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.pass4lead.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

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 2

What Cisco Security Agent Interceptor is in charge of intercepting all read/write requests to the rc files in UNIX?

A. Configuration interceptor

B. Network interceptor

C. File system interceptor

D. Execution space interceptor

Correct Answer: A

Configuration interceptor: Read/write requests to the Registry in Windows or to rc configuration files on UNIX are intercepted. This interception occurs because modification of the operating system configuration can have serious consequences. Therefore, Cisco Security Agent tightly controls read/write requests to the Registry.

QUESTION 3

What is the first command you enter to configure AAA on a new Cisco router?

A. aaa configuration

B. no aaa-configuration

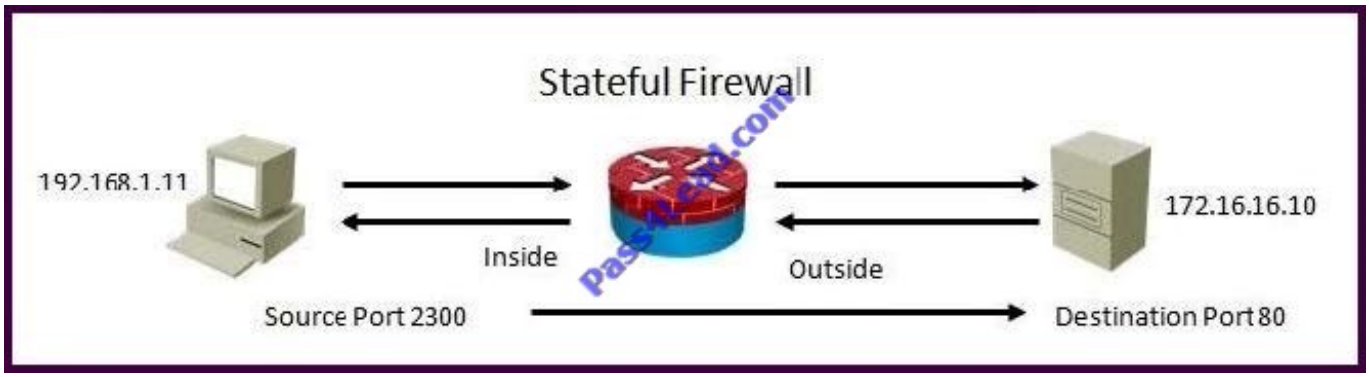
C. no aaa new-model

D. aaa new-model

Correct Answer: D

QUESTION 4

Refer to the exhibit.



Using a stateful packet firewall and given an inside ACL entry of permit ip 192.16.1.0 0.0.0.255 any, what would be the resulting dynamically configured ACL for the return traffic on the outside ACL?

A. permit tcp host 172.16.16.10 eq 80 host 192.168.1.11 eq 2300

B. permit ip 172.16.16.10 eq 80 192.168.1.0 0.0.0.255 eq 2300

C. permit tcp any eq 80 host 192.168.1.11 eq 2300

D. permit ip host 172.16.16.10 eq 80 host 192.168.1.0 0.0.0.255 eq 2300

Correct Answer: A

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/fwinsp.html

Understanding Inspection Rules

Inspection rules configure Context-Based Access Control (CBAC) inspection commands. CBAC inspects traffic that travels through the device to discover and manage state information for TCP and UDP sessions. The device uses this state

information to create temporary openings to allow return traffic and additional data connections for permissible sessions.

CBAC creates temporary openings in access lists at firewall interfaces. These openings are created when inspected traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked)

and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered inspection when exiting through the

firewall.

Inspection rules are applied after your access rules, so any traffic that you deny in the access rule is not inspected. The traffic must be allowed by the access rules at both the input and output interfaces to be inspected. Whereas access rules

allow you to control connections at layer 3 (network, IP) or 4 (transport, TCP or UDP protocol), you can use inspection rules to control traffic using application-layer protocol session information.

For all protocols, when you inspect the protocol, the device provides the following functions:

- Automatically opens a return path for the traffic (reversing the source and destination addresses), so that you do not need to create an access rule to allow the return traffic. Each connection is considered a session, and the device maintains session state information and allows return traffic only for valid sessions. Protocols that use TCP contain explicit session information, whereas for UDP applications, the device models the equivalent of a session based on the source and destination addresses and the closeness in time of a sequence of UDP packets.

These temporary access lists are created dynamically and are removed at the end of a session.

- Tracks sequence numbers in all TCP packets and drops those packets with sequence numbers that are not within expected ranges.

- Uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. When a session is dropped, or reset, the device informs both the source and destination of the session to reset the connection, freeing up resources and helping to mitigate potential Denial of Service (DoS) attacks.

QUESTION 5

Which two options are advantages of a network-based Cisco IPS? (Choose two.)

A. It can examine encrypted traffic.

B. It can protect the host after decryption.

C. It is an independent operating platform.

D. It can observe bottom-level network events.

E. It can block traffic

Correct Answer: CD

To Read the Whole Q&As, please purchase the Complete Version from Our website.

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

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.pass4lead.com/allproducts

Need Help

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