

Exam : Cisco 640-553

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

Update : Demo

1.As a network engineer at Pass4sure.com, you are responsible for Pass4sure network. Which will be necessarily taken into consideration when implementing Syslogging in your network?

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

Correct:D

2.Which classes does the U.S. government place classified data into? (Choose three.)

- A.SBU
- B.Confidential
- C.Secret
- D.Top-secret

Correct:B C D

3.You are a network technician at Pass4sure.com. Which description is correct when you have generated RSA keys on your Cisco router to prepare for secure device management?

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

Correct:B

4.Which method is of gaining access to a system that bypasses normal security measures?

- A.Creating a back door
- B.Starting a Smurf attack
- C.Conducting social engineering
- D.Launching a DoS attack

Correct:A

5.As a candidate for CCNA examination, when you are familiar with the basic commands, if you input the command "enable secret level 5 password" in the global mode , what does it indicate?

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

Correct:E

6.Which statement is true about a Smurf attack?

- A.It sends ping requests to a subnet, requesting that devices on that subnet send ping replies to a target system.
- B.It intercepts the third step in a TCP three-way handshake to hijack a session.
- C.It uses Trojan horse applications to create a distributed collection of "zombie" computers, which can be used to launch a coordinated DDoS attack.
- D.It sends ping requests in segments of an invalid size.

Correct:A

7. Please choose the correct description about Cisco Self-Defending Network characteristics.

P4S1	Interaction amongst services and devices to mitigate attacks
P4S2	Enabling elements in the networks to be a point of policy enforcement
P4S3	Security technologies that evolve with emerging attacks

- A. INTEGRATED - P4S1 COLLABORATIVE - P4S2 ADAPTIVE - P4S3
- B. INTEGRATED - P4S2 COLLABORATIVE - P4S1 ADAPTIVE - P4S3
- C. INTEGRATED - P4S2 COLLABORATIVE - P4S3 ADAPTIVE - P4S1
- D. INTEGRATED - P4S3 COLLABORATIVE - P4S2 ADAPTIVE - P4S1

Correct: B

8. Which three items are Cisco best-practice recommendations for securing a network? (Choose three.)

- A. Deploy HIPS software on all end-user workstations.
- B. Routinely apply patches to operating systems and applications.
- C. Disable unneeded services and ports on hosts.
- D. Require strong passwords, and enable password expiration.

Correct: B C D

9. With the increasing development of network, various network attacks appear. Which statement best describes the relationships between the attack method and the result?

P4S1	Identify operating systems
P4S2	Determine live hosts
P4S3	Determine potential vulnerabilities
P4S4	Identify devices
P4S5	Identify active services

- A. Ping Sweep - P4S1 and P4S3 Port Scan - P4S2, P4S4 and P4S5
- B. Ping Sweep - P4S2 and P4S4 Port Scan - P4S1, P4S3 and P4S5
- C. Ping Sweep - P4S1 and P4S5 Port Scan - P4S2, P4S3 and P4S4
- D. Ping Sweep - P4S2 and P4S3 Port Scan - P4S1, P4S4 and P4S5

Correct: B

10. For the following attempts, which one is to ensure that no one employee becomes a pervasive security threat, that data can be recovered from backups, and that information system changes do not compromise a system's security?

- A. Disaster recovery
- B. Strategic security planning
- C. Implementation security
- D. Operations security

Correct: D

11. For the following options, which one accurately matches the CLI command(s) to the equivalent SDM wizard that performs similar configuration functions?

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

Correct: B

12. Which three options are network evaluation techniques? (Choose three.)

- A. Scanning a network for active IP addresses and open ports on those IP addresses
- B. Using password-cracking utilities
- C. Performing end-user training on the use of antispyware software
- D. Performing virus scans

Correct: A B D

13. Which is the main 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. Host-based IPS can work in promiscuous mode or inline mode.
- 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 deployment requires less planning than network-based IPS.

Correct: C

14. Which one is the most important based on the following common elements of a network design?

- A. Business needs
- B. Best practices
- C. Risk analysis
- D. Security policy

Correct: A

15. Given the exhibit below. You are a network manager of your company. You are reading your Syslog server reports. On the basis of the Syslog message shown, which two descriptions are correct? (Choose two.)

```
Feb 1 10:12:08 PST: %SYS-5-CONFIG_1: Configured from console by vty0 (10.2.2.6)
```

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

Correct: A D

16. Examine the following items, which one offers a variety of security solutions, including firewall, IPS, VPN, antispyware, antivirus, and antiphishing features?

- A. Cisco 4200 series IPS appliance
- B. Cisco ASA 5500 series security appliance

- C. Cisco IOS router
- D. Cisco PIX 500 series security appliance

Correct: B

17...

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

Correct:

18. The enable secret password appears as an MD5 hash in a router's configuration file, whereas the enable password is not hashed (or encrypted, if the password-encryption service is not enabled). What is the reason that Cisco still support the use of both enable secret and enable passwords in a router's configuration?

- A. The enable password is used for IKE Phase I, whereas the enable secret password is used for IKE Phase II.
- B. The enable password is considered to be a router's public key, whereas the enable secret password is considered to be a router's private key.
- C. Because the enable secret password is a hash, it cannot be decrypted. Therefore, the enable password is used to match the password that was entered, and the enable secret is used to verify that the enable password has not been modified since the hash was generated.
- D. The enable password is present for backward compatibility.

Correct: D

19. On the basis of the description of SSL-based VPN, place the correct descriptions in the proper locations.

Match the cryptographic algorithms on the left with the type of algorithm on the right.

3DES	<table border="1"> <tr> <td style="text-align: center;">Symmetric</td> </tr> <tr> <td style="background-color: yellow; height: 20px;"></td> </tr> <tr> <td style="background-color: yellow; height: 20px;"></td> </tr> <tr> <td style="background-color: yellow; height: 20px;"></td> </tr> </table> <table border="1"> <tr> <td style="text-align: center;">Asymmetric</td> </tr> <tr> <td style="background-color: yellow; height: 20px;"></td> </tr> <tr> <td style="background-color: yellow; height: 20px;"></td> </tr> <tr> <td style="background-color: yellow; height: 20px;"></td> </tr> </table>	Symmetric				Asymmetric			
Symmetric									
Asymmetric									
RSA									
Diffie-Hellman									
AES									
IDEA									
Elliptical Curve									

Correct:

Green choice1---->Yellow Choice1

Green choice3---->Yellow Choice2

Green choice5---->Yellow Choice3

20.How does CLI view differ from a privilege level?

A.A CLI view supports only commands configured for that specific view, whereas a privilege level supports commands available to that level and all the lower levels.

B.A CLI view supports only monitoring commands, whereas a privilege level allows a user to make changes to an IOS configuration.

C.A CLI view and a privilege level perform the same function. However, a CLI view is used on a Catalyst switch, whereas a privilege level is used on an IOS router.

D.A CLI view can function without a AAA configuration, whereas a privilege level requires AAA to be configured.

Correct:A

21...

When configuring AAA login authentication on Cisco routers, which two authentication methods should be used as the final method to ensure that the administrator can still log in to the router in case the external AAA server fails? (Choose two.)

- A:krb5
- E:local
- C:enable
- D:group RADIUS
- E:group TACACS+

Correct:

22.When configuring Cisco IOS login enhancements for virtual connections, what is the "quiet period"?

A.A period of time when no one is attempting to log in

B.The period of time in which virtual logins are blocked as security services fully initialize

C.The period of time in which virtual login attempts are blocked, following repeated failed login attempts

D.The period of time between successive login attempts

Correct:C

23.Which result is of securing the Cisco IOS image by use of the Cisco IOS image resilience feature?

A.When the router boots up, the Cisco IOS image will be loaded from a secured FTP location.

B.The Cisco IOS image file will not be visible in the output from the show flash command.

C.The show version command will not show the Cisco IOS image file location.

D.The running Cisco IOS image will be encrypted and then automatically backed up to a TFTP server.

Correct:B

24.Which three statements are valid SDM configuration wizards? (Choose three.)

A.Security Audit

B.VPN

C.STP

D.NAT

Correct:A B D

25.null

**Which two protocols enable Cisco SDM to pull IPS alerts from a Cisco ISR router?
(Choose two.)**

- A:FTP
- B:HTTPS
- C:TFTP
- D:SSH
- E:Syslog
- F:SDEE

Correct:

26.How do you define the authentication method that will be used with AAA?

- A.With a method list
- B.With the method command
- C.With the method aaa command
- D.With a method statement

Correct:A

27.Which three common examples are of AAA implementation on Cisco routers? Please place the correct descriptions in the proper locations.

performing router commands authorization using TACACS+

authenticating remote users who are accessing the corporate LAN through IPsec VPN connections

tracking Cisco Netflow accounting statistics

securing the router by locking down all unused services

implementing PKI to authenticate and authorize IPsec VPN peers using digital certificates

authenticating administrator access to the router console port, auxiliary port, and vty ports

The common examples of AAA implementation.

Help you pass any IT exam!

Three empty purple rectangular boxes, likely representing redacted content or a placeholder for an image.

Correct:

Green choice1---->Yellow Choice1

Green choice2---->Yellow Choice2

Green choice6---->Yellow Choice3

28.What is the objective of the aaa authentication login console-in local command?

- A.It specifies the login authorization method list named console-in using the local RADIUS username-password database.
- B.It specifies the login authorization method list named console-in using the local username-password database on the router.
- C.It specifies the login authentication method list named console-in using the local user database on the router.
- D.It specifies the login authentication list named console-in using the local username- password database on the router.

Correct:C

29.Which description is true about the show login command output displayed in the exhibit?

P4S-R# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100 seconds.
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.

Help you pass any IT exam!

- A.All logins from any sources are blocked for another 193 seconds.
- B.The login block-for command is configured to block login hosts for 93 seconds.
- C.When the router goes into quiet mode, any host is permitted to access the router via Telnet, SSH, and HTTP, since the quiet-mode access list has not been configured.
- D.Three or more login requests have failed within the last 100 seconds.

Correct:D

30.Which one of the following commands can be used to enable AAA authentication to determine if a user can access the privilege command level?

- A.aaa authentication enable default local
- B.aaa authentication enable level
- C.aaa authentication enable method default
- D.aaa authentication enable default

Correct:D