Vendor: Cisco

Exam Code:640-554

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

Version: Demo

QUESTION 1

Which three statements about the Cisco ASA appliance are true? (Choose three.)

A. The DMZ interface(s) on the Cisco ASA appliance most typically use a security level between 1 and 99.

B. The Cisco ASA appliance supports Active/Active or Active/Standby failover.

C. The Cisco ASA appliance has no default MPF configurations.

D. The Cisco ASA appliance uses security contexts to virtually partition the ASA into multiple virtual firewalls.

E. The Cisco ASA appliance supports user-based access control using 802.1x.

F. An SSM is required on the Cisco ASA appliance to support Botnet Traffic Filtering.

Correct Answer: ABD

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/int5505.html

Security Level Overview

Each VLAN interface must have a security level in the range 0 to 100 (from lowest to highest). For example, you should assign your most secure network, such as the inside business network, to level 100. The outside network connected to

the Internet can be level 0. Other networks, such as a home network can be in between. You can assign interfaces to the same security level. See the "Allowing Communication Between VLAN Interfaces on the Same Security Level" section

for more information.

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/failover.html

Active/Standby Failover Overview

Active/Standby failover lets you use a standby security appliance to take over the functionality of a failed unit. When the active unit fails, it changes to the standby state while the standby unit changes to the active state. The unit that becomes

active assumes the IP addresses (or, for transparent firewall, the management IP address) and MAC addresses of the failed unit and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses and MAC

addresses. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network.

Active/Active Failover Overview

Active/Active failover is only available to security appliances in multiple context mode. In an Active/Active failover configuration, both security appliances can pass network traffic.

In Active/Active failover, you divide the security contexts on the security appliance into failover groups. A failover group is simply a logical group of one or more security contexts. You can create a maximum of two failover groups on the

security appliance. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default.

The failover group forms the base unit for failover in Active/Active failover. Interface failure monitoring, failover, and active/standby status are all attributes of a failover group rather than the unit. When an active failover group fails, it changes

to the standby state while the standby failover group becomes active. The interfaces in the failover group that becomes active assume the MAC and IP addresses of the interfaces in the failover group that failed. The interfaces in the failover

group that is now in the standby state take over the standby MAC and IP addresses.

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/contexts.html

Security Context Overview

You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having

multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

QUESTION 2

Which network device does NTP authenticate?

A. Only the time source

B. Only the client device

C. The firewall and the client device

D. The client device and the time source

Correct Answer: A

NTP authentication is used to authenticate the time source, not the recipient. Reference:
http://www.ine.com/resources/ntp-authentication.htm

QUESTION 3

Which Layer 2 protocol provides loop resolution by managing the physical paths to given network segments?

A. root guard

B. port fast

C. HSRP

D. STP

Correct Answer: D

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_configuration_example09186a008009467c.shtml

Introduction Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches. The specification for STP is IEEE 802.1D. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network.

QUESTION 4

Which statement describes a result of securing the Cisco IOS image using the Cisco IOS image resilience feature?

A. The show version command does not show the Cisco IOS image file location.

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

C. When the router boots up, the Cisco IOS image is loaded from a secured FTP location.

D. The running Cisco IOS image is encrypted and then automatically backed up to the NVRAM.

E. The running Cisco IOS image is encrypted and then automatically backed up to a TFTP server.

Correct Answer: B

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

secure boot-config To take a snapshot of the router running configuration and securely archive it in persistent storage, use the secure boot-config command in global configuration mode. To remove the secure configuration archive and disable configuration resilience, use the no form of this command.

secure boot-config [restore filename] no secure boot-config Usage Guidelines Without any parameters, this command takes a snapshot of the router running configuration and securely archives it in persistent storage. Like the image, the configuration archive is hidden and cannot be viewed or removed directly from the command-line interface (CLI) prompt . It is recommended that you run this command after the router has been fully configured to reach a steady state of operation and the running configuration is considered complete for a restoration, if required. A syslog message is printed on the console notifying the user of configuration resilience activation. The secure archive uses the time of creation as its filename. For example, .runcfg-20020616-081702.ar was created July 16 2002 at

8:17:02.

The restore option reproduces a copy of the secure configuration archive as the supplied filename

(disk0:running-config, slot1:runcfg, and so on). The restore operation will work only if configuration resilience is enabled. The number of restored copies that can be created is unlimited.

The no form of this command removes the secure configuration archive and disables configuration resilience.

An enable, disable, enable sequence has the effect of upgrading the configuration archive if any changes were made to the running configuration since the last time the feature was disabled.

The configuration upgrade scenario is similar to an image upgrade. The feature detects a different version of Cisco IOS and notifies the user of a version mismatch. The same command can be run to upgrade the configuration archive to a

newer version after new configuration commands corresponding to features in the new image have been issued.

The correct sequence of steps to upgrade the configuration archive after an image upgrade is as follows:

-

Configure new commands

-

Issue the secure boot-config command secure boot-image To enable Cisco IOS image resilience, use the secure boot-image command in global configuration mode. To disable Cisco IOS image resilience and release the secured image so that it can be safely removed, use the no form of this command.

secure boot-image no secure boot-image Usage Guidelines This command enables or disables the securing of the running Cisco IOS image. The following two possible scenarios exist with this command.

-

When turned on for the first time, the running image (as displayed in the show version command output) is secured, and a syslog entry is generated. This command will function properly only when the system is configured to run an image

from a disk with an Advanced Technology Attachment (ATA) interface. Images booted from a TFTP server cannot be secured. Because this command has the effect of "hiding" the running image, the image file will not be included in any

directory listing of the disk. The no form of this command releases the image so that it can be safely removed.

-

If the router is configured to boot up with Cisco IOS resilience and an image with a different version of Cisco IOS is detected, a message similar to the following is displayed at bootup:

ios resilience :Archived image and configuration version 12.2 differs from running version 12.3.

Run secure boot-config and image commands to upgrade archives to running version.

To upgrade the image archive to the new running image, reenter this command from the console. A message will be displayed about the upgraded image. The old image is released and will be visible in the dir command output.

QUESTION 5

How are Cisco IOS access control lists processed?

A. Standard ACLs are processed first.

B. The best match ACL is matched first.

C. Permit ACL entries are matched first before the deny ACL entries.

D. ACLs are matched from top down.

E. The global ACL is matched first before the interface ACL.

Correct Answer: D

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

Process ACLs Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted. A single-entry ACL with only one deny entry has the effect of denying all traffic. You must have at least one permit statement in an ACL or all traffic is blocked. These two ACLs (101 and 102) have the same effect.

QUESTION 6

Which source port does IKE use when NAT has been detected between two VPN gateways?

A. TCP 4500

B. TCP 500

C. UDP 4500

D. UDP 500

Correct Answer: C

QUESTION 7

When a company puts a security policy in place, what is the effect on the company\\'s business?

A. Minimizing risk

B. Minimizing total cost of ownership

C. Minimizing liability

D. Maximizing compliance

Correct Answer: A

QUESTION 8

With which two NAT types can Cisco ASA implement address translation? (Choose two.)

A. network object NAT

B. destination NAT

C. twice NAT

D. source NAT

E. double NAT

Correct Answer: AC

QUESTION 9

Which three TACACS+ 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: BCE

QUESTION 10

Which Cisco feature can help mitigate spoofing attacks by verifying symmetry of the traffic path?

A. Unidirectional Link Detection

B. Unicast Reverse Path Forwarding

C. TrustSec

D. IP Source Guard

Correct Answer: B

QUESTION 11

Which type of Cisco IOS access control list is identified by 100 to 199 and 2000 to 2699?

A. standard

B. extended

C. named

D. IPv4 for 100 to 199 and IPv6 for 2000 to 2699

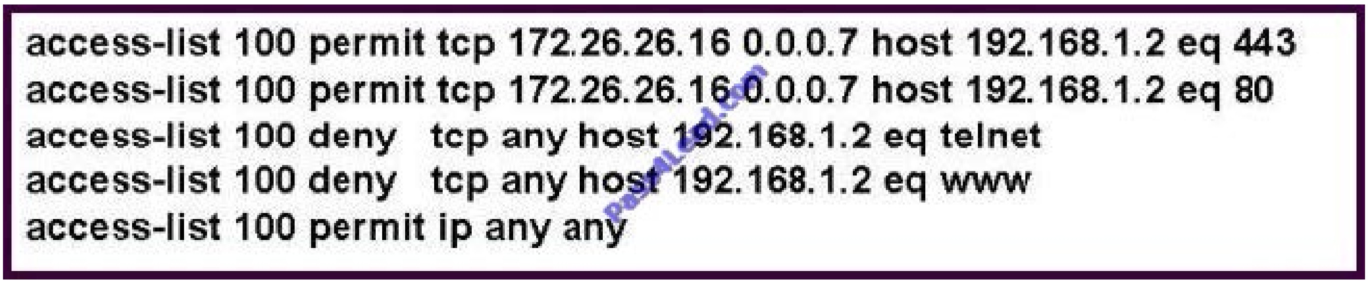
Correct Answer: B

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html

ACL Numbers The number you use to denote your ACL shows the type of access list that you are creating. Table 23-2 lists the access list number and corresponding type and shows whether or not they are supported by the switch. The Catalyst 2950 switch supports IP standard and IP extended access lists, numbers 1 to 199 and 1300 to 2699. 1-99 IP standard access list 100-199 IP extended access list 200-299 Protocol type-code access list 300-399 DECnet access list 400-499 XNS standard access list 500-599 XNS extended access list 600-699 AppleTalk access list 700-799 48-bit MAC address access list 800-899 IPX standard access list 900-999 IPX extended access list 1000-1099 IPX SAP access list 1100-1199 Extended 48-bit MAC address access list 1200-1299 IPX summary address access list 1300-1999 IP standard access list (expanded range) 2000-2699 IP extended access list (expanded range)

QUESTION 12

Refer to the exhibit.



```
access-list 100 permit tcp 172.26.26.16 0.0.0.7 host 192.168.1.2 eq 443
access-list 100 permit tcp 172.26.26.16 0.0.0.7 host 192.168.1.2 eq 80
access-list 100 deny   tcp any host 192.168.1.2 eq telnet
access-list 100 deny   tcp any host 192.168.1.2 eq www
access-list 100 permit ip any any
```

Which traffic is permitted by this ACL?

A. TCP traffic sourced from any host in the 172.26.26.8/29 subnet on any port to host 192.168.1.2 port 80 or 443

B. TCP traffic sourced from host 172.26.26.21 on port 80 or 443 to host 192.168.1.2 on any port

C. any TCP traffic sourced from host 172.26.26.30 destined to host 192.168.1.1

D. any TCP traffic sourced from host 172.26.26.20 to host 192.168.1.2

Correct Answer: C

www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

Extended ACLs

Extended ACLs were introduced in Cisco IOS Software Release 8.3. Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL.

IP

access-list access-list-number

[dynamic dynamic-name [timeout minutes]]

{deny|permit} protocol source source-wildcard

destination destination-wildcard [precedence precedence]

[tos tos] [log|log-input] [time-range time-range-name]

ICMP

access-list access-list-number

[dynamic dynamic-name [timeout minutes]]

{deny|permit} icmp source source-wildcard destination destination-wildcard

[icmp-type [icmp-code] |icmp-message]

[precedence precedence] [tos tos] [log|log-input]

[time-range time-range-name]

TCP

access-list access-list-number

[dynamic dynamic-name [timeout minutes]]

{deny|permit} tcp source source-wildcard [operator [port]]

destination destination-wildcard [operator [port]]

[established] [precedence precedence] [tos tos]

[log|log-input] [time-range time-range-name]

UDP

access-list access-list-number

[dynamic dynamic-name [timeout minutes]]

{deny|permit} udp source source-wildcard [operator [port]]

destination destination-wildcard [operator [port]]

[precedence precedence] [tos tos] [log|log-input]

[time-range time-range-name]

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

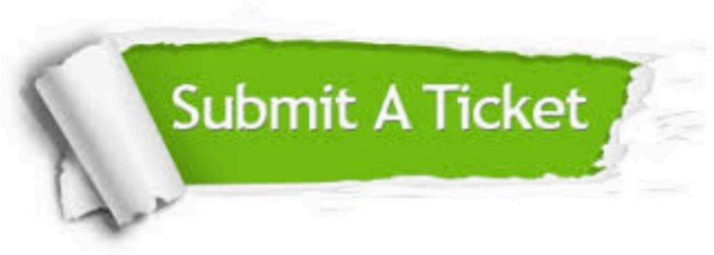
Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

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

Need Help

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



One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.