



**Exam : 640-553**

**Title : IINS Implementing Cisco  
IOS Network Security**

**Version : Demo**

1.Which consideration is important when implementing Syslogging in your network?

- A.Use SSH to access your Syslog information.
- B.Enable the highest level of Syslogging available to ensure you log all possible event messages.
- C.Log all messages to the system buffer so that they can be displayed when accessing the router.
- D.Synchronize clocks on the network with a protocol such as Network Time Protocol.

Answer:D

2.Which statement is true when you have generated RSA keys on your Cisco router to prepare for secure device management?

- A.You must then zeroize the keys to reset secure shell before configuring other parameters.
- B.The SSH protocol is automatically enabled.
- C.You must then specify the general-purpose key size used for authentication with the crypto key generate rsa general-keys modulus command.
- D.All vty ports are automatically enabled for SSH to provide secure management.

Answer:B

3.What does level 5 in the following enable secret global configuration mode command indicate?

router#enable secret level 5 password

- A.The enable secret password is hashed using MD5.
- B.The enable secret password is hashed using SHA.
- C.The enable secret password is encrypted using Cisco proprietary level 5 encryption.
- D.Set the enable secret command to privilege level 5.
- E.The enable secret password is for accessing exec privilege level 5.

Answer:E

4.Drop

Match the descriptions on the left with the correct Cisco Self-Defending Network characteristics on the right. Each item may be used only once.

Interaction amongst services and devices to mitigate attacks

Enabling elements in the network to be a point of policy enforcement

Security technologies that evolve with emerging attacks

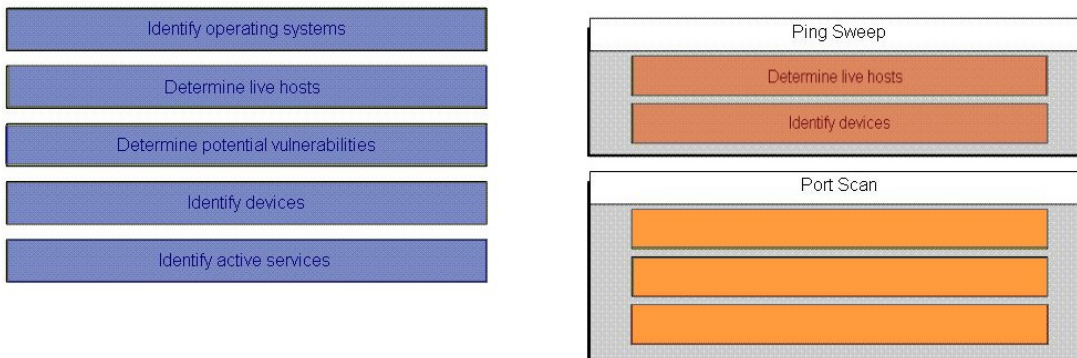
INTEGRATED  
Enabling elements in the network to be a point of policy enforcement

COLLABORATIVE  
Interaction amongst services and devices to mitigate attacks

ADAPTIVE  
Security technologies that evolve with emerging attacks

5.Drop

Drag the result on the left to the corresponding attack method on the right.



6.Which of these correctly matches the CLI command(s) to the equivalent SDM wizard that performs similar configuration functions?

- A.Cisco Common Classification Policy Language configuration commands and the SDM Site-to-Site VPN wizard
- B.auto secure exec command and the SDM One-Step Lockdown wizard
- C.setup exec command and the SDM Security Audit wizard
- D.class-maps, policy-maps, and service-policy configuration commands and the SDM IPS wizard
- E.aaa configuration commands and the SDM Basic Firewall wizard

Answer:B

7.What is the key difference between host-based and network-based intrusion prevention?

- A.Network-based IPS is better suited for inspection of SSL and TLS encrypted data flows.
- B.Network-based IPS provides better protection against OS kernel-level attacks against hosts and servers.
- C.Network-based IPS can provide protection to desktops and servers without the need of installing specialized software on the end hosts and servers.
- D.Host-based IPS can work in promiscuous mode or inline mode.
- E.Host-based IPS is more scalable then network-based IPS.
- F.Host-based IPS deployment requires less planning than network-based IPS.

Answer:C

8.Refer to the exhibit. You are a network manager for your organization. You are looking at your Syslog server reports. Based on the Syslog message shown, which two statements are true? (Choose two.)

**Feb 1 10:12:08 PST: %SYS-5-CONFIG\_I: Configured from console by vty0 (10.2.2.6)**

- A.Service timestamps have been globally enabled.
- B.This is a normal system-generated information message and does not require further investigation.
- C.This message is unimportant and can be ignored.
- D.This message is a level 5 notification message.

Answer:A D

9.You suspect an attacker in your network has configured a rogue layer 2 device to intercept traffic from

multiple VLANS, thereby allowing the attacker to capture potentially sensitive data. Which two methods will help to mitigate this type of activity? (Choose two.)

- A. Turn off all trunk ports and manually configure each VLAN as required on each port
- B. Disable DTP on ports that require trunking
- C. Secure the native VLAN, VLAN 1 with encryption
- D. Set the native VLAN on the trunk ports to an unused VLAN
- E. Place unused active ports in an unused VLAN

Answer: B D

10. Which three statements about SSL-based VPNs are true? (Choose three.)

- A. Asymmetric algorithms are used for authentication and key exchange.
- B. SSL VPNs and IPsec VPNs cannot be configured concurrently on the same router.
- C. Symmetric algorithms are used for bulk encryption.
- D. The authentication process uses hashing technologies.
- E. SSL VPNs require special-purpose client software to be installed on the client machine.
- F. You can also use the application programming interface to extensively modify the SSL client software for use in special applications.

Answer: A C D