Vendor: Cisco

Exam Code: 300-715

Exam Name: Implementing and Configuring Cisco Identity Services Engine (SISE)

Version: DEMO

QUESTION 1
An engineer is configuring static SGT classification. Which configuration should be used when authentication is disabled and third-party switches are in use?

A. VLAN to SGT mapping
B. IP Address to SGT mapping
C. L3IF to SGT mapping
D. Subnet to SGT mapping

Answer: B
Explanation:
The method of sending out IP to SGT mappings from ISE is particularly useful if the access switch does not support TrustSec.
https://community.cisco.com/t5/security-knowledge-base/segmentation-strategy/ta-p/3757424

QUESTION 2
An engineer needs to configure a new certificate template in the Cisco ISE Internal Certificate Authority to prevent BYOD devices from needing to re-enroll when their MAC address changes. Which option must be selected in the Subject Alternative Name field?

A. Common Name and GUID
B. MAC Address and GUID
C. Distinguished Name
D. Common Name

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

QUESTION 3
n administrator has added a new Cisco ISE PSN to their distributed deployment.
Which two features must the administrator enable to accept authentication requests and profile the endpoints correctly, and add them to their respective endpoint identity groups? (Choose two)

A. Session Services
B. Endpoint Attribute Filter
C. Posture Services
D. Profiling Services
E. Radius Service

Answer: AD
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_setup_cisco_ise.html#reference_94D3872F7DED4522909A3FF3ECFCDB23
Policy Service Check this check box to enable any one or all of the following services:
Enable Session Services: Check this check box to enable network access, posture, guest, and client-provisioning services.
Enable Profiling Service: Check this check box to enable the Profiling service.

QUESTION 4
An administrator wants to configure network device administration and is trying to decide whether to use TACACS+ or RADIUS. A reliable protocol must be used that can check command authorization. Which protocol meets these requirements and why?

A. TACACS+ because it runs over TCP
B. RADIUS because it runs over UDP
C. RADIUS because it runs over TCP.
D. TACACS+ because it runs over UDP

Answer: A
Explanation:
TACACS+ can check command authorization with shell profile and command sets respectively.

QUESTION 5
A Cisco device has a port configured in multi-authentication mode and is accepting connections only from hosts assigned the SGT of SGT_0422048549. The VLAN trunk link supports a maximum of 8 VLANS. What is the reason for these restrictions?

A. The device is performing inline tagging without acting as a SXP speaker
B. The device is performing mime tagging while acting as a SXP speaker
C. The IP subnet addresses are dynamically mapped to an SGT.
D. The IP subnet addresses are statically mapped to an SGT

Answer: A
Explanation:
The following restrictions are applicable when running Cisco TrustSec in enforcement mode or inline tagging mode. These restrictions do not apply when these switches are used as an SXP speaker:
- An IP subnet address cannot be statically mapped to a Security Group Tag (SGT).
- If a port is configured in multi-authentication mode, all hosts connecting to that port must be assigned the same SGT.
- Cisco TrustSec enforcement mode on a VLAN trunk line supports only up to eight VLANs. If more than eight VLANs are configured on a VLAN trunk link and Cisco TrustSec is enabled on those VLANs.
https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/sxp_config.html#Restriction%20for%20SGT%20Exchange%20Protocol

QUESTION 6
Which Cisco ISE deployment model provides redundancy by having every node in the deployment configured with the Administration. Policy Service, and Monitoring personas to protect from a complete node failure?

A. distributed
B. dispersed
C. two-node
D. hybrid

Answer: A
Explanation:
Only 2 deployments type for Cisco ISE: Standalone, and Distributed ISE Deployments.

Distributed deployments can have several scenarios:
- Small Network Deployments
- Medium-Sized Network Deployments
- Large Network Deployments
https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/install_guide/b_ise_InstallationGuide23/b_ise_InstallationGuide23_chapter_00.pdf

QUESTION 7
An organization has a fully distributed Cisco ISE deployment. When implementing probes, an administrator must scan for unknown endpoints to learn the IP-to-MAC address bindings. The scan is complete on one FPSN, but the information is not available on the others.
What must be done to make the information available?

A. Scanning must be initiated from the PSN that last authenticated the endpoint
B. Cisco ISE must learn the IP-MAC binding of unknown endpoints via DHCP profiling, not via scanning
C. Scanning must be initiated from the MnT node to centrally gather the information
D. Cisco ISE must be configured to learn the IP-MAC binding of unknown endpoints via RADIUS authentication, not via scanning

Answer: A
Explanation:
Given below is additional information related to the manual NMAP scan results:
- To detect unknown endpoints, NMAP should be able to learn the IP/MAC binding via NMAP or a supporting SNMP scan.
- ISE learns IP/MAC binding of known endpoints via Radius authentication or DHCP profiling.
- The IP/MAC bindings are not replicated across PSN nodes in a deployment. Therefore, you must trigger the manual scan from the PSN, which has the IP/MAC binding in its local database (for example, the PSN against which a mac address was last authenticated with).
- The NMAP scan results do not display any information related to an endpoint that NMAP had previously scanned, manually or automatically.
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/reorg/b_endpoint_profiling_2_4.html#concept_57A4A7ADE3DA429A821900C5CBEA8BF0

QUESTION 8
An administrator needs to allow guest devices to connect to a private network without requiring usernames and passwords.
Which two features must be configured to allow for this? (Choose two.)

A. hotspot guest portal
B. device registration WebAuth
C. central WebAuth
D. local WebAuth
E. self-registered guest portal

Answer: AB
Explanation:
Using Device Registration Web Authentication (Device Registration WebAuth) and the Hotspot Guest portal, you can allow guest devices to connect to a private network without requiring usernames and passwords.

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_guest.html#ID1479

QUESTION 9
An administrator is configuring a Cisco WLC for web authentication.
Which two client profiling methods are enabled by default if the Apply Cisco ISE Default Settings check box has been selected? (Choose two.)

A. CDP
B. DHCP
C. HTTP
D. SNMP
E. LLDP

Answer: BC
Explanation:
By default, the DHCP, RADIUS, Network Mapper (NMAP), Simple Network Management Protocol (SNMP) QUERY, and Active Directory probes are enabled.

QUESTION 10
A network administrator is configuring client provisioning resource policies for client machines and must ensure that an agent pop-up is presented to the client when attempting to connect to the network.
Which configuration item needs to be added to allow for this?

A. the client provisioning URL in the authorization policy
B. a temporal agent that gets installed onto the system
C. a remote posture agent proxying the network connection
D. an API connection back to the client

Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_configure_client_provisioning.html#ID1405
It is mandatory to include the client provisioning URL in authorization policy to enable the agent to popup in the client machines. This prevents request from any random clients and ensures that only clients with proper redirect URL can request for posture assessment.

QUESTION 11
An engineer is implementing network access control using Cisco ISE and needs to separate the traffic based on the network device ID and use the IOS device sensor capability.
Which probe must be used to accomplish this task?

A. HTTP probe
B. NetFlow probe
C. network scan probe
D. RADIUS probe

Answer: D
Explanation:

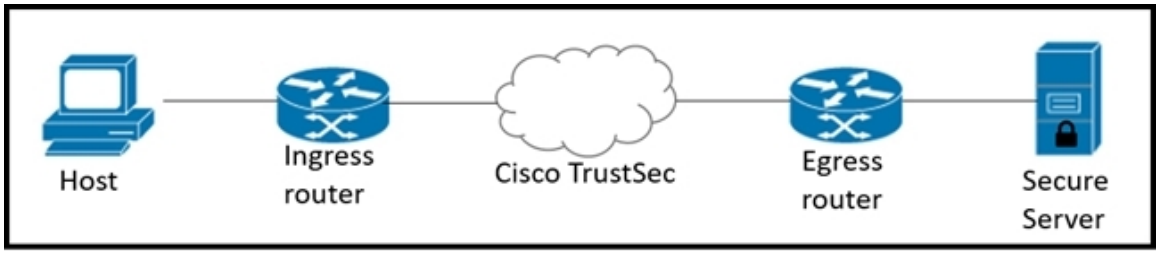
Device Sensor is a feature in a switch or controller that collects endpoint attributes locally and then sends those attributes to ISE within the RADIUS Accounting packets.

QUESTION 12
An administrator is trying to collect metadata information about the traffic going across the network to gam added visibility into the hosts. This Information will be used to create profiling policies for devices us mg Cisco ISE so that network access policies can be used.
What must be done to accomplish this task?

A. Configure the RADIUS profiling probe within Cisco ISE
B. Configure NetFlow to be sent to me Cisco ISE appliance.
C. Configure SNMP to be used with the Cisco ISE appliance
D. Configure the DHCP probe within Cisco ISE

Answer: D
Explanation:
DHCP can be one of the most useful data sources for an endpoint device. A primary use of DHCP in profiling has been to capture the device MAC address, but it can also be used to capture other probes as well. The true value in the DHCP probe is that many other attributes can be gleaned to help identify the type of endpoint. As HTTP carries User-Agent field, DHCP requests carry a Class-Identifier field that helps identify the operating system of a device. Some organizations have been known to use a custom DHCP Class-Identifier string to help identify a device as a corporate asset.

QUESTION 13
Refer to the exhibit. Which component must be configured to apply the SGACL?



A. egress router
B. host
C. secure server
D. ingress router

Answer: A
Explanation:
Cisco TrustSec access control is implemented using ingress tagging and egress enforcement.
https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html#17760

QUESTION 14
An administrator is configuring cisco ISE lo authenticate users logging into network devices using. Which action ensures the users are able to log into the network devices?

A. Enable the device administration service in the Administration persona
B. Enable the session services in the administration persona
C. Enable the service sessions in the PSN persona.
D. Enable the device administration service in the PSN persona.

Answer: D
Explanation:
It is important to know your intended design before you enable the TACACS+ functionality, and you should only enable the Device Admin service on the PSNs that will handle TACACS+ and leave it disabled on any PSNs that are supposed to be dedicated for RADIUS (and vice versa). You should keep the remainder of the session services disabled on the dedicated TACACS+ PSNs.

QUESTION 15
An organization is implementing Cisco ISE posture services and must ensure that a host-based firewall is in place on every Windows and Mac computer that attempts to access the network. They have multiple vendors' firewall applications for their devices, so the engineers creating the policies are unable to use a specific application check in order to validate the posture for this. What should be done to enable this type of posture check?

A. Use the file registry condition to ensure that the firewal is installed and running appropriately.
B. Use a compound condition to look for the Windows or Mac native firewall applications.
C. Enable the default firewall condition to check for any vendor firewall application.
D. Enable the default application condition to identify the applications installed and validade the firewall app.

Answer: C
Explanation:
The Firewall condition checks if a specific Firewall product is enabled on an endpoint. The list of supported Firewall products is based on the OPSWAT support charts. You can enforce policies during initial posture and Periodic Reassessment (PRA). Cisco ISE provides default Firewall conditions for Windows and macOS.
https://community.cisco.com/t5/security-knowledge-base/ise-posture-prescriptive-deployment-guide/ta-p/3680273#toc-hId-1256947692

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**