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.

Question: 1

What are two components of the posture requirement when configuring Cisco ISE posture? (Choose two)

A. updates

B. remediation actions

C. Client Provisioning portal

D. conditions

E. access policy

Answer: B, D

Explanation:

Question: 2

What is a method for transporting security group tags throughout the network?

A. by enabling 802.1AE on every network device

B. by the Security Group Tag Exchange Protocol

C. by embedding the security group tag in the IP header

D. by embedding the security group tag in the 802.1Q header

Answer: B

Explanation:

Question: 3

Which two ports must be open between Cisco ISE and the client when you configure posture on Cisco ISE? (Choose two).

A. TCP 8443

B. TCP 8906

C. TCP 443

D. TCP 80

E. TCP 8905

Answer: A, E

Explanation:

Question: 4

Which profiling probe collects the user-agent string?

A. DHCP

B. AD

C. HTTP

D. NMAP

Answer: C

Explanation:

Question: 5

Which supplicant(s) and server(s) are capable of supporting EAP-CHAINING?

A. Cisco AnyConnect NAM and Cisco Identity Service Engine

B. Cisco AnyConnect NAM and Cisco Access Control Server

C. Cisco Secure Services Client and Cisco Access Control Server

D. Windows Native Supplicant and Cisco Identity Service Engine

Answer: A

Explanation:

Question: 6

Which two values are compared by the binary comparison (unction in authentication that is based on Active Directory?

A. subject alternative name and the common name

B. MS-CHAPv2 provided machine credentials and credentials stored in Active Directory

C. user-presented password hash and a hash stored in Active Directory

D. user-presented certificate and a certificate stored in Active Directory

Answer: A

Explanation:

Basic certificate checking does not require an identity source. If you want binary comparison checking for the certificates, you must select an identity source. If you select Active Directory as an identity source, subject and common name and subject alternative name (all values) can be used to look up a user. 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_01110.html

Question: 7

Which three default endpoint identity groups does cisco ISE create? (Choose three)

A. Unknown

B. whitelist

C. end point

D. profiled

E. blacklist

Answer: A, D , E

Explanation:

Default Endpoint Identity Groups Created for Endpoints

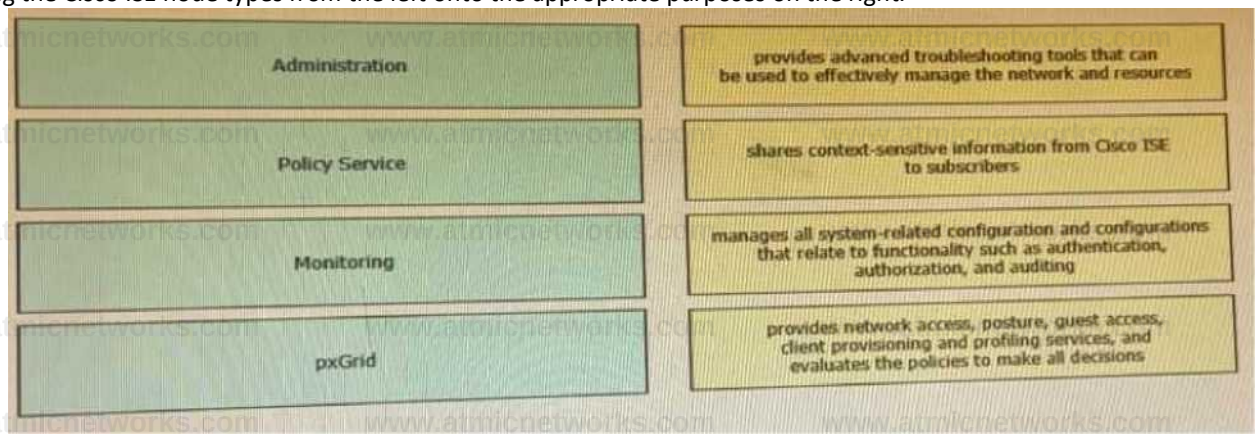
Cisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system.

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_010101.html#ID1678

Question: 8

DRAG DROP

Drag the Cisco ISE node types from the left onto the appropriate purposes on the right.



Answer:

Monitoring = provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources

Policy Service = provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Administration = manages all system-related configuration and configurations that relate to functionality such as authentication, authorization, auditing, and so on

pxGrid = shares context-sensitive information from Cisco ISE to subscribers

https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_011.html#ID57

Question: 9

Which Cisco ISE service allows an engineer to check the compliance of endpoints before connecting to the network?

A. personas

B. qualys

C. nexpose

D. posture

Answer: D

Explanation:

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_010110.html

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. This allows you to control clients to access protected areas of a network.

Question: 10

Which default endpoint identity group does an endpoint that does not match any profile in Cisco ISE become a member of?

A. Endpoint

B. unknown

C. blacklist

D. white list

E. profiled

Answer: B

Explanation:

If you do not have a matching profiling policy, you can assign an unknown profiling policy. The endpoint is therefore profiled as Unknown. The endpoint that does not match any profile is grouped within the Unknown identity group. The endpoint profiled to the Unknown profile requires that you create a profile with an attribute or a set of attributes collected for that endpoint.

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_identities.html

Question: 11

Refer to the exhibit:

```
Interface: GigabitEthernet2/0/36
MAC Address: 000e.84af.59af
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0xE0000000
Runnable methods list:
Method State
dot1x Authc Success
```

Which command is typed within the CU of a switch to view the troubleshooting output?

A. show authentication sessions mac 000e.84af.59af details

B. show authentication registrations

C. show authentication interface gigabitethemet2/0/36

D. show authentication sessions method

Answer: A

Explanation:

Question: 12

What must be configured on the Cisco ISE authentication policy for unknown MAC addresses/identities for successful authentication?

A. pass

B. reject

C. drop

D. continue

Answer: D

Explanation:

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_id_stores.html

Question: 13

Which two probes must be enabled for the ARP cache to function in the Cisco ISE profile service so that a user can reliably bind the IP address and MAC addresses of endpoints? (Choose two.)

A. NetFlow

B. SNMP

C. HTTP

D. DHCP

E. RADIUS

Answer: D, E

Explanation:
Cisco ISE implements an ARP cache in the profiling service, so that you can reliably map the IP addresses and the MAC addresses of endpoints. For the ARP cache to function, you must enable either the DHCP probe or the RADIUS probe. The DHCP and RADIUS probes carry the IP addresses and the MAC addresses of endpoints in the payload data. The dhcp-requested address attribute in the DHCP probe and the Framed-IP-address attribute in the RADIUS probe carry the IP addresses of

endpoints, along with their MAC addresses, which can be mapped and stored in the ARP cache.

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: 14

Which RADIUS attribute is used to dynamically assign the Inactivity active timer for MAB users from the Cisco ISE node?

A. session timeout

B. idle timeout

C. radius-server timeout

D. termination-action

Answer: B

Explanation:

When the inactivity timer is enabled, the switch monitors the activity from authenticated endpoints. When the inactivity timer expires, the switch removes the authenticated session. The inactivity timer for MAB can be statically configured on the switch port, or it can be dynamically assigned using the RADIUS Idle-Timeout attribute

Question: 15

What must match between Cisco ISE and the network access device to successfully authenticate endpoints?

A. SNMP version

B. shared secret

C. certificate

D. profile

Answer: B

Explanation:

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_network_devices.html

Question: 16

Which two methods should a sponsor select to create bulk guest accounts from the sponsor portal? (Choose two)

A. Random

B. Monthly

C. Daily

D. Imported

E. Known

Answer: A, D

Explanation:

Question: 17

How is policy services node redundancy achieved in a deployment?

A. by enabling VIP

B. by utilizing RADIUS server list on the NAD

C. by creating a node group

D. by deploying both primary and secondary node

Answer: C

Explanation:

Question: 18

If a user reports a device lost or stolen, which portal should be used to prevent the device from accessing the network while still providing information about why the device is blocked?

A. Client Provisioning

B. Guest

C. BYOD

D. Blacklist

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.html#90273

The Blacklist identity group is system generated and maintained by ISE to prevent access to lost or stolen devices. In this design guide, two authorization profiles are used to enforce the permissions for wireless and wired devices within the Blacklist:

Blackhole WiFi Access

Blackhole Wired Access

Question: 19

A user reports that the RADIUS accounting packets are not being seen on the Cisco ISE server.

Which command is the user missing in the switch's configuration?

A. radius-server vsa send accounting

B. aaa accounting network default start-stop group radius

C. aaa accounting resource default start-stop group radius

D. aaa accounting exec default start-stop group radios

Answer: A

Explanation:

Question: 20

What are two benefits of TACACS+ versus RADIUS for device administration? (Choose two)

A. TACACS+ supports 802.1X, and RADIUS supports MAB

B. TACACS+ uses UDP, and RADIUS uses TCP

C. TACACS+ has command authorization, and RADIUS does not.

D. TACACS+ provides the service type, and RADIUS does not

E. TACACS+ encrypts the whole payload, and RADIUS encrypts only the password.

Answer: C, E

Explanation:

Question: 21

Which two task types are included in the Cisco ISE common tasks support for TACACS+ profiles?

(Choose two.)

A. Firepower

B. WLC

C. IOS

D. ASA

E. Shell

Answer: B, E

Explanation:

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_0100010.html

TACACS+ Profile

TACACS+ profiles control the initial login session of the device administrator. A session refers to each individual authentication, authorization, or accounting request. A session authorization request to a network device elicits an ISE response. The response includes a token that is interpreted by the network device, which limits the commands that may be executed for the duration of a session. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets. The TACACS+ profile definitions are split into two components:

Common tasks

Custom attributes

There are two views in the TACACS+ Profiles page (Work Centers > Device Administration > Policy

Elements > Results > TACACS Profiles)—Task Attribute View and Raw View. Common tasks can be entered using the Task Attribute View and custom attributes can be created in the Task Attribute View as well as the Raw View.

The Common Tasks section allows you to select and configure the frequently used attributes for a profile. The attributes that are included here are those defined by the TACACS+ protocol

draft specifications. However, the values can be used in the authorization of requests from other services. In the Task Attribute View, the ISE administrator can set the privileges that will be assigned to the device administrator. The common task types are:

Shell

WLC

Nexus

Generic

The Custom Attributes section allows you to configure additional attributes. It provides a list of attributes that are not recognized by the Common Tasks section. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. In the Raw View, you can enter the mandatory attributes using a equal to (=) sign between the attribute name and its value and optional attributes are entered using an asterisk (*) between the attribute name and its value. The attributes entered in the Raw View are reflected in the Custom Attributes section in the Task Attribute View and vice versa. The Raw View is also used to copy paste the attribute list (for example, another product's attribute list) from the clipboard onto ISE. Custom attributes can be defined for nonshell services.

Question: 22

What allows an endpoint to obtain a digital certificate from Cisco ISE during a BYOD flow?

A. Network Access Control

B. My Devices Portal

C. Application Visibility and Control

D. Supplicant Provisioning Wizard

Answer: D

Explanation:

Question: 23

What occurs when a Cisco ISE distributed deployment has two nodes and the secondary node is deregistered?

A. The primary node restarts

B. The secondary node restarts.

C. The primary node becomes standalone

D. Both nodes restart.

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/1-1-1/installation_guide/ise_install_guide/ise_deploy.html

if your deployment has two nodes and you deregister the secondary node, both nodes in this primary-secondary pair are restarted. (The former primary and secondary nodes become standalone.)

Question: 24

Which port does Cisco ISE use for native supplicant provisioning of a Windows laptop?

A. TCP 8909

B. TCP 8905

C. UDP 1812

D. TCP 443

Answer: B

Explanation:

Question: 25

Which statement about configuring certificates for BYOD is true?

A. An Android endpoint uses EST, whereas other operating systems use SCEP for enrollment

B. The SAN field is populated with the end user name.

C. An endpoint certificate is mandatory for the Cisco ISE BYOD

D. The CN field is populated with the endpoint host name

Answer: C

Explanation:

Question: 26

What sends the redirect ACL that is configured in the authorization profile back to the Cisco WLC?

A. Cisco-av-pair

B. Class attribute

C. Event

D. State attribute

Answer: A

Explanation:

Question: 27

Which two events trigger a CoA for an endpoint when CoA is enabled globally for ReAuth? (Choose two.)

A. endpoint marked as lost in My Devices Portal

B. addition of endpoint to My Devices Portal

C. endpoint profile transition from Apple-Device to Apple-iPhone

D. endpoint profile transition from Unknown to Windows 10-Workstation

E. updating of endpoint dACL.

Answer: C, D

Explanation:

Question: 28

What is a requirement for Feed Service to work?

A. TCP port 3080 must be opened between Cisco ISE and the feed server

B. Cisco ISE has a base license.

C. Cisco ISE has access to an internal server to download feed update

D. Cisco ISE has Internet access to download feed update

Answer: C

Explanation:

Question: 29

Which advanced option within a WLAN must be enabled to trigger Central Web Authentication for Wireless users on AireOS controller?

A. DHCP server

B. static IP tunneling

C. override Interface ACL

D. AAA override

Answer: D

Explanation:

Question: 30

What is a valid guest portal type?

A. Sponsored-Guest

B. My Devices

C. Sponsor

D. Captive-Guest

Answer: A

Explanation:

Question: 31

What is needed to configure wireless guest access on the network?

A. endpoint already profiled in ISE

B. WEBAUTH ACL for redirection

C. valid user account in Active Directory

D. Captive Portal Bypass turned on

Answer: D

Explanation:

Question: 32

Which configuration is required in the Cisco ISE authentication policy to allow Central Web Authentication?

A. MAB and if user not found, continue

B. MAB and if authentication failed, continue

C. Dot1x and if user not found, continue

D. Dot1x and if authentication failed, continue

Answer: A

Explanation:

Question: 33

Which portal is used to customize the settings for a user to log in and download the compliance module?

A. Client Profiling

B. Client Endpoint

C. Client Provisioning

D. Client Guest

Answer: C

Explanation:

Question: 34

Which term refers to an endpoint agent that tries to join an 802 1X-enabled network?

A. EAP server
B. supplicant
C. client
D. authenticator

Answer: B

Explanation:

https://www.oreilly.com/library/view/cisco-ise-for/9780133103632/ch16.html#:~:text=What%20is%20a%20supplicant%3F,networks%2C%20both%20wired%20and%20wireless.&text=The%20802.1X%20transactions%20are,Identity%20Services%20Engine%20(ISE).

Question: 35

Which two features are available when the primary admin node is down and the secondary admin node has not been promoted? (Choose two.)

A. hotspot

B. new AD user 802 1X authentication

C. posture

D. BYOD

E. guest AUP

Answer: B, C

Explanation:

Question: 36

Which protocol must be allowed for a BYOD device to access the BYOD portal?

A. HTTP

B. SMTP

C. HTTPS

D. SSH

Answer: C

Explanation:

Question: 37

In which two ways can users and endpoints be classified for TrustSec?

(Choose Two.)

A. VLAN

B. SXP

C. dynamic

D. QoS

E. SGACL

Answer: A, E

Explanation:

Question: 38

Which two fields are available when creating an endpoint on the context visibility page of Cisco IS? (Choose two)

A. Policy Assignment

B. Endpoint Family

C. Identity Group Assignment

D. Security Group Tag

E. IP Address

Answer: A, C

Explanation:

Question: 39

When configuring Active Directory groups, what does the Cisco ISE use to resolve ambiguous group names?

A. MIB

B. TGT

C. OMAB

D. SID

Answer: D

Explanation:

Question: 40

What is the purpose of the ip http server command on a switch?

A. It enables the https server for users for web authentication

B. It enables MAB authentication on the switch

C. It enables the switch to redirect users for web authentication.

D. It enables dot1x authentication on the switch.

Answer: C

Explanation:

Question: 41

What are two requirements of generating a single signing in Cisco ISE by using a certificate provisioning portal, without generating a certificate request? (Choose two)

A. Location the CSV file for the device MAC

B. Select the certificate template

C. Choose the hashing method

D. Enter the common name

E. Enter the IP address of the device

Answer: B, D

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200534-ISE-2-0-Certificate-Provisioning-Portal.html

Question: 42

What service can be enabled on the Cisco ISE node to identity the types of devices connecting to a network?

A. MAB

B. profiling

C. posture

D. central web authentication

Answer: B

Explanation:

Question: 43

What does the dot1x system-auth-control command do?

A. causes a network access switch not to track 802.1x sessions

B. globally enables 802.1x

C. enables 802.1x on a network access device interface

D. causes a network access switch to track 802.1x sessions

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-8-0E/15-24E/configuration/guide/xe-380-configuration/dot1x.html

Question: 44

Which command displays all 802 1X/MAB sessions that are active on the switch ports of a Cisco Catalyst switch?

A. show authentication sessions output

B. Show authentication sessions

C. show authentication sessions interface Gi 1/0/x

D. show authentication sessions interface Gi1/0/x output

Answer: B

Explanation:

Question: 45

Which personas can a Cisco ISE node assume'?

A. policy service, gatekeeping, and monitoring

B. administration, policy service, and monitoring

C. administration, policy service, gatekeeping

D. administration, monitoring, and gatekeeping

Answer: B

Explanation:

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_dis_deploy.html

The persona or personas of a node determine the services provided by a node. An ISE node can assume any or all of the following personas: Administration, Policy Service, and Monitoring. The menu options that are available through the administrative user interface are dependent on the role and personas that an ISE node assumes. See Cisco ISE Nodes and Available Menu Options for more information.

Question: 46

What is a characteristic of the UDP protocol?

A. UDP can detect when a server is down.

B. UDP offers best-effort delivery

C. UDP can detect when a server is slow

D. UDP offers information about a non-existent server

Answer: B

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user- service-radius/13838-10.html

Question: 47

Which two endpoint compliance statuses are possible? (Choose two.)

A. unknown

B. known

C. invalid

D. compliant

E. valid

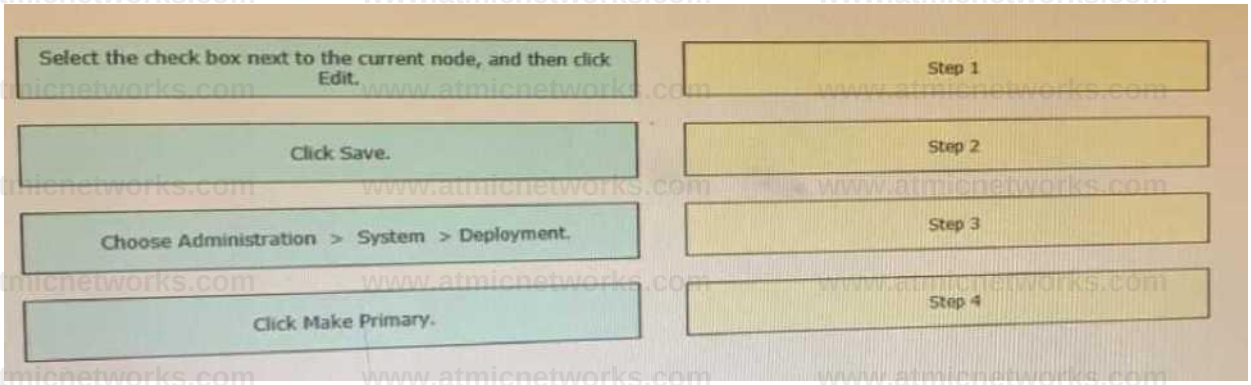
Answer: AD

Explanation:

Question: 48

DRAG DROP

Drag the steps to configure a Cisco ISE node as a primary administration node from the left into the correct order on the night.



Answer:

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_011.html

Step 1

Choose Administration > System > Deployment.

The Register button will be disabled initially. To enable this button, you must configure a Primary PAN.

Step 2

Check the check box next to the current node, and click Edit.

Step 3

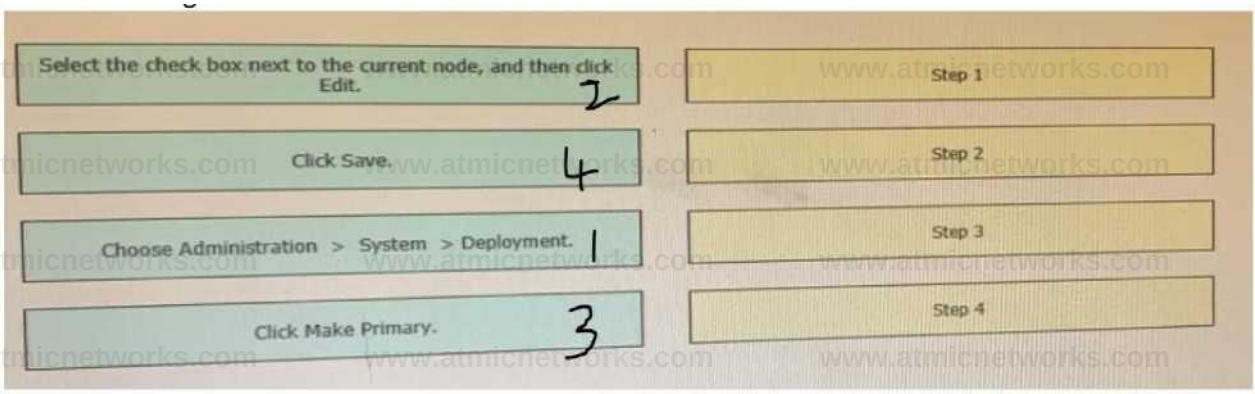
Click Make Primary to configure your Primary PAN.

Step 4

Enter data on the General Settings tab.

Step 5

Click Save to save the node configuration.



Question: 49

Which are two characteristics of TACACS+? (Choose two)

A. It uses TCP port 49.

B. It combines authorization and authentication functions.

C. It separates authorization and authentication functions.

D. It encrypts the password only.

E. It uses UDP port 49.

Answer: A, C

Explanation:

Question: 50

Which two ports do network devices typically use for CoA? (Choose two)

A. 443

B. 19005

C. 8080

D. 3799

E. 1700

Answer: D, E

Explanation:

Question: 51

Which two responses from the RADIUS server to NAS are valid during the authentication process? (Choose two)

A. access-response

B. access-request

C. access-reserved

D. access-accept

E. access-challenge

Answer: B, D

Explanation:

Question: 52

Which two components are required for creating a Native Supplicant Profile within a BYOD flow? (Choose two)

A. Windows Settings

B. Connection Type

C. iOS Settings

D. Redirect ACL

E. Operating System

Answer: B, E

Explanation:

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_010101.html#reference_21024A3B2B27427EAC78495E56962729

Question: 53

What is the minimum certainty factor when creating a profiler policy?

A. the minimum number that a predefined condition provides

B. the maximum number that a predefined condition provides

C. the minimum number that a device certainty factor must reach to become a member of the profile

D. the maximum number that a device certainty factor must reach to become a member of the profile

Answer: C

Explanation:

Question: 54

What gives Cisco ISE an option to scan endpoints for vulnerabilities?

A. authorization policy

B. authentication policy

C. authentication profile

D. authorization profile

Answer: A

Explanation:

Question: 55

A network administrator has just added a front desk receptionist account to the Cisco ISE Guest Service sponsor group. Using the Cisco ISE Guest Sponsor Portal, which guest services can the receptionist provide?

A. Keep track of guest user activities

B. Configure authorization settings for guest users

C. Create and manage guest user accounts

D. Authenticate guest users to Cisco ISE

Answer: C

Explanation:

Question: 56

Which interface-level command is needed to turn on 802 1X authentication?

A. Dofl1x pae authenticator

B. dot1x system-auth-control

C. authentication host-mode single-host

D. aaa server radius dynamic-author

Answer: A

Explanation:

Question: 57

Which permission is common to the Active Directory Join and Leave operations?

A. Create a Cisco ISE machine account in the domain if the machine account does not already exist

B. Remove the Cisco ISE machine account from the domain.

C. Set attributes on the Cisco ISE machine account

D. Search Active Directory to see if a Cisco ISE machine account already ex.sts.

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html

Question: 58

Which two features must be used on Cisco ISE to enable the TACACS. feature? (Choose two)

A. Device Administration License

B. Server Sequence

C. Command Sets

D. Enable Device Admin Service

E. External TACACS Servers

Answer: A, D

Explanation:

Question: 59

During BYOD flow, from where does a Microsoft Windows PC download the Network Setup Assistant?

A. Cisco App Store

B. Microsoft App Store

C. Cisco ISE directly

D. Native OTA functionality

Answer: C

Explanation:

Question: 60

Which use case validates a change of authorization?

A. An authenticated, wired EAP-capable endpoint is discovered

B. An endpoint profiling policy is changed for authorization policy.

C. An endpoint that is disconnected from the network is discovered

D. Endpoints are created through device registration for the guests

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_prof_pol.html

Question: 61

A network engineer is configuring a network device that needs to filter traffic based on security group tags using a security policy on a routed into this task?

A. cts authorization list

B. cts role-based enforcement

C. cts cache enable

D. cts role-based policy priority-static

Answer: B

Explanation:

Question: 62

An engineer is working with a distributed deployment of Cisco ISE and needs to configure various network probes to collect a set of attributes from the used to accomplish this task?

A. policy service

B. monitoring

C. pxGrid

D. primary policy administrator

Answer: B

Explanation:

Question: 63

An engineer is configuring Cisco ISE to reprofile endpoints based only on new requests of INIT-REBOOT and SELECTING message types. Which probe should be used to accomplish this task?

A. MMAP

B. DNS

C. DHCP

D. RADIUS

Answer: C

Explanation:

Question: 64

An engineer is using Cisco ISE and configuring guest services to allow wireless devices to access the network. Which action should accomplish this task?

A. Create the redirectACL on the WLC and add it to the WLC policy

B. Create the redirectACL on the WLC and add it to the Cisco ISE policy.

C. Create the redirectACL on Cisco ISE and add it to the WLC policy

D. Create the redirectACL on Cisco ISE and add it to the Cisco ISE Policy

Answer: B

Explanation:

Question: 65

An engineer is configuring web authentication using non-standard ports and needs the switch to redirect traffic to the correct port. Which command should be used to accomplish this task?

A. permit tcp any any eq <port number>

B. aaa group server radius proxy

C. ip http port <port number>

D. aaa group server radius

Answer: C

Explanation:

Question: 64

An administrator needs to connect ISE to Active Directory as an external authentication source and allow the proper ports through the firewall. Which two ports should be opened to accomplish this task? (Choose two)

A. TELNET 23

B. LDAP 389

C. HTTP 80

D. HTTPS 443

E. MSRPC 445

Answer: B, E

Explanation:

Question: 67

Refer to the exhibit.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authorization network default group radius
```

A network engineers configuring the switch to accept downloadable ACLs from a Cisco ISC server Which two commands should be run to complete the configuration? (Choose two)

A. aaa authorization auth-proxy default group radius

B. radius server vsa sand authentication

C. radius-server attribute 8 include-in-access-req

D. ip device tracking

E. dot1x system-auth-control

Answer: B, C

Explanation:

Question: 68

An engineer is using the low-impact mode for a phased deployment of Cisco ISE and is trying to connect to the network prior to authentication. Which access will be denied in this?

A. HTTP

B. DNS

C. EAP

E. DHCP

Answer: A

Explanation:

Question: 69

A network engineer needs to ensure that the access credentials are not exposed during the 802.1x authentication among components. Which two protocols should complete this task?

A. PEAP

B. EAP-MD5

C. LEAP

D. EAP-TLS

E. EAP-TTLS

Answer: B, D

Explanation:

Question: 70

An engineer is configuring a guest password policy and needs to ensure that the password complexity requirements are set to mitigate brute force attacks. Which two requirement complete this policy? (Choose two)

A. minimum password length

B. active username limit

C. access code control

D. gpassword expiration period

E. username expiration date

Answer: A, D

Explanation:

Question: 71

Which two actions occur when a Cisco ISE server device administrator logs in to a device? (Choose two)

A. The device queries the internal identity store

B. The Cisco ISE server queries the internal identity store

C. The device queries the external identity store

D. The Cisco ISE server queries the external identity store.

E. The device queries the Cisco ISE authorization server

Answer: A, D

Explanation:

Question: 72

When planning for the deployment of Cisco ISE, an organization's security policy dictates that they must use network access authentication via RADIUS. It also states that the deployment provide an adequate amount of security and visibility for the hosts on the network. Why should the engineer configure MAB in this situation?

A. The Cisco switches only support MAB.

B. MAB provides the strongest form of authentication available.

C. The devices in the network do not have a supplicant.

D. MAB provides user authentication.

Answer: C

Explanation:

Question: 73

In a Cisco ISE split deployment model, which load is split between the nodes?

A. AAA

B. network admission

C. log collection

D. device admission

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2- 6/install_guide/b_ise_InstallationGuide26.pdf

Question: 74

An engineer is implementing Cisco ISE and needs to configure 802.1X. The port settings are configured for port-based authentication. Which command should be used to complete this configuration?

A. dot1x pae authenticator

B. dot1x system-auth-control

C. authentication port-control auto

D. aaa authentication dot1x default group radius

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/configuration/guide/conf/dot1x.html#wp1133395

Question: 75

Which two default endpoint identity groups does Cisco ISE create? (Choose two)

A. block list

B. endpoint

C. profiled

D. allow list

E. unknown

Answer: C, E

Explanation:

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

Default Endpoint Identity Groups Created for Endpoints

Cisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system.

Cisco ISE creates the following endpoint identity groups:

Blacklist—This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are block listed in the device registration portal. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.

GuestEndpoints—This endpoint identity group includes endpoints that are used by guest users.

Profiled—This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations in Cisco ISE.

RegisteredDevices—This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list. You can edit, delete, and block these devices that you added through the device registration portal from the endpoints list in the Endpoints page in Cisco ISE. Devices that you have blocked in the device registration portal are assigned to the Blacklist endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blocked devices to a URL, which displays "Unauthorised Network Access", a default portal page to the blocked devices.

Unknown—This endpoint identity group includes endpoints that do not match any profile in Cisco ISE.

In addition to the above system created endpoint identity groups, Cisco ISE creates the following endpoint identity groups, which are associated to the Profiled identity group:

Cisco-IP-Phone—An identity group that contains all the profiled Cisco IP phones on your network.

Workstation—An identity group that contains all the profiled workstations on your network.

Question: 76

In a standalone Cisco ISE deployment, which two personas are configured on a node? (Choose two)

A. publisher

B. administration

C. primary

D. policy service

E. subscriber

Answer: B, D

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_010.html

Question: 77

What happens when an internal user is configured with an external identity store for authentication, but an engineer uses the Cisco ISE admin portal to select an internal identity store as the identity source?

A. Authentication is redirected to the internal identity source.

B. Authentication is redirected to the external identity source.

C. Authentication is granted.

D. Authentication fails.

Answer: D

Explanation:

Question: 78

An engineer is configuring web authentication and needs to allow specific protocols to permit DNS traffic. Which type of access list should be used for this configuration?

A. reflexive ACL

B. extended ACL

C. standard ACL

D. numbered ACL

Answer: B

Explanation:

Question: 79

Which two features should be used on Cisco ISE to enable the TACACS+ feature? (Choose two)

A. External TACACS Servers

B. Device Admin Service

C. Device Administration License

D. Server Sequence

E. Command Sets

Answer: B, C

Explanation:

Question: 80

A network engineer must enforce access control using special tags, without re-engineering the network design. Which feature should be configured to achieve this in a scalable manner?

A. SGT

B. dACL

C. VLAN

D. RBAC

Answer: A

Explanation:

Question: 81

An engineer is configuring a virtual Cisco ISE deployment and needs each persona to be on a different node. Which persona should be configured with the largest amount of storage in this environment?

A. policy Services

B. Primary Administration

C. Monitoring and Troubleshooting

D. Platform Exchange Grid

Answer: C

Explanation:

Question: 82

An engineer is configuring Cisco ISE and needs to dynamically identify the network endpoints and ensure that endpoint access is protected. Which service should be used to accomplish this task?

Profiling

Guest access

Client provisioning

Posture

Answer: A

Explanation:

Question: 83

What should be considered when configuring certificates for BYOD?

An endpoint certificate is mandatory for the Cisco ISE BYOD

An Android endpoint uses EST whereas other operation systems use SCEP for enrollment

The CN field is populated with the endpoint host name.

The SAN field is populated with the end user name

Answer: A

Explanation:

Question: 84

A policy is being created in order to provide device administration access to the switches on a network. There is a requirement to ensure that if the session is not actively being used, after 10 minutes, it will be disconnected. Which task must be configured in order to meet this requirement?

A. session timeout

B. idle time

C. monitor

D. set attribute as

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_admin_accesspolicy_settings.html#reference_0E24B8FBFAB248219E1194435670347F

Question: 85

An administrator is attempting to replace the built-in self-signed certificates on a Cisco ISE appliance. The CA is requesting some information about the appliance in order to sign the new certificate. What must be done in order to provide the CA this information?

A. Install the Root CA and intermediate CA.

B. Generate the CSR.

C. Download the intermediate server certificate.

D. Download the CA server certificate.

Answer: B

Explanation:

Question: 86

An organization is hosting a conference and must make guest accounts for several of the speakers attending. The conference ended two days early but the guest accounts are still being used to access the network. What must be configured to correct this?

A. Create an authorization rule denying sponsored guest access.

B. Navigate to the Guest Portal and delete the guest accounts.

C. Create an authorization rule denying guest access.

D. Navigate to the Sponsor Portal and suspend the guest accounts.

Answer: D

Explanation:

Question: 87

An administrator is configuring posture with Cisco ISE and wants to check that specific services are present on the workstations that are attempting to access the network. What must be configured to accomplish this goal?

A. Create a registry posture condition using a non-OPSWAT API version.

B. Create an application posture condition using a OPSWAT API version.

C. Create a compound posture condition using a OPSWAT API version.

D. Create a service posture condition using a non-OPSWAT API version.

Answer: D

Explanation:

Question: 88

An engineer is configuring 802.1X and wants it to be transparent from the users' point of view. The implementation should provide open authentication on the switch ports while providing strong levels of security for non-authenticated devices. Which deployment mode should be used to achieve this?

A. closed

B. low-impact

C. open

D. high-impact

Answer: B

Explanation:

https://www.lookingpoint.com/blog/cisco-ise-wired-802.1x-deployment-monitormode#:~:text=Low%20impact%20mode%20works%20similar,DHCP%2C%20PXE%20boot%2C%20etc.

Question: 89

What is the deployment mode when two Cisco ISE nodes are configured in an environment?

A. distributed

B. active

C. standalone

D. standard

Answer: A

Explanation:

Question: 90

Which two roles are taken on by the administration person within a Cisco ISE distributed environment? (Choose two.)

A. backup

B. secondary

C. standby

D. primary

E. active

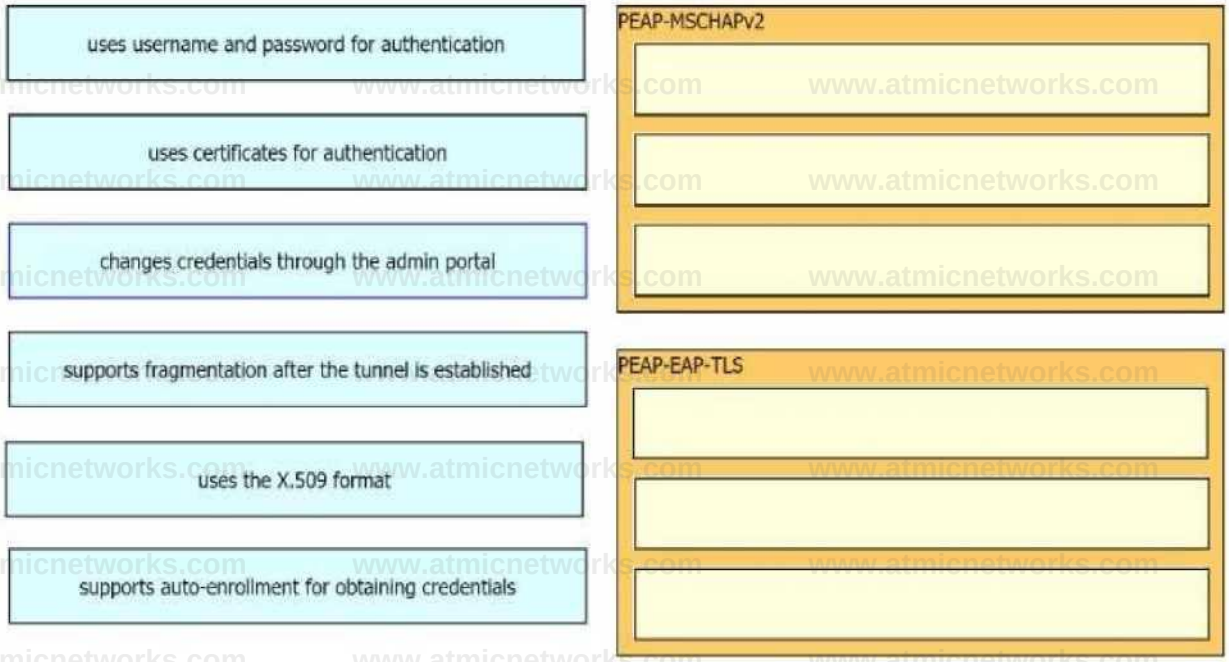
Answer: B, D

Explanation:

Question: 91

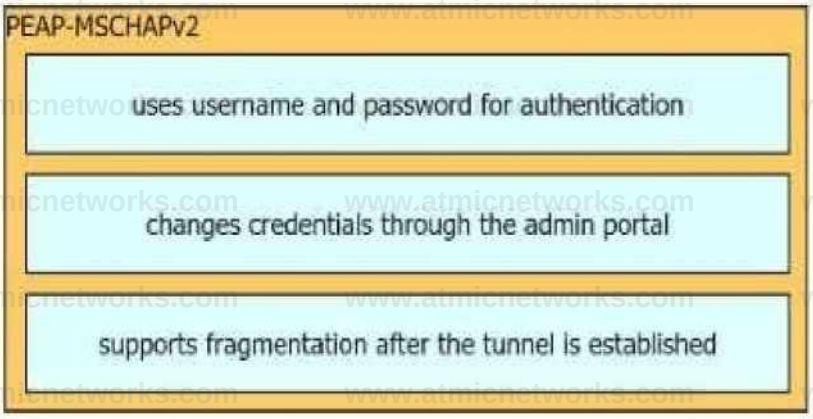
DRAG DROP

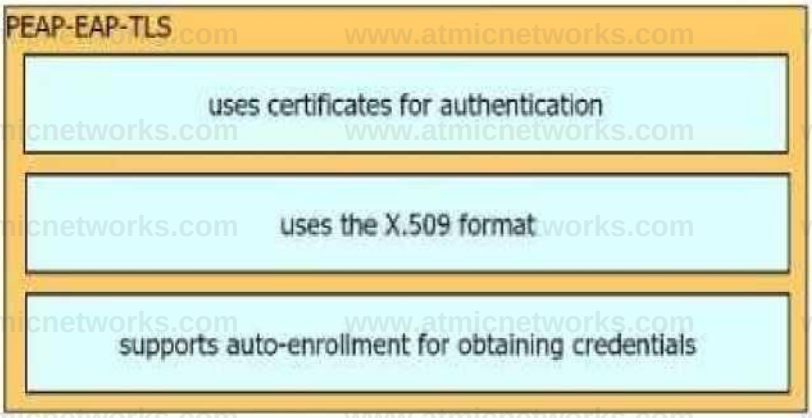
An organization wants to implement 802.1X and is debating whether to use PEAP-MSCHAPv2 or PEAP-EAP-TLS for authentication. Drag the characteristics on the left to the corresponding protocol on the right.



Answer:

Explanation:





Question:
92

A company is attempting to improve their BYOD policies and restrict access based on certain criteri

a. The company's subnets are organized by building. Which attribute should be used in order to gain access based on location?

A. static group assignment

B. IP address

C. device registration status

D. MAC address

Answer: A

Explanation:

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#ID1353

Question: 93

An engineer is migrating users from MAB to 802.1X on the network. This must be done during normal business hours with minimal impact to users. Which CoA method should be used?

A. Port Bounce

B. Port Shutdown

C. Session Termination

D. Session Reauthentication

Answer: D

Explanation:

Question: 94

What must be configured on the WLC to configure Central Web Authentication using Cisco ISE and a WLC?

A. Set the NAC State option to SNMP NAC.

B. Set the NAC State option to RADIUS NAC.

C. Use the radius-server vsa send authentication command.

D. Use the ip access-group webauth in command.

Answer: B

Explanation:

Question: 95

Refer to the exhibit.

An organization recently implemented network device administration using Cisco ISE. Upon testing the ability to access all of the required devices, a user in the Cisco ISE group IT Admins is attempting to login to a device in their organization's finance department but is unable to. What is the problem?

A. The IT training rule is taking precedence over the IT Admins rule.

B. The authorization conditions wrongly allow IT Admins group no access to finance devices.

C. The finance location is not a condition in the policy set.

D. The authorization policy doesn't correctly grant them access to the finance devices.

Answer: D

Explanation:

Question: 96

When creating a policy within Cisco ISE for network access control, the administrator wants to allow different access restrictions based upon the wireless SSID to which the device is connecting. Which policy condition must be used in order to accomplish this?

A. Network Access NetworkDeviceName CONTAINS <SSID Name>

B. DEVICE Device Type CONTAINS <SSID Name>

C. Radius Called-Station-ID CONTAINS <SSID Name>

D. Airespace Airespace-Wlan-Id CONTAINS <SSID Name>

Answer: C

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115734-ise-policies- ssid-00.html

Question: 97

There is a need within an organization for a new policy to be created in Cisco ISE. It must validate that a specific anti-virus application is not only installed, but running on a machine before it is allowed access to the network. Which posture condition should the administrator configure in order for this policy to work?

A. file

B. registry

C. application

D. service

Answer: C

Explanation:

Question: 98

An organization wants to improve their BYOD processes to have Cisco ISE issue certificates to the BYOD endpoints. Currently, they have an active certificate authority and do not want to replace it with Cisco ISE. What must be configured within Cisco ISE to accomplish this goal?

A. Create a certificate signing request and have the root certificate authority sign it.

B. Add the root certificate authority to the trust store and enable it for authentication.

C. Create an SCEP profile to link Cisco ISE with the root certificate authority.

D. Add an OCSP profile and configure the root certificate authority as secondary.

Answer: C

Explanation:

Ref:https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine- software/116068-configure-product-00.html

Question: 99

An administrator is adding network devices for a new medical building into Cisco ISE. These devices must be in a network device group that is identifying them as "Medical Switch" so that the policies can be made

separately for the endpoints connecting through them. Which configuration item must be changed in the network device within Cisco ISE to accomplish this goal?

A. Change the device type to Medical Switch.

B. Change the device profile to Medical Switch.

C. Change the model name to Medical Switch.

D. Change the device location to Medical Switch.

Answer: A

Explanation:

Question: 100

An engineer is designing a new distributed deployment for Cisco ISE in the network and is considering failover options for the admin nodes. There is a need to ensure that an admin node is available for configuration of policies at all times. What is the requirement to enable this feature?

A. one primary admin and one secondary admin node in the deployment

B. one policy services node and one secondary admin node

C. one policy services node and one monitoring and troubleshooting node

D. one primary admin node and one monitoring and troubleshooting node

Answer: A

Explanation:

Question: 101

A company manager is hosting a conference. Conference participants must connect to an open guest SSID and only use a preassigned code that they enter into the guest portal prior to gaining access to the network. How should the manager configure Cisco ISE to accomplish this goal?

A. Create entries in the guest identity group for all participants.

B. Create an access code to be entered in the AUP page.

C. Create logins for each participant to give them sponsored access.

D. Create a registration code to be entered on the portal splash page.

Answer: B

Explanation:

Question: 102

A network security engineer needs to configure 802.1X port authentication to allow a single host to be authenticated for data and another single host to be authenticated for voice. Which command should the engineer run on the interface to accomplish this goal?

A. authentication host-mode single-host

B. authentication host-mode multi-auth

C. authentication host-mode multi-host

D. authentication host-mode multi-domain

Answer: D

Explanation:

Question: 103

When setting up profiling in an environment using Cisco ISE for network access control, an organization must use non-proprietary protocols for collecting the information at layer 2. Which two probes will provide this information without forwarding SPAN packets to Cisco ISE? {Choose two.)

A. DHCP SPAN probe

B. SNMP query probe

C. NetFlow probe

D. RADIUS probe

E. DNS probe

Answer: BD

Explanation:

https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-design

Question: 104

What is a function of client provisioning?

A. Client provisioning ensures that endpoints receive the appropriate posture agents.

B. Client provisioning checks a dictionary attribute with a value.

C. Client provisioning ensures an application process is running on the endpoint.

D. Client provisioning checks the existence, date, and versions of the file on a client.

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_client_prov.html#:~:text=After%20Cisco%20ISE%20classifies%20a,packages%20and%20profiles%2C%20if%20necessary.

Question: 105

An engineer is testing Cisco ISE policies in a lab environment with no support for a deployment server. In order to push supplicant profiles to the workstations for testing, firewall ports will need to be opened. From which Cisco ISE persona should this traffic be originating?

A. monitoring

B. policy service

C. administration

D. authentication

Answer: B

Explanation:

Question: 106

What is an advantage of using EAP-TLS over EAP-MS-CHAPv2 for client authentication?

A. EAP-TLS uses a username and password for authentication to enhance security, while EAP-MS-CHAPv2 does not.

B. EAP-TLS secures the exchange of credentials, while EAP-MS-CHAPv2 does not.

C. EAP-TLS uses a device certificate for authentication to enhance security, while EAP-MS-CHAPv2 does not.

D. EAP-TLS uses multiple forms of authentication, while EAP-MS-CHAPv2 only uses one.

Answer: C

Explanation:

Question: 107

There are several devices on a network that are considered critical and need to be placed into the ISE database and a policy used for them. The organization does not want to use profiling. What must be done to accomplish this goal?

A. Enter the MAC address in the correct Endpoint Identity Group.

B. Enter the MAC address in the correct Logical Profile.

C. Enter the IP address in the correct Logical Profile.

D. Enter the IP address in the correct Endpoint Identity Group.

Answer: A

Explanation:

Question: 108

An engineer is tasked with placing a guest access anchor controller in the DMZ. Which two ports or port sets must be opened up on the firewall to accomplish this task? (Choose two.)

A. UDP port 1812 RADIUS

B. TCP port 161

C. TCP port 514

D. UDP port 79

E. UDP port 16666

Answer: B, C

Explanation:

Question: 109

A network administrator is configuring authorization policies on Cisco ISE There is a requirement to use AD group assignments to control access to network resources After a recent power failure and Cisco ISE rebooting itself, the AD group assignments no longer work What is the cause of this issue?

A. The AD join point is no longer connected.

B. The AD DNS response is slow.

C. The certificate checks are not being conducted.

D. The network devices ports are shut down.

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/ise_active_directory_integration/b_ISE_AD_integration_2x.html#ID612

Question: 110

An administrator is adding a switch to a network that is running Cisco ISE and is only for IP Phones The phones do not have the ability to authenticate via 802 1X Which command is needed on each switch port for authentication?

A. dot1x system-auth-control

B. enable bypass-mac

C. enable network-authentication

D. mab

Answer: D

Explanation:

https://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-2mt/sec-config- mab.html

Question: 111

A network administrator is setting up wireless guest access and has been unsuccessful in testing client access. The endpoint is able to connect to the SSID but is unable to grant access to the guest network through the guest portal. What must be done to identify the problem?

A. Use context visibility to verify posture status.

B. Use the endpoint ID to execute a session trace.

C. Use the identity group to validate the authorization rules.

D. Use traceroute to ensure connectivity.

Answer: B

Explanation:

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_011001.html#concept87916A77E8774545B36D0BB422429596

Question: 112

An administrator is configuring new probes to use with Cisco ISE and wants to use metadata to help

profile the endpoints. The metadata must contain traffic information relating to the endpoints instead of industry-standard protocol information Which probe should be enabled to meet these requirements?

A. NetFlow probe

B. DNS probe

C. DHCP probe

D. SNMP query probe

Answer: C

Explanation:

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

Question: 113

An organization wants to standardize the 802 1X configuration on their switches and remove static

ACLs on the switch ports while allowing Cisco ISE to communicate to the switch what access to provide What must be configured to accomplish this task?

A. security group tag within the authorization policy

B. extended access-list on the switch for the client

C. port security on the switch based on the client's information

D. dynamic access list within the authorization profile

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_sga_pol.html#

Question: 114

A network engineer is configuring guest access and notices that when a guest user registers a second device for access, the first device loses access What must be done to ensure that both devices for a particular user are able to access the guest network simultaneously?

A. Configure the sponsor group to increase the number of logins.

B. Use a custom portal to increase the number of logins

C. Modify the guest type to increase the number of maximum devices

D. Create an Adaptive Network Control policy to increase the number of devices

Answer: C

Explanation:

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-7/admin_guide/b_ise_admin_guide_27/b_ise_admin_guide_27_chapter_01111.html.xml

Question: 115

An organization is implementing Cisco ISE posture services and must ensure that a host-based firewall is in place on every Windows and Mac computer that attempts to access the network They have multiple vendors' firewall applications for their devices, so the engineers creating the policies are unable to use a specific application check in order to validate the posture for this What should be done to enable this type of posture check?

A. Use the file registry condition to ensure that the firewal is installed and running appropriately.

B. Use a compound condition to look for the Windows or Mac native firewall applications.

C. Enable the default firewall condition to check for any vendor firewall application.

D. Enable the default application condition to identify the applications installed and validade the firewall app.

Answer: C

Explanation:

https://www.youtube.com/watch?v=6Kj8P8Hn7dY&t=109s&ab_channel=CiscoISE- IdentityServicesEngine

Question: 116

An administrator is configuring TACACS+ on a Cisco switch but cannot authenticate users with Cisco ISE. The configuration contains the correct key of Cisc039712287. but the switch is not receiving a response from the Cisco ISE instance What must be done to validate the AAA configuration and identify the problem with the TACACS+ servers?

A. Check for server reachability using the test aaa group tacacs+ admin <key> legacy command.

B. Test the user account on the server using the test aaa group radius server CUCS user admin pass <key> legacy command.

C. Validate that the key value is correct using the test aaa authentication admin <key> legacy command.

D. Confirm the authorization policies are correct using the test aaa authorization admin drop legacy command.

Answer: A

Explanation:

https://medium.com/training-course-ccna-security-210-260/ccna-security-part-3-implementing-aaa- in-cisco-ios-4b13ab285f51

Question: 117

Refer to the exhibit

```
Switch (config)# gigabitEthernet 1/0/2
Switch (config)# authentication port-control auto
Switch(config)# authentication host-modemulti-auth
```

Refer to the exhibit. In which scenario does this switch configuration apply?

A. when allowing a hub with multiple clients connected

B. when passing IP phone authentication

C. when allowing multiple IP phones to be connected

D. when preventing users with hypervisor

Answer: A

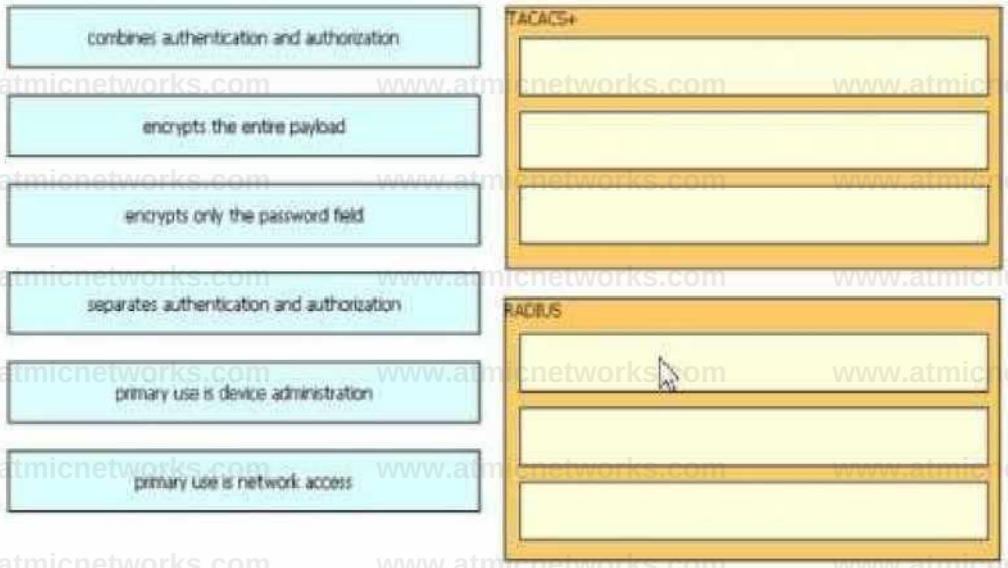
Explanation:

https://www.linkedin.com/pulse/mac-authentication-bypass-priyanka-kumari#:~:text=Multi%2Dauthentication%20host%20mode%3A%20You,allows%20multiple%20source%20MAC%20addresses.

Question: 118

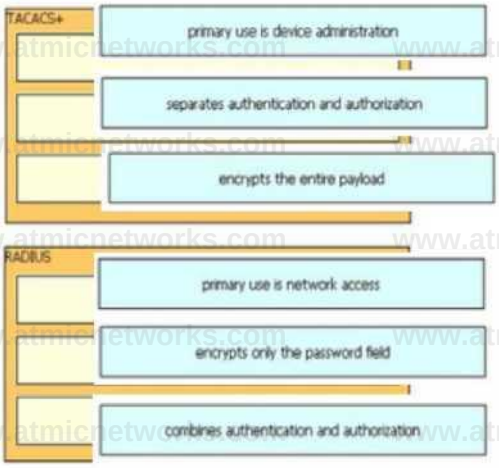
DRAG DROP

Drag and drop the description from the left onto the protocol on the right that is used to carry out system authentication, authentication, and accounting.



Answer:

Explanation:



https://www.mbne.net/tech-notes/aaa-tacacs-radius

Question: 119

When configuring an authorization policy, an administrator cannot see specific Active Directory groups present in their domain to be used as a policy condition. However, other groups that are in the same domain are seen What is causing this issue?

A. Cisco ISE only sees the built-in groups, not user created ones

B. The groups are present but need to be manually typed as conditions

C. Cisco ISE's connection to the AD join point is failing

D. The groups are not added to Cisco ISE under the AD join point

Answer: D

Explanation:

https://www.youtube.com/watch?v=0kuEZEo564s&ab_channel=CiscoISE-IdentityServicesEngine

Question: 120

A network administrator changed a Cisco ISE deployment from pilot to production and noticed that the JVM memory utilization increased significantly. The administrator suspects this is due to replication between the nodes What must be configured to minimize performance degradation?

A. Review the profiling policies for any misconfiguration

B. Enable the endpoint attribute filter

C. Change the reauthenticate interval.

D. Ensure that Cisco ISE is updated with the latest profiler feed update

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/admin_guide/b_ise_admin_guide_23/b_ise_admin_guide_23_chapter_010111.html

Question: 121

An engineer is designing a BYOD environment utilizing Cisco ISE for devices that do not support native supplicants Which portal must the security engineer configure to accomplish this task?

A. MDM

B. Client provisioning

C. My devices

D. BYOD

Answer: C

Explanation:

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_01111.html

Question: 122

A Cisco ISE administrator needs to ensure that guest endpoint registrations are only valid for one day When testing the guest policy flow, the administrator sees that the Cisco ISE does not delete the endpoint in the Guest Endpoints identity store after one day and allows access to the guest network after that period. Which configuration is causing this problem?

A. The Endpoint Purge Policy is set to 30 days for guest devices

B. The RADIUS policy set for guest access is set to allow repeated authentication of the same device

C. The length of access is set to 7 days in the Guest Portal Settings

D. The Guest Account Purge Policy is set to 15 days

Answer: A

Explanation:

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_01101.html#:~:text=Cisco%20ISE%2C%20by%20default%2C%20deletes,5000%20endpoints%20every%20three%20minute s.

Question: 123

A network engineer is configuring Cisco TrustSec and needs to ensure that the Security Group Tag is being transmitted between two devices Where in the Layer 2 frame should this be verified?

A. CMD filed

B. 802.1Q filed

C. Payload

D. 802.1 AE header

Answer: A

Explanation:

https://www.cisco.com/c/dam/global/en_ca/assets/ciscoconnect/2014/pdfs/policy_defined_segmentation_with_trustsec_rob_bleeker.pdf (slide 25)

Question: 124

A Cisco ISE server sends a CoA to a NAD after a user logs in successfully using CWA Which action does the CoA perform?

A. It terminates the client session

B. It applies the downloadable ACL provided in the CoA

C. It applies new permissions provided in the CoA to the client session.

D. It triggers the NAD to reauthenticate the client

Answer: B

Explanation:
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/113362-config-web- auth-ise-00.html

Question: 125

A customer wants to set up the Sponsor portal and delegate the authentication flow to a third party for added security while using Kerberos Which database should be used to accomplish this goal?

A. RSA Token Server

B. Active Directory

C. Local Database

D. LDAP

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_01111.html#concept_srz_bkb_4db

Question: 126

An administrator is configuring a Cisco ISE posture agent in the client provisioning policy and needs to ensure that the posture policies that interact with clients are monitored, and end users are required to comply with network usage rules Which two resources must be added in Cisco ISE to accomplish this goal? (Choose two)

A. AnyConnect

B. Supplicant

C. Cisco ISE NAC

D. PEAP

E. Posture Agent

Answer: AE

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/configure-posture.html

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_configure_client_provisioning.html#task_D1C2E8ECE1D54D259C01BCBF0A5822F1

Question: 127

Refer to the exhibit

```
interface GtgabrtEthernell/0/1 authentication host mode multi auth authentication post-control auto mab
  dot lx pee authenticator
```

Which switch configuration change will allow only one voice and one data endpoint on each port?

A. Multi-auth to multi-domain

B. Mab to dot1x

C. Auto to manual

D. Multi-auth to single-auth

Answer: A

Explanation:

https://community.cisco.com/t5/network-access-control/cisco-ise-multi-auth-or-multi-host/m- p/3750907

Question: 128

An administrator needs to give the same level of access to the network devices when users are logging into them using TACACS+ However, the administrator must restrict certain commands based on one of three user roles that require different commands How is this accomplished without creating too many objects using Cisco ISE?

A. Create one shell profile and multiple command sets.

B. Create multiple shell profiles and multiple command sets.

C. Create one shell profile and one command set.

D. Create multiple shell profiles and one command set

Answer: A

Explanation:

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_0100010.html

https://www.youtube.com/watch?v=IlZwB71Szog&ab_channel=JasonMaynard

Question: 129

An administrator for a small network is configuring Cisco ISE to provide dynamic network access to users. Management needs Cisco ISE to not automatically trigger a CoA whenever a profile change is detected. Instead, the administrator needs to verify the new profile and manually trigger a Co

A. What must be configuring in the profiler to accomplish this goal?

A. Port Bounce

B. No CoA

C. Session Query

D. Reauth

Answer: B

Explanation:

https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-policies

Question: 130

An organization wants to split their Cisco ISE deployment to separate the device administration functionalities from the mam deployment. For this to work, the administrator must deregister any nodes that will become a part of the new deployment, but the button for this option is grayed out Which configuration is causing this behavior?

A. One of the nodes is an active PSN.

B. One of the nodes is the Primary PAN

C. All of the nodes participate in the PAN auto failover.

D. All of the nodes are actively being synched.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/b_ise_27_admin_guide/b_ISE_admin_27_deployment.html#ID185

Question: 131

An organization is adding new profiling probes to the system to improve profiling on Oseo ISE The probes must support a common network management protocol to receive information about the endpoints and the ports to which they are connected What must be configured on the network device to accomplish this goal?

A. ARP

B. SNMP

C. WCCP

D. ICMP

Answer: B

Explanation:

https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456#toc-hId-790343135

Question: 132

A network administrator is configuring a secondary cisco ISE node from the backup configuration of the primary cisco ISE node to create a high availability pair The Cisco ISE CA certificates and keys must be manually backed up from the primary Cisco ISE and copied into the secondary Cisco ISE Which command most be issued for this to work?

A. copy certificate Ise

B. application configure Ise

C. certificate configure Ise

D. Import certificate Ise

Answer: B

Explanation:

https://community.cisco.com/t5/network-access-control/ise-certificate-import-export/m-p/3847746

Question: 133

An employee logs on to the My Devices portal and marks a currently on-boarded device as 'Lost'.

Which two actions occur within Cisco ISE as a result oí this action? (Choose two)

A. Certificates provisioned to the device are not revoked

B. BYOD Registration status is updated to No

C. The device access has been denied

D. BYOD Registration status is updated to Unknown.

E. The device status is updated to Stolen

Answer: AB

Explanation:

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_01111.html

Question: 134

An administrator connects an HP printer to a dot1x enable port, but the printer in not accessible Which feature must the administrator enable to access the printer?

A. MAC authentication bypass

B. change of authorization

C. TACACS authentication

D. RADIUS authentication

Answer: A

Explanation:

https://community.cisco.com/t5/network-access-control/ise-for-printer-security/m-p/3933216

Question: 135

A new employee just connected their workstation to a Cisco IP phone. The network administrator wants to ensure that the Cisco IP phone remains online when the user disconnects their Workstation from the corporate network Which CoA configuration meets this requirement?

A. Port Bounce

B. Reauth

C. NoCoA

D. Disconnect

Answer: C

Explanation:

https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-design

Question: 136

A network administrator must use Cisco ISE to check whether endpoints have the correct version of antivirus installed Which action must be taken to allow this capability?

A. Configure a native supplicant profile to be used for checking the antivirus version

B. Configure Cisco ISE to push the HostScan package to the endpoints to check for the antivirus version.

C. Create a Cisco AnyConnect Network Visibility Module configuration profile to send the antivirus information of the endpoints to Cisco ISE.

D. Create a Cisco AnyConnect configuration within Cisco ISE for the Compliance Module and associated configuration files

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_client_prov.html

About Anyconnect Network Visibility Module

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect45/administration/guide/b_AnyConnect_Administrator_Guide_4-5/nvm.html

Question: 137

A network administrator must configura endpoints using an 802 1X authentication method with EAP identity certificates that are provided by the Cisco ISE When the endpoint presents the identity certificate to Cisco ISE to validate the certificate, endpoints must be authorized to connect to the network Which EAP type must be configured by the network administrator to complete this task?

A. EAP-PEAP-MSCHAPv2

B. EAP-TTLS

C. EAP-FAST

D. EAP-TLS

Answer: D

Explanation:

https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/certificate- requirements-eap-tls-peap

about EAP FAST

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/eap-fast/200322-Understanding- EAP-FAST-and-Chaining-imp.html

Question: 138

Refer to the exhibit. An engineer is creating a new TACACS* command set and cannot use any show commands after togging into the device with this command set authorization Which configuration is causing this issue?

A. Question marks are not allowed as wildcards for command sets.

B. The command set is allowing all commands that are not in the command list

C. The wildcard command listed is in the wrong format

D. The command set is working like an ACL and denying every command.

Answer: A

Explanation:

Question: 139

An organization is migrating its current guest network to Cisco ISE and has 1000 guest users in the current database There are no resources to enter this information into the Cisco ISE database manually. What must be done to accomplish this task effciently?

A. Use a CSV file to import the guest accounts

B. Use SOL to link me existing database to Ctsco ISE

C. Use a JSON fie to automate the migration of guest accounts

D. Use an XML file to change the existing format to match that of Cisco ISE

Answer: A

Explanation:

Question: 140

MacOS users are complaining about having to read through wordy instructions when remediating their workstations to gam access to the network Which alternate method should be used to tell users how to remediate?

A. URL link

B. message text

C. executable

D. file distribution

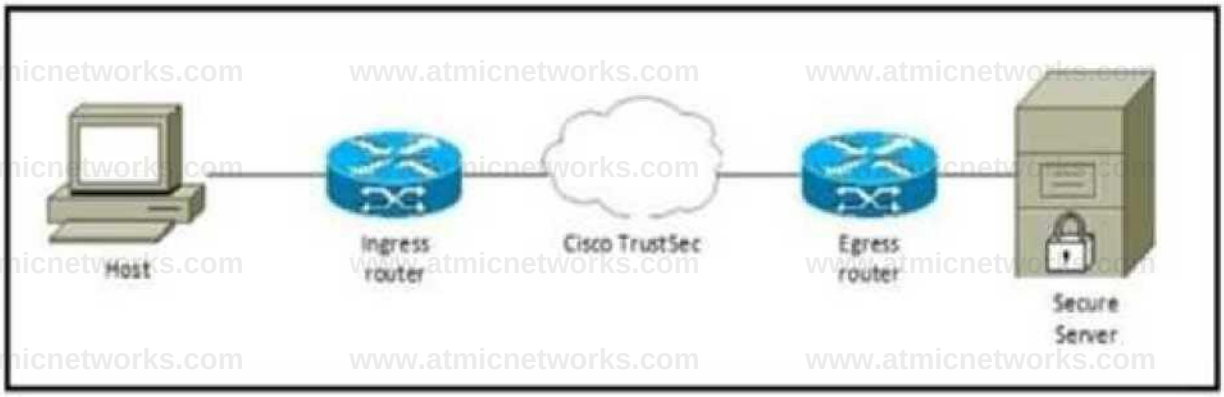
Answer: A

Explanation:

https://www.sciencedirect.com/topics/computer-science/remediation-action

Question: 141

Refer to the exhibit.



Refer to the exhibit Which component must be configured to apply the SGACL?

A. egress router

B. host

C. secure server

D. ingress router

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html#52796

Question: 142

What does a fully distributed Cisco ISE deployment include?

A. PAN and PSN on the same node while MnTs are on their own dedicated nodes.

B. PAN and MnT on the same node while PSNs are on their own dedicated nodes.

C. All Cisco ISE personas on their own dedicated nodes.

D. All Cisco ISE personas are sharing the same node.

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_setup_cisco_ise.html

Question: 143

A network engineer has been tasked with enabling a switch to support standard web authentication for Cisco ISE. This must include the ability to provision for URL redirection on authentication Which two commands must be entered to meet this requirement? (Choose two)

A. Ip http secure-authentication

B. Ip http server

C. Ip http redirection

D. Ip http secure-server

E. Ip http authentication

Answer: B, D

Explanation:

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0111001.html

Question: 144

An engineer is configuring a dedicated SSID for onboarding devices. Which SSID type accomplishes this configuration?

A. dual

B. hidden

C. broadcast

D. guest

Answer: A

Explanation:

https://community.cisco.com/t5/security-documents/ise-byod-dual-vs-single-ssid-onboarding/ta-p/3641422

https://www.youtube.com/watch?v=HH_Xasqd9k4&ab_channel=CiscoISE-IdentityServicesEngine

http://www.labminutes.com/sec0053_ise_1_1_byod_wireless_onboarding_dual_ssid

Question: 145

An engineer is implementing network access control using Cisco ISE and needs to separate the traffic based on the network device ID and use the IOS device sensor capability. Which probe must be used to accomplish this task?

A. HTTP probe

B. NetFlow probe

C. network scan probe

D. RADIUS probe

Answer: D

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure- Device-Sensor-for-ISE-Profilin.html

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

Question: 146

DRAG DROP

Drag the descriptions on the left onto the components of 802.1X on the right.

www.atmicnetworks.com

software on the endpoint that communicates with EAP at layer 2	authenticator
device that controls physical access to the network based on the endpoint authentication status	supplicant
device that validates the identity of the endpoint and provides results to another device	authentication server

Answer:

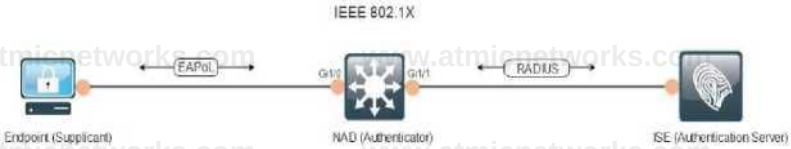
Explanation:

software on the endpoint that communicates with EAP at layer 2

device that validates the identity of the endpoint and provides results to another device

device that controls physical access to the network based on the endpoint authentication status

https://netlabz.wordpress.com/2016/09/24/cisco-ise-fundamentals/



Question: 147

An administrator is trying to collect metadata information about the traffic going across the network to gam added visibility into the hosts. This Information will be used to create profiling policies for devices us mg Cisco ISE so that network access policies can be used What must be done to accomplish this task?

A. Configure the RADIUS profiling probe within Cisco ISE

B. Configure NetFlow to be sent to me Cisco ISE appliance.

C. Configure SNMP to be used with the Cisco ISE appliance

D. Configure the DHCP probe within Cisco ISE

Answer: D

Explanation:

Question: 148

A laptop was stolen and a network engineer added it to the block list endpoint identity group What must be done on a new Cisco ISE deployment to redirect the laptop and restrict access?

A. Select DenyAccess within the authorization policy.

B. Ensure that access to port 8443 is allowed within the ACL.

C. Ensure that access to port 8444 is allowed within the ACL.

D. Select DROP under If Auth fail within the authentication policy.

Answer: C

Explanation:

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_010000.html

Question: 149

An administrator is migrating device administration access to Cisco ISE from the legacy TACACS+

solution that used only privilege 1 and 15 access levels. The organization requires more granular controls of the privileges and wants to customize access levels 2-5 to correspond with different roles and access needs. Besides defining a new shell profile in Cisco ISE. what must be done to accomplish this configuration?

A. Enable the privilege levels in Cisco ISE

B. Enable the privilege levels in the IOS devices.

C. Define the command privileges for levels 2-5 in the IOS devices

D. Define the command privileges for levels 2-5 in Cisco ISE

Answer: B

Explanation:

https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels

Question: 150

An administrator is configuring RADIUS on a Cisco switch with a key set to Cisc403012128 but is receiving the error "Authentication failed: 22040 Wrong password or invalid shared secret. "what must be done to address this issue?

A. Add the network device as a NAD inside Cisco ISE using the existing key.

B. Configure the key on the Cisco ISE instead of the Cisco switch.

C. Use a key that is between eight and ten characters.

D. Validate that the key is correct on both the Cisco switch as well as Cisco ISE.

Answer: D

Explanation:

Question: 151

What is the maximum number of PSN nodes supported in a medium-sized deployment?

A. three

B. five

C. two

D. eight

Answer: B

Explanation:

Question: 152

An organization has a fully distributed Cisco ISE deployment When implementing probes, an administrator must scan for unknown endpoints to learn the IP-to-MAC address bindings. The scan is complete on one FPSN. but the information is not available on the others. What must be done to make the information available?

A. Scanning must be initiated from the PSN that last authenticated the endpoint

B. Cisco ISE must learn the IP-MAC binding of unknown endpoints via DHCP profiling, not via scanning

C. Scanning must be initiated from the MnT node to centrally gather the information

D. Cisco ISE must be configured to learn the IP-MAC binding of unknown endpoints via RADIUS authentication, not via scanning

Answer: B

Explanation:

Question: 153

An administrator is configuring a new profiling policy within Cisco ISE The organization has several endpoints that are the same device type and all have the same Block ID in their MAC address. The profiler does not currently have a profiling policy created to categorize these endpoints. therefore a custom profiling policy must be created Which condition must the administrator use in order to properly profile an ACME Al Connector endpoint for network access with MAC address <MAC ADDRESS>?

A. MAC_OUI_STARTSWITH_<MACADDRESS>

B. CDP_cdpCacheDeviceID_CONTAINS_<MACADDRESS>

C. MAC_MACAddress_CONTAINS_<MACADDRESS>

D. Radius Called Station-ID STARTSWITH <MACADDRESS>

Answer: D

Explanation:

Question: 154

A network administrator is configuring client provisioning resource policies for client machines and must ensure that an agent pop-up is presented to the client when attempting to connect to the network Which configuration item needs to be added to allow for this'?

A. the client provisioning URL in the authorization policy

B. a temporal agent that gets installed onto the system

C. a remote posture agent proxying the network connection

D. an API connection back to the client

Answer: C

Explanation:

Question: 155

A network administrator must configure Cisco SE Personas in the company to share session information via syslog. Which Cisco ISE personas must be added to syslog receivers to accomplish this goal?

A. pxGrid

B. admin

C. policy services

D. monitor

Answer: D

Explanation:

Question: 156

A network administrator notices that after a company-wide shut down, many users cannot connect their laptops to the corporate SSID. What must be done to permit access in a timely manner?

A. Authenticate the user's system to the secondary Cisco ISE node and move this user to the primary with the renewed certificate.

B. Connect this system as a guest user and then redirect the web auth protocol to log in to the network.

C. Add a certificate issue from the CA server, revoke the expired certificate, and add the new certificate in system.

D. Allow authentication for expired certificates within the EAP-TLS section under the allowed protocols.

Answer: A

Explanation:

Question: 157

An administrator adds a new network device to the Cisco ISE configuration to authenticate endpoints to the network. The RADIUS test fails after the administrator configures all of the settings in Cisco ISE and adds the proper configurations to the switch. What is the issue"?

A. The endpoint profile is showing as "unknown."

B. The endpoint does not have the appropriate credentials for network access.

C. The shared secret is incorrect on the switch or on Cisco ISE.

D. The certificate on the switch is self-signed not a CA-provided certificate.

Answer: B

Explanation:

Question: 158

An engineer tests Cisco ISE posture services on the network and must configure the compliance module to automatically download and install on endpoints Which action accomplishes this task for VPN users?

A. Create a Cisco AnyConnect configuration and Client Provisioning policy within Cisco ISE.

B. Configure the compliance module to be downloaded from within the posture policy.

C. Push the compliance module from Cisco FTD prior to attempting posture.

D. Use a compound posture condition to check for the compliance module and download if needed.

Answer: A

Explanation:

Question: 159

Users in an organization report issues about having to remember multiple usernames and passwords. The network administrator wants the existing Cisco ISE deployment to utilize an external identity source to alleviate this issue. Which two requirements must be met to implement this change? (Choose two.)

A. Enable IPC access over port 80.

B. Ensure that the NAT address is properly configured

C. Establish access to one Global Catalog server.

D. Provide domain administrator access to Active Directory.

E. Configure a secure LDAP connection.

Answer: C, D

Explanation:

Question: 160

Which two external identity stores support EAP-TLS and PEAP-TLS? (Choose two.)

A. Active Directory

B. RADIUS Token

C. Internal Database

D. RSA SecurID

E. LDAP

Answer: A, E

Explanation:

Question: 161

What is a function of client provisioning?

A. It ensures an application process is running on the endpoint.

B. It checks a dictionary' attribute with a value.

C. It ensures that endpoints receive the appropriate posture agents

D. It checks the existence date and versions of the file on a client.

Answer: C

Explanation:

Question: 162

An administrator is troubleshooting an endpoint that is supposed to bypass 802 1X and use MAB. The endpoint is bypassing 802.1X and successfully getting network access using MAB. however the endpoint cannot communicate because it cannot obtain an IP address. What is the problem?

A. The DHCP probe for Cisco ISE is not working as expected.

B. The 802.1 X timeout period is too long.

C. The endpoint is using the wrong protocol to authenticate with Cisco ISE.

D. An AC I on the port is blocking HTTP traffic

Answer: B

Explanation:

Question: 163

A Cisco ISE administrator must restrict specific endpoints from accessing the network while in closed mode. The requirement is to have Cisco ISE centrally store the endpoints to restrict access from. What must be done to accomplish this task''

A. Add each MAC address manually to a blocklist identity group and create a policy denying access

B. Create a logical profile for each device's profile policy and block that via authorization policies.

C. Create a profiling policy for each endpoint with the cdpCacheDeviceId attribute.

D. Add each IP address to a policy denying access.

Answer: B

Explanation:

Question: 164

An engineer deploys Cisco ISE and must configure Active Directory to then use information from Active Directory in an authorization policy. Which two components must be configured, in addition to Active Directory groups, to achieve this goat? (Choose two)

A. Active Directory External Identity Sources

B. Library Condition for External Identity. External Groups

C. Identity Source Sequences

D. LDAP External Identity Sources

E Library Condition for Identity Group: User Identity Group

Answer: A, B

Explanation:

Question: 165

An engineer is working with a distributed deployment of Cisco ISE and needs to configure various network probes to collect a set of attributes from the endpoints on the network. Which node should be used to accomplish this task?

A. PSN

B. primary PAN

C. pxGrid

D. MnT

Answer: A

Explanation:

Question: 166

An engineer is configuring TACACS+ within Cisco ISE for use with a non-Cisco network device. They need to send special attributes in the Access-Accept response to ensure that the users are given the appropriate access. What must be configured to accomplish this'?

A. dACLs to enforce the various access policies for the users

B. custom access conditions for defining the different roles

C. shell profiles with custom attributes that define the various roles

D. TACACS+ command sets to provide appropriate access

Answer: C

Explanation:

Question: 167

An engineer is configuring Cisco ISE policies to support MAB for devices that do not have 802.1X capabilities. The engineer is configuring new endpoint identity groups as conditions to be used in the AuthZ policies, but noticed that the endpoints are not hitting the correct policies. What must be done in order to get the devices into the right policies?

A. Manually add the MAC addresses of the devices to endpoint ID groups in the context visibility database.

B. Create an AuthZ policy to identify Unknown devices and provide partial network access prior to profiling.

C. Add an identity policy to dynamically add the IP address of the devices to their endpoint identity groups.

D. Identify the non 802.1X supported device types and create custom profiles for them to profile into.

Answer: D

Explanation:

Question: 168

An administrator is configuring a Cisco WLC for web authentication Which two client profiling methods are enabled by default if the Apply Cisco ISE Default Settings check box has been selected'? (Choose two.)

A. CDP

B. DHCP

C. HTTP

D. SNMP

E. LLDP

Answer: AE

Explanation:

Question: 169

An administrator needs to allow guest devices to connect to a private network without requiring usernames and passwords. Which two features must be configured to allow for this? (Choose two.)

A. hotspot guest portal

B. device registration WebAuth

C. central WebAuth

D. local WebAuth

E. self-registered guest portal

Answer: A, B

Explanation:

Question: 170

An engineer is enabling a newly configured wireless SSID for tablets and needs visibility into which other types of devices are connecting to it. What must be done on the Cisco WLC to provide this information to Cisco ISE9

A. enable IP Device Tracking

B. enable MAC filtering

C. enable Fast Transition

D. enable mDNS snooping

Answer: B

Explanation:

Question: 171

A network administrator is currently using Cisco ISE to authenticate devices and users via 802 1X There is now a need to also authorize devices and users using EAP-TLS. Which two additional components must be configured in Cisco ISE to accomplish this'? (Choose two.)

A. Network Device Group

B. Serial Number attribute that maps to a CA Server

C. Common Name attribute that maps to an identity store

D. Certificate Authentication Profile

E. EAP Authorization Profile

Answer: C, D

Explanation:

Question: 172

An engineer is configuring sponsored guest access and needs to limit each sponsored guest to a maximum of two devices. There are other guest services in production that rely on the default guest types. How should this configuration change be made without disrupting the other guest services currently offering three or more guest devices per user?

A. Create an ISE identity group to add users to and limit the number of logins via the group configuration.

B. Create a new guest type and set the maximum number of devices sponsored guests can register

C. Create an LDAP login for each guest and tag that in the guest portal for authentication.

D. Create a new sponsor group and adjust the settings to limit the devices for each guest.

Answer: D

Explanation:

Question: 173

A Cisco ISE administrator needs to ensure that guest endpoint registrations are only valid for 1 day. When testing the guest policy flow, the administrator sees that the Cisco ISE does not delete the endpoint in the Guest Endpoints identity store after one day and allows access to the guest network after that period. Which configuration is causing this problem?

A. The RADIUS policy set for guest access is set to allow repeated authentication of the same device.

B. The length of access is set to 7 days in the Guest Portal Settings.

C. The Endpoint Purge Policy is set to 30 days for guest devices.

D. The Guest Account Purge Policy is set to 15 days.

Answer: C

Explanation:

Question: 174

An employee must access the internet through the corporate network from a new mobile device that does not support native supplicant provisioning provided by Cisco ISE. Which portal must the employee use to provision to the device?

A. BYOD

B. Personal Device

C. My Devices

D. Client Provisioning

Answer: C

Explanation:

Question: 175

What are two differences between the RADIUS and TACACS+ protocols'? (Choose two.)

A. RADIUS is a Cisco proprietary protocol, whereas TACACS+ is an open standard protocol

B. TACACS+uses TCP port 49. whereas RADIUS uses UDP ports 1812 and 1813.

C. RADIUS offers multiprotocol support, whereas TACACS+ does not

D. RADIUS combines authentication and authorization, whereas TACACS+ does not

E. RADIUS enables encryption of all the packets, whereas with TACACS+. only the password is encrypted.

Answer: B, D

Explanation:

Question: 176

An administrator is configuring a new profiling policy in Cisco ISE for a printer type that is missing from the profiler feed The logical profile Printers must be used in the authorization rule and the rule must be hit. What must be done to ensure that this configuration will be successful^

A. Create a new logical profile for the new printer policy

B. Enable the EndPoints:EndPointPolicy condition in the authorization policy.

C. Add the new profiling policy to the logical profile Printers.

D. Modify the profiler conditions to ensure that it goes into the correct logical profile

Answer: B

Explanation:

Question: 177

Which two default guest portals are available with Cisco ISE? (Choose two.)

A. visitor

B. WIFI-access

C. self-registered

D. central web authentication

E. sponsored

Answer: C, E

Explanation:

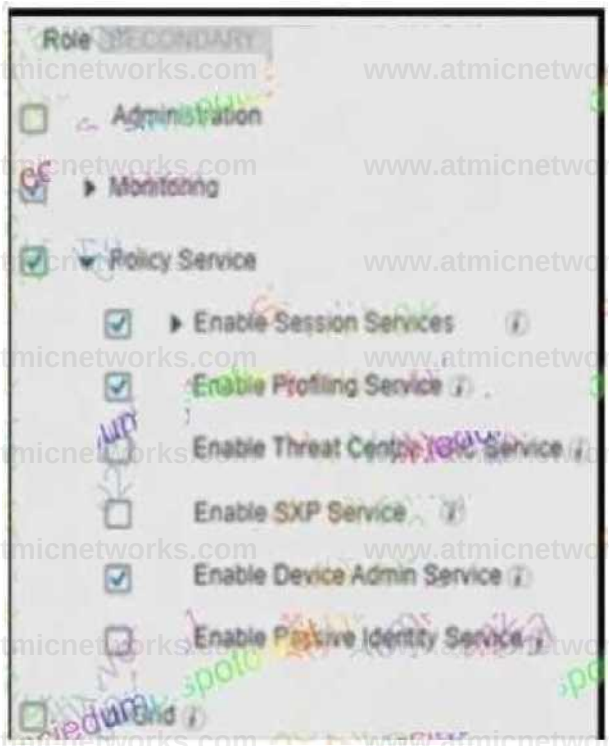
Question: 178

An engineer builds a five-node distributed Cisco ISE deployment The first two deployed nodes are responsible for the primary and secondary administration and monitoring personas Which persona configuration is necessary to have the remaining three Cisco ISE nodes serve as dedicated nodes in the Cisco ISE cube that is responsible only for handling the RADIUS and TACACS+ authentication requests, identity lookups, and policy evaluation?

A)

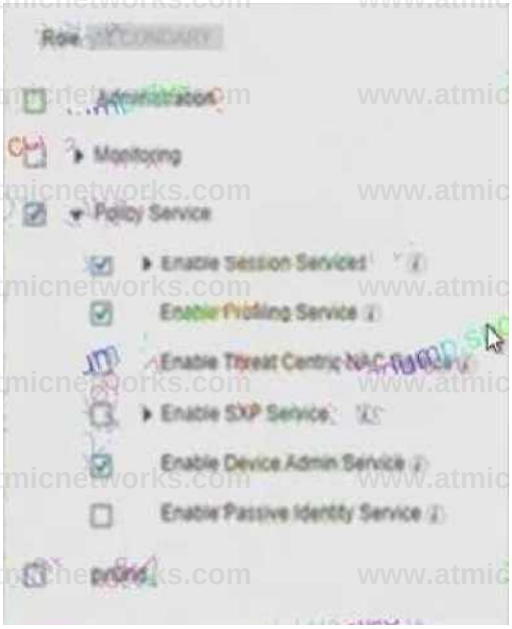
Role SECONDARY
Administration
Monitoring
Policy Service
Enable Session Services
Enable Profiling Service
Enable Threat Centric NAC Service
Enable SXP Service
Enable Device Admin Service
Enable Passive Identity Service

B)


Role SECONDARY
Administration
Monitoring
Policy Service
Enable Session Services
Enable Profiling Service
Enable Threat Centric NAC Service
Enable SXP Service
Enable Device Admin Service
Enable Passive Identity Service

C)

D)



A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

Question: 179

An administrator is configuring a switch port for use with 802 1X What must be done so that the port will allow voice and multiple data endpoints?

A. Configure the port with the authentication host-mode multi-auth command

B. Connect the data devices to the port, then attach the phone behind them.

C. Use the command authentication host-mode multi-domain on the port

D. Connect a hub to the switch port to allow multiple devices access after authentication

Answer: A

Explanation:

Question: 180

An engineer is configuring Cisco ISE for guest services They would like to have any unregistered guests redirected to the guest portal for authentication then have a CoA provide them with full access to the network that is segmented via firewalls Why is the given configuration failing to accomplish this goal?

A. The Guest Flow condition is not in the line that gives access to the quest portal

B. The Network_Access_Authentication_Passed condition will not work with guest services for portal access.

C. The Permit Access result is not set to restricted access in its policy line

D. The Guest Portal and Guest Access policy lines are in the wrong order

Answer: D

Explanation:

Question: 181

An engineer is configuring ISE for network device administration and has devices that support both protocols. What are two benefits of choosing TACACS+ over RADUs for these devices? (Choose two.)

A. TACACS+ is FIPS compliant while RADIUS is not

B. TACACS+ is designed for network access control while RADIUS is designed for role-based access.

C. TACACS+ uses secure EAP-TLS while RADIUS does not.

D. TACACS+ provides the ability to authorize specific commands while RADIUS does not

E. TACACS+ encrypts the entire payload being sent while RADIUS only encrypts the password.

Answer: D, E

Explanation:

Question: 182

During a 802 1X deployment, an engineer must identify failed authentications without causing problems for the connected endpoint. Which command will successfully achieve this''

A. dot1x system-auth-control

B. dot1x pae authenticator

C. authentication open

D. authentication port-control auto

Answer: C

Explanation:

Question: 183

An engineer is configuring 802.1X and is testing out their policy sets. After authentication, some endpoints are given an access-reject message but are still allowed onto the network. What is causing this issue to occur?

A. The switch port is configured with authentication event server dead action authorize vlan.

B. The authorization results for the endpoints include a dACL allowing access.

C. The authorization results for the endpoints include the Trusted security group tag.

D. The switch port is configured with authentication open.

Answer: D

Explanation:

Question: 184

An engineer has been tasked with standing up a new guest portal for customers that are waiting in the lobby. There is a requirement to allow guests to use their social media logins to access the guest network to appeal to more customers What must be done to accomplish this task?

A. Create a sponsor portal to allow guests to create accounts using their social media logins.

B. Create a sponsored guest portal and enable social media in the external identity sources.

C. Create a self-registered guest portal and enable the feature for social media logins

D. Create a hotspot portal and enable social media login for network access

Answer: C

Explanation:

Question: 185

Which Cisco ISE deployment model provides redundancy by having every node in the deployment configured with the Administration. Policy Service, and Monitoring personas to protect from a complete node failure?

A. distributed

B. dispersed

C. two-node

D. hybrid

Answer: C

Explanation:

Question: 186

An administrator enables the profiling service for Cisco ISE to use for authorization policies while in closed mode. When the endpoints connect, they receive limited access so that the profiling probes can gather information and Cisco ISE can assign the correct profiles. They are using the default values within Cisco ISE. but the devices do not change their access due to the new profile. What is the problem'?

A. In closed mode, profiling does not work unless CDP is enabled.

B. The profiling probes are not able to collect enough information to change the device profile

C. The profiler feed is not downloading new information so the profiler is inactive

D. The default profiler configuration is set to No CoA for the reauthentication setting

Answer: D

Explanation:

Question: 187

Which RADIUS attribute is used to dynamically assign the inactivity active timer for MAB users from the Cisco ISE node'?

A. radius-server timeout

B. session-timeout

C. idle-timeout

D. termination-action

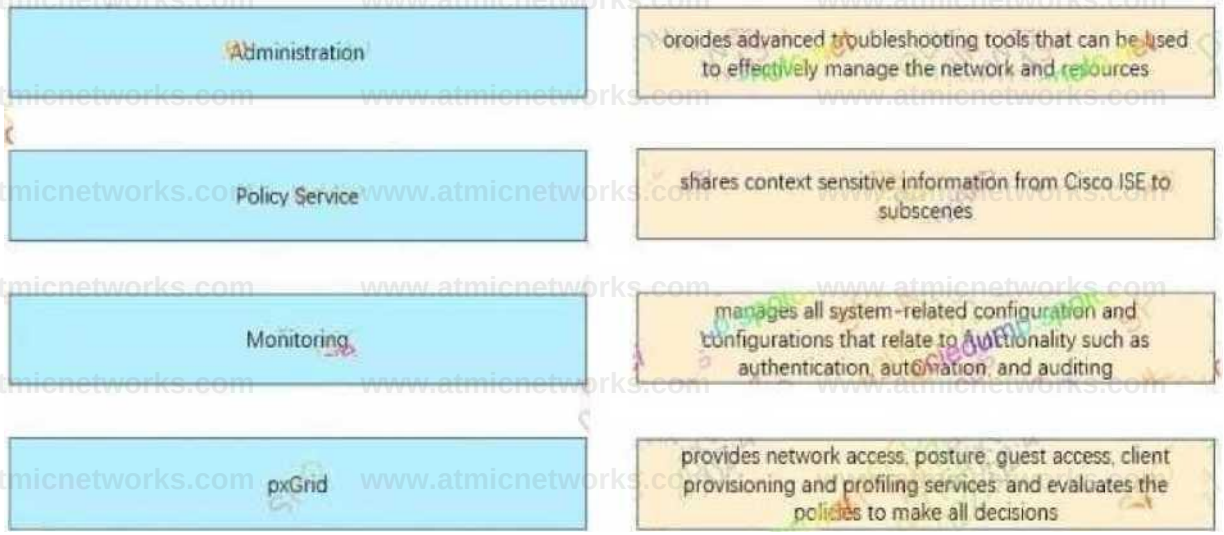
Answer: C

Explanation:

Question: 188

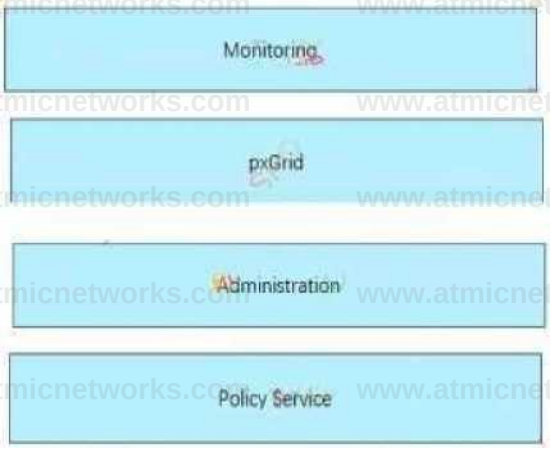
DRAG DROP

Select and Place



Answer:

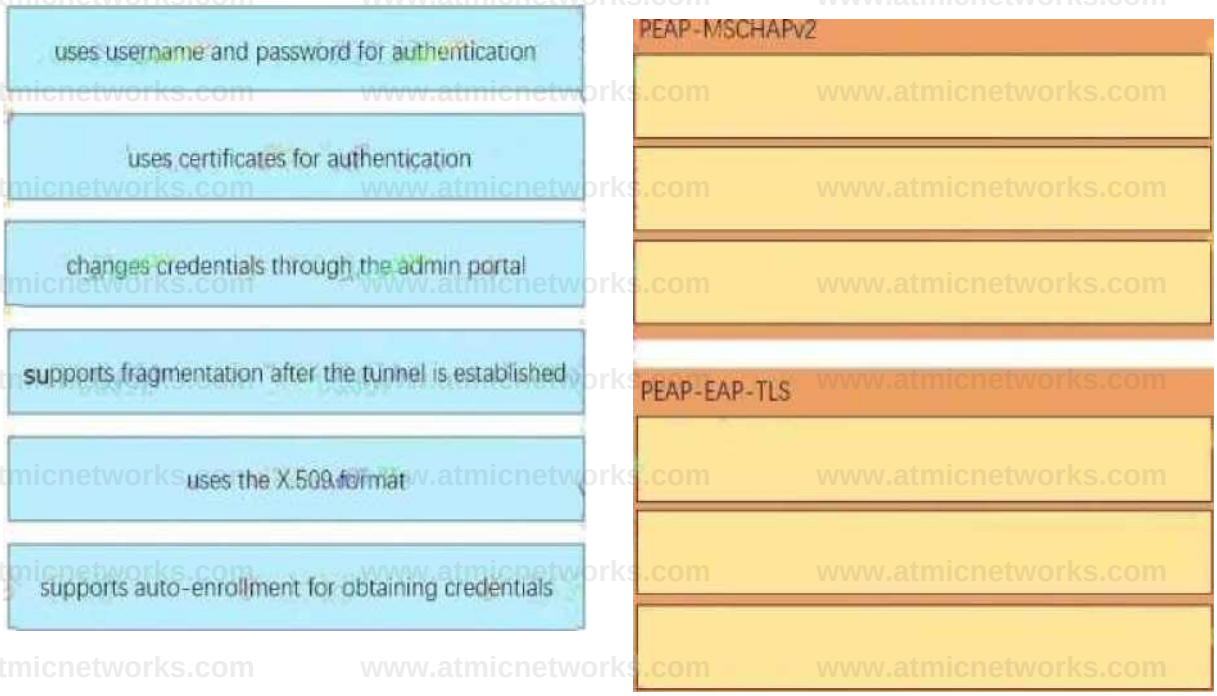
Explanation:



Question: 189

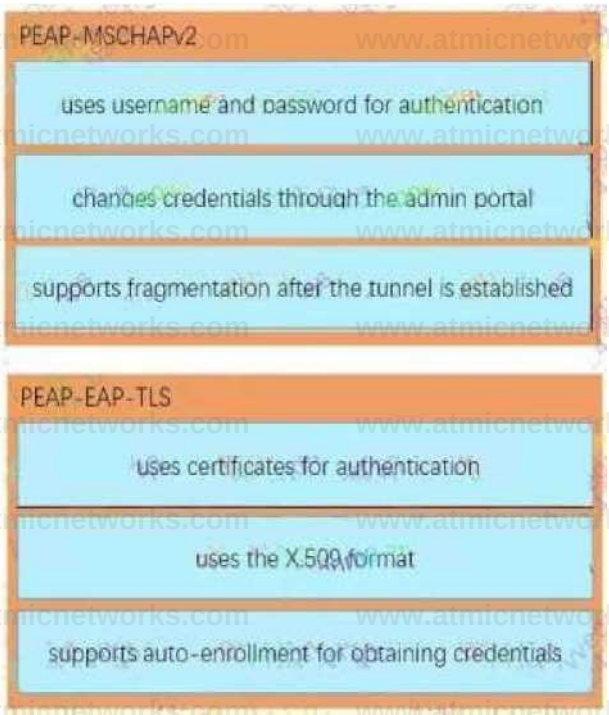
DRAG DROP

Select and Place



Answer:

Explanation:



Question:
190

An engineer is configuring the remote access VPN to use Cisco ISE for AAA and needs to conduct posture checks on the connecting endpoints After the endpoint connects, it receives its initial authorization result and continues onto the compliance scan What must be done for this AAA configuration to allow compliant access to the network?

A. Configure the posture authorization so it defaults to unknown status

B. Fix the CoA port number

C. Ensure that authorization only mode is not enabled

D. Enable dynamic authorization within the AAA server group

Answer: D

Explanation:

Question: 191

Which two Cisco ISE deployment models require two nodes configured with dedicated PAN and MnT personas? (Choose two.)

A. three PSN nodes

B. seven PSN nodes with one PxGrid node

C. five PSN nodes with one PxGrid node

D. two PSN nodes with one PxGrid node

E. six PSN nodes

Answer: CD

Explanation:

Question: 192

Which compliance status is set when a matching posture policy has been defined for that endpomt. but all the mandatory requirements during posture assessment are not met?

A. unauthorized

B. untrusted

C. non-compliant

D. unknown

Answer: C

Explanation:

Question: 193

A Cisco device has a port configured in multi-authentication mode and is accepting connections only from hosts assigned the SGT of SGT_0422048549 The VLAN trunk link supports a maximum of 8 VLANS What is the reason for these restrictions?

A. The device is performing inline tagging without acting as a SXP speaker

B. The device is performing mime tagging while acting as a SXP speaker

C. The IP subnet addresses are dynamically mapped to an SGT.

D. The IP subnet addresses are statically mapped to an SGT

Answer: C

Explanation:

Question: 194

An administrator wants to configure network device administration and is trying to decide whether to use TACACS* or RADIUS. A reliable protocol must be used that can check command authorization

Which protocol meets these requirements and why?

A. TACACS+ because it runs over TCP

B. RADIUS because it runs over UDP

C. RADIUS because it runs over TCP.

D. TACACS+ because it runs over UDP

Answer: A

Explanation:

Question: 195

An administrator has added a new Cisco ISE PSN to their distributed deployment. Which two features must the administrator enable to accept authentication requests and profile the endpoints correctly, and add them to their respective endpoint identity groups? (Choose two)

A. Session Services

B. Endpoint Attribute Filter

C. Posture Services

D. Profiling Services

E. Radius Service

Answer: DE

Explanation:

Question: 196

Refer to the exhibit.

Which two configurations are needed on a catalyst switch for it to be added as a network access device in a Cisco ISE that is being used for 802 1X authentications? (Choose two)

radius server ISE 1
address ipv4 192.168 255 17 auth-port 1645 acct-port 1646
key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52

tacacs server ISE1
address ipv4 192 168.255.15 auth-port 1645 acct-port 1646
key 7 0607542D6F4A0213034C1E0A1F0F2E2122733F3429000D12056A5A52

radius server ISE1
address ipv4 192.168.255.19 auth-port 1645 acct-port 1646
key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52

radius server ISE1
address Ipv4 192.168.255.16 auth-port 1645 acct-port 1646
key 7 0607642D6F4A0213034C1E0A1F0F2E2122733F3429000D12056A6A52

tacacs server ISE1
address ipv4 192.168.255.18 auth-port 1645 acct-port 1646
key 7 0607642D6F4A0213034C1E0A1F0F2E2122733F3429000D12066A6A52

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Answer: AC

Explanation:

Question: 197

An administrator is configuring sponsored guest access using Cisco ISE Access must be restricted to the sponsor portal to ensure that only necessary employees can issue sponsored accounts and employees must be classified to do so What must be done to accomplish this task?

A. Configure an identity-based access list in Cisco ISE to restrict the users allowed to login

B. Edit the sponsor portal to only accept members from the selected groups

C. Modify the sponsor groups assigned to reflect the desired user groups

D. Create an authorization rule using the Guest Flow condition to authorize the administrators

Answer: C

Explanation:

Question: 198

Refer to the exhibit.

Interface	MAC AMrm Method	Domain Statu* Fg	Session ID
Cil/t/t C1VI/1	M24.142d.e47f Mb H5e.54M.I72C dot lx	UNKNOT Auth INMNI Unuth	C*A82M2MMM«C28BAF5D1 C*A829«2HMH1 S2KNHT

An engineer is configuring a client but cannot authenticate to Cisco ISE During troubleshooting, the show authentication sessions command was issued to display the authentication status of each port Which command gives additional information to help identify the problem with the authentication?

A. show authentication sessions

B. show authentication sessions Interface Gil/0/1 output

C. show authentication sessions interface Gi1/0/1 details

D. show authentication sessions output

Answer: C

Explanation:

Question: 199

An administrator is manually adding a device to a Cisco ISE identity group to ensure that it is able to access the network when needed without authentication Upon testing, the administrator notices that the device never hits the correct authorization policy line using the condition EndPoints LogicalProfile EQUALS static_list Why is this occurring?

A. The dynamic logical profile is overriding the statically assigned profile

B. The device is changing identity groups after profiling instead ot remaining static

C. The logical profile is being statically assigned instead of the identity group

D. The identity group is being assigned instead of the logical profile

Answer: C

Explanation:

Question: 200

An engineer is creating a new authorization policy to give the endpoints access to VLAN 310 upon successful authentication The administrator tests the 802.1X authentication for the endpoint and sees that it is authenticating successfully What must be done to ensure that the endpoint is placed into the correct VLAN?

A. Configure the switchport access vlan 310 command on the switch port
B. Ensure that the security group is not preventing the endpoint from being in VLAN 310
C. Add VLAN 310 in the common tasks of the authorization profile

D. Ensure that the endpoint is using The correct policy set

Answer: C

Explanation:

Question: 201

An engineer is configuring posture assessment for their network access control and needs to use an agent that supports using service conditions as conditions for the assessment. The agent should be run as a background process to avoid user interruption but when it is run. the user can see it. What is the problem?

A. The engineer is using the "Anyconnect" posture agent but should be using the "Stealth Anyconnect posture agent

B. The posture module was deployed using the headend instead of installing it with SCCM

C. The user was in need of remediation so the agent appeared m the notifications

D. The proper permissions were no! given to the temporal agent to conduct the assessment

Answer: A

Explanation:

Question: 202

A user is attempting to register a BYOD device to the Cisco ISE deployment, but needs to use the onboarding policy to request a digital certificate and provision the endpoint. What must be configured to accomplish this task?

A. A native supplicant provisioning policy to redirect them to the BYOD portal for onboarding

B. The Cisco AnyConnect provisioning policy to provision the endpoint for onboarding

C. The BYOD flow to ensure that the endpoint will be provisioned prior to registering

D. The posture provisioning policy to give the endpoint all necessary components prior to registering

Answer: A

Explanation:

www.atmicnetworks.com

Question: 203

While configuring Cisco TrustSec on Cisco IOS devices the engineer must set the CTS device ID and password in order for the devices to authenticate with each other. However after this is complete the devices are not able to property authenticate What issue would cause this to happen even if the device ID and passwords are correct?

A. The device aliases are not matching

B. The 5GT mappings have not been defined

C. The devices are missing the configuration cts credentials trustsec verify 1

D. EAP-FAST is not enabled

Answer: B

Explanation:

Question: 204

An engineer is configuring a posture policy for Windows 10 endpoints and wants to ensure that users in each AD group have different conditions to meet to be compliant. What must be done to accomplish this task?

A. identify The users groups needed for different policies and create service conditions to map each one to its posture requirement

B. Configure a simple condition for each AD group and use it in the posture policy for each use case

C. Use the authorization policy within the policy set to group each AD group with their respective posture policy

D. Change the posture requirements to use an AD group lor each use case then use those requirements in the posture policy

Answer: C

Explanation:

Question: 205

An organization wants to enable web-based guest access for both employees and visitors The goal is to use a single portal for both user types Which two authentication methods should be used to meet this requirement? (Choose two)

A. LDAP

B. 802 1X

C. Certificate-based

D. LOCAL

E. MAC based

Answer: DE

Explanation:

Question: 206

An organization is adding nodes to their Cisco ISE deployment and has two nodes designated as

primary and secondary PAN and MnT nodes. The organization also has four PSNs An administrator is adding two more PSNs to this deployment but is having problems adding one of them What is the problem?

A. The new nodes must be set to primary prior to being added to the deployment

B. The current PAN is only able to track a max of four nodes

C. Only five PSNs are allowed to be in the Cisco ISE cube if configured this way.

D. One of the new nodes must be designated as a pxGrid node

Answer: C

Explanation:

Question: 207

Which two authentication protocols are supported by RADIUS but not by TACACS+? (Choose two.)

A. MSCHAPv1

B. PAP

C. EAP

D. CHAP

E. MSCHAPV2

Answer: CE

Explanation:

Question: 208

What is a difference between RADIUS and TACACS+?

A. RADIUS uses connection-oriented transport, and TACACS+ uses best-effort delivery.

B. RADIUS offers multiprotocol support, and TACACS+ supports only IP traffic.

C. RADIUS combines authentication and authorization functions, and TACACS+ separates them.

D. RADIUS supports command accounting, and TACACS+ does not.

Answer: C

Explanation:

Question: 209

An engineer is unable to use SSH to connect to a switch after adding the required CLI commands to the device to enable TACACS+. The device administration license has been added to Cisco ISE, and the required policies have been created. Which action is needed to enable access to the switch?

A. The ip ssh source-interface command needs to be set on the switch

B. 802.1X authentication needs to be configured on the switch.

C. The RSA keypair used for SSH must be regenerated after enabling TACACS+.

D. The switch needs to be added as a network device in Cisco ISE and set to use TACACS+.

Answer: D

Explanation:

Question: 210

DRAG DROP

An engineer needs to export a file in CSV format, encrypted with the password C1$c0438563935, and contains users currently configured in Cisco ISE. Drag and drop the steps from the left into the sequence on the right to complete this task.

Click Export Selected, click Key, and enter the password.	1
Click Administration, and then click Identity Management.	2
Click Start Export, and then click OK.	3
Click Identities, click Users, and then select the list of users.	4

Answer:

Explanation:

Click Administration, and then click Identity Management.
Click Identities, click Users, and then select the list of users.
Click Export Selected, click Key, and enter the password.
Click Start Export, and then click OK.

Question: 211

The IT manager wants to provide different levels of access to network devices when users authenticate using TACACS+. The company needs specific commands to be allowed based on the Active Directory group membership of the different roles within the IT department. The solution must minimize the number of objects created in Cisco ISE. What must be created to accomplish this task?

A. one shell profile and one command set

B. multiple shell profiles and one command set

C. one shell profile and multiple command sets

D. multiple shell profiles and multiple command sets

Answer: C

Explanation:

Question: 212

What are two differences of TACACS+ compared to RADIUS? (Choose two.)

A. TACACS+ uses a connectionless transport protocol, whereas RADIUS uses a connection-oriented transport protocol.

B. TACACS+ encrypts the full packet payload, whereas RADIUS only encrypts the password.

C. TACACS+ only encrypts the password, whereas RADIUS encrypts the full packet payload.

D. TACACS+ uses a connection-oriented transport protocol, whereas RADIUS uses a connectionless transport protocol.

E. TACACS+ supports multiple sessions per user, whereas RADIUS supports one session per user.

Answer: BD

Explanation:

Question: 213

What is a valid status of an endpoint attribute during the device registration process?

A. block listed

B. pending

C. unknown

D. DenyAccess

Answer: B

Explanation:

Question: 214

An administrator is configuring the Native Supplicant Profile to be used with the Cisco ISE posture agents and needs to test the connection using wired devices to determine which profile settings are available. Which two configuration settings should be used to accomplish this task? (Choose two.)

A. authentication mode

B. proxy host/IP

C. certificate template

D. security

E. allowed protocol

Answer: CE

Explanation:

Question: 215

Which Cisco ISE solution ensures endpoints have the latest version of antivirus updates installed before being allowed access to the corporate network?

A. Threat Services

B. Profiling Services

C. Provisioning Services

D. Posture Services

Answer: D

Explanation:

Question: 216

An administrator is configuring posture assessment in Cisco ISE for the first time. Which two components must be uploaded to Cisco ISE to use Anyconnect for the agent configuration in a client provisioning policy? (Choose two.)

A. Anyconnect network visibility module

B. Anyconnect compliance module

C. AnyConnectProfile.xml file

D. AnyConnectProfile.xsd file

E. Anyconnect agent image

Answer: BD

Explanation:

Question: 217

What is a difference between TACACS+ and RADIUS in regards to encryption?

A. TACACS+ encrypts only the password, whereas RADIUS encrypts the username and password.

B. TACACS+ encrypts the username and password, whereas RADIUS encrypts only the password.

C. TACACS+ encrypts the password, whereas RADIUS sends the entire packet in clear text.

D. TACACS+ encrypts the entire packet, whereas RADIUS encrypts only the password.

Answer: D

Explanation:

Question: 218

An administrator must block access to BYOD endpoints that were onboarded without a certificate and have been reported as stolen in the Cisco ISE My Devices Portal. Which condition must be used when configuring an authorization policy that sets DenyAccess permission?

A. Endpoint Identity Group isBlocklist, and the BYOD state is Registered.

B. Endpoint Identify Group isBlocklist, and the BYOD state is Pending.

C. Endpoint Identity Group isBlocklist, and the BYOD state is Lost.

D. Endpoint Identity Group isBlocklist, and the BYOD state is Reinstate.

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ISE_26_admin_guide/b_ISE_admin_26_byod.html

Question: 219

An engineer needs to configure a new certificate template in the Cisco ISE Internal Certificate Authority to prevent BYOD devices from needing to re-enroll when their MAC address changes. Which option must be selected in the Subject Alternative Name field?

A. Common Name and GUID

B. MAC Address and GUID

C. Distinguished Name

D. Common Name

Answer: B

Explanation:

The engineer needs to select the option of MAC Address and GUID in the Subject Alternative Name field when configuring a new certificate template in the Cisco ISE Internal Certificate Authority to prevent BYOD devices from needing to re-enroll when their MAC address changes.

Question: 220

A user changes the status of a device to stolen in the My Devices Portal of Cisco ISE. The device was originally onboarded in the BYOD wireless Portal without a certificate. The device is found later, but the user cannot re-onboard the device because Cisco ISE assigned the device to the Blocklist endpoint identity group. What must the user do in the My Devices Portal to resolve this issue?

A. Manually remove the device from the Blocklist endpoint identity group.

B. Change the device state from Stolen to Not Registered.

C. Change the BYOD registration attribute of the device to None.

D. Delete the device, and then re-add the device.

Answer: B

Explanation:

Question: 221

A security administrator is using Cisco ISE to create a BYOD onboarding solution for all employees who use personal devices on the corporate network. The administrator generates a Certificate Signing Request and signs the request using an external Certificate Authority server. Which certificate

usage option must be selected when importing the certificate into ISE?

A. RADIUS

B. DLTS

C. Portal

D. Admin

Answer: C

Explanation:

Question: 222

DRAG DROP

An engineer needs to configure a compliance policy on Cisco ISE to ensure that the latest encryption software is running on the C drive of all endpoints. Drag and drop the configuration steps from the left into the sequence on the right to accomplish this task.

Answer Area

select Posture and Disk Encryption Condition	step 1
access the Disk Encryption Condition window	step 2
select the Encryption settings	step 3
access Policy Elements and Conditions	step 4

Answer:

Explanation:

Answer Area

select Posture and Disk Encryption Condition	access Policy Elements and Conditions
access the Disk Encryption Condition window	select Posture and Disk Encryption Condition
select the Encryption settings	access the Disk Encryption Condition window
access Policy Elements and Conditions	select the Encryption settings

Question: 223

Which two actions must be verified to confirm that the internet is accessible via guest access when configuring a guest portal? (Choose two.)

A. The guest device successfully associates with the correct SSID.

B. The guest user gets redirected to the authentication page when opening a browser.

C. The guest device has internal network access on the WLAN.

D. The guest device can connect to network file shares.

E. Cisco ISE sends a CoA upon successful guest authentication.

Answer: BE

Explanation:

Question: 224

An administrator made changes in Cisco ISE and needs to apply new permissions for endpoints that have already been authenticated by sending a CoA packet to the network devices. Which IOS command must be configured on the devices to accomplish this goal?

A. aaa server radius dynamic-author

B. authentication command bounce-port

C. authentication command disable-port

D. aaa nas port extended

Answer: A

Explanation:

Question: 225

An engineer needs to configure Cisco ISE Profiling Services to authorize network access for IP speakers that require access to the intercom system. This traffic needs to be identified if the ToS bit is set to 5 and the destination IP address is the intercom system. What must be configured to accomplish this goal?

A. NMAP

B. NETFLOW

C. pxGrid

D. RADIUS

Answer: B

Explanation:

Question: 226

An engineer needs to configure a Cisco ISE server to issue a CoA for endpoints already authenticated to access the network. The CoA option must be enforced on a session, even if there are multiple active sessions on a port. What must be configured to accomplish this task?

A. the Reauth CoA option in the Cisco ISE system profiling settings enabled

B. an endpoint profiling policy with the No CoA option enabled

C. an endpoint profiling policy with the Port Bounce CoA option enabled

D. the Port Bounce CoA option in the Cisco ISE system profiling settings enabled

Answer: A

Explanation:

Question: 227

An administrator replaced a PSN in the distributed Cisco ISE environment. When endpoints authenticate to it, the devices are not getting the right profiles or attributes and as a result, are not hitting the correct policies. This was working correctly on the previous PSN. Which action must be taken to ensure the endpoints get identified?

A. Verify that the MnT node is tracking the session.

B. Verify the shared secret used between the switch and the PSN.

C. Verify that the profiling service is running on the new PSN.

D. Verify that the authentication request the PSN is receiving is not malformed.

Answer: C

Explanation:

Question: 226

Which type of identity store allows for creating single-use access credentials in Cisco ISE?

A. OpenLDAP

B. Local

C. PKI

D. RSA SecurID

Answer: D

Explanation:

Question: 229

A network engineer needs to deploy 802.1x using Cisco ISE in a wired network environment where thin clients download their system image upon bootup using PXE. For which mode must the switch ports be configured?

A. closed

B. restricted

C. monitor

D. low-impact

Answer: D

Explanation:

Question: 230

An ISE administrator must change the inactivity timer for MAB endpoints to terminate the

authentication session whenever a switch port that is connected to an IP phone does not detect packets from the device for 30 minutes. Which action must be taken to accomplish this task?

A. Add the authentication timer reauthenticate server command to the switchport.

B. Add the authentication timer inactivity 3600 command to the switchport.

C. Change the idle-timeout on the Radius server to 3600 seconds for IP Phone endpoints.

D. Configure the session-timeout to be 3600 seconds on Cisco ISE.

Answer: B

Explanation:

Question: 231

An engineer is configuring static SGT classification. Which configuration should be used when authentication is disabled and third-party switches are in use?

A. VLAN to SGT mapping

B. IP Address to SGT mapping

C. L3IF to SGT mapping

D. Subnet to SGT mapping

Answer: B

Explanation:

https://community.cisco.com/t5/security-knowledge-base/segmentation-strategy/ta-p/3757424:

"The method of sending out IP to SGT mappings from ISE is particularly useful if the access switch does not support TrustSec"

Question: 232

An engineer must configure Cisco ISE to provide internet access for guests in which guests are required to

enter a code to gain network access. Which action accomplishes the goal?

A. Configure the hotspot portal for guest access and require an access code.

B. Configure the sponsor portal with a single account and use the access code as the password.

C. Configure the self-registered guest portal to allow guests to create a personal access code.

D. Create a BYOD policy that bypasses the authentication of the user and authorizes access codes.

Answer: A

Explanation:

Question: 233

DRAG DROP

Drag and drop the configuration steps from the left into the sequence on the right to install two Cisco ISE nodes in a distributed deployment.

Register the secondary node.	1
Define personas for the secondary node.	2
Enable Administration and Monitoring personas on the first node.	3
Configure the first node as the primary node.	4

Answer:

Explanation:

Enable Administration and Monitoring personas on the first node.

Configure the first node as the primary node.

Register the secondary node.

Define personas for the secondary node.

Question: 234

An engineer wants to learn more about Cisco ISE and deployed a new lab with two nodes. Which two persona configurations allow the engineer to successfully test redundancy of a failed node? (Choose two.)

A. Configure one of the Cisco ISE nodes as the Health Check node.

B. Configure both nodes with the PAN and MnT personas only.

C. Configure one of the Cisco ISE nodes as the primary PAN and MnT personas and the other as the secondary.

D. Configure both nodes with the PAN, MnT, and PSN personas.

E. Configure one of the Cisco ISE nodes as the primary PAN and PSN personas and the other as the secondary.

Answer: CE

Explanation:

Question: 235

Which Cisco ISE deployment model is recommended for an enterprise that has over 50,000 concurrent active endpoints?

A. large deployment with fully distributed nodes running all personas

B. medium deployment with primary and secondary PAN/MnT/pxGrid nodes with shared PSNs

C. medium deployment with primary and secondary PAN/MnT/pxGrid nodes with dedicated PSNs

D. small deployment with one primary and one secondary node running all personas

Answer: C

Explanation:

Question: 236

What is a restriction of a standalone Cisco ISE node deployment?

A. Only the Policy Service persona can be disabled on the node.

B. The domain name of the node cannot be changed after installation.

C. Personas are enabled by default and cannot be edited on the node.

D. The hostname of the node cannot be changed after installation.

Answer: C

Explanation:

Question: 237

What are the minimum requirements for deploying the Automatic Failover feature on Administration nodes in a distributed Cisco ISE deployment?

A. a primary and secondary PAN and a health check node for the Secondary PAN

B. a primary and secondary PAN and no health check nodes

C. a primary and secondary PAN and a pair of health check nodes

D. a primary and secondary PAN and a health check node for the Primary PAN

Answer: D

Explanation:

Question: 238

An administrator is attempting to join a new node to the primary Cisco ISE node, but receives the error message "Node is Unreachable". What is causing this error?

A. The second node is a PAN node.

B. No administrative certificate is available for the second node.

C. The second node is in standalone mode.

D. No admin privileges are available on the second node.

Answer: B

Explanation:

https://www.ciscopress.com/articles/article.asp?p=2812072

Question: 239

An engineer is starting to implement a wired 802.1X project throughout the campus. The task is for failed authentication to be logged to Cisco ISE and also have a minimal impact on the users. Which command must the engineer configure?

A. authentication open

B. pae dot1x enabled

C. authentication host-mode multi-auth

D. monitor-mode enabled

Answer: D

Explanation:

In the context of a wired 802.1X deployment with Cisco ISE, the requirement is to log failed authentications while minimizing user impact. Let's analyze each option:

A. authentication open - This command configures the port to allow network access regardless of the authentication state. It's useful in situations where specific devices can't perform 802.1X authentication but should still be allowed network access. However, it doesn't specifically address the logging of failed authentications.

B. pae dot1x enabled - PAE (Port Access Entity) refers to the entity on a network device that enforces access control. This command enables 802.1X on the port, which is a prerequisite for implementing 802.1X, but doesn't directly relate to logging failed authentication attempts.

C. authentication host-mode multi-auth - This command configures the port to allow multiple authenticated sessions. This mode is used when multiple devices are connected to the same port (like in a conference room). While it's relevant for 802.1X environments, it doesn't specifically cater to logging failed authentications or minimizing user impact.

D. monitor-mode enabled - This command is used in the context of 802.1X to enable Monitor Mode on a port. Monitor Mode allows a port to grant limited network access to endpoints without 802.1X capabilities. It's often used to ease the deployment of 802.1X by monitoring the authentication status without fully enforcing access control, thereby minimizing user impact. It also helps in logging authentication attempts, including failures.

Given these options, the most appropriate command for logging failed authentications while having minimal impact on users would be D. monitor-mode enabled. This command ensures that authentication attempts are monitored and logged, including failures, without fully restricting access, thus minimizing the impact on users who might face issues with the authentication process.

Question: 240

An engineer is working on a switch and must tag packets with SGT values such that it learns via SXP. Which command must be entered to meet this requirement?

A. ip source guard

B. ip dhcp snooping

C. ip device tracking maximum

D. ip arp inspection

Answer: C

Explanation:

The ip device tracking maximum command is used to configure the maximum number of IP-to-SGT bindings that can be learned via SXP on a switch1. This command also enables the switch to tag packets with SGT values based on the bindings learned from SXP peers. The other commands are not related to SGT tagging or SXP learning.

Question: 241

An enterprise uses a separate PSN for each of its four remote sites. Recently, a user reported receiving an "EAP-TLS authentication failed" message when moving between remote sites. Which configuration must be applied on Cisco ISE?

A. Use a third-party certificate on the network device.

B. Add the device to all PSN nodes in the deployment.

C. Renew the expired certificate on one of the PSN.

D. Configure an authorization profile for the end users.

Answer: B

Explanation:

When using separate PSNs for different sites, the network device must be added to all PSN nodes in the deployment, so that the device can communicate with the appropriate PSN based on the location of the user1. If the device is not added to all PSN nodes, the user may encounter an EAP-TLS authentication failure when moving between sites, as the device may not be able to reach the PSN that issued the certificate2. The other options are not relevant for this scenario, as they do not address the issue of PSN communication.

Question: 242

The security team identified a rogue endpoint with MAC address 00:46:91:02:28:4A attached to the network. Which action must security engineer take within Cisco ISE to effectively

restrict network access for this endpoint?

A. Configure access control list on network switches to block traffic.

B. Create authentication policy to force reauthentication.

C. Add MAC address to the endpoint quarantine list.

D. Implement authentication policy to deny access.

Answer: C

Explanation:

Cisco ISE provides a feature called Adaptive Network Control (ANC) that allows administrators to apply policies to endpoints based on their behavior or status1. One of the ANC policies is Quarantine, which restricts network access for an endpoint by assigning it to a limited-access VLAN or applying an access control list (ACL) on the switch port2. To use the Quarantine policy, the administrator must add the MAC address of the rogue endpoint to the endpoint quarantine list in ISE2. This will trigger a change of authorization (CoA) for the endpoint and apply the Quarantine policy. The other options are not effective for restricting network access for a rogue endpoint, as they do not use the ANC feature of ISE.

Question: 243

A network security administrator needs a web authentication configuration when a guest user connects to the network with a wireless connection using these steps:

. An initial MAB request is sent to the Cisco ISE node.

. Cisco ISE responds with a URL redirection authorization profile if the user's MAC address is unknown in the endpoint identity store.

. The URL redirection presents the user with an AUP acceptance page when the user attempts to go to any URL.

Which authentication must the administrator configure on Cisco ISE?

A. device registration WebAuth

B. WLC with local WebAuth

C. wired NAD with local WebAuth

D. NAD with central WebAuth

Answer: D

Explanation:

Central Web Authentication (CWA) is a feature that allows the network access device (NAD) to redirect the web traffic of a guest user to a web portal hosted by Cisco ISE1. The NAD acts as a proxy between the guest user and the ISE node, and performs the authentication and authorization based on the RADIUS attributes returned by ISE1. To configure CWA on ISE, the administrator must create an authorization profile that contains the URL redirection attribute and assign it to the guest user1. The other options are not correct because they do not use CWA. Device registration WebAuth is a feature that allows users to register their devices on ISE before they can access the network2. WLC with local WebAuth is a feature that allows the wireless LAN controller (WLC) to host the web portal and authenticate the guest user locally3. Wired NAD with local WebAuth is a feature that allows the switch to host the web portal and authenticate the guest user locally

Question: 244

An administrator is configuring cisco ISE lo authenticate users logging into network devices using TACACS+ The administrator is not seeing any oí the authentication in the TACACS+ live logs. Which action ensures the users are able to log into the network devices?

A. Enable the device administration service in the Administration persona

B. Enable the session services in the administration persona

C. Enable the service sessions in the PSN persona.

D. Enable the device administration service in the PSN persona.

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_tacacs_device_admin.html

Question: 245

Which file extension is required when deploying Cisco ISE using a ZTP configuration file in Microsoft Hyper-V?

A. .iso

B. .txt

C. .tar

D. .img

Answer: B

Question: 246

An engineer wants to use certificate authentication for endpoints that connect to a wired network integrated with Cisco ISE. The engineer needs to define the certificate field used as the principal username. Which component would be needed to complete the configuration?

A. Authorization rule

B. Authorization profile

C. Authentication policy

D. Authentication profile

Answer: D

Question: 247

A network engineer is in the predeployment discovery phase of a Cisco ISE deployment and must discover the network. There is an existing network management system in the network.

Which type of probe must be configured to gather the information?

A. RADIUS

B. NMAP

C. NetFlow

D. SNMP

Answer: D

Question: 248

A network engineer must configure a centralized Cisco ISE solution for wireless guest access with users in different time zones. The guest account activation time must be independent of the user time zone, and the guest account must be enabled automatically when the user self-registers on the guest portal.

Which option in the time profile settings must be selected to meet the requirement?

A. Select FromFirstLogin from the Account Type dropdown.

B. Select FromCreation from the Account Type dropdown.

C. Set the Maximum Account Duration to 1 Day.

D. Set the Duration field to 24:00:00.

Answer: B

Question: 249

What is the difference between how RADIUS and TACACS+ handle encryption?

A. RADIUS encrypts only the username and password fields, whereas TACACS+ encrypts the entire packet.

B. RADIUS encrypts the entire packet, whereas TACACS+ only encrypts the password field.

C. RADIUS only encrypts the password field, whereas TACACS+ encrypts the payload of packet.

D. RADIUS encrypts the entire packet, whereas TACACS+ encrypts only the username and password fields.

Answer: C

Question: 250

An engineer must use Cisco ISE to provide network access to endpoints that cannot support 802.1X. The endpoint MAC addresses must be allowlisted by configuring an endpoint identity group. These configurations were performed:

Configured an identity group named allowlist

Configured the endpoints to use the MAC address of incompatible 802.1X devices

Added the endpoints to the allowlist identity group

Configured an authentication policy for MAB users

What must be configured?

A. Authorization profile that has the PermitAccess permission and matches the allowlist identity group

B. Authentication profile that has the PermitAccess permission and matches the allowlist identity group

C. Authorization policy that has the PermitAccess permission and matches the allowlist identity group

D. Logical profile that matches the allowlist identity group based on the configured policy

Answer: C

Question: 251

An engineer is assigned to enhance security across the campus network. The task is to enable MAB across all access switches in the network. Which command must be entered on the switch to enable MAB?

A. Switch(config-if)# mab

B. Switch(config)# mab

C. Switch# authentication port-control auto

D. Switch(config)# authentication port-control auto

Answer: A

Question: 252

Which controller option allows a user to switch from the provisioning SSID to the employee SSID after registration?

A. AP SSID Fallback

B. AAA Override

C. Fast SSID Change

D. User Idle Timeout

Answer: C

Question: 253

An engineer is deploying a new Cisco ISE environment for a company. The company wants the deployment to use TACACS+. The engineer verifies that Cisco ISE has a Device Administration license. What must be configured to enable TACACS+ operations?

A. Device Administration Work Center

B. Device Admin service

C. Device Administration Deployment settings

D. Device Admin Policy Sets settings

Answer: B

Question: 254

Which two VMware features are supported on a Cisco ISE virtual appliance? (Choose two.)

A. multivendor integration

B. VM hardware version 7+

C. VM snapshots

D. OVF support

E. VM cold migration

Answer: B, D

Question: 255

Which nodes are supported in a distributed Cisco ISE deployment?

A. Policy Service nodes for session failover

B. Monitoring nodes for PxGrid services

C. Administration nodes for session failover

D. Policy Service nodes for automatic failover

Answer: B, D

Question: 256

A network engineer must enable a profiling probe. The profiling must take details through the Active Directory. Where in the Cisco ISE interface would the engineer enable the probe?

A. Policy > Policy Elements > Profiling

B. Administration > Deployment > System > Profiling

C. Policy > Deployment > System > Profiling

D. Administration > System > Deployment > Profiling

Answer: D

Question: 257

On which port does Cisco ISE present the Admin certificate for posture and client provisioning?

A. TCP/8000

B. TCP/8080

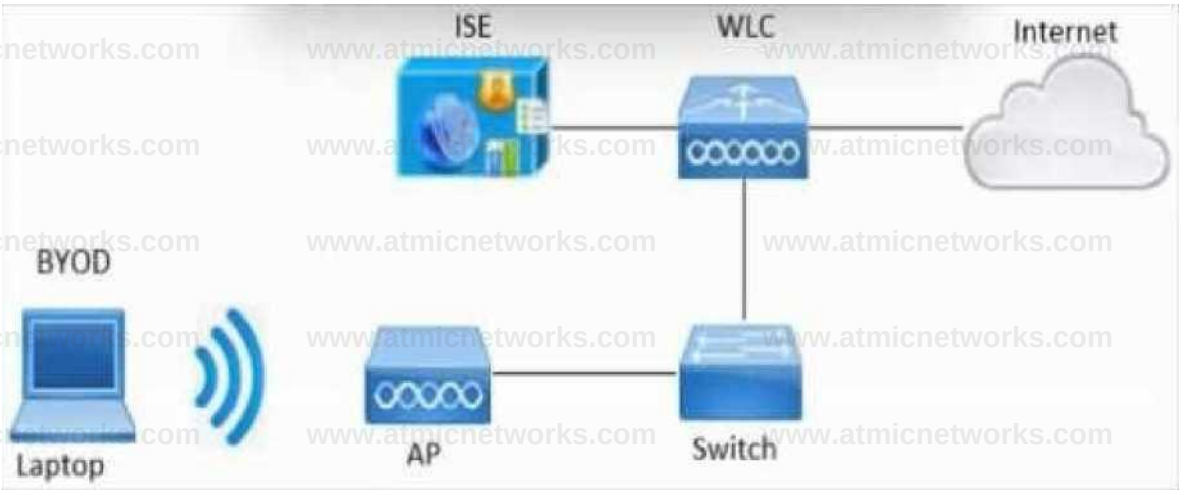
C. TCP/8905

D. TCP/8999

Answer: D

Question: 258

Refer to exhibit.



Refer to the exhibit. An engineer must configure BYOD in Cisco ISE. A single SSID must be used to allow BYOD devices to connect to the network. These configurations have been performed on Wireless LAN Controller already:

RADIUS server

BYOD-Dot1x SSID

Which two configurations must be done in Cisco ISE to meet the requirement? (Choose two.)

A. FlexConnect ACL

B. External identity source

C. Authentication policy

D. Redirect ACL

E. Profiling policy

Answer: C, D

Question: 259

An engineer must use Cisco ISE profiler services to provide network access to Cisco IP phones that cannot support 802.1X. Cisco ISE is configured to use the access switch device sensor information — system-description and platform-type — to profile Cisco IP phones and allow access.

Which two protocols must be configured on the switch to complete the configuration? (Choose two.)

A. LLDP

B. CDP

C. EAPOL

D. SNMP

E. STP

Answer: A, B

Question: 260

An engineer is deploying Cisco ISE in a network that contains an existing Cisco Secure Firewall AS

A. The customer requested that Cisco TrustSec be configured so that Cisco ISE and the firewall can share SGT information.

Which protocol must be configured on Cisco ISE to meet the requirement?

A. PAC

B. SXP

C. RADIUS

D. pxGrid

Answer: B

Question: 261

What is a difference between RADIUS versus TACACS+ with regards to packet encryption?

A. TACACS+ encrypts the entire body of the packet, and RADIUS encrypts the username and password in the access-request packet.

B. RADIUS encrypts the entire body of the packet, and TACACS+ encrypts the username and password in the access-request packet.

C. RADIUS encrypts the entire body of the packet, and TACACS+ encrypts only the password in the access-request packet.

D. TACACS+ encrypts the entire body of the packet, and RADIUS encrypts only the password in the access-request packet.

Answer: D

Explanation:

Question: 262

A network engineer is in the predeployment discovery phase o! a Cisco ISE deployment and must discover the network. There is an existing network management system in the network. Which type of probe must be configured to gather the information?

A. NetFlow

B. RADIUS

C. SNMP

D. NMAP

Answer: C

Explanation:

Question: 263

An administrator plans to use Cisco ISE to deploy posture policies to assess Microsoft Windows endpoints that run Cisco Secure Client. The administrator wants to minimize the occurrence of messages related to unknown posture profiles if Cisco ISE fails to determine the posture of the endpoint. Secure Client is deployed to all the endpoints. and all the required Cisco ISE authentication, authorization, and posture policy configurations were performed. Which action must be taken next to complete the configuration?

A. Install the latest version of the Secure Client client on the endpoints.

B. Enable Cisco ISE posture on Secure Client configuration.

C. Configure a native supplicant on the endpoints to support the posture policies.

D. Install the compliance module on the endpoints.

Answer: D

Explanation:

Question: 264

An engineer must organize endpoints in a Cisco ISE identity management store to improve the operational management of IP phone endpoints. The endpoints must meet these requirements:

- classify endpoints for finance, sales, and marketing departments
- tag each endpoint as profiled

Which action organizes the endpoints?

A. Create an endpoint identity group for each department with the IP phone parent group.

B. Create an endpoint identity group for each department with the profiled parent group.

C. Add a tag for the endpoints of each department and add an endpoint to profiled group.

D. Add a tag for the endpoints of each department and use the identity group filter.

Answer: B

Explanation:

Question: 265

Which default "guest type" is included with Cisco ISE?

A. visitors

B. sponsor

C. guest

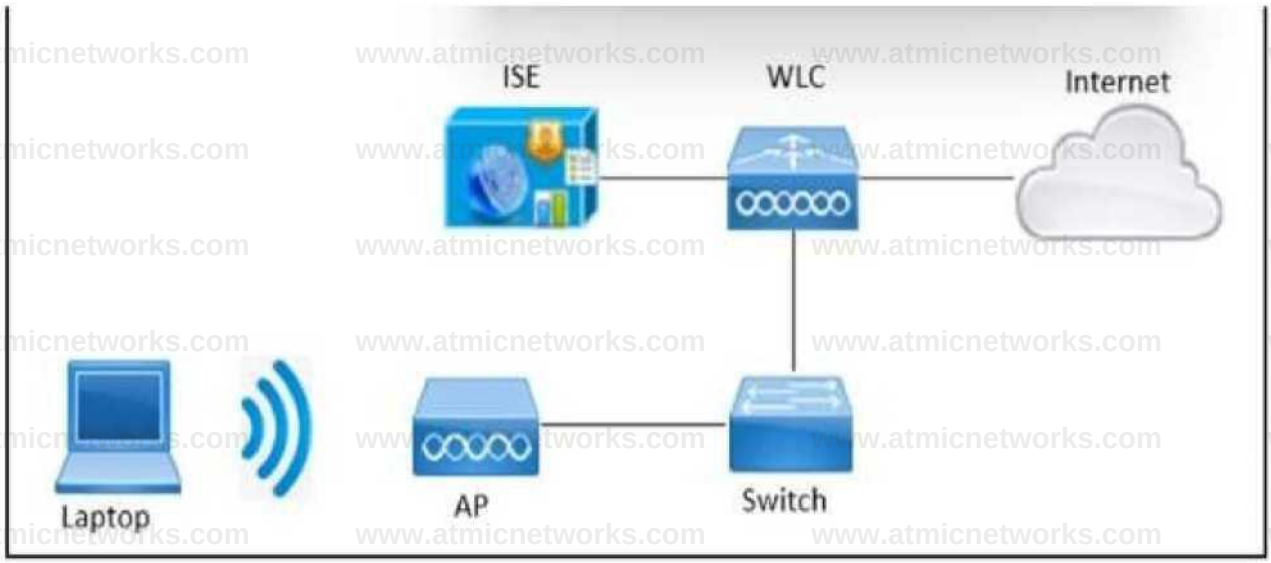
D. contractor

Answer: C

Explanation:

Question: 266

Refer to the exhibit.



Refer to the exhibit. An engineer needs to configure central web authentication on the Cisco Wireless LAN Controller to use Cisco ISE for all guests connected to the wireless network. The components are configured already:

- Cisco Wireless LAN Controller is fully configured
- authorization profile on the Cisco ISE
- authentication policy on the Cisco ISE

Which component would be configured next on Cisco ISE?

A. authorization policy

B. authentication profile

C. accounting profile

D. authorization rule

Answer: A

Explanation:

Question: 267

An engineer is deploying a new guest WLAN for a company. The company wants this WLAN to use a sponsored guest portal for secure guest access. The wireless LAN controller must direct the guests to a web page on Cisco ISE for authentication. Which type of authentication must be configured for the guest portal in Cisco ISE?

A. EWA

B. DWA

C. CWA

D. web portal

Answer: C

Explanation:

Question: 268

What is the Microsoft security policy recommendation (or fast user switching in Cisco ISE?

A. Disable BYOD posture agent.

B. Enable fast user switching.

C. Disable fast user switching.

D. Enable Cisco Secure Client posture agent.

Answer: C

Explanation:

Question: 269

A network engineer must create a guest portal for wireless guests on Cisco ISE. The guest users must not be able to create accounts; however, the portal should require a username and password to connect. Which portal type must be created in Cisco ISE to meet the requirements?

A. Sponsored Guest Access

B. Self Registered Guest Access

C. Custom Guest Portal

D. Hotspot Guest Access

Answer: A

Explanation:

Question: 270

An administrator must deploy the Cisco Secure Client posture agent to employee endpoints that access a wireless network by using URL redirection in Cisco ISE. The compliance module must be downloaded from Cisco and uploaded to the Cisco ISE client provisioning resource. What must be used to upload the compliance module?

A. Secure Client configuration

B. agent resources from the local disk

C. Secure Client posture profile

D. Client Provisioning Portal

Answer: B

Explanation:

Question: 271

An engineer is configuring a new Cisco ISE node. The Cisco ISE must make authorization decisions based on the threat and vulnerability attributes received from the threat and vulnerability adapters. Which persona must be enabled?

A. Policy Service

B. Monitoring

C. pxGrid

D. Administration

Answer: C

Explanation:

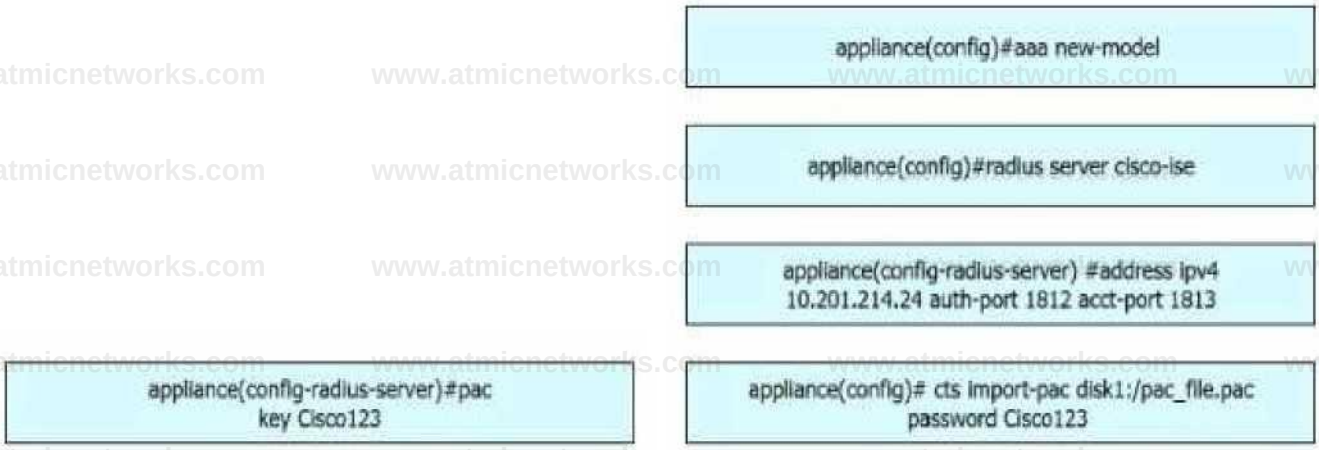
Question: 272

DRAG DROP

A security engineer configures a Cisco Catalyst switch to use Cisco TrustSec. The engineer must define the PAC key to authenticate the switch to Cisco IISE. Drag and drop the commands from the left into sequence on the right. Not all options are used.

Answer:

Explanation:



Question: 273

An administrator is responsible for configuring network access for a temporary network printer. The administrator must only use the printer MAC address 50:89:65: 18:8: AB for authentication. Which authentication method will accomplish the task?

A. Posturing

B. Profiling

C. MAB

D. 802.1x

Answer: C

Explanation:

Question: 274

A network engineer must configure a centralized Cisco ISE solution for wireless guest access with users in different time zones. The guest account activation time must be independent of the user time zone, and the guest account must be enabled automatically when the user self-registers on the guest portal. Which option in the time profile settings must be selected to meet the requirement?

A. Select FromFirstLogin from the Account Type dropdown.

B. Select FromCreation from the Account Type dropdown.

C. Set the Maximum Account Duration to 1 Day.

D. Set the Duration field to 24:00:00.

Answer: B

Explanation:

Question: 275

Wireless network users authenticate to Cisco ISE using 802.1X through a Cisco Catalyst switch. An engineer must create an updated configuration to assign a security group tag to the user's traffic using inline tagging to prevent

unauthenticated users from accessing a restricted server. The configurations were performed:

- configured Cisco ISE as a Cisco TrustSec AAA server
- configured the switch as a RADIUS device in Cisco ISE
- configured the wireless LAN controller as a TrustSec device in Cisco ISE
- created a security group tog for the wireless users
- created a certificate authentication profile
- created an identity source sequence
- assigned an appropriate security group tag to the wireless users
- defined security group access control lists to specify an egress policy
- enforced the access control lists on the TrustSec policy matrix in Cisco ISE
- configured TrustSec on the switch
- configured TrustSec on the wireless LAN controller

Which two actions must be taken to complete the configuration? (Choose two.)

A. Configure Security Group Tag Exchange Protocol on the wireless LAN controller.

B. Configure Security Group Tag Exchange Protocol to distribute IP to security group tags on Cisco ISE.

C. Configure inline tag propagation on the switch and wireless LAN controller.

D. Create static IP-to-SGT mapping for the restricted web server.

E. Configure Security Group Tag Exchange Protocol on the switch.

Answer: C, E

Explanation:

Question: 276

An engineer is starting to implement a wired 802.1X project throughout the campus. The task is to ensure that the authentication procedure is disabled on the ports but still allows all endpoints to connect to the network. Which port-control option must the engineer configure?

A. pae-disabled

B. force-unauthorized

C. auto

D. force-authorized

Answer: D

Explanation:

Question: 277

Which two external identity stores are supported by Cisco ISE for password types? (Choose two.)

A. LDAP

B. OBDC

C. RADIUS Token Server

D. TACACS+ Token Server

E. SOL

Answer: A, C

Explanation:

Question: 278

An administrator needs to add a new third party network device to be used with Cisco ISE for Guest and BYOD authorizations. Which two features must be configured under Network Device Profile to achieve this? (Choose two.)

A. dACL

B. TACACS

C. URL Redirect

D. SNMP community

E. CoA Type

Answer: C, E

Explanation:

Question: 279

An engineer must use Cisco ISE to provide network access to endpoints that cannot support 802.1X. The endpoint MAC addresses must be allowlisted by configuring an endpoint identity group. These configurations were performed:

- configured an identity group named allowlist
- configured the endpoints to use the MAC address of incompatible 802.1X devices
- added the endpoints to the allowlist identity group
- configured an authentication policy for MAB users What must be configured?

A. authorization profile that has the PermitAccess permission and matches the allowlist identity group

B. logical profile that matches the allowlist identity group based on the configured policy

C. authentication profile that has the PermitAccess permission and matches the allowlist identity group authorization

policy that has the PermitAccess permission and matches the allowlist identity group

D. authorization policy that has the PermitAccess permission and matches the allowtist identity group

Answer: D

Explanation:

Question: 280

An engineer is configuring a new Cisco ISE node. Context-sensitive information must be shared between the Cisco ISE and a Cisco AS

A. Which persona must be enabled?

A. Administration

B. Policy Service

C. pxGrid

D. Monitoring

Answer: C

Explanation:

Question: 281

A network engineer is configuring a Cisco Wireless LAN Controller in order to find out more information about the devices that are connecting. This information must be sent to Cisco ISE to be used in authorization policies. Which profiling mechanism must be configured in the Cisco Wireless LAN Controller to accomplish this task?

A. DNS

B. CDP

C. DHCP

D. ICMP

Answer: B

Explanation:

Question: 282

An engineer is assigned to enhance security across the campus network. The task is to enable MAB across all access switches in the network. Which command must be entered on the switch to enable MAB?

A. Switch# authentication port-control auto

B. Switch{conflg)# mab

C. Switch{config-lf) # mab

D. Switch(config)# authentication port-control auto

Answer: C

Explanation:

Question: 283

The Cisco Wireless LAN Controller and guest portal must be set up in Cisco ISE. These configurations were performed:

- configured all the required Cisco Wireless LAN Controller configurations

- added the wireless controller to Cisco ISE network devices
- created an endpoint identity group
- configured credentials to be sent by email
- configured the SMTP server
- configured an authorization profile with redirection to the guest portal and redirected the access control list
- configured an authentication policy for MAB users
- created an authorization policy

Which two components would be required to complete the configuration? (Choose two.)

A. sponsor group

B. hotspot guest portal

C. sponsor portal

D. self-registered guest portal

E. guest type

Answer: C, E

Explanation:

Question: 284

An engineer is configuring Central Web Authentication in Cisco ISE to provide guest access. When an authentication rule is configured in the Default Policy Set for the Wired_MAB or Wireless_MAB conditions, what must be selected for the "if user not found" setting?

A. CONTINUE

B. REJECT

C. ACCEPT

D. DROP

Answer: A

Explanation:

Question: 285

A network security administrator wants to integrate Cisco ISE with Active Directory. Which configuration action must the security administrator take to accomplish the task?

A. Remove Cisco ISE user account from the domain.

B. Remove the ISE machine account from the domain.

C. Join Cisco ISE to the Active Directory domain.

D. Search Active Directory to see if admin user account exists.

Answer: C

Explanation:

Question: 286

A network administrator is configuring a new access switch to use with Cisco ISE for network access control. There is a need to use a centralized server for the reauthentication timers. What must be configured in order to accomplish this task?

A. Configure Cisco ISE to replace the switch configuration with new timers.

B. Configure Cisco ISE to block access after a certain period of time.

C. Issue the authentication timer reauthenticate server command on the switch.

D. Issue the authentication periodic command on the switch.

Answer: C

Explanation:

Question: 287

Which controller option allows a user to switch from the provisioning SSID to the employee SSID after registration?

A. User Idle Timeout

B. Fast SSID Change

C. AP SSID Fallback

D. AAA Override

Answer: B

Explanation:

Question: 288

An administrator must provide wired network access to unidentified Cisco devices that fail 802.1X authentication. Cisco ISE profiling services must be configured to gather Cisco Discovery Protocol and LLDP endpoint information from a Cisco switch. These configurations were performed:

- configured switches to accept SNMP queries from Cisco ISE
- enabled Cisco Discovery Protocol and LLDP on the switches

- added the switch as a NAD to Cisco ISE

What must be enabled to complete the configuration?

A. SNMP traps on the switch

B. SNMP MIBs in Cisco ISE

C. SNMP Trap probe in Cisco ISE

D. SNMP Query probe in Cisco ISE

Answer: D

Explanation:

Question: 289

What is an advantage of TACACS+ versus RADIUS authentication when reviewing reports in Cisco ISE?

A. TACACS+ reduces authentication latency, and RADIUS increases latency by adding additional packet headers.

B. TACACS+ performs secure communication with IPsec, and RADIUS uses DTLS encryption.

C. TACACS+ provides command accounting, and RADIUS combines authentication and authorization.

D. TACACS+ uses SSL certificates, and RADIUS does not have encryption.

Answer: C

Explanation:

Question: 290

A Cisco ISE engineer is creating a certificate authentication profile to be used with machine authentication for the network. The engineer wants to be able to compare the user-presented certificate with a certificate stored in Active Directory. What must be done to accomplish this?

A. Configure the user-presented password hash and a hash stored in Active Directory for comparison

B. Add the subject alternative name and the common name to the CAP.

C. Enable the option for performing binary comparison.

D. Use MS-CHAPv2 since it provides machine credentials and matches them to credentials stored in Active Directory

Answer: C

Explanation:

Question: 291

Which nodes are supported in a distributed Cisco ISE deployment?

A. Policy Service nodes tor automatic failover

B. Administration nodes for session failover

C. Monitoring nodes for PxGrid services

D. Policy Service nodes for session failover

Answer: D

Explanation:

Question: 292

What is the default port used by Cisco ISE for NetFlow version 9 probe?

A. UDP 9996

B. UDP 9997

C. UDP 9998

D. UDP 9999

Answer: A

Explanation:

Question: 293

An engineer must use Cisco ISE profiler services to provide network access to Cisco IP phones that cannot support 802.1X. Cisco ISE is configured to use the access switch device sensor information system-description and platform-type to profile Cisco IP phones and allow access. Which two protocols must be configured on the switch to complete the configuration? (Choose two.)

A. CDP

B. EAPOL

C. LLDP

D. SNMP

E. STP

Answer: A, C

Explanation:

Question: 294

An administrator is editing a csv list of endpoints and wants to reprofile some of the devices indefinitely before importing the list into Cisco ISE. Which field and Boolean value must be changed for the devices before the list is reimported?

A. Identity Group Assignment field and Static Assignment field set to the value FALSE

B. Policy Assignment field and Static Assignment field set to the value TRUE

C. Policy Assignment field and Static Assignment field set to the value FALSE

D. Identity Group Assignment field and Static Assignment field set to the value TRUE

Answer: C

Explanation:

Question: 295

Which CLI command must be configured on the switchport to immediately run the MAB process if a non-802.1X capable endpoint connects to the port?

A. authentication order mab dot1x

B. authentication fallback

C. dot1x pae authenticator

D. access-session port-control auto

Answer: A

Explanation:

Question: 296

A network engineer must configure BYOD using Cisco ISE. In the deployment, the users must be able to submit CSR through the end devices. Which two features must be enabled to meet the requirement?

(Choose two.)

A. Define a certificate group tag.

B. A new BYOD portal must be created.

C. A certificate provisioning portal must be configured.

D. Cisco ISE Internal CA service must be enabled.

E. Add SuperAdmin account into portal admin group.

Answer: C, D

Explanation:

Question: 297

An administrator must configure Cisco ISE to send CoA requests to a Cisco switch using SNMP. These configurations were already performed:

enabled SNMP on the switch

added the switch to Cisco ISE

configured a network device profile

configured the NAD port detection method

configured the operation to be performed on the switch port

configured an authorization profile

Which two configurations must be performed to send the CoA requests? (Choose two.)

A. Select the CoA type as SNMP in the network device profile.

B. Configure the SNMP server in Cisco ISE.

C. Configure SNMP authentication in Cisco ISE.

D. Configure a network device group.

E. Configure the switch SNMP settings of the NAD.

Answer: A, E

Explanation:

Question: 298

An engineer is configuring a new Cisco ISE node. The Cisco ISE must make authorization decisions based on the threat and vulnerability attributes received from the threat and vulnerability adapters. Which persona must be enabled?

A. Monitoring

B. Administration

C. pxGrid

D. Policy Service

Answer: C

Explanation:

Question: 299

Which action must be taken before configuring the Secure Client Agent profile when creating the Secure Client configuration for ISE posture services?

A. Create a posture remediation condition policy for the Agent profile.

B. Configure the posture policy for Secure Client posturing module.

C. Create a posture condition that references the Secure Client package.

D. Upload the Secure Client packages and the Secure Client compliance modules.

Answer: D

Explanation:

Question: 300

An engineer must configure guest access on Cisco ISE for company visitors. Which step must be taken on the Cisco ISE PSNs before a guest portal is configured?

A. Enable profiling services.

B. Install SSL certificates.

C. Create a node group.

D. Enable session services.

Answer: D

Explanation:

Question: 301

A Cisco ISE administrator must authenticate users against Microsoft Active Directory. The solution must meet these requirements:

Users and computers must be authenticated.

User groups must be retrieved during authentication.

Which protocol must be added to the allowed protocols on the policy to authenticate the users?

A. EAP-GTC

B. EAP-TLS

C. LEAP

D. MS-CHAPv2

Answer: D

Explanation:

Question: 302

An administrator must provide network access to legacy Windows endpoints with a specific device type and operating system version using Cisco ISE profiler services. The ISE profiler services and access switches must be configured to identify endpoints using the dhcp-class-identifier and parameters-request-list attributes from the DHCP traffic. These configurations were performed:

enabled the DHCP probe in Cisco ISE

configured the Cisco ISE PSN interface to receive DHCP packets

configured the attributes in custom profiling conditions

configured a custom profiling policy

configured an authorization rule with permit access

Which action completes the configuration?

A. Configure the switches to send copies of the DHCP traffic to the Cisco ISE PSN.

B. Configure the Cisco ISE PSN interface to receive SPAN DHCP traffic.

C. Configure the switches to relay DHCP packets to the Cisco ISE PSN.

D. Enable the DHCP SPAN probe in Cisco ISE primary server.

Answer: A

Explanation:

Question: 303

The security engineer for a company has recently deployed Cisco ISE to perform centralized authentication of all network device logins using TACACS+ against the local AD domain. Some of the other network engineers are having a hard time remembering to enter their AD account password instead of the local admin password that they have used for years. The security engineer wants to change the password prompt to "Use Local AD Password:" as a way of providing a hint to the network engineers when logging in. Under which page in Cisco ISE would this change be made?

A. Work Centers > Device Administration > Settings > Connection Settings

B. Work Centers > Device Administration > Ext Id Sources > Advanced Settings

C. The password prompt cannot be changed on a Cisco IOS device

D. Work Centers > Device Administration > Network Resources > Network Devices

Answer: A

Explanation:

Question: 304

Which platform does a Windows-based device download the Network Assistant Manager from?

A. Microsoft app store

B. Cisco Catalyst Switch

C. native OS

D. Cisco ISE

Answer: D

Explanation:

Question: 305

A user misplaces a personal phone and wants to blacklist the device from accessing the company network. The company uses Cisco ISE for corporate and BYOD device authentication. Which action must the user take in Cisco ISE?

A. Sign in to the BYOD portal and mark the device as Lost.

B. Sign in to the My Devices portal and mark the device as Lost.

C. Sign in to the My Devices portal and mark the device as Irrecoverable.

D. Sign in to the BYOD portal and mark the device as Irrecoverable.

Answer: C

Explanation:

Question: 306

What is the difference between how RADIUS and TACACS+ handle encryption?

A. RADIUS encrypts the entire packet, whereas TACACS+ encrypts only the username and password fields.

B. RADIUS encrypts the entire packet, whereas TACACS+ only encrypts the password field.

C. RADIUS only encrypts the password field, whereas TACACS+ encrypts the payload of the packet.

D. RADIUS encrypts only the username and password fields, whereas TACACS+ encrypts the entire packet.

Answer: C

Explanation: