DUMPSBOSS.

Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)

Cisco 300-740

Version Demo

Total Demo Questions: 7

Total Premium Questions: 73

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture	8
Topic 2, Secure Internet Access	16
Topic 3, Secure Private Access	19
Topic 4, Policy Enforcement	16
Topic 5, Monitoring and Reporting	14
Total	73

QUESTION NO: 1 - (SIMULATION)

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

ANSWER: See the explanation for the answer

Explanation:

The IKEv1 Phase 1 policy must explicitly use AES-256 encryption and SHA-256 hashing. Under the applicable `crypto ikev1 policy` configuration mode, run:

```
encryption aes-256
hash sha256
```

These are the two required policy commands:

```
encryption aes-256
hash sha256
```

For example:

```
crypto ikev1 policy 10
 encryption aes-256
 hash sha256
```

The peer must have a matching IKEv1 policy proposal for Phase 1 negotiation to succeed.

QUESTION NO: 2

Which SAFE component logically arranges the security capabilities into blueprints?

A. Reference Architectures

B. Cisco Validated Designs

C. Places in the Network

D. Secure Domains

ANSWER: A

Explanation:

Reference Architectures is correct because it is the Cisco SAFE component that organizes security capabilities into reusable, outcome-oriented blueprints. A SAFE reference architecture describes how security controls, products, and services should be positioned and integrated to protect a particular environment, use case, or business outcome. Rather than presenting individual technologies in isolation, it provides an architectural view of how capabilities work together across relevant areas of the network and security estate.

This blueprint-oriented structure helps teams translate security requirements into an implementable design. For example, a reference architecture can show the relationships among identity, endpoint protection, secure access, visibility, threat detection, and policy enforcement for a given deployment scenario. It also provides a consistent basis for applying Cisco design guidance and operational best practices while allowing organizations to adapt the design to their own scale and requirements. In SAFE terminology, the architectural blueprint is assembled from broader conceptual elements, including secure domains and places in the network, but the component that logically arranges capabilities into the blueprint itself is the reference architecture. Cisco describes SAFE as a framework of reference architectures and design guidance for building secure solutions: Cisco SAFE. Additional SAFE design resources are available through Cisco SAFE Design Zone.

QUESTION NO: 3

An endpoint has completed a Cisco ISE posture assessment and is marked compliant. The endpoint remains assigned to the restricted authorization result that was applied before the assessment. Which configuration on the network access device must be verified first?

A. RADIUS Change of Authorization support

B. Guest portal sponsorship

C. Local web authentication

D. Static VLAN assignment

ANSWER: A

Explanation:

Change of Authorization must be enabled on the network access device. After ISE receives a compliant posture result, it can send a RADIUS CoA so that the device reauthorizes the session and applies the authorization result for compliant endpoints without requiring the user to reconnect.

Web redirection and client provisioning are necessary to begin many posture workflows, but the assessment has already completed in this scenario. A guest portal configuration does not cause the access device to replace a restricted authorization result after posture status changes.

QUESTION NO: 4

An organization is onboarding users to Duo. Access to protected applications must be denied until a user completes Duo enrollment, but administrators do not want to create individual access policies for every new user. Which Duo configuration should be used?

A. Set the Duo New User Policy to require enrollment.

B. Disable each user until an administrator enrolls a device.

C. Issue a permanent bypass code to each new user.

D. Delete users who have not enrolled a device.

ANSWER: A

Explanation:

The Duo New User Policy determines how Duo handles users who have not completed enrollment. Setting it to require enrollment ensures that a new user must register an authentication method before access to protected applications is granted.

Disabling a user is an incident-containment action, not an enrollment workflow. A bypass code is temporary and does not establish an enrolled factor, while deleting an unenrolled user prevents normal onboarding.

QUESTION NO: 5

An organization requires that users of a SaaS application authenticate with Duo before access is granted. The SaaS provider supports SAML but cannot query the organization’s Active Directory directly. Which design provides centralized authentication and authorization for the application?

A. Configure the SaaS application as the SAML identity provider and Duo as the service provider.

B. Configure Duo Single Sign-On as the SAML identity provider and the SaaS application as the service provider.

C. Configure the SaaS application to use RADIUS directly from each user browser.

D. Install Duo Authentication Proxy on the SaaS provider and use it as the identity provider.

ANSWER: B

Explanation:

Configure Duo Single Sign-On as the SAML identity provider and configure the SaaS application as the service provider. Duo can authenticate the user against its configured identity source, apply Duo access and multifactor-authentication policies, and issue a SAML assertion to the application.

Installing Duo Authentication Proxy on the SaaS provider is not required for a SAML service-provider integration. Configuring the SaaS application as the identity provider reverses the required trust relationship, and using RADIUS alone does not provide the browser-based SAML SSO workflow.

QUESTION NO: 6 - (SIMULATION)

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

E.

Which action must be taken on R1 to enable the connection?

ANSWER: See the explanation for the answer

Explanation:

Configure a reachable DNS resolver in the Umbrella global parameter map. The `%OPENDNS-3-DNS_RES_FAILURE` message indicates that the router cannot resolve the Umbrella service names needed to establish the Umbrella connection.

```
conf t
parameter-map type umbrella global
 dns-resolver 208.67.222.222
 dns-resolver 208.67.220.220
end
```

Ensure that R1 has IP reachability (routing/NAT as applicable) to the configured resolver addresses. The key corrective action is the `dns-resolver` configuration under `parameter-map type umbrella global`, not merely enabling the Umbrella feature.

QUESTION NO: 7

An organization uses Cisco Secure Client with the Umbrella module for remote users. A laptop is connected to an untrusted home network, but DNS requests are sent to the local router resolver instead of receiving the organization's Umbrella DNS-layer protection. The user is correctly assigned to an Umbrella policy. Which endpoint configuration should the administrator verify?

A. The Umbrella roaming security module profile

B. The Cisco ISE authorization result

C. The Duo authentication policy

D. The Cloudlock API integration

ANSWER: A

Explanation:

The administrator should verify that the Umbrella roaming security module profile is deployed and enabled in Cisco Secure Client. The module must be configured to redirect and protect DNS requests for roaming endpoints; policy assignment alone does not cause an endpoint to use Umbrella protection.

An ISE authorization result controls network access but does not configure DNS protection for an off-network endpoint. A Duo authentication policy affects user authentication rather than DNS handling. A Cloudlock API integration evaluates SaaS data and cannot redirect endpoint DNS requests.