

300-208 Dumps

Implementing Cisco Secure Access Solutions (SISAS)

<https://www.certleader.com/300-208-dumps.html>



NEW QUESTION 1

What are three portals provided by PSN? (Choose three.)

- A. Monitoring
- B. Troubleshooting
- C. Sponsor
- D. Guest
- E. My devices
- F. Admin

Answer: CDE

NEW QUESTION 2

Which two protocols are supported with the Cisco IOS Device Sensor? (Choose two.)

- A. SNMP
- B. Cisco Discovery Protocol
- C. RADIUS
- D. LLDP
- E. NetFlow

Answer: BD

NEW QUESTION 3

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

Answer: C

NEW QUESTION 4

What is the purpose of configuring Native Supplicant Profile on the Cisco ISE?

- A. It provides posture assessments and remediation for devices that are attempting to gain access to the corporate network.
- B. It is used to register personal devices on the network.
- C. It enforces the use of MSCHAPv2 or EAP-TLS for 802 1X authentication
- D. It helps employees add and manage new devices by entering the MAC address for the device.

Answer: C

NEW QUESTION 5

What is the SGT assignment when authentication is not available or SGT method for non authenticating devices?

- A. dynamic
- B. static
- C. SXP
- D. Default

Answer: A

NEW QUESTION 6

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

Answer: ABC

NEW QUESTION 7

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

Answer: CD

NEW QUESTION 8

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.

Answer: E

NEW QUESTION 9

Which two endpoint operating systems are supported during BYOD onboarding? (Choose two.)

- A. Red Hat Enterprise Linux
- B. BlackBerry
- C. Nook
- D. Microsoft Windows
- E. Android

Answer: AE

NEW QUESTION 10

Drag and drop the portals from the left onto the correct portal tasks on the right.

Blacklist	Provide a posture assessment for a device
Certificate Provisioning	Request a certificate for a device that is unable to use onboarding support.
Client Provisioning	Remove a device.
My Devices	Register a lost device.

Answer:

Explanation: Certificate provisioning = Request a certificate for a device that is unable to use onboarding support
Client provisioning = Provide a posture assessment for a device

My Devices = Register a lost device
Blacklist = Remove a device

NEW QUESTION 10

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

Answer: C

NEW QUESTION 13

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

Answer: C

NEW QUESTION 15

Which two protocols does Cisco Prime Infrastructure use for device discovery? (Choose two.)

- A. SNAP
- B. LLDP
- C. RARP
- D. DNS
- E. LACP

Answer: BD

NEW QUESTION 19

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

Answer: BC

NEW QUESTION 23

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

Answer: AB

NEW QUESTION 24

An ISE1.3 environment, which path does a network engineer use to set up a self-registered guest portal?

- A. Guest Access > Configure > Guest Portals
- B. Security > Access Control Lists > Guest Portals
- C. Policy > Settings > Guest Portals
- D. Policy > Authorization > Guest Portals

Answer: A

NEW QUESTION 25

Which Cisco IOS IPS feature allows to you remove one or more actions from all active signatures based on the attacker and/or target address criteria, as well as the event risk rating criteria?

- A. signature event action filters
- B. signature event action overrides
- C. signature attack severity rating
- D. signature event risk rating

Answer: A

NEW QUESTION 27

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.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.

Answer: D

NEW QUESTION 29

When configuring NAT, which three protocols that are shown may have limitations or complications when using NAT? (Choose three.)

- A. Kerberos
- B. HTTPS
- C. NTP
- D. SIP
- E. FTP
- F. SQL

Answer: ADE

NEW QUESTION 33

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

- A. It uses UDP ports 1812 and 1813.
- B. It encrypts the payload.
- C. It encrypts the password only
- D. It uses TCP ports 1812 and 1813.
- E. It separates authorization and authentication functions

Answer: AC

NEW QUESTION 34

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

Answer: D

NEW QUESTION 37

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

Answer: B

Explanation:

http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/installation_guide/b_ise_InstallationGuide20/Cisco_SNS_3400_Series_Appliance_Ports_Reference.html

NEW QUESTION 40

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

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

Answer: B

NEW QUESTION 41

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

Answer: D

NEW QUESTION 42

Which two accounting types are used to implement accounting with RADIUS? (Choose two.)

- A. Network
- B. User
- C. Attribute
- D. Device
- E. Resource

Answer: AE

NEW QUESTION 44

The posture run-time services encapsulates which protocol services, and all the interactions that happen between the NAC Agents?

- A. SWISS

- B. MAB
- C. DOT1X
- D. DEFAULT

Answer: A

NEW QUESTION 47

A security engineer has configured a switch port in x closed mode. Which protocol is allowed to pass?

- A. HTTP
- B. EAPOL
- C. Bootps
- D. ARP
- E. PXE

Answer: B

NEW QUESTION 52

A security engineer must provision dynamic TrustSec classifications. Which two classification options must the engineer select to accomplish this task? (Choose two.)

- A. interface
- B. 802.1X
- C. MAB
- D. IP subnet
- E. VLAN

Answer: BE

NEW QUESTION 56

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

Answer: ABC

NEW QUESTION 61

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

Answer: A

NEW QUESTION 62

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.

Answer: B

NEW QUESTION 65

A network administrator configured DUAL SSID, where the first SSID is used for guest provisioning and the other SSID for Employee provisioning. Which option he can use for layer 2 security provision?

- A. MAB
- B. 802.1x
- C. authentication open
- D. shared secret

Answer: A

NEW QUESTION 69

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

Answer: A

NEW QUESTION 71

An engineer wants to allow dynamic vlan assignment from ISE. What must be configured on the switch?

- A. DTP
- B. VTP
- C. AAA authentication
- D. AAA authorization

Answer: D

NEW QUESTION 73

Which characteristic of an 3GT enforcement policy is true?

- A. An SGFW has an implicit permit at the beginning.
- B. An SGFW has an implicit deny at the end.
- C. An SGACL has an implicit deny at the end.
- D. An SGACL has an explicit deny at the beginning.

Answer: C

NEW QUESTION 74

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.

Answer: D

NEW QUESTION 77

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

Answer: AB

NEW QUESTION 80

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

Answer: C

NEW QUESTION 84

Which ISE deployment mode is similar to the industry standard 802.1X behavior?

- A. policy mode
- B. monitor mode
- C. closed mode
- D. low-impact mode

Answer: C

NEW QUESTION 87

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

Answer: A

NEW QUESTION 90

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

- A. Client Provisioning Portals
- B. BYOD Portals
- C. My Devices Portals
- D. MDM Portals

Answer: C

NEW QUESTION 92

What is the first Step for configuring Cisco ISE for the onboarding process?

- A. Configure the default action that must be taken when .in unsupported device attempts to connect and cannot be provisioned
- B. Create the native supplicant profile that is sent to the end user device.
- C. Configure different web portals based on a number of attributes available from the authentication request
- D. Configure the action that is taken when an unsupported device attempts to connect to a secure network

Answer: B

NEW QUESTION 96

You are finding that the 802.1X-configured ports are going into the error-disable state. Which command will show you the reason why the port is in the error-disable state, and which command will automatically be re-enabled after a specific amount of time? (Choose two.)

- A. show error-disable status
- B. show error-disable recovery
- C. show error-disable flap-status
- D. error-disable recovery cause security-violation
- E. error-disable recovery cause dot1x
- F. error-disable recovery cause l2ptguard

Answer: BD

NEW QUESTION 99

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

Answer: AB

NEW QUESTION 100

When is it feasible for a port to be both a guest VLAN and a restricted VLAN?

- A. this configuration scenario is never be implemented
- B. when you have configured the port for promiscuous mode
- C. when private VLANs have been configured to place each end device into different subnets
- D. when you want to allow both types of users the same services

Answer: D

NEW QUESTION 104

Which state is a Cisco IOS IPS signature in if it does not take an appropriate associated action even if it has been successfully compiled?

- A. retired
- B. disabled
- C. unsupported
- D. inactive

Answer: B

NEW QUESTION 108

An organization is deciding between single or dual SSID solutions for onboarding BYOD devices. Which item must be considered before selecting the dual SSID solution?

- A. Wireless coverage is reduced with dual SSIDs
- B. Additional access points are required for dual SSID.
- C. Dedicated controllers are required for dual SSIDs.
- D. The second SSID adds channel overhead

Answer: B

NEW QUESTION 109

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

Answer: AC

NEW QUESTION 110

A manager of Company A is hosting a conference. Conference participants use a code on the AUP page of the hot-spot guest portal Which code must the manager create on Cisco ISE before the meeting?

- A. user code
- B. pass code
- C. access code
- D. registration code

Answer: D

NEW QUESTION 112

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

Answer: ABD

NEW QUESTION 115

An engineer must enable SGACL policy globally for a Cisco TrustSec –enabled routed interface. Which command must be used?

- A. cts role-based monitor enable
- B. cts role-based enforcement
- C. cts role-based sgt-caching with-enforcement
- D. cts role-based monitor permissions from {sgt_num} to {dgt_num}[[ipv4| ipv6]

Answer: B

NEW QUESTION 120

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

- A. Idle-timeout attribute
- B. Session-timeout attribute
- C. Radius-server timeout
- D. Termination-action attribute

Answer: A

NEW QUESTION 125

Cisco IOS IPS uses which alerting protocol with a pull mechanism for getting IPS alerts to the network management application?

- A. HTTPS
- B. SMTP
- C. SNMP
- D. syslog
- E. SDEE
- F. POP3

Answer: E

NEW QUESTION 128

Which protocol provides the real time request to the service running on the CA?

- A. DOS
- B. FILE
- C. MAB
- D. OCSP

Answer: D

NEW QUESTION 133

Which command is needed to enable dot1x globally on the switch?

- A. aaa authentication dot1x default group radius
- B. dot1x system-auth-control
- C. dot1x pae authenticator
- D. authentication port-control auto

Answer: C

NEW QUESTION 134

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

Answer: A

NEW QUESTION 136

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

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

Answer: A

NEW QUESTION 139

A company has implemented a dual SSID BYOD design. A provisioning SSID is used for user registration, and an employee SSID is used for company network access. How is the layer 2 security of the provisioning SSID configured?

- A. 802.1X
- B. Open
- C. WPA2
- D. MAC filtering disabled

Answer: B

NEW QUESTION 141

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.

Answer: AB

Explanation: who possess the proper administrative credentials.

The CLI administrator does not have access to the ACS web GUI.

To create an initial GUI administrator account that allows web access to the ACS SE GUI, use the add-guiadmin command to create a GUI account.

add-guiadmin :

Adds a GUI account that allows access to the SE using the ACS web GUI.

NEW QUESTION 144

Which three statement about Windows Server Update Services remediation are true?

- A. WSUS can install the latest service pack available
- B. WSUS checks for automatic update configuration on Windows
- C. WSUS checks for client behavior anomalies
- D. WSUS remediates Windows client from a locally manage WSUS server
- E. WSUS remediates Windows client from a Microsoft manage WSUS server
- F. WSUS provides links to update AV/AS

Answer:

ADE

NEW QUESTION 149

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

Answer: CEF

NEW QUESTION 150

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

Answer: A

NEW QUESTION 153

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

Answer: BCE

NEW QUESTION 155

Which type of SGT propagation does a WLC in a datacenter require?

- A. SXP
- B. inline
- C. Trust
- D. Inherit

Answer: D

NEW QUESTION 160

What is the result of configuring the command dot1x system-auth-control on a Cisco Catalyst switch?

- A. enables the switch to operate as the 802.1X supplicant
- B. globally enables 802.1X on the switch
- C. globally enables 802.1X and defines ports as 802.1X-capable
- D. places the configuration sub-mode into dot1x-auth mode, in which you can identify the authentication server parameters

Answer: B

NEW QUESTION 165

What attribute could be obtained from the SNMP query probe?

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

Answer: B

NEW QUESTION 167

An administrator can leverage which attribute to assign privileges based on Microsoft Active Directory user groups?

- A. member of
- B. group
- C. class
- D. person

Answer:

A

NEW QUESTION 169

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

Answer: B

NEW QUESTION 171

You are troubleshooting reported connectivity issues from remote users who are accessing corporate headquarters via an IPsec VPN connection. What should be your first step in troubleshooting these issues?

- A. issue a show crypto isakmp policy command to verify matching policies of the tunnel endpoints
- B. ping the tunnel endpoint
- C. run a traceroute to verify the tunnel path
- D. debug the connection process and look for any error messages in tunnel establishment

Answer: B

NEW QUESTION 173

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.

Answer: A

NEW QUESTION 175

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

Answer: A

NEW QUESTION 177

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.

Answer: A

NEW QUESTION 179

You must recover a wireless client from quarantine. You disconnect the client from the network. Which action do you take next?

- A. Reboot the client machine after the idle timeout period expires.
- B. Start a manual reassessment
- C. Reconnect to the network after the idle timeout period expires.
- D. Turn off the MIC of the client

Answer: C

NEW QUESTION 181

When Cisco IOS IPS signatures are being tuned, how is the Target Value Rating assigned?

- A. It is calculated from the Event Risk Rating.
- B. It is calculated from a combination of the Attack Severity Rating and Signature Fidelity Rating
- C. It is manually set by the administrator.
- D. It is set based upon SEAP functions.

Answer: C

NEW QUESTION 185

A network administrator needs to implement a service that enables granular control of IOS commands that can be executed. Which AAA authentication method should be selected?

- A. TACACS+
- B. RADIUS
- C. Windows Active Directory
- D. Generic LDAP

Answer: A

NEW QUESTION 186

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

Answer: ACD

NEW QUESTION 190

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

Answer: ACE

NEW QUESTION 192

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

Answer: BCD

NEW QUESTION 195

An engineer must limit the configuration parameters that can be executed on the Cisco ASAs deployed throughout the network. Which command allows the engineer to complete this task?

- A. AAA-server tacacs1(inside) host 10.5.109.18 timeout 2!aaa authorization command tacacs1
- B. AAA-server tacacs1(inside) host 10.5.109.18 timeout 2!aaa authentication ssh console tacacs1
- C. AAA-server tacacs1(inside) host 10.5.109.18 timeout 2!aaa authorization exec authentication-server
- D. AAA-server tacacs1(inside) host 10.5.109.18 timeout 2!aaa authentication exclude ssh

Answer: A

NEW QUESTION 197

When is it most appropriate to choose IPS functionality based on Cisco IOS software?

- A. when traffic rates are low and a complete signature is not required
- B. when accelerated, integrated performance is required using hardware ASIC-based IPS inspections
- C. when integrated policy virtualization is required
- D. when promiscuous inspection meets security requirements

Answer: A

NEW QUESTION 201

Drag and drop each posture assessment outcome from the left onto the appropriate definition on the right.

compliant	NAC agent determined something on the endpoint is in violation of the defined security policy.
unknown	NAC agent on the endpoint determined that the software assessment on the endpoint adheres to the security policy.
noncompliant	The endpoint failed to report a posture assessment to ISE.

Answer:

Explanation: Noncompliant = NAC agent determined something on the endpoint is in violation of the defined security policy
Compliant = NAC agent on the endpoint determined that the software assessment on the endpoint adheres to the security policy
Unknown = The endpoint failed to report a posture assessment to ISE.

NEW QUESTION 206

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.

Answer: D

NEW QUESTION 211

Which method of registering devices on the BYOD My Devices Portal requires that the user have a supplicant installed?

- A. MAB
- B. single SSID
- C. web authentication
- D. dual SSID

Answer: B

NEW QUESTION 214

A customer has implemented a BYOD policy to allow employees to use personal devices on the corporate network. Which two methods can an employee use to add their devices to the network*? (Choose two.)

- A. Client Information Signaling
- B. My Device portal
- C. Client Handshake Authentication
- D. Helpdesk registration
- E. native supplicants

Answer: BD

NEW QUESTION 219

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.

Answer: BEF

NEW QUESTION 223

When configuring a BYOD portal, which two tasks must be completed? (Choose two.)

- A. Enable policy services.
- B. Create endpoint identity groups
- C. Customize device portals

- D. Create a client provisioning portal.
- E. Create external identity sources.

Answer: AE

NEW QUESTION 227

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

Answer: AD

NEW QUESTION 229

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.

Answer: D

NEW QUESTION 233

Which action does the command `private-vlan association 100,200` take?

- A. configures VLANs 100 and 200 and associates them as a community
- B. associates VLANs 100 and 200 with the primary VLAN
- C. creates two private VLANs with the designation of VLAN 100 and VLAN 200
- D. assigns VLANs 100 and 200 as an association of private VLANs

Answer: B

NEW QUESTION 235

Which Cisco IOS IPS risk rating component uses a low value of 75, a medium value of 100, a high value of 150, and a mission-critical value of 200?

- A. Signature Fidelity Rating
- B. Attack Severity Rating
- C. Target Value Rating
- D. Attack Relevancy Rating
- E. Promiscuous Delta
- F. Watch List Rating

Answer: C

NEW QUESTION 238

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`

Answer: AF

NEW QUESTION 243

Which action is a Cisco recommended practice while attempting to increase efficiency on the monitoring nodes?

- A. Back up data and transfer to a remote repository on regular basis
- B. Remove endpoints when not active.
- C. Re-index the data on a regular basis.
- D. Compress the data regularly

Answer: D

NEW QUESTION 244

Which internal Cisco ISE component reduces demand on JVM memory by limiting the number of devices the profiler handles?

- A. `eventHandlerQueueStze`
- B. `maxEndPomtsInLocalDb`
- C. `NetworkDeviceEventHandter`

D. forwarderQueueSize

Answer: B

NEW QUESTION 248

Which of these is a configurable Cisco IOS feature that triggers notifications if an attack attempts to exhaust critical router resources and if preventative controls have been bypassed or are not working correctly?

- A. Control Plane Protection
- B. Management Plane Protection
- C. CPU and memory thresholding
- D. SNMPv3

Answer: C

NEW QUESTION 252

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

Answer: BDF

NEW QUESTION 256

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

Answer: ABCDE

NEW QUESTION 260

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

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

Answer: DE

NEW QUESTION 265

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

Answer: A

NEW QUESTION 270

Which description of SXP is true?

- A. applies SGT along every hop in the network path
- B. propagates SGT on a device upon which SGT inline tagging is unsupported
- C. removes SGT from every in the network path
- D. propagates SGT on a device which inline tagging is supported

Answer: D

NEW QUESTION 273

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

Answer: A

NEW QUESTION 274

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

Answer: CE

NEW QUESTION 276

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

Answer: C

NEW QUESTION 278

What two values does Cisco recommend you adjust and test to set the optimal timeout value for your network's specific 802.1X MAB deployment?

- A. Max-reauth-req
- B. Supp-timeout
- C. Max-req
- D. Tx-period
- E. Server-timeout

Answer: AD

NEW QUESTION 280

A network administrator must remediate unpatched servers by redirecting them to their remediation portal. Which conditions in the authorization policy must the network administrator provision on Cisco ISE to accomplish this task?

- A. noncompliant
- B. quarantine
- C. compliant
- D. URL redirect

Answer: A

NEW QUESTION 284

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

Answer: A

NEW QUESTION 289

A network administrator found that the IP device tracking table on a switch is not getting updated when the client has a static IP address, but if the address is from DHCP, the table is getting updated. Which description of the cause of this issue is true?

- A. The switch code must be upgraded.
- B. IP device tracking is not configured properly
- C. ARP inspection is on and there is no ARP ACL for static clients
- D. IP device tracking does not work with statically assigned IP addresses

Answer: B

NEW QUESTION 292

In an 802.1X deployment what two components are responsible for facilitating the authentication process? (Choose two.)

- A. MACSec
- B. MAC address
- C. an authentication server
- D. a router
- E. a supplicant

Answer: CE

NEW QUESTION 294

An administrator is configuring an ASA firewall for to secure access on ASA firewall in the essence of controlling configuration command executed on the Firewall. Which command will he use?

- A. aaa authorization ssh console
- B. aaa authorization commands
- C. aaa authentication ssh console
- D. aaa authentication exec server-authentication

Answer: D

NEW QUESTION 295

Which functionality does the Cisco ISE BYOD 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.

Answer: A

NEW QUESTION 300

Which WLC debug command would be used to troubleshoot authentication issues on a 802.1X enabled WLAN?

- A. debug dot11 aaa manager all
- B. debug wps mfp lwapp
- C. debug dot11 state
- D. debug dot1x events

Answer: A

NEW QUESTION 303

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

Answer: BDF

NEW QUESTION 304

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.

Answer: CDE

NEW QUESTION 306

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

Answer: D

NEW QUESTION 307

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.

Answer: B

NEW QUESTION 310

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.

Answer: C

NEW QUESTION 312

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

Answer: BCE

NEW QUESTION 316

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

Answer: B

NEW QUESTION 321

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

Answer: BE

NEW QUESTION 325

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

Answer: C

NEW QUESTION 329

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 ACS SE is not supported.

Answer: BD

NEW QUESTION 334

Which action do you take to define the global authorization exception policy by using a Device Admin Policy Set?

- A. Configure the policy by using Proxy Sequence mode.
- B. Configure a rule-based condition in a policy set.
- C. Define the policy for each group of devices.
- D. Define the policy by configuring a standard profile

Answer: B

NEW QUESTION 335

An engineer wants to migrate 802.1x deployment phase from Open to low impact mode. Which options she select?

- A. Ingress access list applied to the interface
- B. Authentication host mode to multiple domain
- C. Open authentication to the domain
- D. Authentication host mode to multiple authentication

Answer: A

NEW QUESTION 336

Which redirect-URL is pushed by Cisco ISE for posture redirect for corporate users?

- A. <https://ise1.cisco.com:8443/portal/gateway?sessionId=0A00023D0000003A239F78CC&portal=283258a0>
- B. <https://ise1.cisco.com:8443/portal/gateway?sessionId=0A00023D0000003A239F78CC&portal=283258a0>
- C. <https://ise1.cisco.com:8443/portal/gateway?sessionId=0A00023D0000003A239F78CC&portal=283258a0>
- D. <https://ise1.cisco.com:8443/portal/gateway?sessionId=0A00023D0000003A239F78CC&portal=283258a0>

Answer: A

NEW QUESTION 338

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
- C. configuring guest wireless users to obtain DHCP centrally from the corporate DHCP server
- D. disabling guest SSID broadcasting

Answer: A

NEW QUESTION 342

Which operating system type needs access to the Internet to download the application that is required for BYOD on-boarding?

- A. iOS
- B. OSX
- C. Android
- D. Windows

Answer: C

NEW QUESTION 346

Which option is the correct format of username in MAB authentication?

- A. host/LSB67.cisco.com
- B. chris@cisco.com
- C. 10:41:7F:46:9F:89
- D. CISCO\chris

Answer: C

NEW QUESTION 350

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.

Answer: A

NEW QUESTION 353

Which command on the switch ensures that the Service-Type attribute is sent with all RADIUS authentication request?

- A. radius-server attribute 8 include-in-access-req
- B. radius-server attribute 25 access-request include
- C. radius-server attribute 6 on-for-login-auth
- D. radius-server attribute 31 send nas-port-detail

Answer: C

NEW QUESTION 358

Which protocol sends authentication and accounting in different requests?

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

Answer: B

NEW QUESTION 362

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.

Answer: ABC

NEW QUESTION 367

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

Answer:

Explanation:

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 endpoint authenticates to secure SSID using the username and password
The user opens a web browser and is redirected to a registration portal	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 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	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	A CoA is issued and the endpoint is reconnected to the network with the proper access

NEW QUESTION 369

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 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.

Answer: A

NEW QUESTION 371

Which 802.1X command ignores Access-Reject during EAP authentication?

- A. dot1x pae authenticator
- B. switchport mode access
- C. authentication port-control auto
- D. authentication open
- E. authentication host-mode multi-domain

Answer: D

NEW QUESTION 376

Refer to the exhibit.

```
12153 EAP-FAST failed SSL/TLS handshake because the
client rejected the ISE local-certificate.
```

Which two things must be verified if authentication is failing with this error message? (Choose two.)

- A. Cisco ISE EAP identity certificate is valid.
- B. CA cert chain of Cisco ISE EAP certificate is installed on the trusted certs store of the client machine.
- C. CA cert chain of the client certificate is installed on Cisco ISE.
- D. Cisco ISE HTTPS/admin certificate is valid.
- E. Cisco ISE server certificate is installed on the client.

Answer: AB

NEW QUESTION 377

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

Answer: A

NEW QUESTION 382

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

Answer: A

NEW QUESTION 384

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

Answer: BCD

NEW QUESTION 387

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.

Answer: A

NEW QUESTION 392

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

Answer: A

NEW QUESTION 395

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.

Answer: D

NEW QUESTION 399

Which attribute is needed for Cisco ISE to profile a device with HTTP probe?

- A. user-agent
- B. OUI
- C. host-name
- D. cdp-cache-platform
- E. dhcp-class-identifier
- F. sysDescr

Answer: A

NEW QUESTION 400

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.

Answer: A

NEW QUESTION 401

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.

Answer: A

NEW QUESTION 403

What EAP method supports mutual certificate-based authentication?

- A. EAP-TTLS
- B. EAP-MSCHAP
- C. EAP-TLS
- D. EAP-MD5

Answer: C

NEW QUESTION 408

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

Answer: B

NEW QUESTION 409

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

Answer: A

NEW QUESTION 412

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.

Answer: AC

NEW QUESTION 413

Which profiling probe collects the user-agent string?

- A. NetFlow
- B. DHCP
- C. Network Scan
- D. HTTP

Answer: D

NEW QUESTION 417

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.

Answer: D

NEW QUESTION 419

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

Answer: A

NEW QUESTION 424

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

Answer: D

NEW QUESTION 425

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

Answer: A

NEW QUESTION 430

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

Answer: A

NEW QUESTION 431

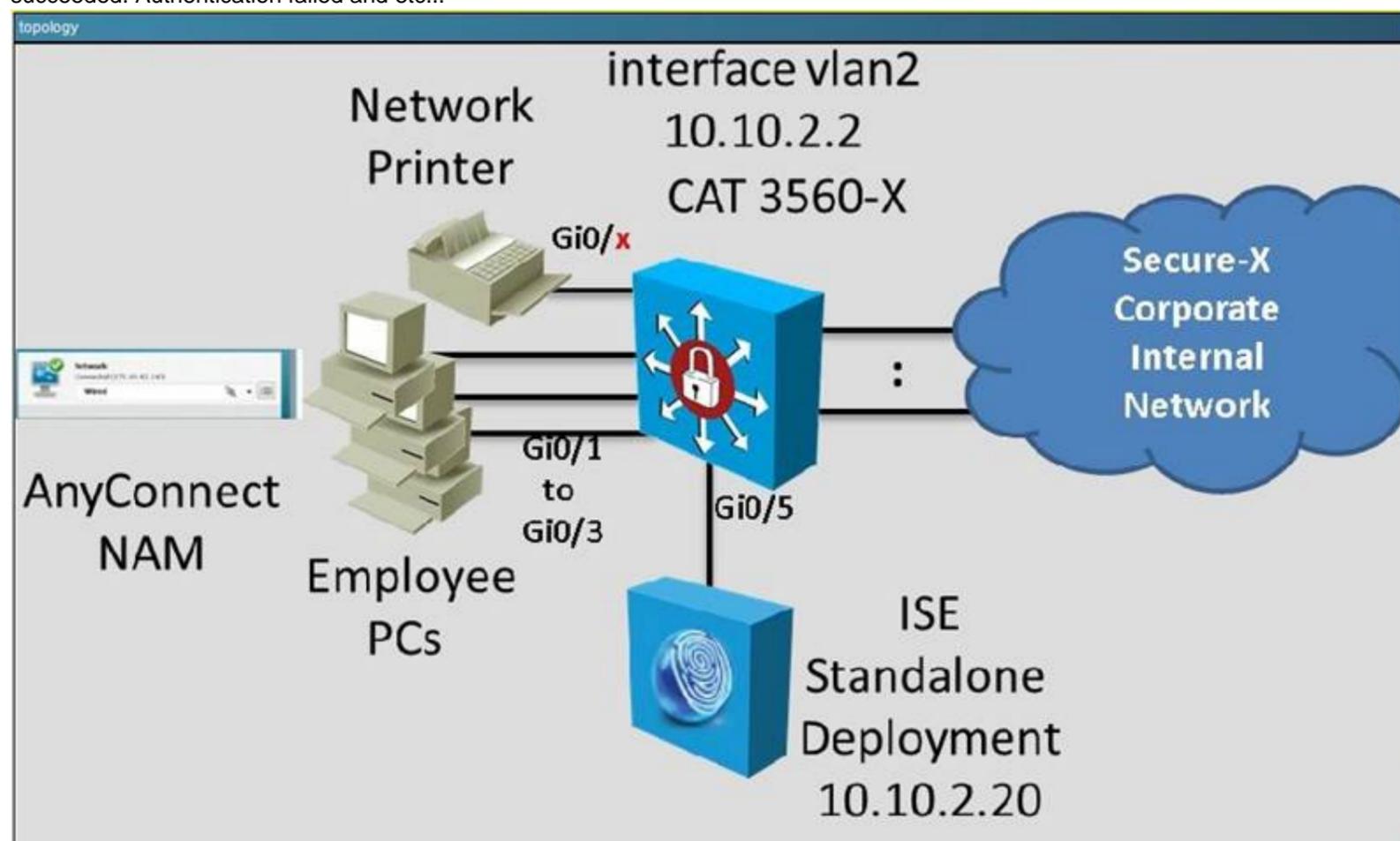
When you select Centralized Web Auth in the ISE Authorization Profile, which two components host the web authentication portal? (Choose two.)

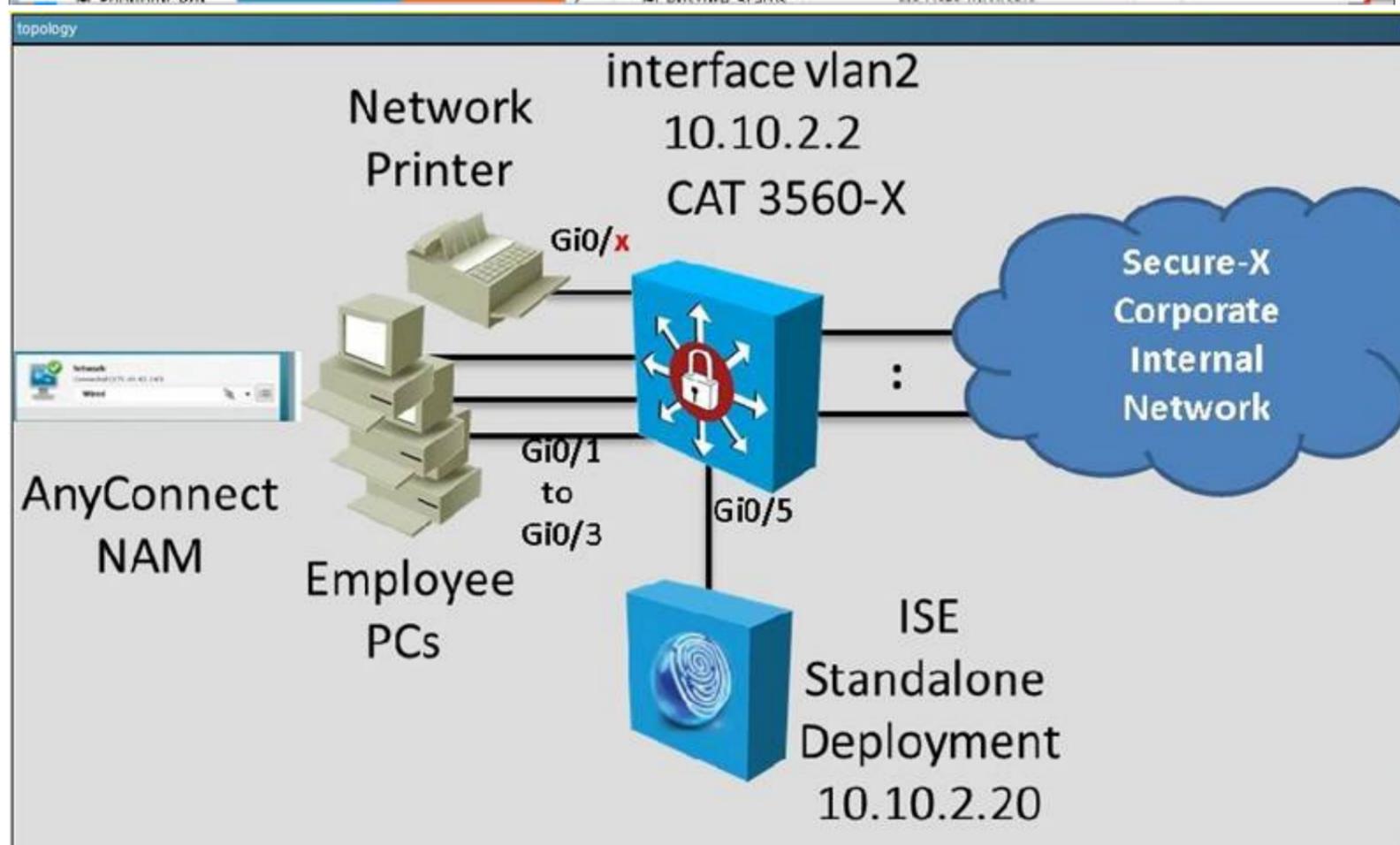
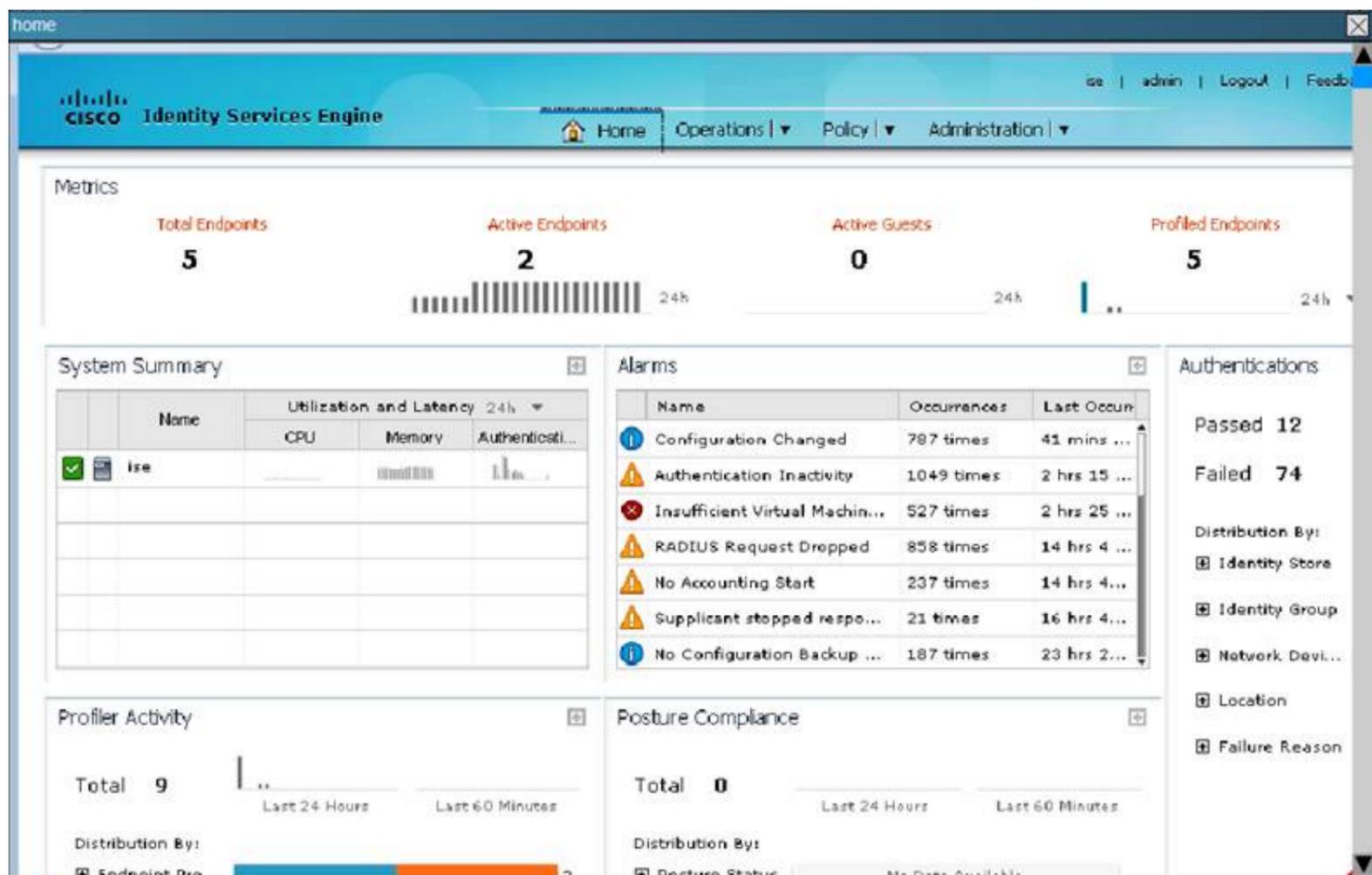
- A. ISE
- B. the WLC
- C. the access point
- D. the switch
- E. the endpoints

Answer: BD

NEW QUESTION 436

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...





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

Answer: AE

Explanation: Event Details:

Identity Services Engine

Overview

Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-Employee_Restricted_DACL-52777003
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	ise
Event	5232 DACL Download Succeeded
Failure Reason	
Resolution	
Root cause	
Username	#ACSACL#-IP-Employee_Restricted_DACL-52777003
User Type	
Endpoint Id	
Endpoint Profile	

NAS Port Type	
Authorization Profile	
Posture Status	
Security Group	
Response Time	3

Other Attributes

ConfigVersionId	8
DestinationPort	1645
Protocol	Radius
AcSSessionID	ise/188683442/376
CPMSessionID	0a0a0214000000635
Location	Location#All Location
Device Type	Device Type#All Devi
RADIUS Username	#ACSACL#-IP-Empto
Device IP Address	10.10.2.2
CiscoAVPair	aaa:service=ip_admin
aaa:event	acl-download

Identity Services Engine

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
Device Type	
Location	HQ
NAS IP Address	10.10.2.2
NAS Port Id	
NAS Port Type	

Protocol	Radius
AcSSessionID	ise/188683442/376
CPMSessionID	0a0a0214000000635
Location	Location#All Location
Device Type	Device Type#All Devi
RADIUS Username	#ACSACL#-IP-Empto
Device IP Address	10.10.2.2
CiscoAVPair	aaa:service=ip_admin
aaa:event	acl-download

Result

State	ReauthSession:0a0a02
Class	CACS.0a0a0214000000
cisco-av-pair	ip:inacl#1=deny icmp a
cisco-av-pair	ip:inacl#2=deny icmp a
cisco-av-pair	ip:inacl#3=deny tcp an
cisco-av-pair	ip:inacl#4=permit ip an

display continue →

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

NEW QUESTION 438

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

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

Answer: D

NEW QUESTION 443

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

Answer: AB

NEW QUESTION 444

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.

Answer: A

NEW QUESTION 449

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

Answer: A

NEW QUESTION 454

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

Answer: A

NEW QUESTION 459

Refer to the exhibit.

In a distributed deployment of Cisco ISE, which column in Figure 1 is used to fill in the Host Name field in Figure 2 to collect captures on Cisco ISE while authenticating the specific endpoint?

- A. Server
- B. Network Device
- C. Endpoint ID
- D. Identity

Answer: A

NEW QUESTION 463

Where is dynamic SGT classification configured?

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

Answer: A

NEW QUESTION 467

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.

Answer: A

NEW QUESTION 471

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

- A. TACACS External Servers
- B. TACACS+ Authentication Settings
- C. TACACS Server Sequence
- D. Enable Device Admin Service
- E. TACACS Command Sets
- F. TACACS Profiles
- G. Device Administration License

Answer: DG

NEW QUESTION 473

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 802.1Xsupplcanto 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.

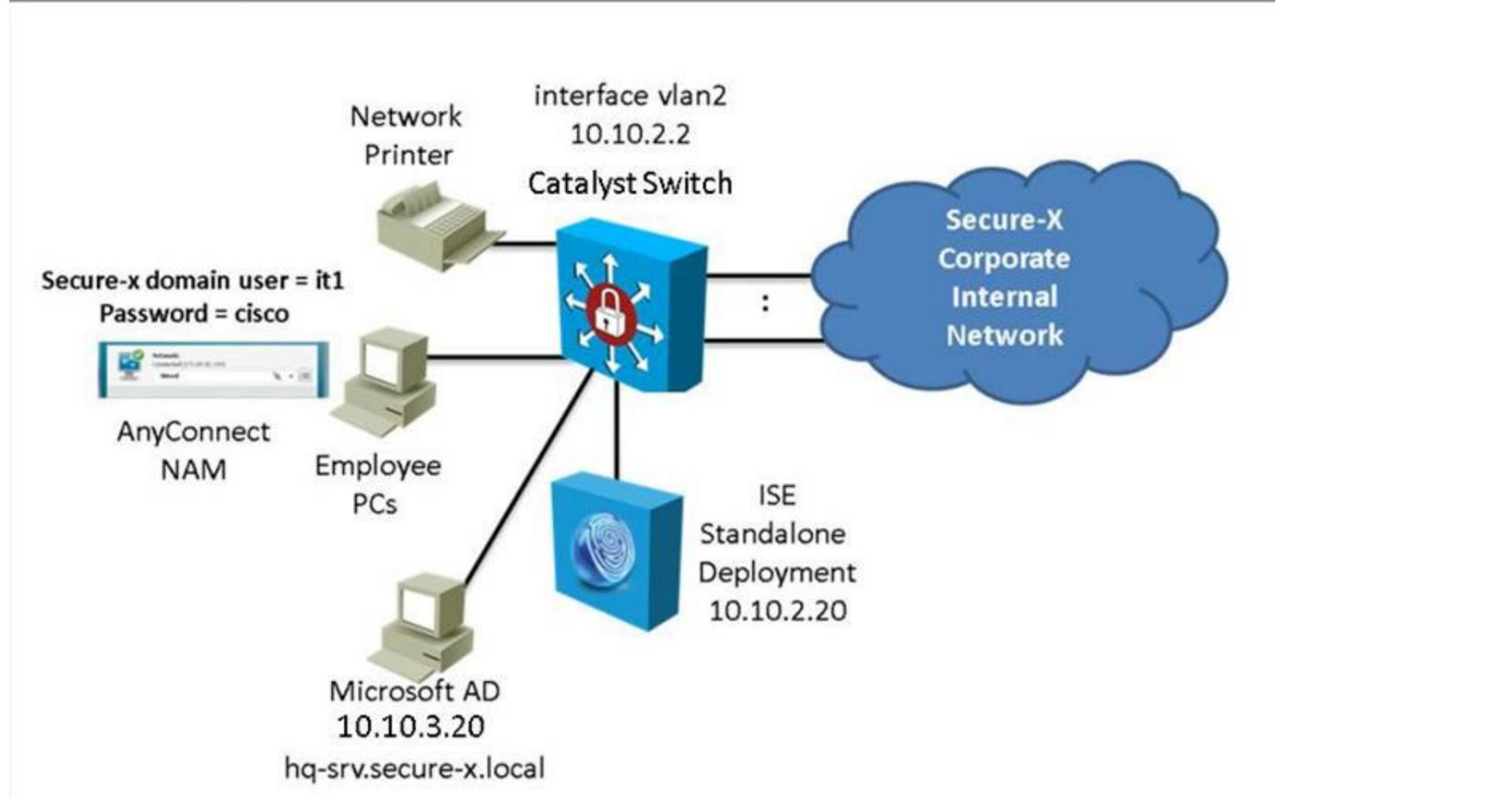
Another network security engineer responsible for managing the Cisco ISE has already pre-configured all the requirements on the Cisco ISE, including adding the network printer MAC address to the Cisco ISE endpoint database and etc...

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 802.1X fails
- 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.

Note: 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.



Answer:

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 state
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

HQ-Sw#
```

NEW QUESTION 478

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.

Answer: A

NEW QUESTION 481

In Cisco ISE 1.3, which feature is available to a sponsor in a sponsor group?

- A. Help employees add and manage new devices by entering the MAC address for the device.
- B. Restrict sponsors from viewing guest passwords.
- C. Allow the user to download a native supplicant profile.
- D. Reinstate or delete devices that were registered previously.

Answer: B

NEW QUESTION 482

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

Answer: A

NEW QUESTION 487

Which two NAC agents support file remediation? (Choose two.)

- A. Web Agent for Macintosh
- B. NAC Agent for Windows
- C. NAC Agent for Macintosh
- D. Web Agent for UNIX
- E. Web Agent for Windows

Answer: BE

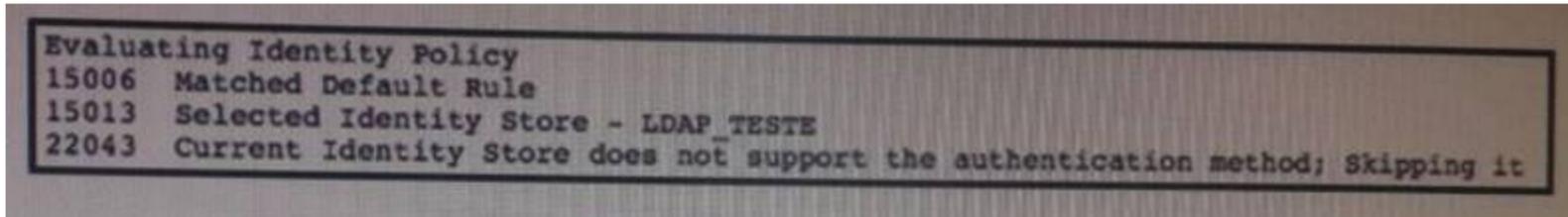
NEW QUESTION 488

Which advanced option within a WLAN must be enabled to trigger central web authentication for wireless users?

- A. AAA override
- B. Static IP tunnelling
- C. Diagnostic channel
- D. DHCP server

Answer: A

NEW QUESTION 490



Refer to the exhibit. Which authentication method is being used?

- A. PEAP-MSCHAP
- B. EAP-GTC
- C. EAP-TLS
- D. PEAP-TLS

Answer: A

Explanation: These authentication methods are supported with LDAP:

Extensible Authentication Protocol – Generic Token Card (EAP-GTC) Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) Protected Extensible Authentication Protocol – Transport Layer Security (PEAP-

NEW QUESTION 494

Which remediation type ensures that Automatic Updates configuration is turned on Windows clients per security policy to remediate Windows clients for posture compliance?

- A. AS Remediation
- B. File Remediation
- C. Launch Program Remediation
- D. Windows Update Remediation
- E. Windows Server Update Services Remediation

Answer: C

NEW QUESTION 495

Scenario:

Currently, many users are experiencing problems using their AnyConnect NAM supplicant to login to the network. The IT desktop support staff have already examined and verified the AnyConnect NAM configuration is correct.

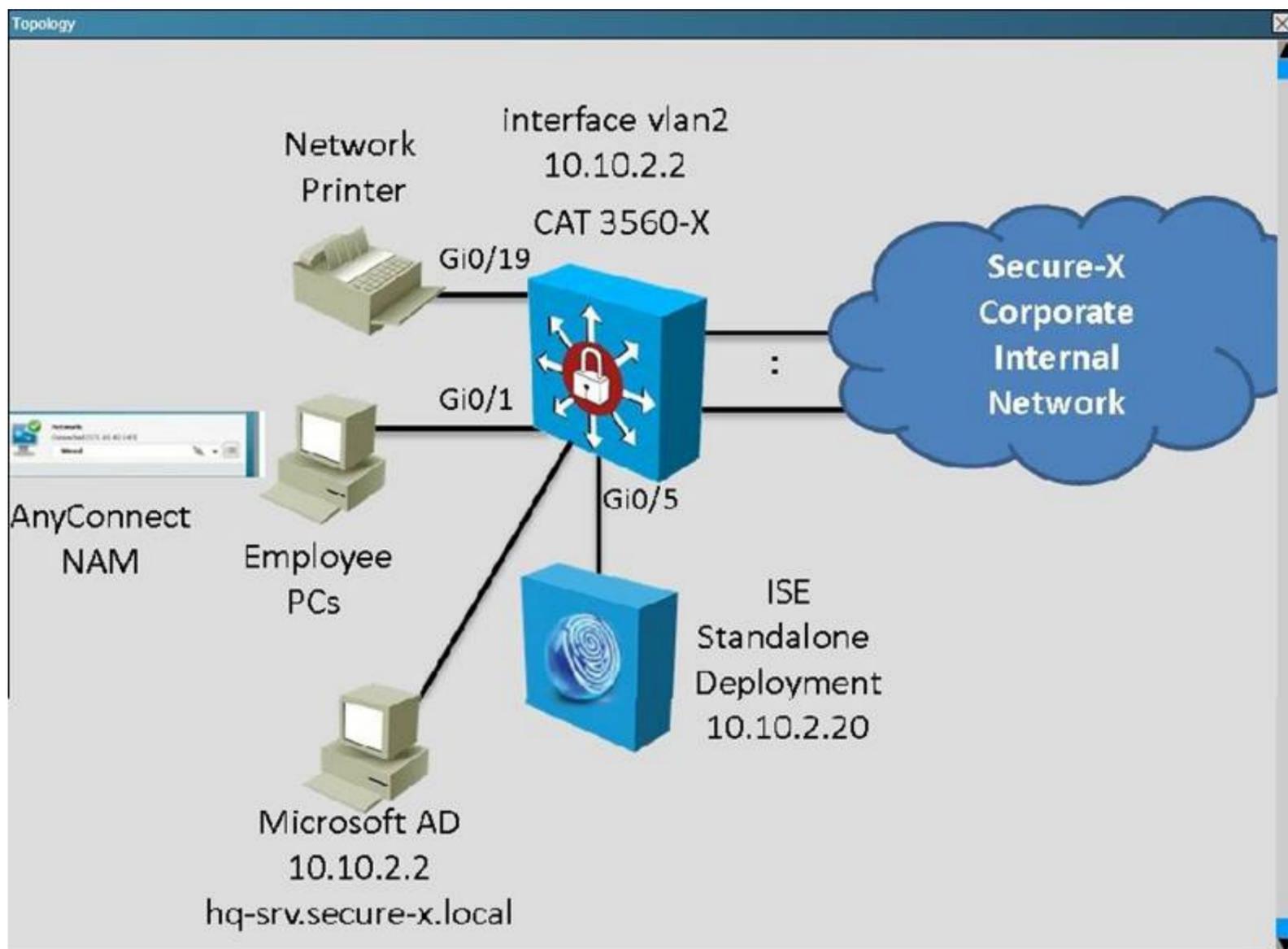
In this simulation, you are tasked to examine the various ISE GUI screens to determine the ISE current configurations to help isolate the problems. Based on the current ISE configurations, you will need to answer three multiple choice questions.

To access the ISE GUI, click on the ISE icon in the topology diagram to access the ISE GUI.

Not all the ISE GUI screens are operational in this simulation and some of the ISE GUI operations have been reduced in this simulation.

Not all the links on each of the ISE GUI screens work, if some of the links are not working on a screen, click Home to go back to the Home page first. From the Home page, you can access all the required screens.

To view some larger GUI screens, use the simulation window scroll bars. Some of the larger GUI screens only show partially but will include all information required to complete this simulation.



The screenshot displays the Cisco ISE administration interface. Key sections include:

- Metrics**: Total Endpoints: 5, Active Endpoints: 2, Active Guests: 0, Profiled Endpoints: 5.
- System Summary**: A table with columns for Name, Utilization and Latency (CPU, Memory), and Authentication.
- Alarms**: A list of events including Configuration Changed (707 times), Authenticator Inactivity (1049 times), Insufficient Virtual Machin... (527 times), RADIUS Request Dropped (858 times), No Accounting Start (237 times), Supplicant stopped respo... (21 times), and No Configuration Backup... (187 times).
- Authentications**: Summary showing 12 Passed and 74 Failed attempts, with a distribution by Identity Store, Identity Group, Network Data..., Location, and Failure Reason.
- Profiler Activity**: Total 9, with a distribution by Endpoint...
- Posture Compliance**: Total 0, with a distribution by Posture Status...

Which two of the following statements are correct? (Choose two.)

- A. The ISE is not able to successfully connect to the hq-srv.secure-x.local AD server.
- B. local AD server.
- C. The ISE internal endpoints database is used to authenticate any users not in the Active Directory domain.
- D. The ISE internal user database has two accounts enabled: student and test that maps to the Employee user identity group.
- E. Guest_Portal_Sequence is a built-in identity source sequence.

Answer: BD

NEW QUESTION 496

Refer to the exhibit.

aaa new-model

radius-server host 10.0.0.12 key secret12

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

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

Answer: B

NEW QUESTION 499

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

- A. Cisco AnyConnect NAM and Cisco Access Control Server
- B. Cisco Secure Services Client and Cisco Access Control Server
- C. Cisco AnyConnect NAM and Cisco Identity Service Engine
- D. Windows Native Supplicant and Cisco Identity Service Engine

Answer: C

NEW QUESTION 502

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

Answer: BC

NEW QUESTION 503

What are two methods of enforcement with SGTs?

- A. SG-ACLs on switches.
- B. SG-ACLs on routers.
- C. SG-Firewalls.
- D. SG-Appliances.
- E. SGTs are not enforced.

Answer: AC

NEW QUESTION 508

A security engineer has configured a switch port in 802.1X closed mode. Which protocol is allowed to pass through before a device is authenticated?

- A. Bootps
- B. HTTP
- C. PXE
- D. EAPoL
- E. ARP

Answer: D

NEW QUESTION 509

A user reports that a switch's RADIUS accounting packets are not being seen on the Cisco ISE server. Which command is the user missing in the switch's configuration?

- A. radius-server vsa send accounting
- B. aaa accounting network default start-stop group radius
- C. aaa accounting resource default start-stop group radius
- D. aaa accounting exec default start-stop group radius

Answer: A

NEW QUESTION 513

Which three options can be pushed from Cisco ISE server as part of a successful 802.1x authentication. (Choose three)

- A. authentication order
- B. posture status
- C. authentication priority

- D. vlan
- E. DACL
- F. re-authentication timer

Answer: DEF

NEW QUESTION 516

An engineer is investigating an issue with their Posture Run-time Services implementation. Which protocol services are used by NAC Agents to communicate with NAC Servers?

- A. SWISS
- B. IPsec
- C. IKEv2
- D. FIX

Answer: A

NEW QUESTION 518

Within a BYOD environment, when employees add devices using the My Devices Portal, which Identity Group does Cisco ISE add the endpoints to?

- A. Registered
- B. Employee
- C. Guest
- D. Profiled

Answer: D

NEW QUESTION 520

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

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

Answer: B

NEW QUESTION 525

Which three events immediately occur when a user clicks "Register" on their device in a single-SSID BYOD onboarding registration process (Choose three).

- A. CA certificate is sent to the device from Cisco ISE
- B. An endpoint is added to a RegisterDevices identity group
- C. RADIUS access request is sent to Cisco ISE
- D. The profile service is sent to the device from Cisco ISE
- E. dACL is sent to the device from Cisco ISE
- F. BYOD registration flag is set by Cisco ISE

Answer: ABF

NEW QUESTION 528

Which description of the use of low-impact mode in a Cisco ISE deployment is correct?

- A. It continues to use the authentication open capabilities of the switch port, which allows traffic to enter the switch before an authentication result.
- B. Low-impact mode must be the final phase in deploying Cisco ISE into a network environment using the phased approach.
- C. The port does not allow any traffic before the authentication (except for EAP, Cisco Discovery Protocol, and LLDP), and then the port is assigned to specific authorization results after the authentication.
- D. It enables authentication (with authentication open), sees exactly which devices fail and which succeed, and corrects the failed authentications before they cause any problems.

Answer: A

NEW QUESTION 532

Which 2 options are functional components of the posture service?

- A. Quarantined policy
- B. Posture policy
- C. Client provisioning
- D. Network provisioning

Answer: BC

NEW QUESTION 534

SGt assignment when authentication is not available or SGT method for non authenticating devices ? Answer: dynamic

Answer:

NEW QUESTION 535

A network administrator wants to use dynamic VLAN assignment from Cisco ISE. Which option must be configured on the switch to support this?

- A. AAA authentication
- B. VTP
- C. DTP
- D. AAA authorization

Answer: D

NEW QUESTION 537

When using endpoint access control, which two access methods are valid for authentication and authorization? (Choose two.)

- A. Microsoft Challenge Handshake Authentication
- B. Protected extensible authentication
- C. MAC Authentication Bypass
- D. Password Authentication Protocol Bypass
- E. Web authentication

Answer: CE

NEW QUESTION 541

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.

Answer: BD

NEW QUESTION 544

An engineer of company A will be sending guest credentials through SMS to conference participants. Which portal must be used to create them?

- A. SMS
- B. Sponsor
- C. Guest
- D. User

Answer: A

NEW QUESTION 549

if user want to use his corporate laptop in another network ,what is only agent can work with this environment?

Answer:

Explanation: Cisco NAC agent.

NEW QUESTION 552

An engineer of Company A wants to know what kind of devices are connecting to the network. Which service can be enabled on the Cisco ISE node?

- A. central web authentication
- B. posture
- C. MAB
- D. profiling

Answer: D

Explanation: Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database.

NEW QUESTION 556

An engineer wants to migrate 802.1X deployment phase from Open to Low-Impact mode. Which option must be configured on the switch port?

- A. open authentication to the domain
- B. ingress access list applied to the interface
- C. authentication host mode to multiple authentication

D. authentication host mode to multiple domain

Answer: B

NEW QUESTION 557

Which CoA type does a Cisco ISE PSN send to a network access device when a NAG agent reports the OS patch status of a noncompliant endpoint?

- A. CoA-Terminate
- B. CoA-PortBounce
- C. CoA-Reauth
- D. CoA-Remediate

Answer: C

NEW QUESTION 561

What are the four code fields which identify the type of an EAP packet?

- A. Request, Reply, Accept, Reject
- B. Request, Reply, Success, Failure
- C. Request, Response, Success, Failure
- D. Request, Respons
- E. Accept Reject

Answer: C

NEW QUESTION 562

What are three ways that an SGT can be assigned to network traffic?

- A. Manual binding of the IP address to an SGT
- B. Manually configured on the switch port
- C. Dynamically assigned by the network access device
- D. Dynamically assigned by the 802.1X authorization result
- E. Manually configured in the NAC agent profile
- F. Dynamically assigned by the AnyConnect network access manager

Answer: ABD

NEW QUESTION 566

Which two attributes are delivered by the DHCP probe to the Cisco ISE? (Choose two.)

- A. dhcp-client-identifier
- B. framed-IP-address
- C. host-name
- D. calling-station-ID
- E. MAC address

Answer: AC

NEW QUESTION 570

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

- A. TCP 8443
- B. TCP/UDP 8905
- C. TCP/UDP 8909
- D. TCP 443

Answer: C

Explanation: 8909 : web, cisco nac agent, supplicant provisioning wizard installation 8905 : Cisco NAC agent update

NEW QUESTION 574

A network administration wants to set up a posture condition on Cisco ISE to check for the file name Posture.txt in C:\ on a Windows machine. Which condition must the network administrator configuration?

- A. Service condition
- B. Registry condition
- C. Application condition
- D. File condition

Answer: D

NEW QUESTION 577

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

Answer: AB

NEW QUESTION 580

Refer to the exhibit.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

Which statement describes this switch configuration?

- A. 802.1x is disabled on the switch port and all traffic is allowed as normal without restriction.
- B. The switch port begins in the unauthorized state and does not allow EAPOL, Cisco Discovery Protocol, and STP traffic.
- C. The switch port begins in the unauthorized state and allows only EAPOL, Cisco Discovery Protocol, and STP traffic.
- D. 802.1x is enabled on the switch port and the switch port ignores all traffic.

Answer: C

NEW QUESTION 582

Scenario:

Currently, many users are experiencing problems using their AnyConnect NAM supplicant to login to the network. The IT desktop support staff have already examined and verified the AnyConnect NAM configuration is correct.

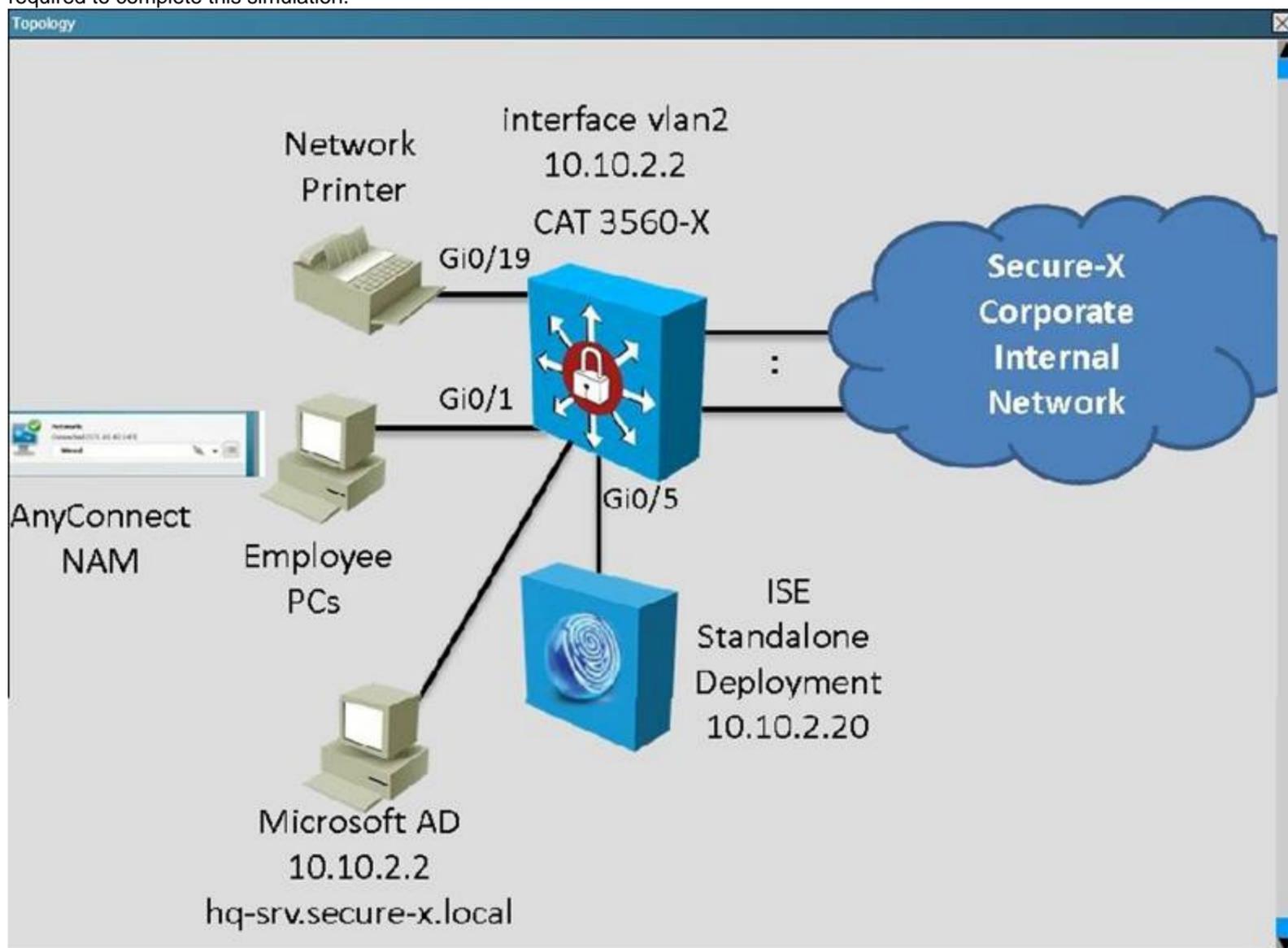
In this simulation, you are tasked to examine the various ISE GUI screens to determine the ISE current configurations to help isolate the problems. Based on the current ISE configurations, you will need to answer three multiple choice questions.

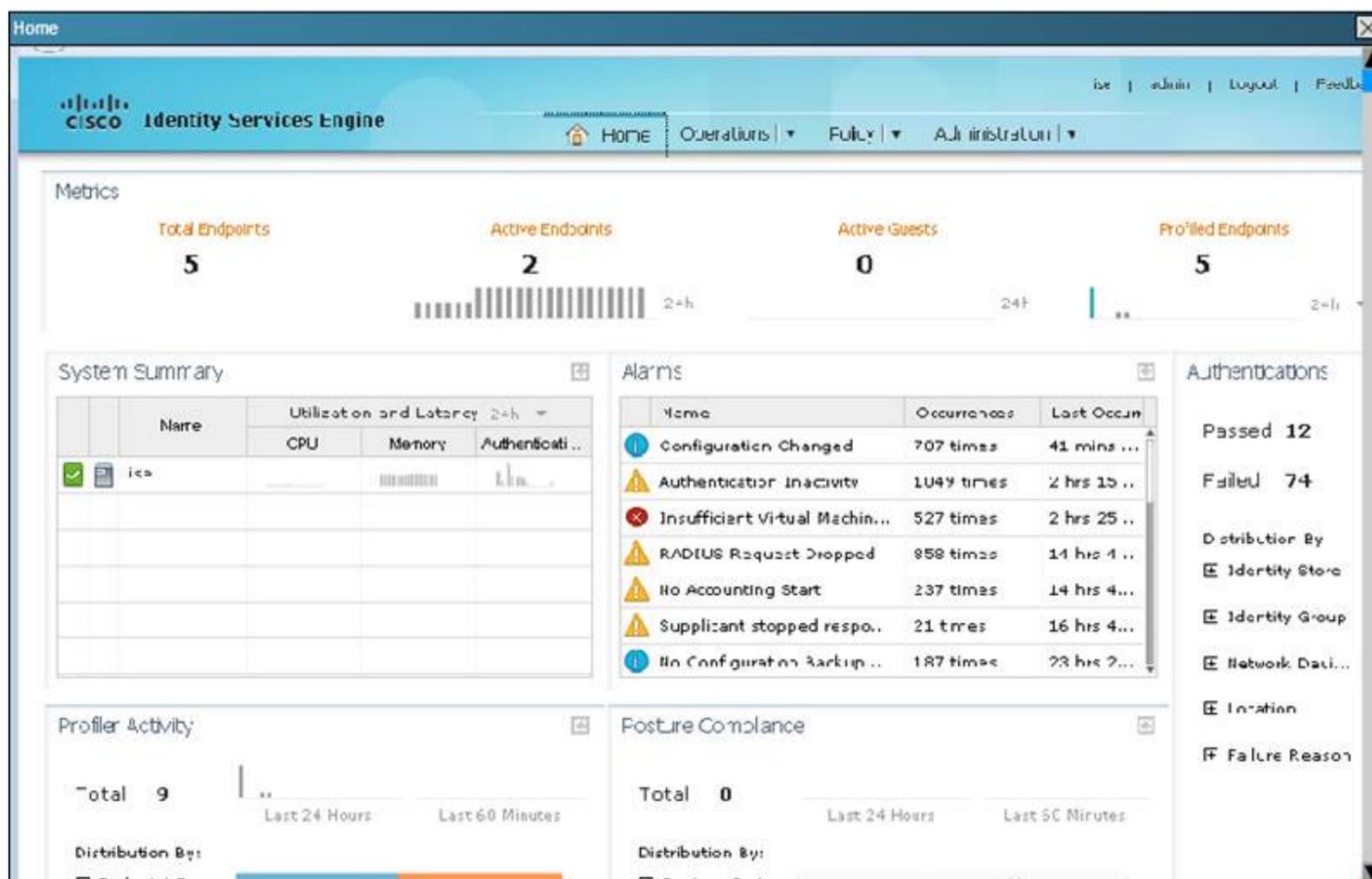
To access the ISE GUI, click on the ISE icon in the topology diagram to access the ISE GUI.

Not all the ISE GUI screen are operational in this simulation and some of the ISE GUI operations have been reduced in this simulation.

Not all the links on each of the ISE GUI screen works, if some of the links are not working on a screen, click Home to go back to the Home page first. From the Home page, you can access all the required screens.

To view some larger GUI screens, use the simulation window scroll bars. Some of the larger GUI screens only shows partially but will include all information required to complete this simulation.





Determine which can be two reasons why many users like the Sales and IT users are not able to authenticate and access the network using their AnyConnect NAM client with EAP-FAST.(Choose two.)

- A. The Dot1X authentication policy is not allowing the EAP-FAST protocol.
- B. The rr_Corp authorization profile has the wrong Access Type configured.
- C. The authorization profile used for the Sales users is misconfigured.
- D. The order for the MAB authentication policy and the Dot1X authentication policy should be reversed.
- E. Many of the IT Sales and IT user machines are not passing the ISE posture assessment.
- F. The PERMr_ALL_TRAFFICDACL is missing the permit ip any any statement at the end.
- G. The Employee_FullAccess_DACL DACL is missing the permit ip any any statement in the end.

Answer: AD

NEW QUESTION 586

Prime Uses Which protocol for devices discovery ?

Answer:

Explanation: RARP,LLDP

NEW QUESTION 587

if the user in non-compliant state and want to Get out of quarantine ?

Answer:

Explanation: download posture

NEW QUESTION 588

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

- A. radius-server timeout
- B. idle-timeout attribute
- C. session-timeout attribute
- D. termination-action attribute

Answer: B

Explanation:

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

When the inactivity timer is enabled, the switch monitors the activity from authenticated endpoints. When the inactivity timer expires, the switch removes the authenticated session.

The inactivity timer for MAB can be statically configured on the switch port, or it can be dynamically assigned using the RADIUS Idle-Timeout attribute (Attribute 28).

Cisco recommends setting the timer using the RADIUS attribute because this approach lets gives you control over which endpoints are subject to this timer and

the length of the timer for each class of endpoints.

For example, endpoints that are known to be quiet for long periods of time can be assigned a longer inactivity timer value than chatty endpoints.

NEW QUESTION 591

Which 802.1x command is needed for ACL to be applied on a switch port?

- A. dot1x system-auth-control
- B. dot1x pae authenticator
- C. authentication port-control auto
- D. radius-server vsa send authentication
- E. aaa authorization network default group radius

Answer: D

NEW QUESTION 592

Which two are best practices to implement profiling services in a distributed environment? (Choose two)

- A. use of device sensor feature
- B. configuration to send syslogs to the appropriate profiler node
- C. netflow probes enabled on central nodes
- D. node-specific probe configuration
- E. global enablement of the profiler service

Answer: BD

Explanation: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html#wp1340515

You can deploy the Cisco ISE profiler service either in a standalone environment (on a single node), or in a distributed environment (on multiple nodes).

Depending on the type of your deployment and the license you have installed, the profiler service of Cisco ISE can run on a single node or on multiple nodes.

You need to install either the base license to take advantage of the basic services or the advanced license to take advantage of all the services of Cisco ISE.

The ISE distributed deployment includes support for the following:

- The Deployment Nodes page supports the infrastructure for the distributed nodes in the distributed deployment.
- A node specific configuration of probes—The Probe Config page allows you to configure the probe per node.
- Global Implementation of the profiler Change of Authorization (CoA).
- Configuration to allow syslogs to be sent to the appropriate profiler node.

NEW QUESTION 596

Which option is the code field of an EAP packet?

- A. one byte and 1=request, 2=response 3=failure 4=success
- B. two byte and 1=request, 2=response, 3=success, 4=failure
- C. two byte and 1=request 2=response 3=failure 4=success
- D. one byte and 1=request 2=response 3=success 4=failure

Answer: D

NEW QUESTION 598

During BYOD flow, where does a Microsoft Windows 8.1 PC download the Network Setup Assistant from?

- A. from Cisco App Store
- B. from Cisco ISE directly
- C. from Microsoft App Store
- D. It uses the native OTA functionality.

Answer: B

NEW QUESTION 600

Which devices support download of environmental data and IP from Cisco ISE to SGT bindings in their SGFW implementation?

- A. Cisco ASA devices
- B. Cisco ISR G2 and later devices with ZBFW
- C. Cisco ISR G3 devices with ZBFW
- D. Cisco ASR devices with ZBFW

Answer: C

NEW QUESTION 602

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. Approvetime
- D. Custom
- E. Starttime

Answer: AB

NEW QUESTION 607

Which two component are required for creating native supplicant profile ?

- A. Operative System
- B. Connection type wired/wireless
- C. Ios Suttten
- D. BYOD

Answer: AB

NEW QUESTION 611

Which two options enable security group tags to the assigned to a session?

- A. Firewall
- B. DHCP
- C. ACL
- D. Source VLAN
- E. ISE

Answer: AE

NEW QUESTION 612

When using CA for identity source, which method can be used to provide real-time certificate validation?

- A. X.509
- B. PKI
- C. OCSP
- D. CRL

Answer: D

NEW QUESTION 614

What are two actions that can occur when an 802.1X-enabled port enters violation mode? (Choose two.)

- A. The port is error disabled.
- B. The port drops packets from any new device that sends traffic to the port.
- C. The port generates a port resistance error.
- D. The port attempts to repair the violation.
- E. The port is placed in quarantine state.
- F. The port is prevented from authenticating indefinitely.

Answer: AB

NEW QUESTION 619

Which type of SGT classification method is required when authentication is unavailable?

- A. Bypass
- B. Dynamic
- C. Static
- D. Inline

Answer: C

NEW QUESTION 621

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

Answer: AC

NEW QUESTION 626

In a Cisco ISE deployment, which traffic is permitted by the default dynamic ACL?

- A. all IP traffic
- B. management traffic only
- C. TCP traffic only
- D. UDP traffic only

Answer: A

NEW QUESTION 627

Which two additional fields are added to an Ethernet frame when implementing MACsec? (Choose two.)

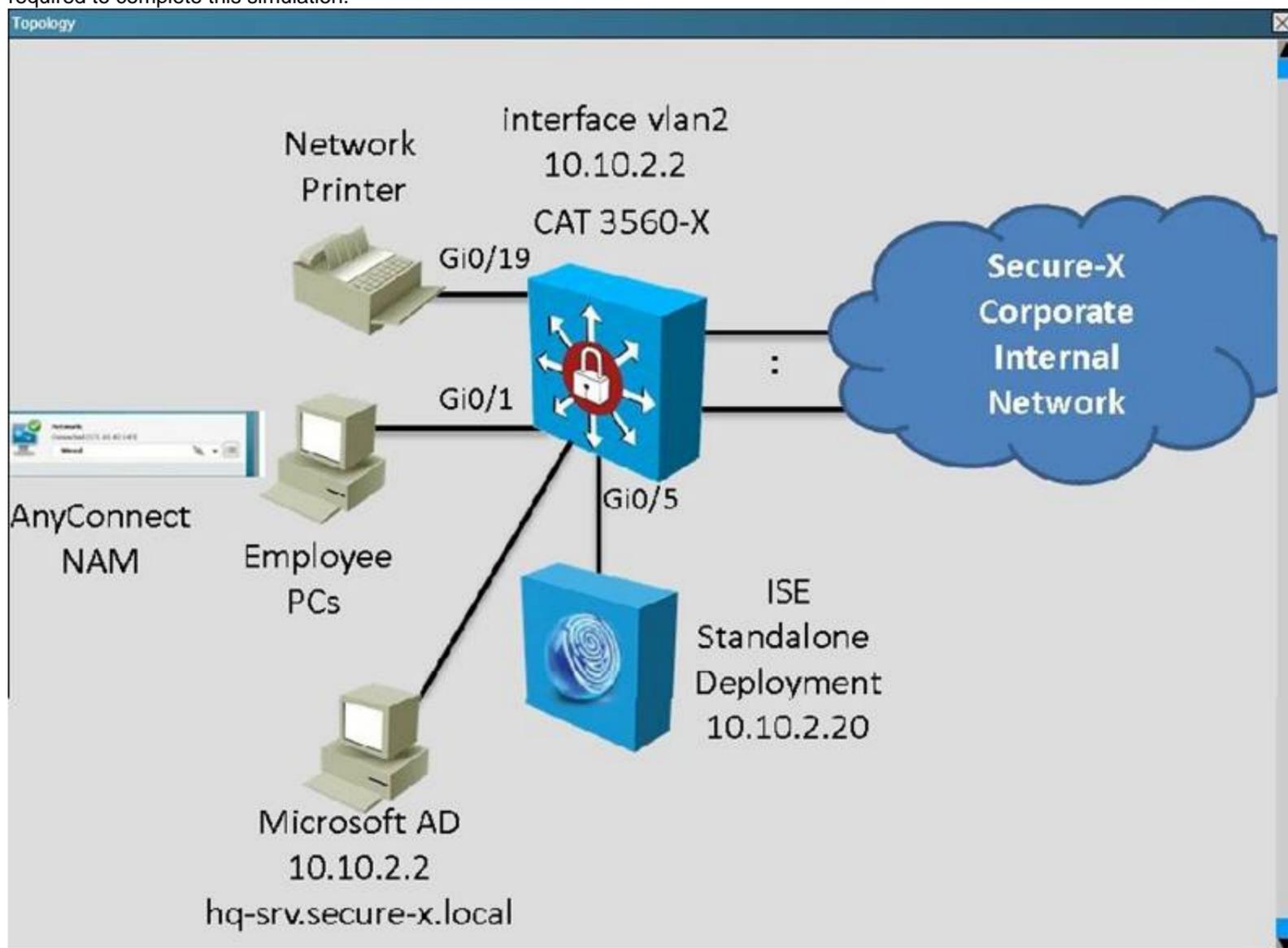
- A. encapsulating security payload
- B. authentication header
- C. message authentication code
- D. authentication host mode
- E. security tag

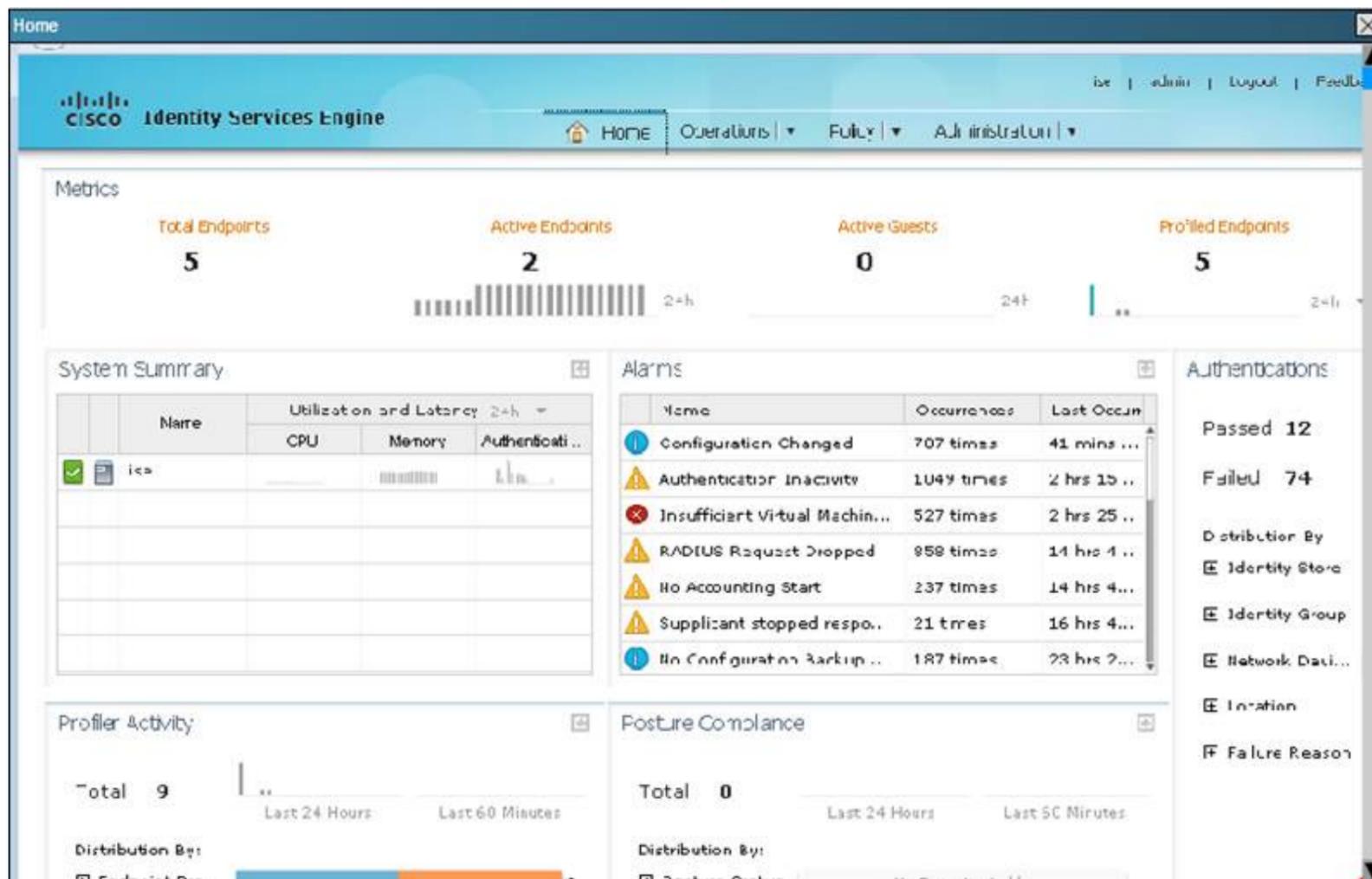
Answer: CE

NEW QUESTION 631

Scenario:

Currently, many users are experiencing problems using their AnyConnect NAM supplicant to login to the network. The rr desktop support staff have already examined and verified the AnyConnect NAM configuration is correct. In this simulation, you are tasked to examine the various ISE GUI screens to determine the ISE current configurations to help isolate the problems. Based on the current ISE configurations, you will need to answer three multiple choice questions. To access the ISE GUI, click on the ISE icon in the topology diagram to access the ISE GUI. Not all the ISE GUI screen are operational in this simulation and some of the ISE GUI operations have been reduced in this simulation. Not all the links on each of the ISE GUI screen works, if some of the links are not working on a screen, click Home to go back to the Home page first. From the Home page, you can access all the required screens. To view some larger GUI screens, use the simulation window scroll bars. Some of the larger GUI screens only shows partially but will include all information required to complete this simulation.





Which of the following statement is correct?

- A. Currently, IT users who successfully authenticate will have their packets tagged with aSGT of 3.
- B. Currently, IT users who successfully authenticate will be assigned to VLAN 9.
- C. Currently, any domain administrator who successfully authenticates will be assigned to VLAN 10.
- D. Computers belonging to the secure-x domain which pass machine authentication but failed user authentication will have the Employee_Restricted_DACL applied.
- E. Print Servers matching the Linksys-PrintServer identity group will have the following access restrictions: permit icmp any host 10.10.2.20 permit tcp any host 10.10.2.20 eq 80 permit icmp any host 10.10.3.20 permit tcp any host 10.10.3.20 eq 80 deny ip any any

Answer: C

NEW QUESTION 634

Which ISE feature is used to facilitate a BYOD deployment?

- A. self-service personal device registration and onboarding
- B. Guest Service Sponsor Portal
- C. Local Web Auth
- D. Guest Identity Source Sequence

Answer: A

NEW QUESTION 636

Which two options can be pushed from Cisco ISE server as part of successful 802.1x authentication?

- A. Reauthentication timer
- B. DACL
- C. Vlan
- D. Authentication order
- E. Posture status
- F. Authentication priority

Answer: BC

NEW QUESTION 637

An engineer must ensure that all client operating systems have the AnyConnect Agent for an upcoming posture implementation. Which two versions of OS does the AnyConnect posture agent support? (Choose two.)

- A. Google Android
- B. Ubuntu
- C. Apple Mac OS X
- D. Microsoft Windows
- E. Red Hat Enterprise Linux

Answer: CD

NEW QUESTION 638

A malicious user gained network access by spoofing printer connections that were authorized using MAB on four different switch ports at the same time. What two catalyst switch security features will prevent further violations? (Choose two)

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

Answer: AE

Explanation: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

DHCP snooping is fully compatible with MAB and should be enabled as a best practice.

Dynamic Address Resolution Protocol (ARP) Inspection (DAI) is fully compatible with MAB and should be enabled as a best practice.

In general, Cisco does not recommend enabling port security when MAB is also enabled.

Since MAB enforces a single MAC address per port (or per VLAN when multidomain authentication is configured for IP telephony), port security is largely redundant and may in some cases interfere with the expected operation of MAB.

NEW QUESTION 639

Which technology performs CoA support Posture Service?

- A. External root CA
- B. Cisco ACS
- C. Cisco ISE
- D. Internal root CA

Answer: C

NEW QUESTION 642

Where is dynamic SGT classification configured?

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

Answer: A

NEW QUESTION 647

Which two simple posture conditions are valid?

- A. Service
- B. Antispyware
- C. Firewall
- D. File
- E. Antivirus

Answer: AD

NEW QUESTION 650

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.

Answer: A

NEW QUESTION 655

If an endpoint is marked noncompliant during that download, a CoA is sent and the device is forced to reauthenticate, providing a different result (such as quarantine).

- A. quarantine
- B. exit
- C. default
- D. end

Answer: A

NEW QUESTION 656

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 300-208 Exam with Our Prep Materials Via below:

<https://www.certleader.com/300-208-dumps.html>