ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"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."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

According to Cisco Security Reference Architecture, which solution provides threat intelligence and malware analytics?

A. Cisco pxGrid
B. Cisco XDR
C. Cisco Talos
D. Cisco Umbrella

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Cisco Talos is Cisco's threat intelligence organization, delivering real-time threat intelligence and malware analytics to help organizations detect and prevent threats before they impact the network. According to the SCAZT guide, Talos provides comprehensive coverage of threat data including signatures, indicators of compromise, and context-driven analytics. This intelligence feeds into Cisco security platforms such as Cisco SecureX and Cisco Secure Endpoint to enhance detection, investigation, and response capabilities. Talos is explicitly referenced in the Threat Response section as the primary source of threat intelligence and malware analytics that supports cloud and endpoint security frameworks.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) Study Guide, Section 6: Threat Response, Pages 112-115.

Question: 2

Which types of algorithm does a web application firewall use for zero-day DDoS protection?

A. Reactive and heuristic-based
B. Stochastic and event-based
C. Correlative and feedback-based
D. Adaptive and behavioral-based

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
According to the SCAZT documentation, web application firewalls (WAFs) designed to protect against zero-day Distributed Denial of Service (DDoS) attacks leverage adaptive and behavioral-based algorithms. These algorithms dynamically analyze traffic patterns, baseline normal behavior, and detect anomalies that could indicate novel or zero-day attacks. Unlike signature-based detection, adaptive and behavioral methods adjust in real-time to emerging threats, learning from ongoing traffic without relying on pre-defined rules. This proactive approach enables rapid detection and mitigation of unknown DDoS vectors, critical for cloud and network security where threats evolve constantly.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) Study Guide, Section 3: Network and Cloud Security, Pages 75-77.

Question: 3

An administrator must deploy an endpoint posture policy for all users. The organization wants to have all endpoints checked against antimalware definitions and operating system updates and ensure that the correct Secure Client modules are installed properly. How must the administrator meet the requirements?

A. Configure the WLC to provide local posture services, and configure Cisco ISE to receive the compliance verification from the WLC to be used in an authorization policy.

B. Create an ASA Firewall posture policy, upload the Secure Client images to the NAD, and create a local client provisioning portal.

C. Create the required posture policy within Cisco ISE, configure redirection on the NAD, and ensure that the client provisioning policy is correct.

D. Identify the antimalware being used, create an endpoint script to ensure that it is updated, and send the update log to Cisco ISE for processing.

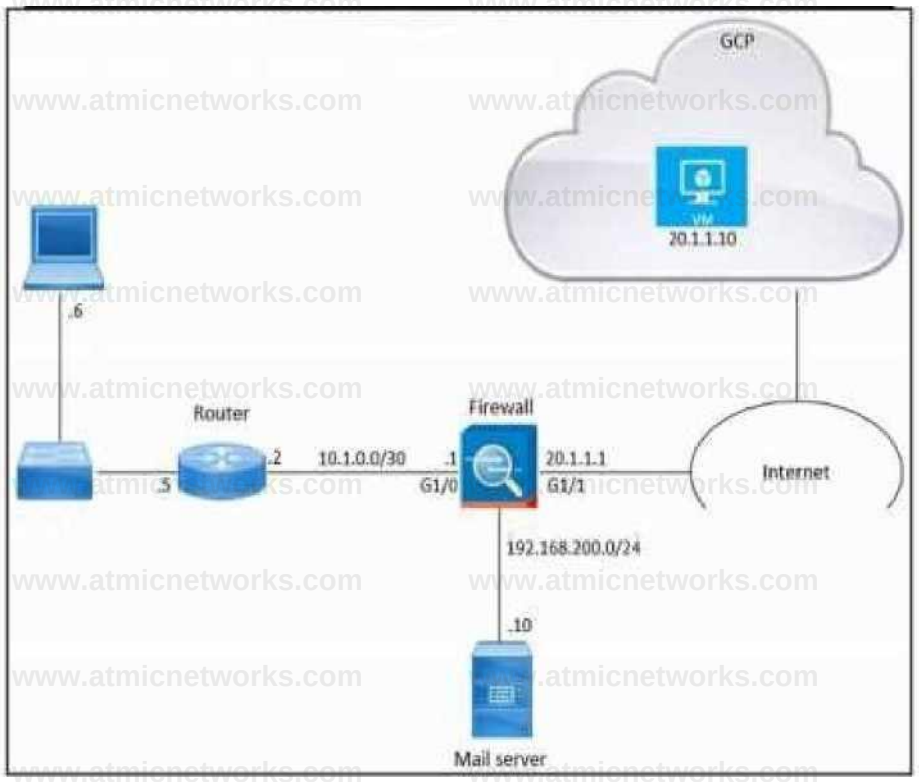
Answer: C

Explanation:

Question: 4

Refer to the exhibit.

iule Numbar	Source	Deitination	Service	Action	Los	Time
1	20.1.1.10	20.1.1.1	Mtp$	Allow	Log	Any
2	Arty	Any	Any	Deny	Log	Any



Refer to the exhibit. An engineer must provide HTTPS access from the Google Cloud Platform virtual machine to the on-premises mail server. All other connections from the virtual machine to the mail server must be blocked. The indicated rules were applied to the firewall; however, the virtual machine cannot access the mail server. Which two actions should be performed on the firewall to meet the requirement? (Choose two.)

A. Set IP address 192.168.200.10 as the destination in rule 1.
B. Move up rule 2.
C. Set IP address 20.1.1.1 as the source in rule 1.
D. Configure a NAT rule.
E. Configure a security group.

Answer: A, D

Explanation:

Question: 5

Refer to the exhibit.

Refer to the exhibit. A security engineer deployed Cisco Secure XDR, and during testing, the log entry shows a security incident. Which action must the engineer take first?

A. Uninstall the malware.

B. Block IP address 10.77.17.45.
C. Isolate the endpoint.
D. Rebuild the endpoint.

Answer: C

Explanation:

Question: 6

Refer to the exhibit.

Refer to the exhibit. An engineer must create a policy in Cisco Secure Firewall Management Center to prevent restricted users from being able to browse any business or mobile phone shopping websites. The indicated policy was applied; however, the restricted users still can browse on the mobile phone shopping websites during business hours. What should be done to meet the requirement?

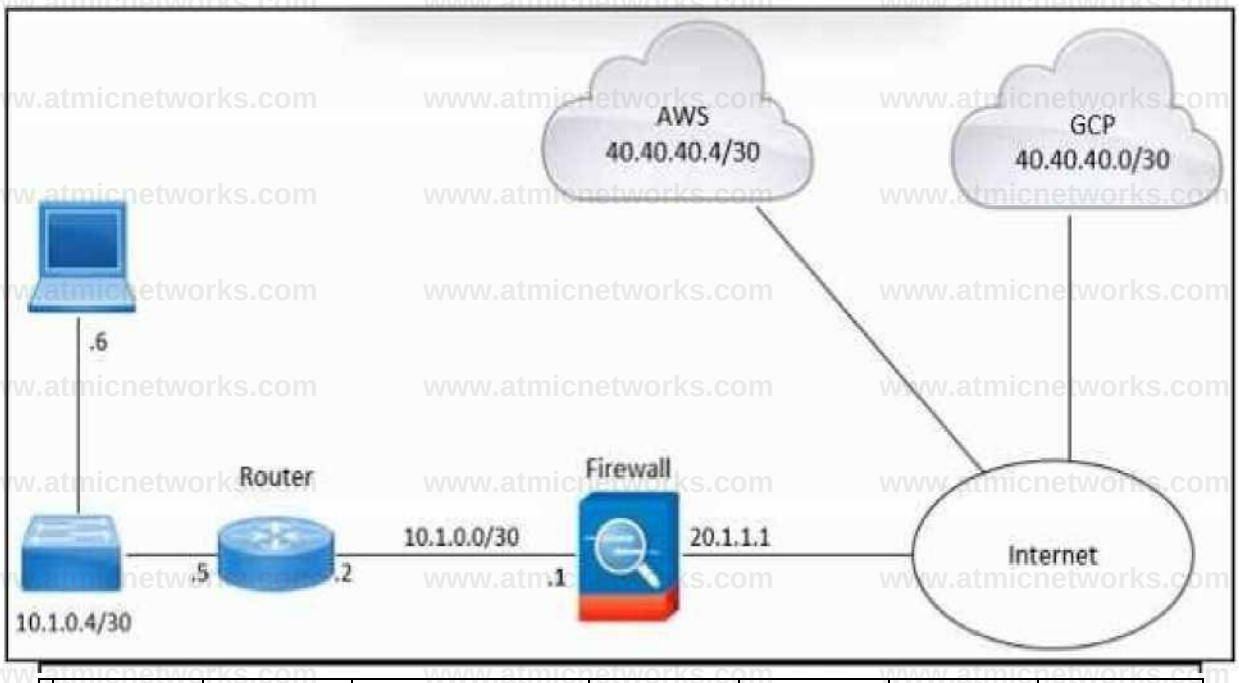
A. Set Dest Zones to Business Mobile Phones Shopping.
B. Set Dest Networks to Business Mobile Phones Shopping.
C. Set Time Range for rule 4 of Access Controlled Groups to All.
D. Move rule 4 Access Controlled Groups to the top.

Answer: D

Explanation:

Question: 7

Refer to the exhibit.



Rule Number	Source	Destination	Service	Action	Log	Time
1	Any	Any	Any	Deny	Log	Any
2	AT,	40.40.40.4/30	RDP	Allow	Log	Any
3	Any	40.40.40.0/30	HTTPS	Allow	Log	Any

Refer to the exhibit. An engineer must provide RDP access to the AWS virtual machines and HTTPS access to the Google Cloud Platform virtual machines. All other connectivity must be blocked. The indicated rules were applied to the firewall; however, none of the virtual machines in AWS and Google Cloud Platform are accessible. What should be done to meet the requirement?

A. Move rule 2 to the first position.
B. Configure a NAT overload rule
C. Configure a virtual private cloud firewall rule
D. Move rule 1 to the last position

Answer: A

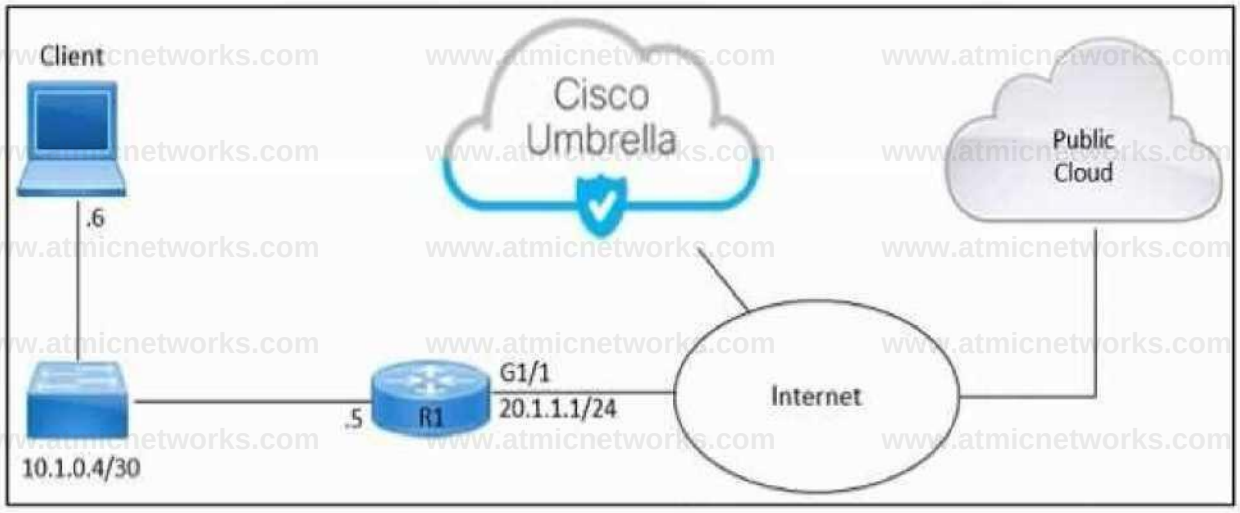
Explanation:

Question: 8

Refer to the exhibit.

```
<output omitted* j
ip domain lookup source-interface GigabitEthernetl/1 l
interface GigabitEthernetl/1
ip vrf forwarding INET
ip flow monitor CISCO-FLOWMONITOR input
ip How monitor CISCO-FLOWMONI TOR Output
ip address 20.1.1.1 255.255.255.0
ip not outside
ip nbar protocol-discovery zone member security INTERNET
```

<output omitted*



Refer to the exhibit. An engineer must connect an on-premises network to the public cloud using Cisco Umbrella as a Cloud Access Security Broker. The indicated configuration was applied to router R1; however, connectivity to Umbrella fails with this error: %OPENDNS-3-DNS_RES_FAILURE. Which action must be taken on R1 to enable the connection?

A. Configure the Open DNS servers with the ip name-server command.
B. Configure a DHCP scope using the ip dhcp pool command.
C. Add the opendns in command to the interface configuration.
D. Add the opendns out command to the interface configuration.

Answer: B

Explanation:

Question: 9

Which mitigation technique does a web application firewall use to protect a web server against DDoS attacks?

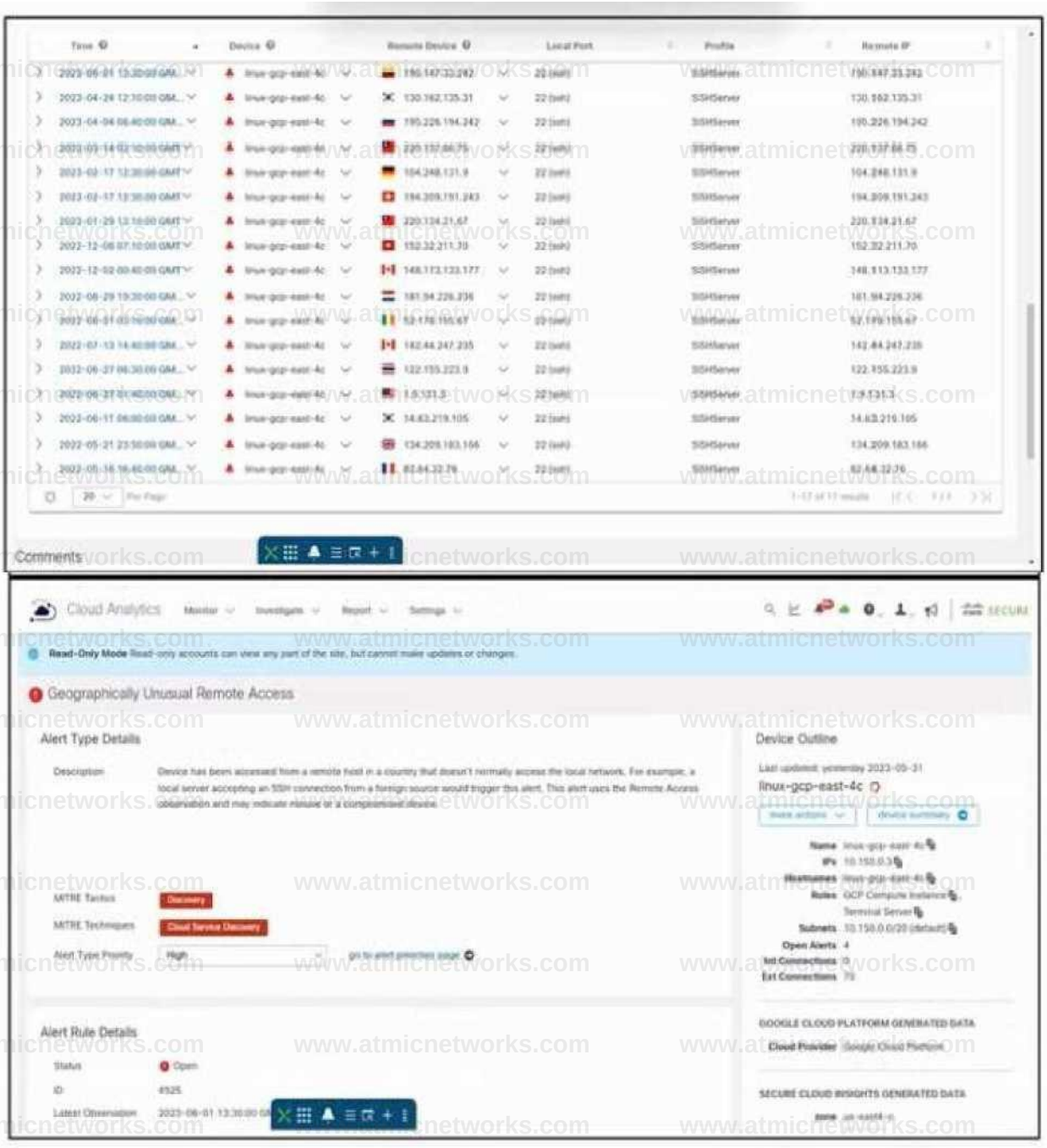
A. Source-specific ACL
B. Standard ACL
C. Packet filtering
D. Rate-based rules

Answer: D

Explanation:

Question: 10

Refer to the exhibit.



Refer to the exhibit. An engineer is investigating an issue by using Cisco Secure Cloud Analytics. The

engineer confirms that the connections are unauthorized and informs the incident management team. Which two actions must be taken next? (Choose two.)

A. Reinstall the host from a recent backup.
B. Quarantine the host
C. Reinstall the host from scratch.
D. Create a firewall rule that has a source of linux-gcp-east-4c, a destination of Any, and a protocol of SSH.
E. Create a firewall rule that has a source of Any, a destination of linux-gcp-east-4c, and a protocol of SSH.

Answer: B, E

Explanation:

Question: 11

In the zero-trust network access model, which criteria is used for continuous verification to modify trust levels?

A. System patching status
B. Detected threat levels
C. User and device behavior
D. Network traffic patterns

Answer: C

Explanation:

Question: 12

Refer to the exhibit.

```
"nnaCt "Allow HTTP",
-parameters-t t
    "HTTPS Consumer*! I
        "type's "Filter",
        "description": "Consumer of tie HTTP service" 1, "HT7M Provider"! I
        "typo": "Filter".
        "description") "Provider of the HTTP service" }

"default colici.es"; [
        ■'output omitted*


        "action"! "BLOCK", "priority": 100.
        "coneumor_filt«r_ref": "HTTP# Consumer",
        "prividet^-^--e-2-*-": "HTTPS Provider", "14_carama": [
```

Refer to the exhibit. An engineer must create a segmentation policy in Cisco Secure Workload to block HTTP traffic. The indicated configuration was applied; however, HTTP traffic is still allowed. What should be done to meet the requirement?

A. Change consumer_filter_ref to HTTP Consumer.
B. Add HTTP to 14_params.

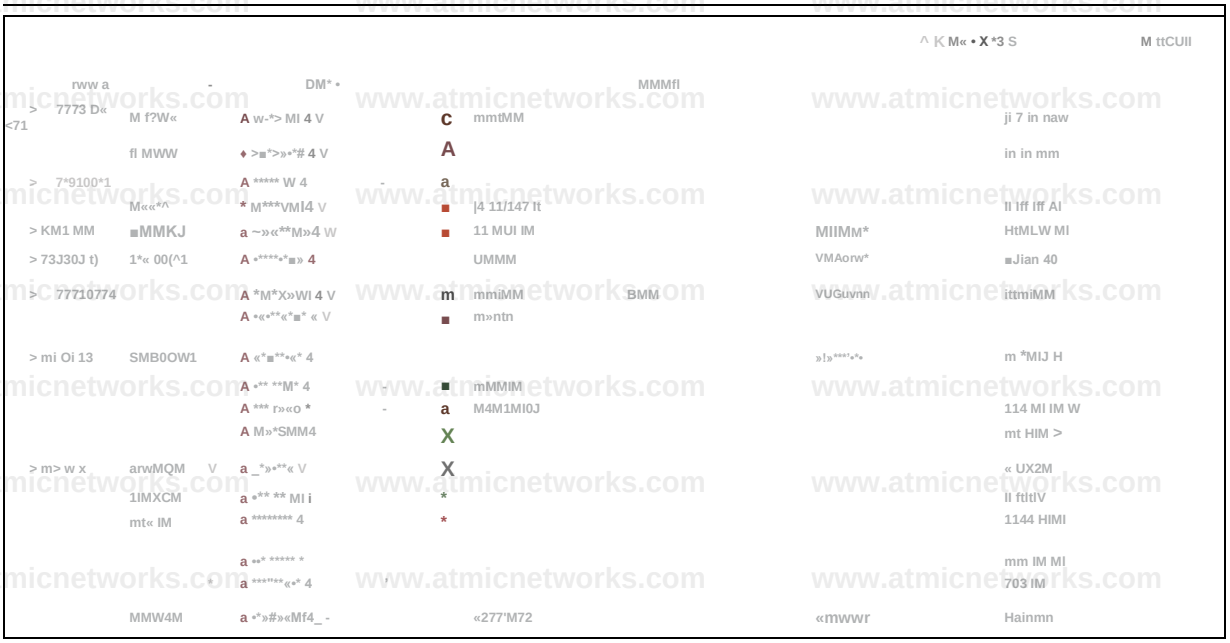
C. Decrease the priority of the template to 50.
D. Increase the priority of the template to 200.

Answer: B

Explanation:

Question: 13

Refer to the exhibit.



Refer to the exhibit. An engineer must analyze the Cisco Secure Cloud Analytics report. What is occurring?

A. Persistent remote-control connections
B. Distributed DDoS attack
C. Geographically unusual remote access
D. Memory exhaustion attempt toward port 22

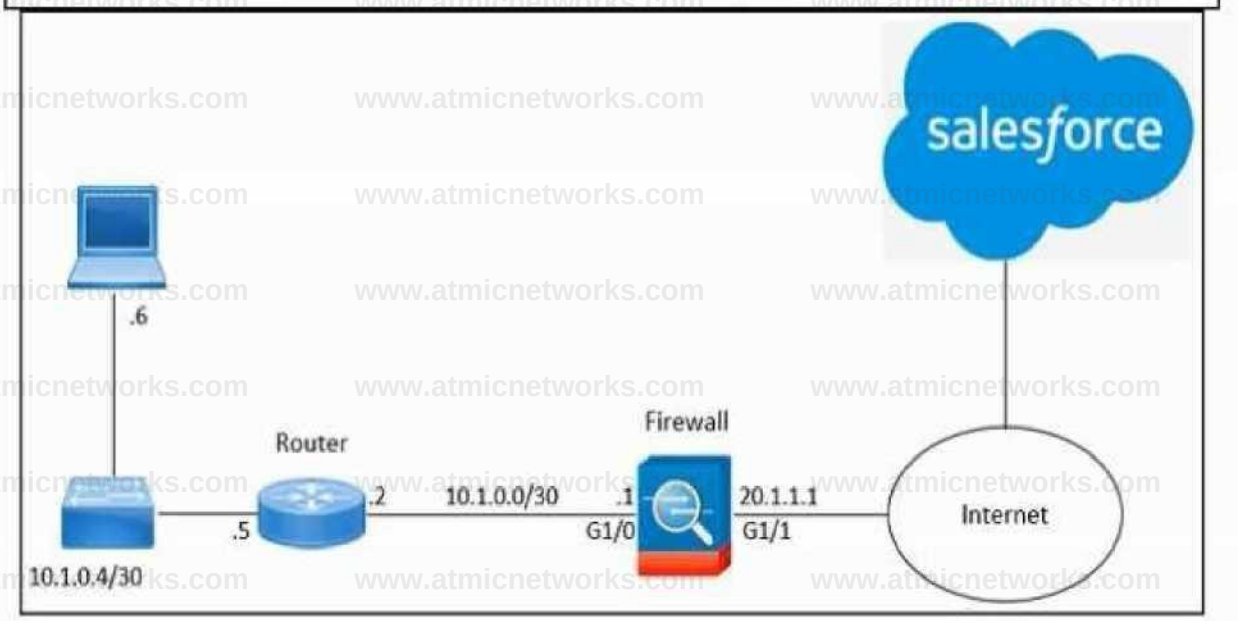
Answer: C

Explanation:

Question: 14

Refer to the exhibit.

Rule Number	Source	Destination	Service	Action	Log	Time
1	10.1.0.4/30	www.salesforce.com	TCP Port 443	Allow	Log	Any
3	10.1.0.0/30	Any	DNS	Deny	Log	Any
4	10.1.0.4/30	4.4.4.4	DNS	Allow	Log	Any
5	10.1.0.4/30	www.salesforce.com	UDP Port 443	Deny	Log	Any
6	10.1.0.4/30	www.salesforce.com	TCP Port 443	Deny	Log	Any
7	Any	Any	Any	Deny	Log	Any



Refer to the exhibit. An engineer must configure the Cisco ASA firewall to allow the client with IP address 10.1.0.6 to access the Salesforce login page at https://www.salesforce.com. The indicated configuration was applied to the firewall and public DNS 4.4.4.4 is used for name resolution; however, the client still cannot access the URL. What should be done to meet the requirements?

A. Remove rule 3
B. Move rule 5 to the top
C. Remove rule 7
D. Move rule 6 to the top

Answer: A

Explanation:

Question: 15

Refer to the exhibit.

```
<output omitted>
crypto ikev1 policy 5
 authentication pre-share
 hash aes-256
 encryption sha-256
 group 1
<output omitted>
```

Refer to the exhibit. An engineer must configure a remote access IPsec/IKEv1 VPN that will use AES256 and SHA256 on a Cisco ASA firewall. The indicated configuration was applied to the firewall; however, the tunnel fails to establish. Which two IKEv1 policy commands must be run to meet the

requirement? (Choose two.)

A. encryption aes-256
B. ipsec-proposal sha-256-aes-256
C. integrity aes-256
D. ipsec-proposal AES256-SHA256
E. hash sha-256

Answer: A, E

Explanation:

Question: 16

Which method is used by a Cisco XDR solution to prioritize actions?

A. Updating antivirus signatures
B. Monitoring endpoint activity
C. Leveraging AI and machine learning
D. Analyzing network traffic patterns

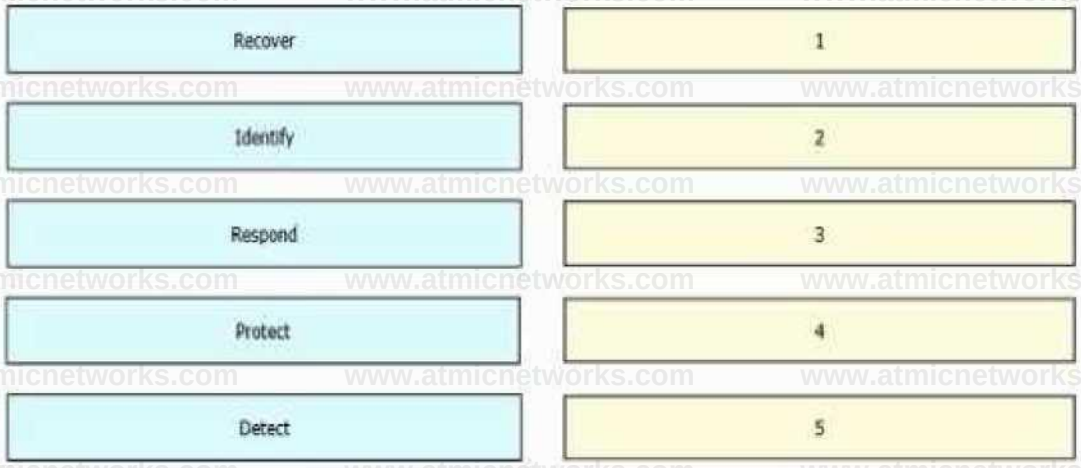
Answer: C

Explanation:

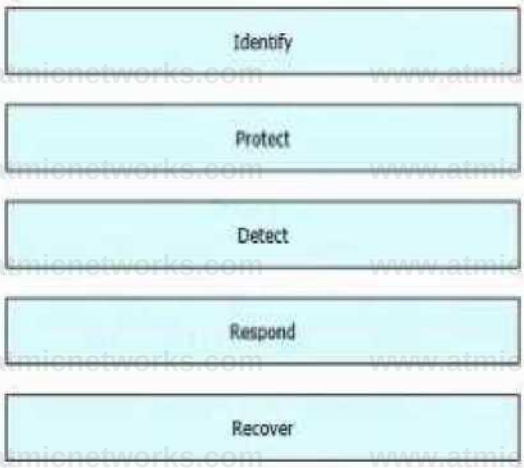
Question: 17

DRAG DROP

Drag and drop the five core functions from the left into the order defined by the NIST Cyber security Framework on the right.



Answer:



Question: 18

Refer to the exhibit.

Refer to the exhibit. An engineer must configure a global allow list in Cisco Umbrella for the cisco.com domain. All other domains must be blocked. After creating a new policy and adding the cisco.com domain, the engineer attempts to access a site outside of cisco.com and is successful. Which additional Security Settings action must be taken to meet the requirement?

A. Limit Content Access.
B. Enforce SafeSearch.
C. Enable Allow-Only Mode
D. Apply Destination List.

Answer: C

Explanation:

Question: 19

An administrator received an incident report indicating suspicious activity of a user using a corporate device. The manager requested that the credentials of user user1@cisco.com be reset and synced via the Active Directory. Removing the account should be avoided and used for further investigation on data leak. Which configuration must the administrator apply on the Duo Admin Panel?

A. Delete the user in the Users tab option and sync it with the domain controller.

B. Quarantine the user from all the policies on the Policies tab, including associated devices.
C. Request the password change on the Device tab on managed devices.
D. Disable the account on the Users tab and reset the password from the Active Directory.

Answer: D

Explanation:

Question: 20

What helps prevent drive-by compromise?

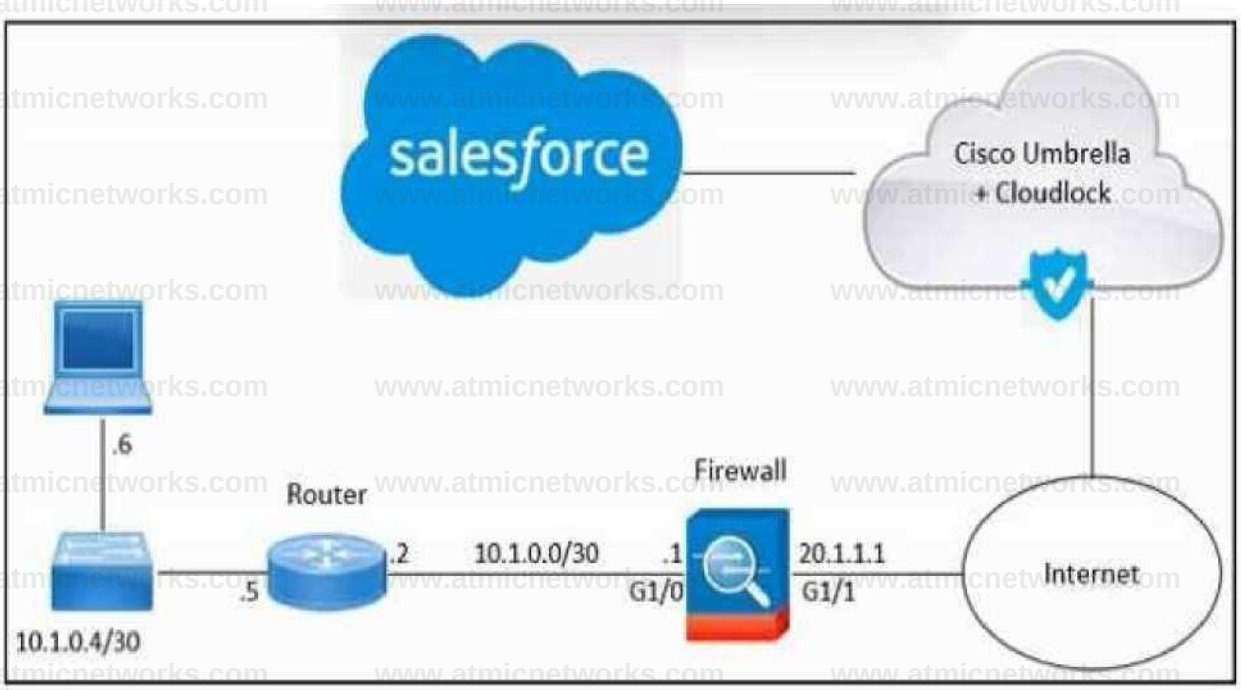
A. Ad blockers
B. VPN
C. Incognito browsing
D. Browsing known websites

Answer: A

Explanation:

Question: 21

Refer to the exhibit.



Refer to the exhibit. An engineer must integrate Cisco Cloudlock with Salesforce in an organization. Despite the engineer's successful execution of the Salesforce integration with Cloudlock, the administrator still lacks the necessary visibility. What should be done to meet the requirement?

A. From Salesforce, configure the service parameters.
B. From Salesforce, enable the View All Data permission.

C. From Cloudlock, configure the service parameters.
D. From Cloudlock, enable the View All Data permission.

Answer: B

Explanation:

Question: 22

What must be automated to enhance the efficiency of a security team response?

A. Changing all user passwords when a threat is detected
B. Changing firewall settings for every detected threat, regardless of its severity
C. Isolating affected systems and applying predefined security policies
D. Sending an email to the entire organization when a threat is detected

Answer: C

Explanation:

Question: 23

Refer to the exhibit.

Rule Number	Source	Destination	Service	Action	Log	Time
1	10.1.0.0/30	Any	SSH	Deny	log	18h00 ShOOam
2	10.1.0.0/30	Any	SSH	Allow	Log	8h00am - 18h00
3	10.1.0.0/30	Any	Any	Allow	Log	18MJ0 - 8h00am
4	10.1.0.4/30	Any	Any	Allow	Log	Any
5	10.1.0.4/30	Any	SSH	Deny	Log	18h00 ■ ShOOam
6	Any	Any	Any	Deny	Log	Any

SSH Traffic ->

Refer to the exhibit. An engineer must troubleshoot an issue with excessive SSH traffic leaving the internal network between the hours of 18:00 and 08:00. The engineer applies a policy to the Cisco ASA firewall to block outbound SSH during the indicated hours; however, the issue persists. What

should be done to meet the requirement?

A. Change the time of rule 2.
B. Delete rule 4
C. Delete rule 3
D. Change the time of rule 5

Answer: B

Explanation:

Question: 24

What does the MITRE ATT&CK framework catalog?

A. Techniques utilized in cyber attacks
B. Patterns of system vulnerabilities
C. Models of threat intelligence sharing
D. Standards for information security management

Answer: A

Explanation:

Question: 25

An organization is distributed across several sites. Each site is connected to the main HQ using site- to-site VPNs implemented using Secure Firewall Threat Defense. Which functionality must be implemented if the security manager wants to send SaaS traffic directly to the internet?

A. Multi-instances
B. IPsec tunnels
C. Policy-based routing
D. ECMP routing

Answer: C

Explanation:

Question: 26

DRAG DROP

Drag and drop the tasks from the left into order on the right to implement adding Duo multifactor authentication to Meraki Client VPN login.

Configure Meraki Client VPN.	step 1
Install and configure the local Duo Authentication Proxy.	step 2
Configure Duo Authentication Proxy to work with Meraki MX.	step 3
Set up the Duo Proxy Primary Authenticator.	step 4

Answer:

Set up the Duo Proxy Primary Authenticator.

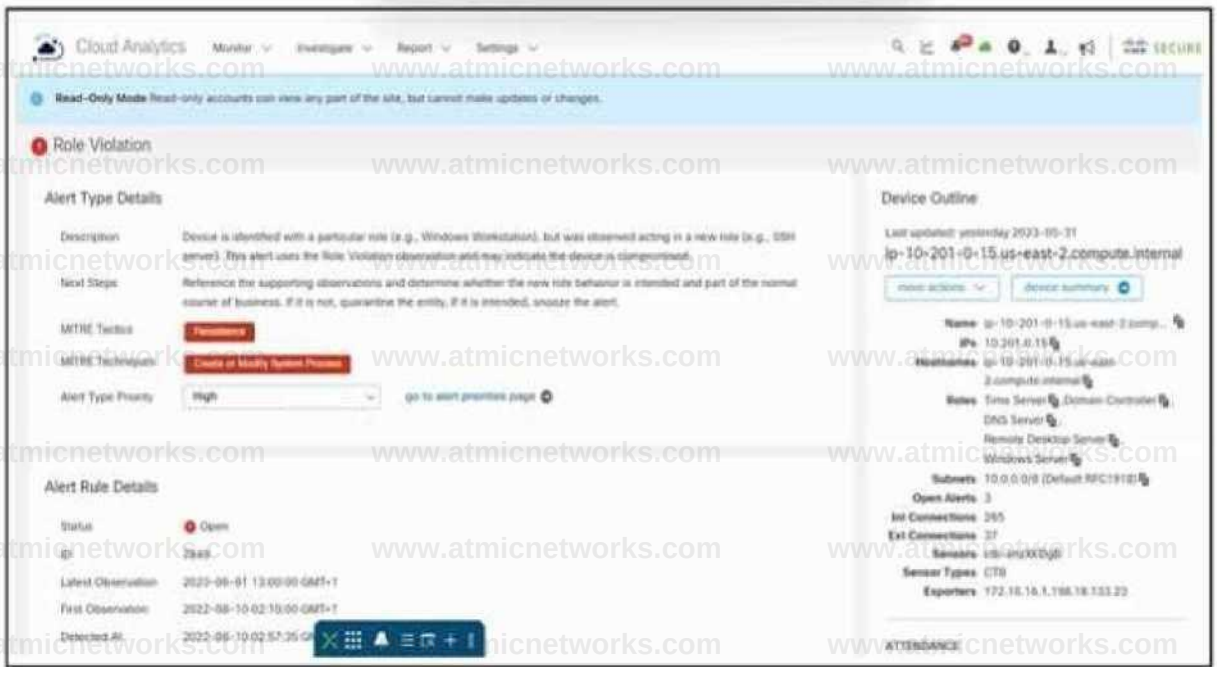
Install and configure the local Duo Authentication Proxy.

Configure Duo Authentication Proxy to work with Meraki MX.

Configure Meraki Client VPN.

Question: 27

Refer to the exhibit.



Refer to the exhibit. An engineer is troubleshooting an incident by using Cisco Secure Cloud Analytics. What is the cause of the issue?

A. An attacker installed an SSH server on the host.
B. An attacker opened port 22 on the host.
C. An FTP client was installed on a domain controller.
D. An FTP client was installed on a workstation.

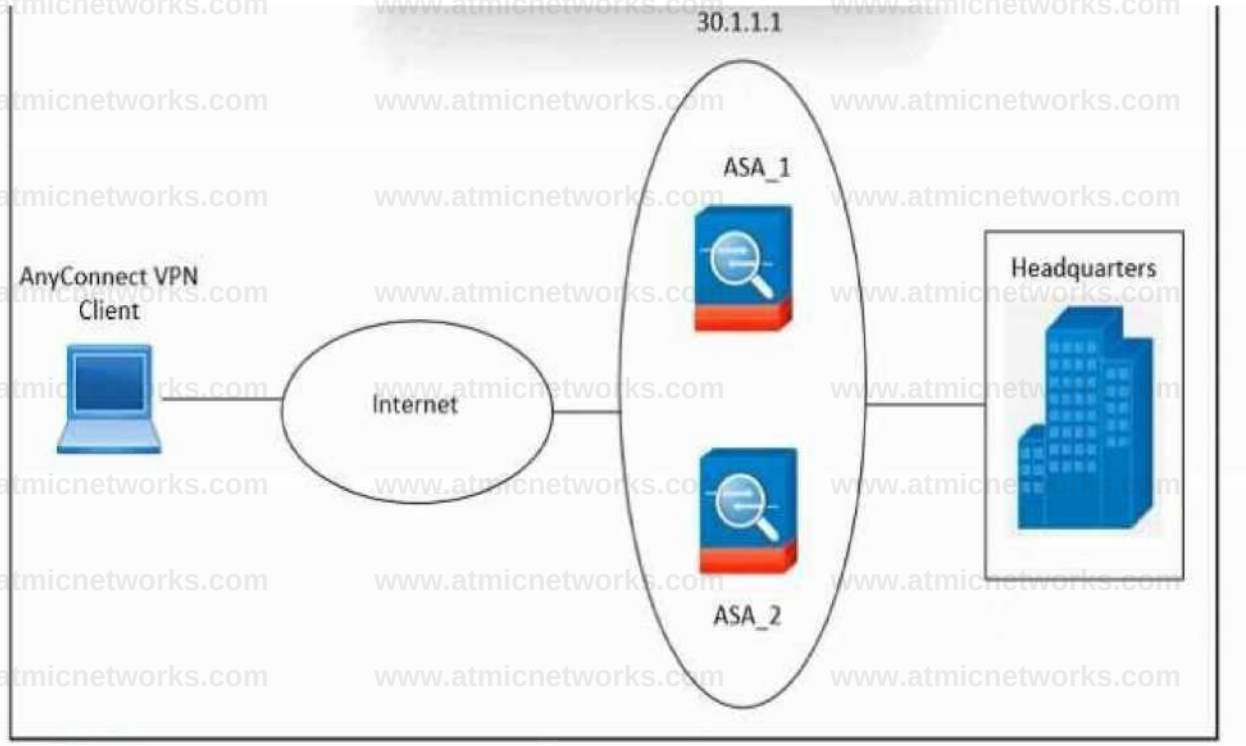
Answer: C

Explanation:

Question: 28

Refer to the exhibit.

```
!
<Ouput omitted>
!
ASA_1(config)#vpn load-balancing
ASA_1(config-load-balancing)#priority 10
ASA_1(config-load-balancing)#cluster key SecretKey01!
ASA_1(config-load-balancing)#cluster ip address 30.1.1.1
!
<Ouput omitted>
!
```



Refer to the exhibit. An engineer must configure VPN load balancing across two Cisco AS

A. The indicated configuration was applied to each firewall; however, the load-balancing encryption scheme fails to work. Which two commands must be run on each firewall to meet the requirements? (Choose two.)

A. cluster port 9024

B. crypto ikev1 policy 1

C. hash sha-256

D. encryption aes 256

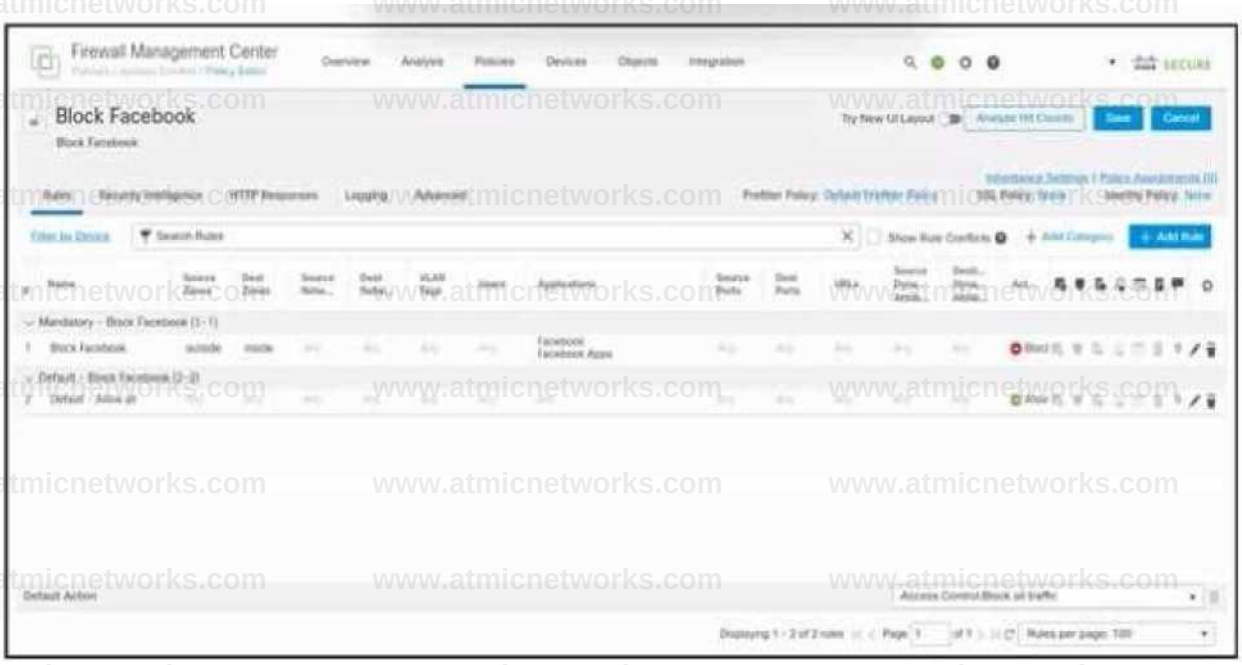
E. cluster encryption

Answer: B, E

Explanation:

Question: 29

Refer to the exhibit.



Refer to the exhibit. An engineer must block internal users from accessing Facebook and Facebook Apps. All other access must be allowed. The indicated policy was created in Cisco Secure Firewall Management Center and deployed to the internet edge firewall; however, users still can access Facebook. Which two actions must be taken to meet the requirement? (Choose two.)

A. Set Destination Zones to outside for rule 2.
B. Set Source Zones to inside for rule 2.
C. Set Applications to Facebook and Facebook Apps for rule 2.
D. Set Destination Zones to outside for rule 1.
E. Set Source Zones to inside for rule 1.

Answer: D, E

Explanation:

Question: 30

What is a crucial component in the MITRE ATT&CK framework?

A. Techniques for accessing credentials
B. Incident response workflow
C. Blueprint for a secure network architecture
D. Best practices for user access management

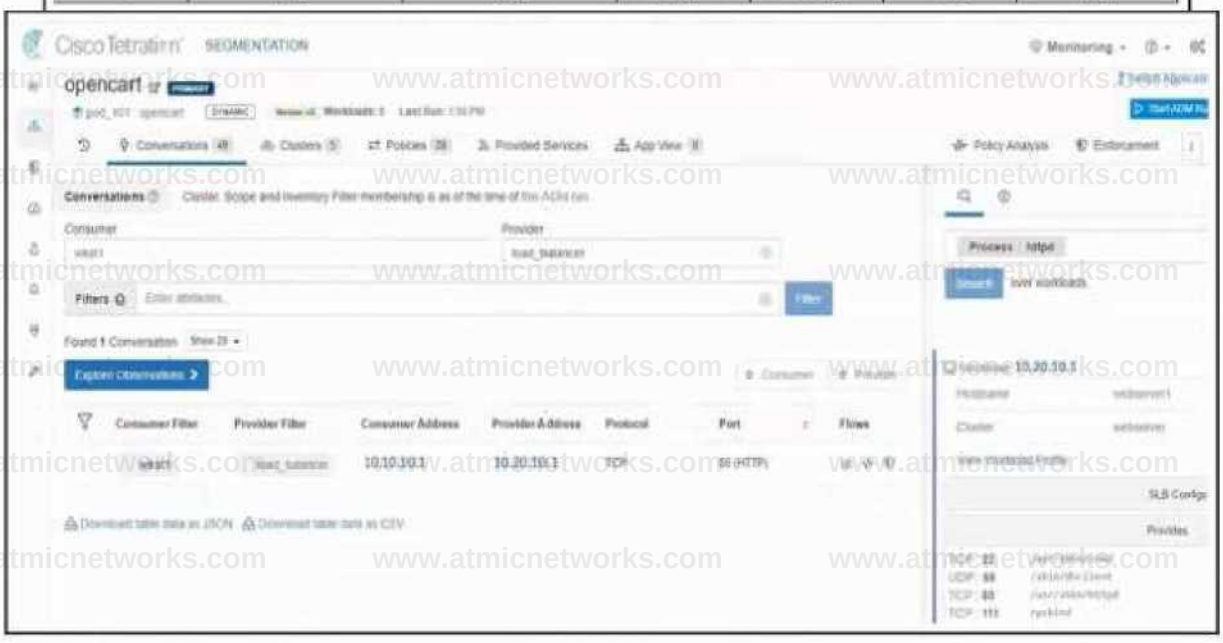
Answer: A

Explanation:

Question: 31

Refer to the exhibit.

Rule Number	Source	Destination	Service	Action	Log	Time
1	10.10.10.1	10.20.10.1	http	Allow	Log	Any
2	10.10.10.1	10.20.10.1	https	Allow	Log	Any
3	10.10.10.1	10.20.10.1	ssh	Allow	Log	Any
4	10.10.10.1	10.20.10.1	UDP port 68	Allow	Log	Any
5	10.20.10.1	10.10.10.1	http	Allow	Log	Any
6	Any	Any	Any	Deny	Log	Any



Refer to the exhibit. An engineer must create a firewall policy to allow web server communication only. The indicated firewall policy was applied; however, a recent audit requires that all firewall policies be optimized. Which set of rules must be deleted?

A. Rules 3 and 4
B. Rules 2 to 4
C. Rules 2 to 5
D. Rules 1 and 5

Answer: A

Explanation:

Question: 32

Refer to the exhibit.

Refer to the exhibit. An engineer must configure SAML SSO in Cisco ISE to use Microsoft Azure AD as an identity provider. These configurations were performed:
Configure a SAML IdP in ISE.
Configure the Azure AD IdP settings.
Which two actions must the engineer take in Cisco ISE? (Choose two.)

A. Add a SAML IdP.
B. Upload metadata from Azure AD to ISE.
C. Configure SAML groups in ISE.
D. Configure the External Identity Sources settings.
E. Configure the Internal Identity Source Sequence setting.

Answer: B, E

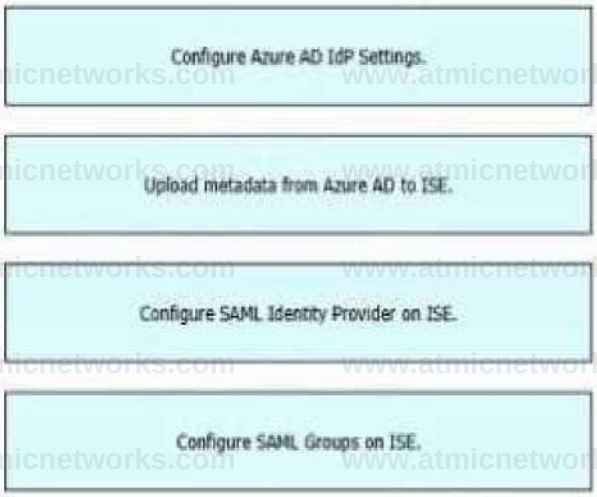
Explanation:

Question: 33

DRAG DROP
Refer to the exhibit.

Refer to the exhibit. An engineer must configure SAML single sign-on in Cisco ISE to use Microsoft Azure AD as an identity provider. Drag and drop the steps from the left into the sequence on the right to configure Cisco ISE with SAML single sign-on.

Answer:



Question: 34

Refer to the exhibit.

Refer to the exhibit. An engineer is analyzing a Cisco Secure Firewall Management Center report.

Which activity does the output verify?

A. An HTTP response from IP address 10.1.104.101 was blocked.

B. An HTTP request to IP address 10.1.113.7 was blocked.

C. A DNS request to IP address 172.17.1.2 was blocked.
D. A DNS response from IP address 10.1.108.100 was blocked.

Answer: D

Explanation:

Question: 35

Which concept is used in the Cisco SAFE key reference model?

A. Secure Domains
B. Cloud Edge
C. Security Intelligence
D. Threat Defense

Answer: A

Explanation:

Question: 36

A security analyst detects an employee endpoint making connections to a malicious IP on the internet and downloaded a file named Test0511127691C.pdf. The analyst discovers the machine is infected by trojan malware. What must the analyst do to mitigate the threat using Cisco Secure Endpoint?

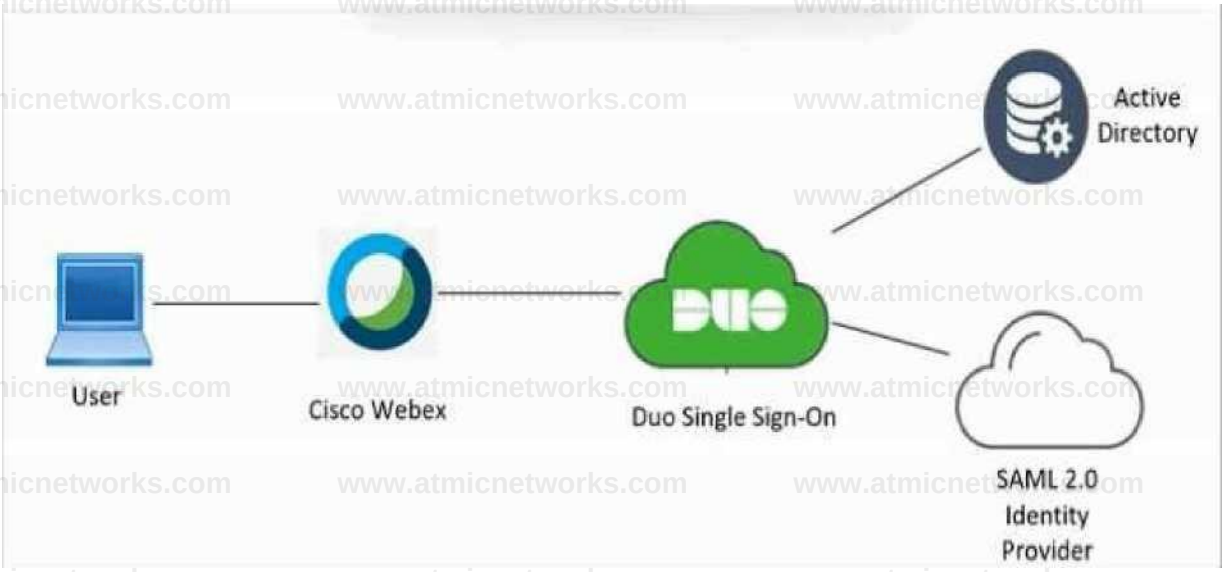
A. Identify the malicious IPs and place them in a blocked list
B. Create an IP Block list and add the IP address of the affected endpoint
C. Enable scheduled scans to detect and block the executable files
D. Start isolation of the machine on the Computers tab

Answer: D

Explanation:

Question: 37

Refer to the exhibit.



Refer to the exhibit. An engineer must configure Duo SSO for Cisco Webex and add the Webex application to the Duo Access Gateway. Which two actions must be taken in Duo? (Choose two.)

A. Upload the application XML metadata file.
B. Upload the SAML application JSON file.
C. Configure the Applications settings for Cisco Webex.
D. Import the Identity Provider metadata.
E. Add a new application to the Duo platform.

Answer: A, E

Explanation:

Question: 38

Which common strategy should be used to mitigate directory traversal attacks in a cloud environment?

A. Use anti-cross-site request forgery tokens.
B. Apply the principle of least privilege.
C. Implement functionality validation.
D. Limit file system permissions.

Answer: D

Explanation:

Question: 39

Which attack mitigation must be in place to prevent an attacker from authenticating to a service using a brute force attack?

A. Forced password change every 6 months
B. Use of a 100 ms delay between each authentication
C. Use of a password manager
D. Use of multifactor authentication for all accounts

Answer: D

Explanation:

Question: 40

What is associated with implementing Cisco zero-trust architecture?

A. It verifies trust before granting access to resources.
B. It focuses on perimeter-based security.
C. It assumes that all network traffic is trustworthy.
D. It provides the same security as the VPN technology.

Answer: A

Explanation:

Question: 41

An engineer configures trusted endpoints with Active Directory with Device Health to determine if an endpoint complies with the policy posture. After a week, an alert is received by one user, reporting problems accessing an application. When the engineer verifies the authentication report, this error is found:
"Endpoint is not trusted because Cisco Secure Endpoint check failed, Check user's endpoint in Cisco Secure Endpoint."
Which action must the engineer take to permit access to the application again?

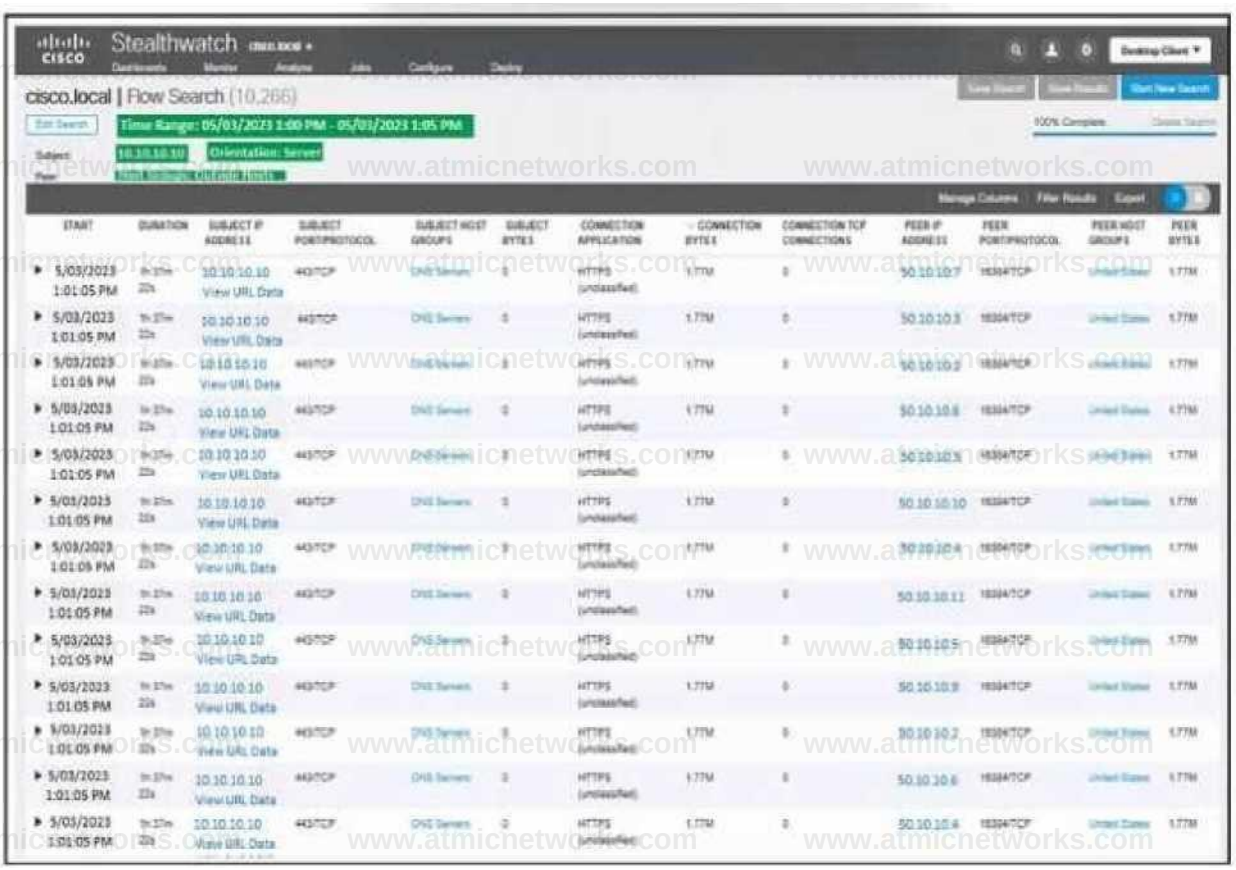
A. Verify the Cisco Secure Endpoint admin panel and approve the access to the user on the Management tab after a complete virus check of the user's laptop.
B. Verify the Trusted Endpoints policy to verify the status of the machine, and after a complete process of analysis, permit the machine to have access to the application.
C. Verify the Duo admin panel, check the EndPoints tab, verify the status of the machine, and after a complete process of analysis, mark the computer as Resolved to permit the user to authenticate again.
D. Verify the Cisco Secure Endpoint admin panel, check the Inbox tab, verify the status of the machine, and after a complete process of analysis, mark the computer as Resolved to permit the user to authenticate again.

Answer: D

Explanation:

Question: 42

Refer to the exhibit.



Refer to the exhibit. An engineer must troubleshoot an incident by using Cisco Secure Cloud Analytics. What is the cause of the issue?

A. SYN flood attack toward the DNS server that has IP address 10.10.10.10
B. DoS attack toward the 50.10.10.0/24 network from an internal IP address
C. Ping of Death attack toward the host that has IP address 10.10.10.10
D. TCP fingerprinting toward the 50.10.10.0/24 network

Answer: A

Explanation:

Question: 43

DRAG DROP

An engineer must configure certificate-based authentication in a cloud-delivered Cisco Secure Firewall Management Center. Drag and drop the steps from left to right to manually enroll certificates on a Cisco Secure Firewall Threat Defense Virtual device.

Obtain an identity certificate from the PKI CA server.	step 1
Import the identity certificate into FTD.	step 2
Select a certificate enrollment object from FTD.	step 3
Generate CSR from FTD.	step 4

Answer:

Select a certificate enrollment object from FTD.

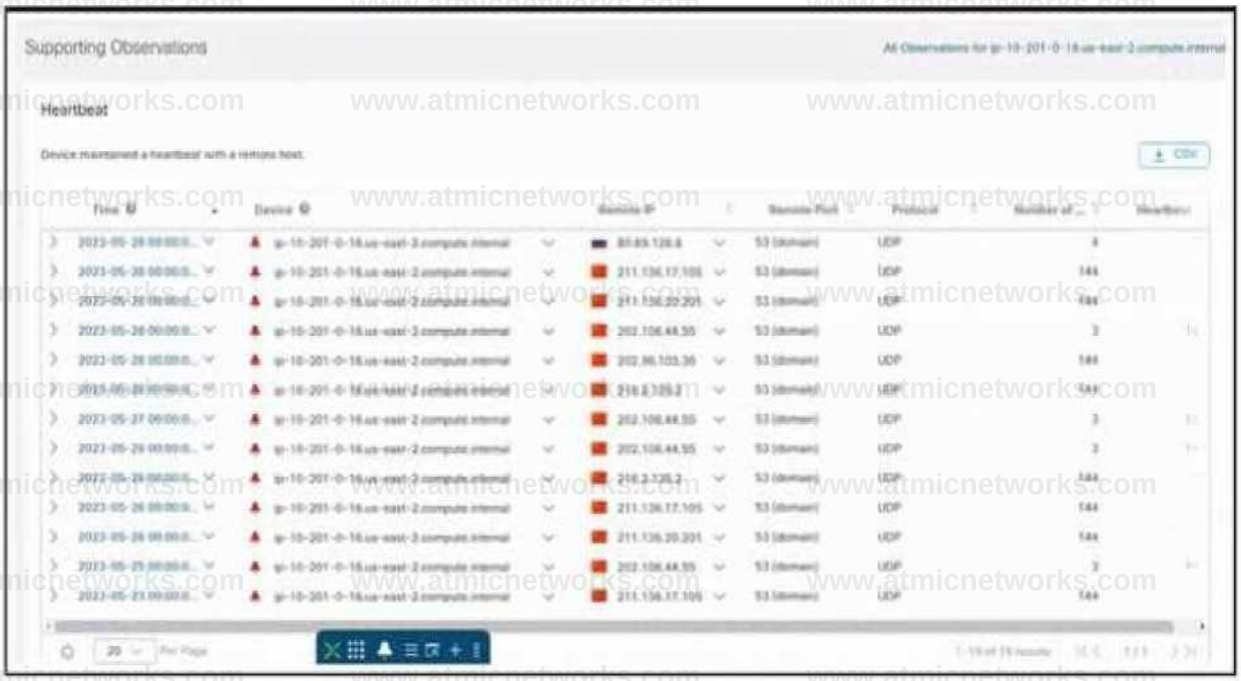
Generate CSR from FTD.

Obtain an identity certificate from the PKI CA server.

Import the identity certificate into FTD.

Question: 44

Refer to the exhibit.



Refer to the exhibit. An engineer is investigating an unauthorized connection issue using Cisco Secure Cloud Analytics. Which two actions must be taken? (Choose two.)

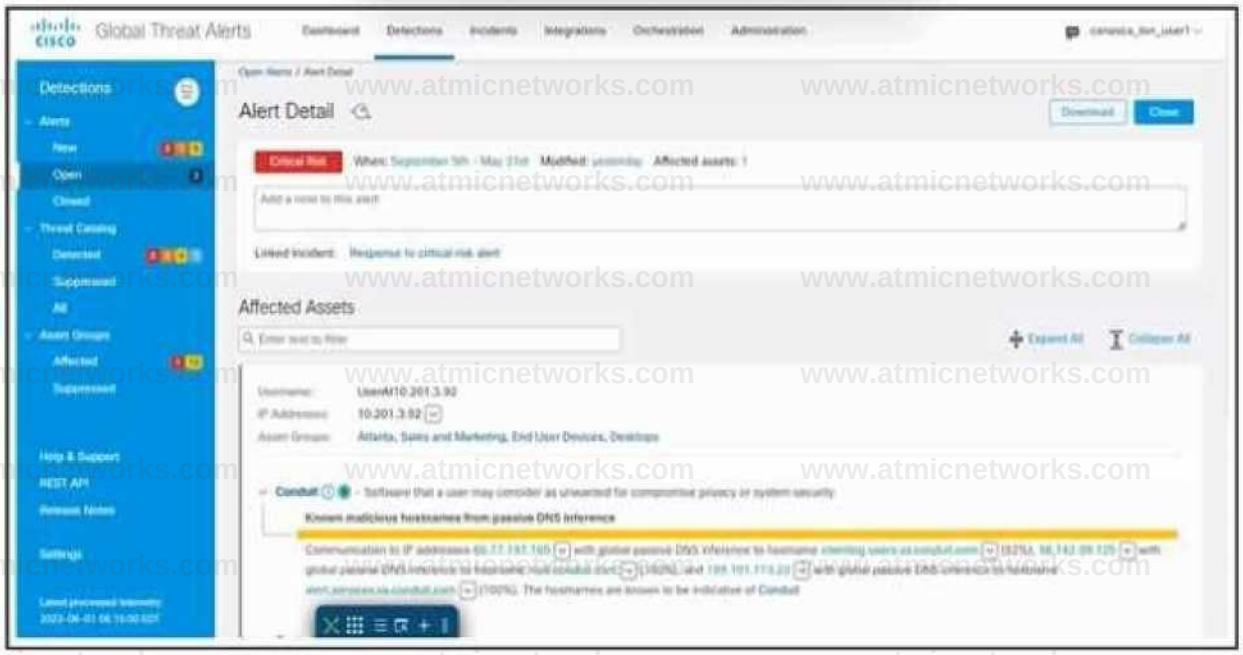
A. Reinstall the host from a recent backup.
B. Inform the incident management team.
C. Validate the IDS logs
D. Block the unwanted IP addresses on the firewall
E. Reinstall the host from scratch.

Answer: B, D

Explanation:

Question: 45

Refer to the exhibit.



Refer to the exhibit. An engineer is investigating the critical alert received in Cisco Secure Network Analytics. The engineer confirms that the incident is valid. Which two actions must be taken? (Choose two.)

A. Inform the incident management team.
B. Block IP address 66.77.197.165
C. Uninstall the Conduit software.
D. Shut down the host.
E. Quarantine the host

Answer: A, B

Explanation:

Question: 46

An engineer is configuring multifactor authentication using Duo. The implementation must use Duo Authentication Proxy and the Active Directory as an identity source. The company uses Azure and a local Active Directory. Which configuration is needed to meet the requirement?

A. Configure the Identity Source as "SAML" on the Single Sign-On tab in the Duo Admin Panel, and configure the forwarding proxy as "local" for the Identity Source.
B. Configure the Identity Source as "SAML" on the Single Sign-On tab, and configure the authentication proxy with the "[cloud]" section.
C. Configure the Identity Source as "Active Directory" on the Single Sign-On tab in the Duo Admin Panel, and configure the permit list to "Local database".
D. Configure the Identity Source as "Active Directory" on the Single Sign-On tab, and configure the authentication proxy with the "[sso]" section.

Answer: D

Explanation:

Question: 47

Refer to the exhibit.

```
<output omitted>
crypto ikev2 policy 5
   authentication pre-share
   encryption aes-256
   group 2
<output omitted>
```

Refer to the exhibit. An engineer must configure a remote access IPsec/IKEv2 VPN that will use SHA- 512 on a Cisco ASA firewall. The indicated configuration was applied to the firewall; however, the tunnel fails to establish. Which command must be run to meet the requirement?

A. integrity sha512
B. protocol esp encryption sha512
C. ipsec-proposal sha512
D. encryption sha512

Answer: C

Explanation:

Question: 48

What does the Cisco Telemetry Broker provide for telemetry data?

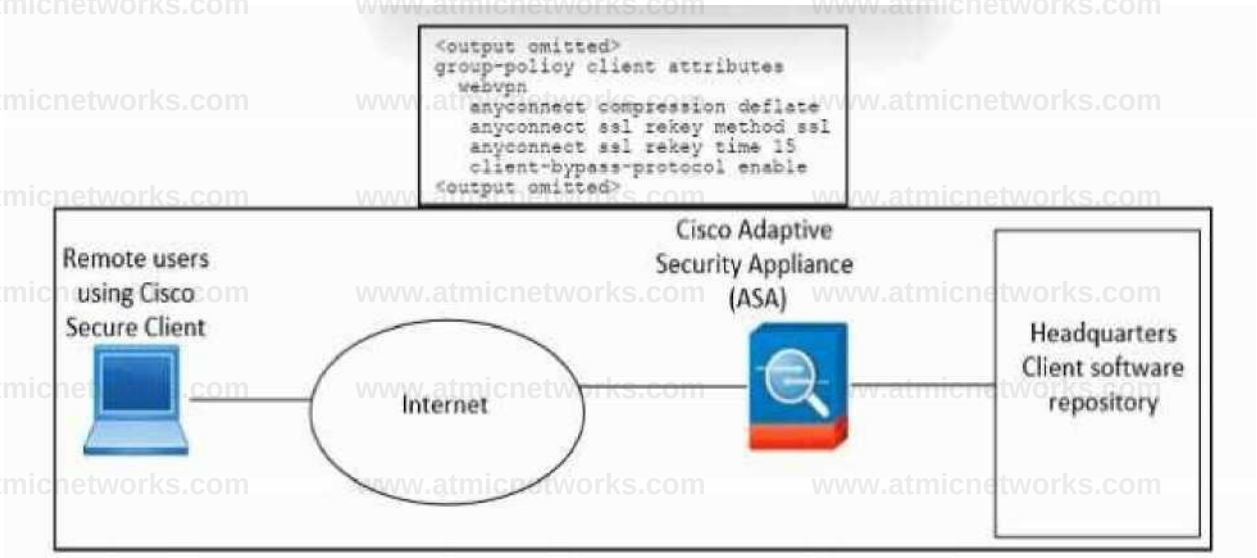
A. Data analytics
B. Data mining
C. Data filtering
D. Data brokering

Answer: D

Explanation:

Question: 49

Refer to the exhibit.



Refer to the exhibit. An engineer must configure Cisco ASA so that the Secure Client deployment is removed when the user laptop disconnects from the VPN. The indicated configuration was applied to the Cisco ASA firewall. Which command must be run to meet the requirement?

A. client-bypass-protocol enable
B. anyconnect keep-installer none
C. anyconnect firewall-rule client-interface
D. client-bypass-protocol disable

Answer: D

Explanation:

Question: 50

Which SAFE component logically arranges the security capabilities into blueprints?

A. Reference Architectures
B. Cisco Validated Designs
C. Places in the Network
D. Secure Domains

Answer: A

Explanation:

Question: 51

A recent InfraGard news release indicates the need to establish a risk ranking for all on-premises and cloud services. The ACME Corporation already performs risk assessments for on-premises services and has applied a risk ranking to them. However, the cloud services that were used lack risk rankings. What Cisco Umbrella function should be used to meet the requirement?

A. Secure Internet Gateway
B. Domain Name Server Filtering

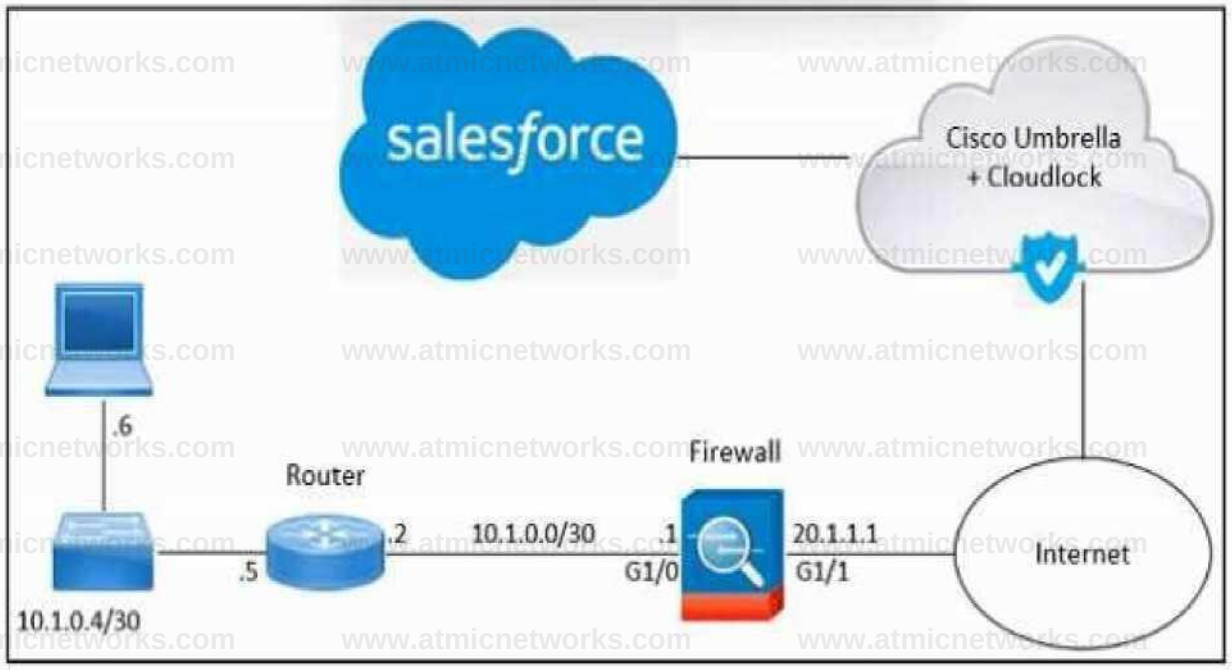
C. URL Categorization by Talos
D. App Discovery

Answer: D

Explanation:

Question: 52

Refer to the exhibit.



Refer to the exhibit. An engineer must enable access to Salesforce using Cisco Umbrella and Cisco Cloudlock. These actions were performed:

From Salesforce, add the Cloudlock IP address to the allow list

From Cloudlock, authorize Salesforce

However, Salesforce access via Cloudlock is still unauthorized. What should be done to meet the requirements?

A. From the Salesforce admin page, grant API access to Cloudlock.
B. From the Salesforce admin page, grant network access to Cloudlock
C. From the Cloudlock dashboard, grant API access to Salesforce.
D. From the Cloudlock dashboard, grant network access to Salesforce.

Answer: A

Explanation:

Question: 53

Refer to the exhibit.

```
3cspa: Appt
  Child ecop* * It ApptiXT
  Child scope 3 2: Apes:HP.
```

Policy Score: Arps
Rule"# li'ALLCKHR -> IT os DC? port 23 Default) Rule # 21 DENY MR -? IT or. TCP port 23 (Absolute, Rule 3 3: Catch All - Allow

Refer to the exhibit. An engineer must analyze a segmentation policy in Cisco Secure Workload. What is the result of applying the policy?

A. The default catch-all rule is applied by using Rule #3.
B. HR cannot use Telnet to connect to IT by using Rule #2.
C. HR can use Telnet to connect to IT by using Rule #1.
D. The explicit deny all rule is applied.

Answer: B

Explanation:

Question: 54

Refer to the exhibit.

```
Clacoas** show vpn-seaaiondb detail anyconnaet UsernaBe s USERI   Index   j 1
Assigned IP : 10.1.2.3            Public IP : 4.5.64
Protocol     : AnyConnect-Parent SSL-Tunnel rc-i-Tunnel
License      : AnyConnect Premium
Bytes Tx     : 465106               Bytes Bx      : 395293
Pkts Tx      : 3310                 Pkts Rx       : 4115
Group Polley : PolicyAllow Tunnel Group : Employee
Login Tim : 01:41:14 CUST Mon Kar 9 2020
Duration : Oh :17a:45a
TCP Dat Port : 443                  Autb Kode     : userPassword
Idle Time Out: 30 Minutes           Idle TO Left : 12 Minutes
```

tunnel-group Employee weevpn-atributes

```
pro-fill-username asL«clienc secondary-pre-fi11-username ss.-cllent group-alias Employee enable
```

Refer to the exhibit. An engineer must implement a remote access VPN solution that provides user and device verification. The company uses Active Directory for user authentication and ID certificates for device identity. Users are currently able to connect using only a valid username and password, even if their computer is missing the required certificate.

Which command from the Cisco ASA tunnel-group completes the requirement of verifying device identity in addition to user identity?

A. ldap-attribute-map PolicyAllow
B. webvpn authorize-device
C. authentication mfa
D. authentication aaa certificate

Answer: B

Explanation:

Question: 55

According to the MITRE ATT&CK framework, which approach should be used to mitigate exploitation risks?

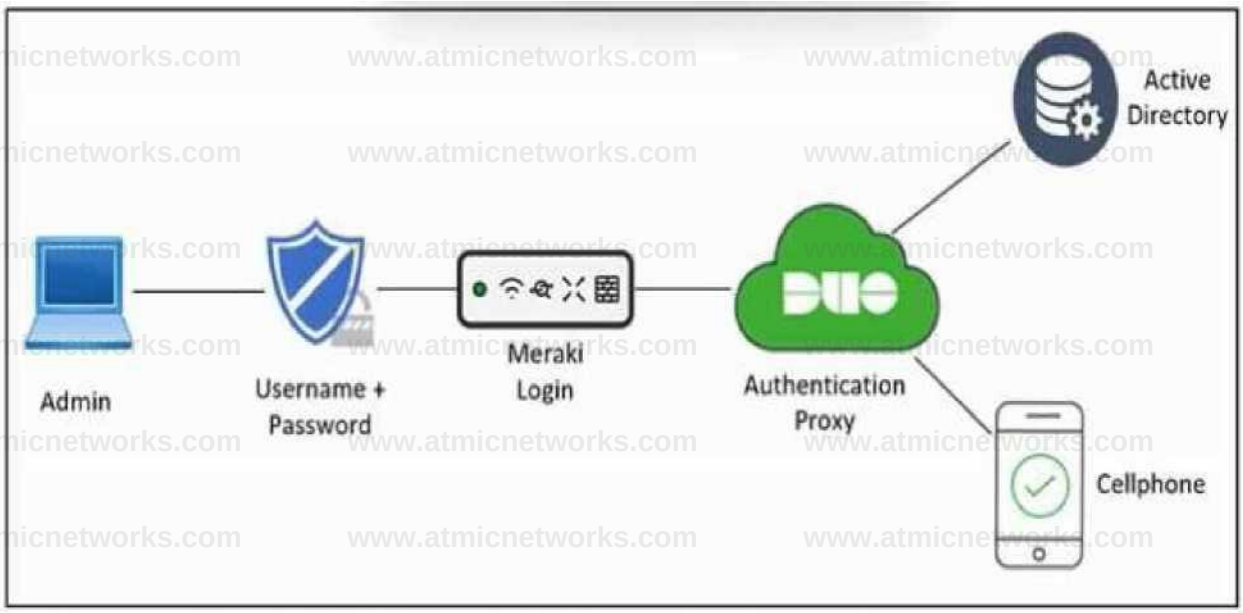
A. Performing regular data backups and testing recovery procedures
B. Keeping systems updated with the latest patches
C. Consistently maintaining up-to-date antivirus software
D. Ensuring that network traffic is closely monitored and controlled

Answer: B

Explanation:

Question: 56

DRAG DROP
Refer to the exhibit.



Refer to the exhibit. An engineer must configure multifactor authentication using the Duo Mobile app to provide admin access to a Cisco Meraki switch. The engineer already configured Duo Mobile and received an activation code. Drag and drop the steps from left to right to complete the configuration.

Answer:

Question: 57

Which web application firewall deployment in the Cisco Secure DDoS protects against application layer and volumetric attacks?

A. Hybrid
B. On-demand
C. Always-on
D. Active/passive

Answer: C

Explanation:

Question: 58

Refer to the exhibit.

Refer to the exhibit. A security engineer must configure a posture policy in Cisco ISE to ensure that employee laptops have a critical patch for WannaCry installed before they can access the network. Which posture condition must the engineer configure?

A. Patch Management Condition
B. File Condition
C. Anti-Virus Condition
D. Anti-Malware Condition

Answer: B

Explanation:

Question: 59

A network administrator uses Cisco Umbrella to protect internal users from malicious content. A customer is using an IPsec tunnel to connect to an Umbrella Organization. The administrator was informed about a zero-day vulnerability that infects user machines and uploads sensitive data through the RDP port. The administrator must ensure that no users are connected to the internet using the RDP protocol. Which Umbrella configuration must the administrator apply?

A. Web policy to block Remote Desktop Manager application type
B. Firewall policy and set port 3389 to be blocked for all outgoing traffic
C. Data loss prevention policy to block all file uploads with RDP application mime type
D. DNS policy to block Remote Desktop Manager application type

Answer: B

Explanation:

Question: 60

Refer to the exhibit.

```
"default policial": [
        I "action"; "BLOCE", "priority": IOC. "conaurer_filter_ref": "   rootscope", "tc. 'ccar_filter_ref ": "_workspacaScope" "14 Parana": *
            'proto": 6).
```

Refer to the exhibit. An engineer configured a default segmentation policy in Cisco Secure Workload to block SMTP traffic. During testing, it is observed that the SMTP traffic is still allowed. Which action must the engineer take to complete the configuration?

A. Add "port": [25, 25] to _rootScope
B. Add _SMTPScope to provider_filter_ref

C. Add "port": [25, 25] to _params
D. Change consumer_filter_ref to: _SMTPScope

Answer: C

Explanation:

Question: 61

How does Cisco XDR perform threat prioritization by using its visibility across multiple platforms?

A. By assigning priority based on the detection platform
B. By correlating detection risk and asset value at risk
C. By prioritizing threats based on their frequency across platforms
D. By using a fixed priority system for all platforms

Answer: B

Explanation: