642-583

Security Solutions for Systems Engineers

Version 3.2

642-583

QUESTION NO: 1

Which Cisco ASA's Unified Communications proxy feature manipulates both the signaling and the media channels?

A. TLS Proxy
B. H.323 Proxy
C. SIP Proxy
D. Phone Proxy
E. CUMA Proxy

Answer: D

QUESTION NO: 2

Deploying logical security controls such as firewall and IPS appliances is an example of which kind of risk-management option?

A. risk avoidance
B. risk transfer
C. risk retention
D. risk reduction
E. risk removal

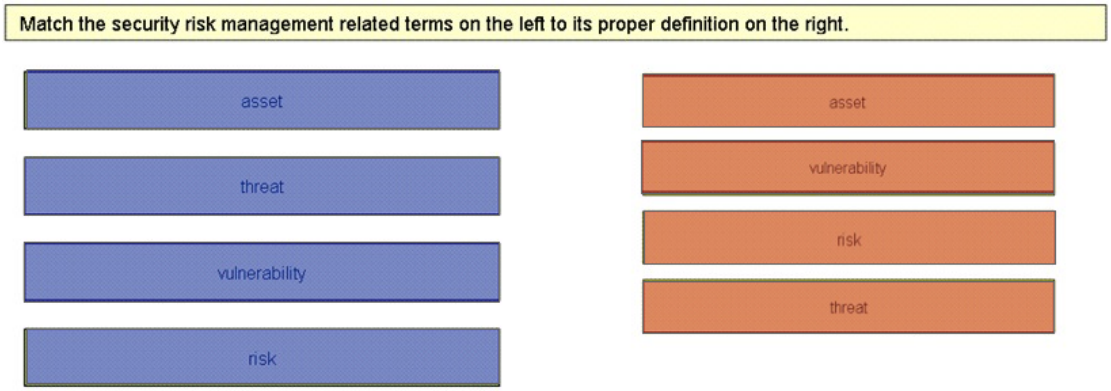
Answer: A

QUESTION NO: 3 DRAG DROP

Match the security risk management related terms on the left to its proper definition on the right.

asset	anything that has value to an organization
threat	a weakness in a system or its design that could be exploited
vulnerability	the likelihood of a particular attack occurring and resulting in an undesirable consequence
risk	any circumstance or event with the potential to cause harm to an information system

Answer:



QUESTION NO: 4

What is the benefit of the Cisco ASA phone proxy feature?

A. allows businesses to securely connect their Cisco Unified Presence clients back to their enterprise networks or to share presence information between Cisco Unified Presence servers in different enterprises
B. allows telecommuters to connect their IP phones to the corporate IP telephony network securely over the Internet, without the need to connect over a VPN tunnel
C. allows businesses to configure granular policies for SCCP traffic, such as enforcing only registered phone calls to send traffic through the Cisco ASA security appliance and filtering on message IDs to allow or disallow specific messages
D. enables deep inspection services for SIP traffic for both User Datagram Protocol (UDP) and TCP-based SIP environments, thus providing granular control for protection against unified communications attacks
E. enables inspection of the RTSP protocols that are used to control communications between the client and server for streaming applications
F. enables advanced H.323 inspection services that support H.323 versions 14 along with Direct Call Signaling (DCS) and Gatekeeper-Routed Call Signaling (GKRCS) to provide flexible security integration in a variety of H.323-driven VoIP environments

Answer: B

QUESTION NO: 5

Which two protocols can be used to implement high-availability IPS design, using the Cisco IPS 4200 Series Sensor appliance? (Choose two.)

A. spanning tree
B. stateful failover
C. EtherChannel load balancing
D. WCCP
E. HSRP
F. SDEE

Answer: A, C

QUESTION NO: 6

What are the advantages and disadvantages of using the "Direct to tower" or PAC file methods for redirecting traffic to ScanSafe?

A. Advantages: ease of deployment, especially for multiple breakout points
Disadvantages: no user granularity
B. Advantages: user granularity
Disadvantages: requires additional hardware for each breakout point
C. Advantages: no browser changes required Disadvantages: not all browsers supported

Answer: C

QUESTION NO: 7

Which statement is true?

A. Three-year commitments cost less per year than three consecutive one-year commitments.
B. Three consecutive one-year commitments cost less than one three-year commitment.
C. Three-year commitments cost the same per year as three consecutive one-year commitments
D. Cisco IronPort does not sell three-year commitments.

Answer: D

QUESTION NO: 8

Which statement regarding the Cisco ASA encrypted voice inspection capability is correct?

A. The Cisco ASA decrypts, inspects, then re-encrypts voice-signaling traffic; all of the existing VoIP inspection functions for SCCP and SIP protocols are preserved.
B. The Cisco ASA acts as a non-transparent TLS proxy between the Cisco IP Phone and Cisco Unified Communications Manager.

C. TLS proxy applies to the encryption layer and is configured by using a Layer 3/4 inspection policy on the Cisco AS**A.**
D. The Cisco ASA does not support PAT and NAT for SCCP inspection.
E. The Cisco ASA serves as a proxy for both client and server, with the Cisco IP Phone and the Session Border Controller.

Answer: A

QUESTION NO: 9

The Cisco IPS Manager Express (IME) can be used to manage how many IPS appliances, at a maximum?

A. 3
B. 5

C. 10
D. 15
E. 20
F. 25

Answer: B

QUESTION NO: 10

Which Cisco ASA configuration is required to implement active/active failover?

A. transparent firewall
B. modular policy framework (MPF)
C. virtual contexts
D. policy-based routing
E. redundant interfaces
F. VLANs

Answer: C

QUESTION NO: 11

Which platform can support the highest number of SSL sessions?

A. Cisco 3845 with AIM-VPN/SSL-3
B. Cisco 7200 NPE-GE+VSA
C. Cisco 7200 NPE-GE+VAM2+
D. Cisco ASR1000-5G
E. Cisco 6500/7600 + VPN SPA
F. Cisco ASA 5580

Answer: F

QUESTION NO: 12

Which option best describes Dynamic Content Filtering on the web security appliance?
A. external DLP option for acceptable use scanning
B. filter for pages and frames with dynamic control asset HTML tags
C. content scanner for streaming videos
D. advanced rule engine for categorizing dark web sites

Answer: B

QUESTION NO: 13

Which countermeasure is best used to protect against rogue access points that are outside the enterprise physical perimeter and that attempt to attract legitimate clients?

A. dedicated rogue detector access points with active and passive RLDP and radio containment
B. personal firewall
C. Management Frame Protection
D. wireless IDS/IPS
E. EAP-TLS bidirectional authentication

Answer: E

QUESTION NO: 14

Which two settings can the Cisco Security Agent (release 5.2 and later) monitor to control user's wireless access? (Choose two.)

A. protection types such as WEP, TKIP
B. wireless card type (802.11a, b, org)
C. SSIDs
D. antivirus version
E. lightweight versus autonomous mode

Answer: A, C

QUESTION NO: 15

Which series of steps illustrates how a challenge-and-response authentication protocol functions?

A.

1. The authenticator sends a random challenge string to the subject being authenticated.
2. The subject being authenticated hashes the challenge using a shared secret password to form a response back to the authenticator.
3. The authenticator performs the same hash method with the same shared secret password. to calculate a local response and compare it with the received response.
4. If these match, the subject is authenticated.

B.

1. The subject being authenticated sends a random challenge string to the authenticator.
2. The authenticator encrypts the challenge string with a private key and sends the encrypted random challenge string back to the subject being authenticated.
3. The subject being authenticated decrypts the random challenge string with the public key and compare it to the original random challenge.
4. If these match, the subject is authenticated.

C.

1. The subject being authenticated sends a random challenge string to the authenticator.
2. The authenticator encrypts the challenge string with a shared secret password and sends the encrypted random challenge string back to the subject being authenticated.
3. The subject being authenticated decrypts the random challenge string using the same shared secret key and compare it to the original random challenge.
4. If these match, the subject is authenticated.

A. Exhibit A

B. Exhibit B

C. Exhibit C

Answer: A

QUESTION NO: 16

What are the four most common approaches used for managing risk? (Choose four.)

A. risk reduction
B. risk avoidance
C. risk cancellation
D. risk elimination
E. risk transfer
F. risk retention/acceptance

Answer: A, B, E, F

QUESTION NO: 17

On Cisco IOS routers that are running BGP, which three kinds of traffic filters can be implemented to limit routing information propagation? (Choose three.)

A. distribute list
B. prefix list
C. passive interface
D. as-path filter
E. Type 3 LSA filter

Answer: A, D, E

QUESTION NO: 18