Vendor: Cisco

Exam Code:640-554

Exam Name: Implementing Cisco IOS Network Security (IINS v2.0)

Version: Demo

QUESTION 1

Which of the following statements about access lists are true? (Choose three.)

A. Extended access lists should be placed as near as possible to the destination

B. Extended access lists should be placed as near as possible to the source

C. Standard access lists should be placed as near as possible to the destination

D. Standard access lists should be placed as near as possible to the source

E. Standard access lists filter on the source address

F. Standard access lists filter on the destination address

Correct Answer: BCE

QUESTION 2

Which two protocols can SNMP use to send messages over a secure communications channel? (Choose two.)

A. DTLS

B. TLS

C. ESP

D. AH

E. ISAKMP

Correct Answer: AB

QUESTION 3

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

A. VoIP hopping

B. Switch spoofing

C. CAM-table overflow

D. Double tagging

Correct Answer: BD

VLAN hopping describes when an attacker connects to a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two VLAN hopping exploit methods: switch spoofing and double tagging.

Reference: https://www.nlogic.co/understanding-vlan-hopping-attacks/

QUESTION 4

What is the transition order of STP states on a Layer 2 switch interface?

A. listening, learning, blocking, forwarding, disabled

B. listening, blocking, learning, forwarding, disabled

C. blocking, listening, learning, forwarding, disabled

D. forwarding, listening, learning, blocking, disabled

Correct Answer: C

Explanation: Each Layer 2 interface on a switch using spanning tree exists in one of these states:

Blocking -- The interface does not participate in frame forwarding.

Listening -- The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.

Learning -- The interface prepares to participate in frame forwarding.

Forwarding -- The interface forwards frames.

Disabled -- The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_22_ea11x/configuration/guide/scg/swstp.html

---

QUESTION 5

Refer to the exhibit.

Which three statements about these three show outputs are true? (Choose three.)

A. Traffic matched by ACL 110 is encrypted.

B. The IPsec transform set uses SHA for data confidentiality.

C. The crypto map shown is for an IPsec site-to-site VPN tunnel.

D. The default ISAKMP policy uses a digital certificate to authenticate the IPsec peer.

E. The IPsec transform set specifies the use of GRE over IPsec tunnel mode.

F. The default ISAKMP policy has higher priority than the other two ISAKMP policies with a priority of 1 and 2

Correct Answer: ACD

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_s3.html

Show crypto map Field Descriptions

Peer

Possible peers that are configured for this crypto map entry.

Extended IP access list Access list that is used to define the data packets that need to be encrypted. Packets that are denied by this access list are forwarded but not encrypted. The "reverse" of this access list is used to check the inbound

return packets, which are also encrypted. Packets that are denied by the "reverse" access list are dropped because they should have been encrypted but were not.

Extended IP access check

Access lists that are used to more finely control which data packets are allowed into or out of the IPsec tunnel. Packets that are allowed by the "Extended IP access list" ACL but denied by the "Extended IP access list check" ACL are dropped.

Current peer Current peer that is being used for this crypto map entry.

Security association lifetime

Number of bytes that are allowed to be encrypted or decrypted or the age of the security association before new encryption keys must be negotiated.

PFS

(Perfect Forward Secrecy) If the field is marked as `Yes\\', the Internet Security Association and Key Management Protocol (ISAKMP) SKEYID-d key is renegotiated each time security association (SA) encryption keys are renegotiated

(requires another Diffie-Hillman calculation). If the field is marked as `No\\', the same ISAKMP SKEYID-d key is used when renegotiating SA encryption keys. ISAKMP keys are renegotiated on a separate schedule, with a default time of 24

hours.

Transform sets

List of transform sets (encryption, authentication, and compression algorithms) that can be used with this crypto map. Interfaces using crypto map test Interfaces to which this crypto map is applied. Packets that are leaving from this interface

are subject to the rules of this crypto map for encryption. Encrypted packets may enter the router on any interface, and they are decrypted. Nonencrypted packets that are entering the router through this interface are subject to the "reverse"

crypto access list check.

QUESTION 6

Which Cisco IOS command will verify authentication between a router and a AAA server?

A. debug aaa authentication

B. test aaa group

C. test aaa accounting

D. aaa new-model

Correct Answer: B

To validate that the Cisco IOS device can access and securely communicate with the RADIUS server the "test aaa" exec mode command can be used:

switch#test aaa group radius user1 cisco new-code User successfully authenticated

Reference: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/whitepaper_C11-731907.html

---

QUESTION 7

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

QUESTION 8

Which statement best represents the characteristics of a VLAN?

A. Ports in a VLAN will not share broadcasts amongst physically separate switches.

B. A VLAN can only connect across a LAN within the same building.

C. A VLAN is a logical broadcast domain that can span multiple physical LAN segments.

D. A VLAN provides individual port security.

Correct Answer: C

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_0_1a/VLANs.html

Configuring VLANs You can use virtual LANs (VLANs) to divide the network into separate logical areas. VLANs can also be considered as broadcast domains. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router.

QUESTION 9

Which of the following are features of IPsec transport mode? (Choose three.)

A. IPsec transport mode is used between end stations

B. IPsec transport mode is used between gateways

C. IPsec transport mode supports multicast

D. IPsec transport mode supports unicast

E. IPsec transport mode encrypts only the payload

F. IPsec transport mode encrypts the entire packet

Correct Answer: ADE

QUESTION 10

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 11

Which address block is reserved for locally assigned unique local addresses?

A. 2002::/16

B. FD00::/8

C. 2001::/32

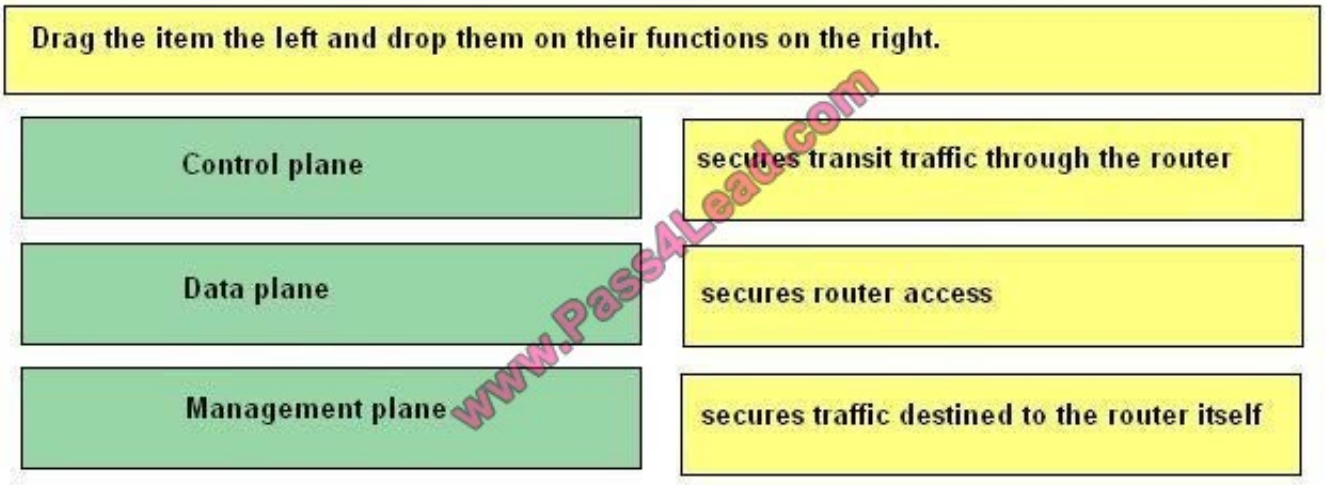
D. FB00::/8

Correct Answer: B

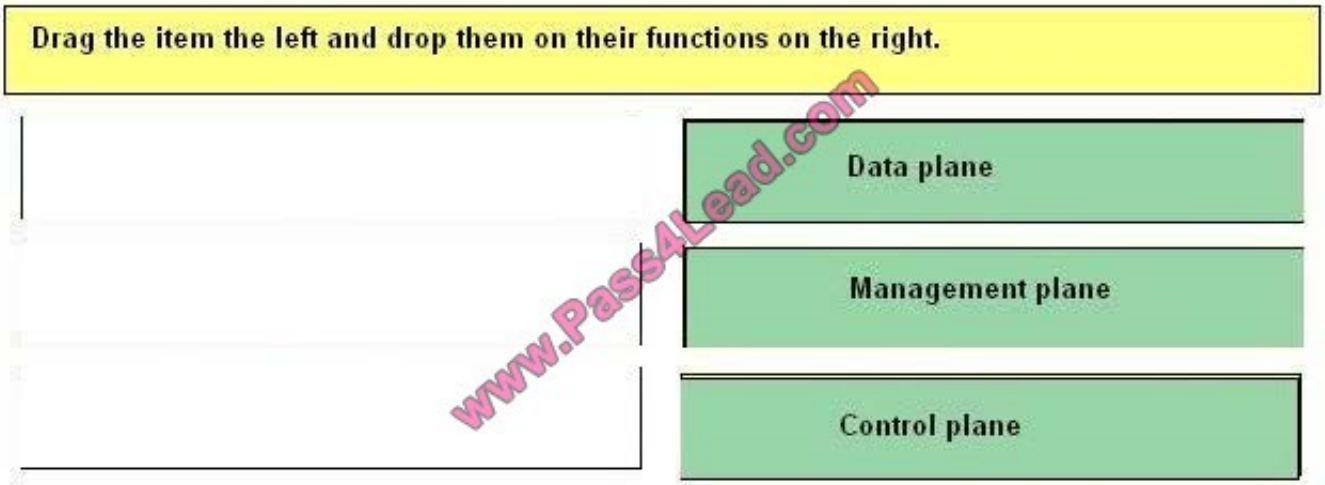
QUESTION 12

DRAG DROP

Select and Place:



Correct Answer:



Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: