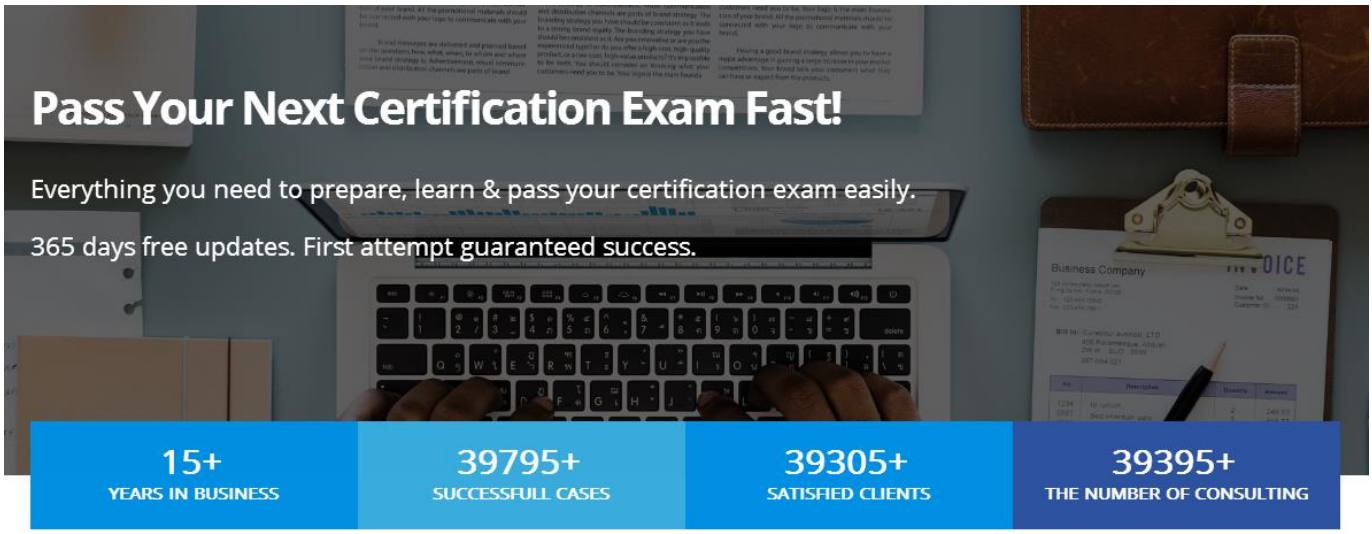
PracticeVCE



TRY BEFORE YOU BUY

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Security & Privacy

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

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

http://www.practicevce.com

Professional Study Tool and Reliable Exam Practice Material

Exam : **640-554**

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

Vendor : Cisco

Version : DEMO

NO.1 Which option describes a function of a virtual VLAN?
A. A virtual VLAN creates a logically partitioned LAN to place switch ports in a separate broadcast domain.
B. A virtual VLAN creates trunks and links two switches together.
C. A virtual VLAN adds every port on a switch to its own collision domain.
D. A virtual VLAN connects many hubs together.
Answer: A

NO.2 Refer to the exhibit.

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

Which statement about the aaa configurations is true?
A. The authentication method list used by the console port is named test.
B. The authentication method list used by the vty port is named test.
C. If the TACACS+ AAA server is not available, no users will be able to establish a Telnet session with the router.
D. If the TACACS+ AAA server is not available, console access to the router can be authenticated using the local database.
E. The local database is checked first when authenticating console and vty access to the router.
Answer: B
Explanation:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a 0080204528.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

NO.3 Which two countermeasures can mitigate STP root bridge attacks? (Choose two.)

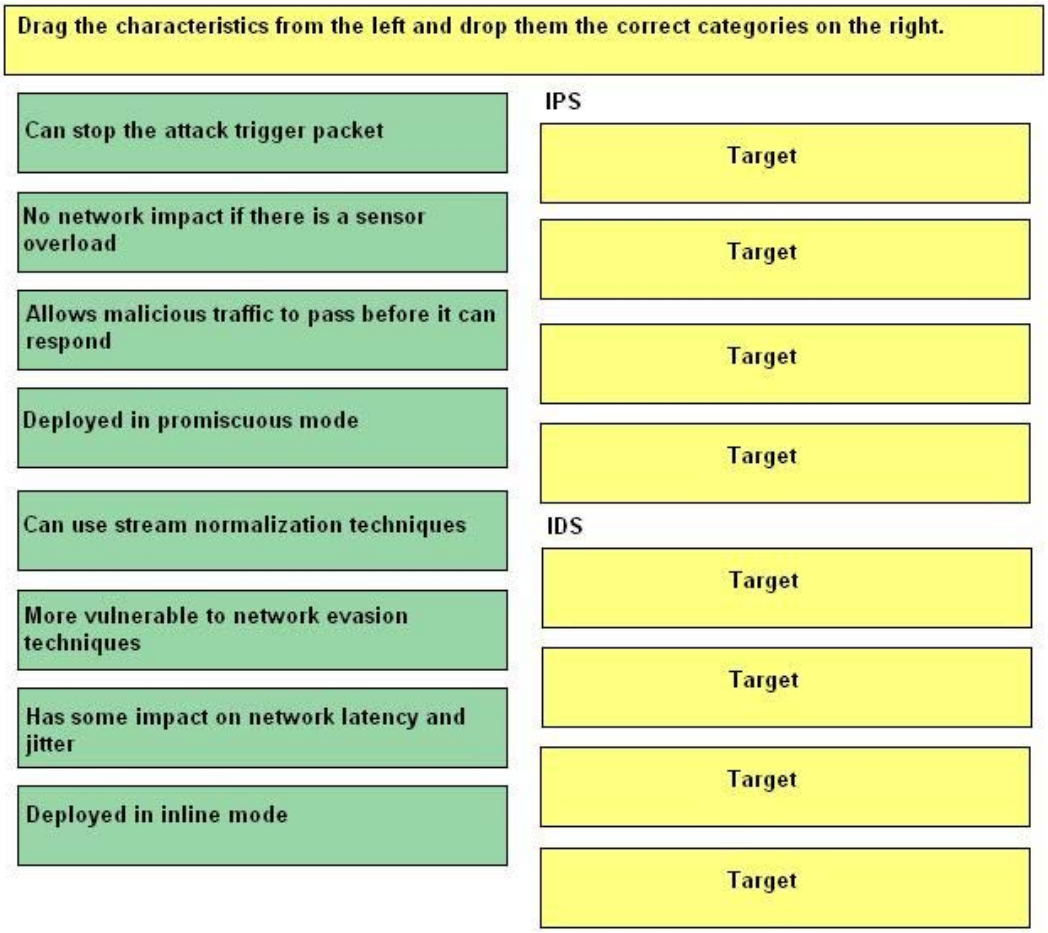
A. root guard
B. BPDU filtering
C. Layer 2 PDU rate limiter
D. BPDU guard
Answer: A,D
Explanation:
The BPDU guard feature is designed to allow network designers to keep the active network topology predictable. BPDU guard is used to protect the switched network from the problems that may be caused by the receipt of BPDUs on ports that should not be receiving them. The receipt of unexpected BPDUs may be accidental or may be part of an unauthorized attempt to add a switch to the network. BPDU guard is best deployed toward user-facing ports to prevent rogue switch network extensions by an attacker. The root guard feature of Cisco switches is designed to provide a way to enforce the placement of root bridges in the network. Root guard limits the switch ports out of which the root bridge may be negotiated. If a root-guard-enabled port receives BPDUs that are superior to those that the current root bridge is sending, then that port is moved to a root-inconsistent state, which is effectively equal to an STP listening state, and no data traffic is forwarded across that port.

NO.4 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:
The Control Plane Policing feature allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe3s/asr1000/qos-plcshp-xe-3s-asr-1000-book/qos-plcshp-ctrl-pln-plc.html

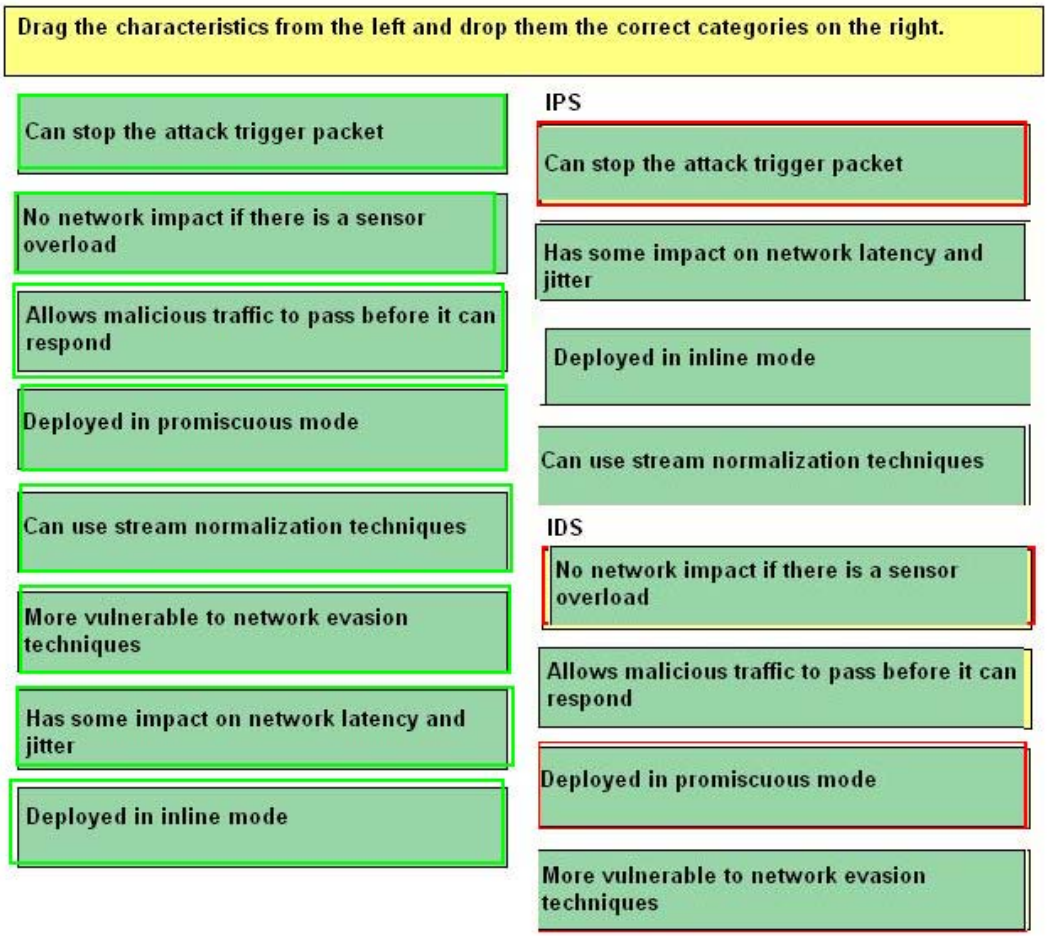
NO.5 Which statement is true when you have generated RSA keys on your Cisco router to prepare for secure device management?
A. You must then zeroize the keys to reset secure shell before configuring other parameters.
B. The SSH protocol is automatically enabled.
C. You must then specify the general-purpose 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.

NO.6 DRAG DROP



Answer:



Explanation:

NO.7 What are three features of IPsec tunnel mode? (Choose three.)
A. IPsec tunnel mode supports multicast.
B. IPsec tunnel mode is used between gateways.
C. IPsec tunnel mode is used between end stations.
D. IPsec tunnel mode supports unicast traffic.
E. IPsec tunnel mode encrypts only the payload.
F. IPsec tunnel mode encrypts the entire packet.
Answer: B,D,F

NO.8 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

NO.9 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

NO.10 Which statement about the Atomic signature engine is true?
A. It can perform signature matching on a single packet only.
B. It can perform signature matching on multiple packets.
C. It can examine applications independent of the platform.
D. It can flexibly match patterns in a session.
Answer: A

NO.11 Which element must you configure to allow traffic to flow from one security zone to another?
A. a zone pair
B. a site-to-site VPN
C. a zone list
D. a zone-based policy
Answer: A

NO.12 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.

NO.13 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

NO.14 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.

NO.15 When a switch has multiple links connected to a downstream switch, what is the first step that STP takes to prevent loops?
A. STP elects the root bridge.
B. STP selects the root port.
C. STP selects the designated port.
D. STP blocks one of the ports.
Answer: A

NO.16 Refer to the exhibit.

```
Feb 1 10:12:08 PST: %SYS-5-CONFIG_I: Configured from console by vty0 (10.2.2.6)
```

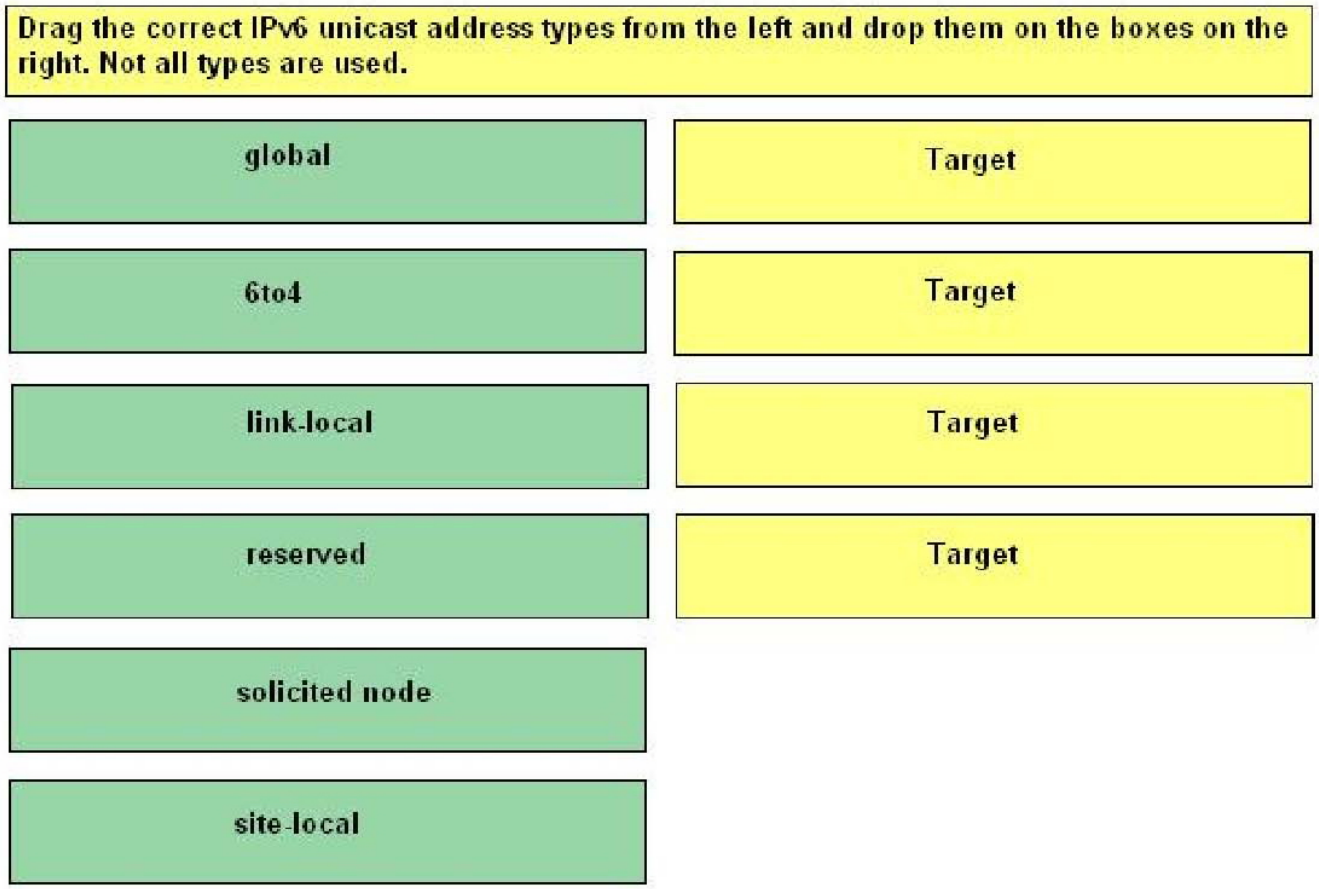
You are a network manager for your organization. You are looking at your Syslog server reports. Based on the Syslog message shown, which two statements are true? (Choose two.)
A. Service timestamps have been globally enabled.
B. This is a normal system-generated information message and does not require 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/configu
r
ation/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)

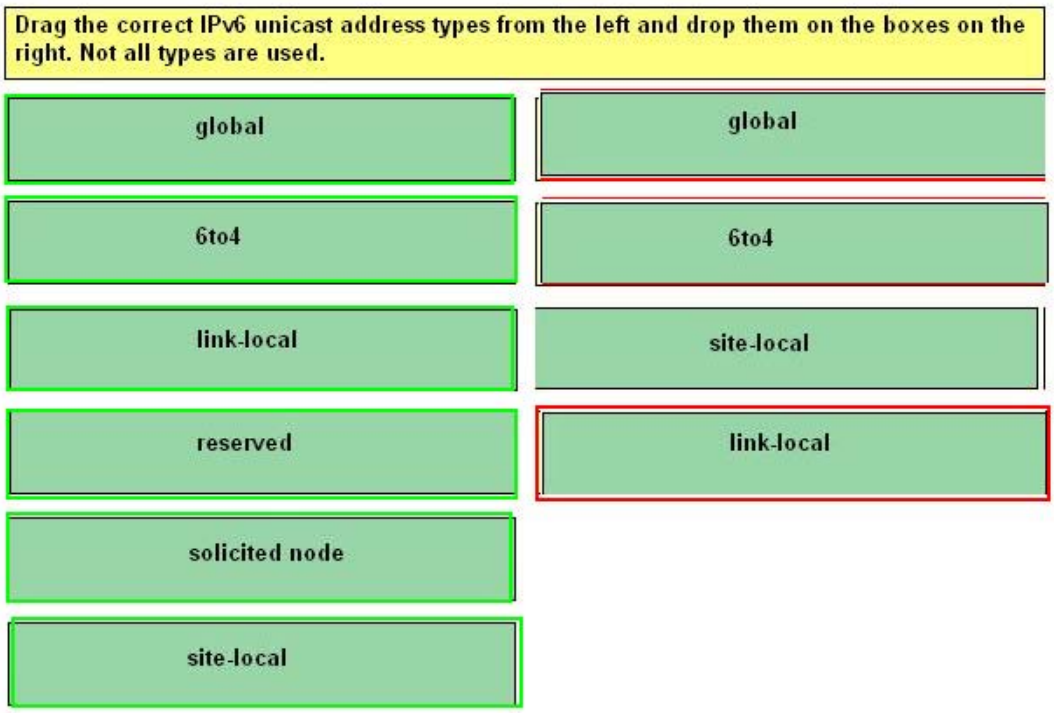
NO.17 Which Cisco IOS command is used to verify that either the Cisco IOS image, the configuration files, or both have been properly backed up and secured?
A. show archive
B. show secure bootset
C. show flash
D. show file systems
E. dir
F. dir archive
Answer: B
Explanation:
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_resil_config_ps6
922_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 Files 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.

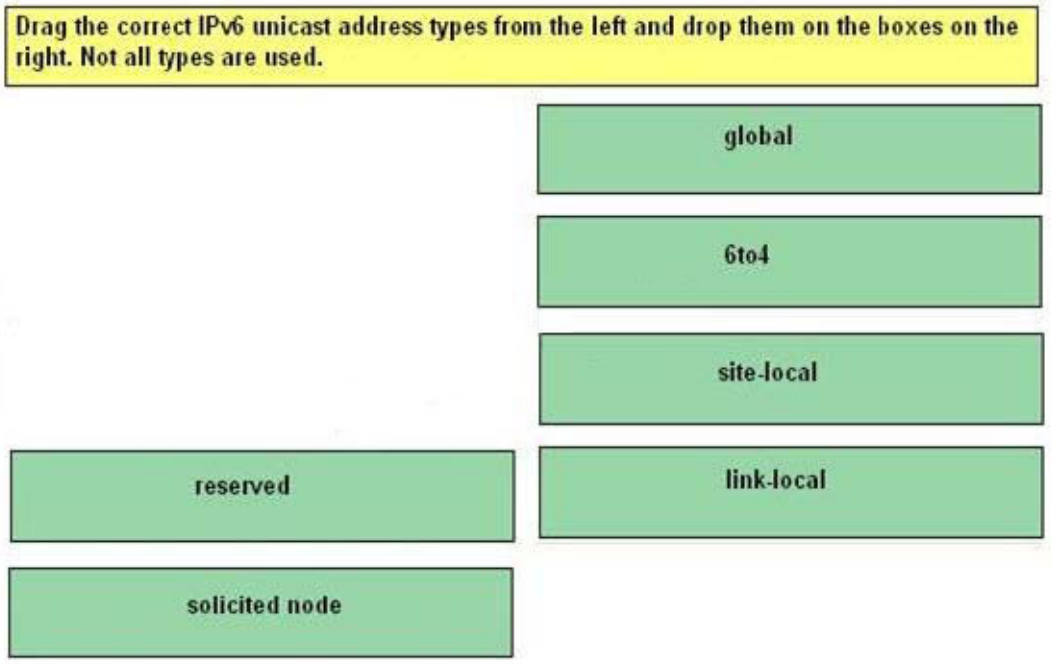
NO.18 DRAG DROP



Answer:



Explanation:



NO.19 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-sheetc78-729751.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:

NO.20 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.