# 640-554 Q&As

Implementing Cisco IOS Network Security (IINS v2.0)

## Pass Cisco 640-554 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.pass4itsure.com/640-554.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

**QUESTION 1**

What are three of the security conditions that Cisco Configuration Professional One-Step Lockdown can automatically detect and correct on a Cisco router? (Choose three.)

A. One-Step Lockdown can set the enable secret password.

B. One-Step Lockdown can disable unused ports.

C. One-Step Lockdown can disable the TCP small servers service.

D. One-Step Lockdown can enable IP Cisco Express Forwarding.

E. One-Step Lockdown can enable DHCP snooping.

F. One-Step Lockdown can enable SNMP version 3.

Correct Answer: ACD

One-Step Lockdown This option tests you router configuration for any potential security problems and automatically makes any necessary configuration changes to correct any problems found. The conditions checked for and, if needed, corrected are as follows: ?Disable Finger Service ?Disable PAD Service ?Disable TCP Small Servers Service ?Disable UDP Small Servers Service ?Disable IP BOOTP Server Service ?Disable IP Identification Service ?Disable CDP ?Disable IP Source Route ?Enable Password Encryption Service ?Enable TCP Keepalives for Inbound Telnet Sessions ?Enable TCP Keepalives for Outbound Telnet Sessions ?Enable Sequence Numbers and Time Stamps on Debugs ?Enable IP CEF ?Disable IP Gratuitous ARPs ?Set Minimum Password Length to Less Than 6 Characters ?Set Authentication Failure Rate to Less Than 3 Retries ?Set TCP Synwait Time ?Set Banner ?Enable Logging ?Set Enable Secret Password ?Disable SNMP ?Set Scheduler Interval ?Set Scheduler Allocate ?Set Users ?Enable Telnet Settings ?Enable NetFlow Switching ?Disable IP Redirects ?Disable IP Proxy ARP ?Disable IP Directed Broadcast ?Disable MOP Service ?Disable IP Unreachables ?Disable IP Mask Reply ?Disable IP Unreachables on NULL Interface ?Enable Unicast RPF on Outside Interfaces ?Enable Firewall on All of the Outside Interfaces ?Set Access Class on HTTP Server Service ?Set Access Class on VTY Lines ?Enable SSH for Access to the Router

Reference: http://www.cisco.com/c/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/SAudt.html

**QUESTION 2**

Refer to the exhibit.

```
router(config)# username admin privilege level 15 secret hardt0cRackPw
router(config)# aaa new-model
router(config)# aaa authentication login default tacacs+
router(config)# aaa authentication login test tacacs+ local
router(config)# line vty 0 4
router(config-line)# login authentication test
router(config-line)# line con 0
router(config-line)# end
```



Which statement about the aaa configurations is true?

A. The authentication method list used by the console port is named test.

B. The authentication method list used by the vty port is named test.

C. If the TACACS+ AAA server is not available, no users will be able to establish a Telnet session with the router.

D. If the TACACS+ AAA server is not available, console access to the router can be authenticated using the local database.

E. The local database is checked first when authenticating console and vty access to the router.

Correct Answer: B

http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml
Configure AAA Authentication for Login

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the login authentication command in line configuration mode. AAA services must also be configured.

Configuration Procedure

In this example, the router is configured to retrieve users\\' passwords from a TACACS+ server when users attempt to connect to the router.

From the privileged EXEC (or "enable") prompt, enter configuration mode and enter the commands to configure the router to use AAA services for authentication:

router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

router(config)#aaa new-model

router(config)#aaa authentication login my-auth-list tacacs+

router(config)#tacacs-server host 192.168.1.101

router(config)#tacacs-server key letmein

Switch to line configuration mode using the following commands. Notice that the prompt changes to reflect the current mode.

router(config)#line 1 8

router(config-line)#

Configure password checking at login.

router(config-line)#login authentication my-auth-list

Exit configuration mode.

router(config-line)#end

router#

%SYS-5-CONFIG_I: Configured from console by console

**QUESTION 3**

Which RADIUS server authentication protocols are supported on Cisco ASA firewalls? (Choose three.)

A. EAP

B. ASCII

C. PAP

D. PEAP

E. MS-CHAPv1

F. MS-CHAPv2

Correct Answer: CEF

The ASA supports the following authentication methods with RADIUS servers:

PAP -- For all connection types.

CHAP and MS-CHAPv1 -- For L2TP-over-IPsec connections.

MS-CHAPv2 -- For L2TP-over-IPsec connections, and for regular IPsec remote access connections when the password management feature is enabled. You can also use MS-CHAPv2 with clientless connections. Authentication Proxy modes

-- For RADIUS-to Active-Directory, RADIUS-to-RSA/SDI, RADIUS- to-Token server, and RSA/SDI-to-RADIUS connections

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/aaa_radius.html

**QUESTION 4**

Which three statements about RADIUS are true? (Choose three.)

A. RADIUS uses TCP port 49.

B. RADIUS uses UDP ports 1645 or 1812.

C. RADIUS encrypts the entire packet.

D. RADIUS encrypts only the password in the Access-Request packet.

E. RADIUS is a Cisco proprietary technology.

F. RADIUS is an open standard.

Correct Answer: BDF

TACACS+ and RADIUS Protocol Comparison

| Point of Comparison | TACACS+ | RADIUS |
|---|---|---|
| **Transmission Protocol** | TCP—Connection-oriented transport-layer protocol, reliable full-duplex data transmission. | UDP—Connectionless transport-layer protocol, datagram exchange without acknowledgments or guaranteed delivery. UDP uses the IP to get a data unit (called a datagram) from one computer to another. |
| **Ports Used** | 49 | Authentication and Authorization: 1645 and 1812<br>Accounting: 1646 and 1813. |
| **Encryption** | Full packet-body encryption. | Encrypts only passwords up to 16 bytes. |
| **AAA Architecture** | Separate control of each service: authentication, authorization, and accounting. | Authentication and authorization combined as one service. |
| **Intended Purpose** | Device management. | User access control. |
| **Open Standards** | Developed by Cisco | Open standard |



Reference: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-2/user/guide/acsuserguide/rad_tac_phase.html

**QUESTION 5**

Under which higher-level policy is a VPN security policy categorized?

A. application policy

B. DLP policy

C. remote access policy

D. compliance policy

E. corporate WAN policy

Correct Answer: C

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.0/user/guide/ravpnpag.html

Remote Access VPN Policy Reference

The Remote Access VPN policy pages are used to configure remote access VPNs on Cisco IOS security routers, PIX Firewalls, Catalyst 6500 /7600 devices, and Adaptive Security Appliance (ASA) devices.

**QUESTION 6**

Which one of the following items may be added to a password stored in MD5 to make it more secure?

A. Ciphertext

B. Salt

C. Cryptotext

D. Rainbow table

Correct Answer: B

Making an Md5 Hash More Secure To make the md5 hash more secure we need to add what is called "salt". Salt in this sense of the meaning is random data appended to the password to make the hash more complicated and difficult to reverse engineer. Without knowing what the salt is, rainbow table attacks are mostly useless. Reference: http://www.marksanborn.net/php/creating-a-secure-md5-hash-for-storing-passwords-in-a-database/

**QUESTION 7**

On Cisco ISR routers, for what purpose is the realm-cisco.pub public encryption key used?

A. used for SSH server/client authentication and encryption

B. used to verify the digital signature of the IPS signature file

C. used to generate a persistent self-signed identity certificate for the ISR so administrators can authenticate the ISR when accessing it using Cisco Configuration Professional

D. used to enable asymmetric encryption on IPsec and SSL VPNs

E. used during the DH exchanges on IPsec VPNs

Correct Answer: B

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

Step 1: Downloading IOS IPS files

The first step is to download IOS IPS signature package files and public crypto key from Cisco.com.

Step 1.1: Download the required signature files from Cisco.com to your PC

?Location: http://tools.cisco.com/support/downloads/go/Model.x?mdfid=28144296and;mdfLevel=Software%20Familand;treeName=Securitand;modelName=Cisco% 20IOS%20Intrusion%20Prevention%20System%20Feature%

20SoftwareandtreeMdfId=268438162

?Files to download:

IOS-Sxxx-CLI.pkg: Signature package - download the latest signature package.

realm-cisco.pub.key.txt: Public Crypto key - this is the crypto key used by IOS IPS

**QUESTION 8**

Which statement about an access control list that is applied to a router interface is true?

A. It only filters traffic that passes through the router.

B. It filters pass-through and router-generated traffic.

C. An empty ACL blocks all traffic.

D. It filters traffic in the inbound and outbound directions.

Correct Answer: A

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-2mt/sec-acl-ov-gdl.html

The Order in Which You Enter Criteria Statements

Note that each additional criteria statement that you enter is appended to the end of the access list statements. Also note that you cannot delete individual statements after they have been created. You can only delete an entire access list.

The order of access list statements is important! When the router is deciding whether to forward or block a packet, the Cisco IOS software tests the packet against each criteria statement in the order in which the statements were created.

After a match is found, no more criteria statements are checked.

If you create a criteria statement that explicitly permits all traffic, no statements added later will ever be checked. If you need additional statements, you must delete the access list and retype it with the new entries.

Apply an Access Control List to an Interface

With some protocols, you can apply up to two access lists to an interfacE. one inbound access list and one outbound access list. With other protocols, you apply only one access list that checks both inbound and outbound packets.

If the access list is inbound, when a device receives a packet, Cisco software checks the access list\\'s criteria statements for a match. If the packet is permitted, the software continues to process the packet. If the packet is denied, the software

discards the packet.

If the access list is outbound, after receiving and routing a packet to the outbound interface, Cisco software checks the access list\\'s criteria statements for a match. If the packet is permitted, the software transmits the packet. If the packet is

denied, the software discards the packet.

Note

Access lists that are applied to interfaces on a device do not filter traffic that originates from that device. The access list check is bypassed for locally generated packets, which are always outbound. By default, an access list that is applied to

an outbound interface for matching locally generated traffic will bypass the outbound access list check; but transit traffic is subjected to the outbound access list check.

**QUESTION 9**

What are two primary attack methods of VLAN hopping? (Choose two.)

A. VoIP hopping

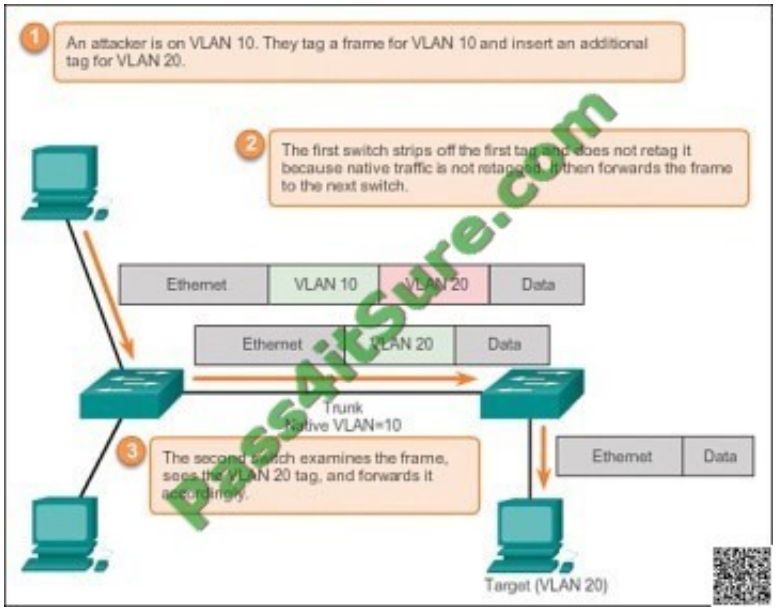
B. switch spoofing

C. CAM-table overflow

D. double tagging

Correct Answer: BD

There are a number of different types of VLAN attacks in modern switched networks. The VLAN architecture simplifies network maintenance and improves performance, but it also opens the door to abuse. It is important to understand the general methodology behind these attacks and the primary approaches to mitigate them. VLAN hopping enables traffic from one VLAN to be seen by another VLAN. Switch spoofing is a type of VLAN hopping attack that works by taking advantage of an incorrectly configured trunk port. By default, trunk ports have access to all VLANs and pass traffic for multiple VLANs across the same physical link, generally between switches. Another type of VLAN attack is a double-tagging (or double-encapsulated) VLAN hopping attack. This type of attack takes advantage of the way that hardware on most switches operates. Most switches perform only one level of 802.1Q deencapsulation, which allows an attacker to embed a hidden 802.1Q tag inside the frame. This tag allows the frame to be forwarded to a VLAN that the original 802.1Q tag did not specify as shown below. An important characteristic of the double- encapsulated VLAN hopping attack is that it works even if trunk ports are disabled, because a host typically sends a frame on a segment that is not a trunk link.




Double-Tagging Attack Reference: http://www.ciscopress.com/articles/article.asp?p=2181837andseqNum=10

**QUESTION 10**

Which statement about the Atomic signature engine is true?

A. It can perform signature matching on a single packet only.

B. It can perform signature matching on multiple packets.

C. It can examine applications independent of the platform.

D. It can flexibly match patterns in a session.

Correct Answer: A

**QUESTION 11**

Which protocols use encryption to protect the confidentiality of data transmitted between two parties? (Choose two.)

A. FTP

B. SSH

C. Telnet

D. AAA

E. HTTPS

F. HTTP

Correct Answer: BE

**QUESTION 12**

Which command configures logging on a Cisco ASA firewall to include the date and time?

A. logging facility

B. logging enable

C. logging timestamp

D. logging buffered debugging

Correct Answer: C