,D

Explanation:

Workload security models refer to the ways of protecting applications, services, and capabilities that run on a cloud resource. There are different types of cloud deployment models, such as public, private, hybrid, and multicloud, and different types of cloud service models, such as IaaS, PaaS, and SaaS. However, these are not workload security models, but rather ways of describing the cloud environment and the level of abstraction. Workload security models are more focused on the location and ownership of the workloads, and how they are secured. The two main workload security models are off-premises and on-premises. Off-premises workload security model means that the workloads are hosted and managed by a third-party cloud service provider, such as AWS, Azure, or GCP. The cloud service provider is responsible for the security of the underlying infrastructure, such as the physical servers, network devices, storage systems, and hypervisors. The customer is responsible for the security of the workloads themselves, such as the guest operating systems, applications, data, and users. The customer can use various tools and techniques to secure their workloads, such as encryption, firewalls, identity and access management, vulnerability scanning, and logging and monitoring. On-premises workload security model means that the workloads are hosted and managed by the customer on their own data center or private cloud. The customer is responsible for the security of both the infrastructure and the workloads, and has full control and visibility over them. The customer can use similar tools and techniques as the off-premises model, but also has to deal with the physical security, network security, and compliance requirements of their own environment. Reference:
What Is Workload Security? On-Premises, Cloud, Kubernetes, and More
What is Cloud Workload Security? - CyberArk
What is Cloud Workload Protection? | Workload Security | VMware What is Cloud Workload Security? - Check Point Software Introduction To Classic Security Models - GeeksforGeeks

Question: 582

[Security Concepts]
Client workstations are experiencing extremely poor response time. An engineer suspects that an attacker is eavesdropping and making independent connections while relaying messages between victims to make them think they are talking to each other over a private connection. Which feature must be enabled and configured to provide relief from this type of attack?

A. Link Aggregation

www.atmicnetworks.com

B. Reverse ARP
C. private VLANs
D. Dynamic ARP Inspection

Answer: D

Explanation:

Dynamic ARP Inspection (DAI) is a security feature that protects ARP (Address Resolution Protocol) from an attack like ARP poisoning. ARP poisoning is a technique where an attacker sends forged ARP responses to trick hosts into associating IP addresses with the attacker's MAC address. This allows the attacker to intercept, modify, or drop traffic between the victims, creating a "man-in-the-middle" scenario. DAI can prevent this attack by validating ARP packets on untrusted interfaces, using information from the DHCP snooping database and/or an ARP access-list. If the ARP packet contains invalid MAC address to IP address bindings, it will be dropped and logged. DAI can also rate-limit ARP packets to mitigate ARP flooding attacks. DAI is configured on a per-VLAN basis and requires DHCP snooping to be enabled on the same VLANs. Reference :=
Some possible references are:
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 2: Network Security, Lesson 2.4: Implement Layer 2 Security
Understanding and Configuring Dynamic ARP Inspection
DAI (Dynamic ARP Inspection)

Question: 583

[Endpoint Protection and Detection]
What does Cisco ISE use to collect endpoint attributes that are used in profiling?

A. probes
B. posture assessment
C. Cisco AnyConnect Secure Mobility Client
D. Cisco pxGrid

Answer: A

Explanation:

Cisco ISE uses probes to collect endpoint attributes that are used in profiling. Probes are software modules that run on the ISE Policy Service Nodes (PSNs) and gather information about the endpoints connected to the network. Probes can use various protocols and methods to collect endpoint attributes, such as RADIUS, DHCP, SNMP, HTTP, DNS, NetFlow, NMAP, Active Directory, and Cisco pxGrid. The collected attributes are then matched to predefined or custom conditions that define the endpoint profiles. Endpoint profiling enables ISE to identify and classify the endpoints and apply the appropriate policies based on their identity, role, and context12. Reference: 1: Cisco ISE 2.4 Endpoint Profiling - Cisco 2: How To Create an Endpoint Profile - Cisco Community Reference:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/ 2-

6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_010100.html.xml#:~:text=Network%20probe%20is%20a%20method,in%20the%20Cisco%20ISE%20database.

Question: 584

[Security Concepts]

Which threat intelligence standard contains malware hashes?

A. advanced persistent threat
B. open command and control
C. structured threat information expression
D. trusted automated exchange of indicator information

Answer: D

Explanation:

The threat intelligence standard that contains malware hashes is trusted automated exchange of indicator information (TAXII). TAXII is a protocol that enables the exchange of cyber threat information in a standardized and automated manner. It supports various types of threat intelligence, such as indicators of compromise (IOCs), observables, incidents, tactics, techniques, and procedures (TTPs), and campaigns. Malware hashes are one example of IOCs that can be shared using TAXII. Malware hashes are cryptographic signatures that uniquely identify malicious files or programs. They can be used to detect and block malware infections on endpoints or networks. TAXII uses STIX (structured threat information expression) as the data format for representing threat intelligence. STIX is a language that defines a common vocabulary and structure for describing cyber threat information. STIX allows threat intelligence producers and consumers to share information in a consistent and interoperable way. STIX defines various objects and properties that can be used to represent different aspects of cyber threat information, such as indicators, observables, incidents, TTPs, campaigns, threat actors, courses of action, and relationships. Malware hashes can be expressed as observables in STIX, which are concrete items or events that are observable in the operational domain. Observables can have various types, such as file, process, registry key, URL, IP address, domain name, etc. Each observable type has a set of attributes that describe its properties. For example, a file observable can have attributes such as name, size, type, hashes, magic number, etc. A hash attribute can have a type (such as MD5, SHA1, SHA256, etc.) and a value (such as the hexadecimal representation of the hash). A file observable can have one or more hash attributes to represent different hashing algorithms applied to the same file. For example, a file observable can have both MD5 and SHA256 hashes to increase the confidence and accuracy of identifying the file. The other options are incorrect because they are not threat intelligence standards that contain malware hashes. Option A is incorrect because advanced persistent threat (APT) is not a standard, but a term that describes a stealthy and sophisticated cyberattack that aims to compromise and maintain access to a target network or system over a long period of time. Option B is incorrect because open command and control (OpenC2) is not a standard that contains malware hashes, but a language that enables the command and control of cyber defense components, such as sensors, actuators, and orchestrators. Option C is incorrect because structured threat information expression (STIX) is not a standard that contains malware hashes, but a data format that represents threat intelligence. STIX uses TAXII as the transport protocol for exchanging threat intelligence, including malware hashes. Reference:

TAXII

STIX

Malware Hashes

www.atmicnetworks.com

Question: 585

[Security Concepts]
Which two commands are required when configuring a flow-export action on a Cisco ASA? (Choose two.)

A. flow-export event-type
B. policy-map
C. access-list
D. flow-export template timeout-rate 15
E. access-group

Answer: A,B

Explanation:

To configure a flow-export action on a Cisco ASA, you need to use the flow-export eventtype command and the policy-map command. The flow-export event-type command specifies the type of events that trigger the export of NetFlow Security Event Logging (NSEL) records to a collector. The policy-map command creates or modifies a policy map that can be applied to one or more interfaces to specify a service policy. A service policy consists of a traffic class and one or more actions to be applied to the traffic class. One of the actions can be a flow-export action that matches the NSEL events and sends them to a collector. The other commands are not required for configuring a flow-export action. The access-list command creates or modifies an access list that can be used to filter traffic or match traffic classes, but it is not mandatory for a flow-export action. The flow-export template timeout-rate command specifies how often the ASA sends the template to the collector, but it is not part of the flow-export action configuration. The access-group command applies an access list to an interface, but it is not related to the flow-export action. Reference:
Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6 - Configuring Network Secure Event Logging (NSEL)
Solved: Flow-Export problem - Cisco Community
How to configure NetFlow on Cisco ASA firewalls - Auvik Support Configuring Cisco's ASA for NSEL Export to the StealthWatch System

Question: 586

[Security Concepts]
Which Cisco security solution secures public, private, hybrid, and community clouds?

A. Cisco ISE
B. Cisco ASAv
C. Cisco Cloudlock
D. Cisco pxGrid

Answer: C

Explanation:

Cisco Cloudlock is a cloud-native security solution that secures public, private, hybrid, and community clouds. It provides visibility, compliance, threat protection, and data security for cloud applications and environments. Cisco Cloudlock integrates with various cloud platforms and services, such as AWS, Azure, Google Cloud, Office 365, Salesforce, Dropbox, and more. Cisco Cloudlock monitors user activities, configurations, and sensitive data across the cloud, and alerts or blocks any violations of policies or regulations. Cisco Cloudlock also leverages user and entity behavior analytics (UEBA) to detect and respond to anomalous or malicious behaviors in the cloud. Cisco Cloudlock helps organizations protect their cloud assets and data, while enabling them to embrace the benefits of cloud computing. Reference :=
Cloud and Application Security - Cisco
Cloud Security Products and Solutions - Cisco
What Is Cloud Security? - Cisco

[Cisco Cloudlock: Cloud-Native CASB and Cloud Cybersecurity Platform]

Question: 587

[Endpoint Protection and Detection]
A university policy must allow open access to resources on the Internet for research, but internal workstations are exposed to malware. Which Cisco AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

A. file prevalence B. file discovery C. file conviction D. file manager

Answer: B

Explanation:

File discovery is a feature of Cisco AMP that allows the engineering team to search for files across all endpoints in the network based on their SHA-256 hashes. File discovery can help identify whether a file is installed on a selected few workstations, and also provide information such as file name, path, size, date, and disposition. File discovery can be used to locate malicious files, unauthorized software, or sensitive data on the endpoints. File discovery can be accessed from the Outbreak Control menu in the AMP console1. Reference: https://www.cisco.com/c/en/us/support/docs/security/amp- endpoints/215176-configure-a-simple-custom-detection-list.html

www.atmicnetworks.com

Question: 588

[Endpoint Protection and Detection]

Which action must be taken in the AMP for Endpoints console to detect specific MD5 signatures on endpoints and then quarantine the files?

A. Configure an advanced custom detection list.
B. Configure an IP Block & Allow custom detection list
C. Configure an application custom detection list
D. Configure a simple custom detection list

Answer: D

Explanation:

A simple custom detection list is a feature of AMP for Endpoints that allows you to specify a list of file hashes (MD5, SHA-1, or SHA-256) that you want to detect, block, and quarantine on your endpoints. You can create a simple custom detection list from the Outbreak Control section of the AMP for Endpoints console, and apply it to a policy that is assigned to your endpoints. When the AMP connector on the endpoint encounters a file that matches the hash in the list, it will perform the action that you specified, such as blocking the file execution, sending an alert, or quarantining the file. A simple custom detection list is useful when you want to quickly and easily block specific files that are known to be malicious or unwanted, without having to create a complex signature or rule12 Reference := 1: Configure a Simple Custom Detection List on the AMP for Endpoints Portal 2: Create an Advanced Custom Detection List in Cisco Secure Endpoint

Question: 589

[Content Security]

What is the target in a phishing attack?

A. perimeter firewall
B. IPS
C. web server
D. endpoint

Answer: D

Explanation:

The target in a phishing attack is the endpoint, which is the device or system that the user interacts with, such as a computer, smartphone, or tablet. Phishing attacks aim to steal or damage sensitive data by deceiving people into revealing personal information like passwords and credit card numbers, or clicking on malicious links or attachments that can install malware on the endpoint. Phishing attacks can be delivered through various channels, such as email, phone, or

text message, but they all rely on social engineering techniques to manipulate the user's trust and curiosity. By compromising the endpoint, attackers can gain access to the user's accounts, files, network, or other resources. Therefore, endpoint security is essential to prevent phishing attacks and protect the user's data and identity.

Reference:

What Is a Phishing Attack? Definition and Types - Cisco 8 types of phishing attacks and how to identify them What Is Phishing? | Microsoft Security

Phishing | What Is Phishing?

Question: 590

[Content Security]

Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)

A. TACACS+
B. CHAP
C. NTLMSSP
D. RADIUS
E. Kerberos

Answer: C,E

Explanation:

The Cisco WSA supports mainly two authentication protocols: LDAP and NTLM. LDAP is a standard protocol for accessing directory services, such as Active Directory or OpenLDAP. NTLM is a proprietary protocol for authenticating Windows clients to Windows servers. NTLM has two versions: NTLMv1 and NTLMv2. NTLMSSP (NT LAN Manager Security Support Provider) is a variant of NTLMv2 that provides additional security features, such as message integrity and confidentiality. The Cisco WSA supports both LDAP and NTLMSSP using basic authentication, which requires the user to enter a username and password. The Cisco WSA also supports Kerberos, which is a network authentication

protocol that uses tickets to authenticate users and services. Kerberos is based on symmetric-key cryptography and requires a trusted third party, called the Key Distribution Center (KDC), to issue and validate tickets. Kerberos is more secure and efficient than NTLM, as it does not require the user to enter credentials repeatedly and does not send passwords over the network. The Cisco WSA supports Kerberos only in standard mode, not in cloud connector mode. The Cisco WSA does not support TACACS+ or CHAP as authentication protocols. TACACS+ is a Cisco proprietary protocol for authenticating network devices and users to a central server. CHAP is a challenge-response protocol for authenticating PPP connections. These protocols are not designed for web security appliances and are not compatible with the Cisco WSA. Reference:

User Guide for AsyncOS 11.0 for Cisco Web Security Appliances (Section: Acquire End-User Credentials)

Cisco WSA Authentication

WSA Authentication

www.atmicnetworks.com

Question: 591

[Endpoint Protection and Detection]
What is the purpose of the Cisco Endpoint IoC feature?

A. It is an incident response tool.
B. It provides stealth threat prevention.
C. It is a signature-based engine.
D. It provides precompromise detection.

Answer: A

Explanation:

The Cisco Endpoint IoC feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers. Endpoint IoCs are imported through the console from OpenIOC-based files written to trigger on file properties such as name, size, hash, and other attributes and system properties such as process information, running services, and Windows Registry entries. The IoC syntax can be used by incident responders to find specific artifacts or use logic to create sophisticated, correlated detections for families of malware. Endpoint IoCs have the advantage of being portable to share within your organization or in industry vertical forums and mailing lists. The Endpoint IoC scanner is available in AMP for Endpoints Windows Connector versions 4 and higher. Running Endpoint IoC scans may require up to 1 GB of free drive space. The Endpoint IoC feature is based on the openioc.com framework, which is an open standard for sharing threat intelligence. Reference:

Cisco Endpoint IOC Attributes, User Guide

What Are Indicators of Compromise (IOC)? - Cisco, Security Indicators of Compromise General questions about AMP - Cisco Community, Post by Cisco Employee

Reference: https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf

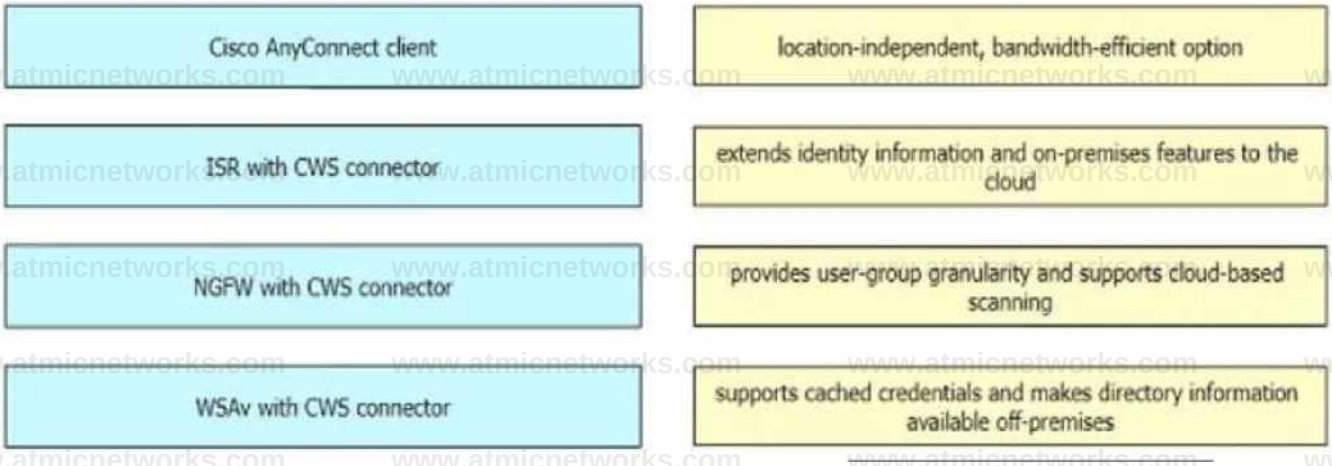
The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

Question: 592

DRAG DROP

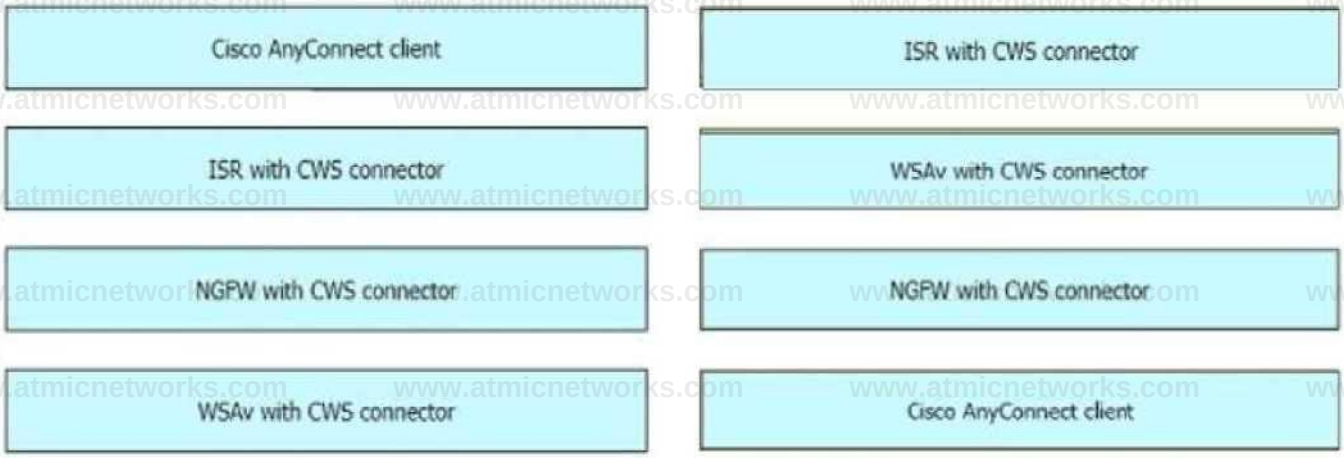
[Security Concepts]

Drag and drop the Cisco CWS redirection options from the left onto the capabilities on the right.



Answer:

Explanation:



Reference: https://www.westconcomstor.com/medias/CWS-data-sheet-c78-729637-1-.pdf?context=bWFzdGVyfHJvb3R8Mjg2MDA4fGFwcGxpY2F0aW9uL3BkZnxoY2QvaDhjLzg3OTcwOTc0OTI1MTAucGRmfDc1MzU2MjFhZmNiOTkwOWNjMDI5ZTFmZmRkYzQ3MzZiZGIyMjE1YzgwZWU1NTFhMTM2YjVhM2UxMjJlNGU5OGQ

Question: 593

[Security Concepts]

An organization is using DNS services for their network and want to help improve the security of the DNS infrastructure. Which action accomplishes this task?

A. Use DNSSEC between the endpoints and Cisco Umbrella DNS servers.

B. Modify the Cisco Umbrella configuration to pass queries only to non-DNSSEC capable zones.

C. Integrate Cisco Umbrella with Cisco CloudLock to ensure that DNSSEC is functional.
D. Configure Cisco Umbrella and use DNSSEC for domain authentication to authoritative servers.

Answer: D

Explanation:

DNSSEC (Domain Name System Security Extensions) is a technology that protects DNS from cache poisoning and spoofing attacks by digitally signing DNS data with cryptographic keys. DNSSEC ensures the integrity and authenticity of DNS responses, preventing attackers from redirecting traffic to malicious domains. Cisco Umbrella supports DNSSEC by performing validation on queries sent from Umbrella resolvers to upstream authorities. This means that Umbrella will only accept DNS responses that are signed and verified by the authoritative servers for each domain. To enable DNSSEC validation, the organization needs to configure Cisco Umbrella and use DNSSEC for domain authentication to authoritative servers. This will ensure that Umbrella resolvers will reject any forged or tampered DNS responses and provide secure DNS resolution for the organization's network. Reference :=
Some possible references are:
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 2: Network Security, Lesson 2.5: Implement DNS Security
What is DNSSEC and Why Is It Important? - Cisco Umbrella
DNSSEC General Availability – Cisco Umbrella

Question: 594

[Endpoint Protection and Detection]
Which Cisco security solution provides patch management in the cloud?

A. Cisco Umbrella
B. Cisco ISE
C. Cisco CloudLock
D. Cisco Tetration

Answer: D

Explanation:

Cisco Tetration is a Cisco security solution that provides patch management in the cloud. Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems to correct security and functionality problems in software and firmware1. Cisco

Tetration is a cloud-native platform that delivers comprehensive workload protection for multicloud data centers by enabling a zero-trust model using segmentation2. One of the features of Cisco Tetration is software vulnerability detection and patch management, which allows users to identify software vulnerabilities on workloads, prioritize patching based on risk scores, and automate patch deployment using orchestration tools3. Cisco Tetration leverages the National Vulnerability Database (NVD) and Cisco Talos Intelligence Group to provide up-to-date information on software vulnerabilities and their severity levels3. Cisco Tetration also supports patch management for both Windows and Linux

operating systems, as well as third-party applications such as Apache, Java, MySQL, and Oracle4. Therefore, the correct answer is D. Cisco Tetration. Reference: 1: RFC 9232: Network Telemetry Framework - Internet Engineering Task Force 2: Cisco Tetration - Workload Protection - Cisco 3: Cisco Tetration Software Vulnerability Detection and Patch Management - Cisco 4: Cisco Tetration Platform Data Sheet - Cisco

Question: 595

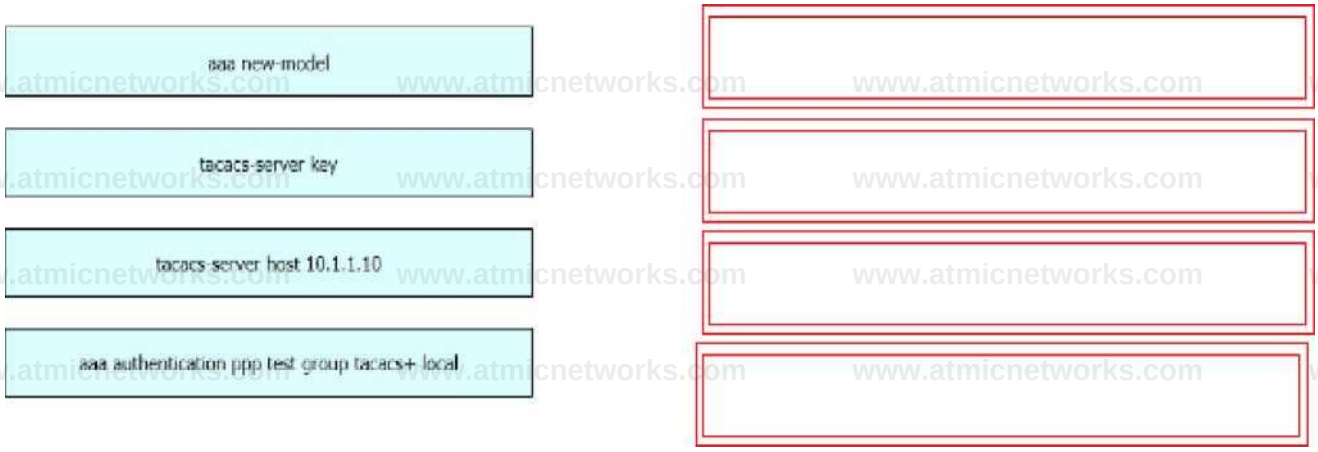
DRAG DROP

[Secure Network Access, Visibility, and Enforcement] Refer to the exhibit.



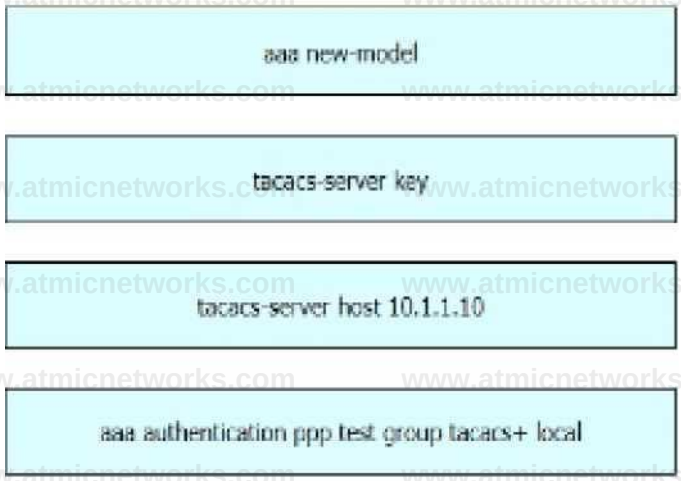
An engineer must configure a Cisco switch to perform PPP authentication via a TACACS server located at IP address 10.1.1.10. Authentication must fall back to the local database using the username LocalUser and password C1Sc0451069341l if the TACACS server is unreachable.

Drag and drop the commands from the left onto the corresponding configuration steps on the right.



Answer:

Explanation:



Question: 596

[Network Security]
Refer to the exhibit,

•Jul 1 15:33:50.027: ISAKMP: (0)Enqueued KEY_MGR_SESSION_CLOSED for TunneK) deletion
•Jul 1 15:33:50.027: ISAKMP: (0):Deleting peer node by peer reap for 2.2.2.2: D1250B0
•Jul 1 15:33:50.029: ISAKMP: (1001):peer does not do paranoid keepalives.
•Jul 1 15:33:54.781: ISAKMP-PAK: (0):received packet from 2.2.2.2 dport 500 sport 500 Global (N) NEW SA
•Jul 1 15:33:54.781: ISAKMP: (0):Created a peer struct for 2.2 2.2, peer port 500
•Jul 1 15:33:54.781: ISAKMP: (0):New peer created peer = 0x11026528 peer_handle = 0x80000004
•Jul 1 15:33:54.781: ISAKMP: (O):Locking peer struct 0x11026528, refcount 1 for crypto_isakmp_process_block
•Jul 1 15:33:54.782: ISAKMP: (0)local port 500, remote port 500
•Jul 1 15:33:54.782: ISAKMP: (0):Find a dup sa in the avl tree during calling isadb_insert sa = 104E3C68
•Jul 1 15:33:54.782: ISAKMP: (0):Input = IKE_MESG FROM.PEER, IKE_MM EXCH
•Jul 1 15:33:54.782: ISAKMP: (0):Old State = IKE_READY New State = IKE_R_MM1

which command results in these messages when attempting to troubleshoot an iPsec VPN connection?

A. debug crypto isakmp
B. debug crypto ipsec endpoint
C. debug crypto Ipsec
D. debug crypto isakmp connection

Answer: A

Explanation:

The command that results in these messages when attempting to troubleshoot an iPsec VPN connection is debug crypto isakmp. This command displays debug information about the Internet Key Exchange (IKE) protocol, which is used to establish security associations (SAs) for IPsec VPNs. The messages in the exhibit show various steps and statuses of the IKE negotiation process, such as creating and deleting peer structures, receiving and sending packets, and checking the compatibility of the security policies and proposals. The other commands are either invalid (debug crypto ipsec endpoint and debug crypto isakmp connection) or display different information (debug crypto ipsec shows the details of the IPsec encryption and decryption operations). Reference: https://www.cisco.com/c/en/us/training-events/training-certifications/training/training- services/courses/implementing-and-operating-cisco-security-core-technologies-scor.htmlhttps://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409- ipsec-

www.atmicnetworks.com

debug-00.html

Question: 597

[Security Concepts]
Which Cisco Umbrella package supports selective proxy for Inspection of traffic from risky domains?

A. SIG Advantage
B. DNS Security Essentials
C. SIG Essentials
D. DNS Security Advantage

Answer: A

Explanation:

The Cisco Umbrella package that supports selective proxy for inspection of traffic from risky domains is SIG Advantage. SIG stands for Secure Internet Gateway, and it is a cloud-based service that provides comprehensive web security and threat intelligence. SIG Advantage includes all the features of DNS Security Advantage, such as DNS-layer protection, intelligent proxy, and cloud-delivered firewall, plus additional features such as full proxy, SSL decryption, advanced malware protection, and data loss prevention. Selective proxy is a feature that allows Umbrella to route risky domain requests to a proxy for deeper URL and file inspection, without impacting the performance or latency of legitimate traffic. Selective proxy is based on the reputation of the domains, which are classified into three categories: good, bad, and grey. Good domains are allowed without proxying, bad domains are blocked at the DNS layer, and grey domains are proxied for further inspection. Selective proxy is available in both DNS Security Advantage and SIG Advantage packages, but only SIG Advantage offers full proxy for all web traffic, which provides more granular control and visibility over web transactions and file types. Reference:

Cisco Umbrella Packages
Why Umbrella DNS Security?
Manage the Intelligent Proxy
Cisco Umbrella - Selected Proxy versus Full Proxy

Question: 598

[Security Concepts]
A security engineer must add destinations into a destination list in Cisco Umbrell
a. What describes the application of these changes?
A. The changes are applied immediately it the destination list is part or a policy.
B. The destination list must be removed from the policy before changes are made to It.
C. The changes are applied only after the configuration is saved in Cisco Umbrella.
D. The user role of Block Page Bypass or higher is needed to perform these changes.

www.atmicnetworks.com

Answer: A

Explanation:

A destination list is a list of internet destinations: domains, URLs, and CIDRs. To control identity access to specific destinations, you can add destination lists to Umbrella and then select them when configuring your Web and DNS policies12. When you add or edit a destination list, the changes are applied immediately if the destination list is part of a policy3. This means that any identities that are associated with the policy will be affected by the changes in the destination list. You do not need to save the configuration or remove the destination list from the policy to apply the changes. However, you do need to have the appropriate user role to manage destination lists. The user role of Block Page Bypass or higher is needed to perform these changes4. Reference := Manage Destination Lists - Umbrella User Guide Manage Destination Lists - Umbrella SIG User Guide
Add a Destination List - Umbrella User Guide
Add a DNS Destination List - Umbrella SIG User Guide

Question: 599

[Secure Network Access, Visibility, and Enforcement]

Which solution is more secure than the traditional use of a username and password and encompasses at least two of the methods of authentication?

A. single-sign on
B. RADIUS/LDAP authentication
C. Kerberos security solution
D. multifactor authentication

Answer: D

Explanation:

Multifactor authentication (MFA) is a solution that requires the user to provide two or more verification factors to gain access to a resource, such as an application, online account, or a VPN. MFA is more secure than the traditional use of a username and password because it reduces the risk of identity theft, phishing, and credential compromise. MFA can use different types of factors, such as something the user knows (e.g., password, PIN), something the user has (e.g., smartphone, token, smart card), or something the user is (e.g., fingerprint, facial recognition). MFA can be implemented using various methods, such as security defaults, Conditional Access policies, or third-party solutions123. Reference:

https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c- be60-d123-eda06bddf661
https://www.onelogin.com/learn/what-is-mfa

Question: 600

[Security Concepts]
Which Cisco network security device supports contextual awareness?

A. Firepower
B. CISCO ASA
C. Cisco IOS
D. ISE

Answer: A

Explanation:

Contextual awareness is the ability to collect and analyze information about the network environment, such as users, devices, applications, threats, and vulnerabilities, and use it to enhance security policies and actions. Cisco Firepower is a network security device that supports contextual awareness by providing real-time visibility into network traffic and activity, security intelligence from Cisco Talos and other sources, and advanced threat protection with Cisco AMP and sandboxing. Cisco Firepower can also leverage Cisco pxGrid to share contextual data with other security solutions, such as SIEM and TD platforms, to enable faster and more accurate threat detection and response123 Reference := 1: Cisco Firepower NGIPS Data Sheet - Cisco 2: Cisco Identity Services Engine with Integrated Security Information and Event Management and Threat Defense Platforms At-a-Glance - Cisco 3: A Visibility-Driven Approach to Next-Generation Firewalls

Question: 601

[Network Security]
Which VPN provides scalability for organizations with many remote sites?

A. DMVPN
B. site-to-site iPsec
C. SSL VPN
D. GRE over IPsec

Answer: A

Explanation:

Dynamic Multipoint VPN (DMVPN) is a Cisco IOS Software-based security solution for building scalable enterprise VPNs that support distributed applications such as voice and video. DMVPN provides scalability for organizations with many remote sites by using a hub-and-spoke topology with dynamic tunnels between spokes. This reduces the number of static tunnels required and simplifies the configuration and management of the VPN. DMVPN also supports dynamic routing protocols, multicast traffic, and quality of service (QoS) features, making it suitable for various network scenarios and

requirements12 Reference := 1: Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications 2: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Question: 602

[Security Concepts]
Based on the NIST 800-145 guide, which cloud architecture is provisioned for exclusive use by a specific group of consumers from different organizations and may be owned, managed, and operated by one or more of those organizations?

A. hybrid cloud
B. private cloud
C. community cloud
D. public cloud

Answer: C

Explanation:

According to the NIST 800-145 guide1, a community cloud is a cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. A community cloud differs from a private cloud, which is provisioned for exclusive use by a single organization, and a public cloud, which is provisioned for open use by the general public. A hybrid cloud is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). Reference := 1: NIST SP 800-145,

The NIST Definition of Cloud Computing, page 3.

Question: 603

[Secure Network Access, Visibility, and Enforcement]
When MAB is configured for use within the 802.1X environment, an administrator must create a policy that allows the devices onto the network. Which information is used for the username and password?

A. The MAB uses the IP address as username and password.
B. The MAB uses the call-station-ID as username and password.
C. Each device must be set manually by the administrator.
D. The MAB uses the MAC address as username and password.

www.atmicnetworks.com

Answer: D

Explanation:

MAB is a fallback authentication method for devices that do not support 802.1X. When MAB is enabled on a switchport, the switch will first try 802.1X and if it fails, it will use the MAC address of the device as the username and password to authenticate it with a RADIUS server. The RADIUS server must have a database of MAC addresses that are allowed on the network. MAB can also support dynamic VLAN assignment and ACLs from the RADIUS server. MAB is not a very secure method because MAC addresses can be easily spoofed or changed. Therefore, MAB should be used with caution and only for devices that cannot use 802.1X. Reference :=
Some possible references are:
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Securing Networks with Cisco Firepower Next Generation Firewall, Lesson 3.2: Deploying Cisco Firepower Next-Generation Firewall, Topic 3.2.2: 802.1X and MAB
MAC Authentication Bypass Deployment Guide, Cisco, MAB Overview, What is MAB?
MAC Authentication Bypass (MAB), NetworkLessons.com, How MAB Works
MAC-based authentication (MAB), RADIUSaaS Docs, How it works
MAC authentication and username/password, Cisco Community, Answer by hslai

Question: 604

[Endpoint Protection and Detection]
An engineer must configure Cisco AMP for Endpoints so that it contains a list of files that should not be executed by users. These files must not be quarantined. Which action meets this configuration requirement?

A. Identity the network IPs and place them in a blocked list.
B. Modify the advanced custom detection list to include these files.
C. Create an application control blocked applications list.
D. Add a list for simple custom detection.

Answer: C

Explanation:

create an application control blocked applications list. This option allows you to specify a list of files that you want to prevent from running on the endpoints that have the AMP connector installed. The files are identified by their SHA-256 hashes, and you can upload them individually or in a batch. The files are not quarantined, but they are blocked from execution and reported as events in the AMP console1. This option is different from the simple custom detection list, which is used to detect and quarantine specific files that are considered malicious2. The advanced custom detection list is also used to detect and quarantine files, but it allows you to specify more criteria such as file size, file name, and file path3. The IP block and allow lists are used to control the network traffic to and from the endpoints, not the file execution4. Reference: 1: Configure Application Control on the AMP for Endpoints Portal 2: Configure a Simple Custom Detection List on the AMP for Endpoints Portal 3: [Configure an Advanced Custom Detection List on the AMP for Endpoints Portal] 4:

[Configure IP Block and Allow Lists on the AMP for Endpoints Portal]

Question: 605

[Security Concepts]
Which Cisco security solution gives the most complete view of the relationships and evolution of Internet domains IPs, and flies, and helps to pinpoint attackers' infrastructures and predict future threat?

A. Cisco Secure Network Analytics
B. Cisco Secure Cloud Analytics
C. Cisco Umbrella Investigate
D. Cisco pxGrid

Answer: C

Explanation:

Cisco Umbrella Investigate is a cloud-based service that provides interactive threat intelligence on domains, IPs, and files. It helps security analysts to uncover the attacker's infrastructure and predict future threats by analyzing the relationships and evolution of internet domains, IPs, and files. It also integrates with other Cisco security solutions, such as Cisco Secure Network Analytics, Cisco Secure Cloud Analytics, and Cisco pxGrid, to provide a holistic view of the network and cloud security posture. Cisco Umbrella Investigate is based on the data collected by Cisco Umbrella, which

processes more than 620 billion DNS requests per day from over 190 countries. Cisco Umbrella Investigate uses statistical and machine learning models to automatically score and classify the data, and provides a risk score for each domain, IP, and file, along with the contributing factors and historical context. Cisco Umbrella Investigate also allows security analysts to query the data using a web-based console or an API, and to visualize the results using graphs, tables, and maps. Cisco Umbrella Investigate is the most complete and interactive threat intelligence solution that helps to prevent cyber attacks before they happen. Reference := Some possible references are:
Cisco Umbrella Investigate
Cyber Attack Prevention - Cisco Umbrella
Cisco Umbrella Investigate - Cisco Umbrella

Question: 606

[Network Security]
An engineer must modify an existing remote access VPN using a Cisco AnyConnect Secure Mobility client solution and a Cisco Secure Firewall. Currently, all the traffic generate by the user Is sent to the VPN tunnel and the engineer must now exclude some servers and access them directly instead.
Which element must be modified to achieve this goat?

A. NAT exemption
B. encryption domain
C. routing table

www.atmicnetworks.com

D. group policy

Answer: D

Explanation:

To achieve the goal of excluding some servers from the VPN tunnel and accessing them directly, the engineer must modify the group policy that is applied to the remote access VPN users. The group policy contains the settings for split tunneling, which is a feature that allows the VPN client to route some traffic through the VPN tunnel and some traffic directly to the internet. Split tunneling can be configured based on the destination IP address, the application, or the domain name of the traffic. By modifying the group policy, the engineer can specify which servers or networks should be excluded from the VPN tunnel and accessed directly by the VPN client. This can improve the performance and efficiency of the VPN connection, as well as reduce the load on the VPN gateway and the corporate network. However, split tunneling also introduces some security risks, such as exposing the VPN client to internet threats, bypassing the corporate firewall and security policies, and leaking sensitive data. Therefore, the engineer must carefully evaluate the trade-offs and best practices of using split tunneling for remote access VPNs. Reference := Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Secure Connectivity, Lesson 3.1: Implementing and Troubleshooting Remote Access VPN, Topic 3.1.4: Configure and Verify Remote Access VPN, Subtopic 3.1.4.2: Configure and Verify Split Tunneling VPN Split Tunneling: What It Is & Pros and Cons

Cisco ASA - Enable Split Tunnel for Remote VPN Clients

Question: 607

[Network Security]

A network engineer must create an access control list on a Cisco Adaptive Security Appliance firewall. The access control list must permit HTTP traffic to the internet from the organization's inside network 192.168.1.0/24. Which IOS command must oe used to create the access control list?

A.

```
access-list HTTP-ONLY extended permit tcp 192.168.1.0
255.255.255.0.
```

B.

```
access-list extended permit tcp 192.168.1.0
255.255.255.0 any eq 80.
```

C.

```
access-list HTTP-ONLY extended permit tcp 192.168.1.0
255.255.255.0 any eq 80.
```

D.

```
access-list permit http 192.168.1.0 255.255.255.0 any.
```

A. Option A B. Option B C. Option C D. Option D

Answer: D

Explanation:

To create an access control list (ACL) on a Cisco Adaptive Security Appliance (ASA) firewall, you need to use the access-list command followed by the name of the ACL, the action (permit or deny), the protocol, the source address and mask, and the destination address and mask. For example, to permit HTTP traffic from the inside network 192.168.1.0/24 to any destination on the internet, you can use this command:

access-list inside_access_in permit tcp 192.168.1.0 255.255.255.0 any eq www

This command creates an ACL named inside_access_in that permits TCP traffic from the source

network 192.168.1.0/24 to any destination with the destination port equal to 80 (www).

The eq keyword is used to specify the port number or name. You can also use the range keyword to specify a range of ports.

To apply the ACL to an interface, you need to use the access-group command followed by the name of the ACL and the direction (in or out). For example, to apply the ACL to the inside interface in the inbound direction, you can use this command: access-group inside_access_in in interface inside

This command applies the ACL inside_access_in to the interface named inside in the inbound direction. This means that the ACL will filter the traffic that enters the firewall through the inside interface.

Option D is the only option that matches the syntax of the access-list command for the ASA firewall. Option A is incorrect because it uses the ip keyword instead of the tcp keyword. Option B is incorrect because it uses the any keyword for both the source and destination addresses. Option C is incorrect because it uses the host keyword for the source address, which is not valid for a network address. Reference:

Configure ASA Access Control List for Various Scenarios

Cisco ASA Access Lists Concepts and Configuration

How to Configure Access Control Lists (ACL) on Cisco ASA 5500 Firewalls

www.atmicnetworks.com

Question: 608

[Network Security]
Which problem Is solved by deploying a multicontext firewall?

A. overlapping IP addressing plan
B. more secure policy
C. resilient high availability design
D. faster inspection

Answer: A

Explanation:

A multicontext firewall is a feature that allows a single physical firewall to be divided into multiple virtual firewalls, also known as security contexts. Each context operates as an independent device, with its own security policy, interfaces, and administrators. This feature is useful for service providers, large enterprises, or any network that requires more than one firewall. One of the problems that a multicontext firewall can solve is an overlapping IP addressing plan. This means that different contexts can use the same IP addresses without causing conflicts, as long as they are separated by different interfaces or VLANs. This allows for more efficient use of IP address space and easier management of multiple networks. A multicontext firewall can also support dynamic routing protocols and VPNs within each context, providing more flexibility and functionality12 Reference := 1: What Are Multi-Context Firewalls? - Franklin Fitch 2: Multiple Context Mode - Cisco

Question: 609

[Security Concepts]
An organization wants to reduce their attach surface for cloud applications. They want to understand application communications, detect abnormal application Behavior, and detect vulnerabilities within the applications. Which action accomplishes this task?

A. Configure Cisco Secure Workload to detect anomalies and vulnerabilities.
B. Use Cisco ISE to provide application visibility and restrict access to them.
C. Implement Cisco Umbrella lo control the access each application is granted.
D. Modify the Cisco Duo configuration to restrict access between applications.

Answer: A

Explanation:

Cisco Secure Workload (formerly Tetration) is a solution that provides visibility, segmentation, and security for cloud applications. It can monitor application communications, detect abnormal application behavior, and identify vulnerabilities within the applications. Cisco Secure Workload can also enforce granular policies to control the traffic between applications and prevent unauthorized access. Reference: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 6: Cloud and Content Security, Lesson 6.2: Cisco Cloud Security Solutions, Topic 6.2.2: Cisco Secure Workload

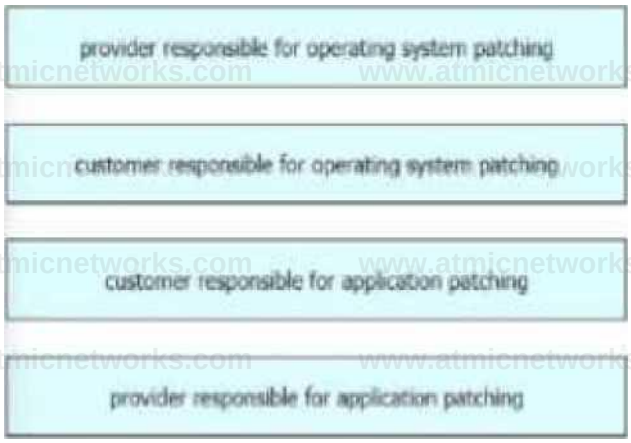
www.atmicnetworks.com

Question: 610

DRAG DROP

[Security Concepts]

Drag and drop the security responsibilities from the left onto the corresponding cloud service models on the right.





Answer:

Explanation:



The cloud security shared responsibility model is a way of describing how the security tasks and obligations are divided between the cloud service provider (CSP) and the customer, depending on the type of cloud service model used.

The cloud service models are:

Software as a Service (SaaS): The CSP provides and manages the entire software stack, including the applications, data, runtime, middleware, operating system, virtualization, servers, storage, and networking. The customer only needs to access the software through a web browser or an application. The customer is responsible for managing their own data and identities, as well as configuring the security settings of the software. The CSP is responsible for everything else, including patching the operating system and the applications12

Platform as a Service (PaaS): The CSP provides and manages the platform layer, including the runtime, middleware, operating system, virtualization, servers, storage, and networking. The customer can deploy and run their own applications and data on the platform, using the tools and languages supported by the CSP. The customer is responsible for managing their own applications and data, as well as configuring the security settings of the platform. The CSP is responsible for patching the operating system and

the middleware12

Infrastructure as a Service (IaaS): The CSP provides and manages the infrastructure layer, including the virtualization, servers, storage, and networking. The customer can provision and use virtual machines, containers, or bare metal servers, and install their own operating system, middleware, applications, and dat

a. The customer is responsible for managing and patching their own operating system, middleware, applications, and data, as well as configuring the security settings of the infrastructure. The CSP is responsible for the physical security and availability of the infrastructure12

Reference := 1: Shared responsibility in the cloud - Microsoft Azure 2: Cloud security shared responsibility model - NCSC

Question: 611

[Endpoint Protection and Detection]

What is a functional difference between Cisco Secure Endpoint and Cisco Umbrella Roaming Client?

A. Secure Endpoint authenticates users and provides segmentation, and the Umbrella Roaming Client allows only for VPN connectivity.

B. Secure Endpoint stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats.

C. The Umbrella Roaming Client authenticates users and provides segmentation, and Secure Endpoint allows only for VPN connectivity.

D. The Umbrella Roaming client stops and tracks malicious activity on hosts, and Secure Endpoint tracks only URL-based threats.

Answer: B

Explanation:

The functional difference between Cisco Secure Endpoint (formerly known as AMP for Endpoints) and Cisco Umbrella Roaming Client lies in their approach to security. Cisco Secure Endpoint is designed to prevent, detect, and respond to threats on the endpoint devices. It provides comprehensive protection by stopping and tracking malicious files and activities on hosts, utilizing continuous analysis and retrospective security to address threats at various stages of the attack continuum. On the other hand, Cisco Umbrella Roaming Client is focused on DNS and IP layer enforcement to prevent internet-based threats before a connection is established. It primarily tracks and blocks URL-based threats by enforcing security at the DNS layer, thus preventing access to malicious domains. Therefore, while Secure Endpoint provides broad endpoint protection against a variety of threats, the Umbrella Roaming Client specifically targets URL-based threats.

Question: 612

[Security Concepts]

What is the purpose of a denial-of-service attack?

A. to disrupt the normal operation of a targeted system by overwhelming It
B. to exploit a security vulnerability on a computer system to steal sensitive information
C. to prevent or limit access to data on a computer system by encrypting It

D. to spread throughout a computer system by self-replicating to additional hosts

Answer: A

Explanation:

The purpose of a Denial-of-Service (DoS) attack is to disrupt the normal operation of a targeted system, server, or network by overwhelming it with a flood of internet traffic. This is achieved by utilizing multiple compromised computer systems as sources of attack traffic. The overwhelming amount of traffic can cause the targeted system to slow down significantly or even crash and become unavailable to legitimate users, thereby denying service to intended users.

Question: 613

[Network Security]
A network administrator is setting up Cisco FMC to send logs to Cisco Security Analytics and Logging (SaaS). The network administrator is anticipating a high volume of logging events from the firewalls and wants lo limit the strain on firewall resources. Which method must the administrator use to send these logs to Cisco Security Analytics and Logging?

A. SFTP using the FMCCLI
B. syslog using the Secure Event Connector
C. direct connection using SNMP traps
D. HTTP POST using the Security Analytics FMC plugin

Answer: B

Explanation:

The Secure Event Connector is a component of the Security Analytics and Logging (SaaS) solution that enables the FMC to send logs to the cloud-based service. The Secure Event Connector uses syslog to forward events from the FMC and the managed devices to the cloud. This method reduces the load on the firewall resources, as the events are sent in batches and compressed before transmission. The Secure Event Connector also provides encryption, authentication, and reliability for the log data. The other methods are not supported by the Security Analytics and Logging (SaaS) solution12
Reference := 1: Cisco Security Analytics and Logging (On Premises)

Question: 614

[Security Concepts]
What is the purpose of the Trusted Automated exchange cyber threat intelligence industry standard?

A. public collection of threat intelligence feeds
B. threat intelligence sharing organization
C. language used to represent security information
D. service used to exchange security information

Answer: D

Explanation:

Trusted Automated eXchange of Intelligence Information (TAXII) is a collection of services and message exchanges that enable the sharing of cyber threat intelligence across product, service, and organizational boundaries. It is designed to support the exchange of CTI represented in STIX, but is not limited to STIX. TAXII defines an API that aligns with common sharing models, such as hub-and- spoke, peer-to-peer, and subscribe/publish. TAXII is not a public collection of threat intelligence feeds, a threat intelligence sharing organization, or a language used to represent security information. Those are possible descriptions of STIX, which is a complementary standard to TAXII. Reference: STIX and TAXII Approved as OASIS Standards to Enable Automated Exchange of Cyber Threat Intelligence, STIX V2.1 and TAXII V2.1 OASIS Standards are published, What is STIX/TAXII? | Cloudflare, What is STIX / TAXII? Learn about the industry standards for Cyber …, What are STIX/TAXII Standards I Resources I Anomali

Question: 615

[Secure Network Access, Visibility, and Enforcement]

Which action configures the IEEE 802.1X Flexible Authentication feature lo support Layer 3 authentication mechanisms?

A. Identity the devices using this feature and create a policy that allows them to pass Layer 2 authentication.
B. Configure WebAuth so the hosts are redirected to a web page for authentication.
C. Modify the Dot1x configuration on the VPN server lo send Layer 3 authentications to an external authentication database
D. Add MAB into the switch to allow redirection to a Layer 3 device for authentication.

Answer: D

Explanation:

Configuring the IEEE 802.1X Flexible Authentication feature to support Layer 3 authentication mechanisms involves adding MAC Authentication Bypass (MAB) into the switch configuration. This

allows devices that do not support 802.1X to be authenticated using their MAC address. Once MAB identifies the device, it can then be redirected to a Layer 3 device for further authentication, thus providing a mechanism to support devices requiring Layer 3 authentication methods.

Question: 616

[Security Concepts]

Which Cisco solution provides a comprehensive view of Internet domains. IP addresses, and autonomous systems to help pinpoint attackers and malicious infrastructures?

A. Cisco Threat Indication Database
B. Cisco Advanced Malware Investigate

C. Cisco Umbrella Investigate
D. Cisco Secure Workload Cloud

Answer: C

Explanation:

Cisco Umbrella Investigate provides a comprehensive view of Internet domains, IP addresses, and autonomous systems, offering a wealth of information about the infrastructure of the internet. It helps security analysts and threat investigators to pinpoint current and emerging threats by providing access to data from Cisco's global network, thereby enabling the identification of attackers and malicious infrastructures.

Question: 617

[Security Concepts]
A security test performed on one of the applications shows that user input is not validated. Which security vulnerability is the application more susceptible to because of this lack of validation?

A. denial -of-service
B. cross-site request forgery
C. man-in-the-middle
D. SQL injection

Answer: D

Explanation:

An application that does not validate user input is particularly susceptible to SQL injection attacks. In an SQL injection attack, an attacker can insert or "inject" a SQL query via the input data from the client to the application. Due to the lack of validation, the malicious SQL commands are executed by
the database server, leading to unauthorized access or manipulation of the database.

Question: 618

[Network Security]
A network administrator is modifying a remote access VPN on an FTD managed by an FMC. The administrator wants to ofload traffic to certain trusted domains. The administrator wants this traffic to go out of the client's local internet and send other internet-bound traffic over the VPN Which feature must the administrator configure?

A. dynamic split tunneling
B. local LAN access
C. dynamic access policies
D. reverse route injection

Answer: A

Explanation:

In a remote access VPN configuration, dynamic split tunneling allows traffic to certain trusted domains to bypass the VPN tunnel and exit through the client's local internet gateway. This feature selectively directs only the necessary traffic over the VPN, while allowing direct internet access for specific domains or traffic deemed safe or trusted, optimizing bandwidth and performance for remote users.

Question: 619

[Security Concepts]
What is a benefit of a Cisco Secure Email Gateway Virtual as compared to a physical Secure Email Gateway?

A. simplifies the distribution of software updates
B. provides faster performance
C. provides an automated setup process
D. enables the allocation of additional resources

Answer: D

Explanation:

One of the benefits of a Cisco Secure Email Gateway Virtual appliance compared to a physical one is the ability to allocate additional resources as needed. Virtual appliances can be easily scaled up by allocating more CPU, memory, or storage resources, providing flexibility and scalability in response to
changing demands or growth.

Question: 620

[Security Concepts]
Which method must be used to connect Cisco Secure Workload to external orchestrators at a client site when the client does not allow incoming connections?

A. source NAT
B. reverse tunnel
C. GRE tunnel
D. destination NAT

Answer: B

Explanation:

To connect Cisco Secure Workload to external orchestrators at a client site where incoming connections are not allowed, a reverse tunnel must be used. A reverse tunnel initiates the connection from the inside of the client's network out to the external orchestrator, thereby bypassing restrictions on incoming connections and enabling secure communication.

Question: 621

[Network Security]
Which technology must De used to Implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

A. GET VPN
B. IPsec DVTI
C. DMVPN
D. FlexVPN

Answer: A

Explanation:

Group Encrypted Transport VPN (GET VPN) is used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity. GET VPN provides a way to encrypt traffic between sites without the need for point-to-point tunnels, supporting efficient, scalable, and secure communication across a broad network infrastructure.

Question: 622

[Security Concepts]
Which two devices support WCCP for traffic redirection? (Choose two.)

A. Cisco Secure Web Appliance
B. Cisco IOS
C. proxy server
D. Cisco ASA
E. Cisco IPS

Answer: B,D

Explanation:

Web Cache Communication Protocol (WCCP) is supported on Cisco IOS routers and Cisco ASA firewalls. WCCP allows these devices to redirect traffic to a WCCP-capable device, such as a web cache or a Cisco Secure Web Appliance, for processing. This redirection can be used for tasks like content filtering, web caching, and load balancing.

Question: 623

[Security Concepts]
Which two types of connectors are used to generate telemetry data from IPFIX records in a Cisco Secure Workload implementation? (Choose two.)

A. ADC
B. ERSPAN
C. Cisco ASA
D. NetFlow
E. Cisco Secure Workload

Answer: D,E

Explanation:

In a Cisco Secure Workload implementation, telemetry data can be generated from IPFIX (Internet Protocol Flow Information Export) records using NetFlow connectors and Cisco Secure Workload itself. NetFlow provides insights into network traffic flow and volume, while Cisco Secure Workload uses this data for visibility, segmentation, and security analytics within the data center.

Question: 624

[Network Security]
What is a difference between GRE over IPsec and IPsec with crypto map?

A. Multicast traffic is supported by IPsec with crypto map.
B. GRE over IPsec supports non-IP protocols.
C. GRE provides its own encryption mechanism.
D. IPsec with crypto map oilers better scalability.

Answer: B

Explanation:

The difference between GRE over IPsec and IPsec with crypto map is that GRE (Generic Routing Encapsulation) over IPsec can encapsulate and transport non-IP protocols across an IP network, whereas IPsec with crypto map is typically used for IP traffic. GRE tunnels wrapped in IPsec provide a way to transport multicast traffic and other protocol types across an IPsec VPN, offering greater flexibility in the types of traffic that can be secured.

Question: 625

[Secure Network Access, Visibility, and Enforcement]
A network administrator has configured TACACS on a network device using the key Cisc0467380030 tor authentication

purposes. However, users are unable to authenticate. TACACS server is reachable, but authentication is tailing. Which configuration step must the administrator complete?

A. Implement synchronized system clock on TACACS server that matches the network device.
B. Install a compatible operating system version on the TACACS server.
C. Configure the TACACS key on the server to match with the network device.
D. Apply an access control list on TACACS server to allow communication with the network device.

Answer: C

Explanation:

For TACACS authentication to work, the key configured on the network device must match the key configured on the TACACS server. If users are unable to authenticate despite the TACACS server being reachable, it is likely due to a mismatch in the keys. Ensuring that both the network device and the TACACS server have the same key configured is crucial for successful authentication.

Question: 626

[Endpoint Protection and Detection]
What must be configured on Cisco Secure Endpoint to create a custom detection tile list to detect

and quarantine future files?

A. Use the simple custom detection feature and add each detection to the list.
B. Add a network IP block allowed list to the configuration and add the blocked files.
C. Create an advanced custom detection and upload the hash of each file
D. Configure an application control allowed applications list to block the files

Answer: C

Explanation:

In Cisco Secure Endpoint, to create a custom detection file list for detecting and quarantining future files, an advanced custom detection should be created, and the hash of each file to be detected and quarantined should be uploaded. This allows the system to uniquely identify and take action on files based on their hash values, providing a precise method for targeting specific malicious or unwanted files.

Question: 627

[Security Concepts]
What is the default action before identifying the URL during HTTPS inspection in Cisco Secure Firewall Threat Defense software?

A. reset
B. buffer
C. pass
D. drop

Answer: C

Explanation:

Before identifying the URL during HTTPS inspection in Cisco Secure Firewall Threat Defense software, the default action is to "pass." This means that the traffic is allowed through without inspection until the URL can be identified, at which point appropriate security policies can be applied based on the URL categorization and reputation.

Question: 628

[Security Concepts]

Which term describes when the Cisco Secure Firewall downloads threat intelligence updates from Cisco Tables?

A. analysis
B. sharing
C. authoring
D. consumption

Answer: D

Explanation:

When the Cisco Secure Firewall downloads threat intelligence updates from Cisco Talos, it is engaged in "consumption." This term refers to the process of receiving and utilizing threat intelligence data to enhance security measures. Cisco Talos provides comprehensive threat intelligence that Cisco Secure Firewall consumes to update its threat detection and prevention capabilities.

Question: 629

[Network Security]

What is a difference between a zone-based firewall and a Cisco Adaptive Security Appliance firewall?

A. Zone-based firewalls provide static routing based on interfaces, and Cisco Adaptive Security Appliance firewalls provide dynamic routing.
B. Zone-based firewalls support virtual tunnel interfaces across different locations, and Cisco Adaptive Security Appliance firewalls support DMVPN.
C. Zone-based firewalls have a default allow-all policy between interfaces in the same zone, and Cisco Adaptive

Security Appliance firewalls have a deny-all policy.

D. Zone-based firewalls are used in large deployments with multiple areas, and Cisco Adaptive Security Appliance firewalls are used in small deployments.

Answer: C

Explanation:

Question: 630

[Secure Network Access, Visibility, and Enforcement]

Refer to the exhibit. A network engineer must configure a Cisco router to send traps using SNMPv3. The engineer configures a remote user to receive traps and sets the security level to use authentication without privacy. Which command completes the configuration?

A. snmp-server host 10.12.8.4 informs version 3 noauthno remoteuser config

B. snmp-server host 10.12.8.4 informs version 3 noauthnoPriv remoteuser config

C. snmp-server user TrapUser group2 remote 10.12.8.4 v3 auth md5 password1

D. snmp-server user TrapUser group2 remote 10.12.8.4 v3 auth md5 password1 priv access des56

Answer: C

Explanation:

Question: 631

[Security Concepts]

A network engineer must configure a Cisco Secure Email Gateway to prompt users to enter two forms of information before gaining access. The Secure Email Gateway must also join a cluster machine using preshared keys. What must be configured to meet these requirements?

A. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Secure Email Gateway CLI.

B. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Secure Email Gateway CLI.

C. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Secure Email Gateway GUI.

D. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Secure Email Gateway GUI.

www.atmicnetworks.com

Answer: A

Explanation:

Question: 632

[Endpoint Protection and Detection]
How does Cisco Secure Endpoint provide next-generation protection?

A. It integrates with Cisco FTD devices.
B. It encrypts data on user endpoints to protect against ransomware.
C. It leverages an endpoint protection platform and endpoint detection and response.
D. It utilizes Cisco pxGrid, which allows Secure Endpoint to pull threat feeds from threat intelligence centers.

Answer: C

Explanation:

Question: 633

[Content Security]
Email security has become a high-priority task for a security engineer at a large multi-national organization due to ongoing phishing campaigns. To help control this, the engineer has deployed an Incoming Content Filter with a URL reputation of (-10.00 to -6.00) on the Cisco Secure Email Gateway. Which action will the system perform to disable any links in messages that match the filter?

A. FilterAction
B. ScreenAction
C. Quarantine
D. Defang

Answer: D

Explanation:

www.atmicnetworks.com

Question: 634

[Network Security]
Which Secure Email Gateway implementation method segregates inbound and outbound email?

A. Pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address
B. One listener on one logical IPv4 address on a single logical interface
C. Pair of logical IPv4 listeners and a pair of IPv6 listeners on two physically separate interfaces
D. One listener on a single physical interface

Answer: A

Explanation:

Question: 635

[Network Security]
While using Cisco Secure Firewall's Security Intelligence policies, which two criteria is blocking based upon? (Choose two.)

A. URLs
B. MAC addresses
C. Port numbers
D. IP addresses
E. Protocol IDs

Answer: A,D

Explanation:

Question: 636

[Endpoint Protection and Detection]
An engineer must deploy a Cisco Secure Web Appliance. Antimalware scanning must use the Outbreak Heuristics antimalware category on files identified as malware before performing any other processes. What must be configured on the Secure Web Appliance to meet the requirements?

A. Sophos scanning engine
B. Webroot scanning engine

C. McAfee scanning engine
D. Adaptive Scanning

Answer: D

Explanation:

Question: 637

[Secure Network Access, Visibility, and Enforcement]
Which action configures the IEEE 802.1X Flexible Authentication feature to support Layer 3 authentication mechanisms?

A. Add MAB into the switch to allow redirection to a Layer 3 device for authentication.
B. Identify the devices using this feature and create a policy that allows them to pass Layer 2 authentication.
C. Modify the Dot1x configuration on the VPN server to send Layer 3 authentications to an external authentication database.
D. Configure WebAuth so the hosts are redirected to a web page for authentication.

Answer: A

Explanation:

Question: 638

[Endpoint Protection and Detection]
An engineer is configuring Cisco Secure Endpoint to enhance security by preventing the execution of certain files by users. The engineer needs to ensure that the specific executable file name Cisco_Software_0505446151.exe is blocked from running while never being quarantined. What must the engineer configure to meet the requirement?

A. Create advanced custom detection list.
B. Configure application control blocked applications list.
C. Implement simple custom detection list.
D. Enable scheduled scans to detect and block the executable files.

www.atmicnetworks.com

Answer: B

Explanation:

Question: 639

[Security Concepts]
Which feature is used to restrict communication between interfaces on a Cisco ASA?

A. VLAN subinterfaces
B. Traffic zones
C. Security levels
D. VxLAN interfaces

Answer: C

Explanation:

Question: 640

[Security Concepts]
A security administrator is designing an email protection solution for an onsite email server and must meet these requirements:
Remove malware from email before it reaches corporate premises
Drop emails with risky links automatically
Block access to newly infected sites with real-time URL analysis
Which solution must be used?

A. Cisco Secure Email Cloud
B. Cisco Security for Office 365
C. Cisco Stealthwatch Cloud
D. Cisco Secure Email and Web Manager Cloud

Answer: A

Explanation:

Question: 641

[Endpoint Protection and Detection]

In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

A. When there is a need to have more advanced detection capabilities
B. When there is a need for traditional anti-malware detection
C. When there is no need to have the solution centrally managed
D. When there is no firewall on the network

Answer: A

Explanation:

Question: 642

[Network Security]

```
crypto ikev2 name-mangier MANGIER
    dn organization-unit
```

Refer to the exhibit. An engineer is implementing a certificate-based VPN. What is the result of the existing configuration?

A. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER.
B. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.
C. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully.
D. The OU of the IKEv2 peer certificate is set to MANGLER.

Answer: C

Explanation:

Question: 643

[Endpoint Protection and Detection]

A web hosting company must upgrade its older, unsupported on-premises servers. The company wants a cloud solution in which the cloud provider is responsible for:

Server patching
Application maintenance
Data center security

Disaster recovery

Which type of cloud meets the requirements?

A. Hybrid
B. IaaS
C. SaaS
D. PaaS

Answer: C

Explanation:

Question: 644

[Security Concepts]

For a given policy in Cisco Umbrella, how should a customer block websites based on a custom list?

A. By adding the websites to a blocked type destination list
B. By specifying blocked domains in the policy settings
C. By adding the website IP addresses to the Cisco Umbrella blocklist
D. By specifying the websites in a custom blocked category

Answer: D

Explanation:

Question: 645

[Security Concepts]

What are two benefits of workload security? (Choose two.)

A. Tracked application security
B. Automated patching
C. Reduced attack surface
D. Scalable security policies
E. Workload modeling

Answer: C,D

Explanation:

Question: 646

[Security Concepts]

Which two methods are available in Cisco Secure Web Appliance to process client requests when configured in Transparent mode? (Choose two.)

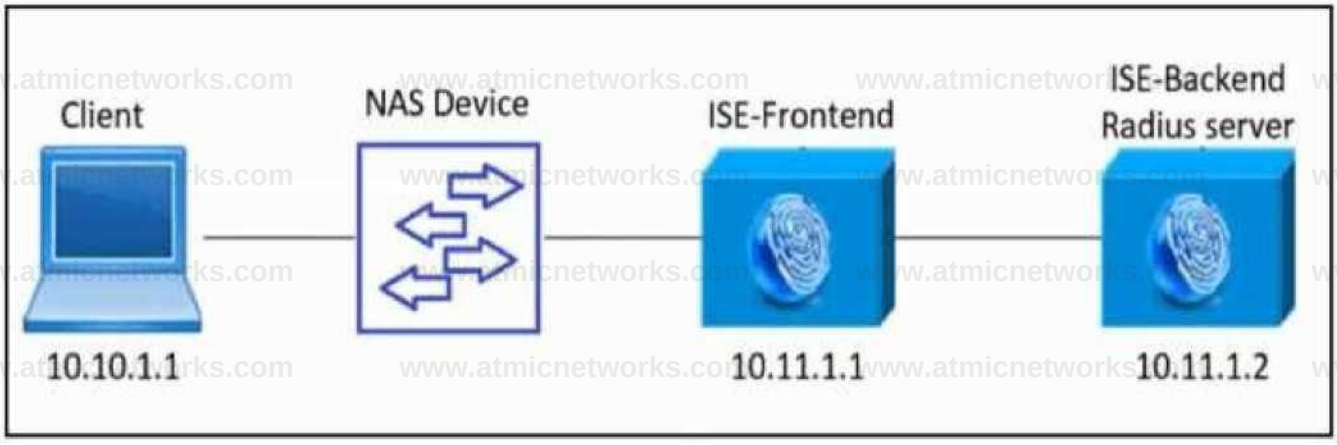
A. WCCP
B. Browser settings
C. WPAD
D. PAC files
E. PBR

Answer: A,E

Explanation:

Question: 647

[Secure Network Access, Visibility, and Enforcement]



Refer to the exhibit. An engineer must configure a new Cisco ISE backend server as a RADIUS server to provide AAA for all access requests from the client to the ISE-Frontend server.

Which Cisco ISE configuration must be used?

A. Set 10.11.1.2 as a network device in ISE-Frontend. Set port 1700/2083 for RADIUS authentication.
B. Set 10.11.1.1 as the external RADIUS server in ISE-Frontend. Set ports 1812/1813 for authentication and accounting.
C. Set 10.11.1.2 as the external RADIUS server in ISE-Frontend. Set ports 1812/1813 for authentication and accounting.
D. Set 10.11.1.1 as a network device in ISE-Frontend. Set ports 1700/2083 for RADIUS authentication.

Answer: C

Explanation:

Question: 648

[Network Security]

Which VPN technology supports a multivendor environment and secure traffic between sites?

A. FlexVPN
B. DMVPN
C. SSL VPN
D. GET VPN

Answer: A

Explanation:

Question: 649

[Network Security]

Which key feature of Cisco ZFW is unique among other Cisco IOS firewall solutions?

A. Security levels
B. Stateless inspection
C. Security zones
D. SSL inspection

Answer: C

Explanation:

Question: 650

[Security Concepts]

www.atmicnetworks.com

4-9-8-2-2-3-8-5-4-6-2-9-2-3-8-8-redacted -7-.0-0-0-0-0-0-O-O-0-0-O-0-0-0-0-49-O-0-0-0-0-

0- 0 -0-0- 0-0- 0 - 0. info

5-2-4-6-3-2-2-7-4-8-3-6-7-l-2-3-redacted-0-.0-0-0-0-0-0-0-0-0-0-0-0-0-0-49-0-0-0-0-0-

O-O-O-O-O-O-O-O.info

6-t-y-s-8-l l-p-6-6-x-q-2'l-2-9-x-7 -redacted—a-.O-O-O-O-O-O'O-O'O-O-O-O-O-45-O-O-O-O-O

O-OO-O-O-O-O-O.info

7-8-5-4-1-2-7-2-7-8-4-5-1-5-0-7-redacted -O-.0-O-0-O-O-O-0-O-0-O-O-O-O-O-28-0-O-O-0-O-

O-O-O-O-O-O-O-O-O.info

Refer to the exhibit. Consider that any feature of DNS requests, such as the length of the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared.
Which type of malicious attack are these values associated with?

A. W32/AutoRun worm
B. HeartBleed SSL Bug
C. Spectre Worm
D. Eternal Blue Windows

Answer: A

Explanation:

Question: 651

[Security Concepts]
How is a cross-site scripting attack executed?

A. Force a currently authenticated end user to execute unwanted actions on a web app
B. Execute malicious client-side scripts injected to a client via a web app
C. Inject a database query via the input data from the client to a web app
D. Intercept communications between a client and a web server

Answer: B

Explanation:

Question: 652

[Security Concepts]
Which two Cisco Umbrella security categories are used to prevent command-and-control callbacks on port 53 and protect users from being tricked into providing confidential information? (Choose two.)

A. DNS Tunneling VPN
B. Dynamic DNS
C. Newly Seen Domains
D. Potentially Harmful Domains
E. Phishing Attacks

Answer: A,E

Explanation:

Question: 653

[Content Security]
An engineer must deploy Cisco Secure Email with Cloud URL Analysis and must meet these requirements:
To protect the network from large-scale virus outbreaks
To protect the network from non-viral attacks such as phishing scams and malware distribution
To provide active analysis of the structure of the URL and information about the domain and page contents
Which two prerequisites must the engineer ensure are configured? (Choose two.)

A. Scanning enabled for each Verdict, Prepend Subject and Deliver.
B. Outbreak Filters must be enabled globally.
C. Enable TLS by setting to Preferred to the Default Domain.
D. Service Logs must be enabled.
E. Enable Rejected Connection Logging.

Answer: A,B

Explanation:

Question: 654

[Security Concepts]
Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application

www.atmicnetworks.com

traffic?

A. Cisco Catalyst Center
B. Cisco Security Intelligence
C. Cisco Model Driven Telemetry
D. Cisco Application Visibility and Control

Answer: D

Explanation:

Question: 655

[Security Concepts]
A Cisco Secure Email Gateway network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Secure Email Gateway is not dropping files that have an undetermined verdict. What is causing this issue?

A. The file has a reputation score that is below the threshold.
B. The file has a reputation score that is above the threshold.
C. The policy was created to disable file analysis.
D. The policy was created to send a message to quarantine instead of drop.

Answer: B

Explanation:

Question: 656

[Endpoint Protection and Detection]
Which Cisco AMP feature allows an engineer to look back to trace past activities, such as file and

process activity on an endpoint?

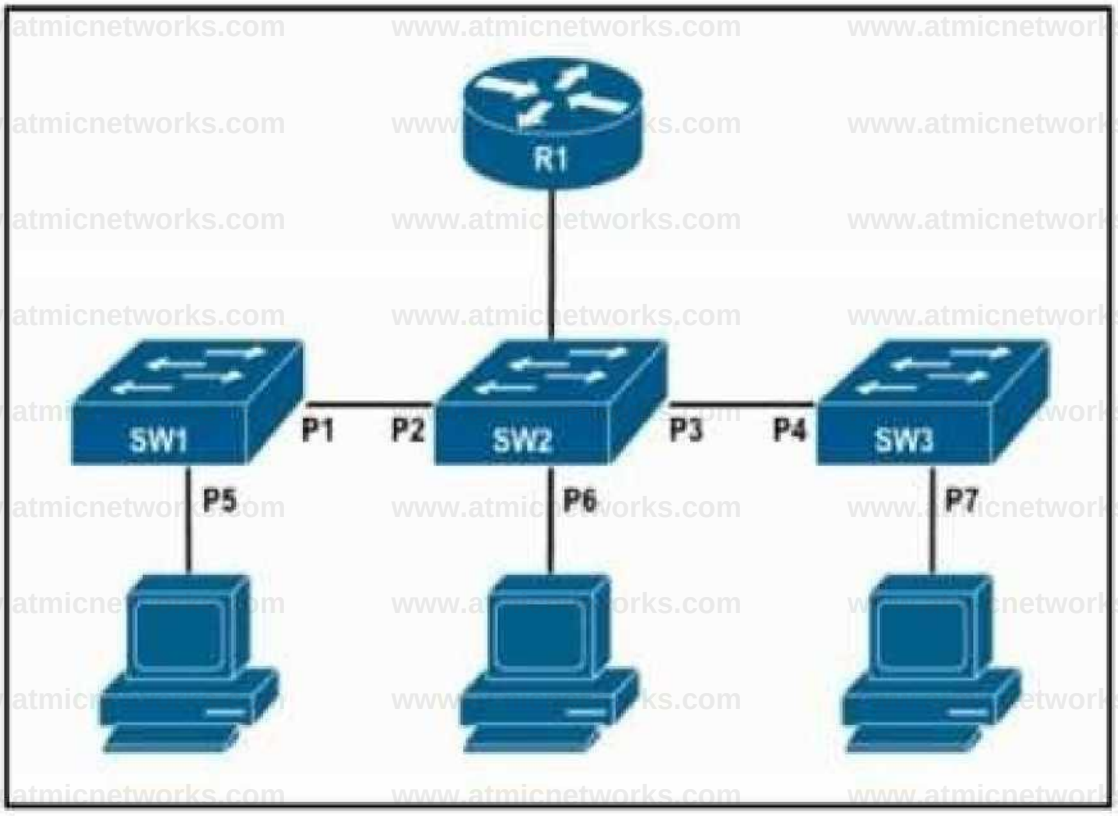
A. Retrospective security
B. Endpoint isolation
C. Advanced investigation
D. Advanced search

Answer: A

Explanation:

Question: 657

[Security Concepts]



Refer to the exhibit. The DHCP snooping database resides on router R1, and dynamic ARP inspection is configured only on switch SW2. Which ports must be configured as untrusted so that dynamic ARP inspection operates normally?

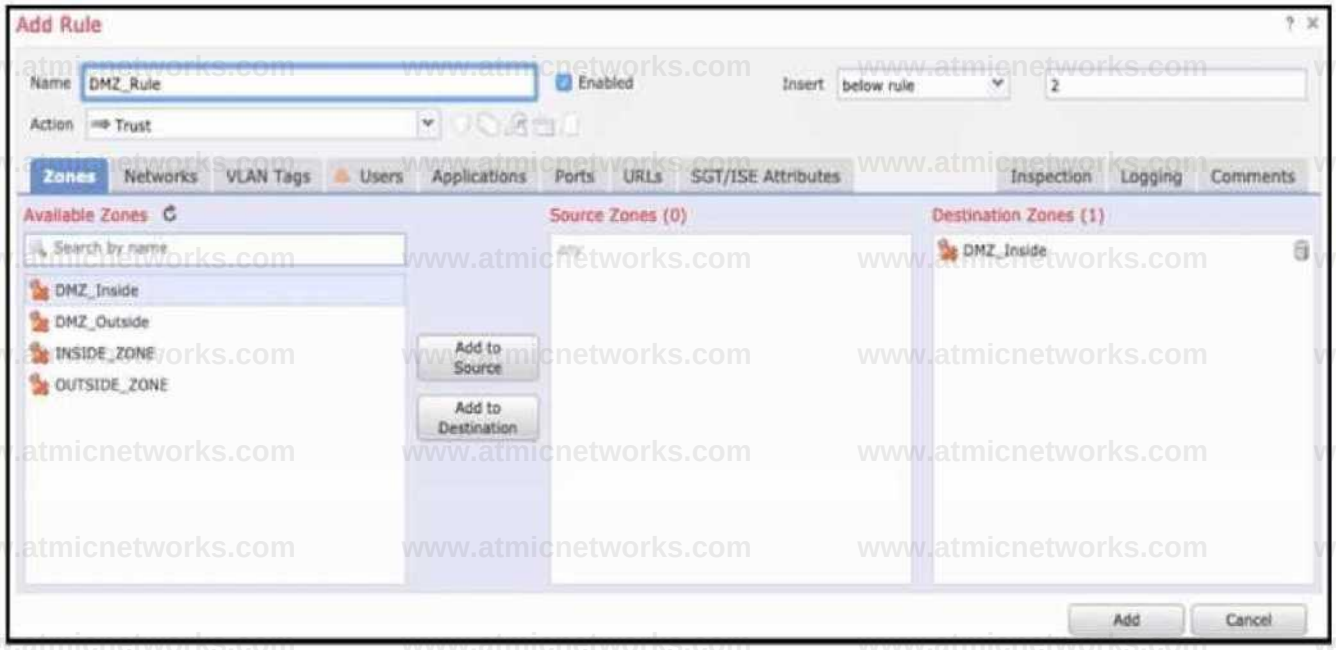
A. P2 and P3 only
B. P2, P3, and P6 only
C. P5, P6, and P7 only
D. P1, P2, P3, and P4 only

Answer: B

Explanation:

Question: 658

[Security Concepts]



Refer to the exhibit. When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZ_inside zone once the configuration is deployed?

A. All traffic from any zone will be allowed to the DMZ_inside zone only after inspection.
B. No traffic will be allowed through to the DMZ_inside zone regardless of if it's trusted or not.
C. No traffic will be allowed through to the DMZ_inside zone unless it's already trusted.
D. All traffic from any zone to the DMZ_inside zone will be permitted with no further inspection.

Answer: D

Explanation:

Question: 659

[Secure Network Access, Visibility, and Enforcement]

An engineer is implementing NAC for LAN users on a segmented network. The engineer confirms that the device of each user is supported and the Cisco switch configuration is correct.

www.atmicnetworks.com

Which configuration should be made next to ensure there are no authentication issues?

A. Disable the host firewall.
B. Enable TACACS+ on the switch.
C. Open TCP port 49.
D. Permit UDP port 1812.

Answer: D

Explanation:

Question: 660

[Endpoint Protection and Detection]

An engineer is configuring guest WLAN access using Cisco ISE and the Cisco WLC. Which action temporarily gives guest endpoints access dynamically while maintaining visibility into who or what is connecting?

A. Modify the WLC configuration to require local WLC logins for the authentication prompts.
B. Configure ISE and the WLC for guest redirection and services using a self-registered portal.
C. Configure ISE and the WLC for guest redirection and services using a hotspot portal.
D. Modify the WLC configuration to allow any endpoint to access an internet-only VLAN.

Answer: B

Explanation:

Question: 661

[Security Concepts]

Which process is used to obtain a certificate from a CA?

A. Registration
B. Enrollment
C. Signing
D. Approval

Answer: B

Explanation:

www.atmicnetworks.com

Question: 662

[Security Concepts]
Which policy does a Cisco Secure Web Appliance use to block or monitor URL requests based on the reputation score?

A. Encryption
B. Enforcement Security
C. Cisco Data Security
D. Outbound Malware Scanning

Answer: B

Explanation:

Question: 663

[Security Concepts]
Which two capabilities of Integration APIs are utilized with Cisco Catalyst Center? (Choose two.)

A. Create new SSIDs on a wireless LAN controller
B. Connect to ITSM platforms
C. Automatically deploy new virtual routers
D. Upgrade software on switches and routers
E. Third party reporting

Answer: B,E

Explanation:

Question: 664

[Security Operations]
An engineer is configuring cloud logging on Cisco ASA and needs events to compress. Which component must be configured to accomplish this goal?

A. CDO event viewer
B. SWC service
C. Cisco analytics
D. SDC VM

Answer: D

Explanation:

Question: 665

[Security Concepts]

What is the recommendation in a zero-trust model before granting access to corporate applications and resources?

A. To use a wired network, not wireless
B. To use strong passwords
C. To use multifactor authentication
D. To disconnect from the network when inactive

Answer: C

Explanation:

Question: 666

[Security Concepts]

Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco Secure Email Gateway?

A. outbreakconfig
B. websecurityconfig
C. webadvancedconfig

D.
websecurityadvancedconfig

Answer: D

Explanation:

Question: 667

[Security Concepts]
What are two characteristics of Cisco Catalyst Center APIs? (Choose two.)

A. Postman is required to utilize Cisco Catalyst Center API calls.
B. They are Cisco proprietary.
C. They do not support Python scripts.
D. They view the overall health of the network.
E. They quickly provision new devices.

Answer: B,E

Explanation:

Question: 668

[Endpoint Protection and Detection]
What is a benefit of an endpoint patch management strategy?

A. Patches are deployed without a testing phase.
B. Fewer staff is needed to manage the endpoints.
C. Endpoints are resistant to vulnerabilities.
D. Ensures adherence to regulatory and compliance standards.

Answer: D

Explanation:

Question: 669

[Security Concepts]

```
SET api/running/interfaces?deep HTT? 1.1
Hest 1 2 222 4 c:  _ L C- c
Authorization: Basic YWRtaW46YgRtaW4=

Accept: app 1 i ca t i on 7 vnd. yang. da t a * j s
or.

Cache-Centrcl: no-cache Eastman-Token: 93bfbd7d-
c25t-993b-2ed2-b4€4e"d?26de
```

Refer to the exhibit. A network engineer must retrieve the interface configuration on a Cisco router by using the NETCONF API. The engineer uses a python script to automate the activity. Which code snippet completes the script?

A. Content-Type: application/vnd.yang.data+json
B. Content-Type: application/vnd.yang.data
C. Content-Type: application/vnd.yang.data+api
D. Content-Type: applications/json/vnd.yang.data

Answer: A

Explanation:

Question: 670

[Security Operations]

Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

A. Cisco CTA
B. Cisco Encrypted Traffic Analytics
C. Cisco Umbrella
D. Cisco Secure Network Analytics

Answer: D

Explanation:

Question: 671

[Security Concepts]

Which attack gives unauthorized access to files on the web server?

A. Distributed DoS
B. Broadcast storm
C. DHCP snooping
D. Path traversal

Answer: D

Explanation:

Question: 672

[Secure Network Access, Visibility, and Enforcement]
A Cisco Secure Cloud Analytics administrator is setting up a private network monitor sensor to monitor an on-premises environment. Which two pieces of information from the sensor are used to link to the Secure Cloud Analytics portal? (Choose two.)

A. Unique service key
B. NAT ID
C. SSL certificate
D. Public IP address
E. Private IP address

Answer: A,B

Explanation:

Question: 673

[Security Concepts]
An engineer must modify a policy to block specific addresses using Cisco Umbrell
a. The policy is created already and is actively used by devices, using many of the default policy elements.
What else must be done to accomplish this task?

A. Modify the application settings to allow only applications to connect to required addresses.
B. Create a destination list for addresses to be allowed or blocked.
C. Add the specified addresses to the identities list and create a block action.
D. Use content categories to block or allow specific addresses.

www.atmicnetworks.com

Answer: B

Explanation:

Question: 674

[Security Concepts]
Which two global commands must the network administrator implement to limit the attack surface of an internet-facing Cisco router? (Choose two.)

A. no service password-recovery
B. no cdp run
C. service tcp-keepalives-in
D. no ip http server
E. ip ssh version 2

Answer: B,D

Explanation:

Question: 675

[Security Concepts]
What is an attribute of Cisco Talos?

A. Introduction of attributes that use objects and narrative relations
B. Fast and intelligent responses based on threat data
C. Cyber threat intelligence interchange and maintenance
D. Cyber threats posing as authorized users and devices

Answer: B

Explanation:

Question: 676

[Security Concepts]
When a Cisco Secure Web Appliance checks a web request, what occurs if it is unable to match a user-defined policy?

A. It applies the next identification profile policy.
B. It applies the advanced policy.
C. It applies the global policy.
D. It blocks the request.

Answer: C

Explanation:

Question: 677

[Security Concepts]
An organization is implementing URL blocking using Cisco Umbrell
a. The users are able to go to some sites but other sites are not accessible due to an error. Why is the error occurring?

A. Client computers do not have the Cisco Umbrella Root CA certificate installed.
B. IP-Layer Enforcement is not configured.
C. Intelligent proxy and SSL decryption is disabled in the policy.
D. Client computers do not have an SSL certificate deployed from an internal CA server.

Answer: A

Explanation:

Question: 678

[Security Concepts]

```
RouterA(config) crypto key generate rsa general-keys label SSH modulus 2048

RouterA(config) ip ssh keypair-name SSH

RouterA(config) ip ssh version2
```

Refer to the exhibit. An engineer must enable secure SSH protocols and enters this configuration. What are two results of running this set of commands on a Cisco router? (Choose two.)

A. Labels the key pair to be used for SSH
B. Uses the FQDN with the label command C. Generates AES key pairs on the router D. Generates RSA key pair on the router E. Enables SSHv1 on the router

www.atmicnetworks.com

Answer: A,D

Explanation:

Question: 679

[Secure Network Access, Visibility, and Enforcement]
An engineer must implement a file transfer solution between a company's data center and branches. The company has numerous servers hosted in a hybrid cloud implementation. The file transfer protocol must support authentication, protect the data against unauthorized access, and ensure that users cannot list directories or remove files remotely. Which protocol must be used?

A. SCP
B. SSH
C. FTPS
D. SFTP

Answer: A

Explanation:

Question: 680

[Security Concepts]

An engineer is deploying a Cisco Secure Email Gateway and must ensure it reaches the Cisco update servers to retrieve new rules. The engineer must now manually configure the Outbreak Filter rules on an AsyncOS for Cisco Secure Email Gateway. Only outdated rules must be replaced. Up-to-date rules must be retained. Which action must the engineer take next to complete the configuration?

A. Select Outbreak Filters
B. Perform a backup/restore of the database
C. Use the outbreakconfig command in CLI
D. Click Update Rules Now

Answer: C

Explanation:

www.atmicnetworks.com

Question: 681

[Security Concepts]
A network engineer is configuring a Cisco Catalyst switch. The network engineer must prevent traffic on the network from being interrupted by broadcast packets flooding the network using a predefined threshold. What must be configured on the switch?

A. DHCP Snooping
B. Embedded Event Monitoring
C. Storm Control
D. Loop Guard

Answer: C

Explanation:

Question: 682

[Security Concepts]
Which service allows a user to export application usage and performance statistics with Cisco Application Visibility and Control?

A. SNMP
B. 802.1X
C. NetFlow
D. SNORT

Answer: C

Explanation:

Question: 683

[Security Concepts]
Which two products are used to forecast capacity needs accurately in real time? (Choose two.)

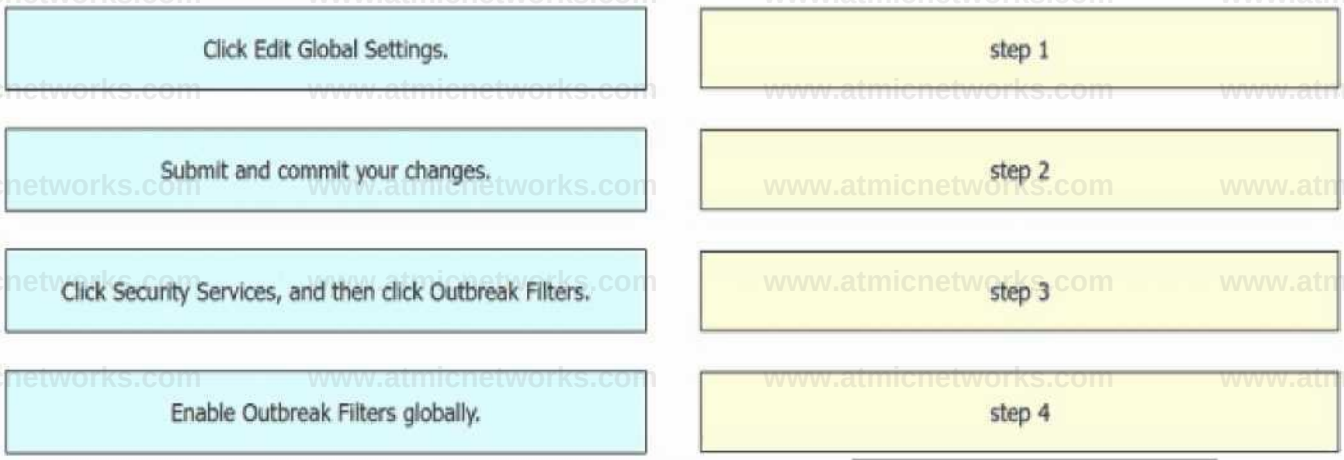
A. Cisco Secure Workload
B. Cisco Umbrella
C. Cisco Workload Optimization Manager
D. Cisco AppDynamics
E. Cisco Cloudlock

Answer: C,D

Explanation:

Question: 684

DRAG DROP
[Endpoint Protection and Detection]
An engineer must enable Outbreak Filters globally on an AsyncOS for Cisco Secure Email Gateway to protect the network from large-scale malware attacks. Drag and drop the steps from the left into the sequence on the right to complete the configuration.



Answer:

Explanation:



Question: 685

[Security Concepts]

A company identified a phishing vulnerability during a pentest. What are two ways the company can protect employees from the attack? (Choose two.)

A. using Cisco Umbrella
B. using Cisco FTD
C. using Cisco ISE
D. using Cisco Secure Email Gateway
E. using an inline IPS/IDS in the network

Answer: B,E

Explanation:

Question: 686

[Security Concepts]
An organization recently installed a Cisco Secure Web Appliance and would like to take advantage of the AVC engine to allow the organization to create a policy to control application-specific activity. After enabling the AVC engine, what must be done to implement this?

A. Use an access policy group to configure application control settings.
B. Use security services to configure the traffic monitor.
C. Use URL categorization to prevent the application traffic.
D. Use web security reporting to validate engine functionality.

Answer: A

Explanation:

Question: 687

[Security Concepts]

www.atmicnetworks.com

```
            Interface:  GigabitEthernet1/0/18
                IIF-ID:  0x14E3317D
           MAC Address:  0001.2e34.f101
          IPv6 Address:  fe80::f86d:7f42:8d7b:58f3
          IPv4 Address:  192.168.41.7
            User-Name:  00-01-2E-34-F1-01
          Device-type:  Microsoft-Workstation
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  C0A82902000004CABED04789
      Acct Session ID:  0x00000039
               Handle:  0xd300004c
       Current Policy:  POLICY_Gi1/0/18

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure

Server Policies:

Method status list:
       Method           State
        dot1x           Stopped
          mab           Authc Success
```

Refer to the exhibit. Which configuration item makes it possible to have the AAA session on the network?

A. aaa authorization exec default ise
B. aaa authentication enable default enable
C. aaa authorization network default group ise
D. aaa authorization login console ise

Answer: C

Explanation:

Question: 688

[Security Concepts]
A networking team must harden an organization's network from VLAN hopping attacks. The team disables Dynamic Trunking Protocol and puts any unused ports in an unused VLAN. A trunk port is used as a trunk link. What must the team configure next to harden the network against VLAN hopping attacks?

A. disable STP on the network devices
B. dedicated VLAN ID for all trunk ports
C. DHCP snooping on all the switches
D. enable port-based network access control

Answer: B

Explanation:

Question: 689

[Security Concepts]
What is a benefit of using Cisco AVC (Application Visibility and Control) for application control?

A. management of application sessions
B. retrospective application analysis
C. zero-trust approach
D. dynamic application scanning

Answer: D

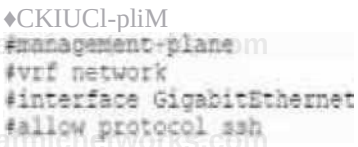
Explanation:

Question: 690

An administrator is implementing management plane protection and must configure an interface on a Cisco router to only terminate management packets that are destined for the router. Which set of IOS commands must be used to complete the implementation?
A.

```
#control-plane
#management-plane
#out-of-band
#vrf network
#interface GigabitEthernet 0/6
#allow protocol ssh
```

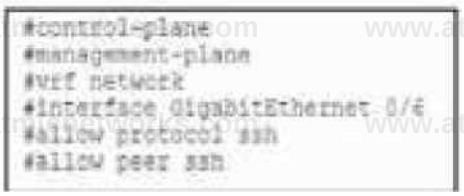
B.



C.



D.



A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

Question: 691

Which Cisco Secure Client module is integrated with Splunk Enterprise to provide monitoring capabilities to administrators to allow them to view endpoint application usage?

A. Umbrella Roaming Security
B. Network Visibility
C. AMP Enabler
D. ISE Posture

Answer: B

Explanation:

Question: 692

Refer to the exhibit.



```
reportlnq_ur I * "http#://report*.epi .umbraI. a.con/v] /organirat Iona.'"

time • dateline.now(».isoforaat ()
dearie cs - (
        'Authorisation': "Basie * - baae64
req • requeue.get (report ing_url ■ hoauers^neaders)
output - req.JaonO
1£ (req,atatus_*ode — 200):
                    or i nt ("5tTT~5~ at ){time)a: thia la the meat recent security activity: I (output) a* I Ctiee': Him.
                    'output': output!)
»U*I
                    prin'("An error has occurred with the following code Horror) please consult
                    the follow.ng link: https://doca.umbralia.caa/ invest Igata-ap:/• I |'error':
                    req.atatua code i
```

Refer to the exhibit. Which task is the Python script performing by using the Cisco Umbrella API?

A. Creating a list of the latest security events B. Copying a list of the latest security activity C. Retrieving a list of the latest security events D. Sending a list of the latest security activity

Answer: C

Explanation:

Question: 693

Which two activities are performed using Cisco Catalyst Center? (Choose two.)

A. DHCP
B. Design
C. Provision
D. DNS
E. Accounting

Answer: B, C

Explanation:

Question: 694

Which firewall mode does a Cisco Adaptive Security Appliance use to inspect Layer 2 traffic?

A. Routed
B. Passive
C. Inline
D. Transparent

Answer: D

Explanation:

Question: 695

Refer to the exhibit.



Refer to the exhibit. Traffic is not passing through IPsec site-to-site VPN on the Secure Firewall Threat Defense appliance. What is causing this issue?

A. No split-tunnel policy is defined on the Secure Firewall Threat Defense appliance.
B. Site-to-site VPN preshared keys are mismatched.
C. The access control policy is not allowing VPN traffic in.
D. Site-to-site VPN peers are using different encryption algorithms.

Answer: C

Explanation:

Question: 696

An engineer implements Cisco CloudLock to secure a Microsoft Office 365 application in the cloud. The engineer must configure protection for corporate files in case of any incidents. Which two actions must be taken to complete the implementation? (Choose two.)

A. Expire the public share URL
B. Send Cisco Webex message to specified users when an incident is triggered
C. Transfer ownership of the files to a specified owner and folder
D. Remove all users as collaborators on the files
E. Disable the ability for commenters and viewers to download and copy the files

Answer: A, D

Explanation:

Question: 697

Which two actions does the Cisco ISE posture module provide that ensures endpoint security? (Choose two.)

A. A centralized management solution is deployed.
B. Patch management remediation is performed.
C. The latest antivirus updates are applied before access is allowed.
D. Assignments to endpoint groups are made dynamically, based on endpoint attributes.
E. Endpoint supplicant configuration is deployed.

Answer: B, C

Explanation:

Question: 698

What are the components of endpoint protection against social engineering attacks?

A. IPsec
B. IDS
C. Firewall
D. Cisco Secure Email Gateway

Answer: D

Explanation:

Question: 699

What is a difference between weak passwords and missing encryption?

A. Weak passwords allow programs to be renamed, and missing encryption hides .exe extensions.
B. Weak passwords cause programs to crash, and missing encryption sends data to a memory location.
C. Weak passwords consume bandwidth, and missing encryption allows user information to be hijacked.
D. Weak passwords are guessed easily, and missing encryption allows information to be decrypted.

Answer: D

Explanation:

Question: 700

A network engineer is deciding whether to use stateful or stateless failover when configuring two Cisco ASAs for high availability. What is the connection status in both cases?

A. Need to be reestablished with both stateful and stateless failover

B. Need to be reestablished with stateful failover and preserved with stateless failover
C. Preserved with both stateful and stateless failover
D. Preserved with stateful failover and need to be reestablished with stateless failover

Answer: D

Explanation:

Question: 701

Which Cisco solution integrates industry-leading artificial intelligence and machine learning analytics and an assurance database to review the security posture and maintain visibility of an organization's cloud environment?

A. Cisco CSR1000v
B. Cisco Secure Workload
C. Cisco DNA
D. Cisco FTD

Answer: B

Explanation:

Question: 702

Which file type is supported when performing a bulk upload of destinations into a destination list on Cisco Umbrella?

A. TXT
B. RTF
C. XLS
D. CSV

Answer: D

Explanation:

Question: 703

Which type of dashboard does Cisco Catalyst Center provide for complete control of the network?

A. Distributed management
B. Centralized management
C. Application management
D. Service management

Answer: B

Explanation:

Question: 704

Which Cisco firewall solution supports configuration via Cisco Policy Language?

A. CBAC
B. ZFW
C. IPS
D. NGFW

Answer: B

Explanation:

Question: 705

What is the difference between deceptive phishing and spear phishing?

A. Deceptive phishing is an attack aimed at a specific user in the organization who holds a C-level role.
B. A spear phishing campaign is aimed at a specific person versus a group of people.
C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Answer: B

Explanation:

Question: 706

Which interface mode does a Cisco Secure IPS device use to block suspicious traffic?

A. Passive
B. Inline
C. Promiscuous
D. Active

Answer: B

Explanation:

Question: 707

What is the difference between EPP and EDR?

A. EDR focuses solely on prevention at the perimeter.
B. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.
C. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.
D. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.

Answer: C

Explanation:

Question: 708

Which two request methods of REST API are valid on the Cisco ASA Platform? (Choose two.)

A. GET
B. CONNECT
C. PUSH
D. OPTIONS
E. PUT

Answer: A, E

Explanation:

Question: 709

What is an advantage of using a next-generation firewall compared to a traditional firewall?

A. Next-generation firewalls have stateless inspection capabilities, and traditional firewalls use stateful inspection.
B. Next-generation firewalls use dynamic packet filtering, and traditional firewalls use static packet filtering.
C. Next-generation firewalls have threat intelligence feeds, and traditional firewalls use signature detection.
D. Next-generation firewalls use intrusion prevention policies, and traditional firewalls use intrusion detection policies.

Answer: C

Explanation:

Question: 710

Where are individual sites specified to be block listed in Cisco Umbrella?

A. Application settings
B. Security settings
C. Destination lists
D. Content categories

Answer: C

Explanation:

Question: 711

In which two customer environments is the Cisco Secure Web Appliance Virtual connector traffic direction method selected? (Choose two.)

A. Customer needs to support roaming users.
B. Customer does not own Cisco hardware and needs Transparent Redirection (WCCP).
C. Customer owns ASA Appliance and Virtual Form Factor is required.
D. Customer does not own Cisco hardware and needs Explicit Proxy.
E. Customer owns ASA Appliance and SSL Tunneling is required.

Answer: B, D

Explanation:

Question: 712

An organization plans to upgrade its current email security solutions, and an engineer must deploy Cisco Secure Email. The requirements for the upgrade are:
Implement Data Loss Prevention
Implement mail encryption
Integrate with an existing Cisco IronPort Secure Email Gateway solution
Which Cisco Secure Email license is needed to accomplish this task?

A. Cisco Secure Email Outbound Essentials
B. Cisco Secure Email Phishing Defense
C. Cisco Secure Email Domain Protection
D. Cisco Secure Email Inbound Essentials

Answer: A

Explanation:

Question: 713

A company deploys an application that contains confidential data and has a hybrid hub-and-spoke topology. The hub resides in a public cloud environment, and the spoke resides on-premises. An engineer must secure the application to ensure that confidential data in transit between the hub- and-spoke servers is accessible only to authorized users. The engineer performs these configurations: Segregation of duties Role-based access control
Privileged access management
What must be implemented to protect the data in transit?

A. MD5
B. AES-256
C. SHA-512
D. TLS 1.3

Answer: D

Explanation:

Question: 714

Refer to the exhibit.



Refer to the exhibit. An engineer must configure an incoming mail policy so that each email sent from usera1@example.com to a domain of @cisco.com is scanned for antispam and advanced malware protection. All other settings will use the default behavior. What must be configured in the incoming mail policy to meet the requirements?

A. Policy Name: Default Policy Sender: usera1@example.com Recipient: @cisco.com
B. Policy Name: usera1 policy Sender: usera1@example.com Recipient: @cisco.com
C. Policy Name: Anti-Malware policy Sender: usera1@example.com Recipient: @cisco.com
D. Policy Name: cisco.com policy Sender: usera1@example.com Recipient: @cisco.com

www.atmicnetworks.com

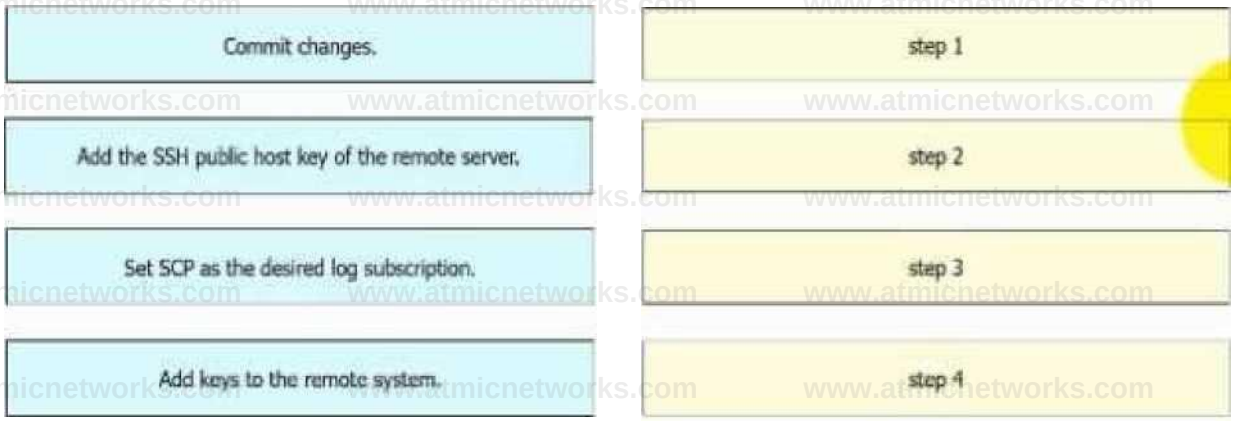
Answer: B

Explanation:

Question: 715

DRAG DROP

An engineer must configure AsyncOS for Cisco Secure Web Appliance to push log files to a syslog server using the SCP retrieval method. Drag and drop the steps from the left into the sequence on the right to complete the configuration.



Answer:

Set SCP as the deseed og subscription.

Add the S5H puttie host key of the remote server

Commit changes

Add keys to the remote system.

Question: 716

A network administrator needs a solution to match traffic and allow or deny the traffic based on the type of application, not just the source or destination address and port used. Which kind of security product must the network administrator implement to meet this requirement?

A. Next-generation Intrusion Prevention System
B. Next-generation Firewall
C. Web Application Firewall
D. Intrusion Detection System

Answer: B

Explanation:

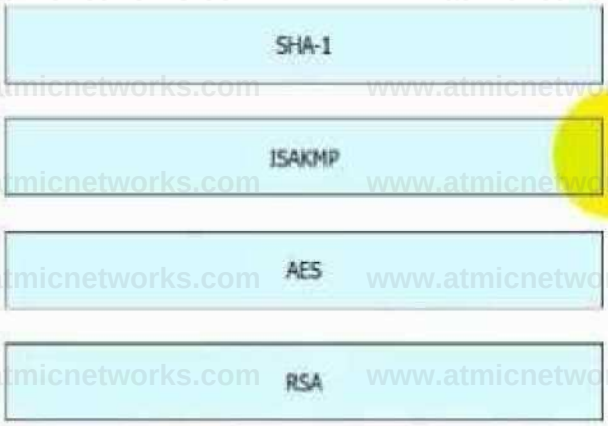
Question: 717

DRAG DROP

Drag and drop the VPN functions from the left onto the descriptions on the right.



Answer:



Question: 718

Which API technology with SDN architecture is used to communicate with a controller and network devices such as routers and switches?

A. REST APIs
B. Northbound APIs
C. Unprotected APIs
D. Southbound APIs

Answer: D

Explanation:

Question: 719

A security engineer must create a policy based on the reputation verdict of a file from a Cisco Secure Email Gateway. The file with an undetermined verdict must be dropped. Which action must the security engineer take to meet the requirement?

A. Configure threshold settings for files with no score to be allowed.
B. Set up a policy to automatically drop files with no reputation score.
C. Implement a policy to disable file analysis.
D. Create a policy to send a file to quarantine.

Answer: B

Explanation:

Question: 720

In which cloud services model is the customer responsible for scanning for and mitigation of application vulnerabilities?

A. PaaS
B. VMaaS
C. IaaS
D. SaaS

Answer: C

Explanation:

Question: 721

A security engineer is tasked with configuring TACACS on a Cisco ASA firewall. The engineer must be able to access the firewall command line interface remotely. The authentication must fall back to the local user database of the Cisco ASA firewall. AAA server group named TACACS-GROUP is already configured with TACACS server IP address 192.168.10.10 and key C1sc0512222832!. Which configuration must be done next to meet the requirement?

A. aaa authentication ssh console LOCAL TACACS-GROUP
B. aaa authentication ssh console TACACS-GROUP LOCAL
C. aaa authentication serial console LOCAL TACACS-GROUP
D. aaa authentication http console TACACS-GROUP LOCAL

Answer: B

Explanation:

Question: 722

An administrator has been tasked with configuring the Cisco Secure Email Gateway to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two.)

A. Deploy the Secure Email Gateway in the DMZ.
B. Use outbreak filters from Cisco Talos.
C. Configure a recipient access table.

D. Enable a message tracking service.
E. Scan quarantined emails using AntiVirus signatures.

Answer: B, E

Explanation:

Question: 723

What are two differences between a Cisco Secure Web Appliance that is running in transparent mode and one running in explicit mode? (Choose two.)

A. The Cisco Secure Web Appliance responds with its own IP address only if it is running in transparent mode.
B. When the Cisco Secure Web Appliance is running in transparent mode, it uses the Secure Web Appliance's own IP address as the HTTP request destination.
C. The Cisco Secure Web Appliance responds with its own IP address only if it is running in explicit mode.
D. The Cisco Secure Web Appliance is configured in a web browser only if it is running in transparent mode.
E. The Cisco Secure Web Appliance uses a Layer 3 device to redirect traffic only if it is running in transparent mode.

Answer: C, E

Explanation:

Question: 724

What is a feature of an endpoint detection and response solution?

A. Preventing attacks by identifying harmful events with machine learning and conduct-based defense
B. Rapidly and consistently observing and examining data to mitigate threats
C. Capturing and clarifying data on email, endpoints, and servers to mitigate threats
D. Ensuring the security of network devices by choosing which devices are allowed to reach the network

Answer: B

Explanation:

Question: 725

How does a Cisco Secure Firewall help to lower the risk of exfiltration techniques that steal customer data?

A. Blocking UDP port 53
B. Blocking TCP port 53
C. Encrypting the DNS communication
D. Inspecting the DNS traffic

Answer: D

Explanation:

Question: 726

An engineer is deploying a Cisco Secure Email Gateway and must configure a sender group that decides which mail policy will process the mail. The configuration must accept incoming mails and relay the outgoing mails from the internal server. Which component must be configured to accept the connection to the listener and meet these requirements on a Cisco Secure Email Gateway?

A. RAT
B. HAT
C. Sender list
D. Access list

Answer: B

Explanation:

Question: 727

For which type of attack is multifactor authentication an effective deterrent?

A. Ping of death
B. Teardrop
C. SYN flood
D. Phishing

Answer: D

Explanation: