

Cisco 640-554



Implementing Cisco IOS Network Security (IINS v2.0)

Version: 20.0

Topic 1, Volume A

QUESTION NO: 1

Which two features are supported by Cisco IronPort Security Gateway? (Choose two.)

- A. Spam protection
- B. Outbreak intelligence
- C. HTTP and HTTPS scanning
- D. Email encryption
- E. DDoS protection

Answer: A,D

Explanation: <http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10154/data-sheet-c78-729751.html>

Product Overview

Over the past 20 years, email has evolved from a tool used primarily by technical and research professionals to become the backbone of corporate communications. Each day, more than 100 billion corporate email messages are exchanged. As the level of use rises, security becomes a greater priority. Mass spam campaigns are no longer the only concern. Today, spam and malware are just part of a complex picture that includes inbound threats and outbound risks.

Cisco® Email Security solutions defend mission-critical email systems with appliance, virtual, cloud, and hybrid solutions. The industry leader in email security solutions, Cisco delivers:

QUESTION NO: 2

Which option is a feature of Cisco ScanSafe technology?

- A. spam protection
- B. consistent cloud-based policy
- C. DDoS protection
- D. RSA Email DLP

Answer: B

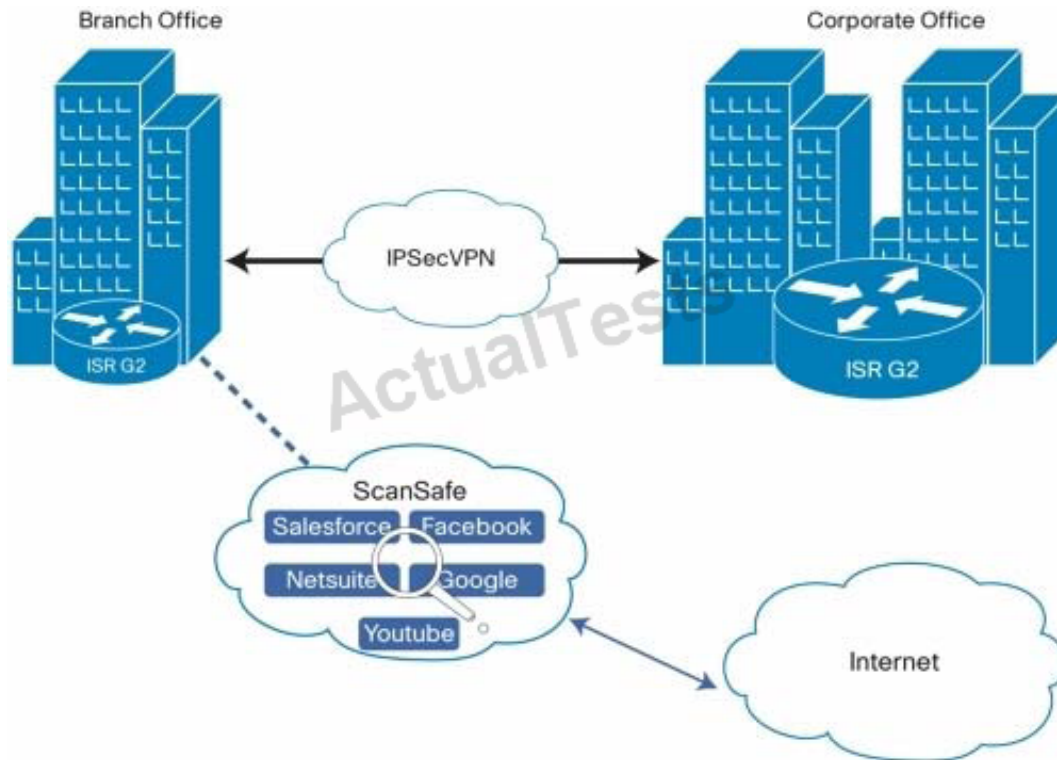
Explanation:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6525/ps6538/ps6540/data_sheet_c78-655324.html

Cisco Enterprise Branch Web Security

The Cisco® Integrated Services Router G2 (ISR G2) Family delivers numerous security services, including firewall, intrusion prevention, and VPN. These security capabilities have been extended with Cisco ISR Web Security with Cisco ScanSafe for a simple, cost-effective, on-demand web security solution that requires no additional hardware. Organizations can deploy and enable market-leading web security quickly and easily, and can enable secure local Internet access for all sites and users, saving bandwidth, money, and resources.

Figure 1. Typical Cisco ISR Web Security with Cisco ScanSafe Deployment



Cisco ISR Web Security with Cisco ScanSafe enables branch offices to intelligently redirect web traffic to the cloud to enforce granular security and control policy over dynamic Web 2.0 content, protecting branch office users from threats such as Trojans, back doors, rogue scanners, viruses, and worms. The Cisco ISR Web Security with Cisco ScanSafe feature will be available in the Security SEC K9 license bundle

QUESTION NO: 3

Which two characteristics represent a blended threat? (Choose two.)

- A. man-in-the-middle attack
- B. trojan horse attack

- C. pharming attack
- D. denial of service attack
- E. day zero attack

Answer: B,E

Explanation:

http://www.cisco.com/web/IN/about/network/threat_defense.html

Rogue developers create such threats by using worms, viruses, or application-embedded attacks. Botnets can be used to seed an attack, for example, rogue developers can use worms or application-embedded attacks, that is an attack that is hidden within application traffic such as web traffic or peer-to-peer shared files, to deposit "Trojans". This combination of attack techniques - a virus or worm used to deposit a Trojan, for example-is relatively new and is known as a blended attack. A blended attack can also occur in phases: an initial attack of a virus with a Trojan that might open up an unsecured port on a computer, disable an access control list (ACL), or disarm antivirus software, with the goal of a more devastating attack to follow soon after. Host Firewall on servers and desktops/laptops, day zero protection & intelligent behavioral based protection from application vulnerability and related flaws (within or inserted by virus, worms or Trojans) provided great level of confidence on what is happening within an organization on a normal day and when there is a attack situation, which segment and what has gone wrong and gives flexibility and control to stop such situations by having linkages of such devices with monitoring, log-analysis and event co-relation system.

QUESTION NO: 4

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

Answer: C

Explanation:

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 NO: 5

Refer to the exhibit.

```
router#sh run | include username
username test secret 5 $1$knm.$GOGQBIL8TK77P0LWxvX4O0
```

What does the option secret 5 in the username global configuration mode command indicate about the user password?

- A. It is hashed using SHA.
- B. It is encrypted using DH group 5.
- C. It is hashed using MD5.
- D. It is encrypted using the service password-encryption command.
- E. It is hashed using a proprietary Cisco hashing algorithm.
- F. It is encrypted using a proprietary Cisco encryption algorithm.

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/120s_md5.html

Feature Overview

Using the Enhanced Password Security feature, you can configure MD5 encryption for username passwords.

Before the introduction of this feature there were two types of passwords associated with usernames. Type 0 is a clear text password visible to any user who has access to privileged mode on the router. Type 7 is a password with a weak, exclusive-or type encryption. Type 7 passwords can be retrieved from the encrypted text by using publicly available tools.

MD5 encryption is a one-way hash function that makes reversal of an encrypted password impossible, providing strong encryption protection. Using MD5 encryption, you cannot retrieve clear text passwords. MD5 encrypted passwords cannot be used with protocols that require that the clear text password be retrievable, such as Challenge Handshake Authentication Protocol (CHAP).

Use the username (secret) command to configure a user name and an associated MD5 encrypted secret.

Configuring Enhanced Security Password

Router(config)# username name secret 0 password

Configures a username and encrypts a clear text password with MD5 encryption.

or

Router(config)# username name secret 5 encrypted-secret

Configures a username and enters an MD5 encrypted text string which is stored as the MD5 encrypted password for the specified username.

QUESTION NO: 6

What does level 5 in this enable secret global configuration mode command indicate?

router#enable secret level 5 password

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

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfpass.html

To configure the router to require an enable password, use either of the following commands in global configuration mode:

Router(config)# enable password [level level] {password| encryption-type encrypted-password}

Establishes a password for a privilege command mode.

Router(config)# enable secret [level level] {password | encryption-type encrypted-password}

Specifies a secret password, saved using a non-reversible encryption method. (If enable password and enable secret are both set, users must enter the enable secret password.)

Use either of these commands with the level option to define a password for a specific privilege level.

After you specify the level and set a password, give the password only to users who need to have access at this level. Use the privilege level configuration command to specify commands accessible at various levels.

QUESTION NO: 7

Which Cisco management tool provides the ability to centrally provision all aspects of device configuration across the Cisco family of security products?

- A. Cisco Configuration Professional
- B. Security Device Manager
- C. Cisco Security Manager
- D. Cisco Secure Management Server

Answer: C

Explanation:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/data_sheet_c78-27090.html

Cisco Security Manager 4.4 Data Sheet

Cisco® Security Manager is a comprehensive management solution that enables advanced management and rapid troubleshooting of multiple security devices. Cisco Security Manager provides scalable, centralized management from which administrators can efficiently manage a wide range of Cisco security devices, gain visibility across the network deployment, and securely share information with other essential network services such as compliance systems and advanced security analysis systems. Designed to maximize operational efficiency, Cisco Security Manager also includes a powerful suite of automated capabilities, such as health and performance monitoring, software image management, auto-conflict detection, and integration with ticketing systems.

QUESTION NO: 8

Which option is the correct representation of the IPv6 address 2001:0000:150C:0000:41B1:45A3:041D?

- A. 2001::150c::41b1:45a3:041d
- B. 2001:0:150c:0::41b1:45a3:04d1
- C. 2001:150c::41b1:45a3::41d
- D. 2001:0:150c::41b1:45a3:41d

Answer: D

Explanation:

http://www.cisco.com/web/strategy/docs/gov/IPv6_WP.pdf

Address Representation

The first area to address is how to represent these 128 bits. Due to the size of the numbering space, hexadecimal numbers and colons were chosen to represent IPv6 addresses. An example IPv6 address is:

2001:0DB8:130F:0000:0000:7000:0000:140B

Note the following:

- There is no case sensitivity. Lower case "a" means the same as capital "A".
- There are 16 bits in each grouping between the colons.
 - 8 fields * 16 bits/field = 128 bits

There are some accepted ways to shorten the representation of the above address:

- Leading zeroes can be omitted, so a field of zeroes can be represented by a single 0.
- Trailing zeroes must be represented.
- Successive fields of zeroes can be shortened down to "::". This shorthand representation can only occur once in the address.

Taking these rules into account, the address shown above can be shortened to:

2001:0DB8:130F:0000:0000:7000:0000:140B

2001:DB8:130F:0:0:7000:0:140B (Leading zeroes)

2001:DB8:130F:0:0:7000:0:140B (Trailing zeroes)

2001:DB8:130F::7000:0:140B (Successive field of zeroes)

QUESTION NO: 9

Which three options are common examples of AAA implementation on Cisco routers? (Choose three.)

- A.** authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
- B.** authenticating administrator access to the router console port, auxiliary port, and vty ports
- C.** implementing PKI to authenticate and authorize IPsec VPN peers using digital certificates
- D.** tracking Cisco NetFlow accounting statistics
- E.** securing the router by locking down all unused services
- F.** performing router commands authorization using TACACS+

Answer: A,B,F

Explanation:

http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.html

Need for AAA Services

Security for user access to the network and the ability to dynamically define a user's profile to gain access to network resources has a legacy dating back to asynchronous dial access. AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers, which is usually the function of a router or access server.

Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage time for billing purposes.

AAA information is typically stored in an external database or remote server such as RADIUS or TACACS+.

The information can also be stored locally on the access server or router. Remote security servers, such as RADIUS and TACACS+, assign users specific privileges by associating attribute-value (AV) pairs, which define the access rights with the appropriate user. All authorization methods must be defined through AAA.

QUESTION NO: 10

When AAA login authentication is configured 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. group RADIUS
- B. group TACACS+
- C. local
- D. krb5
- E. enable
- F. if-authenticated

Answer: C,E

Explanation:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scftplus.html

TACACS+ Authentication Examples

The following example shows how to configure TACACS+ as the security protocol for PPP authentication:

```
aaa new-model
aaa authentication ppp test group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
```

ppp authentication chap pap test

The lines in the preceding sample configuration are defined as follows:

- The aaa new-model command enables the AAA security services.
- The aaa authentication command defines a method list, "test," to be used on serial interfaces running PPP.

The keyword group tacacs+ means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword local indicates that authentication will be attempted using the local database on the network access server.

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800946a3.shtml

Authentication Start to configure TAC+ on the router.

Enter enable mode and type configure terminal before the command set. This command syntax ensures that you are not locked out of the router initially, providing the tac_plus_executable is not running:

!--- Turn on TAC+.

aaa new-model

enable password whatever

!--- These are lists of authentication methods.

!--- "linmethod", "vtymethod", "conmethod", and

!--- so on are names of lists, and the methods

!--- listed on the same lines are the methods

!--- in the order to be tried. As used here, if

!--- authentication fails due to the

!--- tac_plus_executable not being started, the

!--- enable password is accepted because

!--- it is in each list.

!

aaa authentication login linmethod tacacs+ enable

aaa authentication login vtymethod tacacs+ enable

aaa authentication login conmethod tacacs+ enable

QUESTION NO: 11

Which two characteristics of the TACACS+ protocol are true? (Choose two.)

- A. uses UDP ports 1645 or 1812
- B. separates AAA functions
- C. encrypts the body of every packet
- D. offers extensive accounting capabilities
- E. is an open RFC standard protocol

Answer: B,C

Explanation:

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

Packet Encryption

RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.

TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.

Authentication and Authorization RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.

TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.

During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

QUESTION NO: 12

Refer to the exhibit.

```

Oct13 19:46:06.170: AAA/MEMORY: create_user (0x4C5E1F60) user='tecteam'
ruser='NULL' ds0=0 port='tty515' rem_addr='10.0.2.13' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
Oct13 19:46:06.170: AAA/AUTHEN/START (2600878790): port='tty515' list=""
action=LOGIN service=ENABLE
Oct13 19:46:06.170: AAA/AUTHEN/START (2600878790): console enable - default to
enable password (if any)
Oct13 19:46:06.170: AAA/AUTHEN/START (2600878790): Method=ENABLE
Oct13 19:46:06.170: AAA/AUTHEN (2600878790): status = GETPASS
Oct13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): continue_login
(user='(undef)')
Oct13 19:46:07.266: AAA/AUTHEN (2600878790): status = GETPASS
Oct13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): Method=ENABLE
Oct13 19:46:07.266: AAA/AUTHEN (2600878790): password incorrect
Oct13 19:46:07.266: AAA/AUTHEN (2600878790): status = FAIL
Oct13 19:46:07.266: AAA/MEMORY: free_user (0x4C5E1F60) user='NULL'
ruser='NULL' port='tty515' rem_addr='10.0.2.13' authen_type=ASCII service=ENABLE
priv=15 vrf= (id=0)

```

Which statement about this output is true?

- A. The user logged into the router with the incorrect username and password.
- B. The login failed because there was no default enable password.
- C. The login failed because the password entered was incorrect.
- D. The user logged in and was given privilege level 15.

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfaaa.html

debug aaa authentication

To display information on AAA/Terminal Access Controller Access Control System Plus (TACACS+) authentication, use the debug aaa authentication privileged EXEC command. To disable debugging command, use the no form of the command.

debug aaa authentication

no debug aaa authentication

The following is sample output from the debug aaa authentication command. A single EXEC login that uses the "default" method list and the first method, TACACS+, is displayed. The TACACS+ server sends a GETUSER request to prompt for the username and then a GETPASS request to prompt for the password, and finally a PASS response to indicate a successful login. The number 50996740 is the session ID, which is unique for each authentication. Use this ID number to distinguish between different authentications if several are occurring concurrently.

Router# debug aaa authentication

6:50:12: AAA/AUTHEN: create_user user="" ruser="" port='tty19' rem_addr='172.31.60.15'

authen_type=1 service=1 priv=1

6:50:12: AAA/AUTHEN/START (0): port='tty19' list="" action=LOGIN service=LOGIN
6:50:12: AAA/AUTHEN/START (0): using "default" list
6:50:12: AAA/AUTHEN/START (50996740): Method=TACACS+
6:50:12: TAC+ (50996740): received authen response status = GETUSER
6:50:12: AAA/AUTHEN (50996740): status = GETUSER
6:50:15: AAA/AUTHEN/CONT (50996740): continue_login
6:50:15: AAA/AUTHEN (50996740): status = GETUSER
6:50:15: AAA/AUTHEN (50996740): Method=TACACS+
6:50:15: TAC+: send AUTHEN/CONT packet
6:50:15: TAC+ (50996740): received authen response status = GETPASS
6:50:15: AAA/AUTHEN (50996740): status = GETPASS
6:50:20: AAA/AUTHEN/CONT (50996740): continue_login
6:50:20: AAA/AUTHEN (50996740): status = GETPASS
6:50:20: AAA/AUTHEN (50996740): Method=TACACS+
6:50:20: TAC+: send AUTHEN/CONT packet
6:50:20: TAC+ (50996740): received authen response status = PASS
6:50:20: AAA/AUTHEN (50996740): status = PASS

QUESTION NO: 13

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

Answer: C

Explanation:

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]
```

QUESTION NO: 14

Refer to the exhibit.

```
access-list 2 permit 10.10.0.10
access-list 2 deny 10.10.0.0.0.255.255
access-list 2 permit 10.0.0.0.0.255.255.255
interface FastEthernet0/0
 ip access-group 2 in
```

Which statement about this partial CLI configuration of an access control list is true?

- A.** The access list accepts all traffic on the 10.0.0.0 subnets.
- B.** All traffic from the 10.10.0.0 subnets is denied.
- C.** Only traffic from 10.10.0.10 is allowed.
- D.** This configuration is invalid. It should be configured as an extended ACL to permit the associated wildcard mask.
- E.** From the 10.10.0.0 subnet, only traffic sourced from 10.10.0.10 is allowed; traffic sourced from the other 10.0.0.0 subnets also is allowed.
- F.** The access list permits traffic destined to the 10.10.0.10 host on FastEthernet0/0 from any source.

Answer: E

Explanation:

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 NO: 15

Which type of Cisco ASA access list entry can be configured to match multiple entries in a single statement?

- A. nested object-class
- B. class-map
- C. extended wildcard matching
- D. object groups

Answer: D

Explanation:

<http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/objectgroups.html>

Information About Object Groups

By grouping like objects together, you can use the object group in an ACE instead of having to enter an ACE for each object separately. You can create the following types of object groups:

- Protocol
- Network
- Service
- ICMP type

For example, consider the following three object groups:

- MyServices—Includes the TCP and UDP port numbers of the service requests that are allowed access to the internal network.
 - TrustedHosts—Includes the host and network addresses allowed access to the greatest range of services and servers.
 - PublicServers—Includes the host addresses of servers to which the greatest access is provided.
- After creating these groups, you could use a single ACE to allow trusted hosts to make specific service requests to a group of public servers.

You can also nest object groups in other object groups.

QUESTION NO: 16

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.

Answer: A

Explanation:

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 NO: 17

You have been tasked by your manager to implement syslog in your network. Which option is an important factor to consider in your implementation?

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

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/sec_chap5.html

Time Synchronization

When implementing network telemetry, it is important that dates and times are both accurate and synchronized across all network infrastructure devices. Without time synchronization, it is very difficult to correlate different sources of telemetry.

Enabling Network Time Protocol (NTP) is the most common method of time synchronization.

General best common practices for NTP include:

- A common, single time zone is recommended across an entire network infrastructure in order to enable the consistency & synchronization of time across all network devices.
- The time source should be from an authenticated, limited set of authorized NTP servers.

Detailed information on NTP and NTP deployment architectures is available in the Network Time Protocol: Best

Practices White Paper at the following URL:

<http://www.cisco.com/warp/public/126/ntpm.pdf>

Timestamps and NTP Configuration

In Cisco IOS, the steps to enable timestamps and NTP include:

Step 1 Enable timestamp information for debug messages.

Step 2 Enable timestamp information for log messages.

Step 3 Define the network-wide time zone.

Step 4 Enable summertime adjustments.

Step 5 Restrict which devices can communicate with this device as an NTP server.

Step 6 Restrict which devices can communicate with this device as an NTP peer.

Step 7 Define the source IP address to be used for NTP packets.

Step 8 Enable NTP authentication.

Step 9 Define the NTP servers.

Step 10 Define the NTP peers.

Step 11 Enable NTP to update the device hardware clock

QUESTION NO: 18

Which protocol secures router management session traffic?

A. SSTP

B. POP

- C. Telnet
- D. SSH

Answer: D

Explanation:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Encrypting Management Sessions

Because information can be disclosed during an interactive management session, this traffic must be encrypted so that a malicious user cannot gain access to the data being transmitted.

Encrypting the traffic allows a secure remote access connection to the device. If the traffic for a management session is sent over the network in cleartext, an attacker can obtain sensitive information about the device and the network. An administrator is able to establish an encrypted and secure remote access management connection to a device by using the SSH or HTTPS (Secure Hypertext Transfer Protocol) features. Cisco IOS software supports SSH version 1.0 (SSHv1), SSH version 2.0 (SSHv2), and HTTPS that uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for authentication and data encryption. Note that SSHv1 and SSHv2 are not compatible.

Cisco IOS software also supports the Secure Copy Protocol (SCP), which allows an encrypted and secure connection for copying device configurations or software images. SCP relies on SSH. This example configuration enables SSH on a Cisco IOS device:

```
!  
ip domain-name example.com  
!  
crypto key generate rsa modulus 2048  
!  
ip ssh time-out 60  
ip ssh authentication-retries 3  
ip ssh source-interface GigabitEthernet 0/1  
!  
line vty 0 4  
transport input ssh  
!
```

QUESTION NO: 19

Which two considerations about secure network management are important? (Choose two.)

- A. log tampering
- B. encryption algorithm strength
- C. accurate time stamping
- D. off-site storage
- E. Use RADIUS for router commands authorization.
- F. Do not use a loopback interface for device management access.

Answer: A,C

Explanation:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/best/practices/recommendations.html>

Enable Timestamped Messages

Enable timestamps on log messages:

Router(config)# service timestamps log datetime localtime show-timezone msec

Enable timestamps on system debug messages:

Router(config)# service timestamps debug datetime localtime show-timezone msec

QUESTION NO: 20

Which command enables Cisco IOS image resilience?

- A. secure boot-<IOS image filename>
- B. secure boot-running-config
- C. secure boot-start
- D. secure boot-image

Answer: D

Explanation:

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 NO: 21

Which router management feature provides for the ability to configure multiple administrative views?

- A. role-based CLI
- B. virtual routing and forwarding
- C. secure config privilege {level}
- D. parser view view name

Answer: A

Explanation:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html

Role-Based CLI Access

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

QUESTION NO: 22

You suspect that an attacker in your network has configured a rogue Layer 2 device to intercept

traffic from multiple VLANs, which allows 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. Place unused active ports in an unused VLAN.
- C. Secure the native VLAN, VLAN 1, with encryption.
- D. Set the native VLAN on the trunk ports to an unused VLAN.
- E. Disable DTP on ports that require trunking.

Answer: D,E

Explanation:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/layer2.html>

Layer 2 LAN Port Modes

Table 17-2 lists the Layer 2 LAN port modes and describes how they function on LAN ports.

switchport mode access

Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.

switchport mode dynamic desirable

Makes the LAN port actively attempt to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk, desirable, or auto mode. This is the default mode for all LAN ports.

switchport mode dynamic auto

Makes the LAN port willing to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk or desirable mode.

switchport mode trunk

Puts the LAN port into permanent trunking mode and negotiates to convert the link into a trunk link. The LAN port becomes a trunk port even if the neighboring port does not agree to the change.

switchport nonegotiate

Puts the LAN port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

Double Encapsulation Attack

When double-encapsulated 802.1Q packets are injected into the network from a device whose VLAN happens to be the native VLAN of a trunk, the VLAN identification of those packets cannot be preserved from end to end since the 802.1Q trunk would always modify the packets by stripping their outer tag. After the external tag is removed, the internal tag permanently becomes the packet's only VLAN identifier. Therefore, by doubleencapsulating packets with two different tags, traffic can be made to hop across VLANs.

This scenario is to be considered a misconfiguration, since the 802.1Q standard does not necessarily force the users to use the native VLAN in these cases. As a matter of fact, the proper configuration that should always be used is to clear the native VLAN from all 802.1Q trunks (alternatively, setting them to 802.1q-all-tagged mode achieves the exact same result). In cases where the native VLAN cannot be cleared, then always pick an unused VLAN as native VLAN of all the trunks; don't use this VLAN for any other purpose.

Protocols like STP, DTP, and UDLD (check out [3]) should be the only rightful users of the native VLAN and their traffic should be completely isolated from any data packets.

QUESTION NO: 23

Which statement describes a best practice when configuring trunking on a switch port?

- A. Disable double tagging by enabling DTP on the trunk port.
- B. Enable encryption on the trunk port.
- C. Enable authentication and encryption on the trunk port.
- D. Limit the allowed VLAN(s) on the trunk to the native VLAN only.
- E. Configure an unused VLAN as the native VLAN.

Answer: E

Explanation:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

Double Encapsulation Attack

When double-encapsulated 802.1Q packets are injected into the network from a device whose VLAN happens to be the native VLAN of a trunk, the VLAN identification of those packets cannot be preserved from end to end since the 802.1Q trunk would always modify the packets by stripping their outer tag. After the external tag is removed, the internal tag permanently becomes the packet's only VLAN identifier. Therefore, by double encapsulating packets with two different

tags, traffic can be made to hop across VLANs.

This scenario is to be considered a misconfiguration, since the 802.1Q standard does not necessarily force the users to use the native VLAN in these cases. As a matter of fact, the proper configuration that should always be used is to clear the native VLAN from all 802.1Q trunks (alternatively, setting them to 802.1q-all-tagged mode achieves the exact same result). In cases where the native VLAN cannot be cleared, then always pick an unused VLAN as native VLAN of all the trunks; don't use this VLAN for any other purpose. Protocols like STP, DTP, and UDLD (check out [3]) should be the only rightful users of the native VLAN and their traffic should be completely isolated from any data packets.

QUESTION NO: 24

Which type of Layer 2 attack causes a switch to flood all incoming traffic to all ports?

- A. MAC spoofing attack
- B. CAM overflow attack
- C. VLAN hopping attack
- D. STP attack

Answer: B

Explanation:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_603836.htm
ISummary

The MAC Address Overflow attack is effective if the proper mitigation techniques are not in place on the Cisco Catalyst 6500 series switch. By using publicly (free) and available Layer 2 attack tools found on the Internet, anyone who understands how to setup and run these tools could potentially launch an attack on your network.

MAC address monitoring is a feature present on Cisco Catalyst 6500 Series switches. This feature helps mitigate MAC address flooding and other CAM overflow attacks by limiting the total number of MAC addresses learned by the switch on per-port or per-VLAN basis. With MAC Address Monitoring, a maximum threshold for the total number of MAC addresses can be configured and enforced on a per-port and/or per-VLAN basis.

MAC address monitoring in Cisco IOS Software allows the definition of a single upper (maximum) threshold. In addition, the number of MAC addresses learned can only be monitored on a per-port or per-VLAN basis, and not a per-port-per-VLAN. By default, MAC address monitoring is disabled in Cisco IOS Software. However, the maximum threshold for all ports and VLANs is configured to 500 MAC address entries, and when the threshold is exceeded the system is set to generate a

system message along with a syslog trap. These default values take effect only when MAC address monitoring is enabled. The system can be configured to notify or disable the port or VLAN every time the number of learned MAC addresses exceeds the predefined threshold. In our test, we used the "mac-address-table limit" command on the access layer port interface to configure the MAC address monitoring feature.

QUESTION NO: 25

What is the best way to prevent a VLAN hopping attack?

- A. Encapsulate trunk ports with IEEE 802.1Q.
- B. Physically secure data closets.
- C. Disable DTP negotiations.
- D. Enable BDPU guard.

Answer: C

Explanation:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

802.1Q and ISL Tagging Attack

Tagging attacks are malicious schemes that allow a user on a VLAN to get unauthorized access to another VLAN. For example, if a switch port were configured as DTP auto and were to receive a fake DTP packet, it might become a trunk port and it might start accepting traffic destined for any VLAN. Therefore, a malicious user could start communicating with other VLANs through that compromised port.

Sometimes, even when simply receiving regular packets, a switch port may behave like a full-fledged trunk port (for example, accept packets for VLANs different from the native), even if it is not supposed to. This is commonly referred to as "VLAN leaking" (see [5] for a report on a similar issue).

QUESTION NO: 26

Which statement about PVLAN Edge is true?

- A. PVLAN Edge can be configured to restrict the number of MAC addresses that appear on a single port.
- B. The switch does not forward any traffic from one protected port to any other protected port.

- C. By default, when a port policy error occurs, the switchport shuts down.
- D. The switch only forwards traffic to ports within the same VLAN Edge.

Answer: B

Explanation:

http://www.cisco.com/en/US/tech/tk389/tk814/technologies_configuration_example09186a008017acad.shtml

NotE. Some switches (as specified in the Private VLAN Catalyst Switch Support Matrix) currently support only the PVLAN Edge feature. The term "protected ports" also refers to this feature.

PVLAN Edge ports have a restriction that prevents communication with other protected ports on the same switch. Protected ports on separate switches, however, can communicate with each other. Do not confuse this feature with the normal PVLAN configurations that this document shows. For more information on protected ports, refer to the Configuring Port Security section of the document Configuring Port-Based Traffic Control.

http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_13_ea1/configuration/guide/swtrafc.html

Configuring Protected Ports

Some applications require that no traffic be forwarded between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch.

Protected ports have these features:

- A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Traffic cannot be forwarded between protected ports at Layer 2; all traffic passing between protected ports must be forwarded through a Layer 3 device.
 - Forwarding behavior between a protected port and a nonprotected port proceeds as usual.
- The default is to have no protected ports defined.

QUESTION NO: 27

If you are implementing VLAN trunking, which additional configuration parameter should be added to the trunking configuration?

- A. no switchport mode access
- B. no switchport trunk native VLAN 1
- C. switchport mode DTP
- D. switchport nonnegotiate

Answer: D

Explanation:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/layer2.html>

Layer 2 LAN Port Modes

Table 17-2 lists the Layer 2 LAN port modes and describes how they function on LAN ports.

switchport mode access Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.

switchport mode dynamic desirable

Makes the LAN port actively attempt to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk, desirable, or auto mode. This is the default mode for all LAN ports.

switchport mode dynamic auto

Makes the LAN port willing to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk or desirable mode.

switchport mode trunk Puts the LAN port into permanent trunking mode and negotiates to convert the link into a trunk link. The LAN port becomes a trunk port even if the neighboring port does not agree to the change.

switchport nonegotiate

Puts the LAN port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.

QUESTION NO: 28

When Cisco IOS zone-based policy firewall is configured, which three actions can be applied to a traffic class? (Choose three.)

- A. pass
- B. police
- C. inspect
- D. drop
- E. queue
- F. shape

Answer: A,C,D

Explanation:

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml

Zone-Based Policy Firewall Actions

ZFW provides three actions for traffic that traverses from one zone to another:

Drop—This is the default action for all traffic, as applied by the "class class-default" that terminates every inspect-type policy-map. Other class-maps within a policy-map can also be configured to drop unwanted traffic.

Traffic that is handled by the drop action is "silently" dropped (i.e., no notification of the drop is sent to the relevant end-host) by the ZFW, as opposed to an ACL's behavior of sending an ICMP "host unreachable" message to the host that sent the denied traffic. Currently, there is not an option to change the "silent drop" behavior. The log option can be added with drop for syslog notification that traffic was dropped by the firewall.

Pass—This action allows the router to forward traffic from one zone to another. The pass action does not track the state of connections or sessions within the traffic. Pass only allows the traffic in one direction. A corresponding policy must be applied to allow return traffic to pass in the opposite direction. The pass action is useful for protocols such as IPsec ESP, IPsec AH, ISAKMP, and other inherently secure protocols with predictable behavior. However, most application traffic is better handled in the ZFW with the inspect action.

Inspect—The inspect action offers state-based traffic control. For example, if traffic from the private zone to the Internet zone in the earlier example network is inspected, the router maintains connection or session information for TCP and User Datagram Protocol (UDP) traffic. Therefore, the router permits return traffic sent from Internet-zone hosts in reply to private zone connection requests. Also, inspect can provide application inspection and control for certain service protocols that might carry vulnerable or sensitive application traffic.

Audit-trail can be applied with a parameter-map to record connection/session start, stop, duration, the data volume transferred, and source and destination addresses.

QUESTION NO: 29

With Cisco IOS zone-based policy firewall, by default, which three types of traffic are permitted by the router when some of the router interfaces are assigned to a zone? (Choose three.)

- A.** traffic flowing between a zone member interface and any interface that is not a zone member
- B.** traffic flowing to and from the router interfaces (the self zone)
- C.** traffic flowing among the interfaces that are members of the same zone

- D. traffic flowing among the interfaces that are not assigned to any zone
- E. traffic flowing between a zone member interface and another interface that belongs in a different zone
- F. traffic flowing to the zone member interface that is returned traffic

Answer: B,C,D

Explanation:

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml

Rules For Applying Zone-Based Policy Firewall

Router network interfaces' membership in zones is subject to several rules that govern interface behavior, as is the traffic moving between zone member interfaces:

A zone must be configured before interfaces can be assigned to the zone.

An interface can be assigned to only one security zone.

All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.

Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone. In order to permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.

The self zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

Traffic cannot flow between a zone member interface and any interface that is not a zone member. Pass, inspect, and drop actions can only be applied between two zones.

Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection/CBAC configuration.

If it is required that an interface on the box not be part of the zoning/firewall policy. It might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy) between that zone and any other zone to which traffic flow is desired.

From the preceding it follows that, if traffic is to flow among all the interfaces in a router, all the interfaces must be part of the zoning model (each interface must be a member of one zone or another).

The only exception to the preceding deny by default approach is the traffic to and from the router, which will be permitted by default. An explicit policy can be configured to restrict such traffic.

QUESTION NO: 30

Which option is a key difference between Cisco IOS interface ACL configurations and Cisco ASA

appliance interface ACL configurations?

- A.** The Cisco IOS interface ACL has an implicit permit-all rule at the end of each interface ACL.
- B.** Cisco IOS supports interface ACL and also global ACL. Global ACL is applied to all interfaces.
- C.** The Cisco ASA appliance interface ACL configurations use netmasks instead of wildcard masks.
- D.** The Cisco ASA appliance interface ACL also applies to traffic directed to the IP addresses of the Cisco ASA appliance interfaces.
- E.** The Cisco ASA appliance does not support standard ACL. The Cisco ASA appliance only support extended ACL.

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/acl_extended.html

Additional Guidelines and Limitations

The following guidelines and limitations apply to creating an extended access list:

- When you enter the access-list command for a given access list name, the ACE is added to the end of the access list unless you specify the line number.
- Enter the access list name in uppercase letters so that the name is easy to see in the configuration. You might want to name the access list for the interface (for example, INSIDE), or you can name it for the purpose for which it is created (for example, NO_NAT or VPN).
- Typically, you identify the ip keyword for the protocol, but other protocols are accepted. For a list of protocol names, see the "Protocols and Applications" section.
- Enter the host keyword before the IP address to specify a single address. In this case, do not enter a mask.

Enter the any keyword instead of the address and mask to specify any address.

- You can specify the source and destination ports only for the tcp or udp protocols. For a list of permitted keywords and well-known port assignments, see the "TCP and UDP Ports" section. DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, and Talk each require one definition for TCP and one for UDP. TACACS+ requires one definition for port 49 on TCP.
- You can specify the ICMP type only for the icmp protocol. Because ICMP is a connectionless protocol, you either need access lists to allow ICMP in both directions (by applying access lists to the source and destination interfaces), or you need to enable the ICMP inspection engine. (See the "Adding an ICMP Type Object Group" section.) The ICMP inspection engine treats ICMP sessions as stateful connections. To control ping, specify echo-reply (0) (ASA to host) or echo (8) (host to ASA). See the "Adding an ICMP Type Object Group" section for a list of ICMP types.
- When you specify a network mask, the method is different from the Cisco IOS software access-list command. The ASA uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
- To make an ACE inactive, use the inactive keyword. To reenable it, enter the entire ACE without the inactive keyword. This feature enables you to keep a record of an inactive ACE in your

configuration to make
reenabling easier.

- Use the disable option to disable logging for a specified ACE.

QUESTION NO: 31

Which two options are advantages of an application layer firewall? (Choose two.)

- A. provides high-performance filtering
- B. makes DoS attacks difficult
- C. supports a large number of applications
- D. authenticates devices
- E. authenticates individuals

Answer: B,E

Explanation:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_white_paper0900aecd8058ec85.html

Adding Intrusion Prevention

Gartner's definition of a next-generation firewall is one that combines firewall filtering and intrusion prevention systems (IPSs). Like firewalls, IPSs filter packets in real time. But instead of filtering based on user profiles and application policies, they scan for known malicious patterns in incoming code, called signatures. These signatures indicate the presence of malware, such as worms, Trojan horses, and spyware.

Malware can overwhelm server and network resources and cause denial of service (DoS) to internal employees, external Web users, or both. By filtering for known malicious signatures, IPSs add an extra layer of security to firewall capabilities; once the malware is detected by the IPS, the system will block it from the network.

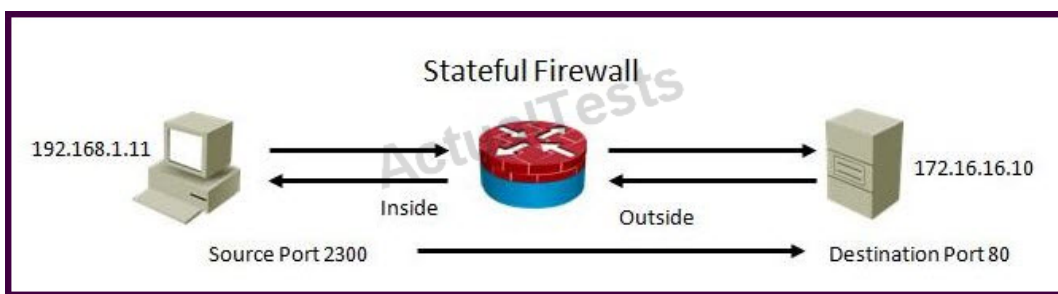
Firewalls provide the first line of defense in any organization's network security infrastructure. They do so by matching corporate policies about users' network access rights to the connection information surrounding each access attempt. If the variables don't match, the firewall blocks the access connection. If the variables do match, the firewall allows the acceptable traffic to flow through the network.

In this way, the firewall forms the basic building block of an organization's network security architecture. It pays to use one with superior performance to maximize network uptime for business-critical operations. The reason is that the rapid addition of voice, video, and collaborative

traffic to corporate networks is driving the need for firewall engines that operate at very high speeds and that also support application-level inspection. While standard Layer 2 and Layer 3 firewalls prevent unauthorized access to internal and external networks, firewalls enhanced with application-level inspection examine, identify, and verify application types at Layer 7 to make sure unwanted or misbehaving application traffic doesn't join the network. With these capabilities, the firewall can enforce endpoint user registration and authentication and provide administrative control over the use of multimedia applications.

QUESTION NO: 32

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`

Answer: A

Explanation:

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 NO: 33

Which option is the resulting action in a zone-based policy firewall configuration with these conditions?

Source: Zone 1
Destination: Zone 2
Zone pair exists?: Yes
Policy exists?: No

- A. no impact to zoning or policy
- B. no policy lookup (pass)
- C. drop
- D. apply default policy

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-zone-pol-fw.html

Zone Pairs

A zone pair allows you to specify a unidirectional firewall policy between two security zones. To define a zone pair, use the zone-pair security command. The direction of the traffic is specified by source and destination zones. The source and destination zones of a zone pair must be security zones.

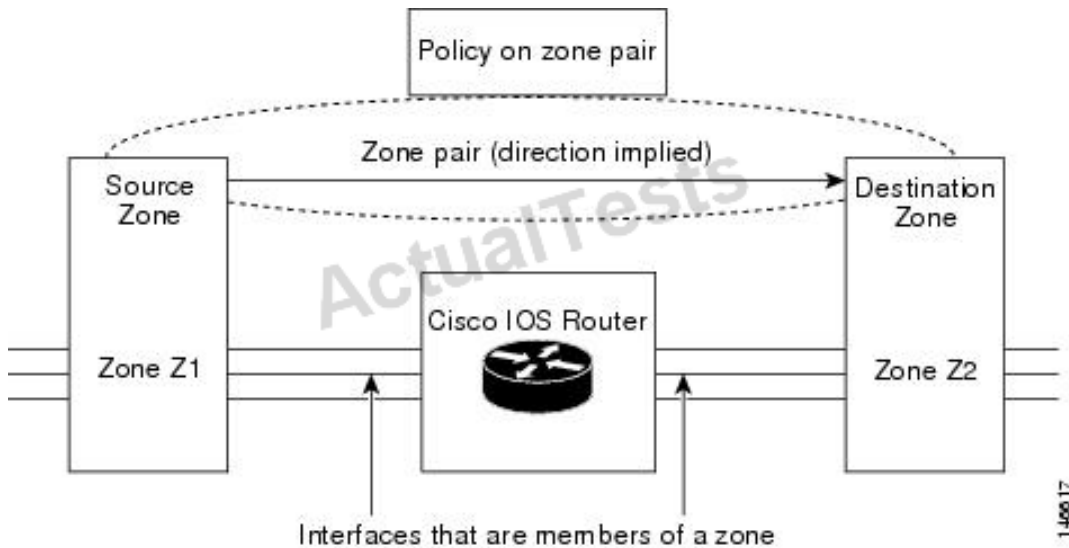
You can select the default or self zone as either the source or the destination zone. The self zone is a systemdefined zone which does not have any interfaces as members. A zone pair that includes the self zone, along with the associated policy, applies to traffic directed to the device or traffic generated by the device. It does not apply to traffic through the device.

The most common usage of firewall is to apply them to traffic through a device, so you need at least two zones (that is, you cannot use the self zone).

To permit traffic between zone member interfaces, you must configure a policy permitting (or inspecting) traffic between that zone and another zone. To attach a firewall policy map to the target zone pair, use the servicepolicy type inspect command.

The figure below shows the application of a firewall policy to traffic flowing from zone Z1 to zone Z2, which means that the ingress interface for the traffic is a member of zone Z1 and the egress interface is a member of zone Z2.

Figure 2. Zone Pairs



If there are two zones and you require policies for traffic going in both directions (from Z1 to Z2 and Z2 to Z1), you must configure two zone pairs (one for each direction).

If a policy is not configured between zone pairs, traffic is dropped. However, it is not necessary to configure a zone pair and a service policy solely for the return traffic. By default, return traffic is not allowed. If a service policy inspects the traffic in the forward direction and there is no zone pair and service policy for the return traffic, the return traffic is inspected. If a service policy passes the traffic in the forward direction and there is no zone pair and service policy for the return traffic, the return traffic is dropped. In both these cases, you need to configure a zone pair and a service policy to allow the return traffic. In the above figure, it is not mandatory that you configure a zone pair source and destination for allowing return traffic from Z2 to Z1. The service policy on Z1 to Z2 zone pair takes care of it.

QUESTION NO: 34

A Cisco ASA appliance has three interfaces configured. The first interface is the inside interface with a security level of 100. The second interface is the DMZ interface with a security level of 50. The third interface is the outside interface with a security level of 0.

By default, without any access list configured, which five types of traffic are permitted? (Choose five.)

- A. outbound traffic initiated from the inside to the DMZ
- B. outbound traffic initiated from the DMZ to the outside
- C. outbound traffic initiated from the inside to the outside

- D. inbound traffic initiated from the outside to the DMZ
- E. inbound traffic initiated from the outside to the inside
- F. inbound traffic initiated from the DMZ to the inside
- G. HTTP return traffic originating from the inside network and returning via the outside interface
- H. HTTP return traffic originating from the inside network and returning via the DMZ interface
- I. HTTP return traffic originating from the DMZ network and returning via the inside interface
- J. HTTP return traffic originating from the outside network and returning via the inside interface

Answer: A,B,C,G,H

Explanation:

<http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/intparam.html>

Security Level Overview

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See the "Allowing Communication Between Interfaces on the Same Security Level" section for more information.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface. If you enable communication for same security interfaces (see the "Allowing Communication Between Interfaces on the Same Security Level" section), there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.

- NetBIOS inspection engine—Applied only for outbound connections.

- OraServ inspection engine—If a control connection for the OraServ port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.

- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

For same security interfaces, you can filter traffic in either direction.

- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- established command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the

lower level host.

For same security interfaces, you can configure established commands for both directions.

QUESTION NO: 35

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

- A. syslog
- B. SDEE
- C. FTP
- D. TFTP
- E. SSH
- F. HTTPS

Answer: B,F

Explanation:

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

Step 4: Enabling IOS IPS

The fourth step is to configure IOS IPS using the following sequence of steps:

Step 4.1: Create a rule name (This will be used on an interface to enable IPS)

```
ip ips name <rule name> < optional ACL>
```

```
router#configure terminal router(config)# ip ips name iosips
```

You can specify an optional extended or standard access control list (ACL) to filter the traffic that will be scanned by this rule name. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

```
router(config)#ip ips name ips list ?
```

<1-199> Numbered access list

WORD Named access list

Step 4.2: Configure IPS signature storage location, this is the directory 'ips' created in Step 2

```
ip ips config location flash:<directory name>
```

```
router(config)#ip ips config location flash:ips
```

Step 4.3: Enable IPS SDEE event notification

```
ip ips notify sdee router(config)#ip ips notify sdee
```

To use SDEE, the HTTP server must be enabled (via the 'ip http server' command). If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot see the

requests. SDEE notification is disabled by default and must be explicitly enabled.

QUESTION NO: 36

Which two functions are required for IPsec operation? (Choose two.)

- A. using SHA for encryption
- B. using PKI for pre-shared key authentication
- C. using IKE to negotiate the SA
- D. using AH protocols for encryption and authentication
- E. using Diffie-Hellman to establish a shared-secret key

Answer: C,E

Explanation:

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094203.shtml

Configure ISAKMP

IKE exists only to establish SAs for IPsec. Before it can do this, IKE must negotiate an SA (an ISAKMP SA) relationship with the peer. Since IKE negotiates its own policy, it is possible to configure multiple policy statements with different configuration statements, then let the two hosts come to an agreement. ISAKMP negotiates:

Oakley

This is a key exchange protocol that defines how to acquire authenticated keying material. The basic mechanism for Oakley is the Diffie-Hellman key exchange algorithm. You can find the standard in RFC 2412: The OAKLEY Key Determination Protocol [leavingcisco.com](http://www.ietf.org/rfc/rfc2412.txt).

QUESTION NO: 37

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

Answer: B

Explanation:

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=281442967&mdfLevel=Software%20Family&treeName=Security&modelName=Cisco%20IOS%20Intrusion%20Prevention%20System%20Feature%20Software&treeMdfid=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 NO: 38

Which four tasks are required when you configure Cisco IOS IPS using the Cisco Configuration Professional IPS wizard? (Choose four.)

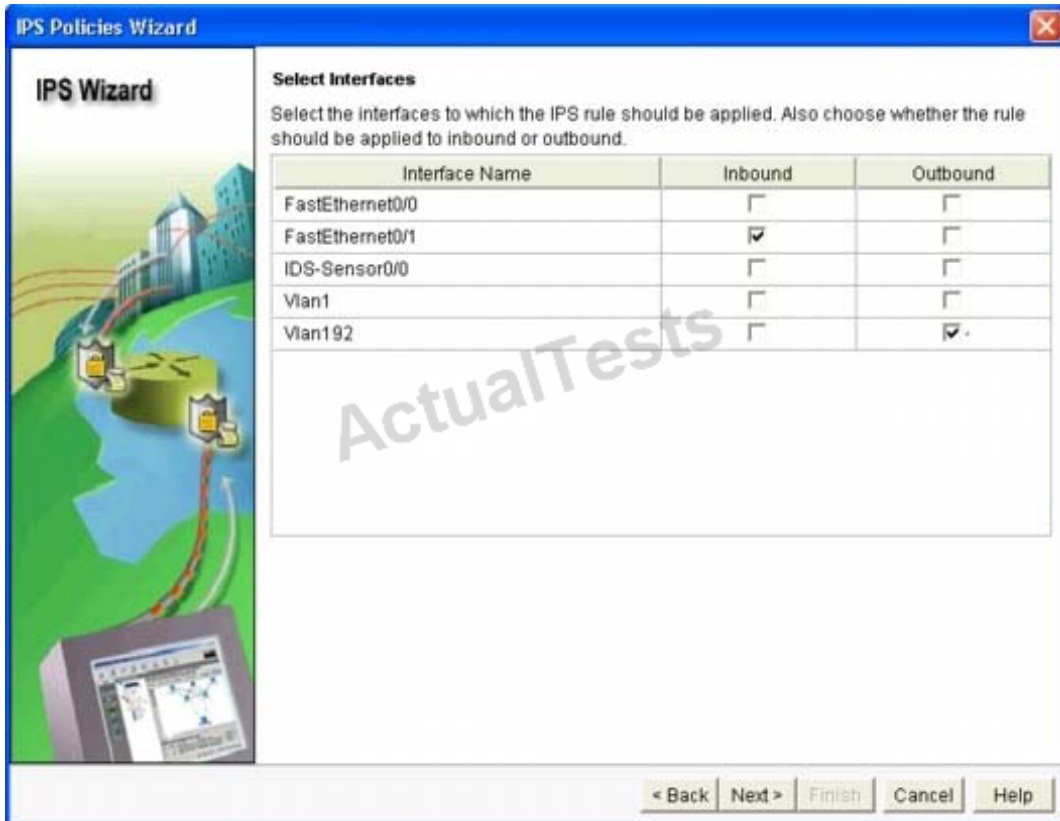
- A. Select the interface(s) to apply the IPS rule.
- B. Select the traffic flow direction that should be applied by the IPS rule.
- C. Add or remove IPS alerts actions based on the risk rating.
- D. Specify the signature file and the Cisco public key.
- E. Select the IPS bypass mode (fail-open or fail-close).
- F. Specify the configuration location and select the category of signatures to be applied to the selected interface(s).

Answer: A,B,D,F

Explanation:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8066d265.html

Step 11. At the 'Select Interfaces' screen, select the interface and the direction that IOS IPS will be applied to, then click 'Next' to continue.



IPS Wizard

Select Interfaces

Select the interfaces to which the IPS rule should be applied. Also choose whether the rule should be applied to inbound or outbound.

Interface Name	Inbound	Outbound
FastEthernet0/0	☐	☐
FastEthernet0/1	☒	☐
IDS-Sensor0/0	☐	☐
Vlan1	☐	☐
Vlan192	☐	☒

< Back Next > Finish Cancel Help

Step 12. At the 'IPS Policies Wizard' screen, in the 'Signature File' section, select the first radio button "Specify the signature file you want to use with IOS IPS", then click the "..." button to bring up a dialog box to specify the location of the signature package file, which will be the directory specified in Step 6. In this example, we use tftp to download the signature package to the router.



Specify Signature File

☐ Specify signature file on flash

File Name on flash:

☒ Specify signature file using URL

Protocol:

tftp://

Example: http://10.10.10.1/IOS-S259-CLI.pkg

☐ Specify signature file on the PC

Location: Browse...

OK Cancel Help

Step 13. In the 'Configure Public Key' section, enter 'realm-cisco.pub' in the 'Name' text field, then copy and paste the following public key's key-string in the 'Key' text field. This public key can be download from

Cisco.com at: <http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup>. Click 'Next' to continue.

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```

IPS Policies Wizard

IPS Wizard

Signature File and Public Key

Signature File

☒ Specify the signature file you want to use with IOS IPS.

Signature File:

☐ Get the latest signature file from Cisco.com and save to PC.

Location:

Configure Public Key

Name:

Key:

< Back Next > Finish Cancel Help

QUESTION NO: 39

Which statement is a benefit of using Cisco IOS IPS?

- A.** It uses the underlying routing infrastructure to provide an additional layer of security.
- B.** It works in passive mode so as not to impact traffic flow.
- C.** It supports the complete signature database as a Cisco IPS sensor appliance.
- D.** The signature database is tied closely with the Cisco IOS image.

Answer: A

Explanation:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/product_data_sheet0900aecd803137cf.html

Product Overview

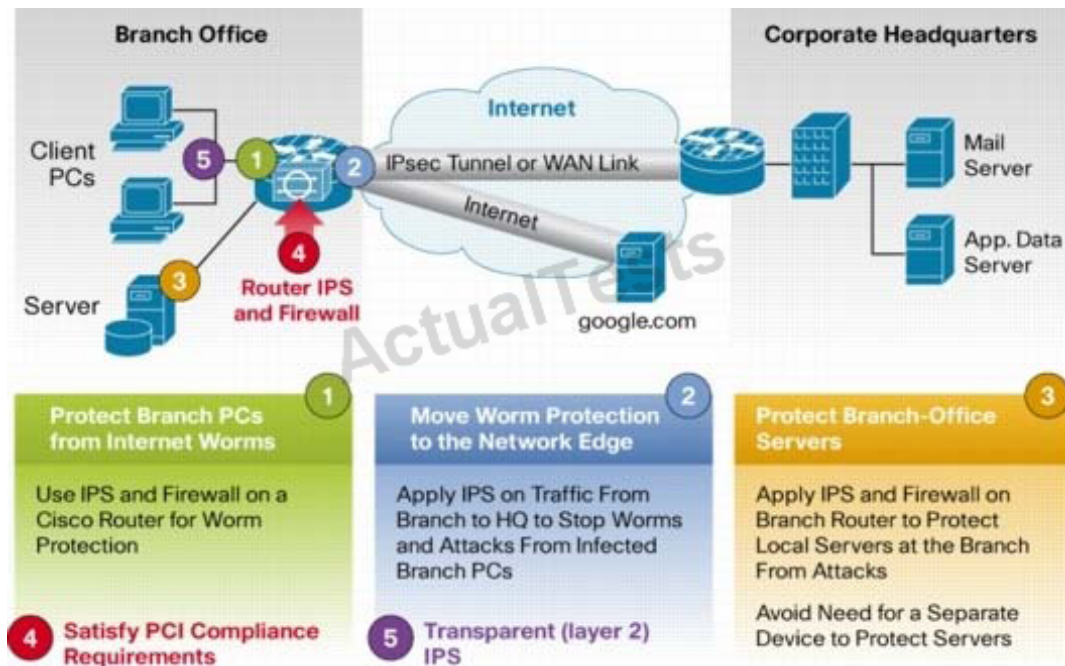
In today's business environment, network intruders and attackers can come from outside or inside the network.

They can launch distributed denial-of-service attacks, they can attack Internet connections, and they can exploit network and host vulnerabilities. At the same time, Internet worms and viruses can spread across the world in a matter of minutes. There is often no time to wait for human intervention-the network itself must possess the intelligence to recognize and mitigate these attacks, threats, exploits, worms and viruses.

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based solution that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, distributing the network level defense to stop malicious traffic close to its entry point at branch or telecommuter offices is also critical.

Cisco IOS IPS: Major Use Cases and Key Benefits

IOS IPS helps to protect your network in 5 ways:



Key Benefits

- Provides network-wide, distributed protection from many attacks, exploits, worms and viruses exploiting vulnerabilities in operating systems and applications
- Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as small and medium-sized business networks
- Unique, risk rating based signature event action processor dramatically improves the ease of management of

IPS policies

- Offers field-customizable worm and attack signature set and event actions
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router
- Supports more than 3700 signatures from the same signature database available for Cisco Intrusion Prevention System (IPS) appliances

QUESTION NO: 40

You are the security administrator for a large enterprise network with many remote locations. You have been given the assignment to deploy a Cisco IPS solution.

Where in the network would be the best place to deploy Cisco IOS IPS?

- A. Inside the firewall of the corporate headquarters Internet connection
- B. At the entry point into the data center
- C. Outside the firewall of the corporate headquarters Internet connection
- D. At remote branch offices

Answer: D

Explanation:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/product_data_sheet0900aecd803137cf.html

Product Overview

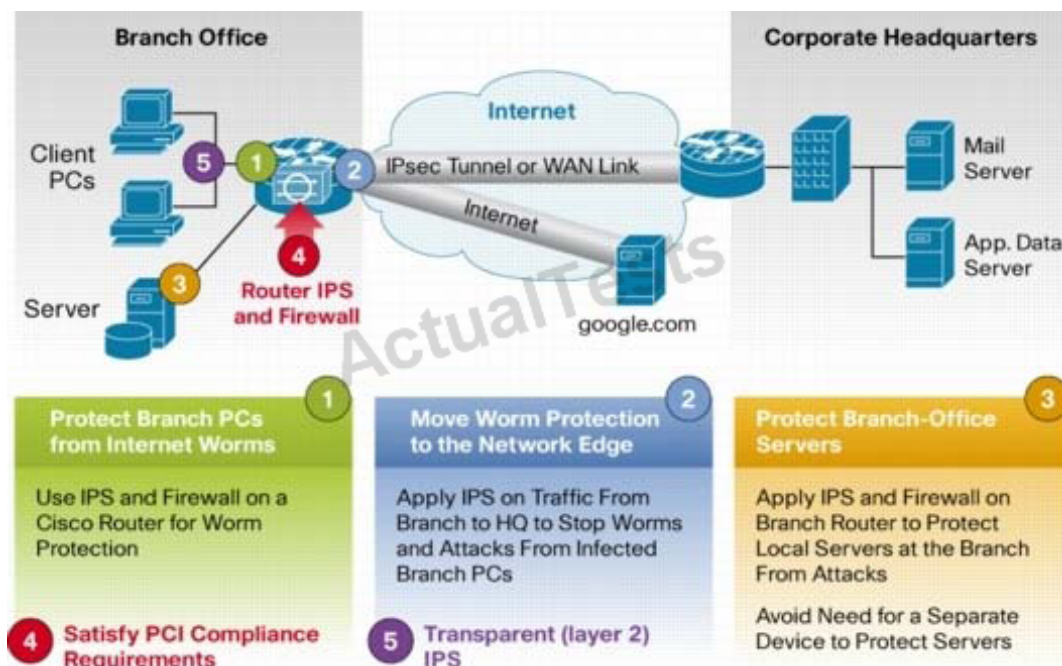
In today's business environment, network intruders and attackers can come from outside or inside the network.

They can launch distributed denial-of-service attacks, they can attack Internet connections, and they can exploit network and host vulnerabilities. At the same time, Internet worms and viruses can spread across the world in a matter of minutes. There is often no time to wait for human intervention-the network itself must possess the intelligence to recognize and mitigate these attacks, threats, exploits, worms and viruses.

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based solution that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, distributing the network level defense to stop malicious traffic close to its entry point at branch or telecommuter offices is also critical.

Cisco IOS IPS: Major Use Cases and Key Benefits

IOS IPS helps to protect your network in 5 ways:



Key Benefits

- Provides network-wide, distributed protection from many attacks, exploits, worms and viruses exploiting vulnerabilities in operating systems and applications
- Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as small and medium-sized business networks
- Unique, risk rating based signature event action processor dramatically improves the ease of management of IPS policies
- Offers field-customizable worm and attack signature set and event actions
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router
- Supports more than 3700 signatures from the same signature database available for Cisco Intrusion Prevention System (IPS) appliances

QUESTION NO: 41

Which IPS technique commonly is used to improve accuracy and context awareness, aiming to detect and respond to relevant incidents only and therefore, reduce noise?

- A. Attack relevancy
- B. Target asset value
- C. Signature accuracy
- D. Risk rating

Answer: D

Explanation:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd806e7299.html

Risk Rating Calculation

Risk rating is a quantitative measure of your network's threat level before IPS mitigation. For each event fired by IPS signatures, Cisco IPS Sensor Software calculates a risk rating number. The factors used to calculate risk rating are:

- Signature fidelity rating: This IPS-generated variable indicates the degree of attack certainty.
- Attack severity rating: This IPS-generated variable indicates the amount of damage an attack can cause.
- Target value rating: This user-defined variable indicates the criticality of the attack target. This is the only factor in risk rating that is routinely maintained by the user. You can assign a target value

rating per IP address in Cisco IPS Device Manager or Cisco Security Manager. The target value rating can raise or lower the overall risk rating for a network device. You can assign the following target values:

- 75: Low asset value
- 100: Medium asset value
- 200: Mission-critical asset value
- Attack relevancy rating: This IPS-generated value indicates the vulnerability of the attack target.
- Promiscuous delta. The risk rating of an IPS deployed in promiscuous mode is reduced by the promiscuous delta. This is because promiscuous sensing is less accurate than inline sensing. The promiscuous delta can be configured on a per-signature basis, with a value range of 0 to 30. (The promiscuous delta was introduced in Cisco IPS Sensor Software Version 6.0.)
- Watch list rating: This IPS-generated value is based on data found in the Cisco Security Agent watch list. The Cisco Security Agent watch list contains IP addresses of devices involved in network scans or possibly contaminated by viruses or worms. If an attacker is found on the watch list, the watch list rating for that attacker is added to the risk rating. The value for this factor is between 0 and 35. (The watch list rating was introduced in Cisco IPS Sensor Software Version 6.0.) Risk rating can help enhance your productivity as it intelligently assesses the level of risk of each event and helps you focus on high-risk events.

QUESTION NO: 42

Which two statements about SSL-based VPNs are true? (Choose two.)

- A. Asymmetric algorithms are used for authentication and key exchange.
- B. SSL VPNs and IPsec VPNs cannot be configured concurrently on the same router.
- C. The application programming interface can be used to modify extensively the SSL client software for use in special applications.
- D. The authentication process uses hashing technologies.
- E. Both client and clientless SSL VPNs require special-purpose client software to be installed on the client machine.

Answer: A,D

Explanation:

http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/25/software/user/guide/IKE.html

Add or Edit IKE Policy

Priority

An integer value that specifies the priority of this policy relative to the other configured IKE

policies. Assign the lowest numbers to the IKE policies that you prefer that the router use. The router will offer those policies first during negotiations.

Encryption

The type of encryption that should be used to communicate this IKE policy. Cisco SDM supports a variety of encryption types, listed in order of security. The more secure an encryption type, the more processing time it requires.

Note If your router does not support an encryption type, the type will not appear in the list.

Cisco SDM supports the following types of encryption:

- Data Encryption Standard (DES)—This form of encryption supports 56-bit encryption.
- Triple Data Encryption Standard (3DES)—This is a stronger form of encryption than DES, supporting 168-bit encryption.
- AES-128—Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than triple DES.
- AES-192—Advanced Encryption Standard (AES) encryption with a 192-bit key.
- AES-256—Advanced Encryption Standard (AES) encryption with a 256-bit key.

Hash

The authentication algorithm to be used for the negotiation. There are two options:

- Secure Hash Algorithm (SHA)
- Message Digest 5 (MD5)

Authentication

The authentication method to be used.

- Pre-SHARE. Authentication will be performed using pre-shared keys.
- RSA_SIG. Authentication will be performed using digital signatures.

D-H Group

Diffie-Hellman (D-H) Group. Diffie-Hellman is a public-key cryptography protocol that allows two routers to establish a shared secret over an unsecure communications channel. The options are as follows:

- group1—768-bit D-H Group. D-H Group 1.
- group2—1024-bit D-H Group. D-H Group 2. This group provides more security than group 1, but requires more processing time.
- group5—1536-bit D-H Group. D-H Group 5. This group provides more security than group 2, but requires more processing time.

Note•If your router does not support group5, it will not appear in the list.

- Easy VPN servers do not support D-H Group 1.

Lifetime This is the lifetime of the security association, in hours, minutes and seconds. The default is one day, or 24:00:00.

QUESTION NO: 43

Which option describes the purpose of Diffie-Hellman?

- A. used between the initiator and the responder to establish a basic security policy
- B. used to verify the identity of the peer
- C. used for asymmetric public key encryption
- D. used to establish a symmetric shared key via a public key exchange process

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/25/software/user/guide/IKE.html

D-H Group

Diffie-Hellman (D-H) Group. Diffie-Hellman is a public-key cryptography protocol that allows two routers to establish a shared secret over an unsecure communications channel. The options are as follows:

- group1—768-bit D-H Group. D-H Group 1.
- group2—1024-bit D-H Group. D-H Group 2. This group provides more security than group 1, but requires more processing time.
- group5—1536-bit D-H Group. D-H Group 5. This group provides more security than group 2, but requires more processing time.

Note•If your router does not support group5, it will not appear in the list.

- Easy VPN servers do not support D-H Group 1.

QUESTION NO: 44

Which three statements about the IPsec ESP modes of operation are true? (Choose three.)

- A. Tunnel mode is used between a host and a security gateway.
- B. Tunnel mode is used between two security gateways.
- C. Tunnel mode only encrypts and authenticates the data.
- D. Transport mode authenticates the IP header.
- E. Transport mode leaves the original IP header in the clear.

Answer: A,B,E

Explanation:

http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/2.0/ip_security/provisioning/guide/IPsecPG1.html

The Encapsulating Security Payload (ESP)

The Encapsulating Security Payload (ESP) contains six parts as described below. The first two parts are not encrypted, but they are authenticated. Those parts are as follows:

- The Security Parameter Index (SPI) is an arbitrary 32-bit number that tells the device receiving the packet what group of security protocols the sender is using for communication. Those protocols include the particular algorithms and keys, and how long those keys are valid.
- The Sequence Number is a counter that is incremented by 1 each time a packet is sent to the same address and uses the same SPI. The sequence number indicates which packet is which, and how many packets have been sent with the same group of parameters. The sequence number also protects against replay attacks.

Replay attacks involve an attacker who copies a packet and sends it out of sequence to confuse communicating devices.

The remaining four parts of the ESP are all encrypted during transmission across the network. Those parts are as follows:

- The Payload Data is the actual data that is carried by the packet.
- The Padding, from 0 to 255 bytes of data, allows certain types of encryption algorithms to require the data to be a multiple of a certain number of bytes. The padding also ensures that the text of a message terminates on a four-byte boundary (an architectural requirement within IP).
- The Pad Length field specifies how much of the payload is padding rather than data.
- The Next Header field, like a standard IP Next Header field, identifies the type of data carried and the protocol.

The ESP is added after a standard IP header. Because the packet has a standard IP header, the network can route it with standard IP devices. As a result, IPsec is backwards-compatible with IP routers and other equipment even if that equipment isn't designed to use IPsec. ESP can support any number of encryption protocols. It's up to the user to decide which ones to use. Different protocols can be used for every person a user communicates with. However, IPsec specifies a basic DES-Cipher Block Chaining mode (CBC) cipher as the default to ensure minimal interoperability among IPsec networks. ESP's encryption capability is designed for symmetric encryption algorithms. IPsec employs asymmetric algorithms for such specialized purposes as negotiating keys for symmetric encryption.

Tunneling with ESP

Tunneling takes an original IP packet header and encapsulates it within the ESP. Then, it adds a new IP header containing the address of a gateway device to the packet. Tunneling allows a user to send illegal IP addresses through a public network (like the Internet) that otherwise would not accept them. Tunneling with ESP offers the advantage of hiding original source and destination addresses from users on the public network. Hiding these addresses reduces the power of traffic analysis attacks. A traffic analysis attack employs network monitoring techniques to determine

how much data and what type of data is being communicated between two users.

QUESTION NO: 45

When configuring SSL VPN on the Cisco ASA appliance, which configuration step is required only for Cisco AnyConnect full tunnel SSL VPN access and not required for clientless SSL VPN?

- A. user authentication
- B. group policy
- C. IP address pool
- D. SSL VPN interface
- E. connection profile

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_sslvpn/configuration/15-2mt/sec-conn-sslvpnssl-vpn.html

Cisco AnyConnect VPN Client Full Tunnel Support

Remote Client Software from the SSL VPN Gateway

Address Pool

Manual Entry to the IP Forwarding Table

Remote Client Software from the SSL VPN Gateway

The Cisco AnyConnect VPN Client software package is pushed from the SSL VPN gateway to remote clients when support is needed. The remote user (PC or device) must have either the Java Runtime Environment for Windows (version 1.4 later), or the browser must support or be configured to permit Active X controls. In either scenario, the remote user must have local administrative privileges.

Address Pool

The address pool is first defined with the `ip local pool` command in global configuration mode. The standard configuration assumes that the IP addresses in the pool are reachable from a directly connected network.

Address Pools for Nondirectly Connected Networks

If you need to configure an address pool for IP addresses from a network that is not directly connected, perform the following steps:

Create a local loopback interface and configure it with an IP address and subnet mask from the address pool.

Configure the address pool with the ip local pool command. The range of addresses must fall under the subnet mask configured in Step 1.

Set up the route. If you are using the Routing Information Protocol (RIP), configure the router rip command and then the network command, as usual, to specify a list of networks for the RIP process. If you are using the Open Shortest Path First (OSPF) protocol, configure the ip ospf network point-to-point command in the loopback interface. As a third choice (instead of using the RIP or OSPF protocol), you can set up static routes to the network.

Configure the svc address-pool command with the name configured in Step 2.

Manual Entry to the IP Forwarding Table

If the SSL VPN software client is unable to update the IP forwarding table on the PC of the remote user, the following error message will be displayed in the router console or syslog:

Error : SSL VPN client was unable to Modify the IP forwarding table

This error can occur if the remote client does not have a default route. You can work around this error by performing the following steps:

Open a command prompt (DOS shell) on the remote client.

Enter the route print command.

If a default route is not displayed in the output, enter the route command followed by the add and mask keywords. Include the default gateway IP address at the end of the route statement. See the following example:

```
C:\>route ADD 0.0.0.0 MASK 0.0.0.0 10.1.1.1
```

QUESTION NO: 46

For what purpose is the Cisco ASA appliance web launch SSL VPN feature used?

- A. to enable split tunneling when using clientless SSL VPN access
- B. to enable users to login to a web portal to download and launch the AnyConnect client
- C. to enable smart tunnel access for applications that are not web-based
- D. to optimize the SSL VPN connections using DTLS
- E. to enable single-sign-on so the SSL VPN users need only log in once

Answer: B

Explanation:

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/administration/guide/ac01intro.html

AnyConnect Standalone and WebLaunch Options

The user can use the AnyConnect Client in the following modes:

- Standalone mode—Lets the user establish a Cisco AnyConnect VPN client connection without the need to use a web browser. If you have permanently installed the AnyConnect client on the user's PC, the user can run in standalone mode. In standalone mode, a user opens the AnyConnect client just like any other application and enters the username and password credentials into the fields of the AnyConnect GUI. Depending on how you configure the system, the user might also be required to select a group. When the connection is established, the security appliance checks the version of the client on the user's PC and, if necessary, downloads the latest version.
- WebLaunch mode—Lets the user enter the URL of the security appliance in the Address or Location field of a browser using the https protocol. The user then enters the username and password information on a Logon screen and selects the group and clicks submit. If you have specified a banner, that information appears, and the user acknowledges the banner by clicking Continue.

The portal window appears. To start the AnyConnect client, the user clicks Start AnyConnect on the main pane. A series of documentary windows appears. When the Connection Established dialog box appears, the connection is working, and the user can proceed with online activities. Whether connecting via standalone mode or WebLaunch mode, the AnyConnect client package must be installed on the security appliance in order for the client to connect. This ensures that the security appliance is the single point of enforcement as to which versions of the client can establish a session, even if you deploy the client with an enterprise software deployment system. When you load a client package on the security appliance, you enforce a policy that only versions as new as the one loaded can connect. AnyConnect users must upgrade their clients by loading the latest version of the client with the latest security features on the security appliance.

QUESTION NO: 47

Which statement describes how VPN traffic is encrypted to provide confidentiality when using asymmetric encryption?

- A.** The sender encrypts the data using the sender's private key, and the receiver decrypts the data using the sender's public key.
- B.** The sender encrypts the data using the sender's public key, and the receiver decrypts the data using the sender's private key.
- C.** The sender encrypts the data using the sender's public key, and the receiver decrypts the data using the receiver's public key.
- D.** The sender encrypts the data using the receiver's private key, and the receiver decrypts the

data using the receiver's public key.

E. The sender encrypts the data using the receiver's public key, and the receiver decrypts the data using the receiver's private key.

F. The sender encrypts the data using the receiver's private key, and the receiver decrypts the data using the sender's public key.

Answer: E

Explanation:

http://www.cisco.com/en/US/tech/tk1132/technologies_white_paper09186a00800e79cb.shtml

Public-Key Cryptography and Asymmetric Encryption

In asymmetric encryption, two different keys are used to render data illegible to anyone who may be eavesdropping on a conversation. The certificates contain the two components of asymmetric encryption:

public key and private key.

Data that is encrypted with the public key can be decrypted with the private key, and vice versa. However, data encrypted with the public key cannot be decrypted with the public key. The parties who need to encrypt their communications will exchange their public keys (contained in the certificate), but will not disclose their private keys. The sending party will use the public key of the receiving party to encrypt message data and forward the ciphertext (encrypted data) to the other party. The receiving party will then decrypt the ciphertext with their private key.

Data encrypted with the public key cannot be decrypted with the public key. This prevents someone from compromising the ciphertext after acquiring both public keys by eavesdropping on the certificate exchange.

QUESTION NO: 48

Which four types of VPN are supported using Cisco ISRs and Cisco ASA appliances? (Choose four.)

- A.** SSL clientless remote-access VPNs
- B.** SSL full-tunnel client remote-access VPNs
- C.** SSL site-to-site VPNs
- D.** IPsec site-to-site VPNs
- E.** IPsec client remote-access VPNs
- F.** IPsec clientless remote-access VPNs

Answer: A,B,D,E

Explanation:

https://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/ravpnbas.pdf

SSL VPN Access Modes

SSL VPN provides three modes of remote access on IOS routers: Clientless, Thin Client and Full Client. On ASA devices, there are two modes: Clientless (which includes Clientless and Thin Client port forwarding) and AnyConnect Client (a full client).

Clientless Access Mode

In Clientless mode, the remote user accesses the internal or corporate network using a Web browser on the client machine. No applet downloading is required. Clientless mode is useful for accessing most content that you would expect in a Web browser, such as Internet access, databases, and online tools that employ a Web interface. It supports Web browsing (using HTTP and HTTPS), file sharing using Common Internet File System (CIFS), and Outlook Web Access (OWA) email. For Clientless mode to work successfully, the remote user's PC must be running Windows 2000, Windows XP, or Linux operating systems. Browser-based SSL VPN users connecting from Windows operating systems can browse shared file systems and perform the following operations: view folders, view folder and file properties, create, move, copy, copy from the local host to the remote host, copy from the remote host to the local host, and delete. Internet Explorer indicates when a Web folder is accessible. Accessing this folder launches another window, providing a view of the shared folder, on which users can perform web folder functions, assuming the properties of the folders and documents permit them.

Thin Client Access Mode

Thin Client mode, also called TCP port forwarding, assumes that the client application uses TCP to connect to a well-known server and port. In this mode, the remote user downloads a Java applet by clicking the link provided on the portal page. The Java applet acts as a TCP proxy on the client machine for the services configured on the SSL VPN gateway. The Java applet starts a new SSL connection for every client connection. The Java applet initiates an HTTP request from the remote user client to the SSL VPN gateway. The name and port number of the internal email server is included in the HTTP request. The SSL VPN gateway creates a TCP connection to that internal email server and port. Thin Client mode extends the capability of the cryptographic functions of the Web browser to enable remote access to TCP-based applications such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, and Secure Shell (SSH).

Note

The TCP port-forwarding proxy works only with Sun's Java Runtime Environment (JRE) version 1.4 or later. A Java applet is loaded through the browser that verifies the JRE version. The Java applet refuses to run if a compatible JRE version is not detected. When using Thin Client mode, you should be aware of the following:

- The remote user must allow the Java applet to download and install.
- For TCP port-forwarding applications to work seamlessly, administrative privileges must be enabled for remote users.
- You cannot use Thin Client mode for applications such as FTP, where the ports are negotiated dynamically.

That is, you can use TCP port forwarding only with static ports.

Full Tunnel Client Access Mode

Full Tunnel Client mode enables access to the corporate network completely over an SSL VPN tunnel, which is used to move data at the network (IP) layer. This mode supports most IP-based applications, such as Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail, and Telnet. Being part of the SSL VPN is completely transparent to the applications run on the client. A Java applet is downloaded to handle the tunneling between the client host and the SSL VPN gateway. The user can use any application as if the client host was in the internal network.

The tunnel connection is determined by the group policy configuration. The SSL VPN client (SVC) or AnyConnect client is downloaded and installed to the remote client, and the tunnel connection is established when the remote user logs in to the SSL VPN gateway. By default, the client software is removed from the remote client after the connection is closed, but you can keep it installed, if required. [https://learningnetwork.cisco.com/servlet/JiveServlet/downloadBody/12870-102-1-48375/Cisco%20VPN%20\(5\).pdf](https://learningnetwork.cisco.com/servlet/JiveServlet/downloadBody/12870-102-1-48375/Cisco%20VPN%20(5).pdf)

LAN-to-LAN IPsec Implementations

LAN-to-LAN IPsec is a term often used to describe an IPsec tunnel created between two LANs. These are also called site to site IPsec VPNs. LAN-to-LAN VPNs are created when two private networks are merged across a public network such that the users on either of these networks can access resources on the other network as if they were on their own private network.

Remote-Access Client IPsec Implementations

Remote-access client IPsec VPNs are created when a remote user connects to an IPsec router or access server using an IPsec client installed on the remote user's machine. Generally, these remote-access machines connect to the public network or the Internet using dialup or some other similar means of connectivity. As soon as basic connectivity to the Internet is established, the IPsec client can set up an encrypted tunnel across the public network or the Internet to an IPsec termination device located at the edge of the private network to which the client wants to connect and be a part of. These IPsec termination devices are also known as IPsec remoteaccess concentrators.

QUESTION NO: 49

Which description of the Diffie-Hellman protocol is true?

- A.** It uses symmetrical encryption to provide data confidentiality over an unsecured communications channel.
- B.** It uses asymmetrical encryption to provide authentication over an unsecured communications channel.
- C.** It is used within the IKE Phase 1 exchange to provide peer authentication.
- D.** It provides a way for two peers to establish a shared-secret key, which only they will know, even though they are communicating over an unsecured channel.
- E.** It is a data integrity algorithm that is used within the IKE exchanges to guarantee the integrity of the message of the IKE exchanges.

Answer: D

Explanation:

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

Modulus Group

The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are:

- 1—Diffie-Hellman Group 1 (768-bit modulus).
- 2—Diffie-Hellman Group 2 (1024-bit modulus).
- 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group.
- 7—Diffie-Hellman Group 7 (163-bit elliptical curve field size).
- 14—Diffie-Hellman Group 14 (2048-bit modulus, considered good protection for 128-bit keys).
- 15—Diffie-Hellman Group 15 (3072-bit modulus, considered good protection for 192-bit keys).
- 16—Diffie-Hellman Group 16 (4096-bit modulus, considered good protection for 256-bit keys).

QUESTION NO: 50

Which IPsec transform set provides the strongest protection?

- A.** crypto ipsec transform-set 1 esp-3des esp-sha-hmac
- B.** crypto ipsec transform-set 2 esp-3des esp-md5-hmac
- C.** crypto ipsec transform-set 3 esp-aes 256 esp-sha-hmac
- D.** crypto ipsec transform-set 4 esp-aes esp-md5-hmac
- E.** crypto ipsec transform-set 5 esp-des esp-sha-hmac

F. crypto ipsec transform-set 6 esp-des esp-md5-hmac**Answer: C****Explanation:**

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

Table 22-2 IKEv2 Proposal Dialog Box

Name The name of the policy object. A maximum of 128 characters is allowed.

Description A description of the policy object. A maximum of 1024 characters is allowed.

Priority The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number.

Valid values range from 1 to 65535. The lower the number, the higher the priority. If you leave this field blank,

Security Manager assigns the lowest unassigned value starting with 1, then 5, then continuing in increments of 5.

Encryption Algorithm

The encryption algorithm used to establish the Phase 1 SA for protecting Phase 2 negotiations.

Click **Select** and select all of the algorithms that you want to allow in the VPN:

- AES—Encrypts according to the Advanced Encryption Standard using 128-bit keys.
- AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys.
- AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys.
- DES—Encrypts according to the Data Encryption Standard using 56-bit keys.
- 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
- Null—No encryption algorithm.

Integrity (Hash) Algorithm

The integrity portion of the hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Click **Select** and select all of the algorithms that you want to allow in the VPN:

- SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5.
- MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.

Prf Algorithm The pseudo-random function (PRF) portion of the hash algorithm used in the IKE proposal. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Click **Select** and select all of the algorithms that you want to allow in the VPN:

- SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5.

•MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA. Modulus Group

The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Click Select and select all of the groups that you want to allow in the

VPN:

- 1—Diffie-Hellman Group 1 (768-bit modulus).
- 2—Diffie-Hellman Group 2 (1024-bit modulus). This is the minimum recommended setting.
- 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys). Select this option if you are using AES encryption.

Lifetime

The lifetime of the security association (SA), in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 120 to 2147483647 seconds. The default is 86400.

Category The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.

QUESTION NO: 51

Which two options are characteristics of the Cisco Configuration Professional Security Audit wizard? (Choose two.)

- A. displays a screen with fix-it check boxes to let you choose which potential security-related configuration changes to implement
- B. has two modes of operation: interactive and non-interactive
- C. automatically enables Cisco IOS firewall and Cisco IOS IPS to secure the router
- D. uses interactive dialogs and prompts to implement role-based CLI
- E. requires users to first identify which router interfaces connect to the inside network and which connect to the outside network

Answer: A,E

Explanation:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/v2_7/olh/ccp.pdf

Perform Security Audit

This option starts the Security Audit wizard. The Security Audit wizard tests your router configuration to determine if any potential security problems exist in the configuration, and then

presents you with a screen that lets you determine which of those security problems you want to fix. Once determined, the Security Audit wizard will make the necessary changes to the router configuration to fix those problems

To have Cisco CP perform a security audit and then fix the problems it has found:

Step 1

In the Feature bar, select Configure > Security > Security Audit.

Step 2

Click Perform Security Audit.

The Welcome page of the Security Audit wizard appears.

Step 3

Click Next>.

The Security Audit Interface Configuration page appears.

Step 4

The Security Audit wizard needs to know which of your router interfaces connect to your inside network and which connect outside of your network. For each interface listed, check either the Inside or Outside check box to indicate where the interface connects.

Step 5

Click Next> .

The Security Audit wizard tests your router configuration to determine which possible security problems may exist. A screen showing the progress of this action appears, listing all of the configuration options being tested for, and whether or not the current router configuration passes those tests. If you want to save this report to a file, click Save Report.

Step 6

Click Close.

The Security Audit Report Card screen appears, showing a list of possible security problems.

Step 7

Check the Fix it boxes next to any problems that you want Cisco Configuration Professional (Cisco CP) to fix.

For a description of the problem and a list of the Cisco IOS commands that will be added to your configuration, click the problem description to display a help page about that problem.

Step 8

Click Next>.

Step 9

The Security Audit wizard may display one or more screens requiring you to enter information to fix certain problems. Enter the information as required and click Next> for each of those screens.

Step 10

The Summary page of the wizard shows a list of all the configuration changes that Security Audit will make.

Click Finish to deliver those changes to your router.

QUESTION NO: 52

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.

Answer: B

Explanation:

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 NO: 53

Which aaa accounting command is used to enable logging of the start and stop records for user terminal sessions on the router?

- A. aaa accounting network start-stop tacacs+
- B. aaa accounting system start-stop tacacs+
- C. aaa accounting exec start-stop tacacs+
- D. aaa accounting connection start-stop tacacs+
- E. aaa accounting commands 15 start-stop tacacs+

Answer: C

Explanation:

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

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the aaa accounting command in global configuration mode or template configuration mode. To disable AAA accounting, use the no form of this command.

aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default | list-name | guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name}

no aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default | listname | guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name} exec

Runs accounting for the EXEC shell session.

start-stop

Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.

QUESTION NO: 54

Which access list permits HTTP traffic sourced from host 10.1.129.100 port 3030 destined to host 192.168.1.10?

- A. access-list 101 permit tcp any eq 3030
- B. access-list 101 permit tcp 10.1.128.0 0.0.1 .255 eq 3030 192.1 68.1 .0 0.0.0.15 eq www
- C. access-list 101 permit tcp 10.1.129.0 0.0.0.255 eq www 192.168.1.10 0.0.0.0 eq www
- D. access-list 101 permit tcp host 192.1 68.1 .10 eq 80 10.1.0.0 0.0.255.255 eq 3030
- E. access-list 101 permit tcp 192.168.1.10 0.0.0.0 eq 80 10.1.0.0 0.0.255.255
- F. access-list 101 permit ip host 10.1.129.100 eq 3030 host 192.168.1.10 eq 80

Answer: B

Explanation:

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]

QUESTION NO: 55

Which location is recommended for extended or extended named ACLs?

- A. an intermediate location to filter as much traffic as possible
- B. a location as close to the destination traffic as possible
- C. when using the established keyword, a location close to the destination point to ensure that return traffic is allowed
- D. a location as close to the source traffic as possible

Answer: D

Explanation:

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

Apply ACLs

You can define ACLs without applying them. But, the ACLs have no effect until they are applied to the interface of the router. It is a good practice to apply the ACL on the interface closest to the source of the traffic.

QUESTION NO: 56

Which statement about asymmetric encryption algorithms is true?

- A. They use the same key for encryption and decryption of data.
- B. They use the same key for decryption but different keys for encryption of data.

- C. They use different keys for encryption and decryption of data.
- D. They use different keys for decryption but the same key for encryption of data.

Answer: C

Explanation:

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_12-4/124_ssh.html

Transport Layer Protocol

Server authentication occurs at the transport layer, based on the server possessing a public-private key pair. A server may have multiple host keys using multiple different asymmetric encryption algorithms. Multiple hosts may share the same host key. In any case, the server host key is used during key exchange to authenticate the identity of the host. For this authentication to be possible, the client must have presumptive knowledge of the server public host key. RFC 4251 dictates two alternative trust models that can be used:

The client has a local database that associates each host name (as typed by the user) with the corresponding public host key. This method requires no centrally administered infrastructure and no third-party coordination.

The downside is that the database of name-to-key associations may become burdensome to maintain.

The host name-to-key association is certified by a trusted Certification Authority (CA). The client knows only the CA root key and can verify the validity of all host keys certified by accepted CAs. This alternative eases the maintenance problem, because ideally only a single CA key needs to be securely stored on the client. On the other hand, each host key must be appropriately certified by a central authority before authorization is possible.

QUESTION NO: 57

Which option can be used to authenticate the IPsec peers during IKE Phase 1?

- A. Diffie-Hellman Nonce
- B. pre-shared key
- C. XAUTH
- D. integrity check value
- E. ACS
- F. AH

Answer: B

Explanation:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfike.html

Encryption algorithm

56-bit DES-CBC, des, Default 56-bit DES-CBC

168-bit DES, 3des, Default 168-bit DES

Hash algorithm

SHA-1 (HMAC variant), sha, Default SHA-1

MD5 (HMAC variant), md5

Authentication method

RSA signatures, rsa-sig, Default RSA signatures

RSA encrypted nonces, rsa-encr

preshared keys, pre-share

Diffie-Hellman group identifier

768-bit Diffie-Hellman, 1, Default 768-bit Diffie-Hellman

1024-bit Diffie-Hellman, 2 Lifetime of the security association

Any number of seconds, Default 86400 seconds (one day)

QUESTION NO: 58

Which single Cisco IOS ACL entry permits IP addresses from 172.16.80.0 to 172.16.87.255?

- A. permit 172.16.80.0 0.0.3.255
- B. permit 172.16.80.0 0.0.7.255
- C. permit 172.16.80.0 0.0.248.255
- D. permit 176.16.80.0 255.255.252.0
- E. permit 172.16.80.0 255.255.248.0
- F. permit 172.16.80.0 255.255.240.0

Answer: B

Explanation:

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

ACL Summarization

NotE. Subnet masks can also be represented as a fixed length notation. For example, 192.168.10.0/24

represents 192.168.10.0 255.255.255.0.

This list describes how to summarize a range of networks into a single network for ACL optimization. Consider

these networks.

192.168.32.0/24

192.168.33.0/24

192.168.34.0/24

192.168.35.0/24

192.168.36.0/24

192.168.37.0/24

192.168.38.0/24

192.168.39.0/24

The first two octets and the last octet are the same for each network. This table is an explanation of how to summarize these into a single network.

The third octet for the previous networks can be written as seen in this table, according to the octet bit position and address value for each bit.

Decimal 128 64 32 16 8 4 2 1

32 0 0 1 0 0 0 0

33 0 0 1 0 0 0 1

34 0 0 1 0 0 1 0

35 0 0 1 0 0 1 1

36 0 0 1 0 1 0 0

37 0 0 1 0 1 0 1

38 0 0 1 0 1 1 0

39 0 0 1 0 1 1 1

M M M M M D D D

Since the first five bits match, the previous eight networks can be summarized into one network (192.168.32.0/21 or 192.168.32.0 255.255.248.0). All eight possible combinations of the three low-order bits are relevant for the network ranges in question. This command defines an ACL that permits this network. If you subtract 255.255.248.0 (normal mask) from 255.255.255.255, it yields 0.0.7.255.

```
access-list acl_permit permit ip 192.168.32.0 0.0.7.255
```

QUESTION NO: 59

You want to use the Cisco Configuration Professional site-to-site VPN wizard to implement a site-to-site IPsec VPN using pre-shared key.

Which four configurations are required (with no defaults)? (Choose four.)

- A. the interface for the VPN connection
- B. the VPN peer IP address
- C. the IPsec transform-set
- D. the IKE policy
- E. the interesting traffic (the traffic to be protected)
- F. the pre-shared key

Answer: A,B,E,F

Explanation:

http://www.cisco.com/en/US/products/ps9422/products_configuration_example09186a0080ba1d0a.shtml

3. In the next window, provide the VPN Connection Information in the respective spaces. Choose the interface of the VPN Tunnel from the drop-down menu. Here, FastEthernet0 is chosen. In the Peer Identity section, choose Peer with static IP address and provide the remote peer IP address. Then, provide the Pre-shared Keys (cisco123 in this example) in the Authentication section. Lastly, click Next.

Site-to-Site VPN Wizard

VPN Wizard

VPN Connection Information

Select the interface for this VPN connection: FastEthernet0/0 Details...

Peer Identity

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer: 172.17.1.1

Authentication

Authentication ensures that each end of the VPN connection uses the same secret key.

☒ Pre-shared Keys ☐ Digital Certificates

pre-shared key: cisco123

Re-enter Key: cisco123

< Back Next > Finish Cancel Help

10. In the following window, provide the details about the Traffic to be protected through the VPN Tunnel.

Provide the Source and Destination Networks of the traffic to be protected so that the traffic between the specified source and destination networks are protected. In this example, the Source network is 10.10.10.0 and the Destination network is 10.20.10.0. Click Next.

Site-to-Site VPN Wizard

VPN Wizard

Traffic to protect
IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected.

☒ Protect all traffic between the following subnets

Local Network	Remote Network
Enter the IP address and subnet mask of the network where IPSec traffic originates.	Enter the IP Address and Subnet Mask of the destination Network.
IP Address: 10.10.10.0	IP Address: 10.20.10.0
Subnet Mask: 255.255.255.0 or 24	Subnet Mask: 255.255.255.0 or 24

☐ Create/Select an access-list for IPSec traffic

< Back **Next >** Finish Cancel Help

QUESTION NO: 60

Which two options represent a threat to the physical installation of an enterprise network? (Choose two.)

- A. surveillance camera
- B. security guards
- C. electrical power
- D. computer room access
- E. change control

Answer: C,D

Explanation:

http://www.cisco.com/E-Learning/bulk/public/celc/CRS/media/targets/1_3_1.swf

QUESTION NO: 61

Which option represents a step that should be taken when a security policy is developed?

- A. Perform penetration testing.
- B. Determine device risk scores.
- C. Implement a security monitoring system.
- D. Perform quantitative risk analysis.

Answer: D

Explanation:

QUESTION NO: 62

Which type of network masking is used when Cisco IOS access control lists are configured?

- A. extended subnet masking
- B. standard subnet masking
- C. priority masking
- D. wildcard masking

Answer: D

Explanation:

http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014f945.shtml

Conduct a Risk Analysis

A risk analysis should identify the risks to your network, network resources, and data. This doesn't mean you should identify every possible entry point to the network, nor every possible means of attack. The intent of a risk analysis is to identify portions of your network, assign a threat rating to each portion, and apply an appropriate level of security. This helps maintain a workable balance between security and required network access.

Assign each network resource one of the following three risk levels:

Low Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.

Medium Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial

ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.

High Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Assign a risk level to each of the following: core network devices, distribution network devices, access network devices, network monitoring devices (SNMP monitors and RMON probes), network security devices (RADIUS and TACACS), e-mail systems, network file servers, network print servers, network application servers (DNS and DHCP), data application servers (Oracle or other standalone applications), desktop computers, and other devices (standalone print servers and network fax machines).

Network equipment such as switches, routers, DNS servers, and DHCP servers can allow further access into the network, and are therefore either medium or high risk devices. It is also possible that corruption of this equipment could cause the network itself to collapse. Such a failure can be extremely disruptive to the business.

QUESTION NO: 63

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.

Answer: D

Explanation:

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 NO: 64

Which type of management reporting is defined by separating management traffic from production traffic?

- A. IPsec encrypted
- B. in-band
- C. out-of-band
- D. SSH

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap9.html#wp1054536

OOB Management Best Practices

The OOB network segment hosts console servers, network management stations, AAA servers, analysis and correlation tools, NTP, FTP, syslog servers, network compliance management, and any other management and control services. A single OOB management network may serve all the enterprise network modules located at the headquarters. An OOB management network should be deployed using the following best practices:

- Provide network isolation
- Enforce access control
- Prevent data traffic from transiting the management network

QUESTION NO: 65

Which syslog level is associated with LOG_WARNING?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

- F. 6
- G. 7
- H. 0

Answer: D

Explanation:

Level Number	Severity Level	Description
0	emergencies	System is unusable.
1	alert	Immediate action is needed.
2	critical	Critical conditions.
3	error	Error conditions.
4	warning	Warning conditions.
5	notification	Normal but significant conditions.
6	informational	Informational messages only.
7	debugging	Debugging messages only.

QUESTION NO: 66

In which type of Layer 2 attack does an attacker broadcast BDPUs with a lower switch priority?

- A. MAC spoofing attack
- B. CAM overflow attack
- C. VLAN hopping attack
- D. STP attack

Answer: D

Explanation:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_605972.htm
|

Introduction

The purpose of this paper is to identify how easily the Spanning-Tree Protocol (STP) can be compromised to allow eavesdropping in a switched corporate environment and how to mitigate this vulnerability using L2 security features that are available on the Cisco® Catalyst® 6500.

The Spanning Tree Protocol (STP) Man in The Middle (MiTM) attack compromises the STP "Root

Bridge" election process and allows a hacker to use their PC to masquerade as a "Root Bridge," thus controlling the flow of L2 traffic. In order to understand the attack, the reader must have a basic understanding of the "Root Bridge" Election process and the initial STP operations that build the loop free topology. Therefore, the first section of this document, Overview of the STP Root Bridge Election Process, will be devoted to providing a simplified explanation of 802.1d STP operations as it pertains to understanding the STP MiTM attack. If you require a more comprehensive overview of STP, please review the LAN Switching Chapter of the Cisco Catalyst 6500 Configuration Guide on Cisco.com.

QUESTION NO: 67

Which security measure must you take for native VLANs on a trunk port?

- A. Native VLANs for trunk ports should never be used anywhere else on the switch.
- B. The native VLAN for trunk ports should be VLAN 1.
- C. Native VLANs for trunk ports should match access VLANs to ensure that cross-VLAN traffic from multiple switches can be delivered to physically disparate switches.
- D. Native VLANs for trunk ports should be tagged with 802.1Q.

Answer: A

Explanation:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

Double Encapsulation Attack

When double-encapsulated 802.1Q packets are injected into the network from a device whose VLAN happens to be the native VLAN of a trunk, the VLAN identification of those packets cannot be preserved from end to end since the 802.1Q trunk would always modify the packets by stripping their outer tag. After the external tag is removed, the internal tag permanently becomes the packet's only VLAN identifier. Therefore, by double encapsulating packets with two different tags, traffic can be made to hop across VLANs.

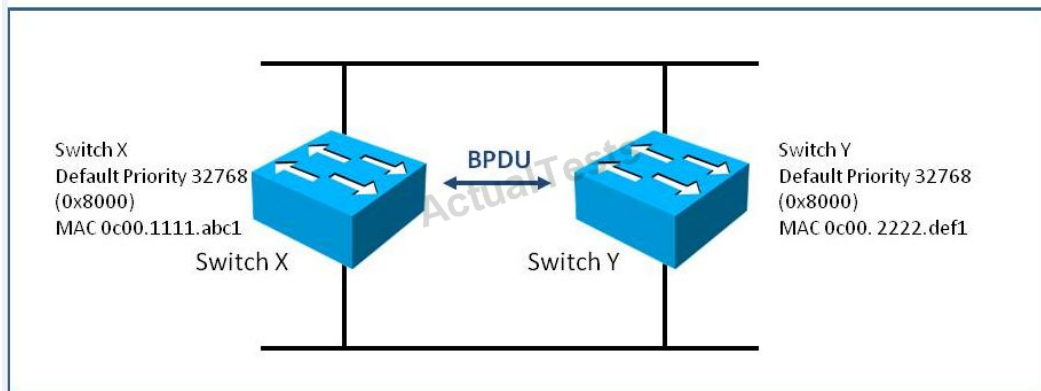
This scenario is to be considered a misconfiguration, since the 802.1Q standard does not necessarily force the users to use the native VLAN in these cases. As a matter of fact, the proper configuration that should always be used is to clear the native VLAN from all 802.1Q trunks (alternatively, setting them to 802.1q-all-tagged mode achieves the exact same result). In cases where the native VLAN cannot be cleared, then always pick an unused VLAN as native VLAN of all the trunks; don't use this VLAN for any other purpose.

Protocols like STP, DTP, and UDLD (check out [3]) should be the only rightful users of the native

VLAN and their traffic should be completely isolated from any data packets.

QUESTION NO: 68

Refer to the exhibit.



Which switch is designated as the root bridge in this topology?

- A. It depends on which switch came on line first.
- B. Neither switch would assume the role of root bridge because they have the same default priority.
- C. switch X
- D. switch Y

Answer: C

Explanation:

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

Rules of Operation

This section lists rules for how STP works. When the switches first come up, they start the root switch selection process. Each switch transmits a BPDU to the directly connected switch on a per-VLAN basis.

As the BPDU goes out through the network, each switch compares the BPDU that the switch sends to the BPDU that the switch receives from the neighbors. The switches then agree on which switch is the root switch. The switch with the lowest bridge ID in the network wins this election process.

QUESTION NO: 69

Which type of firewall technology is considered the versatile and commonly used firewall technology?

- A. static packet filter firewall
- B. application layer firewall
- C. stateful packet filter firewall
- D. proxy firewall
- E. adaptive layer firewall

Answer: C

Explanation:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/product_implementation_design_guide09186a00800fd670.html

Cisco IOS Firewall includes multiple security features:

- Cisco IOS Firewall stateful packet inspection provides true firewall capabilities to protect networks against unauthorized traffic and control legitimate business-critical data.
- Authentication proxy controls access to hosts or networks based on user credentials stored in an authentication, authorization, and accounting (AAA) server.
- Multi-VRF firewall offers firewall services on virtual routers with virtual routing and forwarding (VRF), accommodating overlapping address space to provide multiple isolated private route spaces with a full range of security services.
- Transparent firewall adds stateful inspection without time-consuming, disruptive IP addressing modifications.
- Application inspection controls application activity to provide granular policy enforcement of application usage, protecting legitimate application protocols from rogue applications and malicious activity.

QUESTION NO: 70

Which type of NAT is used where you translate multiple internal IP addresses to a single global, routable IP address?

- A. policy NAT
- B. dynamic PAT
- C. static NAT
- D. dynamic NAT
- E. policy PAT

Answer: B

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/nat_dynamic.html

Task Flow for Configuring Dynamic NAT and PAT

Use the following guidelines to configure either Dynamic NAT or PAT:

- First configure a nat command, identifying the real addresses on a given interface that you want to translate.
- Then configure a separate global command to specify the mapped addresses when exiting another interface.

(In the case of PAT, this is one address.) Each nat command matches a global command by comparing the NAT ID, a number that you assign to each command.

Note The configuration for dynamic NAT and PAT are almost identical; for NAT you specify a range of mapped addresses, and for PAT you specify a single address.

Figure 29-9 shows a typical dynamic NAT scenario. Only translated hosts can create a NAT session, and responding traffic is allowed back. The mapped address is dynamically assigned from a pool defined by the global command.

Figure 29.9 Dynamic NAT

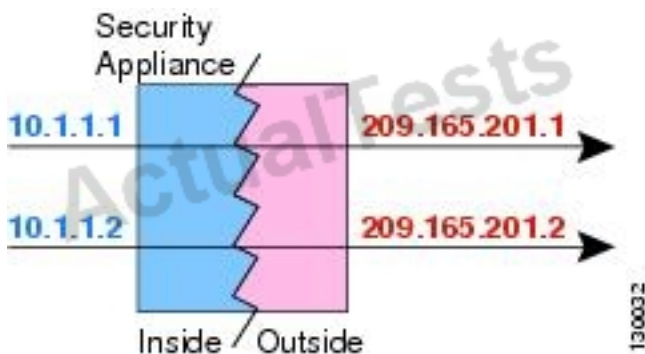


Figure 29-10 shows a typical dynamic PAT scenario. Only translated hosts can create a NAT session, and responding traffic is allowed back. The mapped address defined by the global command is the same for each translation, but the port is dynamically assigned.

Figure 29-10 Dynamic PAT



QUESTION NO: 71

Which Cisco IPS product offers an inline, deep-packet inspection feature that is available in integrated services routers?

- A. Cisco iSDM
- B. Cisco AIM
- C. Cisco IOS IPS
- D. Cisco AIP-SSM

Answer: C

Explanation:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/product_data_sheet0900aecd803137cf.html

Product Overview

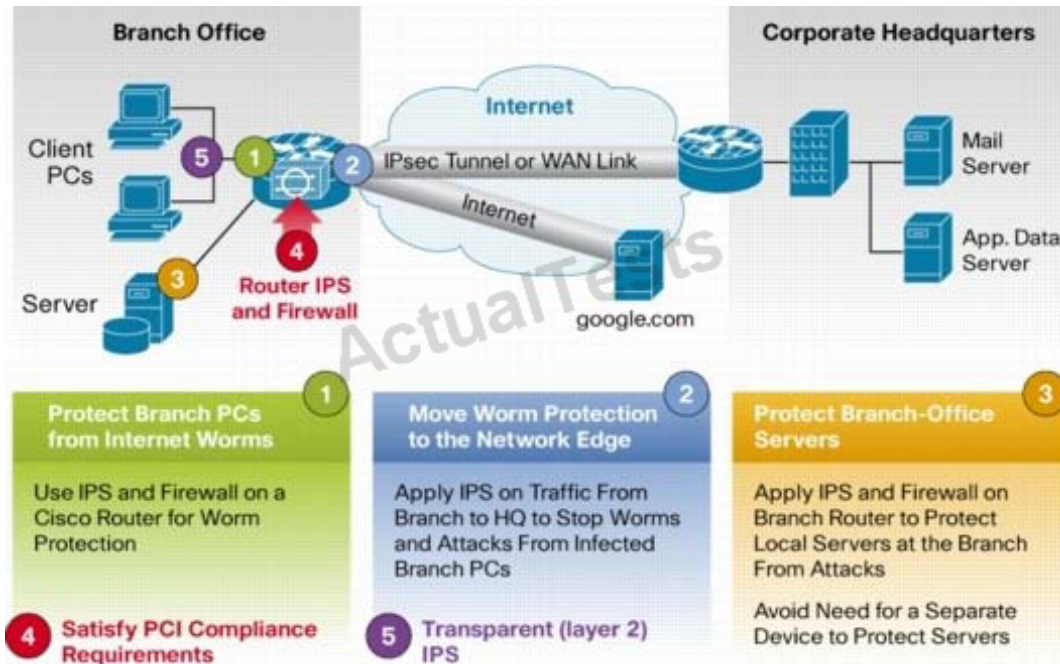
In today's business environment, network intruders and attackers can come from outside or inside the network.

They can launch distributed denial-of-service attacks, they can attack Internet connections, and they can exploit network and host vulnerabilities. At the same time, Internet worms and viruses can spread across the world in a matter of minutes. There is often no time to wait for human intervention-the network itself must possess the intelligence to recognize and mitigate these attacks, threats, exploits, worms and viruses.

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based solution that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, distributing the network level defense to stop malicious traffic close to its entry point at branch or telecommuter offices is also critical.

Cisco IOS IPS: Major Use Cases and Key Benefits

IOS IPS helps to protect your network in 5 ways:



Key Benefits

- Provides network-wide, distributed protection from many attacks, exploits, worms and viruses exploiting vulnerabilities in operating systems and applications
- Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as small and medium-sized business networks
- Unique, risk rating based signature event action processor dramatically improves the ease of management of IPS policies
- Offers field-customizable worm and attack signature set and event actions
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router
- Supports more than 3700 signatures from the same signature database available for Cisco Intrusion Prevention System (IPS) appliances

QUESTION NO: 72

Which three modes of access can be delivered by SSL VPN? (Choose three.)

- A. full tunnel client
- B. IPsec SSL
- C. TLS transport mode

- D. thin client
- E. clientless
- F. TLS tunnel mode

Answer: A,D,E

Explanation:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html

SSL VPN

The SSL VPN feature (also known as WebVPN) provides support, in Cisco IOS software, for remote user access to enterprise networks from anywhere on the Internet. Remote access is provided through a Secure Socket Layer- (SSL-) enabled SSL VPN gateway. The SSL VPN gateway allows remote users to establish a secure Virtual Private Network (VPN) tunnel using a web browser. This feature provides a comprehensive solution that allows easy access to a broad range of web resources and web-enabled applications using native HTTP over SSL (HTTPS) browser support. SSL VPN delivers three modes of SSL VPN access: clientless, thin-client, and full-tunnel client support.

QUESTION NO: 73

During role-based CLI configuration, what must be enabled before any user views can be created?

- A. multiple privilege levels
- B. usernames and passwords
- C. aaa new-model command
- D. secret password for the root user
- E. HTTP and/or HTTPS server
- F. TACACS server group

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html

Configuring a CLI View

Use this task to create a CLI view and add commands or interfaces to the view, as appropriate.

Prerequisites

Before you create a view, you must perform the following tasks:

- Enable AAA via the aaa new-model command. (For more information on enabling AAA, see the chapter

"Configuring Authentication" in the Cisco IOS Security Configuration Guide, Release 12.3.

- Ensure that your system is in root view—not privilege level 15.

SUMMARY STEPS

1. enable view
2. configure terminal
3. parser view view-name
4. secret 5 encrypted-password
5. commands parser-mode {include | include-exclusive | exclude} [all] [interface interface-name | command]
6. exit
7. exit
8. enable [privilege-level] [view view-name]
9. show parser view [all]

QUESTION NO: 74

Which three statements about applying access control lists to a Cisco router are true? (Choose three.)

- A.** Place more specific ACL entries at the top of the ACL.
- B.** Place generic ACL entries at the top of the ACL to filter general traffic and thereby reduce “noise” on the network.
- C.** ACLs always search for the most specific entry before taking any filtering action.
- D.** Router-generated packets cannot be filtered by ACLs on the router.
- E.** If an access list is applied but it is not configured, all traffic passes.

Answer: A,D,E

Explanation: 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 NO: 75

When port security is enabled on a Cisco Catalyst switch, what is the default action when the configured maximum number of allowed MAC addresses value is exceeded?

- A. The port remains enabled, but bandwidth is throttled until old MAC addresses are aged out.
- B. The port is shut down.
- C. The MAC address table is cleared and the new MAC address is entered into the table.
- D. The violation mode of the port is set to restrict.

Answer: B

Explanation:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/20ewa/configuration/guide/port_

sec.html

Default Port Security Configuration

Port security

Disabled on a port

Maximum number of secure MAC addresses

1

Violation mode Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.

Aging

Disabled

Aging type

Absolute

Static Aging

Disabled

Sticky

Disabled

QUESTION NO: 76

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.

Answer: A,B,D

Explanation:

<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 NO: 77

Refer to the exhibit.

```
access-list 102 permit tcp any 192.168.15.32 0.0.0.31 eq www
access-list 102 deny ip any 192.168.15.32 0.0.0.31
access-list 102 permit ip any any
```

```
Current configuration : 156 bytes
!
interface FastEthernet0
 ip address 192.168.32.13 255.255.255.0
 ip access-group IOS in
 ip flow ingress
 ip flow egress
 duplex auto
 speed auto
!
end

Router(config-ext-nacl)#do show access-l IOS
Extended IP access list IOS
 10 permit tcp host 10.1.1.1 eq 1030 host 192.168.15.80 eq telnet
 20 permit tcp host 10.1.1.1 eq 1030 host 192.168.15.66 eq 8080
 30 permit tcp host 10.1.1.1 eq 1030 host 192.168.15.36 eq www
 40 permit tcp host 10.1.1.1 eq 1030 host 192.168.15.63 eq www
Router(config-ext-nacl)#
```

This Cisco IOS access list has been configured on the FA0/0 interface in the inbound direction.

Which four TCP packets sourced from 10.1.1.1 port 1030 and routed to the FA0/0 interface are permitted? (Choose four.)

- A. destination ip address: 192.168.15.37 destination port: 22
- B. destination ip address: 192.168.15.80 destination port: 23
- C. destination ip address: 192.168.15.66 destination port: 8080
- D. destination ip address: 192.168.15.36 destination port: 80
- E. destination ip address: 192.168.15.63 destination port: 80
- F. destination ip address: 192.168.15.40 destination port: 21

Answer: B,C,D,E

Explanation:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml

Extended ACLs (registered customers only) control traffic by comparing the source and destination addresses of the IP packets to the addresses configured in the ACL. You can also make extended ACLs more granular and configured to filter traffic by criteria such as:

Protocol

Port numbers

Differentiated services code point (DSCP) value

Precedence value

State of the synchronize sequence number (SYN) bit

The command syntax formats of extended ACLs are:

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][fragments]

Internet Control Message Protocol (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]] [precedenceprecedence] [tos tos] [log |

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

Transport Control Protocol (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][fragments]

User Datagram Protocol (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][fragments]

QUESTION NO: 78

You use Cisco Configuration Professional to enable Cisco IOS IPS. Which state must a signature

be in before any actions can be taken when an attack matches that signature?

- A. Enabled
- B. Unretired
- C. Successfully complied
- D. Successfully complied and unretired
- E. Successfully complied and enabled
- F. Unretired and enabled
- G. Enabled, unretired, and successfully complied

Answer: G

Explanation:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8066d265.html

Step 21. Verify the signatures are loaded properly by using this command at the router prompt:

```
router#show ip ips signatures count
```

Cisco SDF release version S353.0

Trend SDF release version V0.0

|

snip

|

Total Signatures: 2363

Total Enabled Signatures: 1025

Total Retired Signatures: 1796

Total Compiled Signatures: 567

Total Obsolete Signatures: 15

Step 23. To retire/unretire and enable/disable signatures, select the Edit IPS tab, then select Signatures.

Highlight the signature(s), and then click the Enable, Disable, Retire, or Unretire button. Notice the status changed in the Enabled or the Retired column. A yellow icon appears for the signature(s) in the column next to Enabled. The yellow icon means changes have been made to the signature, but have not been applied. Click the Apply Changes button to make the changes take effect.

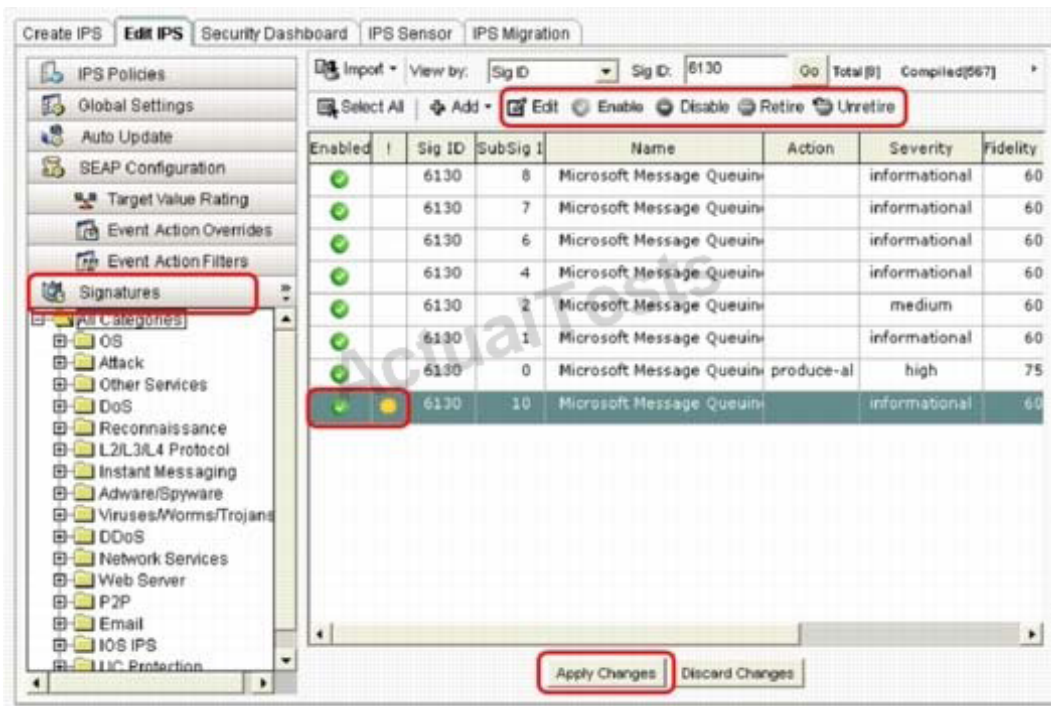
Retire/unretire is to select/de-select which signatures are being used by IOS IPS to scan traffic. Retiring a signature means IOS IPS will NOT compile that signature into memory for scanning. Unretiring a signature instructs IOS IPS to compile the signature into memory and use the signature to scan traffic.

Enable/disable does NOT select/de-select signatures to be used by IOS IPS.

Enabling a signature means that when triggered by a matching packet (or packet flow), the signature takes the appropriate action associated with it. However, only unretired AND

successfully compiled signatures will take the action when they are enabled. In other words, if a signature is retired, even though it is enabled, it will not be compiled (because it is retired) and it will not take the action associated with it.

Disabling a signature means that when triggered by a matching packet (or packet flow), the signature DOES NOT take the appropriate action associated with it. In other words, when a signature is disabled, even though it is unretired and successfully compiled, it will not take the action associated with it.



QUESTION NO: 79

Which statement describes how the sender of the message is verified when asymmetric encryption is used?

- A.** The sender encrypts the message using the sender's public key, and the receiver decrypts the message using the sender's private key.
- B.** The sender encrypts the message using the sender's private key, and the receiver decrypts the message using the sender's public key.
- C.** The sender encrypts the message using the receiver's public key, and the receiver decrypts the message using the receiver's private key.
- D.** The sender encrypts the message using the receiver's private key, and the receiver decrypts the message using the receiver's public key.

E. The sender encrypts the message using the receiver's public key, and the receiver decrypts the message using the sender's public key.

Answer: C

Explanation:

http://www.cisco.com/en/US/tech/tk1132/technologies_white_paper09186a00800e79cb.shtml

Public-Key Cryptography and Asymmetric Encryption

In asymmetric encryption, two different keys are used to render data illegible to anyone who may be eavesdropping on a conversation. The certificates contain the two components of asymmetric encryption: public key and private key.

Data that is encrypted with the public key can be decrypted with the private key, and vice versa. However, data encrypted with the public key cannot be decrypted with the public key. The parties who need to encrypt their communications will exchange their public keys (contained in the certificate), but will not disclose their private keys. The sending party will use the public key of the receiving party to encrypt message data and forward the cipher text (encrypted data) to the other party. The receiving party will then decrypt the cipher text with their private key.

Data encrypted with the public key cannot be decrypted with the public key. This prevents someone from compromising the cipher text after acquiring both public keys by eavesdropping on the certificate exchange.

QUESTION NO: 80

Refer to the exhibit.

```

router#show crypto isakmp policy
Protection suite of priority 1
  encryption algorithm: 3DES - Data Encryption Standard (168 bit keys).
  hash algorithm: Secure Hash Standard
  authentication method: preshared
  Diffie-Hellman group: #2 (1024 bit)
  lifetime: 86400 seconds, no volume limit
Protection suite of priority 2
  encryption algorithm: DES - Data Encryption Standard (56 bit keys).
  hash algorithm: Secure Hash Standard
  authentication method: preshared
  Diffie-Hellman group: #2 (1024 bit)
  lifetime: 86400 seconds, no volume limit
Default protection suite
  encryption algorithm: DES - Data Encryption Standard (56 bit keys).
  hash algorithm: Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman group: #1 (768 bit)
  lifetime: 86400 seconds, no volume limit

router#show crypto ipsec transform-set
Transform set mine: { esp-128-aes esp-sha-hmac } will negotiate = { Tunnel, },

router#show crypto map
Crypto Map "mymap" 10 ipsec-isakmp
  Peer = 172.16.1.2
  Extended IP access list 110
    access-list 110 permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
  Current peer: 172.16.1.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={ mine, }

```

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

Answer: A,C,D

Explanation:

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 NO: 81

Which type of security control is defense in depth?

A. threat mitigation

- B. risk analysis
- C. botnet mitigation
- D. overt and covert channels

Answer: A

Explanation:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap1.html

SAFE Design Blueprint

The Cisco SAFE uses the infrastructure-wide intelligence and collaboration capabilities provided by Cisco products to control and mitigate well-known and zero-day attacks. Under the Cisco SAFE design blueprints, intrusion protection systems, firewalls, network admission control, endpoint protection software, and monitoring and analysis systems work together to identify and dynamically respond to attacks. As part of threat control and containment, the designs have the ability to identify the source of a threat, visualize its attack path, and to suggest, and even dynamically enforce, response actions. Possible response actions include the isolation of compromised systems, rate limiting, packet filtering, and more.

Control is improved through the actions of harden, isolate, and enforce. Following are some of the objectives of the Cisco SAFE design blueprints:

- Adaptive response to real-time threats—Source threats are dynamically identified and may be blocked in realtime.
- Consistent policy enforcement coverage—Mitigation and containment actions may be enforced at different places in the network for defense in-depth.
- Minimize effects of attack—Response actions may be dynamically triggered as soon as an attack is detected, minimizing damage.
- Common policy and security management—A common policy and security management platform simplifies control and administration, and reduces operational expense.

QUESTION NO: 82

Which two options are two of the built-in features of IPv6? (Choose two.)

- A. VLSM
- B. native IPsec
- C. controlled broadcasts
- D. mobile IP
- E. NAT

Answer: B,D

Explanation:

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-tunnel.html>

IPv6 IPsec Site-to-Site Protection Using Virtual Tunnel Interface

The IPv6 IPsec feature provides IPv6 crypto site-to-site protection of all types of IPv6 unicast and multicast traffic using native IPsec IPv6 encapsulation. The IPsec virtual tunnel interface (VTI) feature provides this function, using IKE as the management protocol.

An IPsec VTI supports native IPsec tunneling and includes most of the properties of a physical interface. The IPsec VTI alleviates the need to apply crypto maps to multiple interfaces and provides a routable interface.

The IPsec VTI allows IPv6 routers to work as security gateways, establish IPsec tunnels between other security gateway routers, and provide crypto IPsec protection for traffic from internal network when being transmitting across the public IPv6 Internet.

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mobile.html>

Mobile IPv6 Overview

Mobile IPv4 provides an IPv4 node with the ability to retain the same IPv4 address and maintain uninterrupted network and application connectivity while traveling across networks. In Mobile IPv6, the IPv6 address space enables Mobile IP deployment in any kind of large environment. No foreign agent is needed to use Mobile IPv6.

System infrastructures do not need an upgrade to accept Mobile IPv6 nodes. IPv6 autoconfiguration simplifies mobile node (MN) Care of Address (CoA) assignment.

Mobile IPv6 benefits from the IPv6 protocol itself; for example, Mobile IPv6 uses IPv6 option headers (routing, destination, and mobility) and benefits from the use of neighbor discovery.

Mobile IPv6 provides optimized routing, which helps avoid triangular routing. Mobile IPv6 nodes work transparently even with nodes that do not support mobility (although these nodes do not have route optimization).

Mobile IPv6 is fully backward-compatible with existing IPv6 specifications. Therefore, any existing host that does not understand the new mobile messages will send an error message, and communications with the mobile node will be able to continue, albeit without the direct routing optimization.

QUESTION NO: 83

Which option is a characteristic of the RADIUS protocol?

A. uses TCP

- B. offers multiprotocol support
- C. combines authentication and authorization in one process
- D. supports bi-directional challenge

Answer: C

Explanation:

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

Authentication and Authorization

RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.

TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.

During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

QUESTION NO: 84

Refer to the below.

```
Router# debug tacacs
```

```
14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source
10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15
(AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15
(AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15
(AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

Which statement about this debug output is true?

- A. The requesting authentication request came from username GETUSER.
- B. The TACACS+ authentication request came from a valid user.
- C. The TACACS+ authentication request passed, but for some reason the user's connection was closed immediately.
- D. The initiating connection request was being spoofed by a different source address.

Answer: B

Explanation:

http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfser.html

debug tacacs

To display information associated with the TACACS, use the debug tacacs privileged EXEC command. The no form of this command disables debugging output.

debug tacacs

no debug tacacs

The following is sample output from the debug tacacs command for a TACACS login attempt that was successful, as indicated by the status PASS:

```
Router# debug tacacs
```

```
14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15
(AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
```

14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15
(AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15
(AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15

QUESTION NO: 85

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

Answer: B

Explanation:

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 NO: 86

Which priority is most important when you plan out access control lists?

- A.** Build ACLs based upon your security policy.
- B.** Always put the ACL closest to the source of origination.
- C.** Place deny statements near the top of the ACL to prevent unwanted traffic from passing through the router.
- D.** Always test ACLs in a small, controlled production environment before you roll it out into the larger production network.

Answer: A

Explanation:

QUESTION NO: 87

Which step is important to take when implementing secure network management?

- A. Implement in-band management whenever possible.
- B. Implement telnet for encrypted device management access.
- C. Implement SNMP with read/write access for troubleshooting purposes.
- D. Synchronize clocks on hosts and devices.
- E. Implement management plane protection using routing protocol authentication.

Answer: D

Explanation:

http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Background Information

Network time synchronization, to the degree required for modern performance analysis, is an essential exercise. Depending on the business models, and the services being provided, the characterization of network performance can be considered an important competitive service differentiator. In these cases, great expense may be incurred deploying network management systems and directing engineering resources towards analyzing the collected performance data. However, if proper attention is not given to the often-overlooked principle of time synchronization, those efforts may be rendered useless.

QUESTION NO: 88

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.

Answer: C

Explanation:

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 NO: 89

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

Answer: D

Explanation:

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 NO: 90

When STP mitigation features are configured, where should the root guard feature be deployed?

- A. toward ports that connect to switches that should not be the root bridge
- B. on all switch ports
- C. toward user-facing ports
- D. Root guard should be configured globally on the switch.

Answer: A

Explanation:

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800ae96b.shtml

The root guard feature provides a way to enforce the root bridge placement in the network. The root guard ensures that the port on which root guard is enabled is the designated port. Normally, root bridge ports are all designated ports, unless two or more ports of the root bridge are connected together. If the bridge receives superior STP Bridge Protocol Data Units (BPDUs) on a root guard-enabled port, root guard moves this port to a root-inconsistent STP state. This root-inconsistent state is effectively equal to a listening state. No traffic is forwarded across this port. In this way, the root guard enforces the position of the root bridge.

QUESTION NO: 91

Which option is a characteristic of a stateful firewall?

- A. can analyze traffic at the application layer
- B. allows modification of security rule sets in real time to allow return traffic
- C. will allow outbound communication, but return traffic must be explicitly permitted
- D. supports user authentication

Answer: B

Explanation:

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 NO: 92

Which type of NAT would you configure if a host on the external network required access to an internal host?

- A. Outside global NAT
- B. NAT overload
- C. Dynamic outside NAT
- D. Static NAT

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/nat_static.html

Information About Static NAT

Static NAT creates a fixed translation of real address(es) to mapped address(es). With dynamic NAT and PAT, each host uses a different address or port for each subsequent translation.

Because the mapped address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the destination network to initiate traffic to a translated host (if an access list exists that allows it).

The main difference between dynamic NAT and a range of addresses for static NAT is that static NAT allows a remote host to initiate a connection to a translated host (if an access list exists that allows it), while dynamic NAT does not. You also need an equal number of mapped addresses as real addresses with static NAT.

Figure 28-1 shows a typical static NAT scenario. The translation is always active so both translated and remote hosts can originate connections, and the mapped address is statically assigned by the static command.

Figure 28-1 Static NAT



QUESTION NO: 93

Which statement about disabled signatures when using Cisco IOS IPS is true?

- A. They do not take any actions, but do produce alerts.
- B. They are not scanned or processed.
- C. They still consume router resources.
- D. They are considered to be "retired" signatures.

Answer: C

Explanation:

Disabled means that the signature does not produce an alert but is compiled into memory and inspection takes place. There are advantages of having signatures disabled, such as allowing the customer to quickly enable the signature without waiting for it to be loaded into memory and for inspection to take place.

QUESTION NO: 94

Which type of intrusion prevention technology is the primary type used by the Cisco IPS security appliances?

- A. profile-based
- B. rule-based
- C. protocol analysis-based
- D. signature-based
- E. NetFlow anomaly-based

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_fwids.html

The Signature Definition File

A Signature Definition file (SDF) has definitions for each signature it contains. After signatures are loaded and compiled onto a router running Cisco IOS IPS, IPS can begin detecting the new signatures immediately. If customers do not use the default, built-in signatures that are shipped with the routers, users can choose to download one of two different types of SDFs: the attack-drop.sdf file (which is a static file) or a dynamic SDF (which is dynamically updated and accessed from Cisco.com).

The attack-drop.sdf file is available in flash on all Cisco access routers that are shipped with Cisco IOS Release 12.3(8)T or later. The attack-drop.sdf file can then be loaded directly from flash into the Cisco IOS IPS system. If flash is erased, the attack-drop.sdf file may also be erased. Thus, if you are copying a Cisco IOS image to flash and are prompted to erase the contents of flash before copying the new image, you might risk erasing the attack-drop.sdf file. If this occurs, the router will refer to the built-in signatures within the Cisco IOS

image. The attack-drop.sdf file can also be downloaded onto your router from Cisco.com.

To help detect the latest vulnerabilities, Cisco provides signature updates on Cisco.com on a regular basis. Users can use SDM or VMS to download these signature updates, tune the signature parameters as necessary, and deploy the new SDF to a Cisco IOS IPS router.

QUESTION NO: 95

Which two services are provided by IPsec? (Choose two.)

- A. Confidentiality
- B. Encapsulating Security Payload
- C. Data Integrity
- D. Authentication Header
- E. Internet Key Exchange

Answer: A,C

Explanation:

http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/2.0/ip_security/provisioning/guide/IPsecPG1.html

IPsec Overview

A secure network starts with a strong security policy that defines the freedom of access to information and dictates the deployment of security in the network. Cisco Systems offers many technology solutions for building a custom security solution for Internet, extranet, intranet, and remote access networks. These scalable solutions seamlessly interoperate to deploy enterprise-wide network security. Cisco System's IPsec delivers a key technology component for providing a total security solution. Cisco's IPsec offering provides privacy, integrity, and authenticity for transmitting sensitive information over the Internet.

Cisco's end-to-end offering allows customers to implement IPsec transparently into the network infrastructure without affecting individual workstations or PCs. Cisco IPsec technology is available across the entire range of computing infrastructure. Windows 95, Windows NT 4.0, and Cisco IOS software.

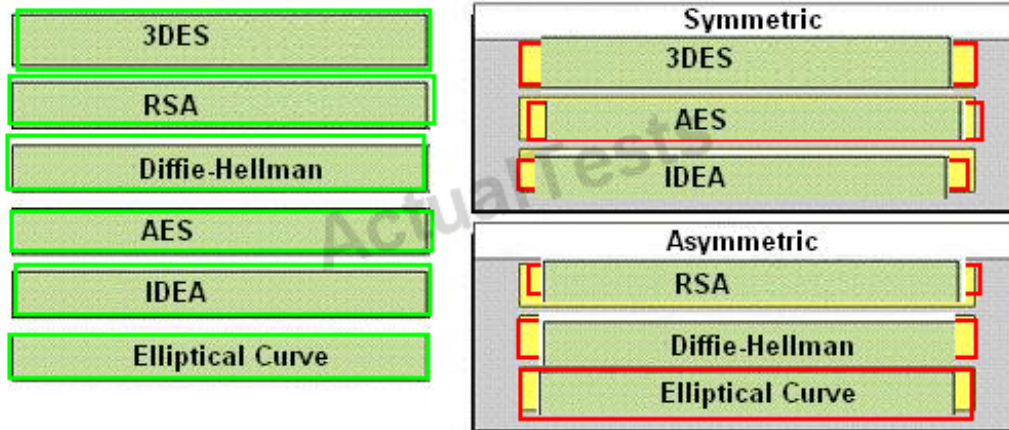
IPsec is a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPsec ensures confidentiality, integrity, and authenticity of data communications across a public network. IPsec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.

QUESTION NO: 96 DRAG DROP

Drag from Left to Right in Correct Area.

3DES	Symmetric
RSA	
Diffie-Hellman	
AES	Asymmetric
IDEA	
Elliptical Curve	

Answer:

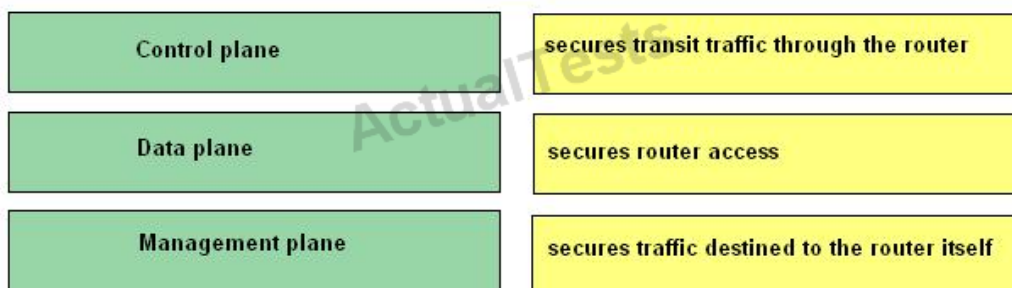


Explanation:



QUESTION NO: 97 DRAG DROP

Drag the item the left and drop them on their functions on the right.



Answer:

Drag the item the left and drop them on their functions on the right.

Control plane

Data plane

Data plane

Management plane

Management plane

Control plane

Explanation:

Drag the item the left and drop them on their functions on the right.

Data plane

Management plane

Control plane

QUESTION NO: 98 DRAG DROP

Drag the items from the left and drop them on their definitions on the right.

False positive

A signature is not fired when non-offending traffic is captured and analyzed

False negative

A signature is not fired when offending traffic is detected

True positive

An alarm is triggered by normal traffic or a benign action

True negative

Generates an alarm when offending traffic is detected

Answer:

Drag the items from the left and drop them on their definitions on the right.

False positive

True negative

False negative

False negative

True positive

False positive

True negative

True positive

Explanation:

Drag the items from the left and drop them on their definitions on the right.

True negative

False negative

False positive

True positive

QUESTION NO: 99 DRAG DROP

Drag the IPS detection approaches from the left and drop on the correct IPS detection technology categories on the right.

Detects attacks based on known attack fingerprints

policy-based

Detects unexpected traffic spikes

anomaly-based

Only allows HTTPS traffic to the web server

signature-based

Detects events based on correlations with a blacklist downloaded from a dynamically updated database

reputation-based

Answer:

Drag the IPS detection approaches from the left and drop on the correct IPS detection technology categories on the right.

Detects attacks based on known attack fingerprints

Only allows HTTPS traffic to the web server

Detects unexpected traffic spikes

Detects unexpected traffic spikes

Only allows HTTPS traffic to the web server

Detects attacks based on known attack fingerprints

Detects events based on correlations with a blacklist downloaded from a dynamically updated database

Detects events based on correlations with a blacklist downloaded from a dynamically updated database

Explanation:

Drag the IPS detection approaches from the left and drop on the correct IPS detection technology categories on the right.

Only allows HTTPS traffic to the web server

Detects unexpected traffic spikes

Detects attacks based on known attack fingerprints

Detects events based on correlations with a blacklist downloaded from a dynamically updated database

QUESTION NO: 100 DRAG DROP

Drag the correct IPv6 unicast address types from the left and drop them on the boxes on the right. Not all types are used.

global	Target
6to4	Target
link-local	Target
reserved	Target
solicited node	
site-local	

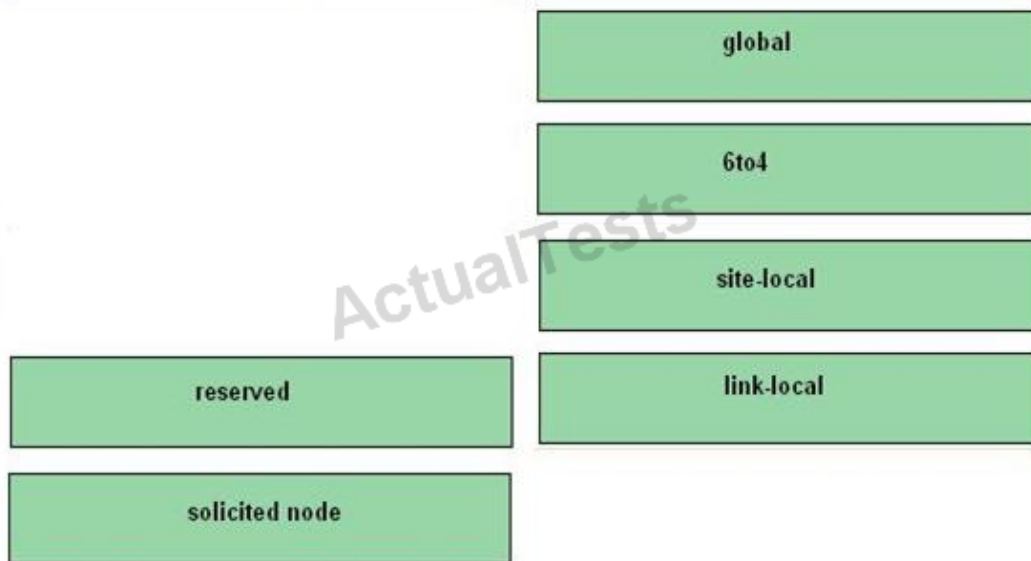
Answer:

Drag the correct IPv6 unicast address types from the left and drop them on the boxes on the right. Not all types are used.

global	global
6to4	6to4
link-local	site-local
reserved	link-local
solicited node	
site-local	

Explanation:

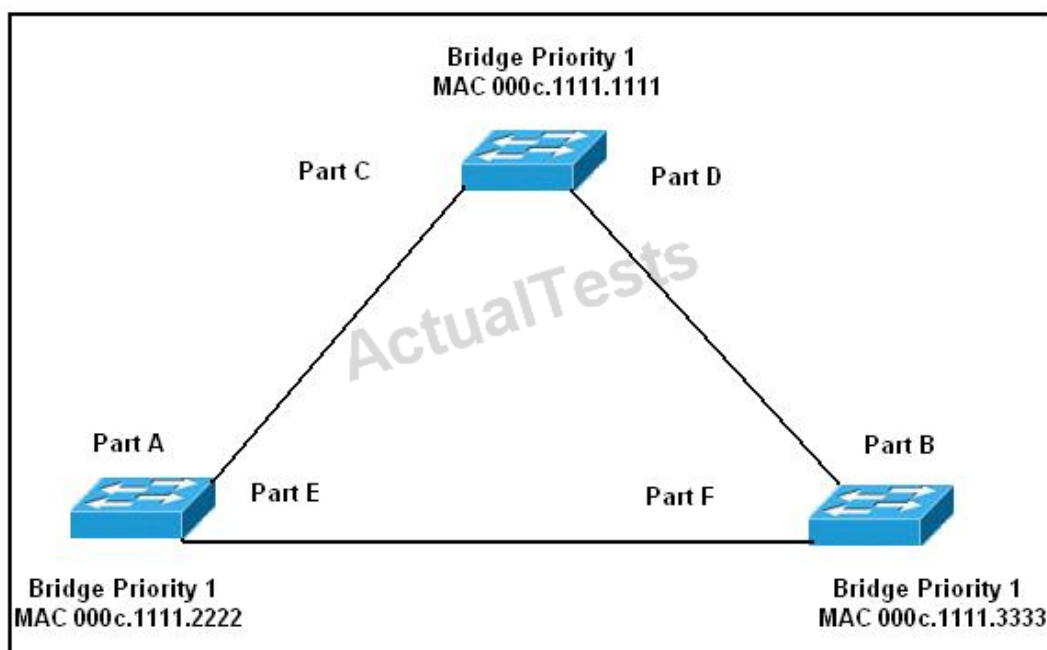
Drag the correct IPv6 unicast address types from the left and drop them on the boxes on the right. Not all types are used.



Topic 2, Volume B

QUESTION NO: 101 DRAG DROP

Refer to the exhibit. Drag the port(s) from the left and drop them on the correct STP roles on the right. Not all options on the left are used.



Port E	root port(s)
Port F	designated port(s)
Ports A and B	non-designated port(s)
Ports C and D	
Ports C, D, and E	
Ports A, B, and F	
Ports A, B, and E	
Ports A, B, C, and D	

Answer:

Port E	Ports A and B
Port F	Ports C, D, and E
Ports A and B	Port F
Ports C and D	
Ports C, D, and E	
Ports A, B, and F	
Ports A, B, and E	
Ports A, B, C, and D	

Explanation:

Port E	Ports A and B
	Ports C, D, and E
	Port F
Ports C and D	
Ports A, B, and F	
Ports A, B, and E	
Ports A, B, C, and D	

QUESTION NO: 102 DRAG DROP

Match the descriptions on the left with the IKE phases on the right.

Perform a Diffie-Hellman exchange

Establish IPsec SAs

Negotiate IPsec security policies

Negotiate IKE policy sets and authenticate peers

Perform an optional Diffie-Hellman exchange

IKE Phase 1

IKE Phase 2

Answer:

Match the descriptions on the left with the IKE phases on the right.

Perform a Diffie-Hellman exchange

Establish IPsec SAs

Negotiate IPsec security policies

Negotiate IKE policy sets and authenticate peers

Perform an optional Diffie-Hellman exchange

IKE Phase 1

Perform a Diffie-Hellman exchange

Negotiate IKE policy sets and authenticate peers

IKE Phase 2

Establish IPsec SAs

Negotiate IPsec security policies

Perform an optional Diffie-Hellman exchange

Explanation:

Match the descriptions on the left with the IKE phases on the right.

IKE Phase 1

Perform a Diffie-Hellman exchange

Negotiate IKE policy sets and authenticate peers

IKE Phase 2

Establish IPsec SAs

Negotiate IPsec security policies

Perform an optional Diffie-Hellman exchange

QUESTION NO: 103 DRAG DROP

Drag the characteristics from the left and drop them the correct categories on the right.

	IPS
Can stop the attack trigger packet	Target
No network impact if there is a sensor overload	Target
Allows malicious traffic to pass before it can respond	Target
Deployed in promiscuous mode	Target
Can use stream normalization techniques	Target
More vulnerable to network evasion techniques	Target
Has some impact on network latency and jitter	Target
Deployed in inline mode	Target

Answer:

Drag the characteristics from the left and drop them the correct categories on the right.

	IPS
Can stop the attack trigger packet	Can stop the attack trigger packet
No network impact if there is a sensor overload	
Allows malicious traffic to pass before it can respond	Has some impact on network latency and jitter
Deployed in promiscuous mode	Deployed in inline mode
Can use stream normalization techniques	Can use stream normalization techniques
More vulnerable to network evasion techniques	
Has some impact on network latency and jitter	No network impact if there is a sensor overload
Deployed in inline mode	Allows malicious traffic to pass before it can respond
	Deployed in promiscuous mode
	More vulnerable to network evasion techniques

Explanation:

Drag the characteristics from the left and drop them the correct categories on the right.

IPS

Can stop the attack trigger packet

Has some impact on network latency and jitter

Deployed in inline mode

Can use stream normalization techniques

IDS

No network impact if there is a sensor overload

Allows malicious traffic to pass before it can respond

Deployed in promiscuous mode

More vulnerable to network evasion techniques

QUESTION NO: 104 DRAG DROP

Drag the protocol characteristics from the left and drop them on the correct protocols on the right. Not all the options on the left used.

	TACACS+
Uses TCP	
Uses UDP	
Uses IP protocol number 49	
Separates the authentication, authorization, and accounting functions	
Combines the authentication and authorization functions	
Encrypts the entire body of the packet	
Encrypts the password only	
Supports authorization of router commands on a per-user or per-group basis	
Uses a trusted third party called the key distribution center	
Uses a peer-to-peer architecture	

	RADIUS

Answer:

Drag the protocol characteristics from the left and drop them on the correct protocols on the right. Not all the options on the left used.

	TACACS+
Uses TCP	Uses TCP
Uses UDP	Separates the authentication, authorization, and accounting functions
Uses IP protocol number 49	Encrypts the entire body of the packet
Separates the authentication, authorization, and accounting functions	Supports authorization of router commands on a per-user or per-group basis
Combination of the authentication and authorization functions	
Encrypts the entire body of the packet	
Encrypts the password only	
Supports authorization of router commands on a per-user or per-group basis	
Uses a trusted third party called the key distribution center	
Uses a peer-to-peer architecture	

	RADIUS
	Uses UDP
	Combination of the authentication and authorization functions
	Encrypts the password only

Explanation:

Drag the protocol characteristics from the left and drop them on the correct protocols on the right. Not all the options on the left used.

TACACS+	
Uses TCP	Uses TCP
Uses UDP	Separates the authentication, authorization, and accounting functions
Uses IP protocol number 49	Encrypts the entire body of the packet
Separates the authentication, authorization, and accounting functions	Supports authorization of router commands on a per-user or per-group basis
Combinations the authentication and authorization functions	
Encrypts the entire body of the packet	
Encrypts the password only	
Supports authorization of router commands on a per-user or per-group basis	
Uses a trusted third party called the key distribution center	
Uses a peer-to-peer architecture	

RADIUS	
	Uses UDP
	Combinations the authentication and authorization functions
	Encrypts the password only

Reference. TACACS+ and RADIUS Comparison

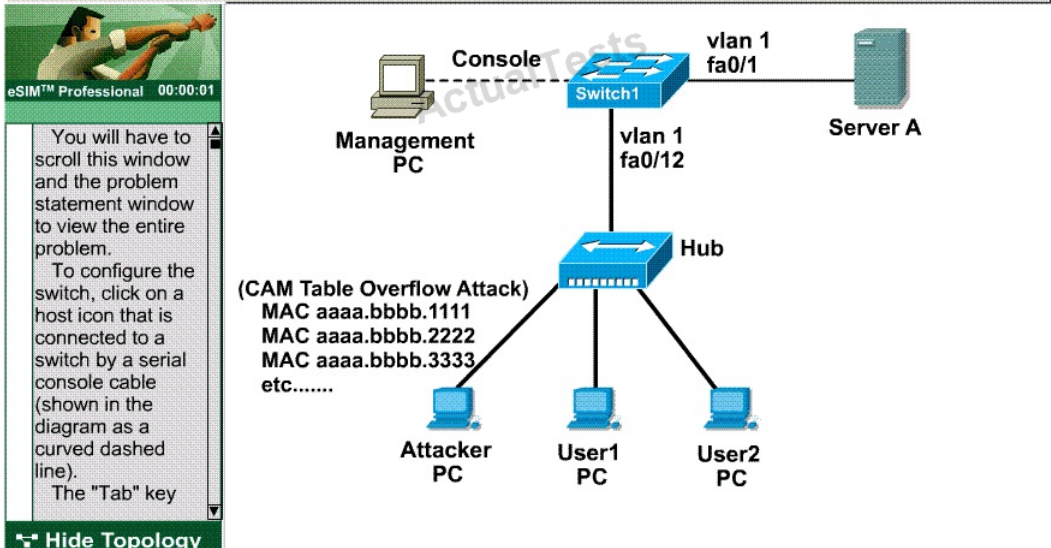
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml#comp_packet_encrypt

QUESTION NO: 105 CORRECT TEXT

You are the network security administrator for Big Money Bank Co. You are informed that an attacker has performed a CAM table overflow attack by sending spoofed MAC addresses on one of the switch ports. The attacker has since been identified and escorted out of the campus. You now need to take action to configure the switch port to protect against this kind of attack in the future.

For purposes of this test, the attacker was connected via a hub to the Fa0/12 interface of the switch. The topology is provided for your use. The enable password of the switch is cisco. Your task is to configure the Fa0/12 interface on the switch to limit the maximum number of MAC addresses that are allowed to access the port to two and to shutdown the interface when there is a violation.

Enable password: cisco



```
--S#show run
Building configuration...
Current configuration :
!
version 12.1
no service pad
Service timestamps debug uptime
Service timestamps log uptime
No service password-encryption
!
Hostname -S
!
!
Enable secret 5 $1$0/yw#toqA0XRiCtY8gh7pM06fS0
!
Ip subnet-zero
!
Ip ssh time-out 120
Ip ssh authentication-retries 3
!
Spanning-tree mode pvst
No spanning-tree optimize bpdu transmission
Spanning-tree extend system-id
!
.....
!
Interface FastEthernet0/22
!
Interface FastEthernet0/23
!
Interface FastEthernet0/24
  switchport mode trunk
!
Interface GigabitEthernet0/1
!
Interface GigabitEthernet0/2
!
Interface vlan1
  ip address 172.26.26.202 255.255.255.0
  no ip route-cache
!
Ip http server
!
!
!
!
Line con 0
Line aux 0

Line vty 5 15
  password cisco
Login
!
End
-S#
```

Answer: Switch1>enable

Switch1#config t

```

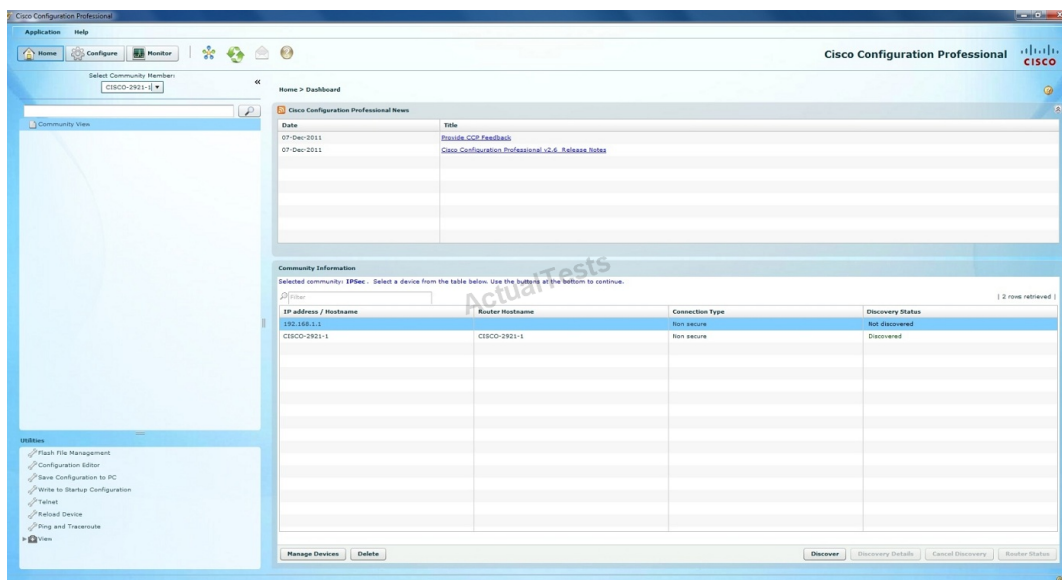
Switch1(config)#interface fa0/12
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport port-security maximum 2
Switch1(config-if)#switchport port-security violation shutdown
Switch1(config-if)#no shut
Switch1(config-if)#end
Switch1#copy run start

```

QUESTION NO: 106

Scenario:

You are the security admin for a small company. This morning your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your business question.



Which four properties are included in the inspection Cisco Map OUT_SERVICE? (Choose four)

- A. FTP
- B. HTTP
- C. HTTPS
- D. SMTP
- E. P2P
- F. ICMP

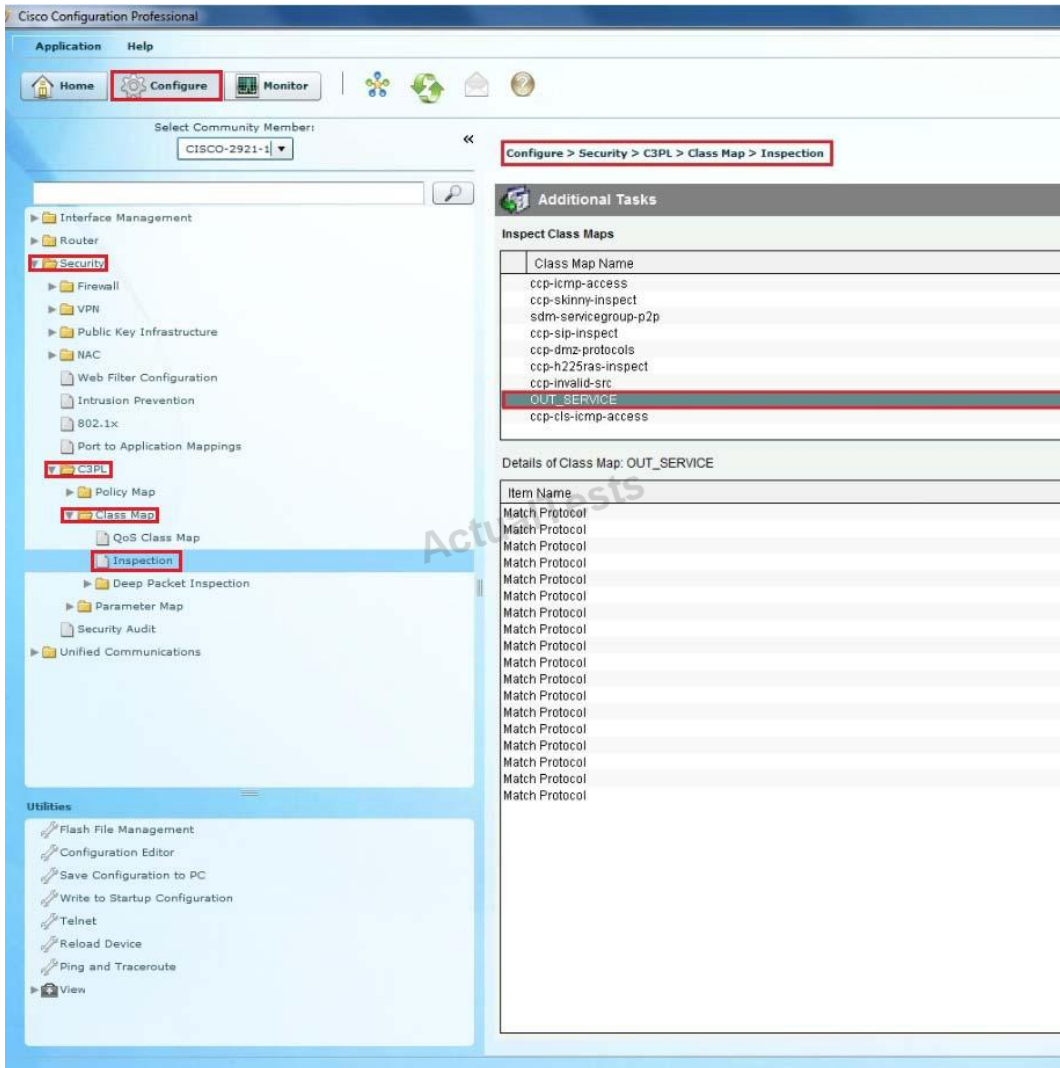
Answer: A,B,E,F

Explanation: First option:

The screenshot shows the Cisco Configuration Professional interface. The top navigation bar includes 'Application' and 'Help' menus. Below it, there are 'Home', 'Configure', and 'Monitor' tabs. The 'Configure' tab is active, and the breadcrumb path 'Configure > Security > Firewall > Firewall' is shown. The left sidebar contains a tree view with categories like 'Interface Management', 'Router', 'Security', 'Firewall', 'VPN', 'Public Key Infrastructure', 'NAC', 'Web Filter Configuration', 'Intrusion Prevention', '802.1x', 'Port to Application Mappings', 'C3PL', 'Policy Map', 'Class Map', 'Parameter Map', 'Security Audit', and 'Unified Communications'. The 'Firewall' category is expanded, showing sub-items like 'Firewall Components', 'Zone Pairs', 'Zones', 'Policy Map', 'Class Map', 'Parameter Map', 'Security Audit', and 'Unified Communications'. The main area displays the 'Edit Firewall Policy' tab, which contains a table of traffic classification rules. A search box is visible at the top left, and a 'Utilities' section is at the bottom left.

ID	Source	Destination	Service	Action
ccp-permit-dmzservice (in-zone to dmz-zone, out-zone to dmz-zone)				
1	any	10.1.1.1	rsvd	Inspect
2	Unmatched Traffic			Drop
ccp-permit (out-zone to self)				
1	any	any	h323	Inspect
2	any	any	h225ras	Inspect
3	Unmatched Traffic			Drop
ccp-permit-icmpreply (self to out-zone)				
1	any	any	icmp	Inspect
2	any	any	tcp	Inspect
3	any	any	udp	Inspect
4	any	any	h323	Inspect
5	any	any	h225ras	Inspect
6	Unmatched Traffic			Allow
ccp-inspect (in-zone to out-zone)				
1	100	any	any	Drop
2	any	any	OUT_SERVICE	Inspect
3	any	any	h323	Inspect
4	any	any	h225ras	Inspect
5	any	any	h225ras	Inspect
6	Unmatched Traffic			Drop

Second option:



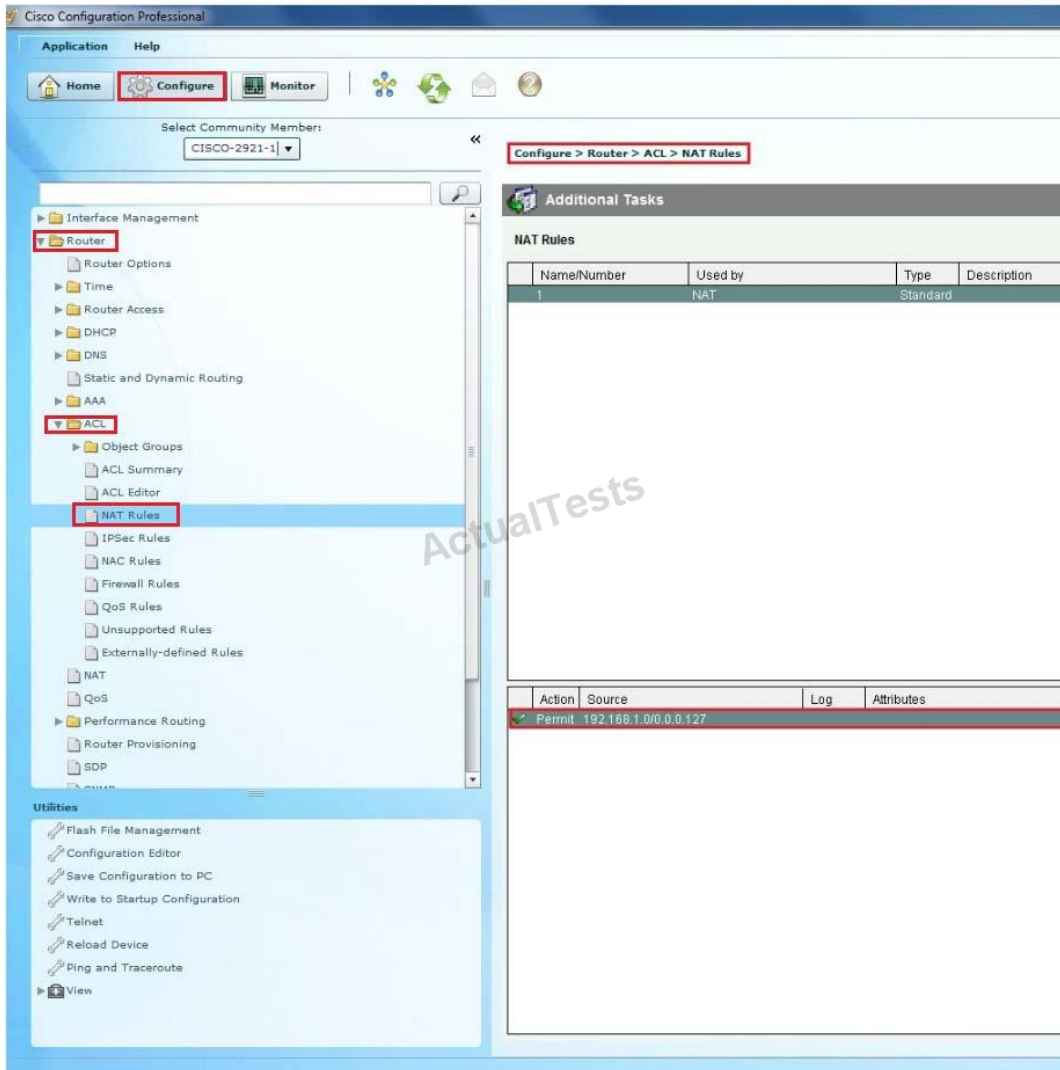
QUESTION NO: 107

Scenario:

You are the security admin for a small company. This morning your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your business question.

A. 192.168.1.0/25
B. GlobalEthernet0/0 interface address.
C. 172.25.223.0/24
D. 10.0.10.0/24

"Pass Any Exam. Any Time." - www.actualtests.com 126



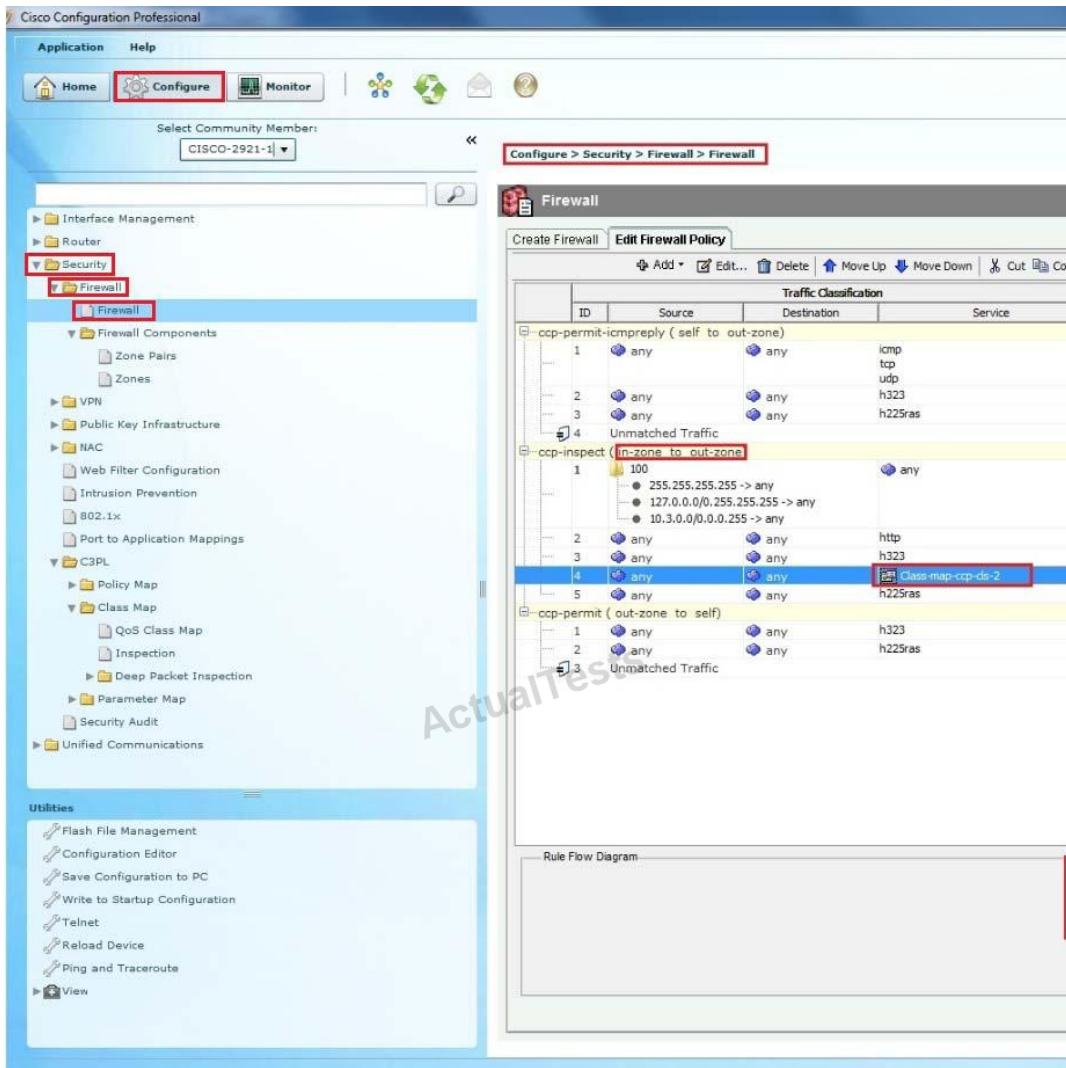
QUESTION NO: 108

Scenario:

You are the security admin for a small company. This morning your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your business question.

A. SERVICE_IN
B. Class-map-ccp-cls-2
C. Ccp-cts-2
D. Class-map SERVICE_IN

Explanation:



QUESTION NO: 109

Scenario:

You are the security admin for a small company. This morning your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your business question.

A. Sdm-cls-http
B. OUT_SERVICE
C. Ccp-policy-ccp-cls-1
D. Ccp-policy-ccp-cls-2

Explanation:

Configure > Security > Firewall > Firewall Components > Zone Pairs

Additional Tasks

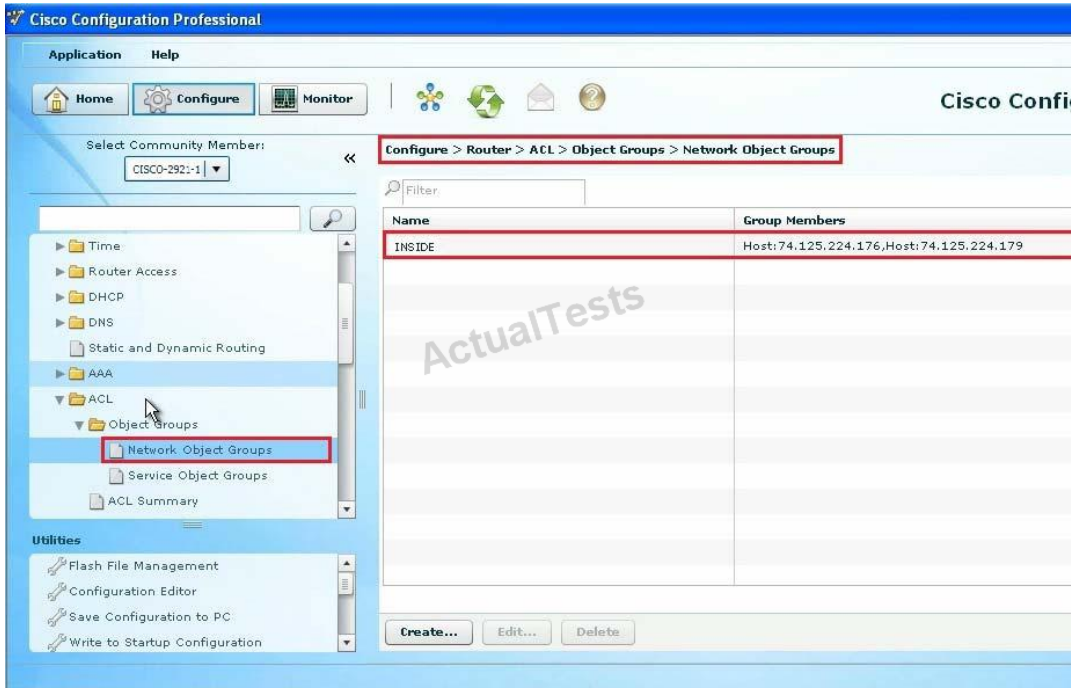
Zone Pairs

Zone Pair	Source	Destination
sdm-zip-OUT-IN	out-zone	in-zone
ccp-zp-self-out	self	out-zone
ccp-zp-in-out	in-zone	out-zone
ccp-zp-in-dmz	in-zone	dmz-zone
ccp-zp-out-dmz	out-zone	dmz-zone
ccp-zp-out-self	out-zone	self

QUESTION NO: 110

Scenario:

You are the security admin for a small company. This morning your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your business question.



What is included in the Network Object Group INSIDE? (Choose two)

- A. Network 192.168.1.0/24
- B. Network 175.25.133.0/24
- C. Network 10.0.10.0/24
- D. Network 10.0.0.0/8
- E. Network 192.168.1.0/8

Answer: B,C

Explanation:

QUESTION NO: 111 CORRECT TEXT

Instruction

This item contains a simulation task. Refer to the scenario and topology before starting. Open the Topology window and click the required device to open the GUI window on a virtual terminal. Check your configuration from the client system in the topology.

Scenario

You are the security administrator for a small company. You need to modify an existing configuration of a Cisco Integrated Services Router. Using Cisco Configuration Professional (CCP), you will need to add the following configurations to the router to meet security policy requirements.

Configure Network Time Protocol (NTP)
 Preferred NTP Server IP 192.168.4.2
 Source Interface FastEthernet 0/1
 Authentication key of 1 with a key value of cisco

Create a new Access Rule
 Name Inbound
 Type Extended Rule

Create and add a new Rule Entry to the Access Rule
 Permit any source and any destination for protocol eigrp

Add an additional Rule Entry to the Access Rule
 Permit any source to the 10.0.2.0/24 network for protocol 80

Associate this new Access Rule to the OUTSIDE interface in the INBOUND direction
 NOTE: Allow CCP to add an entry rule to allow NTP traffic

TOPOLOGY

Scenario topology

Virtual Terminal

http://127.0.0.1:8600/Counterpoint/CPMain.html?rand=9185 - Windows Internet Explorer provided by Cisco

Application Help

Home Configure Monitor

Select Community Member: 10.0.2.1 << Home >>

Community View

Community View

Utilities

- Flash File Management
- Software Upgrade
- Configuration Editor
- Save Configuration to PC
- Write to Startup Configuration
- Telnet

Cisco Configuration Professional

Cisco Configuration Professional News

Date	Title
22-Jul-2010	Provide CCP Feedback

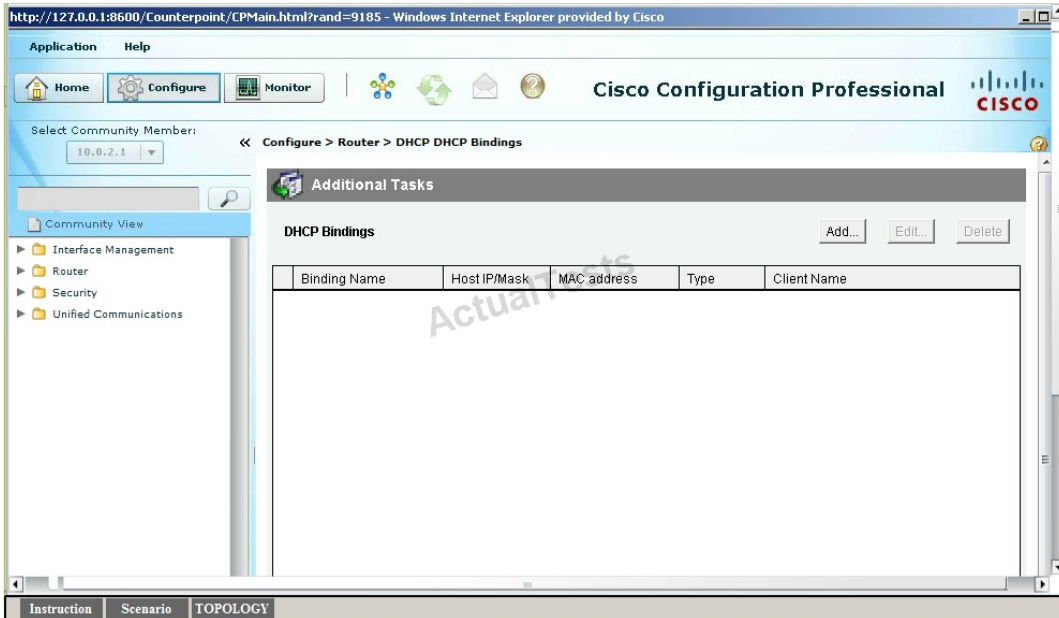
Community Information

Selected community: **New Community**. Select a device from the table below. Use the buttons at the bottom to continue.

Filter | 1 rows retrieved |

IP address / Hostname	Router Hostname	Connection Type	Discovery Status
10.0.2.1	pod-2-isr	Secure	discovered

Manage Devices Delete Discover Discovery Details Cancel Discovery Router Status



Answer: For the NTP portion:

Click on Router – Time – NTP and SNTP on left hand pane.

Then click the Add button. Enter the Server IP address and source interface and key information as specified. Also be sure to click the Prefer button.

For the access rule portion:

Click on Router – ACL – ACL Editor. Click Add button. Then enter Inbound for the name and make sure rule is extended. Then click Add at the rule entry. Then ensure that permit is selected and that source and destination boxes both say Any IP Address (They should already).

Under Protocol and Service select EIGRP. Hit OK.

Then click add button again. Leave the source as any and click the destination box as “A network” and type in 10.0.2.0 and select the wildcard mask as 0.0.0.255. Click on the TCP protocol button and select “www” Hit OK.

Finally, click on edit for this rule and click on the Associate button. Select the outside interface and select the inbound direction.

QUESTION NO: 112 HOTSPOT

Questions

1
2
3
4
5

0% Complete

Instructions

You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Scenario

You are the security admin for a small company. This morning, your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your bosses questions. Not all screens are active for this exercise.

CCP

Application Help

Home Configure Monitor

Select Community Member: CISCO-2921-1

Home >

Cisco Configuration Professional News

Date	Title
22-Jul-2010	Provide CCP Feedback

Community Information

Selected community: New Community. Select a device from the table below. Use the buttons at the bottom

Filter

IP address / Hostname	Router Hostname	Connection Type	Discovery
CISCO-887-1	CISCO-887-1	Non secure	Discover
CISCO-1861-W	CISCO-1861-W	Non secure	Discover
CISCO-2921-1	CISCO-2921-1	Non secure	Discover

Manage Devices Delete Discover Discovery Details Cancel Discovery

Utilities

- Flash File Management
- Software Upgrade
- Configuration Editor
- Save Configuration to PC
- Write to Startup Configuration
- Telnet

CCP

Application Help

Home Configure Monitor

Select Community Member: CISCO-2921-1

Home >

Cisco Configuration Professional

Interfaces and Connections

Create Connection Edit Interface/Connection

Create New Connection

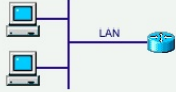
Select a connection and click Create New Connection

Ethernet LAN

Information

Configure Ethernet LAN interface for straight routing and 802.1q trunking

Use Case Scenario



Question 1

What NAT address will be assigned by ACL 1?

- ☐ 192.168.1.0/25
- ☐ GigabitEthernet0/0 interface address
- ☐ 172.25.223.0/24
- ☐ 10.0.10.0/24

Answer:

Question 1

What NAT address will be assigned by ACL 1?

- ☒ 192.168.1.0/25
- ☐ GigabitEthernet0/0 interface address
- ☐ 172.25.223.0/24
- ☐ 10.0.10.0/24

Explanation:

Question 1

What NAT address will be assigned by ACL 1?

- ☒ 192.168.1.0/25
- ☐ GigabitEthernet0/0 interface address
- ☐ 172.25.223.0/24
- ☐ 10.0.10.0/24

QUESTION NO: 113 HOTSPOT

Questions

1

2

3

4

5

0% Complete

Instructions

You can click on the grey buttons below to view the different windows.
Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Scenario

You are the security admin for a small company. This morning, your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your bosses questions. Not all screens are active for this exercise.

CISCO

CCP

Application Help

Home Configure Monitor

Cisco Configuration Professional

Select Community Member: CISCO-2921-1

Community View

Utilities

- Flash File Management
- Software Upgrade
- Configuration Editor
- Save Configuration to PC
- Write to Startup Configuration
- Telnet

Cisco Configuration Professional News

Date	Title
22-Jul-2010	Provide CCP Feedback

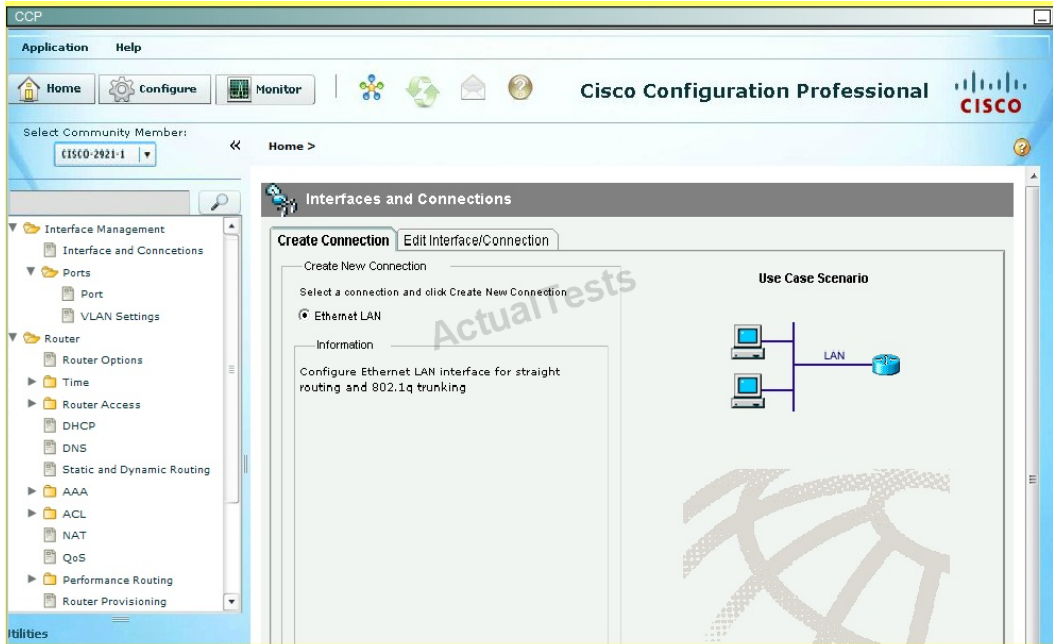
Community Information

Selected community: New Community. Select a device from the table below. Use the buttons at the bottom.

Filter

IP address / Hostname	Router Hostname	Connection Type	Discovery
CISCO-887-1	CISCO-887-1	Non-secure	Discover
CISCO-1861-W	CISCO-1861-W	Non-secure	Discover
CISCO-2921-1	CISCO-2921-1	Non-secure	Discover

Manage Devices Delete Discover Discovery Details Cancel Discovery



Question 2

Which four protocols are included in the Inspection Class Map OUT_SERVICE? (Choose four)

- ☐ FTP
- ☐ HTTP
- ☐ HTTPS
- ☐ SMTP
- ☐ P2P
- ☐ ICMP

Answer:

Question 2

Which four protocols are included in the Inspection Class Map OUT_SERVICE? (Choose four)

- ☐ FTP
- ☒ HTTP
- ☒ HTTPS
- ☒ SMTP
- ☐ P2P
- ☒ ICMP

Explanation:

http, https, smtp, icmp

Click on Router – Security – C3PL – Class Map – Inspection. Then select the OUT_SERVICE map and see the four protocols listed.

QUESTION NO: 114 HOTSPOT

Questions

1

2

3

4

5

0% Complete

Instructions

You can click on the grey buttons below to view the different windows.
Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Scenario

You are the security admin for a small company. This morning, your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your bosses questions. Not all screens are active for this exercise.

CISCO

CCP

Application Help

Home Configure Monitor

Select Community Member: CISCO-2921-1 << Home >

Community View

Utilities

- Flash File Management
- Software Upgrade
- Configuration Editor
- Save Configuration to PC
- Write to Startup Configuration
- Telnet

Cisco Configuration Professional News

Date	Title
22-Jul-2010	Provide CCP Feedback

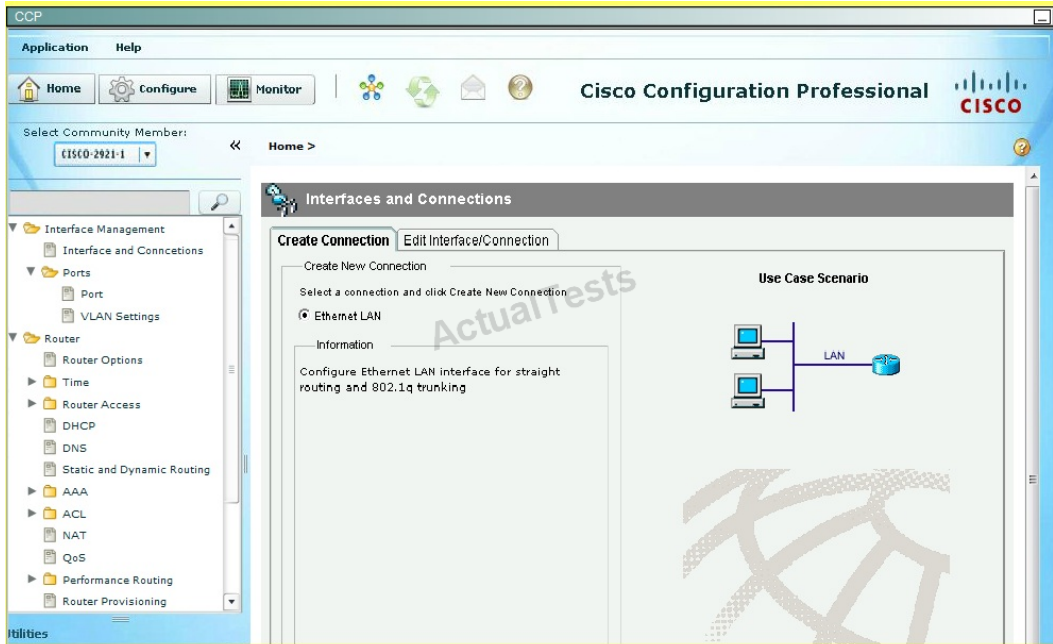
Community Information

Selected community: **New Community** . Select a device from the table below. Use the buttons at the bottom

Filter

IP address / Hostname	Router Hostname	Connection Type	Discovery
CISCO-887-1	CISCO-887-1	Non-secure	Discover
CISCO-1861-W	CISCO-1861-W	Non-secure	Discover
CISCO-2921-1	CISCO-2921-1	Non-secure	Discover

Manage Devices Delete Discover Discovery Details Cancel Discovery



Question 3

Which Class Map is used by the INBOUND Rule?

- ☐ SERVICE_IN
- ☐ Class-map ccp-cls-2
- ☐ Ccp-cls-2
- ☐ Class-map SERVICE_IN

Answer:

Question 3

Which Class Map is used by the INBOUND Rule?

- ☐ SERVICE_IN
- ☒ Class-map ccp-cls-2
- ☐ Ccp-cls-2
- ☐ Class-map SERVICE_IN

Explanation:

Question 3

Which Class Map is used by the INBOUND Rule?

- ☐ SERVICE_IN
- ☒ Class-map ccp-cls-2
- ☐ Ccp-cls-2
- ☐ Class-map SERVICE_IN

QUESTION NO: 115 HOTSPOT

Questions

1

2

3

4

5

0% Complete

Instructions

You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Scenario

You are the security admin for a small company. This morning, your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your bosses questions. Not all screens are active for this exercise.

CISCO

CCP

Application

Help

Home

Configure

Monitor

Cisco Configuration Professional

Select Community Member:
CISCO-2921-1

Home

Community View

Community Information

Selected community: New Community . Select a device from the table below. Use the buttons at the bottom.

Filter

IP address / Hostname	Router Hostname	Connection Type	Discovery
CISCO-887-1	CISCO-887-1	Non-secure	Discover
CISCO-1861-W	CISCO-1861-W	Non-secure	Discover
CISCO-2921-1	CISCO-2921-1	Non-secure	Discover

Manage Devices

Delete

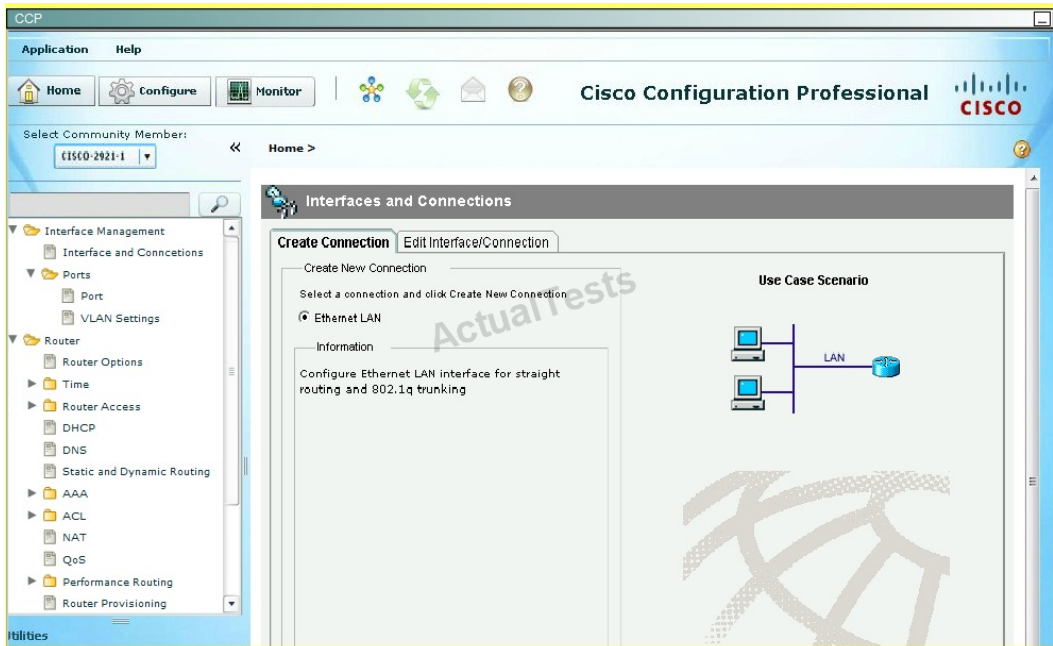
Discover

Discovery Details

Cancel Discovery

Utilities

- Flash File Management
- Software Upgrade
- Configuration Editor
- Save Configuration to PC
- Write to Startup Configuration
- Telnet



Question 4

What is included in the Network Object Group INSIDE? (Choose two.)

- ☐ Network 192.168.1.0/24
- ☐ Network 172.25.133.0/24
- ☐ Network 10.0.10.0/24
- ☐ Network 10.0.0.0/8
- ☐ Network 192.168.1.0/8

Answer:

Question 4

What is included in the Network Object Group INSIDE? (Choose two.)

- ☐ Network 192.168.1.0/24
- ☒ Network 172.25.133.0/24
- ☒ Network 10.0.10.0/24
- ☐ Network 10.0.0.0/8
- ☐ Network 192.168.1.0/8

Explanation:

Question 4

What is included in the Network Object Group INSIDE? (Choose two.)

- ☐ Network 192.168.1.0/24
- ☒ Network 172.25.133.0/24
- ☒ Network 10.0.10.0/24
- ☐ Network 10.0.0.0/8
- ☐ Network 192.168.1.0/8

QUESTION NO: 116 HOTSPOT

Questions

1

2

3

4

5

0% Complete

Instructions

You can click on the grey buttons below to view the different windows.
Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Scenario

You are the security admin for a small company. This morning, your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your bosses questions. Not all screens are active for this exercise.

CISCO

CCP

Application Help

Home

Configure

Monitor

Cisco Configuration Professional

Select Community Member:
CISCO-2921-1

Home

Community View

Cisco Configuration Professional News

Date	Title
22-Jul-2010	Provide CCP Feedback

Community Information

Selected community: **New Community**. Select a device from the table below. Use the buttons at the bottom.

Filter

IP address / Hostname	Router Hostname	Connection Type	Discovery
CISCO-887-1	CISCO-887-1	Non-secure	Discover
CISCO-1861-W	CISCO-1861-W	Non-secure	Discover
CISCO-2921-1	CISCO-2921-1	Non-secure	Discover

Manage Devices

Delete

Discover

Discovery Details

Cancel Discovery

Utilities

Flash File Management

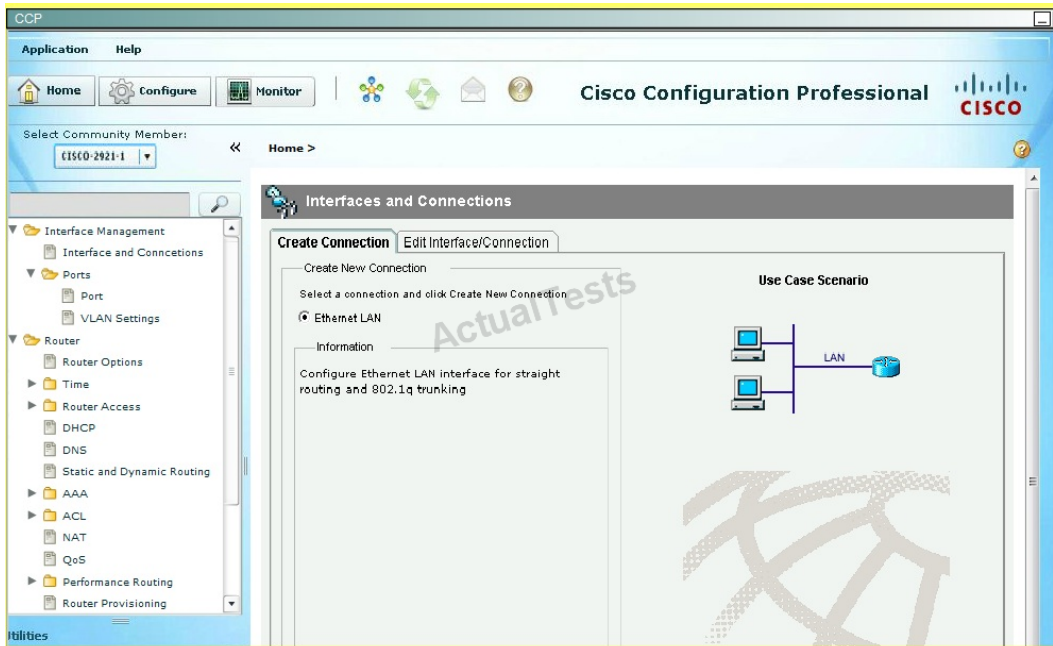
Software Upgrade

Configuration Editor

Save Configuration to PC

Write to Startup Configuration

Telnet



Question 5

Which policy is assigned to Zone Pair sdm-zp-OUT-IN?

- ☐ sdm-cls-http
- ☐ OUT_SERVICE
- ☐ ccp-policy-ccp-cls-1
- ☐ ccp-policy-ccp-cls-2

Answer:

Question 5

Which policy is assigned to Zone Pair sdm-zp-OUT-IN?

- ☐ sdm-cls-http
- ☐ OUT_SERVICE
- ☐ ccp-policy-ccp-cls-1
- ☒ ccp-policy-ccp-cls-2

Explanation:**Question 5**

Which policy is assigned to Zone Pair sdm-zp-OUT-IN?

- ☐ sdm-cls-http
- ☐ OUT_SERVICE
- ☐ ccp-policy-ccp-cls-1
- ☒ ccp-policy-ccp-cls-2

QUESTION NO: 117 DRAG DROP

Drag each AAA function from the left and drop it on the protocol that it corresponds to on the right.

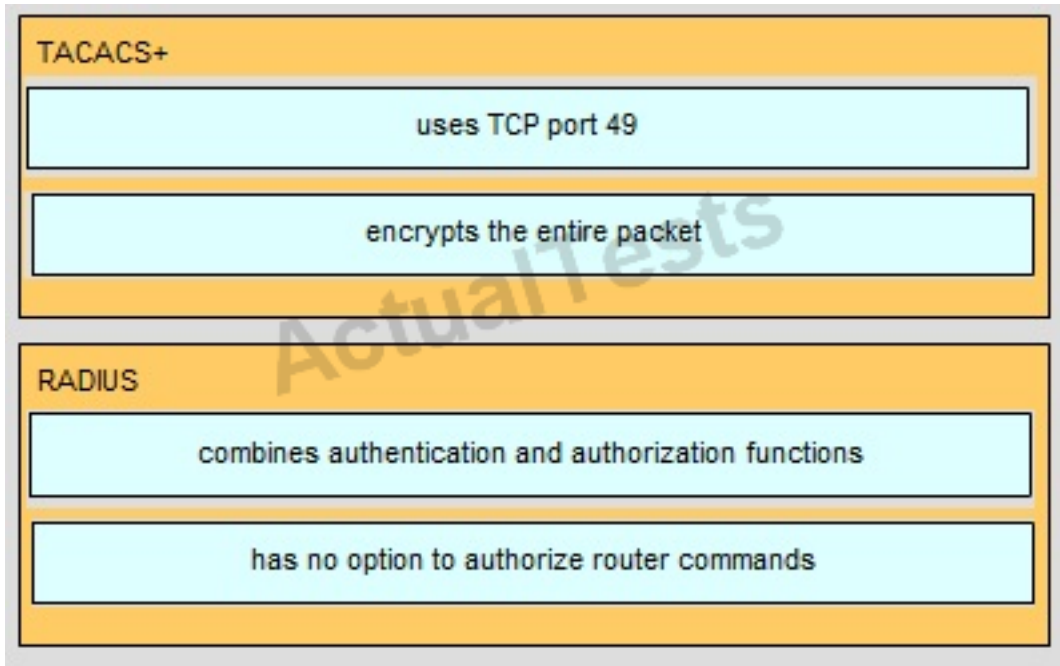
has no option to authorize router commands	TACACS+
encrypts the entire packet	
combines authentication and authorization functions	
uses TCP port 49	
	RADIUS

Answer:

Drag each AAA function from the left and drop it on the protocol that it corresponds to on the right.

has no option to authorize router commands	TACACS+
encrypts the entire packet	uses TCP port 49
combines authentication and authorization functions	encrypts the entire packet
uses TCP port 49	
	RADIUS
	combines authentication and authorization functions
	has no option to authorize router commands

Explanation:

**QUESTION NO: 118 DRAG DROP**

Drag the IKE steps or modes from the left and drop them on the correct categories on the right.

IKE Steps or Modes	IKEv1 Phase 1	IKEv1 Phase 2
quick mode	Target	Target
supports main or aggressive mode	Target	Target
negotiates the IKE policy	Target	Target
establishes the IPsec SAs	Target	Target
authenticates the peer using PSK or digital certificate	Target	Target
negotiates the IPsec security parameters	Target	Target
uses DH during the second message exchanges	Target	Target
can optionally perform additional DH exchanges	Target	Target

Answer:

Drag the IKE steps or modes from the left and drop them on the correct categories on the right.

IKE Steps or Modes (Left)	IKEv1 Phase 1	IKEv1 Phase 2
quick mode	supports main or aggressive mode	quick mode
supports main or aggressive mode	negotiates the IKE policy	establishes the IPsec SAs
negotiates the IKE policy	authenticates the peer using PSK or digital certificate	negotiates the IPsec security parameters
establishes the IPsec SAs	uses DH during the second message exchanges	can optionally perform additional DH exchanges
authenticates the peer using PSK or digital certificate		
negotiates the IPsec security parameters		
uses DH during the second message exchanges		
can optionally perform additional DH exchanges		

Explanation:

IKEv1 Phase 1

- supports main or aggressive mode
- negotiates the IKE policy
- authenticates the peer using PSK or digital certificate
- uses DH during the second message exchanges

IKEv1 Phase 2

- quick mode
- establishes the IPsec SAs
- negotiates the IPsec security parameters
- can optionally perform additional DH exchanges

QUESTION NO: 119 DRAG DROP

Drag the items from the left that are part of a secure network lifecycle and drop them in the spaces on the right. Not all items are used.

initiation	Target
implementation	Target
acquisition and development	Target
disposition	Target
staff roles and responsibilities	Target
operations and management	
incident response policy	

Answer:

Drag the items from the left that are part of a secure network lifecycle and drop them in the spaces on the right. Not all items are used.

initiation	initiation
implementation	
acquisition and development	acquisition and development
disposition	implementation
staff roles and responsibilities	operations and management
operations and management	disposition
incident response policy	

Explanation:

1. Initiation
2. Acquisition and development
3. Implementation
4. Operations and maintenance
5. Disposition

Secure Network Life Cycle

By framing security within the context of IT governance, compliance, and risk management, and by building it with a sound security architecture at its core, the result is usually a less expensive and more effective process. Including security early in the information process within the system design life cycle (SDLC) usually results in less-expensive and more-effective security when compared to adding it to an operational system.

A general SDLC includes five phases:

1. Initiation
2. Acquisition and development
3. Implementation
4. Operations and maintenance

5. Disposition

Each of these five phases includes a minimum set of security steps that you need to follow to effectively incorporate security into a system during its development. An organization either uses the general SDLC or develops a tailored SDLC that meets its specific needs. In either case, the National Institute of Standards and Technology (NIST) recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process.

QUESTION NO: 120 DRAG DROP

Drag the disaster recovery concepts from the left and drop them on their definitions on the right.

recovery point objective	the age of the data you want the ability to recover in event of a system outage
maximum tolerable downtime	the amount of downtime accepted for a system resource outage
recovery time objective	the amount of downtime accepted for a mission-critical business process outage

Answer:

Drag the disaster recovery concepts from the left and drop them on their definitions on the right.

recovery point objective	recovery point objective
maximum tolerable downtime	recovery time objective
recovery time objective	maximum tolerable downtime

Explanation:

recovery point objective
recovery time objective
maximum tolerable downtime

QUESTION NO: 121 DRAG DROP

Drag the items from the left and drop them on their functions on the right.

control plane	secures transit traffic through the router
data plane	secures router access
management plane	secures traffic destined to the router itself

Answer:

Drag the items from the left and drop them on their functions on the right.

control plane	data plane
data plane	management plane
management plane	control plane

Explanation:

data plane
management plane
control plane

QUESTION NO: 122 DRAG DROP

Drag the characteristics of a static packet filter firewall rule and drop them on the right. Not all characteristics are used.

can permit or deny traffic based on IP address	Target
maintains connection state	Target
can permit or deny traffic based on protocol	Target
can permit or deny traffic based on source and destination ports	
can dynamically filter traffic based on port negotiations	
can permit or deny traffic based on fragmented packets	

Answer:

Drag the characteristics of a static packet filter firewall rule and drop them on the right. Not all characteristics are used.

can permit or deny traffic based on IP address	can permit or deny traffic based on IP address
maintains connection state	can permit or deny traffic based on source and destination ports
can permit or deny traffic based on protocol	can permit or deny traffic based on protocol
can permit or deny traffic based on source and destination ports	
can dynamically filter traffic based on port negotiations	
can permit or deny traffic based on fragmented packets	

Explanation:

can permit or deny traffic based on IP address

can permit or deny traffic based on source and destination ports

can permit or deny traffic based on protocol

QUESTION NO: 123 DRAG DROP

Drag the CLI configuration steps to implement a zone-based policy firewall from the left and drop them in the correct order on the right.

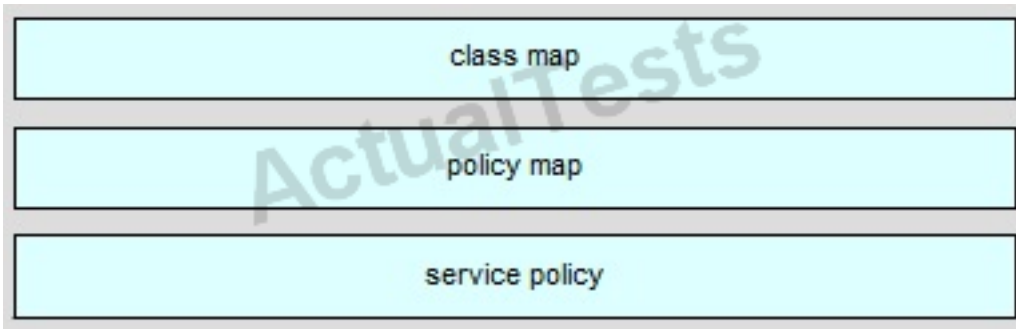
policy map	Target
service policy	Target
class map	Target

Answer:

Drag the CLI configuration steps to implement a zone-based policy firewall from the left and drop them in the correct order on the right.

policy map	class map
service policy	policy map
class map	service policy

Explanation:

**QUESTION NO: 124 DRAG DROP**

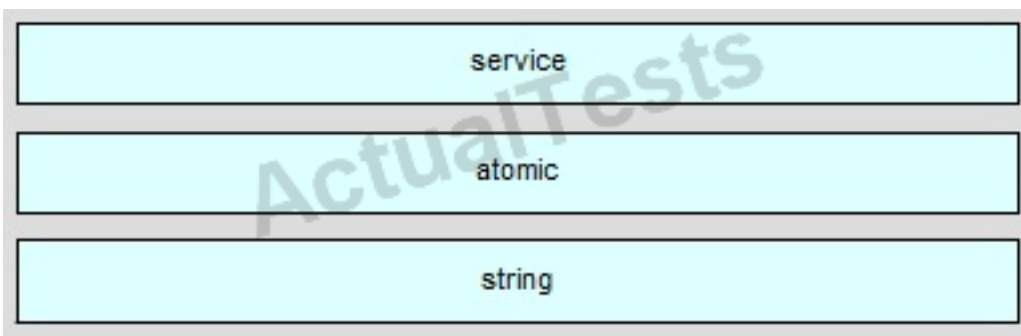
Drag the signature engines from the left and drop them on their characteristics on the right. Not all engines are used.

other	inspects and analyzes things such as HTTP, FTP, and SMTP
string	examines simple packets
atomic	uses regular expression-based pattern inspection
multi-string	
service	

Answer:

Drag the signature engines from the left and drop them on their characteristics on the right. Not all engines are used.

other	service
string	atomic
atomic	string
multi-string	
service	

Explanation:

QUESTION NO: 125

Which statement is true when you have generated RSA keys on your Cisco router to prepare for secure device management?

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

Answer: B

Explanation:

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

Generate an RSA key pair for your router, which automatically enables SSH. carter(config)#crypto key generate rsa

Refer to crypto key generate rsa - Cisco IOS Security Command Reference, Release 12.3 for more information on the usage of this command.

QUESTION NO: 126

What is the key 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. Network-based IPS provides better protection against OS kernel-level attacks against hosts and servers.
- 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 can work in promiscuous mode or inline mode.
- E. Host-based IPS is more scalable than network-based IPS.
- F. Host-based IPS deployment requires less planning than network-based IPS.

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2.1/8_NIDS.

html

Cisco Network-Based Intrusion Detection—Functionalities and Configuration

This chapter highlights the need for and the benefits of deploying network-based intrusion detection in the data center. It addresses mitigation techniques, deployment models, and the management of the infrastructure.

Intrusion detection systems help data centers and other computer installations prepare for and deal with electronic attacks. Usually deployed as a component of a security infrastructure with a set of security policies for a larger, comprehensive information system, the detection systems themselves are of two main types.

Network-based systems inspect traffic "on the wire" and host-based systems monitor only individual computer server traffic.

Network intrusion detection systems deployed at several points within a single network topology, together with host-based intrusion detection systems and firewalls, can provide a solid, multi-pronged defense against both outside, Internet-based attacks, and internal threats, including network misconfiguration, misuse, or negligent practices. The Cisco Intrusion Detection System (IDS) product line provides flexible solutions for data center security.

QUESTION NO: 127

Refer to the exhibit.

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

You are a network manager for your organization. You are looking at your Syslog server reports. Based on the Syslog message shown, which two statements are true? (Choose two.)

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

Answer: A,D

Explanation:

http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/swlog.html

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Messages appear in this format:

seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)

The part of the message preceding the percent sign depends on the setting of the service sequence-numbers, service timestamps log datetime, service timestamps log datetime [localtime] [msec] [show-timezone], or service timestamps log uptime global configuration command.

seq no:

Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured.

For more information, see the "Enabling and Disabling Sequence Numbers in Log Messages" section.

timestamp formats:

mm/dd hh:mm:ss

or

hh:mm:ss (short uptime)

or

d h (long uptime)

Date and time of the message or event. This information appears only if the service timestamps log [datetime | log] global configuration command is configured.

For more information, see the "Enabling and Disabling Time Stamps on Log Messages" section.

facility
The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 29-4.

severity
Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 29-3.

MNEMONIC

Text string that uniquely describes the message.

description

Text string containing detailed information about the event being reported.

http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/swlog.html

This example shows part of a logging display with the service timestamps log datetime global configuration command enabled:

*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) (Switch-2)

QUESTION NO: 128

Refer to the exhibit.

```
router# 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.

Which statement is correct based on the show login command output shown?

- A. 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.
- B. The login block-for command is configured to block login hosts for 93 seconds.
- C. All logins from any sources are blocked for another 193 seconds.
- D. Three or more login requests have failed within the last 100 seconds.

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_login_enhance_ps6922_TSD_Products_Configuration_Guide_Chapter.html

Showing login Parameters: Example

The following sample output from the show login command verifies that the router is in quiet mode. In this example, the login block-for command was configured to block login hosts for 100 seconds if 3 or more login requests fail within 100 seconds.

```
Router# 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.

QUESTION NO: 129

Which four methods are used by hackers? (Choose four.)

- A. footprint analysis attack
- B. privilege escalation attack
- C. buffer Unicode attack
- D. front door attacks
- E. social engineering attack
- F. Trojan horse attack

Answer: A,B,E,F

Explanation:

[https://learningnetwork.cisco.com/servlet/JiveServlet/download/15823-1-57665/CCNA%20Security%20\(640-554\)%20Portable%20Command%20Guide_ch01.pdf](https://learningnetwork.cisco.com/servlet/JiveServlet/download/15823-1-57665/CCNA%20Security%20(640-554)%20Portable%20Command%20Guide_ch01.pdf)

Thinking Like a Hacker

The following seven steps may be taken to compromise targets and applications:

Step 1 Perform footprint analysis

Hackers generally try to build a complete profile of a target company's security posture using a broad range of easily available tools and techniques. They can discover organizational domain names, network blocks, IP addresses of systems, ports, services that are used, and more.

Step 2 Enumerate applications and operating systems

Special readily available tools are used to discover additional target information. Ping sweeps use Internet Control Message Protocol (ICMP) to discover devices on a network. Port scans discover TCP/UDP port status.

Other tools include Netcat, Microsoft EPDump and Remote Procedure Call (RPC) Dump, GetMAC, and software development kits (SDKs).

Step 3 Manipulate users to gain access

Social engineering techniques may be used to manipulate target employees to acquire passwords. They may call or email them and try to convince them to reveal passwords without raising any concern or suspicion.

Step 4 Escalate privileges

To escalate their privileges, a hacker may attempt to use Trojan horse programs and get target users to unknowingly copy malicious code to their corporate system.

Step 5 Gather additional passwords and secrets

With escalated privileges, hackers may use tools such as the pwdump and LSADump applications to gather passwords from machines running Windows.

Step 6 Install back doors

Hacker may attempt to enter through the "front door," or they may use "back doors" into the system. The backdoor method means bypassing normal authentication while attempting to remain undetected. A common backdoor point is a listening port that provides remote access to the system.

Step 7 Leverage the compromised system

After hackers gain administrative access, they attempt to hack other systems.

QUESTION NO: 130

Which statement about Cisco IOS IPS on Cisco IOS Release 12.4(11)T and later is true?

- A. uses Cisco IPS 5.x signature format
- B. requires the Basic or Advanced Signature Definition File
- C. supports both inline and promiscuous mode
- D. requires IEV for monitoring Cisco IPS alerts
- E. uses the built-in signatures that come with the Cisco IOS image as backup
- F. supports SDEE, SYSLOG, and SNMP for sending Cisco IPS alerts

Answer: A

Explanation:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_ios_ips/configuration/12-4t/sec-ips5-sig-fsue.html

Signature Categories

Cisco IPS appliances and Cisco IOS IPS with Cisco 5.x format signatures operate with signature categories.

All signatures are pregrouped into categories; the categories are hierarchical. An individual signature can belong to more than one category. Top-level categories help to define general types of signatures.

Subcategories exist beneath each top-level signature category. (For a list of supported top-level categories, use your router CLI help (?).)

Router Configuration Files and Signature Event Action Processor (SEAP)

As of Cisco IOS Release 12.4(11)T, SDFs are no longer used by Cisco IOS IPS. Instead, routers access signature definition information through a directory that contains three configuration files--the default configuration, the delta configuration, and the SEAP configuration. Cisco IOS accesses this directory through the `ip ips config location` command.

QUESTION NO: 131

Which characteristic is the foundation of Cisco Self-Defending Network technology?

- A. secure connectivity

- B. threat control and containment
- C. policy management
- D. secure network platform

Answer: D

Explanation:

http://www.cisco.com/en/US/solutions/ns170/networking_products_genericcontent0900aecd8051f378.html

Create a Stronger Defense Against Threats

Each day, you reinvent how you conduct business by adopting Internet-based business models. But Internet connectivity without appropriate security can compromise the gains you hope to make. In today's connected environment, outbreaks spread globally in a matter of minutes, which means your security systems must react instantly.

Maintaining security using tactical, point solutions introduces complexity and inconsistency, but integrating security throughout the network protects the information that resides on it.

Three components are critical to effective information security:

- A secure network platform with integrated security to which you can easily add advanced security technologies and services
- Threat control services focused on antivirus protection and policy enforcement that continuously monitor network activity and prevent or mitigate problems
- Secure communication services that maintain the privacy and confidentiality of sensitive data, voice, video, and wireless communications while cost-effectively extending the reach of your network

QUESTION NO: 132

Which kind of table do most firewalls use today to keep track of the connections through the firewall?

- A. dynamic ACL
- B. reflexive ACL
- C. netflow
- D. queuing
- E. state
- F. express forwarding

Answer: E

Explanation:

<http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/intro.html>

Stateful Inspection Overview

All traffic that goes through the ASA is inspected using the Adaptive Security Algorithm and either allowed through or dropped. A simple packet filter can check for the correct source address, destination address, and ports, but it does not check that the packet sequence or flags are correct. A filter also checks every packet against the filter, which can be a slow process.

A stateful firewall like the ASA, however, takes into consideration the state of a packet:

- Is this a new connection?

If it is a new connection, the ASA has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the "session management path," and depending on the type of traffic, it might also pass through the "control plane path."

The session management path is responsible for the following tasks:

- Performing the access list checks
- Performing route lookups
- Allocating NAT translations (xlates)
- Establishing sessions in the "fast path"

The ASA creates forward and reverse flows in the fast path for TCP traffic; the ASA also creates connection state information for connectionless protocols like UDP, ICMP (when you enable ICMP inspection), so that they can also use the fast path.

Some packets that require Layer 7 inspection (the packet payload must be inspected or altered) are passed on to the control plane path. Layer 7 inspection engines are required for protocols that have two or more channels:

A data channel, which uses well-known port numbers, and a control channel, which uses different port numbers for each session. These protocols include FTP, H.323, and SNMP.

- Is this an established connection?

If the connection is already established, the ASA does not need to re-check packets; most matching packets can go through the "fast" path in both directions. The fast path is responsible for the following tasks:

- IP checksum verification
- Session lookup
- TCP sequence number check
- NAT translations based on existing sessions
- Layer 3 and Layer 4 header adjustments

Data packets for protocols that require Layer 7 inspection can also go through the fast path.

Some established session packets must continue to go through the session management path or the control plane path. Packets that go through the session management path include HTTP packets that require inspection or content filtering. Packets that go through the control plane path include the control packets for protocols that require Layer 7 inspection.

QUESTION NO: 133

Which Cisco IOS command is used to verify that either the Cisco IOS image, the configuration files, or both have been properly backed up and secured?

- A. show archive
- B. show secure bootset
- C. show flash
- D. show file systems
- E. dir
- F. dir archive

Answer: B

Explanation:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_resil_config_ps6922_TSD_Products_Configuration_Guide_Chapter.html

Restrictions for Cisco IOS Resilient Configuration

- This feature is available only on platforms that support a Personal Computer Memory Card International Association (PCMCIA) Advanced Technology Attachment (ATA) disk. There must be enough space on the storage device to accommodate at least one Cisco IOS image (two for upgrades) and a copy of the running configuration. IOS File System (IFS) support for secure file systems is also needed by the software.
- It may be possible to force removal of secured files using an older version of Cisco IOS software that does not contain file system support for hidden files.
- This feature can be disabled only by using a console connection to the router. With the exception of the upgrade scenario, feature activation does not require console access.
- You cannot secure a bootset with an image loaded from the network. The running image must be loaded from persistent storage to be secured as primary.
- Secured files will not appear on the output of a dir command issued from an executive shell because the IFS prevents secure files in a directory from being listed. ROM monitor (ROMMON) mode does not have any such restriction and can be used to list and boot secured files. The running image and running configuration archives will not be visible in the Cisco IOS dir command output. Instead, use the show secure bootset command to verify archive existence.

QUESTION NO: 134

What does the secure boot-config global configuration accomplish?

- A. enables Cisco IOS image resilience

- B. backs up the Cisco IOS image from flash to a TFTP server
- C. takes a snapshot of the router running configuration and securely archives it in persistent storage
- D. backs up the router running configuration to a TFTP server
- E. stores a secured copy of the Cisco IOS image in its persistent storage

Answer: C

Explanation:

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 NO: 135

Refer to the exhibit.

```

Class-map: TEST-Class (match-all)
  Match: access-group 110
  Match: protocol http
  Inspect
    Established Sessions
      Session 643BCF8S (10.0.2.12:3364)=>(172.26.26.51:80) http SIS_OPEN
        Created 00:00:10, Last heard 00:00:00
        Bytes sent (initiator:responder) [1268:64324]
      Session 643BB9C8 (10.0.2.12:3361)=>(172.26.26.51:80) http SIS_OPEN
        Created 00:00:16, Last heard 00:00:06
        Bytes sent (initiator:responder) [2734:38447]
      Session 643BD240 (10.0.2.12:3362)=>(172.26.26.51:80) http SIS_OPEN
        Created 00:00:14, Last heard 00:00:07
        Bytes sent (initiator:responder) [2219:39813]
      Session 643BBF38 (10.0.2.12:3363)=>(172.26.26.51:80) http SIS_OPEN
        Created 00:00:14, Last heard 00:00:06
        Bytes sent (initiator:responder) [2106:19895]
  Class-map: class-default (match-any)
    Match: any
    Drop (default action)
      58 packets, 2104 bytes

```

Based on the show policy-map type inspect zone-pair session command output shown, what can be determined about this Cisco IOS zone based firewall policy?

- A. All packets will be dropped since the class-default traffic class is matching all traffic.
- B. This is an inbound policy (applied to traffic sourced from the less secured zone destined to the more secured zone).
- C. This is an outbound policy (applied to traffic sourced from the more secured zone destined to the less secured zone).
- D. Stateful packet inspection will be applied only to HTTP packets that also match ACL 110.
- E. All non-HTTP traffic will be permitted to pass as long as it matches ACL 110.
- F. All non-HTTP traffic will be inspected.

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_m1.html

Match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the match access-group command in class-map configuration mode. To remove ACL match criteria from a class map, use the no form of this command.

```
match access-group {access-group | name access-group-name}
```

```
no match access-group access-group
```

```
match protocol
```

To configure the match criterion for a class map on the basis of a specified protocol, use the match protocol command in class-map configuration mode. To remove the protocol-based match

criterion from the class map, use the no form of this command.
Match protocol protocol-name no match protocol protocol-name

QUESTION NO: 136

When using a stateful firewall, which information is stored in the stateful session flow table?

- A. the outbound and inbound access rules (ACL entries)
- B. the source and destination IP addresses, port numbers, TCP sequencing information, and additional flags for each TCP or UDP connection associated with a particular session
- C. all TCP and UDP header information only
- D. all TCP SYN packets and the associated return ACK packets only
- E. the inside private IP address and the translated inside global IP address

Answer: B

Explanation:

<http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/intro.html>

Stateful Inspection Overview

All traffic that goes through the ASA is inspected using the Adaptive Security Algorithm and either allowed through or dropped. A simple packet filter can check for the correct source address, destination address, and ports, but it does not check that the packet sequence or flags are correct. A filter also checks every packet against the filter, which can be a slow process.

A stateful firewall like the ASA, however, takes into consideration the state of a packet:

- Is this a new connection?

If it is a new connection, the ASA has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the "session management path," and depending on the type of traffic, it might also pass through the "control plane path."

The session management path is responsible for the following tasks:

- Performing the access list checks
- Performing route lookups
- Allocating NAT translations (xlates)
- Establishing sessions in the "fast path"

The ASA creates forward and reverse flows in the fast path for TCP traffic; the ASA also creates connection state information for connectionless protocols like UDP, ICMP (when you enable ICMP inspection), so that they can also use the fast path.

Some packets that require Layer 7 inspection (the packet payload must be inspected or altered) are passed on to the control plane path. Layer 7 inspection engines are required for protocols that

have two or more channels:

A data channel, which uses well-known port numbers, and a control channel, which uses different port numbers for each session. These protocols include FTP, H.323, and SNMP.

- Is this an established connection?

If the connection is already established, the ASA does not need to re-check packets; most matching packets can go through the "fast" path in both directions. The fast path is responsible for the following tasks:

- IP checksum verification
- Session lookup
- TCP sequence number check
- NAT translations based on existing sessions
- Layer 3 and Layer 4 header adjustments

Data packets for protocols that require Layer 7 inspection can also go through the fast path.

Some established session packets must continue to go through the session management path or the control plane path. Packets that go through the session management path include HTTP packets that require inspection or content filtering. Packets that go through the control plane path include the control packets for protocols that require Layer 7 inspection.

QUESTION NO: 137

Which statement is true about configuring access control lists to control Telnet traffic destined to the router itself?

- A. The ACL is applied to the Telnet port with the ip access-group command.
- B. The ACL should be applied to all vty lines in the in direction to prevent an unwanted user from connecting to an unsecured port.
- C. The ACL applied to the vty lines has no in or out option like ACL being applied to an interface.
- D. The ACL must be applied to each vty line individually.

Answer: B

Explanation:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/12-4t/sec-cntrl-acc-vtl.html

Controlling Access to a Virtual Terminal Line

You can control who can access the virtual terminal lines (vty) to a router by applying an access list to inbound vtys. You can also control the destinations that the vtys from a router can reach by applying an access list to outbound vtys.

Benefits of Controlling Access to a Virtual Terminal Line

By applying an access list to an inbound vty, you can control who can access the lines to a router. By applying an access list to an outbound vty, you can control the destinations that the lines from a router can reach.

QUESTION NO: 138

When configuring role-based CLI on a Cisco router, which step is performed first?

- A. Log in to the router as the root user.
- B. Create a parser view called "root view."
- C. Enable role-based CLI globally on the router using the privileged EXEC mode Cisco IOS command.
- D. Enable the root view on the router.
- E. Enable AAA authentication and authorization using the local database.
- F. Create a root local user in the local database.

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html

Role-Based CLI Access

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

Configuring a CLI View

Prerequisites

Before you create a view, you must perform the following tasks:

- Enable AAA via the `aaa new-model` command. (For more information on enabling AAA, see the chapter

"Configuring Authentication" in the Cisco IOS Security Configuration Guide, Release 12.3.

- Ensure that your system is in root view—not privilege level 15.

SUMMARY STEPS

1. enable view
2. configure terminal
3. parser view view-name
4. secret 5 encrypted-password

5. commands parser-mode {include | include-exclusive | exclude} [all] [interface interface-name | command]
6. exit
7. exit
8. enable [privilege-level] [view view-name]
9. show parser view [all]

DETAILED STEPS

Step 1

Enable view

Router> enable view

Enables root view.

QUESTION NO: 139

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.

Answer: B

Explanation:

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 NO: 140

Which characteristic is a potential security weakness of a traditional stateful firewall?

- A. It cannot support UDP flows.
- B. It cannot detect application-layer attacks.
- C. It cannot ensure each TCP connection follows a legitimate TCP three-way handshake.
- D. It works only in promiscuous mode.
- E. The status of TCP sessions is retained in the state table after the sessions terminate.
- F. It has low performance due to the use of syn-cookies.

Answer: B

Explanation:

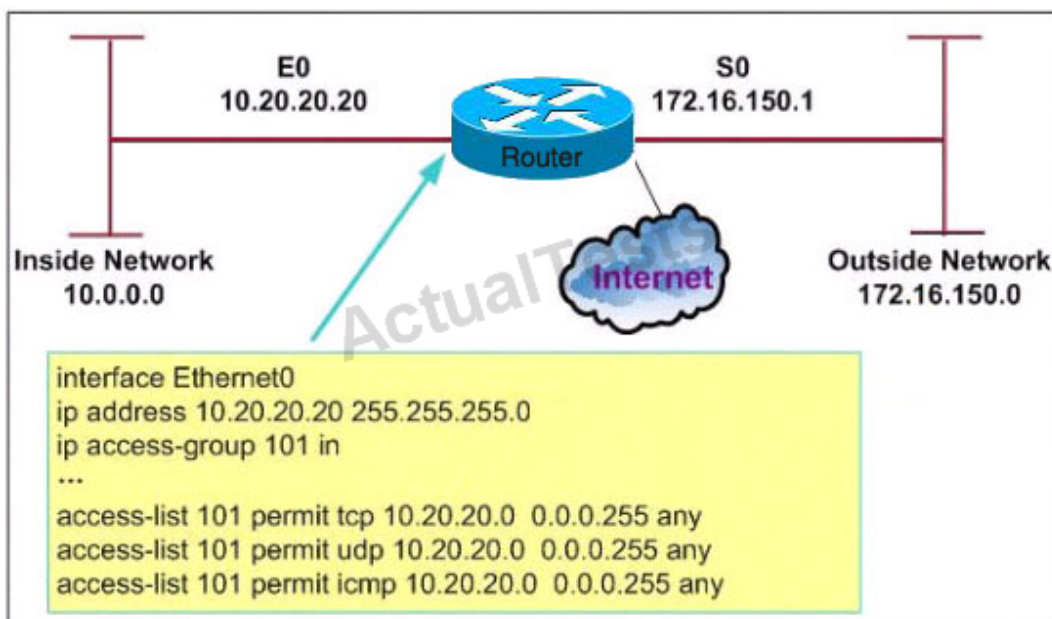
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/product_implementation_design_guide09186a00800fd670.html

Cisco IOS Firewall consists of several major subsystems:

- Stateful Packet Inspection provides a granular firewall engine
- Authentication Proxy offers a per-host access control mechanism
- Application Inspection features add protocol conformance checking and network use policy control Enhancements to these features extend these capabilities to VRF instances to support multiple virtual routers per device, and to Cisco Integrated Route-Bridging features to allow greater deployment flexibility, reduce implementation timelines, and ease requirements to add security to existing networks.

QUESTION NO: 141

Refer to the exhibit and partial configuration.



Which statement is true?

- A. All traffic destined for network 172.16.150.0 will be denied due to the implicit deny all.
- B. All traffic from network 10.0.0.0 will be permitted.
- C. Access-list 101 will prevent address spoofing from interface E0.
- D. This is a misconfigured ACL resulting in traffic not being allowed into the router in interface S0.
- E. This ACL will prevent any host on the Internet from spoofing the inside network address as the source address for packets coming into the router from the Internet.

Answer: C

Explanation:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

Transit ACL Sections

In general, a transit ACL is composed of four sections.

Special-use address and anti-spoofing entries that deny illegitimate sources and packets with source addresses that belong within your network from entering the network from an external source NotE. RFC 1918 leavingcisco.com defines reserved address space that is not a valid source address on the Internet. RFC 3330 leavingcisco.com defines special-use addresses that might require filtering. RFC 2827 leavingcisco.com provides anti-spoofing guidelines.

Explicitly permitted return traffic for internal connections to the Internet

Explicitly permitted externally sourced traffic destined to protected internal addresses

Explicit deny statement NotE. Although all ACLs contain an implicit deny statement, Cisco recommends use of an explicit deny statement, for example, deny ip any any. On most platforms, such statements maintain a count of the number of denied packets that can be displayed using the show access-list command.

QUESTION NO: 142

What will be disabled as a result of the no service password-recovery command?

- A. changes to the config-register setting
- B. ROMMON
- C. password encryption service
- D. aaa new-model global configuration command
- E. the xmodem privilege EXEC mode command to recover the Cisco IOS image

Answer: B

Explanation:

http://www.cisco.com/en/US/products/hw/routers/ps274/products_configuration_example09186a00801d8113.shtml

Background

ROMMON security is designed not to allow a person with physical access to the router view the configuration file. ROMMON security disables access to the ROMMON, so that a person cannot set the configuration register to ignore the start-up configuration. ROMMON security is enabled when the router is configured with the no service password-recovery command.

Caution: Because password recovery that uses ROMMON security destroys the configuration, it is

recommended that you save the router configuration somewhere off the router, such as on a TFTP server.

Risks

If a router is configured with the `no service password-recovery` command, this disables all access to the ROMMON. If there is no valid Cisco IOS software image in the Flash memory of the router, the user is not able to use the ROMMON XMODEM command in order to load a new Flash image. In order to fix the router, you must get a new Cisco IOS software image on a Flash SIMM, or on a PCMCIA card, for example on the 3600 Series Routers.

In order to minimize this risk, a customer who uses ROMMON security must also use dual Flash bank memory and put a backup Cisco IOS software image in a separate partition.

QUESTION NO: 143

What does the MD5 algorithm do?

- A. takes a message less than 2^{64} bits as input and produces a 160-bit message digest
- B. takes a variable-length message and produces a 168-bit message digest
- C. takes a variable-length message and produces a 128-bit message digest
- D. takes a fixed-length message and produces a 128-bit message digest

Answer: C

Explanation:

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094203.shtml

Message Digest 5 (MD5)—This is a one way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4, which is designed to strengthen the security of this hashing algorithm. SHA is more secure than MD4 and MD5. Cisco uses hashes for authentication within the IPsec framework.

QUESTION NO: 144

You have configured a standard access control list on a router and applied it to interface Serial 0 in an outbound direction. No ACL is applied to Interface Serial 1 on the same router. What happens when traffic being filtered by the access list does not match the configured ACL statements for Serial 0?

- A. The resulting action is determined by the destination IP address.
- B. The resulting action is determined by the destination IP address and port number.
- C. The source IP address is checked, and, if a match is not found, traffic is routed out interface Serial 1.
- D. The traffic is dropped.

Answer: D

Explanation:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml

Introduction

This document provides sample configurations for commonly used IP Access Control Lists (ACLs), which filter

IP packets based on:

Source address

Destination address

Type of packet

Any combination of these items

In order to filter network traffic, ACLs control whether routed packets are forwarded or blocked at the router interface. Your router examines each packet to determine whether to forward or drop the packet based on the criteria that you specify within the ACL. ACL criteria include:

Source address of the traffic

Destination address of the traffic

Upper-layer protocol

Complete these steps to construct an ACL as the examples in this document show:

Create an ACL.

Apply the ACL to an interface.

The IP ACL is a sequential collection of permit and deny conditions that applies to an IP packet.

The router tests packets against the conditions in the ACL one at a time.

The first match determines whether the Cisco IOS® Software accepts or rejects the packet.

Because the Cisco IOS Software stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the router rejects the packet because of an implicit deny all clause.

QUESTION NO: 145

In a brute-force attack, what percentage of the keyspace must an attacker generally search through until he or she finds the key that decrypts the data?

- A. Roughly 50 percent
- B. Roughly 66 percent
- C. Roughly 75 percent
- D. Roughly 10 percent

Answer: A

Explanation:

QUESTION NO: 146

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

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

Answer: A,B,D

Explanation:

QUESTION NO: 147

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

Answer: A

Explanation: Explanation

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 NO: 148

Information about a managed device's resources and activity is defined by a series of objects. What defines the structure of these management objects?

- A. MIB
- B. FIB
- C. LDAP
- D. CEF

Answer: A

Explanation: Explanation

Management Information Base (MIB) is the database of configuration variables that resides on the networking device.

QUESTION NO: 149

Refer to Cisco IOS Zone-Based Policy Firewall, where will the inspection policy be applied?

- A. to the zone-pair
- B. to the zone
- C. to the interface
- D. to the global service policy

Answer: A

Explanation:

QUESTION NO: 150

Which statement is true about vishing?

- A. Influencing users to forward a call to a toll number (for example, a long distance or international number)
- B. Influencing users to provide personal information over a web page
- C. Using an inside facilitator to intentionally forward a call to a toll number (for example, a long distance or international number)
- D. Influencing users to provide personal information over the phone

Answer: D

Explanation:

Explanation

Vishing (voice phishing) uses telephony to glean information, such as account details, directly from users. Because many users tend to trust the security of a telephone versus the security of the web, some users are more likely to provide confidential information over the telephone. User education is the most effective method to combat vishing attacks.

QUESTION NO: 151

Which item is the great majority of software vulnerabilities that have been discovered?

- A. Stack vulnerabilities
- B. Heap overflows
- C. Software overflows
- D. Buffer overflows

Answer: D

Explanation:

QUESTION NO: 152

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

Answer: B

Explanation:

QUESTION NO: 153

In which two modes can Cisco Configuration Professional Security Audit operate? (Choose two.)

- A. Security Audit wizard
- B. Lockdown
- C. One-Step Lockdown
- D. AutoSecure

Answer: A,C

Explanation:

QUESTION NO: 154

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.

Answer: A,C,D

Explanation:

QUESTION NO: 155

Which statement about Control Plane Policing is true?

- A. Control Plane Policing allows QoS filtering to protect the control plane against DoS attacks.
- B. Control Plane Policing classifies traffic into three categories to intercept malicious traffic.
- C. Control Plane Policing allows ACL-based filtering to protect the control plane against DoS attacks.
- D. Control Plane Policing intercepts and classifies all traffic.

Answer: A

Explanation:

QUESTION NO: 156

Which three applications comprise Cisco Security Manager? (Choose three.)

- A. Configuration Manager
- B. Packet Tracer
- C. Device Manager
- D. Event Viewer
- E. Report Manager
- F. Syslog Monitor

Answer: A,D,E

Explanation:

QUESTION NO: 157

When a network transitions from IPv4 to IPv6, how many bits does the address expand to?

- A. 64 bits
- B. 128 bits
- C. 96 bits
- D. 156 bits

Answer: B

Explanation:

QUESTION NO: 158

On which Cisco Configuration Professional screen do you enable AAA?

- A. AAA Summary
- B. AAA Servers and Groups
- C. Authentication Policies
- D. Authorization Policies

Answer: A

Explanation:

QUESTION NO: 159

Under which option do you create a AAA authentication policy in Cisco Configuration Professional?

- A. Authentication Policies
- B. Authentication Policies – Login
- C. AAA Servers and Groups
- D. AAA Summary

Answer: B

Explanation:

QUESTION NO: 160

Which three statements about TACACS+ are true? (Choose three.)

- A. TACACS+ uses TCP port 49.
- B. TACACS+ uses UDP ports 1645 and 1812.
- C. TACACS+ encrypts the entire packet.
- D. TACACS+ encrypts only the password in the Access-Request packet.
- E. TACACS+ is a Cisco proprietary technology.
- F. TACACS+ is an open standard.

Answer: A,C,E

Explanation:

QUESTION NO: 161

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.

Answer: B,D,F

Explanation:

QUESTION NO: 162

Which network security framework is used to set up access control on Cisco Appliances?

- A. RADIUS
- B. AAA
- C. TACACS+
- D. NAS

Answer: B

Explanation:

QUESTION NO: 163

Which two protocols are used in a server-based AAA deployment? (Choose two.)

- A. RADIUS
- B. TACACS+
- C. HTTPS
- D. WCCP
- E. HTTP

Answer: A,B

Explanation:

QUESTION NO: 164

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

Answer: B

Explanation:

QUESTION NO: 165

Which AAA feature can automate record keeping within a network?

- A. TACACS+

- B. authentication
- C. authorization
- D. accounting

Answer: D

Explanation:

QUESTION NO: 166

Which two statements about IPv6 access lists are true? (Choose two).

- A. IPv6 access lists support numbered access lists.
- B. IPv6 access lists support wildcard masks.
- C. IPv6 access lists support standard access lists.
- D. IPv6 access lists support named access lists.
- E. IPv6 access lists support extended access lists.

Answer: D,E

Explanation:

QUESTION NO: 167

Which command enables subnet 192.168.8.4/30 to communicate with subnet 192.168.8.32/27 on IP protocol 50?

- A. permit esp 192.168.8.4 255.255.255.252 192.168.8.32 255.255.255.224
- B. permit esp 192.168.8.4 0.0.0.31 192.168.8.32 0.0.0.31
- C. permit esp 192.168.8.4 255.255.255.252 224.168.8.32 255.255.255.192
- D. permit esp 192.168.8.4 0.0.0.3 192.168.8.32 0.0.0.31

Answer: D

Explanation:

QUESTION NO: 168

Which two types of access lists can be used for sequencing? (Choose two.)

- A. reflexive

- B. standard
- C. dynamic
- D. extended

Answer: B,D

Explanation:

QUESTION NO: 169

Which command will block IP traffic to the destination 172.16.0.1/32?

- A. access-list 101 deny ip host 172.16.0.1 any
- B. access-list 101 deny ip any host 172.16.0.1
- C. access-list 101 deny ip any any
- D. access-list 11 deny host 172.16.0.1

Answer: B

Explanation:

QUESTION NO: 170

Which two considerations about secure network monitoring are important? (Choose two.)

- A. log tampering
- B. encryption algorithm strength
- C. accurate time stamping
- D. off-site storage
- E. Use RADIUS for router commands authorization.
- F. Do not use a loopback interface for device management access.

Answer: A,C

Explanation:

QUESTION NO: 171

Which two countermeasures can mitigate STP root bridge attacks? (Choose two.)

- A. root guard

- B. BPDU filtering
- C. Layer 2 PDU rate limiter
- D. BPDU guard

Answer: A,D

Explanation:

QUESTION NO: 172

Which two countermeasures can mitigate MAC spoofing attacks? (Choose two.)

- A. IP source guard
- B. port security
- C. root guard
- D. BPDU guard

Answer: A,B

Explanation:

QUESTION NO: 173

Which statement correctly describes the function of a private VLAN?

- A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains.
- B. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomains.
- C. A private VLAN enables the creation of multiple VLANs using one broadcast domain.
- D. A private VLAN combines the Layer 2 broadcast domains of many VLANs into one major broadcast domain.

Answer: A

Explanation:

QUESTION NO: 174

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

- A. VoIP hopping
- B. switch spoofing

- C. CAM-table overflow
- D. double tagging

Answer: B,D

Explanation:

QUESTION NO: 175

Which type of attack can be prevented by setting the native VLAN to an unused VLAN?

- A. VLAN-hopping attacks
- B. CAM-table overflow
- C. denial-of-service attacks
- D. MAC-address spoofing

Answer: A

Explanation:

QUESTION NO: 176

What is the purpose of a trunk port?

- A. A trunk port carries traffic for multiple VLANs.
- B. A trunk port connects multiple hubs together to increase bandwidth.
- C. A trunk port separates VLAN broadcast domains.
- D. A trunk port provides a physical link specifically for a VPN.

Answer: A

Explanation:

QUESTION NO: 177

The host A Layer 2 port is configured in VLAN 5 on switch 1, and the host B Layer 2 port is configured in VLAN 10 on switch 1. Which two actions you can take to enable the two hosts to communicate with each other? (Choose two.)

- A. Configure inter-VLAN routing.
- B. Connect the hosts directly through a hub.

- C. Configure switched virtual interfaces.
- D. Connect the hosts directly through a router.

Answer: A,C

Explanation:

QUESTION NO: 178

Which two pieces of information should you acquire before you troubleshoot an STP loop? (Choose two.)

- A. topology of the routed network
- B. topology of the switched network
- C. location of the root bridge
- D. number of switches in the network

Answer: B,C

Explanation:

QUESTION NO: 179

Which two options are symmetric-key algorithms that are recommended by Cisco? (Choose two.)

- A. Twofish
- B. Advanced Encryption Standard
- C. Blowfish
- D. Triple Data Encryption Standard

Answer: B,D

Explanation:

QUESTION NO: 180

Which technology provides an automated digital certificate management system for use with IPsec?

- A. ISAKMP
- B. public key infrastructure

- C. Digital Signature Algorithm
- D. Internet Key Exchange

Answer: B

Explanation:

QUESTION NO: 181

Which two IPsec protocols are used to protect data in motion? (Choose two.)

- A. Encapsulating Security Payload Protocol
- B. Transport Layer Security Protocol
- C. Secure Shell Protocol
- D. Authentication Header Protocol

Answer: A,D

Explanation:

QUESTION NO: 182

On which protocol number does Encapsulating Security Payload operate?

- A. 06
- B. 47
- C. 50
- D. 51

Answer: C

Explanation:

QUESTION NO: 183

On which protocol number does the authentication header operate?

- A. 06
- B. 47
- C. 50
- D. 51

Answer: D**Explanation:****QUESTION NO: 184**

Refer to the exhibit.

ROUTER A	ROUTER B
<pre> crypto isakmp policy 10 encryption aes 256 authentication pre-share group 14 lifetime 180 ! crypto isakmp key ciscoll2213 address 10.0.10.2 ! crypto ipsec transform-set AES esp-aes 256 esp-sha-hmac mode transport ! crypto map MAP 10 ipsec-isakmp set peer 10.0.10.2 set transform-set AES match address 110 ! interface FastEthernet0/0 ip address 192.168.10.1 255.255.255.0 ! interface Serial0/0 10.0.10.1 255.255.255.0 crypto map MAP ! ip route 0.0.0.0 0.0.0.0 Serial0/0 ! access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 </pre>	<pre> crypto isakmp policy 10 encryption aes 256 authentication pre-share group 14 lifetime 180 ! crypto isakmp key ciscoll2213 address 10.0.10.1 ! crypto ipsec transform-set AES esp-aes 256 esp-sha-hmac mode tunnel ! crypto map MAP 10 ipsec-isakmp set peer 10.0.10.1 set transform-set AES match address 110 ! interface FastEthernet0/0 ip address 192.168.20.1 255.255.255.0 ! interface Serial0/0 10.0.10.2 255.255.255.0 crypto map MAP ! ip route 0.0.0.0 0.0.0.0 Serial0/0 ! access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 </pre>

Which two changes must you make to the given IOS site-to-site VPN configuration to enable the routers to form a connection? (Choose two.)

- A. Configure a valid route on Router A.
- B. Configure the access list on Router B to mirror Router A.
- C. Configure Router B's ISAKMP policy to match the policy on Router A.
- D. Configure the tunnel modes on the two routers to match.

Answer: B,D**Explanation:****QUESTION NO: 185**

In an IPsec VPN, what determination does the access list make about VPN traffic?

- A. whether the traffic should be blocked
- B. whether the traffic should be permitted

- C. whether the traffic should be encrypted
- D. the peer to which traffic should be sent

Answer: C

Explanation:

QUESTION NO: 186

Which command verifies phase 2 of an IPsec VPN on a Cisco router?

- A. show crypto map
- B. show crypto ipsec sa
- C. show crypto isakmp sa
- D. show crypto engine connection active

Answer: B

Explanation:

QUESTION NO: 187

You are troubleshooting a Cisco AnyConnect VPN on a firewall and issue the command show webvpn anyconnect. The output shows the message "SSL VPN is not enabled" instead of showing the AnyConnect package. Which action can you take to resolve the problem?

- A. Issue the enable outside command.
- B. Issue the anyconnect enable command.
- C. Issue the enable inside command.
- D. Reinstall the AnyConnect image.

Answer: B