

Cisco.Actualtests.300-208.v2015-07-08-2015.by.Ralph.174.vce

Number: 300-208
Passing Score: 848
Time Limit: 120 min
File Version: 1.0



Implementing Cisco Secure Access Solutions
Version: 6.0

Went through, about 80% of this is new questions when compared to anything else as of 8/10/2015. Good luck!

Exam A

QUESTION 1

Cisco 802.1X phasing enables flexible deployments through the use of open, low-impact, and closed modes. What is a unique characteristic of the most secure mode?

- A. Granular ACLs applied prior to authentication
- B. Per user dACLs applied after successful authentication
- C. Only EAPoL traffic allowed prior to authentication
- D. Adjustable 802.1X timers to enable successful authentication

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 2

A network administrator must enable which protocol extension to utilize EAP-Chaining?

- A. EAP-FAST
- B. EAP-TLS
- C. MSCHAPv2
- D. PEAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 3

In the command 'aaa authentication default group tacacs local', how is the word 'default' defined?

- A. Command set
- B. Group name
- C. Method list
- D. Login type

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 4

Changes were made to the ISE server while troubleshooting, and now all wireless certificate authentications are failing. Logs indicate an EAP failure. What is the most likely cause of the problem?

- A. EAP-TLS is not checked in the Allowed Protocols list
- B. Certificate authentication profile is not configured in the Identity Store
- C. MS-CHAPv2 is not checked in the Allowed Protocols list
- D. Default rule denies all traffic
- E. Client root certificate is not included in the Certificate Store

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 5

The NAC Agent uses which port and protocol to send discovery packets to an ISE Policy Service Node?

- A. tcp/8905
- B. udp/8905
- C. http/80
- D. https/443

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 6

Which two conditions are valid when configuring ISE for posturing? (Choose two.)

- A. Dictionary
- B. member Of
- C. Profile status
- D. File
- E. Service

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 7

Refer to the exhibit.

```
device(config)#aaa new-model
device(config)#tacacs-server host 209.165.200.226
device(config)#tacacs-server host 209.165.200.227
device(config)#tacacs-server key 0 $$50#$$!!1
```

Which three statements about the given configuration are true? (Choose three.)

- A. TACACS+ authentication configuration is complete.
- B. TACACS+ authentication configuration is incomplete.
- C. TACACS+ server hosts are configured correctly.
- D. TACACS+ server hosts are misconfigured.
- E. The TACACS+ server key is encrypted.
- F. The TACACS+ server key is unencrypted.

Correct Answer: BCF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 8

In AAA, what function does authentication perform?

- A. It identifies the actions that the user can perform on the device.
- B. It identifies the user who is trying to access a device.
- C. It identifies the actions that a user has previously taken.
- D. It identifies what the user can access.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 9

Which identity store option allows you to modify the directory services that run on TCP/IP?

- A. Lightweight Directory Access Protocol
- B. RSA SecurID server
- C. RADIUS
- D. Active Directory

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 10

Which term describes a software application that seeks connectivity to the network via a network access device?

- A. authenticator
- B. server
- C. supplicant
- D. WLC

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 11

Cisco ISE distributed deployments support which three features? (Choose three.)

- A. global implementation of the profiler service CoA
- B. global implementation of the profiler service in Cisco ISE
- C. configuration to send system logs to the appropriate profiler node
- D. node-specific probe configuration
- E. server-specific probe configuration
- F. NetFlow probes

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 12

How frequently does the Profiled Endpoints dashlet refresh data?

- A. every 30 seconds
- B. every 60 seconds
- C. every 2 minutes
- D. every 5 minutes

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 13

Which command in the My Devices Portal can restore a previously lost device to the network?

- A. Reset
- B. Found
- C. Reinstate
- D. Request

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 14

What is the first step that occurs when provisioning a wired device in a BYOD scenario?

- A. The smart hub detects that the physically connected endpoint requires configuration and must use MAB to authenticate.
- B. The URL redirects to the Cisco ISE Guest Provisioning portal.
- C. Cisco ISE authenticates the user and deploys the SPW package.
- D. The device user attempts to access a network URL.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 15

Which three features should be enabled as best practices for MAB? (Choose three.)

- A. MD5
- B. IP source guard
- C. DHCP snooping
- D. storm control
- E. DAI
- F. URPF

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 16

When MAB is configured, how often are ports reauthenticated by default?

- A. every 60 seconds
- B. every 90 seconds
- C. every 120 seconds
- D. never

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 17

What is a required step when you deploy dynamic VLAN and ACL assignments?

- A. Configure the VLAN assignment.
- B. Configure the ACL assignment.
- C. Configure Cisco IOS Software 802.1X authenticator authorization.
- D. Configure the Cisco IOS Software switch for ACL assignment.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 18

Which model does Cisco support in a RADIUS change of authorization implementation?

- A. push

- B. pull
- C. policy
- D. security

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 19

An organization has recently deployed ISE with the latest models of Cisco switches, and it plans to deploy Trustsec to secure its infrastructure. The company also wants to allow different network access policies for different user groups (e.g., administrators). Which solution is needed to achieve these goals?

- A. Cisco Security Group Access Policies in order to use SGACLs to control access based on SGTs assigned to different users
- B. MACsec in Multiple-Host Mode in order to open or close a port based on a single authentication
- C. Identity-based ACLs on the switches with user identities provided by ISE
- D. Cisco Threat Defense for user group control by leveraging Netflow exported from the switches and login information from ISE

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 20

Security Group Access requires which three syslog messages to be sent to Cisco ISE? (Choose three.)

- A. IOS-7-PROXY_DROP
- B. AP-1-AUTH_PROXY_DOS_ATTACK
- C. MKA-2-MACDROP
- D. AUTHMGR-5-MACMOVE
- E. ASA-6-CONNECT_BUILT
- F. AP-1-AUTH_PROXY_FALLBACK_REQ

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 21

Which administrative role has permission to assign Security Group Access Control Lists?

- A. System Admin
- B. Network Device Admin
- C. Policy Admin
- D. Identity Admin

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 22

Refer to the exhibit.

```
asal(config)# time-range WeekendHours
asal(config-time-range)# periodic friday 18:00 to monday 8:00
asal(config)# access-list Outside extended deny ip any object-group vpnserver time-range WeekendHours log
asal(config)# access-group Outside in outside
```

If the given configuration is applied to the object-group vpnserver, during which time period are external users able to connect?

- A. From Friday at 6:00 p.m. until Monday at 8:00 a.m.
- B. From Monday at 8:00 a.m. until Friday at 6:00 p.m.
- C. From Friday at 6:01 p.m. until Monday at 8:01 a.m.
- D. From Monday at 8:01 a.m. until Friday at 5:59 p.m.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 23

Which set of commands allows IPX inbound on all interfaces?

- A. ASA1(config)# access-list IPX-Allow ethertype permit ipx ASA1(config)# access-group IPX-Allow in interface global
- B. ASA1(config)# access-list IPX-Allow ethertype permit ipx ASA1(config)# access-group IPX-Allow in interface inside
- C. ASA1(config)# access-list IPX-Allow ethertype permit ipx ASA1(config)# access-group IPX-Allow in interface outside
- D. ASA1(config)# access-list IPX-Allow ethertype permit ipx ASA1(config)# access-group IPX-Allow out interface global

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 24

Which command enables static PAT for TCP port 25?

- A. nat (outside,inside) static 209.165.201.3 209.165.201.226 eq smtp
- B. nat static 209.165.201.3 eq smtp
- C. nat (inside,outside) static 209.165.201.3 service tcp smtp smtp
- D. static (inside,outside) 209.165.201.3 209.165.201.226 netmask 255.255.255.255

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 25

Which command is useful when troubleshooting AAA Authentication between a Cisco router and the AAA server?

- A. test aaa-server test cisco cisco123 all new-code
- B. test aaa group7 tacacs+ auth cisco123 new-code
- C. test aaa group tacacs+ cisco cisco123 new-code

D. test aaa-server tacacs+ group7 cisco cisco123 new-code

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 26

In a multi-node ISE deployment, backups are not working on the MnT node. Which ISE CLI option would help mitigate this issue?

- A. repository
- B. ftp-url
- C. application-bundle
- D. collector

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 27

Which command can check a AAA server authentication for server group Group1, user cisco, and password cisco555 on a Cisco ASA device?

- A. ASA# test aaa-server authentication Group1 username cisco password cisco555
- B. ASA# test aaa-server authentication group Group1 username cisco password cisco555
- C. ASA# aaa-server authorization Group1 username cisco password cisco555
- D. ASA# aaa-server authentication Group1 roger cisco555

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 28

Which statement about system time and NTP server configuration with Cisco ISE is true?

- A. The system time and NTP server settings can be configured centrally on the Cisco ISE.
- B. The system time can be configured centrally on the Cisco ISE, but NTP server settings must be configured individually on each ISE node.
- C. NTP server settings can be configured centrally on the Cisco ISE, but the system time must be configured individually on each ISE node.
- D. The system time and NTP server settings must be configured individually on each ISE node.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 29

Wireless client supplicants attempting to authenticate to a wireless network are generating excessive log messages. Which three WLC authentication settings should be disabled? (Choose three.)

- A. RADIUS Server Timeout
- B. RADIUS Aggressive-Failover
- C. Idle Timer
- D. Session Timeout
- E. Client Exclusion
- F. Roaming

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 30

Which two authentication stores are supported to design a wireless network using PEAP EAP- MSCHAPv2 as the authentication method? (Choose two.)

- A. Microsoft Active Directory
- B. ACS
- C. LDAP
- D. RSA Secure-ID
- E. Certificate Server

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 31

What is another term for 802.11i wireless network security?

- A. 802.1x
- B. WEP
- C. TKIP
- D. WPA
- E. WPA2

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 32

Which two EAP types require server side certificates? (Choose two.)

- A. EAP-TLS
- B. PEAP
- C. EAP-MD5
- D. LEAP
- E. EAP-FAST
- F. MSCHAPv2

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 33

Where is client traffic decrypted in a controller-based wireless network protected with WPA2 Security?

- A. Access Point
- B. Switch
- C. Wireless LAN Controller
- D. Authentication Server

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 34

Which setting provides the best security for a WLAN and authenticates users against a centralized directory store?

- A. WPA2 AES-CCMP and 801.X authentication
- B. WPA2 AES-CCMP and PSK authentication
- C. WPA2 TKIP and PSK authentication
- D. WPA2 TKIP and 802.1X authentication

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 35

What is a feature of Cisco WLC and IPS synchronization?

- A. Cisco WLC populates the ACLs to prevent repeat intruder attacks.
- B. The IPS automatically send shuns to Cisco WLC for an active host block.
- C. Cisco WLC and IPS synchronization enables faster wireless access.
- D. IPS synchronization uses network access points to provide reliable monitoring.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 36

Which two components are required to connect to a WLAN network that is secured by EAP-TLS authentication? (Choose two.)

- A. Kerberos authentication server
- B. AAA/RADIUS server
- C. PSKs
- D. CA server

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 37

Which statement about Cisco Management Frame Protection is true?

- A. It enables stations to remain in power-save mode, except at specified intervals to receive data from the access point.
- B. It detects spoofed MAC addresses.
- C. It identifies potential RF jamming attacks.
- D. It protects against frame and device spoofing.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 38

Which three statements about the Cisco wireless IPS solution are true? (Choose three.)

- A. It enables stations to remain in power-save mode, except at specified intervals to receive data from the access point.

- B. It detects spoofed MAC addresses.
- C. It identifies potential RF jamming attacks.
- D. It protects against frame and device spoofing.
- E. It allows the WLC to failover because of congestion.

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 39

In a basic ACS deployment consisting of two servers, for which three tasks is the primary server responsible? (Choose three.)

- A. configuration
- B. authentication
- C. sensing
- D. policy requirements
- E. monitoring
- F. repudiation

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 40

In a split ACS deployment with primary and secondary servers, which three statements about AAA load handling are true? (Choose three.)

- A. During normal operations, each server processes the full workload of both servers.
- B. If a AAA connectivity problem occurs, the servers split the full load of authentication requests.
- C. If a AAA connectivity problem occurs, each server processes the full workload of both servers.
- D. During normal operations, the servers split the full load of authentication requests.
- E. During normal operations, each server is used for specific operations, such as device administration and network admission.
- F. The primary servers are used to distribute policy information to other servers in the enterprise.

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 41

Which three personas can a Cisco ISE assume in a deployment? (Choose three.)

- A. connection
- B. authentication
- C. administration
- D. testing
- E. policy service
- F. monitoring

Correct Answer: CEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 42

Which three components comprise the Cisco ISE profiler? (Choose three.)

- A. the sensor, which contains one or more probes
- B. the probe manager
- C. a monitoring tool that connects to the Cisco ISE
- D. the trigger, which activates ACLs
- E. an analyzer, which uses configured policies to evaluate endpoints
- F. a remitter tool, which fails over to redundant profilers

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 43

Which three statements about the Cisco ISE profiler are true? (Choose three.)

- A. It sends endpoint data to AAA servers.
- B. It collects endpoint attributes.
- C. It stores MAC addresses for endpoint systems.
- D. It monitors and polices router and firewall traffic.
- E. It matches endpoints to their profiles.
- F. It stores endpoints in the Cisco ISE database with their profiles.

Correct Answer: BEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 44

From which location can you run reports on endpoint profiling?

- A. Reports > Operations > Catalog > Endpoint
- B. Operations > Reports > Catalog > Endpoint
- C. Operations > Catalog > Reports > Endpoint
- D. Operations > Catalog > Endpoint

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 45

Which two services are included in the Cisco ISE posture service? (Choose two.)

- A. posture administration
- B. posture run-time
- C. posture monitoring
- D. posture policing

E. posture catalog

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 46

What is a requirement for posture administration services in Cisco ISE?

- A. at least one Cisco router to store Cisco ISE profiling policies
- B. Cisco NAC Agents that communicate with the Cisco ISE server
- C. an ACL that points traffic to the Cisco ISE deployment
- D. the advanced license package must be installed

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 47

Which two statements about Cisco NAC Agents that are installed on clients that interact with the Cisco ISE profiler are true? (Choose two.)

- A. They send endpoint data to AAA servers.
- B. They collect endpoint attributes.
- C. They interact with the posture service to enforce endpoint security policies.
- D. They block access from the network through noncompliant endpoints.
- E. They store endpoints in the Cisco ISE with their profiles.
- F. They evaluate clients against posture policies, to enforce requirements.

Correct Answer: CF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 48

What steps must you perform to deploy a CA-signed identify certificate on an ISE device?

- A. 1. Download the CA server certificate.
2. Generate a signing request and save it as a file.
3. Access the CA server and submit the ISE request.
4. Install the issued certificate on the ISE.
- B. 1. Download the CA server certificate.
2. Generate a signing request and save it as a file.
3. Access the CA server and submit the ISE request.
4. Install the issued certificate on the CA server.
- C. 1. Generate a signing request and save it as a file.
2. Download the CA server certificate.
3. Access the ISE server and submit the CA request.
4. Install the issued certificate on the CA server.
- D. 1. Generate a signing request and save it as a file.
2. Download the CA server certificate.
3. Access the CA server and submit the ISE request.
4. Install the issued certificate on the ISE.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 49

What implementation must be added to the WLC to enable 802.1X and CoA for wireless endpoints?

- A. the ISE
- B. an ACL
- C. a router
- D. a policy server

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 50

What are the initial steps must you perform to add the ISE to the WLC?

- A. 1. With a Web browser, establish an HTTP connection to the WLC pod.
2. Navigate to Administration > Authentication > New.
3. Enter server values to begin the configuration.
- B. 1. With a Web browser, establish an FTP connection to the WLC pod.
2. Navigate to Security > Administration > New.
3. Add additional security features for FTP authentication.
- C. 1. With a Web browser, establish an HTTP connection to the WLC pod.
2. Navigate to Authentication > New.
3. Enter ACLs and Authentication methods to begin the configuration.
- D. 1. With a Web browser connect, establish an HTTPS connection to the WLC pod.
2. Navigate to Security > Authentication > New.
3. Enter server values to begin the configuration.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 51

Which command configures console port authorization under line con 0?

- A. authorization default|WORD
- B. authorization exec line con 0|WORD
- C. authorization line con 0|WORD
- D. authorization exec default|WORD

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 52

Which two statements about administrative access to the ACS Solution Engine are true? (Choose two.)

- A. The ACS Solution Engine supports command-line connections through a serial-port connection.
- B. For GUI access, an administrative GUI user must be created with the add-guiadmin command.
- C. The ACS Solution Engine supports command-line connections through an Ethernet interface.
- D. An ACL-based policy must be configured to allow administrative-user access.
- E. GUI access to the ACS Solution Engine is not supported.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 53

What is the purpose of the Cisco ISE Guest Service Sponsor Portal?

- A. It tracks and stores user activity while connected to the Cisco ISE.
- B. It securely authenticates guest users for the Cisco ISE Guest Service.
- C. It filters guest users from account holders to the Cisco ISE.
- D. It creates and manages Guest User accounts.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 54

What is the effect of the ip http secure-server command on a Cisco ISE?

- A. It enables the HTTP server for users to connect on the command line.
- B. It enables the HTTP server for users to connect using Web-based authentication.
- C. It enables the HTTPS server for users to connect using Web-based authentication.
- D. It enables the HTTPS server for users to connect on the command line.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 55

When RADIUS NAC and AAA Override are enabled for WLC on a Cisco ISE, which two statements about RADIUS NAC are true? (Choose two.)

- A. It will return an access-accept and send the redirection URL for all users.
- B. It establishes secure connectivity between the RADIUS server and the ISE.
- C. It allows the ISE to send a CoA request that indicates when the user is authenticated.
- D. It is used for posture assessment, so the ISE changes the user profile based on posture result.
- E. It allows multiple users to authenticate at the same time.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 56

What are the initial steps to configure an ACS as a TACACS server?

- A. 1. Choose Network Devices and AAA Clients > Network Resources.
2. Click Create.
- B. 1. Choose Network Resources > Network Devices and AAA Clients.
2. Click Create.
- C. 1. Choose Network Resources > Network Devices and AAA Clients.
2. Click Manage.
- D. 1. Choose Network Devices and AAA Clients > Network Resources.
2. Click Install.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 57

Which two statements about administrative access to the Cisco Secure ACS SE are true? (Choose two.)

- A. The Cisco Secure ACS SE supports command-line connections through a serial-port connection.
- B. For GUI access, an administrative GUI user must be created by using the add-guiadmin command.
- C. The Cisco Secure ACS SE supports command-line connections through an Ethernet interface.
- D. An ACL-based policy must be configured to allow administrative-user access.
- E. GUI access to the Cisco Secure ASC SE is not supported.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 58

When RADIUS NAC and AAA Override are enabled for a WLC on a Cisco ISE, which two statements about RADIUS NAC are true? (Choose two.)

- A. It returns an access-accept and sends the redirection URL for all users.
- B. It establishes secure connectivity between the RADIUS server and the Cisco ISE.
- C. It allows the Cisco ISE to send a CoA request that indicates when the user is authenticated.
- D. It is used for posture assessment, so the Cisco ISE changes the user profile based on posture result.
- E. It allows multiple users to authenticate at the same time.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 59

In the command 'aaa authentication default group tacacs local', how is the word 'default' defined?

- A. Command set
- B. Group name
- C. Method list
- D. Login type

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 60

In an 802.1X authorization process, a network access device provides which three functions? (Choose three.)

- A. Filters traffic prior to authentication
- B. Passes credentials to authentication server
- C. Enforces policy provided by authentication server
- D. Hosts a central web authentication page
- E. Confirms supplicant protocol compliance
- F. Validates authentication credentials

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 61

Which two switchport commands enable MAB and allow non-802.1X capable devices to immediately run through the MAB process? (Choose two.)

- A. authentication order mab dot1x
- B. authentication order dot1x mab
- C. no authentication timer
- D. dot1x timeout tx-period
- E. authentication open
- F. mab

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 62

Which two attributes must match between two Cisco ASA devices to properly enable high availability? (Choose two.)

- A. model, interface configuration, and RAM
- B. major and minor software release
- C. tcp dead-peer detection protocol
- D. 802.1x authentication identity

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 63

What are two client-side requirements of the NAC Agent and NAC Web Agent installation? (Choose two.)

- A. Administrator workstation rights
- B. Active Directory Domain membership
- C. Allowing of web browser activex installation
- D. WSUS service running

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 64

Which three algorithms should be avoided due to security concerns? (Choose three.)

- A. DES for encryption
- B. SHA-1 for hashing
- C. 1024-bit RSA
- D. AES GCM mode for encryption
- E. HMAC-SHA-1
- F. 256-bit Elliptic Curve Diffie-Hellman

G. 2048-bit Diffie-Hellman

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 65

In the command 'aaa authentication default group tacacs local', how is the word 'default' defined?

- A. Command set
- B. Group name
- C. Method list
- D. Login type

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 66

Which statement about IOS accounting is true?

- A. A named list of AAA methods must be defined.
- B. A named list of accounting methods must be defined.
- C. Authorization must be configured before accounting.
- D. A named list of tracking methods must be defined.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 67

What are the initial steps to configure an ACS as a TACACS server?

- A. 1. Choose Network Devices and AAA Clients > Network Resources.
2. Click Create.
- B. 1. Choose Network Resources > Network Devices and AAA Clients.
2. Click Create.
- C. 1. Choose Network Resources > Network Devices and AAA Clients.
2. Click Manage.
- D. 1. Choose Network Devices and AAA Clients > Network Resources.
2. Click Install.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 68

Which effect does the ip http secure-server command have on a Cisco ISE?

- A. It enables the HTTP server for users to connect on the command line.
- B. It enables the HTTP server for users to connect by using web-based authentication.
- C. It enables the HTTPS server for users to connect by using web-based authentication.
- D. It enables the HTTPS server for users to connect on the command line.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 69

The NAC Agent v4.9.x uses which ports and protocols to communicate with an ISE Policy Service Node?

- A. tcp/8905, http/80, ftp/21
- B. tcp/8905, http/80, https/443
- C. udp/8905, telnet/23, https/443
- D. udp/8906, http/80, https/443

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 70

Which two are valid ISE posture conditions? (Choose two.)

- A. Dictionary
- B. memberOf
- C. Profile status
- D. File
- E. Service

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 71

A network engineer is configuring HTTP based CWA on a switch. Which three configuration elements are required? (Choose three.)

- A. HTTP server enabled
- B. Radius authentication on the port with MAB
- C. Redirect access-list
- D. Redirect-URL
- E. HTTP secure server enabled
- F. Radius authentication on the port with 802.1x
- G. Pre-auth port based access-list

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 72

Which three statements describe differences between TACACS+ and RADIUS? (Choose three.)

- A. RADIUS encrypts the entire packet, while TACACS+ encrypts only the password.
- B. TACACS+ encrypts the entire packet, while RADIUS encrypts only the password.
- C. RADIUS uses TCP, while TACACS+ uses UDP.
- D. TACACS+ uses TCP, while RADIUS uses UDP.
- E. RADIUS uses ports 1812 and 1813, while TACACS+ uses port 49.
- F. TACACS+ uses ports 1812 and 1813, while RADIUS uses port 49

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 73

Which two identity store options allow you to authorize based on group membership? (Choose two).

- A. Lightweight Directory Access Protocol
- B. RSA SecurID server
- C. RADIUS
- D. Active Directory

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 74

What attribute could be obtained from the SNMP query probe?

- A. FQDN
- B. CDP
- C. DHCP class identifier
- D. User agent

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When you configure SNMP settings on the network devices, you must ensure that the Cisco Discovery Protocol is enabled (by default) on all the ports of the network devices. If you disable the Cisco Discovery Protocol on any of the ports on the network devices, then you may not be able to profile properly because you will miss the Cisco Discovery Protocol information of all the connected endpoints.

You can enable the Cisco Discovery Protocol globally by using the `cdp run` command on a network device, and enable the Cisco Discovery Protocol by using the `cdp enable` command on any interface of the network access device. To disable the Cisco Discovery Protocol on the network device and on the interface, use the `no` keyword at the beginning of the commands.

http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_prof_pol.html#pgfId-2071593

QUESTION 75

What is a required configuration step for an 802.1X capable switch to support dynamic VLAN and ACL assignments?

- A. Configure the VLAN assignment.
- B. Configure the ACL assignment.
- C. Configure 802.1X authenticator authorization.
- D. Configure port security on the switch port.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 76

Which network component would issue the CoA?

- A. switch
- B. endpoint
- C. Admin Node
- D. Policy Service Node

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 77

What steps must you perform to deploy a CA-signed identity certificate on an ISE device?

- A. 1. Download the CA server certificate and install it on ISE.
2. Generate a signing request and save it as a file.
3. Access the CA server and submit the CA request.
4. Install the issued certificate on the ISE.
- B. 1. Download the CA server certificate and install it on ISE.
2. Generate a signing request and save it as a file.
"Pass Any Exam. Any Time." - www.actualtests.com 29
3. Access the CA server and submit the CSR.
4. Install the issued certificate on the CA server.
- C. 1. Generate a signing request and save it as a file.
2. Download the CA server certificate and install it on ISE.
3. Access the ISE server and submit the CA request.
4. Install the issued certificate on the CA server.
- D. 1. Generate a signing request and save it as a file.
2. Download the CA server certificate and install it on ISE.
3. Access the CA server and submit the CSR.
4. Install the issued certificate on the ISE.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 78

An organization has recently deployed ISE with Trustsec capable Cisco switches and would like to allow differentiated network access based on user groups. Which solution is most suitable for achieving these goals?

- A. Cyber Threat Defense for user group control by leveraging Netflow exported from the Cisco switches and identity information from ISE
- B. MACsec in Multiple-Host Mode in order to encrypt traffic at each hop of the network infrastructure
- C. Identity-based ACLs preconfigured on the Cisco switches with user identities provided by ISE
- D. Cisco Security Group Access Policies to control access based on SGTs assigned to different user groups

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 79

Which three are required steps to enable SXP on a Cisco ASA? (Choose three).

- A. configure AAA authentication
- B. configure password
- C. issue the aaa authorization command aaa-server group command
- D. configure a peer
- E. configure TACACS
- F. issue the cts sxp enable command

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 80

Which three network access devices allow for static security group tag assignment? (Choose three.)

- A. intrusion prevention system
- B. access layer switch
- C. data center access switch
- D. load balancer
- E. VPN concentrator
- F. wireless LAN controller

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 81

Which option is required for inline security group tag propagation?

- A. Cisco Secure Access Control System
- B. hardware support
- C. Security Group Tag Exchange Protocol (SXP) v4
- D. Cisco Identity Services Engine

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 82

Which two fields are characteristics of IEEE 802.1AE frame? (Choose two.)

- A. destination MAC address
- B. source MAC address
- C. 802.1AE header in EtherType
- D. security group tag in EtherType
- E. integrity check value
- F. CRC/FCS

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 83

Which two options are valid for configuring IEEE 802.1AE MACSec between switches in a TrustSec network? (Choose two.)

- A. manually on links between supported switches
- B. in the Cisco Identity Services Engine
- C. in the global configuration of a TrustSec non-seed switch
- D. dynamically on links between supported switches

- E. in the Cisco Secure Access Control System
- F. in the global configuration of a TrustSec seed switch

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 84

Which three pieces of information can be found in an authentication detail report? (Choose three.)

- A. DHCP vendor ID
- B. user agent string
- C. the authorization rule matched by the endpoint
- D. the EAP method the endpoint is using
- E. the RADIUS username being used
- F. failed posture requirement

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 85

Certain endpoints are missing DHCP profiling data.

Which option describes what can be used to determine if DHCP requests from clients are reaching Cisco ISE?

- A. output of show interface gigabitEthernet 0 from the CLI
- B. output of debug logging all 7 from the CLI
- C. output of show logging application profiler.log from the CLI
- D. the TCP dump diagnostic tool through the GUI
- E. the posture troubleshooting diagnostic tool through the GUI

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 86

Which debug command on a Cisco WLC shows the reason that a client session was terminated?

- A. debug dot11 state enable
- B. debug dot1x packet enable
- C. debug client mac addr
- D. debug dtls event enable
- E. debug ap enable cisco ap

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 87

Which two identity databases are supported when PEAP-MSCHAPv2 is used as EAP type? (Choose two.)

- A. Windows Active Directory
- B. LDAP
- C. RADIUS token server
- D. internal endpoint store
- E. internal user store
- F. certificate authentication profile
- G. RSA SecurID

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 88

Which two Cisco Catalyst switch interface commands allow only a single voice device and a single data device to be connected to the IEEE 802.1X-enabled interface? (Choose two.)

- A. authentication host-mode single-host
- B. authentication host-mode multi-domain
- C. authentication host-mode multi-host
- D. authentication host-mode multi-auth

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 89

Which RADIUS attribute is used primarily to differentiate an IEEE 802.1x request from a Cisco MAB request?

- A. RADIUS Attribute (5) NAS-Port
- B. RADIUS Attribute (6) Service-Type
- C. RADIUS Attribute (7) Framed-Protocol
- D. RADIUS Attribute (61) NAS-Port-Type

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 90

Which authorization method is the Cisco best practice to allow endpoints access to the Apple App store or Google Play store with Cisco WLC software version 7.6 or newer?

- A. dACL
- B. DNS ACL
- C. DNS ACL defined in Cisco ISE
- D. redirect ACL

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 91

Which time allowance is the minimum that can be configured for posture reassessment interval?

- A. 5 minutes
- B. 20 minutes
- C. 60 minutes
- D. 90 minutes

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 92

Which advanced authentication setting is needed to allow an unknown device to utilize Central WebAuth?

- A. If Authentication failed > Continue
- B. If Authentication failed > Drop
- C. If user not found > Continue
- D. If user not found > Reject

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 93

Which option restricts guests from connecting more than one device at a time?

- A. Guest Portal policy > Set Device registration portal limit

- B. Guest Portal Policy > Set Allow only one guest session per user
- C. My Devices Portal > Set Maximum number of devices to register
- D. Multi-Portal Policy > Guest users should be able to do device registration

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 94

In Cisco ISE, which two actions can be taken based on matching a profiler policy? (Choose two).

- A. exception
- B. network scan (NMAP)
- C. delete endpoint
- D. automatically remediate
- E. create matching identity group

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 95

Which statement about the Cisco ISE BYOD feature is true?

- A. Use of SCEP/CA is optional.
- B. BYOD works only on wireless access.
- C. Cisco ISE needs to integrate with MDM to support BYOD.
- D. Only mobile endpoints are supported.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 96

What user rights does an account need to join ISE to a Microsoft Active Directory domain?

- A. Create and Delete Computer Objects
- B. Domain Admin
- C. Join and Leave Domain
- D. Create and Delete User Objects

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 97

A network administrator must enable which protocol to utilize EAP-Chaining?

- A. EAP-FAST
- B. EAP-TLS
- C. MSCHAPv2
- D. PEAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 98

The corporate security policy requires multiple elements to be matched in an authorization policy. Which elements can be combined to meet the requirement?

- A. Device registration status and device activation status
- B. Network access device and time condition
- C. User credentials and server certificate
- D. Built-in profile and custom profile

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 99

A network administrator needs to determine the ability of existing network devices to deliver key BYOD services. Which tool will complete a readiness assessment and outline hardware and software capable and incapable devices?

- A. Prime Infrastructure
- B. Network Control System
- C. Cisco Security Manager
- D. Identity Services Engine

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 100

Which EAP method uses a modified version of the MS-CHAP authentication protocol?

- A. EAP-POTP
- B. EAP-TLS
- C. LEAP
- D. EAP-MD5

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 101

Under which circumstance would an inline posture node be deployed?

- A. When the NAD does not support CoA
- B. When the NAD cannot support the number of connected endpoints
- C. When a PSN is overloaded
- D. To provide redundancy for a PSN

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 102

Which Cisco ISE 1.x protocol can be used to control admin access to network access devices?

- A. TACACS+
- B. RADIUS
- C. EAP
- D. Kerberos

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 103

A user is on a wired connection and the posture status is noncompliant.

Which state will their EPS session be placed in?

- A. disconnected
- B. limited
- C. no access
- D. quarantined

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 104

Which three posture states can be used for authorization rules? (Choose three.)

- A. unknown
- B. known
- C. noncompliant
- D. quarantined
- E. compliant
- F. no access
- G. limited

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 105

Which two Cisco ISE administration options are available in the Default Posture Status setting? (Choose two.)

- A. Unknown
- B. Compliant
- C. FailOpen
- D. FailClose
- E. Noncompliant

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 106

Which two portals can be configured to use portal FQDN? (Choose two.)

- A. admin
- B. sponsor
- C. guest
- D. my devices
- E. monitoring and troubleshooting

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 107

Which five portals are provided by PSN? (Choose five.)

- A. guest
- B. sponsor
- C. my devices
- D. blacklist
- E. client provisioning
- F. admin
- G. monitoring and troubleshooting

Correct Answer: ABCDE

Section: (none)

Explanation

Explanation/Reference:

Answer: A,B,C,D,E

Explanation:

QUESTION 108

When you add a new PSN for guest access services, which two options must be enabled under deployment settings? (Choose two.)

- A. Admin
- B. Monitoring

- C. Policy Service
- D. Session Services
- E. Profiling

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 109

In Cisco ISE, which probe must be enabled to collect profiling data using Device Sensor?

- A. RADIUS
- B. SNMPQuery
- C. SNMPTrap
- D. Network Scan
- E. Syslog

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 110

Which two profile attributes can be collected by a Cisco Catalyst Switch that supports Device Sensor? (Choose two.)

- A. LLDP agent information
- B. user agent
- C. DHCP options
- D. open ports
- E. operating system
- F. trunk ports

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 111

Which two profile attributes can be collected by a Cisco Wireless LAN Controller that supports Device Sensor? (Choose two.)

- A. LLDP agent information
- B. user agent
- C. DHCP options
- D. open ports
- E. CDP agent information
- F. FQDN

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 112

Which statement about Cisco ISE BYOD is true?

- A. Dual SSID allows EAP-TLS only when connecting to the secured SSID.
- B. Single SSID does not require endpoints to be registered.
- C. Dual SSID allows BYOD for guest users.
- D. Single SSID utilizes open SSID to accommodate different types of users.
- E. Single SSID allows PEAP-MSCHAPv2 for native supplicant provisioning.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 113

Which two types of client provisioning resources are used for BYOD implementations? (Choose two.)

- A. user agent
- B. Cisco NAC agent
- C. native supplicant profiles
- D. device sensor
- E. software provisioning wizards

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 114

Which protocol sends authentication and accounting in different requests?

- A. RADIUS
- B. TACACS+
- C. EAP-Chaining
- D. PEAP
- E. EAP-TLS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 115

You enabled the guest session limit feature on the Cisco ISE. However, end users report that the same guest can log in from multiple devices simultaneously.

Which configuration is missing on the network access device?

- A. RADIUS authentication
- B. RADIUS accounting
- C. DHCP required
- D. AAA override

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 116

A properly configured Cisco ISE Policy Service node is not receiving any profile data from a Cisco switch that runs Device Sensor.

Which option is the most likely reason for the failure?

- A. Syslog is configured for the Policy Administration Node.
- B. RADIUS Accounting is disabled.
- C. The SNMP community strings are mismatched.
- D. RADIUS Authentication is misconfigured.
- E. The connected endpoints support CDP but not DHCP.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 117

DRAG DROP

Drag and drop the BYOD user experiences on an iPad on the left into the correct order on the right.	
The CSR is generated on the endpoint and is sent to the Cisco ISE, which forwards it to the SCEP server	1
The user opens a web browser and is redirected to a registration portal	2
A CoA is issued and the endpoint is reconnected to the network with the proper access	3
The endpoint installs a signed certificate that is returned from the Cisco ISE along with the wireless network setting	4
The endpoint authenticates to secure SSID using the username and password	5

A. Authenticate, Opens, Generated, Installs, Issued (Authenticate, User, Forwards, Signed Certificate, to the Network)

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Drag and drop the BYOD user experiences on an iPad on the left into the correct order on the right.

The CSR is generated on the endpoint and is sent to the Cisco ISE, which forwards it to the SCEP server

The user opens a web browser and is redirected to a registration portal

A CoA is issued and the endpoint is reconnected to the network with the proper access

The endpoint installs a signed certificate that is returned from the Cisco ISE along with the wireless network setting

The endpoint authenticates to secure SSID using the username and password

The endpoint authenticates to secure SSID using the username and password

The user opens a web browser and is redirected to a registration portal

The CSR is generated on the endpoint and is sent to the Cisco ISE, which forwards it to the SCEP server

The endpoint installs a signed certificate that is returned from the Cisco ISE along with the wireless network setting

A CoA is issued and the endpoint is reconnected to the network with the proper access

Explanation:

The endpoint authenticates to secure SSID using the username and password

The user opens a web browser and is redirected to a registration portal

The CSR is generated on the endpoint and is sent to the Cisco ISE, which forwards it to the SCEP server

The endpoint installs a signed certificate that is returned from the Cisco ISE along with the wireless network setting

A CoA is issued and the endpoint is reconnected to the network with the proper access

QUESTION 118

Changes were made to the ISE server while troubleshooting, and now all wireless certificate authentications are failing. Logs indicate an EAP failure. What are the two possible causes of the problem? (Choose two.)

- A. EAP-TLS is not checked in the Allowed Protocols list
- B. Client certificate is not included in the Trusted Certificate Store
- C. MS-CHAPv2-is not checked in the Allowed Protocols list
- D. Default rule denies all traffic
- E. Certificate authentication profile is not configured in the Identity Store

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 119

Which action must an administrator take after joining a Cisco ISE deployment to an Active Directory domain?

- A. Choose an Active Directory user.
- B. Configure the management IP address.
- C. Configure replication.
- D. Choose an Active Directory group.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 120

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 121

After an endpoint has completed authentication with MAB, a security violation is triggered because a different MAC address was detected. Which host mode must be active on the port?

- A. single-host mode
- B. multidomain authentication host mode
- C. multiauthentication host mode
- D. multihost mode

Correct Answer: A

Section: (none)

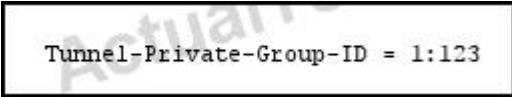
Explanation

Explanation/Reference:

Explanation:

QUESTION 122

Refer to the exhibit.



Tunnel-Private-Group-ID = 1:123

You are configuring permissions for a new Cisco ISE standard authorization profile. If you configure the Tunnel-Private-Group-ID attribute as shown, what does the value 123 represent?

- A. the VLAN ID
- B. the VRF ID
- C. the tunnel ID
- D. the group ID

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 123

Where would a Cisco ISE administrator define a named ACL to use in an authorization policy?

- A. In the conditions of an authorization rule.
- B. In the attributes of an authorization rule.
- C. In the permissions of an authorization rule.
- D. In an authorization profile associated with an authorization rule.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 124

Refer to the exhibit.

Web Login Page

Web Authentication Type: External (Redirect to external server)

Redirect URL after login: http://www.cisco.com

External Webauth URL:

Which URL must you enter in the External Webauth URL field to configure Cisco ISE CWA correctly?

- A. https://ip_address:8443/guestportal/Login.action
- B. https://ip_address:443/guestportal/Welcome.html
- C. https://ip_address:443/guestportal/action=cpp
- D. https://ip_address:8905/guestportal/Sponsor.action

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 125

When you configure an endpoint profiling policy rule, which option describes the purpose of the minimum certainty factor?

- A. It is compared to the total certainty metric of an individual endpoint to determine whether the "Pass Any Exam. Any Time." - www.actualtests.com 47 endpoint can be trusted.
- B. It is compared to the assigned certainty value of an individual endpoint in a device database to determine whether the endpoint can be trusted.
- C. It is used to compare the policy condition to other active policies.
- D. It is used to determine the likelihood that an endpoint is an active, trusted device on the network.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 126

You have configured a Cisco ISE 1.2 deployment for self-registration of guest users. What two options can you select from to determine when the account duration timer begins? (Choose two.)

- A. CreateTime
- B. FirstLogin
- C. BeginLogin
- D. StartTime

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 127

Which error in a redirect ACL can cause the redirection of an endpoint to the provisioning portal to fail?

- A. The redirect ACL is blocking access to ports 80 and 443.
- B. The redirect ACL is applied to an incorrect SVI.
- C. The redirect ACL is blocking access to the client provisioning portal.
- D. The redirect ACL is blocking access to Cisco ISE port 8905.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 128

Where must periodic re-authentication be configured to allow a client to come out of the quarantine state and become compliant?

- A. on the switch port
- B. on the router port
- C. on the supplicant
- D. on the controller

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 129

Which functionality does the Cisco ISE self-provisioning flow provide?

- A. It provides support for native supplicants, allowing users to connect devices directly to the network.
- B. It provides the My Devices portal, allowing users to add devices to the network.
- C. It provides support for users to install the Cisco NAC agent on enterprise devices.
- D. It provides self-registration functionality to allow guest users to access the network.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 130

During client provisioning on a Mac OS X system, the client system fails to renew its IP address. Which change can you make to the agent profile to correct the problem?

- A. Enable the Agent IP Refresh feature.
- B. Enable the Enable VLAN Detect Without UI feature.
- C. Enable CRL checking.
- D. Edit the Discovery Host parameter to use an IP address instead of an FQDN.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 131

Where is dynamic SGT classification configured?

- A. Cisco ISE
- B. NAD
- C. supplicant
- D. RADIUS proxy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 132

What is the function of the SGACL policy matrix on a Cisco TrustSec domain with SGT Assignment?

- A. It determines which access policy to apply to the endpoint.
- B. It determines which switches are trusted within the TrustSec domain.
- C. It determines the path the SGT of the packet takes when entering the Cisco TrustSec domain.
- D. It lists all servers that are permitted to participate in the TrustSec domain.

E. It lists all hosts that are permitted to participate in the TrustSec domain.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 133

You are configuring SGA on a network device that is unable to perform SGT tagging. How can the device propagate SGT information?

- A. The device can use SXP to pass IP-address-to-SGT mappings to a TrustSec-capable hardware peer.
- B. The device can use SXP to pass MAC-address-to-STG mappings to a TrustSec-capable hardware peer.
- C. The device can use SXP to pass MAC-address-to-IP mappings to a TrustSec-capable hardware peer.
- D. The device can propagate SGT information in an encapsulated security payload.
- E. The device can use a GRE tunnel to pass the SGT information to a TrustSec-capable hardware peer.

Correct Answer: A

Section: (none)

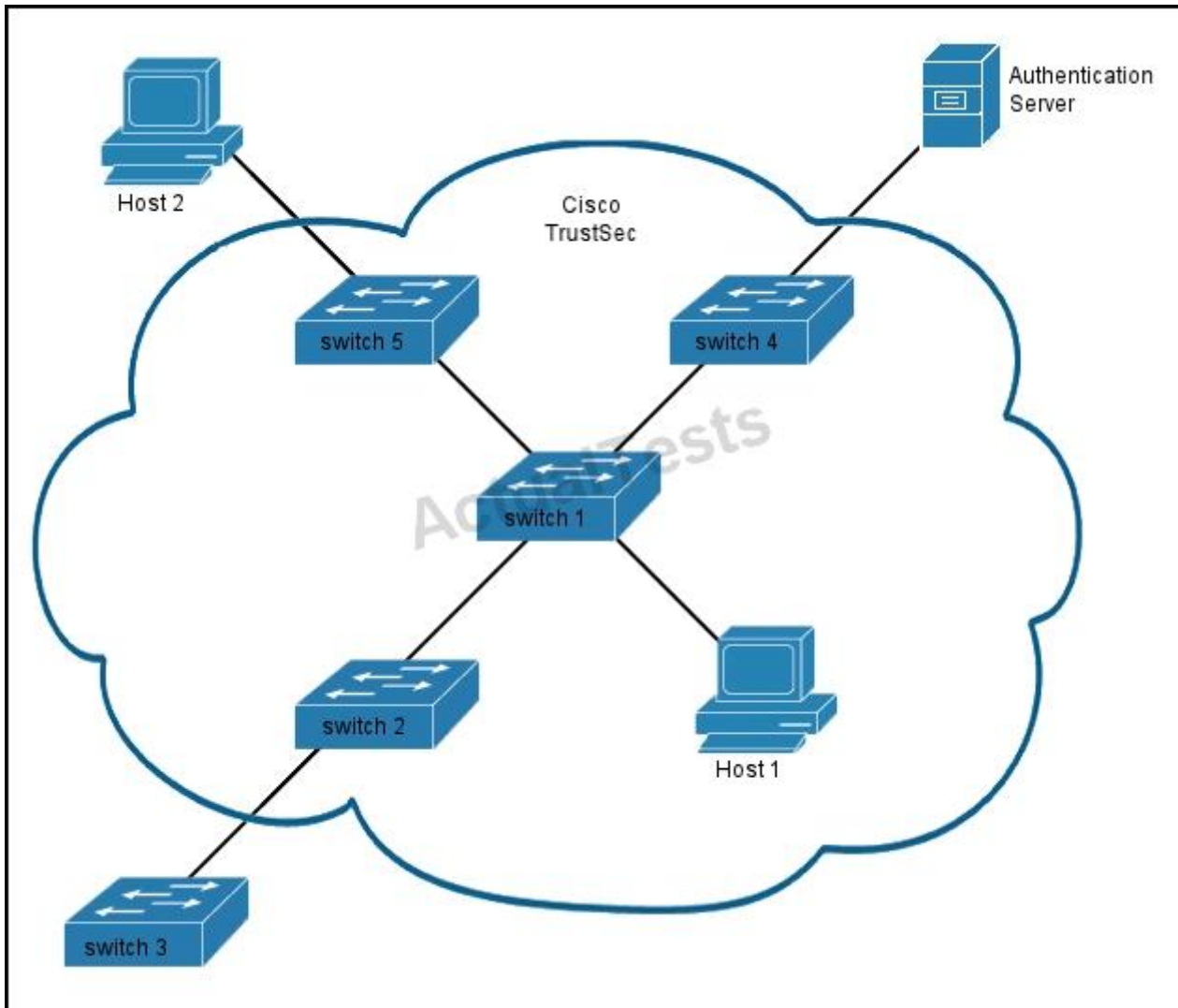
Explanation

Explanation/Reference:

Explanation:

QUESTION 134

Refer to the exhibit.



The links outside the TrustSec area in the given SGA architecture are unprotected. On which two links does EAC take place? (Choose two.)

- A. between switch 2 and switch 3
- B. between switch 5 and host 2
- C. between host 1 and switch 1

- D. between the authentication server and switch 4
- E. between switch 1 and switch 2
- F. between switch 1 and switch 5

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

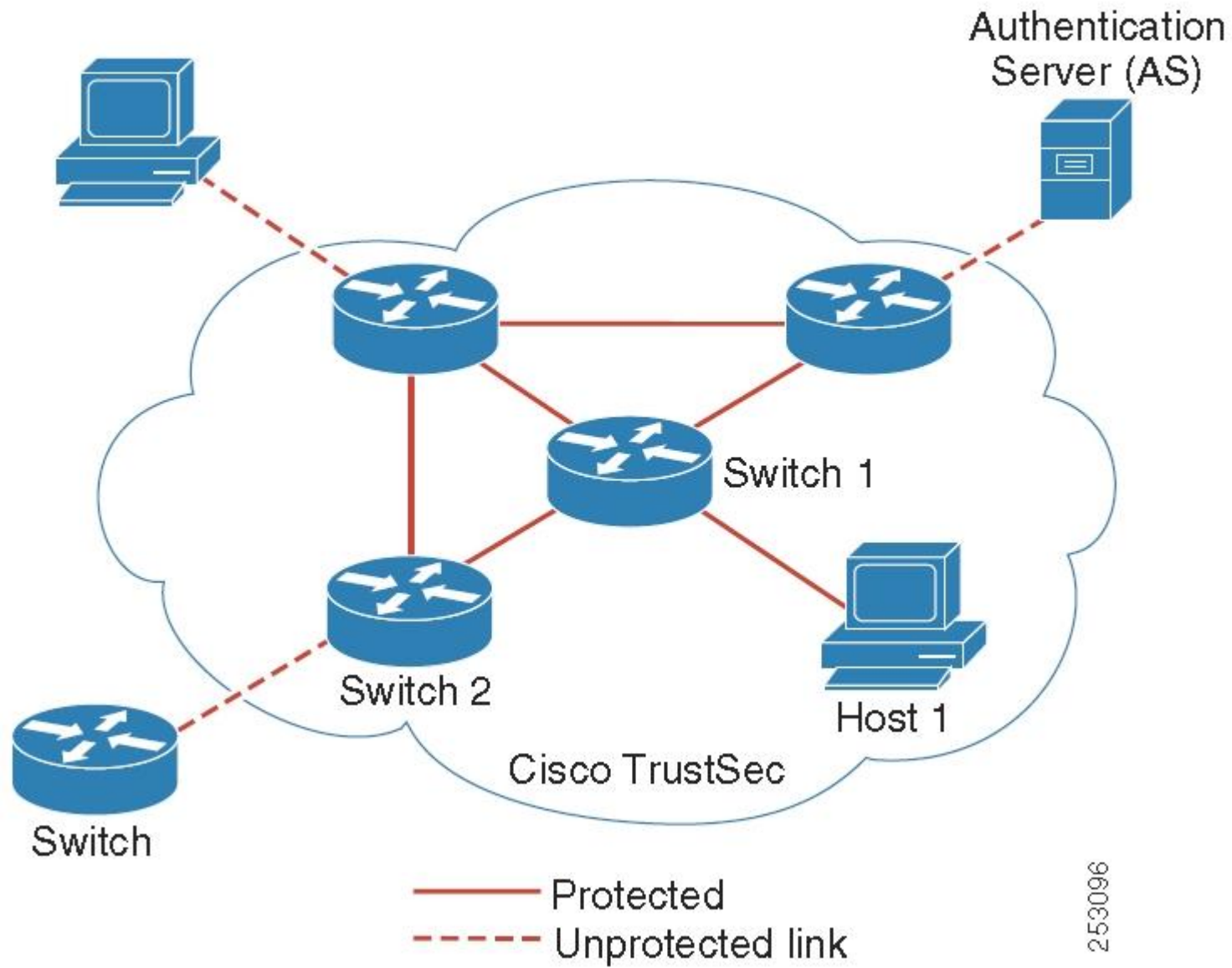
Explanation: In TrustSec networks, packets are filtered at the egress, not the ingress to the network. In TrustSec endpoint authentication, a host accessing the TrustSec domain (endpoint IP address) is associated with a Security Group Tag (SGT) at the access device through DHCP snooping and IP device tracking. The access device transmits that association (binding) through SXP to TrustSec hardware-capable egress devices, which maintain a continually updated table of Source IP to SGT bindings. Packets are filtered

on egress by the TrustSec hardware-capable devices by applying security group ACLS (SGACLs).

Endpoint Admission Control (EAC) access methods for authentication and authorization can include the following:

- 802.1X port-based Authentication
- MAC Authentication Bypass (MAB)
- Web Authentication (WebAuth)

Figure 1-1 ***Cisco TrustSec Network Domain Example***



EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain.

Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).

QUESTION 135

Which three host modes support MACsec? (Choose three.)

- A. multidomain authentication host mode
- B. multihost mode
- C. multi-MAC host mode
- D. single-host mode
- E. dual-host mode
- F. multi-auth host mode

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 136

You are troubleshooting wired 802.1X authentications and see the following error: "Authentication failed: 22040 Wrong password or invalid shared secret." What should you inspect to determine the problem?

- A. RADIUS shared secret
- B. Active Directory shared secret
- C. Identity source sequence
- D. TACACS+ shared secret
- E. Certificate authentication profile

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 137

Refer to the exhibit.

```

Jun 7 04:05:11.350: RADIUS(00000000): Config NAS IP: 10.1.1.100
Jun 7 04:05:11.350: RADIUS(00000000): Config NAS IPv6: ::
Jun 7 04:05:11.350: RADIUS(00000000): sending
Jun 7 04:05:11.350: RADIUS/DECODE(00000000): There is no General DB. Want server details may not be specified
Jun 7 04:05:11.350: RADIUS(00000000): Sending a IPv4 Radius Packet
Jun 7 04:05:11.350: RADIUS(00000000): Send Access-Request to 10.1.1.108:1812 id 1645/61, len 60
Jun 7 04:05:11.350: RADIUS: authenticator 20 40 EF 41 E6 06 9A 11 - E5 3B 64 68 F0 B7 89 9E
Jun 7 04:05:11.351: RADIUS: User-Password [2] 18 *
Jun 7 04:05:11.351: RADIUS: User-Name [1] 10 "jdoe"
Jun 7 04:05:11.351: RADIUS: Service-Type [6] 6 Login [1]
Jun 7 04:05:11.351: RADIUS: NAS-IP-Address [4] 6 10.1.1.100
Jun 7 04:05:11.351: RADIUS(00000000): Started 5 sec timeout
Jun 7 04:05:11.457: RADIUS: Received from id 1645/61 10.1.1.108:1812, Access-Reject, len 20
Jun 7 04:05:11.457: RADIUS: authenticator 6A 48 81 FA BC BC 1D 9B - 31 CA 84 AC 24 8F 0B 8B
Jun 7 04:05:11.457: RADIUS/DECODE(00000000): There is no General DB. Reply server details may not be recorded
Jun 7 04:05:11.457: RADIUS(00000000): Received from id 1645/61

```

You are troubleshooting RADIUS issues on the network and the debug radius command returns the given output. What is the most likely reason for the failure?

- A. An invalid username or password was entered.
- B. The RADIUS port is incorrect.
- C. The NAD is untrusted by the RADIUS server.
- D. The RADIUS server is unreachable.
- E. RADIUS shared secret does not match

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 138

What are two possible reasons why a scheduled nightly backup of ISE to a FTP repository would fail? (Choose two.)

- A. ISE attempted to write the backup to an invalid path on the FTP server.
- B. The ISE and FTP server clocks are out of sync.

- C. The username and password for the FTP server are invalid.
- D. The server key is invalid or misconfigured.
- E. TCP port 69 is disabled on the FTP server.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 139

Which two statements about MAB are true? (Choose two.)

- A. It requires a preexisting database of the MAC addresses of permitted devices.
- B. It is unable to control network access at the edge.
- C. If MAB fails, the device is unable to fall back to another authentication method.
- D. It is unable to link the IP and MAC addresses of a device.
- E. It is unable to authenticate individual users.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 140

Which type of access list is the most scalable that Cisco ISE can use to implement network authorization enforcement for a large number of users?

- A. downloadable access lists
- B. named access lists
- C. VLAN access lists
- D. MAC address access lists

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 141

When you select Centralized Web Auth in the ISE Authorization Profile, which two components host the web authentication portal? (Choose two.)

- A. ISE
- B. the WLC
- C. the access point
- D. the switch
- E. the endpoints

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 142

What is the default posture status for non-agent capable devices, such as Linux and iDevices?

- A. Unknown
- B. Validated
- C. Default
- D. Compliant

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 143

Your guest-access wireless network is experiencing degraded performance and excessive latency due to user saturation. Which type of rate limiting can you implement on your network to correct the problem?

- A. per-device
- B. per-policy
- C. per-access point

- D. per-controller
- E. per-application

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 144

You are installing Cisco ISE on nodes that will be used in a distributed deployment. After the initial bootstrap process, what state will the Cisco ISE nodes be in?

- A. Remote
- B. Policy service
- C. Administration
- D. Standalone

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 145

What three changes require restarting the application service on an ISE node? (Choose three.)

- A. Registering a node.
- B. Changing the primary node to standalone.
- C. Promoting the administration node.
- D. Installing the root CA certificate.
- E. Changing the guest portal default port settings.
- F. Adding a network access device.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 146

Which two Active Directory authentication methods are supported by Cisco ISE? (Choose two.)

- A. MS-CHAPv2
- B. PEAP
- C. PPTP
- D. EAP-PEAP
- E. PPP

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 147

Which statement about a distributed Cisco ISE deployment is true?

- A. It can support up to two monitoring Cisco ISE nodes for high availability.
- B. It can support up to three load-balanced Administration ISE nodes.
- C. Policy Service ISE nodes can be configured in a redundant failover configuration.
- D. The Active Directory servers of Cisco ISE can be configured in a load-balanced configuration.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 148

Which Cisco ISE feature can differentiate a corporate endpoint from a personal device?

- A. EAP chaining
- B. PAC files
- C. authenticated in-band provisioning

D. machine authentication

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 149

Which configuration must you perform on a switch to deploy Cisco ISE in low-impact mode?

- A. Configure an ingress port ACL on the switchport.
- B. Configure DHCP snooping globally.
- C. Configure IP-device tracking.
- D. Configure BPDU filtering.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 150

Which profiling capability allows you to gather and forward network packets to an analyzer?

- A. collector
- B. spanner
- C. retriever
- D. aggregator

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 151

Which network access device feature can you configure to gather raw endpoint data?

- A. Device Sensor
- B. Device Classifier
- C. Switched Port Analyzer
- D. Trust Anchor

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 152

Which method does Cisco prefer to securely deploy guest wireless access in a BYOD implementation?

- A. deploying a dedicated Wireless LAN Controller in a DMZ
- B. configuring a guest SSID with WPA2 Enterprise authentication "Pass Any Exam. Any Time." - www.actualtests.com 58
- C. configuring guest wireless users to obtain DHCP centrally from the corporate DHCP server
- D. disabling guest SSID broadcasting

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 153

Which mechanism does Cisco ISE use to force a device off the network if it is reported lost or stolen?

- A. CoA
- B. dynamic ACLs
- C. SGACL
- D. certificate revocation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 154

You discover that the Cisco ISE is failing to connect to the Active Directory server. Which option is a possible cause of the problem?

- A. NTP server time synchronization is configured incorrectly.
- B. There is a certificate mismatch between Cisco ISE and Active Directory.
- C. NAT statements required for Active Directory are configured incorrectly.
- D. The RADIUS authentication ports are being blocked by the firewall.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 155

Which type of remediation does Windows Server Update Services provide?

- A. automatic remediation
- B. administrator-initiated remediation
- C. redirect remediation
- D. central Web auth remediation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 156

Which three remediation actions are supported by the Web Agent for Windows? (Choose three.)

- A. Automatic Remediation
- B. Message text
- C. URL Link
- D. File Distribution

- E. AV definition update
- F. Launch Program

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 157

What endpoint operating system provides native support for the SPW?

- A. Apple iOS
- B. Android OS
- C. Windows 8
- D. Mac OS X

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 158

Which condition triggers wireless authentication?

- A. NAS-Port-Type is set to IEEE 802.11.
- B. Framed-Compression is set to None.
- C. Service-Type is set to Framed.
- D. Tunnel-Type is set to VLAN.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 159

Which feature enables the Cisco ISE DHCP profiling capabilities to determine and enforce authorization policies on mobile devices?

- A. disabling the DHCP proxy option
- B. DHCP option 42
- C. DHCP snooping
- D. DHCP spoofing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 160

With which two appliance-based products can Cisco Prime Infrastructure integrate to perform centralized management? (Choose two.)

- A. Cisco Managed Services Engine
- B. Cisco Email Security Appliance
- C. Cisco Wireless Location Appliance
- D. Cisco Content Security Appliance
- E. Cisco ISE

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 161

Which two options are EAP methods supported by Cisco ISE? (Choose two.)

- A. EAP-FAST
- B. EAP-TLS
- C. EAP-MS-CHAPv2
- D. EAP-GTC

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 162

You configured wired 802.1X with EAP-TLS on Windows machines. The ISE authentication detail report shows "EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain." What is the most likely cause of this error?

- A. The ISE certificate store is missing a CA certificate.
- B. The Wireless LAN Controller is missing a CA certificate.
- C. The switch is missing a CA certificate.
- D. The Windows Active Directory server is missing a CA certificate.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 163

What type of identity group is the Blacklist identity group?

- A. endpoint
- B. user
- C. blackhole
- D. quarantine
- E. denied systems

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 164

Which feature must you configure on a switch to allow it to redirect wired endpoints to Cisco ISE?

- A. the http secure-server command
- B. RADIUS Attribute 29
- C. the RADIUS VSA for accounting
- D. the RADIUS VSA for URL-REDIRECT

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 165

CORRECT TEXT

The Secure-X company has recently successfully tested the 802.1X authentication deployment using the Cisco Catalyst switch and the Cisco ISEv1.2 appliance. Currently, each employee desktop is connected to an 802.1X enabled switch port and is able to use the Cisco AnyConnect NAM 802.1Xsupplicantto log in and connect to the network.

Currently, a new testing requirement is to add a network printer to the Fa0/19 switch port and have it connect to the network. The network printer does not support 802.1X supplicant. The Fa0/19 switch port is now configured to use 802.1X authentication only.

To support this network printer, the Fa0/19 switch port configuration needs to be edited to enable the network printer to authenticate using its MAC address. The network printer should also be on VLAN 9.

Another network security engineer responsible for managing the Cisco ISE has already per- configured all the requirements on the Cisco ISE, including adding the network printer MAC address to the Cisco ISE endpoint database and etc...

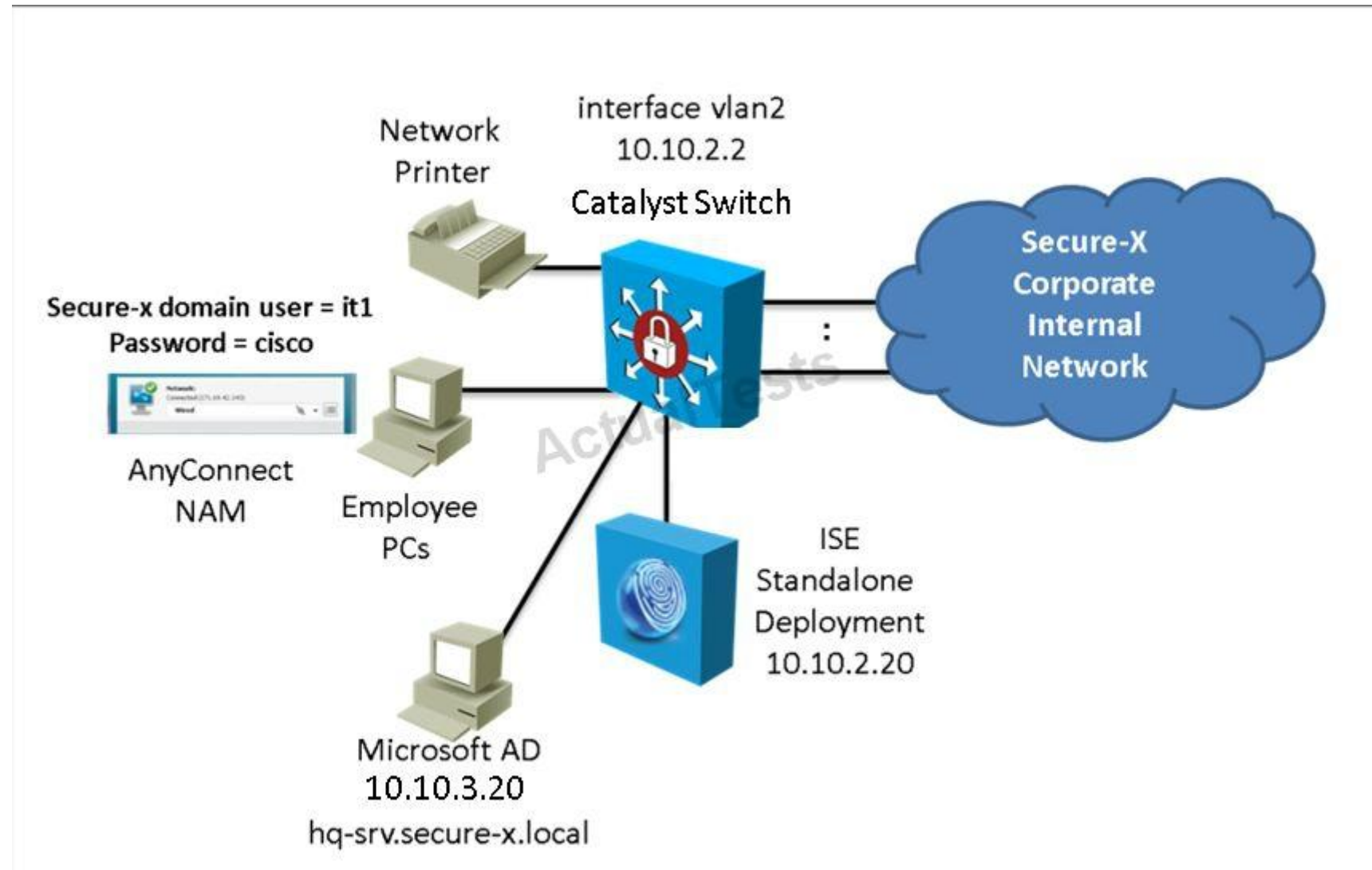
Your task in the simulation is to access the Cisco Catalyst Switch console then use the CLI to:

- Enable only the Cisco Catalyst Switch Fa0/19 switch port to authenticate the network printer using its MAC address and:
- Ensure that MAC address authentication processing is not delayed until 802.1Xfails
- Ensure that even if MAC address authentication passes, the switch will still perform 802.1X authentication if requested by a 802.1X supplicant
- Use the required show command to verify the MAC address authentication on the Fa0/19 is successful

The switch enable password is Cisco

For the purpose of the simulation, to test the network printer, assume the network printer will be unplugged then plugged back into the Fa0/19 switch port after you have finished the required configurations on the Fa0/19 switch port.

For this simulation, you will not need and do not have access to the ISE GUI To access the switch CLI, click the Switch icon in the topology diagram



- A.
- B.
- C.

D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Answer: Review the explanation for full configuration and solution.

Explanation:

Initial configuration for fa 0/19 that is already done:

```
interface FastEthernet0/19
description Employee PC
switchport access vlan 9
switchport mode access
ip access-group Basic-ACL in
authentication host-mode multi-auth
authentication open
authentication port-control auto
authentication periodic
authentication timer reauthenticate server
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
!
interface FastEthernet0/20
!
```

AAA configuration has already been done for us. We need to configure mac address bypass on this port to achieve the goal stated in the question. To

do this we simply need to add this command under the interface:

mab

Then do a shut/no shut on the interface.

Verification:

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/19, changed s
to down

HQ-Sw(config-if)#end

HQ-Sw#show authentication sessions interface fa 0/19

Interface: FastEthernet0/19
MAC Address: 0014.bf70.b5fb
IP Address: Unknown
Status: Running
Domain: UNKNOWN
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A0A02020000003300670553
Acct Session ID: 0x0000000F
Handle: 0x42000034

Runnable methods list:

Method	State
dot1x	Failed over
mab	Authc Success

QUESTION 166
CORRECT TEXT

The Secure-X company has started to test the 802.1X authentication deployment using the Cisco Catalyst 3560-X layer 3 switch and the Cisco ISEv2 appliance. Each employee desktop will be connected to the 802.1X enabled switch port and will use the Cisco AnyConnect NAM 802.1X supplicant to log in and connect to the network.

Your particular tasks in this simulation are to create a new identity source sequence named AD_internal which will first use the Microsoft Active Directory (AD1) then use the ISE Internal User database. Once the new identity source sequence has been configured, edit the existing Dot1X authentication policy to use the new AD_internal identity source sequence.

The Microsoft Active Directory (AD1) identity store has already been successfully configured, you just need to reference it in your configuration.



* Domain Name

* Identity Store Name

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

<input type="checkbox"/>	ISE Node	ISE Node Role	Status
<input type="checkbox"/>	ise.secure-x.local	STANDALONE	<input checked="" type="checkbox"/> Connected to: hq-srv.secure-x.local

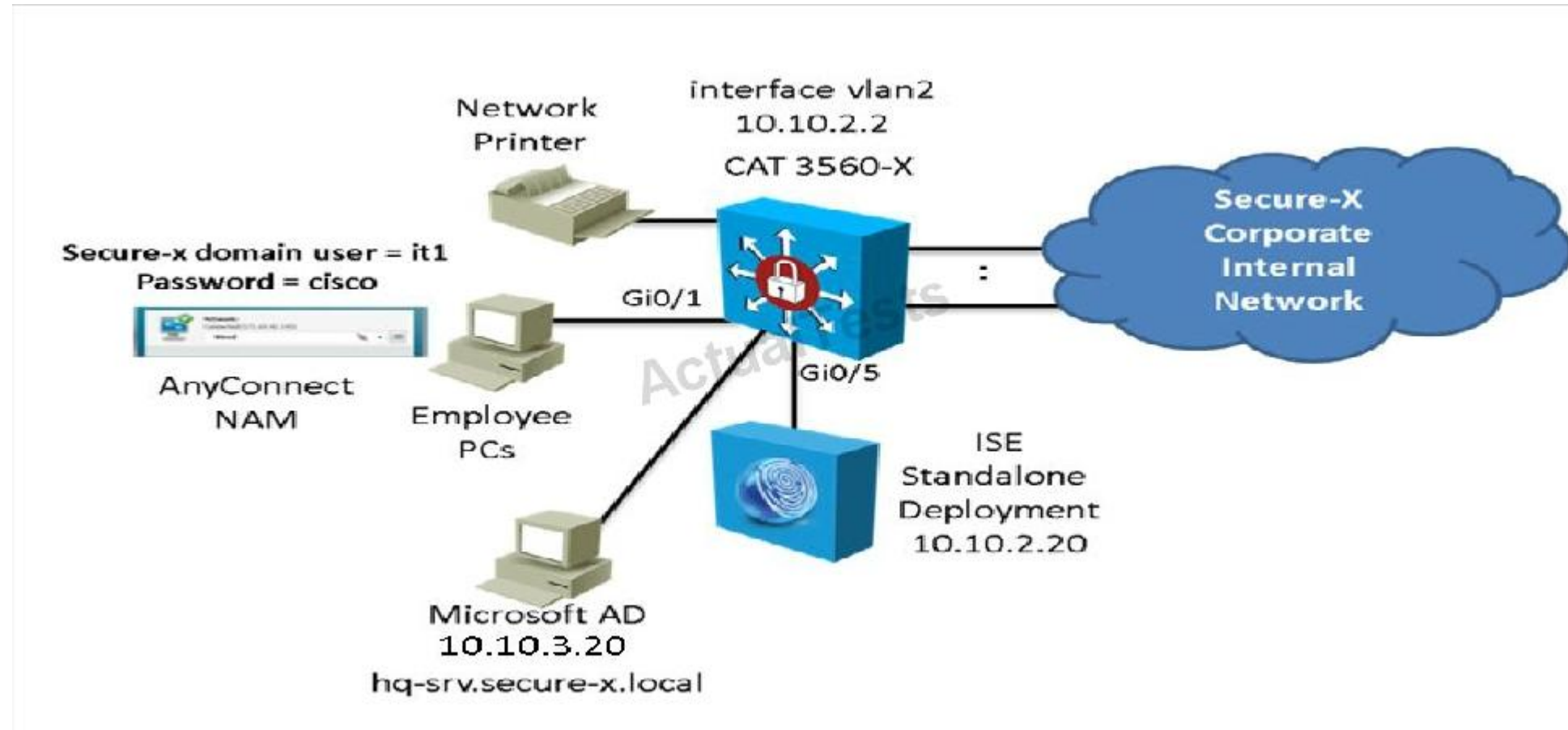
In addition to the above, you are also tasked to edit the IT users authorization policy so IT users who successfully authenticated will get the permission of the existing IT_Corp authorization profile.

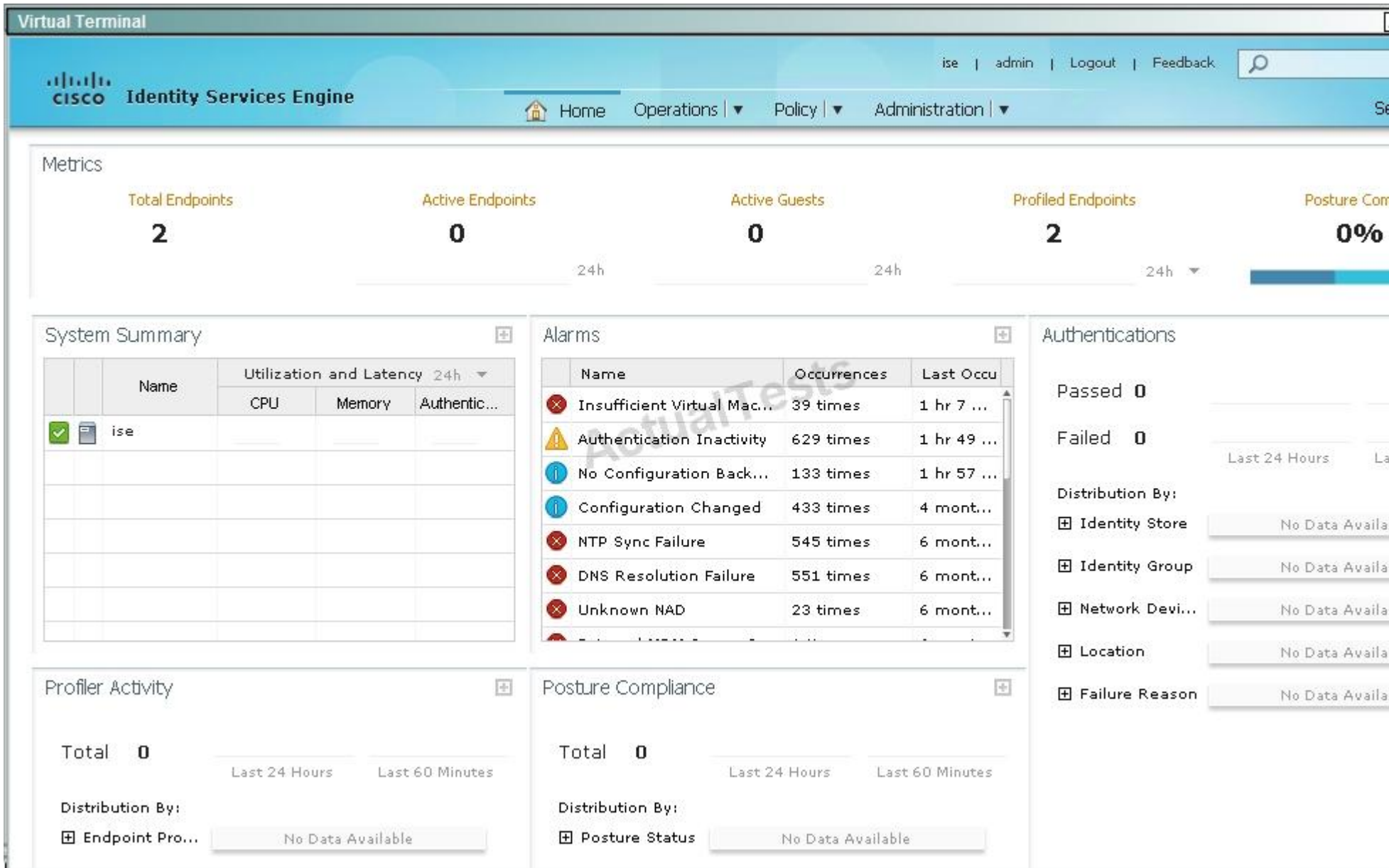
Perform this simulation by accessing the ISE GUI to perform the following tasks:

- Create a new identity source sequence named AD_internal to first use the Microsoft Active Directory (AD1) then use the ISE Internal User database
- Edit the existing Dot1X authentication policy to use the new AD_internal identity source sequence:
- If authentication failed-reject the access request
- If user is not found in AD-Drop the request without sending a response
- If process failed-Drop the request without sending a response
- Edit the IT users authorization policy so IT users who successfully authenticated will get the permission of the existing IT_Corp authorization profile.

To access the ISE GUI, click the ISE icon in the topology diagram. To verify your configurations, from the ISE GUI, you should also see the Authentication Succeeded event for the it1 user after you have successfully defined the Dot1X authentication policy to use the Microsoft Active Directory first then use the ISE Internal User Database to authenticate the user. And in the Authentication Succeeded event, you should see the IT_Corp authorization profile being applied to the it1 user. If your configuration is not correct and ISE can't authenticate the user against the Microsoft Active Directory, you should see the Authentication Failed event instead for the it1 user.

Note: If you make a mistake in the Identity Source Sequence configuration, please delete the Identity Source Sequence then re-add a new one. The edit Identity Source Sequence function is not implemented in this simulation.





A.

- B.
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Answer: Review the explanation for full configuration and solution.

Explanation:

Step 1: create a new identity source sequence named AD_internal which will first use the Microsoft Active Directory (AD1) then use the ISE Internal User database as shown below:



Identity Source Sequence

Identity Source Sequence

* Name

AD_Internal

Description

▼ Certificate Based Authentication



Select Certificate Authentication Profile

CommonName



▼ Authentication Search List



A set of identity sources that will be accessed in sequence until first authentication succeeds

ActualTests

Step 2: Edit the existing Dot1x policy to use the newly created Identity Source:



Authentication



Authorization



Profiling



Posture



Client Provisioning



Security

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices.

Policy Type ☐ Simple ☒ Rule-Based



MAB

: If

Wired_802.1X OR
Wireless_802.1X

Allow Protocol

and



Default

: use

Default

ActualTests



Dot1X

: If

Wired_802.1X OR Wireless_802.1X



Allow Protocol



Default

Use

Internal Endpoints

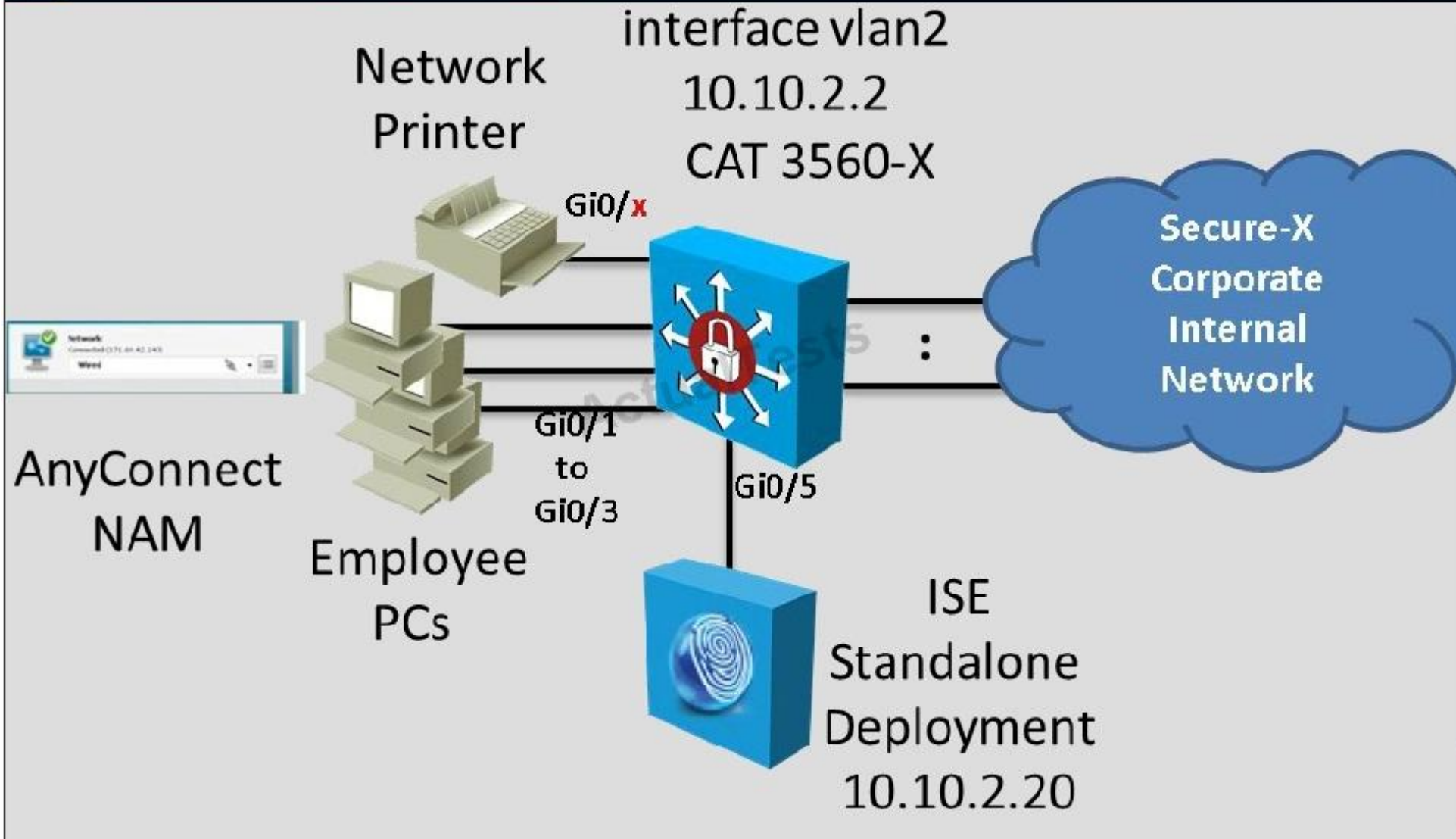
Identity Source

AD_Internal

Then hit Done and save.

QUESTION 167

In this simulation, you are task to examine the various authentication events using the ISE GUI. For example, you should see events like Authentication succeeded. Authentication failed and etc...





Metrics

Total Endpoints

5

Active Endpoints

2



Active Guests

0

24h

Profiled Endpoints

5



System Summary



		Name	Utilization and Latency 24h ▾		
			CPU	Memory	Authenticati...
✓	ise				

Alarms



	Name	Occurrences	Last Occur...
i	Configuration Changed	787 times	41 mins ...
!	Authentication Inactivity	1049 times	2 hrs 15 ...
✗	Insufficient Virtual Machin...	527 times	2 hrs 25 ...
!	RADIUS Request Dropped	858 times	14 hrs 4 ...
!	No Accounting Start	237 times	14 hrs 4...
!	Supplicant stopped respo...	21 times	16 hrs 4...
i	No Configuration Backup ...	187 times	23 hrs 2...

Profiler Activity



Total 9



Last 24 Hours

Last 60 Minutes

Distribution By:

Endpoint Pro



Posture Compliance



Total 0

Last 24 Hours

Last 60 Minutes

Distribution By:

Posture Status

No Data Available

Which four statements are correct regarding the event that occurred at 2014-05-07 00:19:07.004? (Choose four.)

- A. The IT_Corp authorization profile were applied.
- B. The it1 user was matched to the IT_Corp authorization policy.
- C. The it1 user supplicant used the PEAP (EAP-MSCHAPv2) authentication method.
- D. The it1 user was authenticated using MAB.
"Pass Any Exam. Any Time." - www.actualtests.com 69
- E. The it1 user was successfully authenticated against AD1 identity store.
- F. The it1 user machine has been profiled as a Microsoft-Workstation.
- G. The it1 user machine has passed all the posture assessment tests.

Correct Answer: BCEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Here are the details shown for this event:

it1 succeed

Overview

Event	5200 Authentication succeeded
Username	it1
Endpoint Id	44:03:A7:62:41:7F
Endpoint Profile	Microsoft-Workstation
Authorization Profile	IT_Corp
AuthorizationPolicyMatchedRule	IT users
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-05-07 00:19:07.003
Received Timestamp	2014-05-07 00:19:07.004
Policy Server	ise
Event	5200 Authentication succeeded
Failure Reason	
Resolution	

NAS I

Autho

Postu

Secur

Resp

Other

Confi

Desti

Proto

NAS-I

Frame

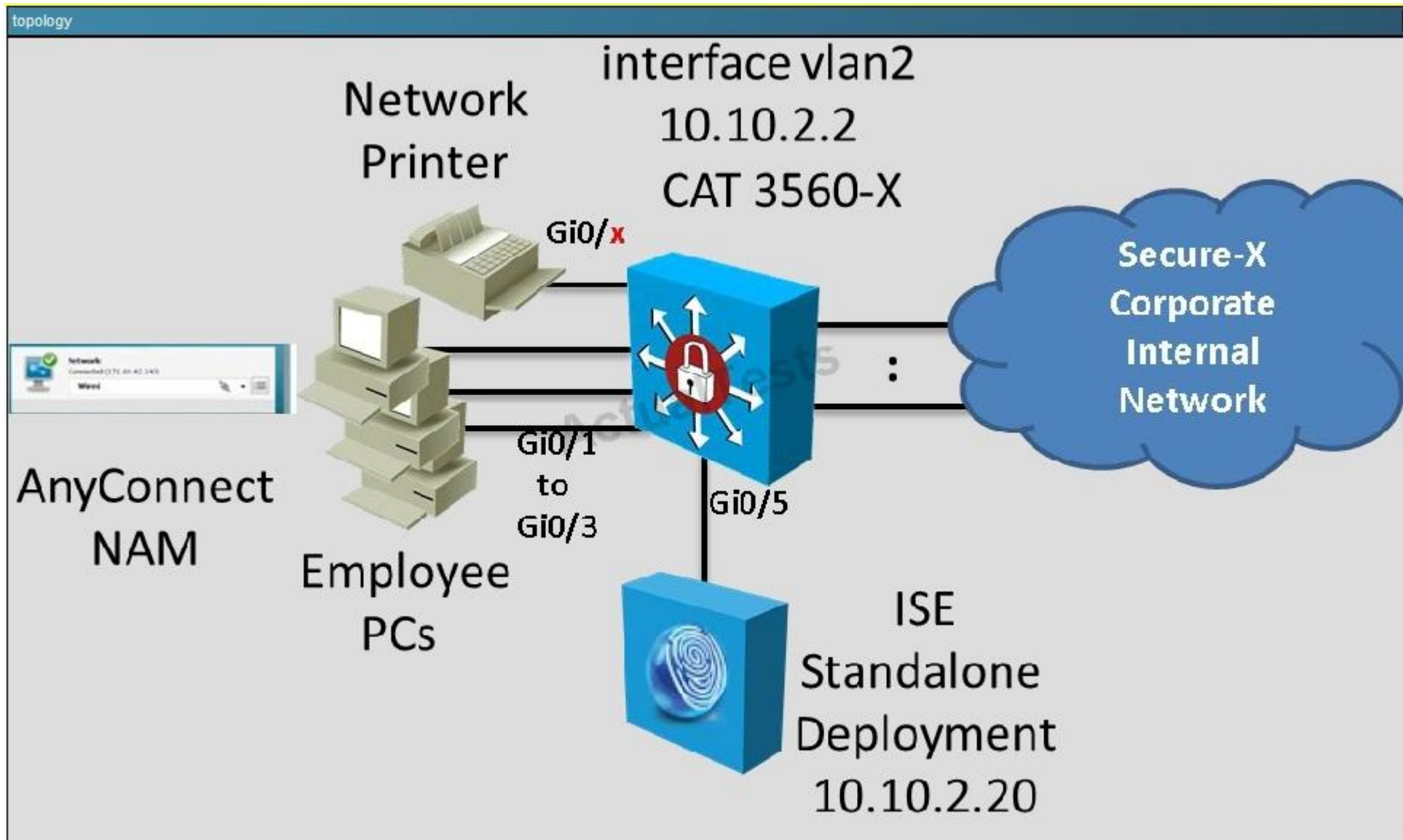
State

Acc S

Sele

QUESTION 168

In this simulation, you are task to examine the various authentication events using the ISE GUI. For example, you should see events like Authentication succeeded. Authentication failed and etc...





Metrics

Total Endpoints

5

Active Endpoints

2



Active Guests

0

24h

Profiled Endpoints

5



System Summary



		Name	Utilization and Latency 24h ▾		
			CPU	Memory	Authenticati...
✓	ise				

Alarms



	Name	Occurrences	Last Occur...
i	Configuration Changed	787 times	41 mins ...
!	Authentication Inactivity	1049 times	2 hrs 15 ...
✗	Insufficient Virtual Machin...	527 times	2 hrs 25 ...
!	RADIUS Request Dropped	858 times	14 hrs 4 ...
!	No Accounting Start	237 times	14 hrs 4...
!	Supplicant stopped respo...	21 times	16 hrs 4...
i	No Configuration Backup ...	187 times	23 hrs 2...

Profiler Activity



Total 9



Last 24 Hours

Last 60 Minutes

Distribution By:

Endpoint Pro



Posture Compliance



Total 0

Last 24 Hours

Last 60 Minutes

Distribution By:

Posture Status

No Data Available

Which three statements are correct regarding the events with the 20 repeat count that occurred at 2014-05-07 00:22:48.748? (Choose three.)

- A. The device was successfully authenticated using MAB.
- B. The device matched the Machine_Corp authorization policy.
- C. The Print Servers authorization profile were applied.
- D. The device was profiled as a Linksys-PrintServer.
- E. The device MAC address is 00:14:BF:70:B5:FB.
- F. The device is connected to the Gi0/1 switch port and the switch IP address is 10.10.2.2.

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Event Details:

MAB

There have been 20 repeated authentications with the same authentication result.
The authentication details of the first passed attempt is shown here.

Location

NAS IP Address

NAS Port Id

NAS Port Type

Authorization

Posture Status

Security Group

Response

Overview

Event **5200 Authentication succeeded**

Username 00:14:BF:70:B5:FB

Endpoint Id 00:14:BF:70:B5:FB

Endpoint Profile Linksys-PrintServer

Authorization Profile Machine_Corp

AuthorizationPolicyMatchedRule Print Servers

ISEPolicySetName Default

IdentitySelectionMatchedRule Default

ActualTests

Other Attributes

ConfigVersion

Destination

Protocol

NAS-Port

Framed-MTU

Original User

Acct Session

Authentication Details

Source Timestamp 2014-05-05 17:20:50.32

>

...continued:

Authentication Details

Source Timestamp	2014-05-05 17:20:50.32
Received Timestamp	2014-05-05 17:20:50.32
Policy Server	ise
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	00:14:BF:70:B5:FB
User Type	Host
Endpoint Id	00:14:BF:70:B5:FB
Endpoint Profile	Linksys-PrintServer
IP Address	
Identity Store	Internal Endpoints
Identity Group	Linksys-PrintServer
Audit Correlation Id	0A0A0000000000000000000000000000

Destination

Protocol

NAS-Port

Framed-M

Original Us

Acs Sessio

Use Case

SelectedA

Authorizati

CPMSessi

EndPointM

ISEPolicy3

AllowedPr

IdentitySel

HostIdentit

Location

Device Typ

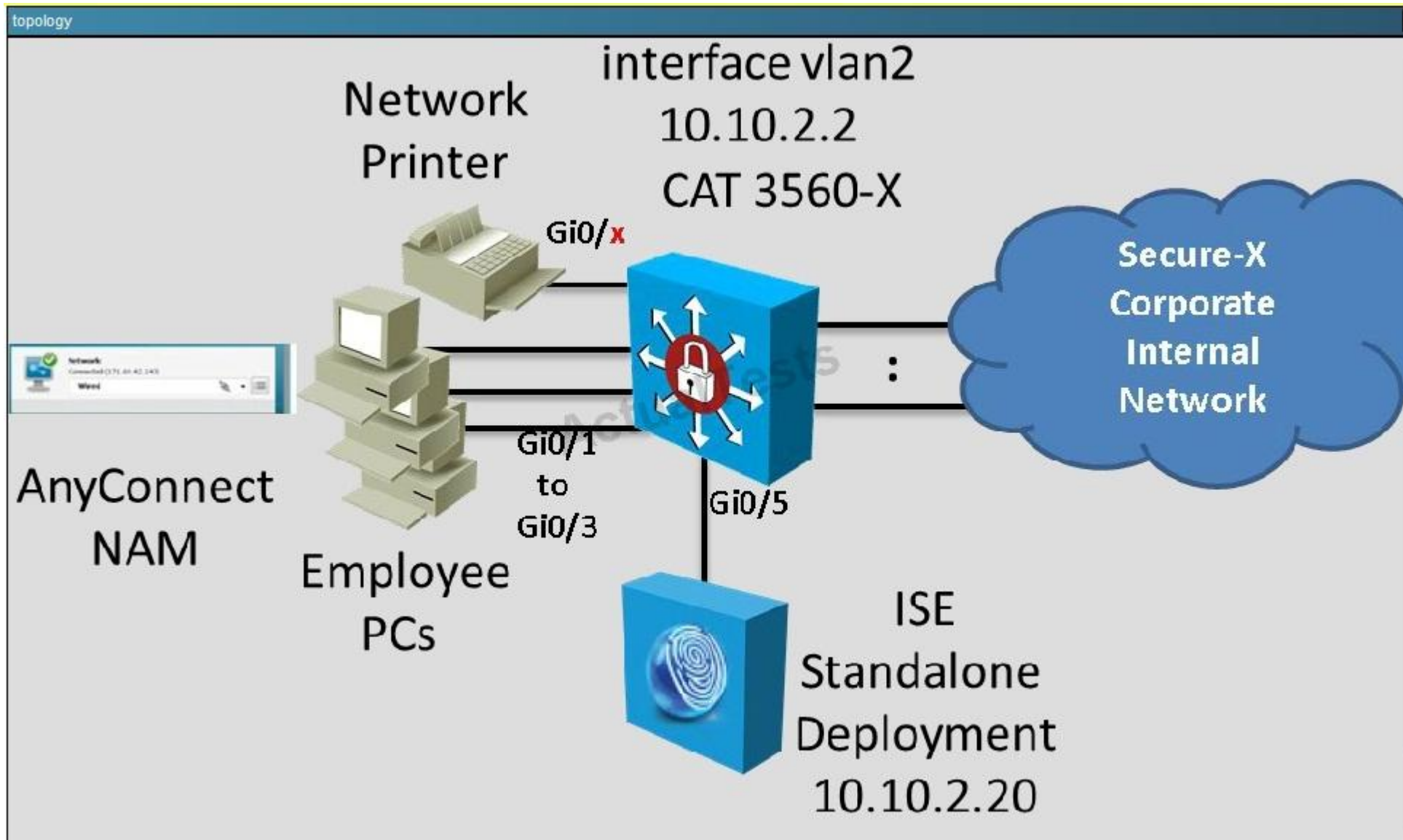
RADIUS Us

Device IP

ActualTests

QUESTION 169

In this simulation, you are task to examine the various authentication events using the ISE GUI. For example, you should see events like Authentication succeeded. Authentication failed and etc...





Metrics

Total Endpoints

5

Active Endpoints

2



Active Guests

0

24h

Profiled Endpoints

5



System Summary



		Name	Utilization and Latency 24h ▾		
			CPU	Memory	Authenticati...
✓	ise				

Alarms



	Name	Occurrences	Last Occur...
i	Configuration Changed	787 times	41 mins ...
!	Authentication Inactivity	1049 times	2 hrs 15 ...
✗	Insufficient Virtual Machin...	527 times	2 hrs 25 ...
!	RADIUS Request Dropped	858 times	14 hrs 4 ...
!	No Accounting Start	237 times	14 hrs 4...
!	Supplicant stopped respo...	21 times	16 hrs 4...
i	No Configuration Backup ...	187 times	23 hrs 2...

Profiler Activity



Total 9



Last 24 Hours

Last 60 Minutes

Distribution By:

Endpoint Pro



Posture Compliance



Total 0

Last 24 Hours

Last 60 Minutes

Distribution By:

Posture Status

No Data Available

Which two statements are correct regarding the event that occurred at 2014-05-07 00:22:48.175? (Choose two.)

- A. The DACL will permit http traffic from any host to 10.10.2.20
- B. The DACL will permit http traffic from any host to 10.10.3.20
- C. The DACL will permit icmp traffic from any host to 10.10.2.20
- D. The DACL will permit icmp traffic from any host to 10.10.3.20
- E. The DACL will permit https traffic from any host to 10.10.3.20

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Event Details:



Overview

Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-Employee_Restricted_DACL-52777cc3
Endpoint Id	
Endpoint Profile	
Authorization Profile	

Authentication Details

Source Timestamp	2014-05-07 00:22:48.174
Received Timestamp	2014-05-07 00:22:48.175
Policy Server	ize
Event	5232 DACL Download Succeeded
Failure Reason	

ActualTests

Authentication Details

Source Timestamp	2014-05-07 00:22:48.174
Received Timestamp	2014-05-07 00:22:48.175
Policy Server	ise
Event	5232 DACL Download Succeeded
Failure Reason	
Resolution	
Root cause	
Username	#ACSACL#-IP-Employee_Restricted_DACL-52777003
User Type	
Endpoint Id	
Endpoint Profile	
IP Address	
Identity Store	
Identity Group	
Audit Session Id	
Authentication Method	
Authentication Protocol	
Service Type	
Network Device	HQ-SW

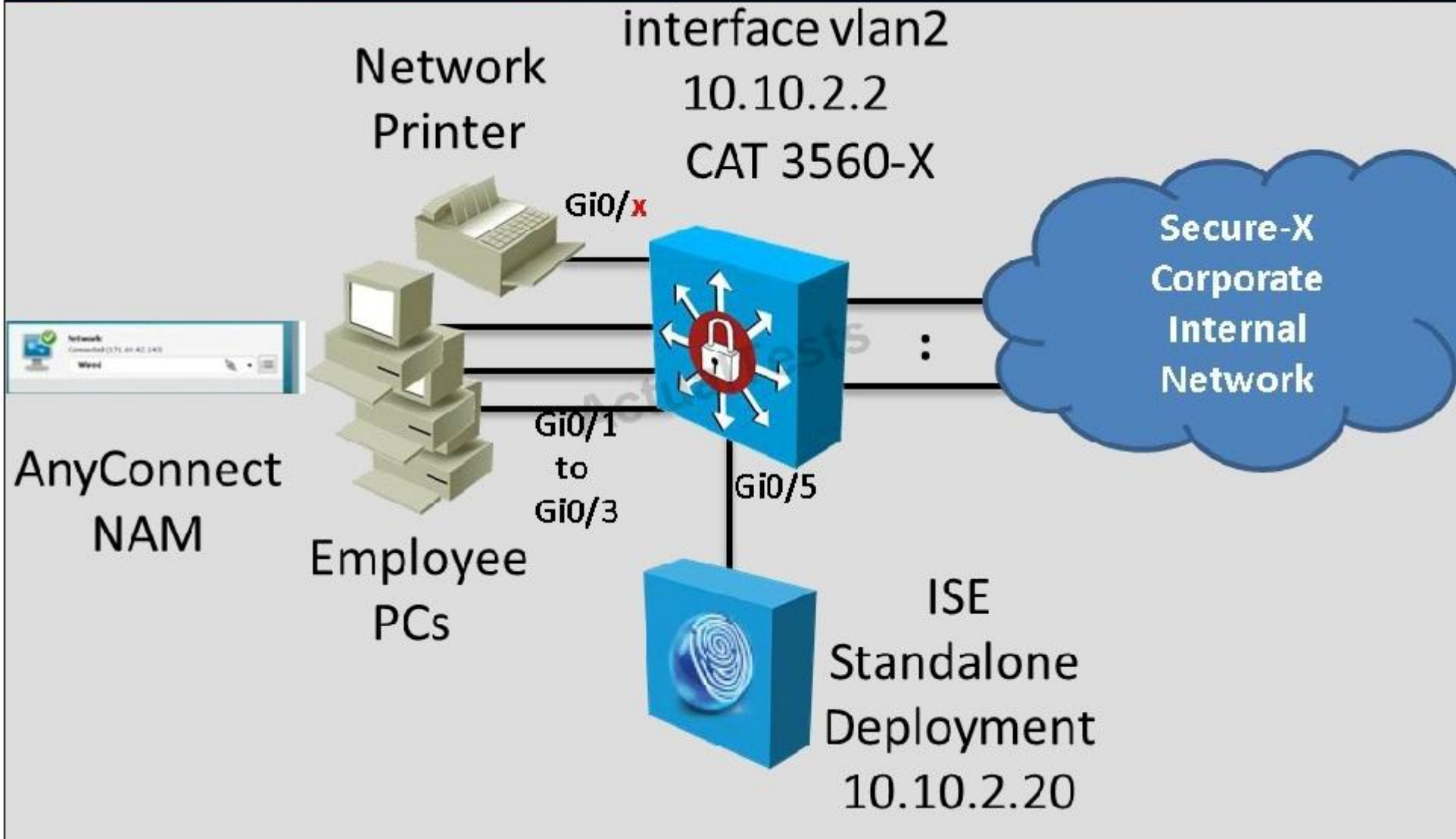
ActualTests

Result

State	ReauthSession:0a0a02140000006353697CD8
Class	CACS:0a0a02140000006353697CD8:ise/188683442/376
cisco-av-pair	ip:inac1#1=deny icmp any host 10.10.2.20
cisco-av-pair	ip:inac1#2=deny icmp any host 10.10.3.20
cisco-av-pair	ip:inac1#3=deny tcp any host 10.10.3.20 eq 80
cisco-av-pair	ip:inac1#4=permit ip any any

QUESTION 170

In this simulation, you are task to examine the various authentication events using the ISE GUI. For example, you should see events like Authentication succeeded. Authentication failed and etc...





Metrics

Total Endpoints

5

Active Endpoints

2



Active Guests

0

24h

Profiled Endpoints

5



System Summary



		Name	Utilization and Latency 24h ▾		
			CPU	Memory	Authenticati...
✓	ise				

Alarms



	Name	Occurrences	Last Occur...
i	Configuration Changed	787 times	41 mins ...
!	Authentication Inactivity	1049 times	2 hrs 15 ...
✗	Insufficient Virtual Machin...	527 times	2 hrs 25 ...
!	RADIUS Request Dropped	858 times	14 hrs 4 ...
!	No Accounting Start	237 times	14 hrs 4...
!	Supplicant stopped respo...	21 times	16 hrs 4...
i	No Configuration Backup ...	187 times	23 hrs 2...

Profiler Activity



Total 9



Last 24 Hours

Last 60 Minutes

Distribution By:

Endpoint Pro



Posture Compliance



Total 0

Last 24 Hours

Last 60 Minutes

Distribution By:

Posture Status

No Data Available

Which two statements are correct regarding the event that occurred at 2014-05-07 00:16:55.393? (Choose two.)

- A. The failure reason was user entered the wrong username.
- B. The supplicant used the PAP authentication method.
- C. The username entered was it1.
- D. The user was authenticated against the Active Directory then also against the ISE internal user database and both fails.
- E. The NAS switch port where the user connected to has a MAC address of 44:03:A7:62:41:7F
- F. The user is being authenticated using 802.1X.
- G. The user failed the MAB.
- H. The supplicant stopped responding to ISE which caused the failure.

Correct Answer: CF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Event Details:

it1 failed

Overview

Event	5400 Authentication failed
Username	it1
Endpoint Id	44:03:A7:62:41:7F
Endpoint Profile	
Authorization Profile	
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-05-07 00:16:55.392
------------------	-------------------------

+

it1 failed

Authentication Details

Source Timestamp	2014-05-07 00:16:55.392
Received Timestamp	2014-05-07 00:16:55.393
Policy Server	ise
Event	5400 Authentication failed
Failure Reason	24408 User authentication against Active Directory the wrong password
Resolution	Check the user password credentials. If the RADIUS authentication, also check the Shared Secret configuration.
Root cause	User authentication against Active Directory failed s wrong password
Username	it1
User Type	
Endpoint Id	44:03:A7:62:41:7F