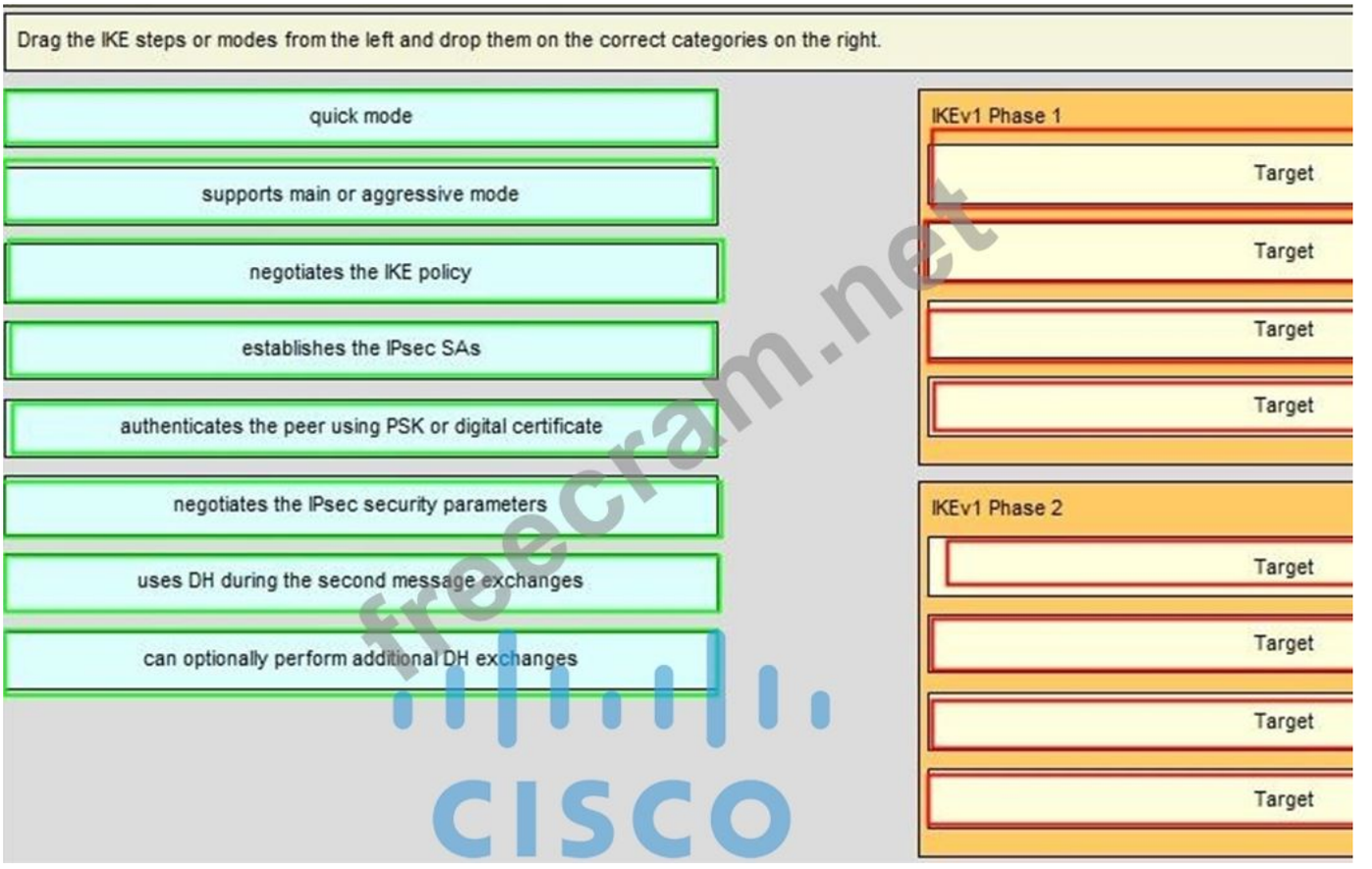
Cisco.210-260.v2018-06-27.q172

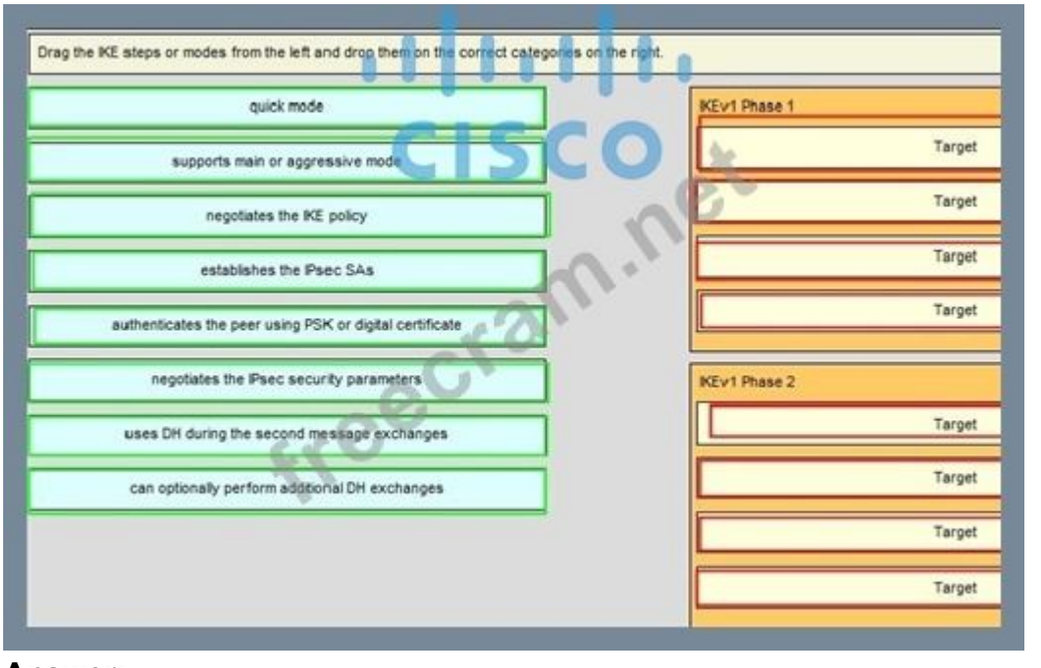
Exam Code:	210-260
Exam Name:	Implementing Cisco Network Security
Certification Provider:	Cisco
Free Question Number:	172
Version:	v2018-06-27
# of views:	1339
# of Questions views:	64721
https://www.freecram.net/torrent/Cisco.210-260.v2018-06-27.q172.html	

NEW QUESTION: 1
Which two protocols are used in a server-based AAA deployment? (Choose two).
A. RADIUS
B. HTTP
C. HTTPS
D. WCCP
E. TACACS+
Answer: (SHOW ANSWER)

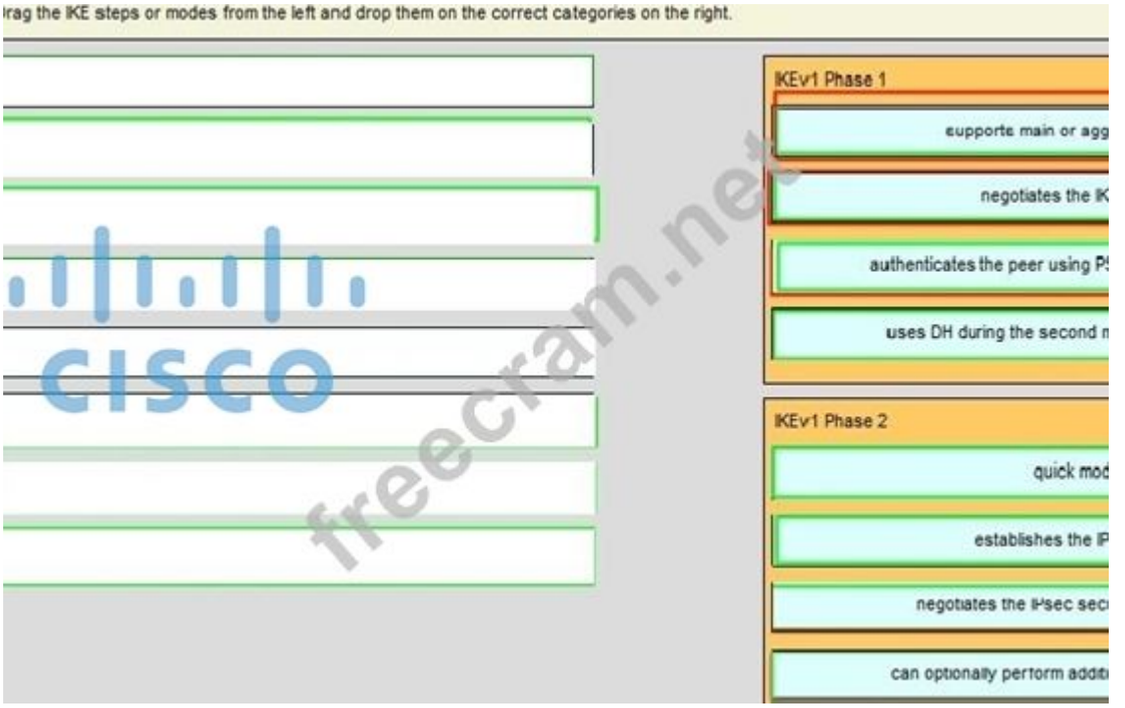
NEW QUESTION: 2



Select and Place:



Answer:



NEW QUESTION: 3

Refer to the exihibit:

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: (SHOW ANSWER)

NEW QUESTION: 4

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?

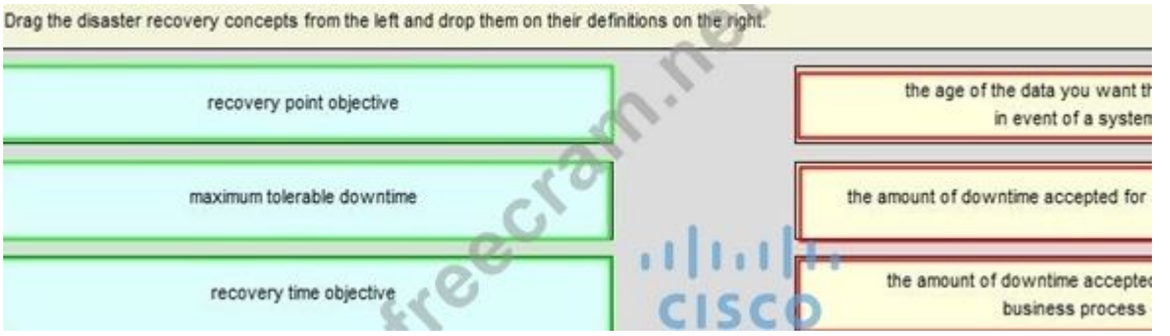
A. risk rating
B. signature accuracy
C. attack relevancy
D. target asset value
Answer: (SHOW ANSWER)

NEW QUESTION: 5
When port securits, 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 MAC address table is cleared and the new MAC address is entered into the table.
C. The violation mode of the port is set to restrict.
D. The port is shutdown.
Answer: (SHOW ANSWER)

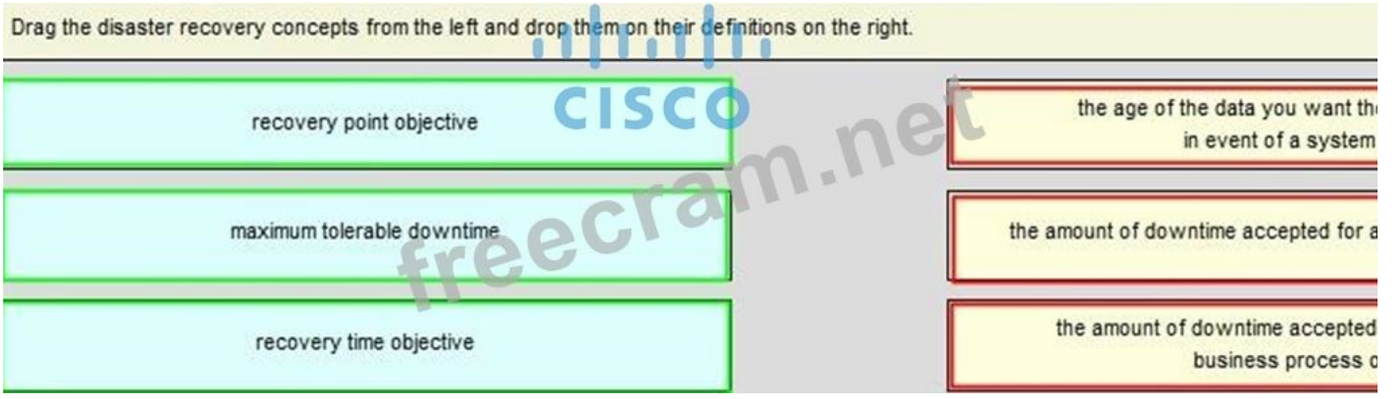
NEW QUESTION: 6
Which four methods are used by hackers? (Choose four.)
A. footprint analysis attack
B. privilege escalation attack
C. buffer Unicode attack
D. front door attacks
E. social engineering attack
F. Trojan horse attack
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 7
Which type of Cisco ASA access list entry can be configured to match multiple entries in a single statement?
A. object groups
B. extended wildcard matching
C. class-map
D. nested object-class
Answer: (SHOW ANSWER)

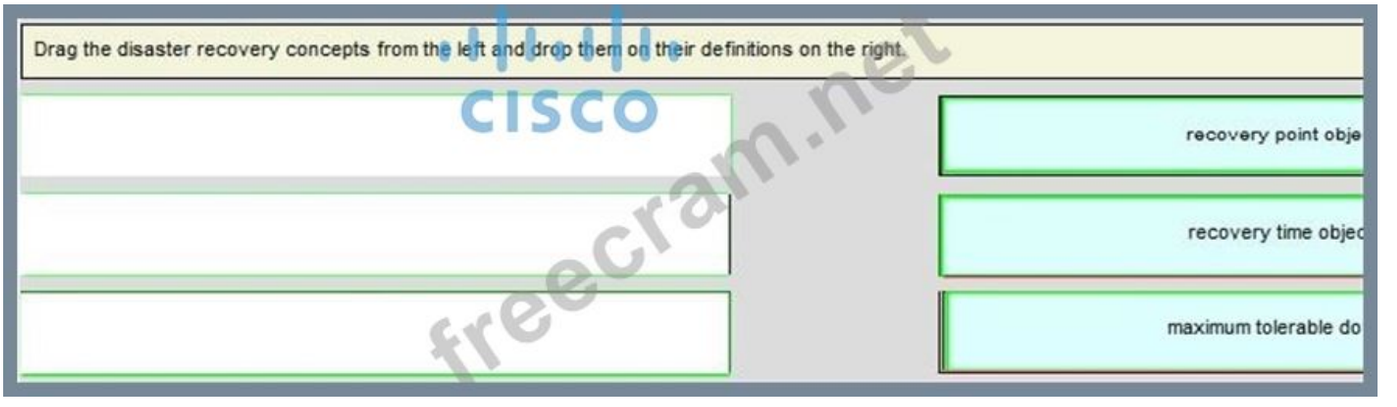
NEW QUESTION: 8



Select and Place:



Answer:



NEW QUESTION: 9

On which protocol number does the authentication header operate?

A. 51

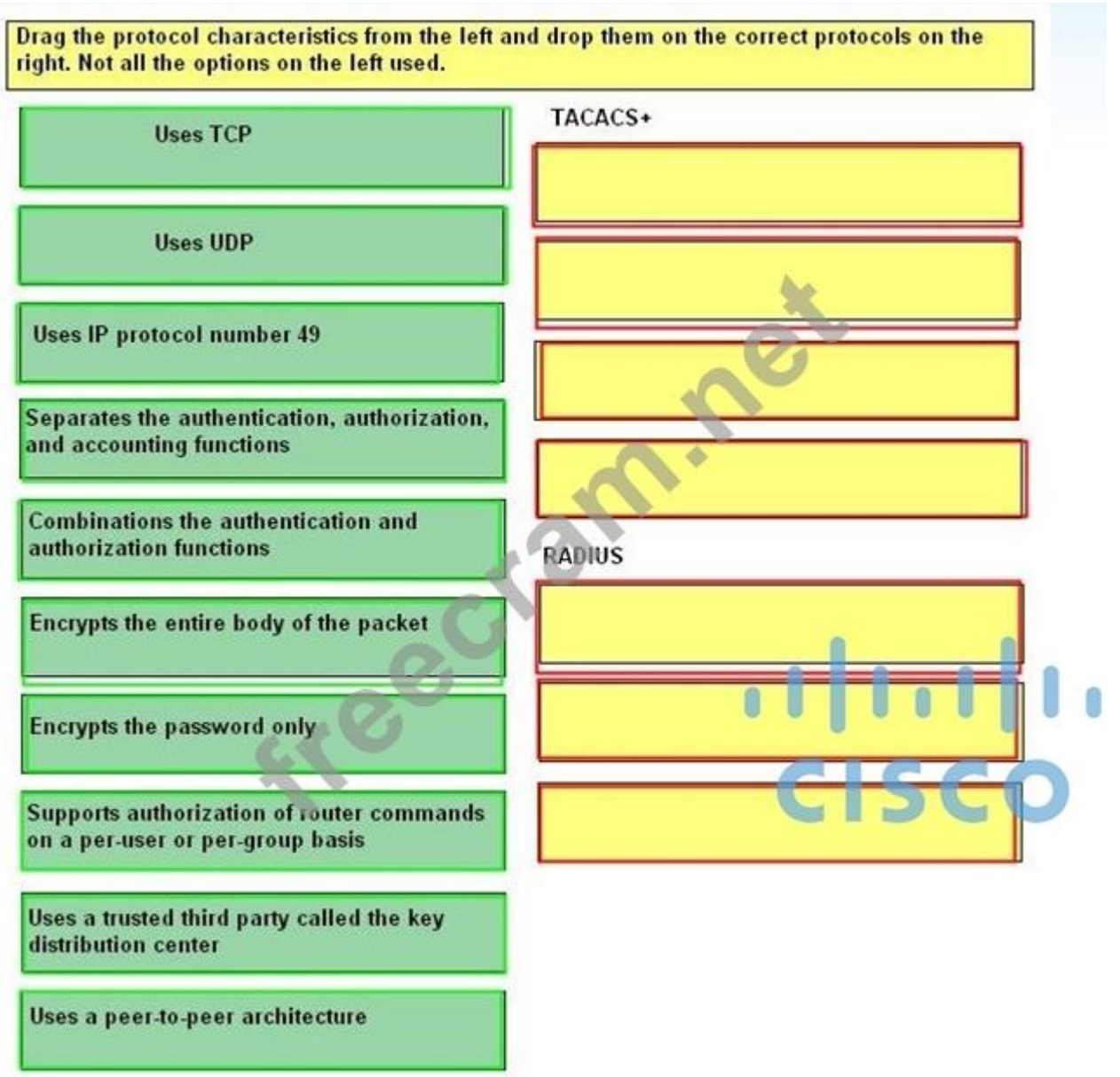
B. 06

C. 47

D. 50

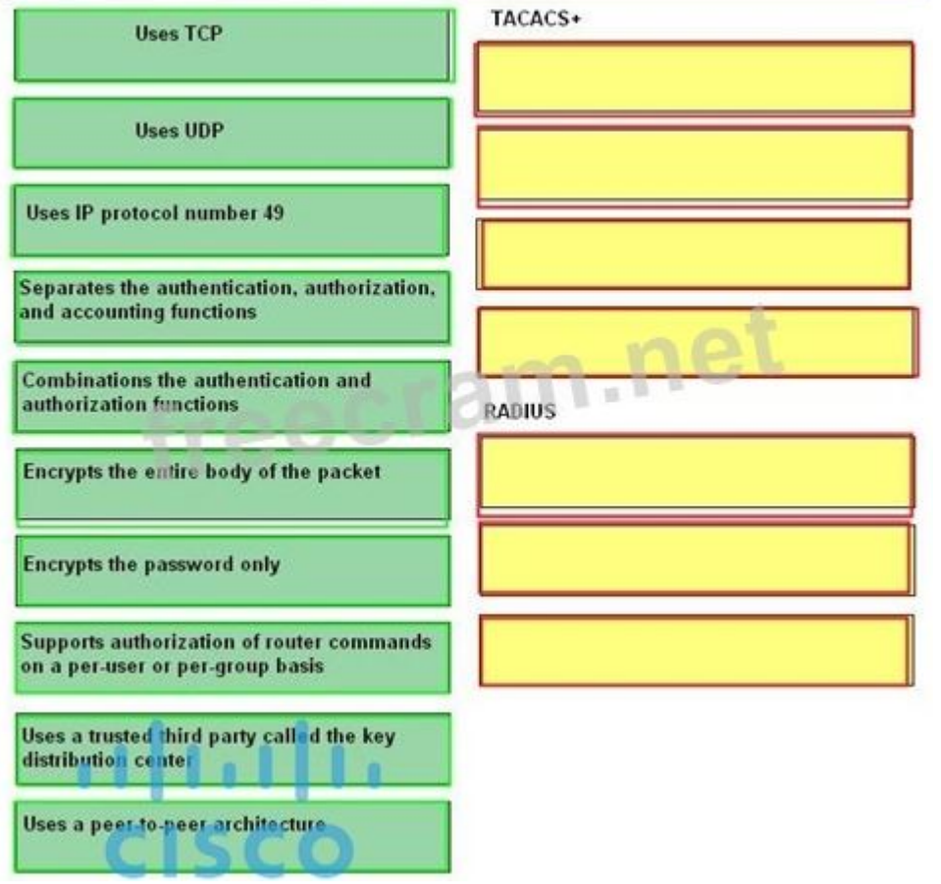
Answer: (SHOW ANSWER)

NEW QUESTION: 10

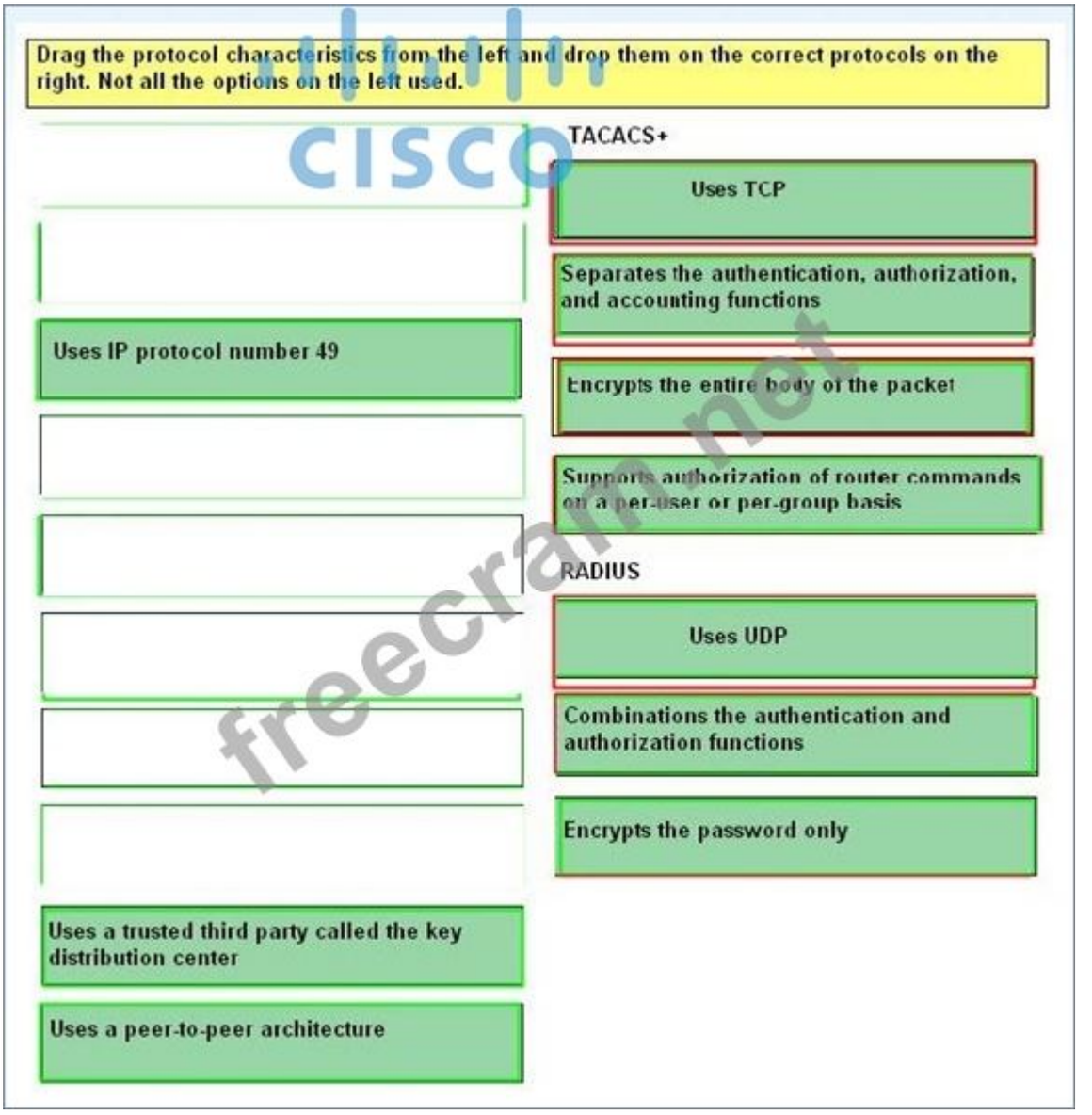


Select and Place:

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.



Answer:



NEW QUESTION: 11

Refer to the exhibit:

```
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 initiating connection request was being spoofed by a different source address.

B. The requesting authentication request came from username GETUSER.

C. The TACACS+ authentication request passed, but for some reason the user's connection was closed immediately.

D. The TACACS+ authentication request came from a valid user.

Answer: (SHOW ANSWER)

NEW QUESTION: 12

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

A. traffic flowing to and from the router interfaces (the self zone)

B. traffic flowing between a zone member interface and any interface that is not a zone member

C. traffic flowing among the interfaces that are members of the same zone

D. traffic flowing to the zone member interface that is returned traffic

E. traffic flowing between a zone member interface and another interface that belongs in a different zone

F. traffic flowing among the interfaces that are not assigned to any zone

Answer: (SHOW ANSWER)

NEW QUESTION: 13

What Cisco Security Agent interceptor is in change of intercepting all read write requests to the rc files in UNIX?

A. Network interceptor

B. File system interceptor

C. Execution space interceptor

D. Configuration interceptor

Answer: D (LEAVE A REPLY)

NEW QUESTION: 14

Which statement is a benefit of using Cisco IOS IPS?

A. It uses the underlying routing infrastructure to provide an additional layer of security.

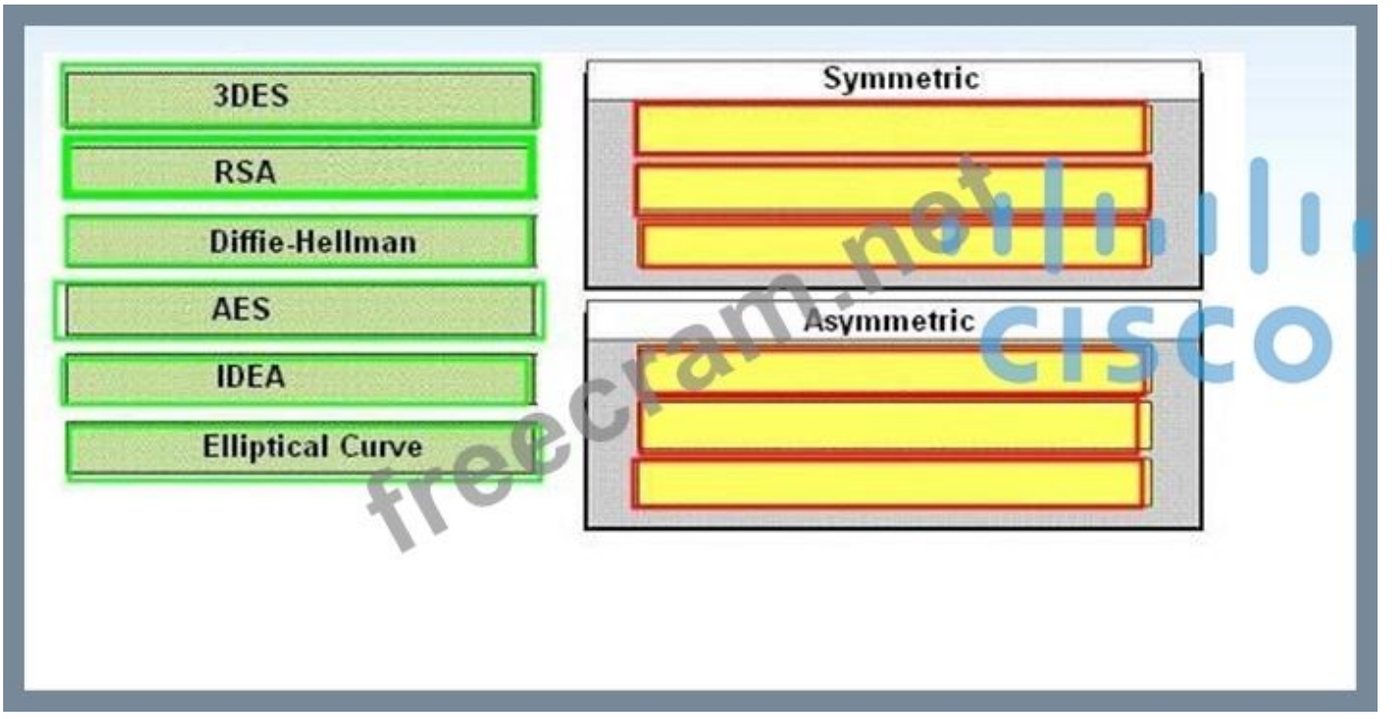
B. It supports the complete signature database as a Cisco IPS sensor appliance.

C. It works in passive mode so as notto impact traffic flow.

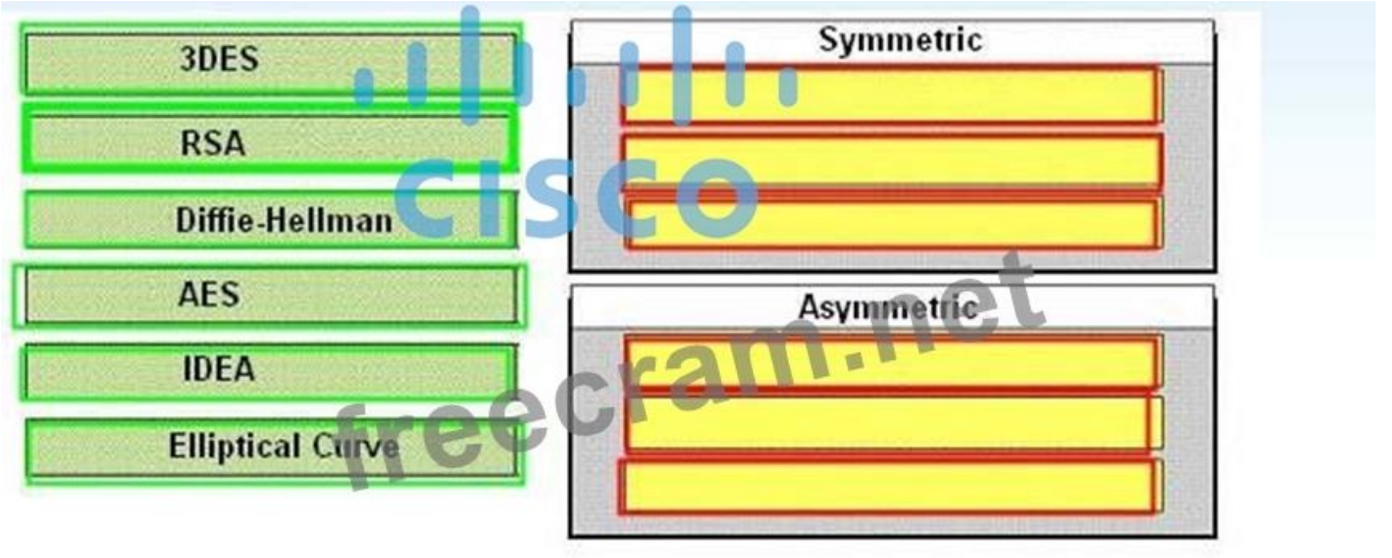
D. The signature database is tied closelywith the Cisco IOS image.

Answer: (SHOW ANSWER)

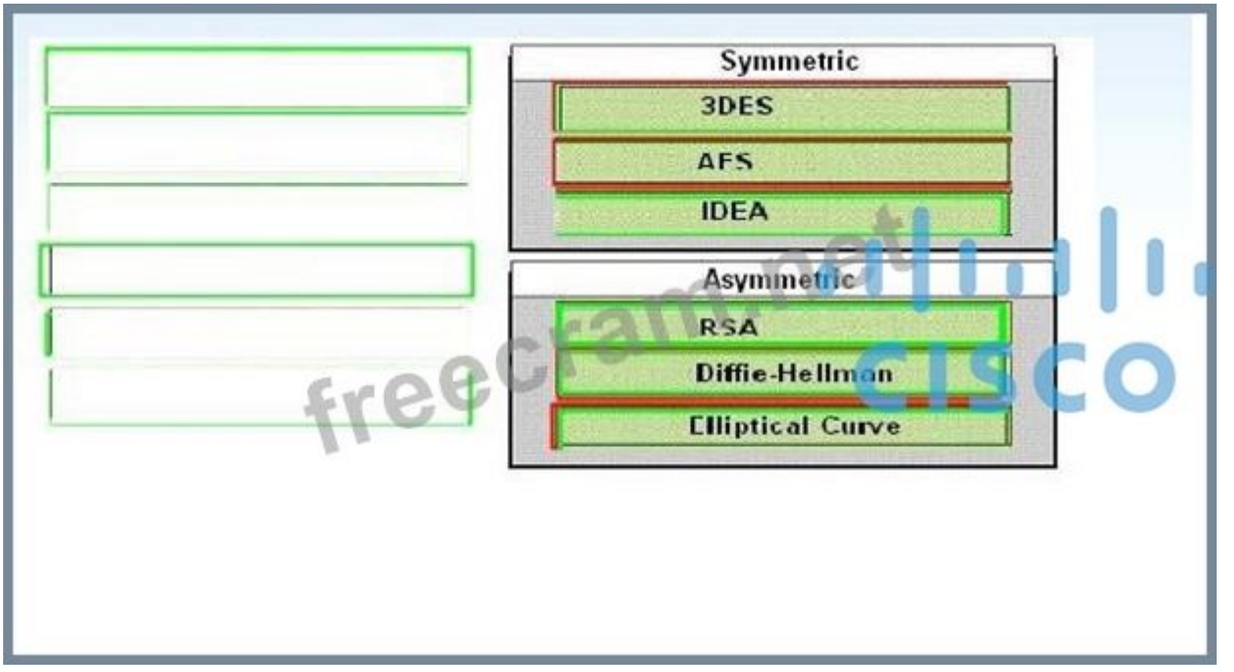
NEW QUESTION: 15



Select and Place:



Answer:



NEW QUESTION: 16

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. requires users to first identify which router interfaces connect to the inside network and which connect to the outside network

D. automatically enables Cisco IOS firewall and Cisco IOS IPS to secure the router
E. uses interactive dialogs and prompts to implement role-based CLI
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 17
You are troubleshooting a Cisco Anyconnect VPN on a firewall and issue the command show webvpn anyconnect. The output the message "SSL VPN is not enable" instead of showing the AnyConnect package. Which action can you take to resolve the problem?
A. Issue the anyconnect enable command
B. Reinstal the AnyConnect image
C. Issue the enable outside command
D. Issue the enable inside command
Answer: (SHOW ANSWER)

NEW QUESTION: 18
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: (SHOW ANSWER)
Explanation

NEW QUESTION: 19
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 permits traffic destined to the 10.10.0.10 host on FastEthernet0/0 from any source.
B. This configuration is invalid. It should be configured as an extended ACL to permit the associated wildcard mask.
C. The access list accepts all traffic on the 10.0.0.0 subnets.
D. Only traffic from 10.10.0.10 is allowed.
E. All traffic from the 10.10.0.0 subnets is denied.
F. 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.
Answer: (SHOW ANSWER)

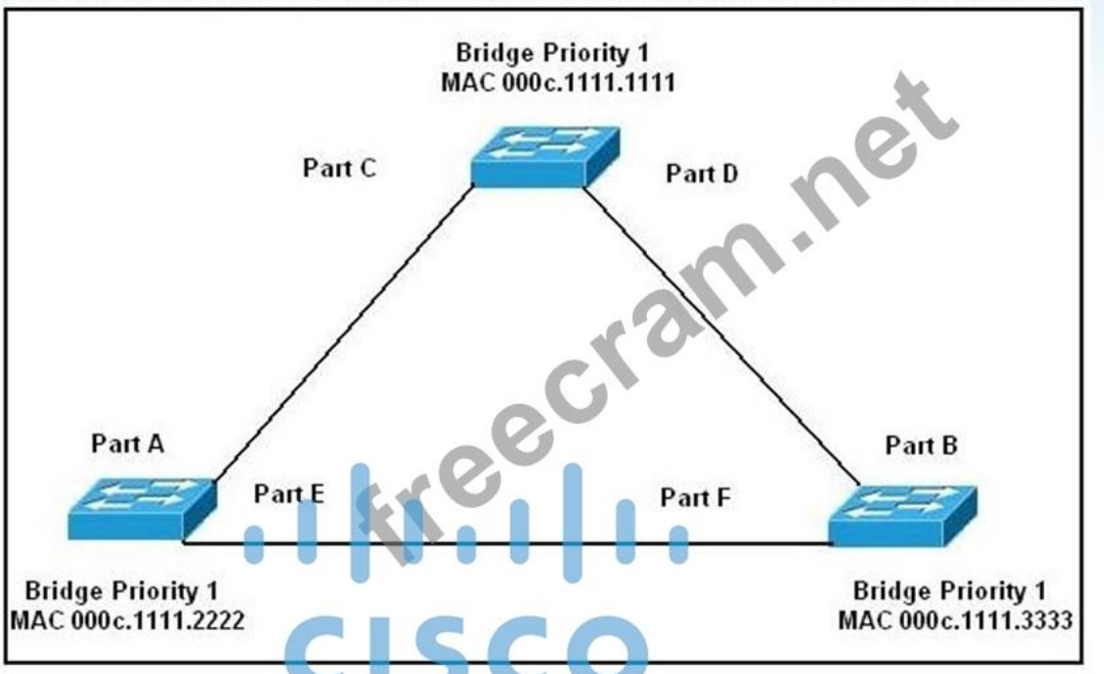
NEW QUESTION: 20
If you are implementing VLAN trunking, which additional configuration parameter should be added to the trunking configuration?

A. no switchport mode access
B. switchport mode DTP
C. no switchport trunk native VLAN 1
D. switchport nonnegotiate
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Which location is recommended for extended or extended named ACLs?
A. a location as close to the source 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. an intermediate location to filter as much traffic as possible
Answer: (SHOW ANSWER)

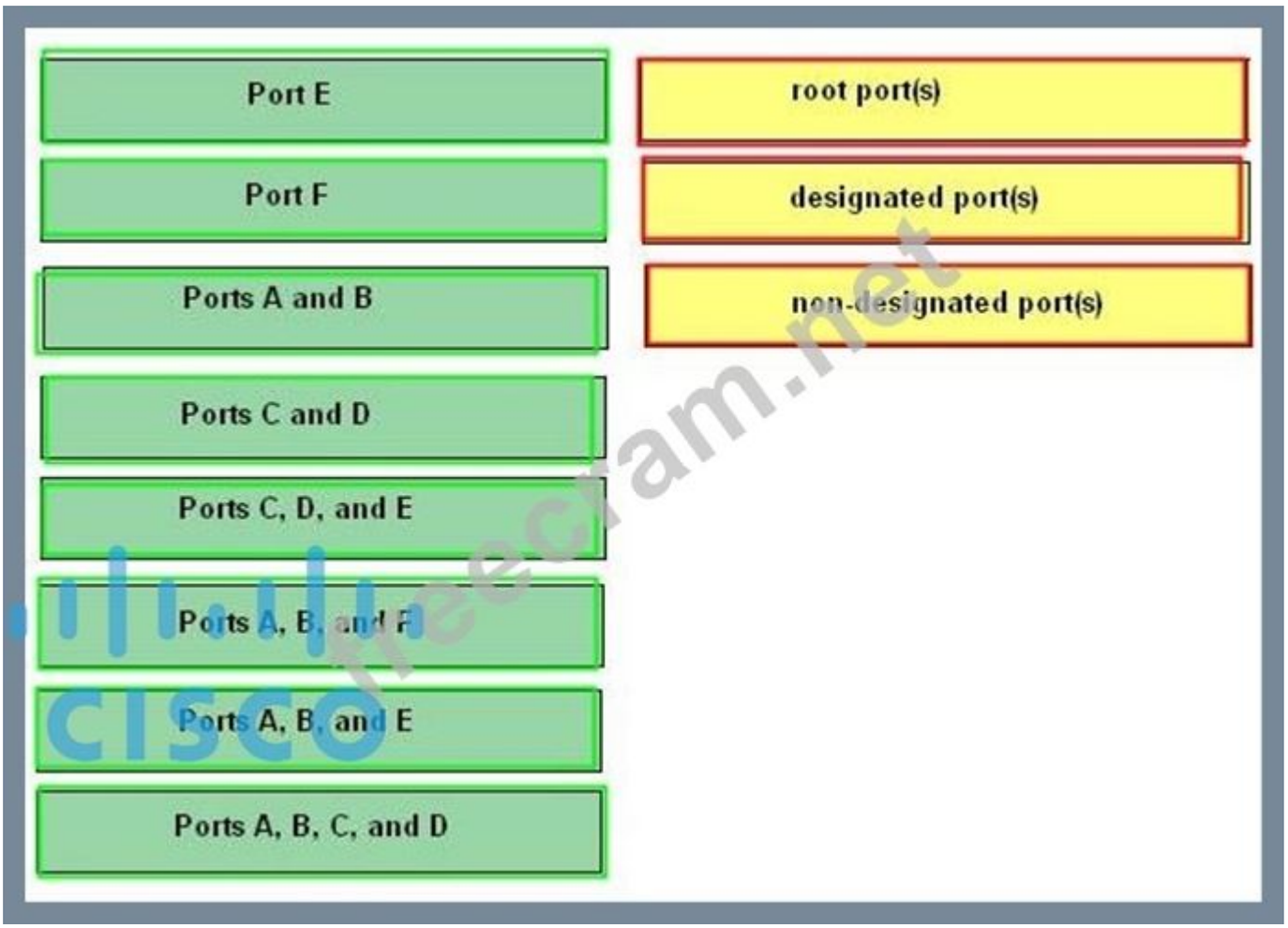
NEW QUESTION: 22

Refer to the exhibit. Drag the port(s) from the left and drop them on the correct STP roles on the right. No

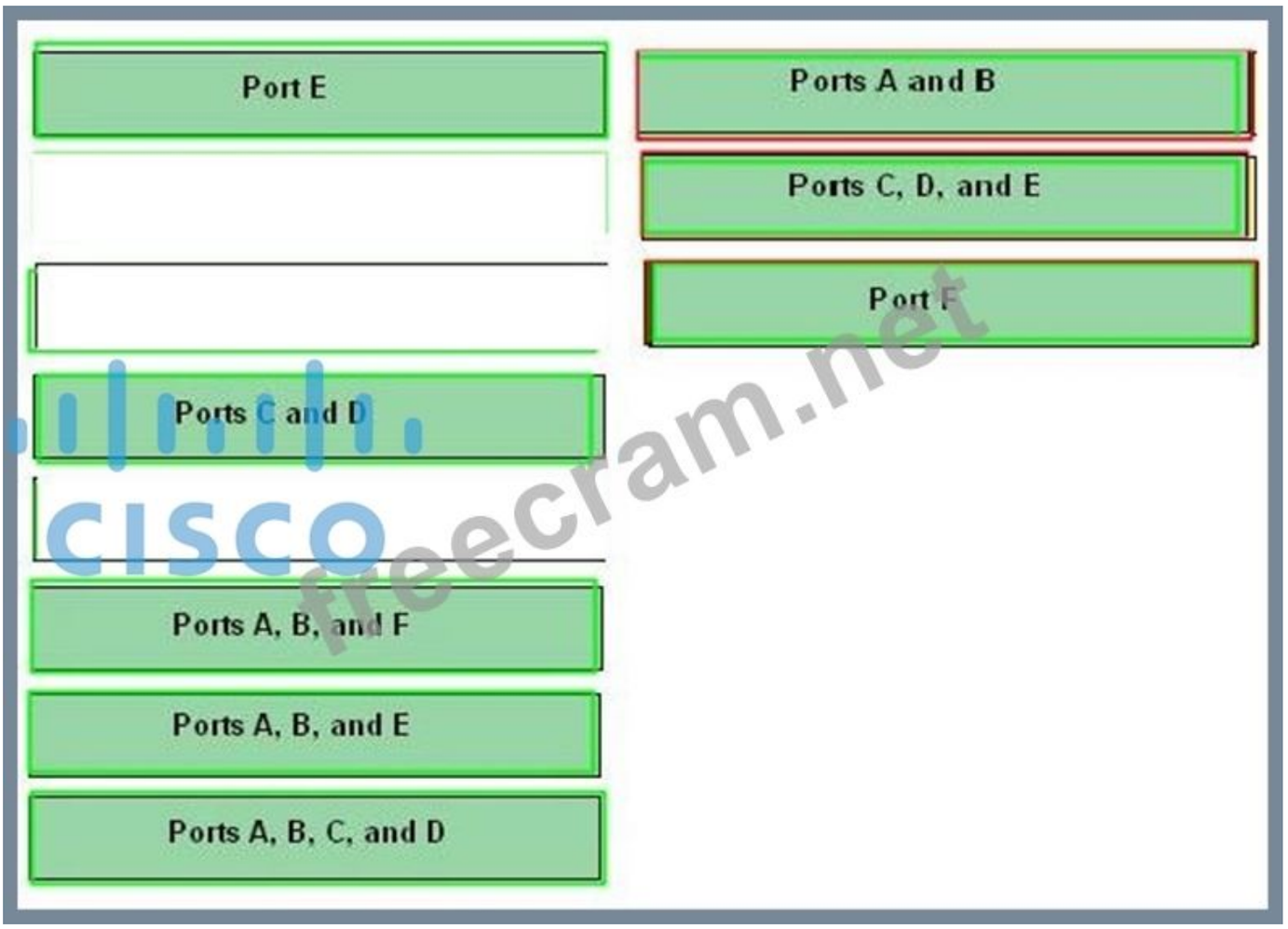


Port E	root port(s)
Port F	designated port(s)
Ports A and B	non-designated port(s)
Ports C and D	
Ports C, D, and E	
Ports A, B, and F	
Ports A, B, and E	
Ports A, B, C, and D	

Select and Place:


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

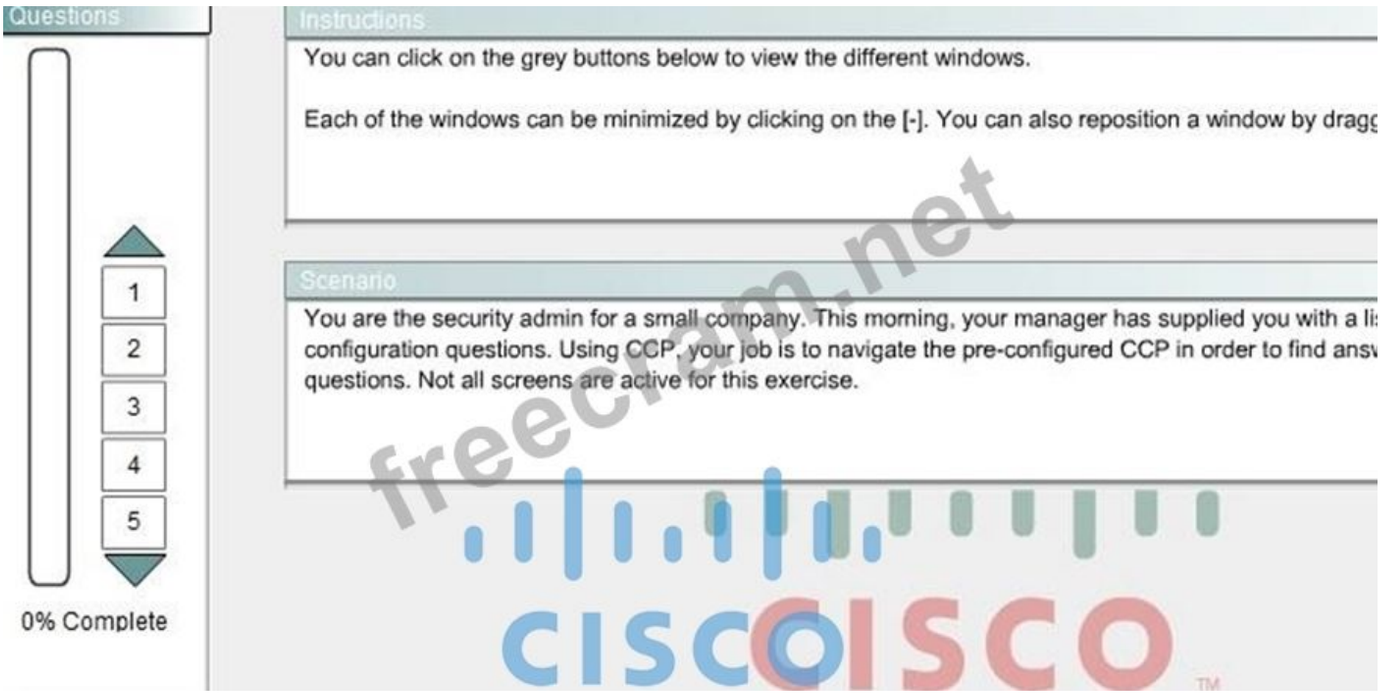
Answer:

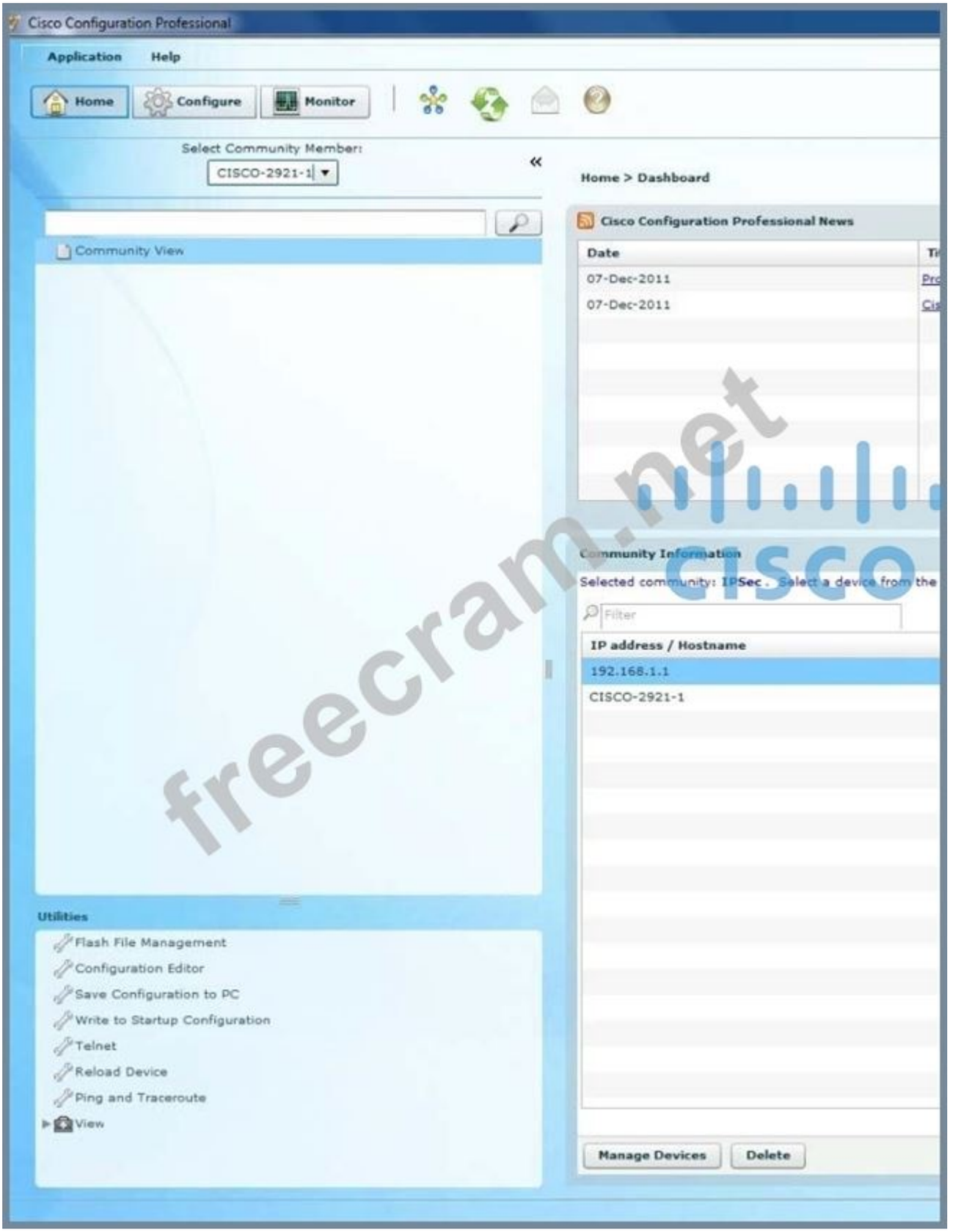


NEW QUESTION: 23
Which two countermeasures can mitigate MAC spoofing attacks? (Choose two).
A. Root guard
B. BPDU guard
C. IP Source guard
D. Port security
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Which protocol secures router management session traffic?
A. SSH
B. Telnet
C. POP
D. SSTP
Answer: (SHOW ANSWER)

NEW QUESTION: 25


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 dragg
Scenario
You are the security admin for a small company. This morning, your manager has supplied you with a li
configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answ
questions. Not all screens are active for this exercise.
freecram.net
CISCO
CISCO



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

A. Sdm-cls-http

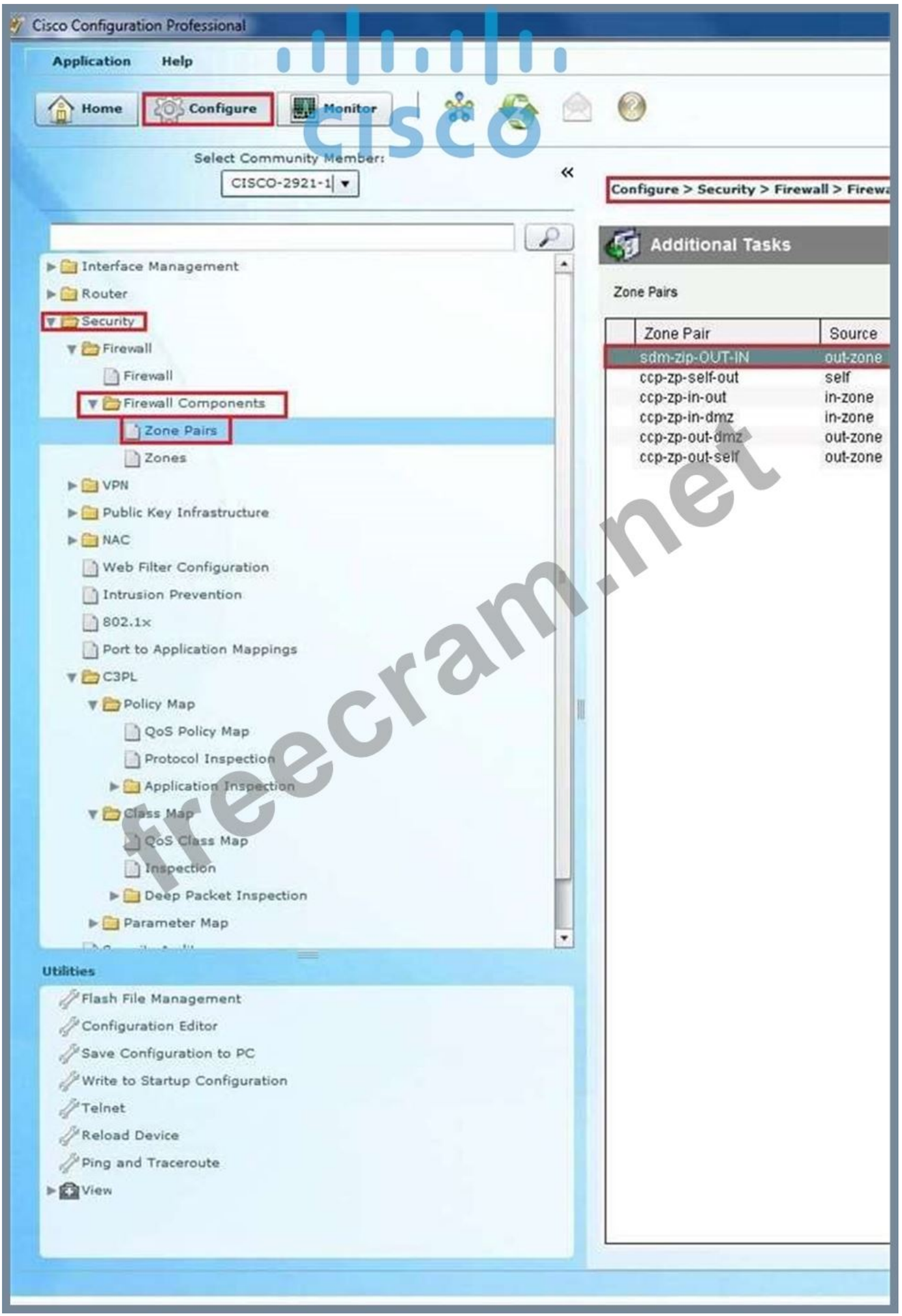
B. OUT_SERVICE

C. Ccp-policy-ccp-cls-1

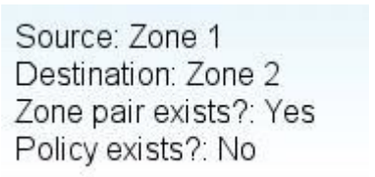
D. Ccp-policy-ccp-cls-2

Answer: (SHOW ANSWER)

Explanation/Reference:



NEW QUESTION: 26
Which option is the resulting action in a zone-based policy firewall configuration with these conditions?



A. no impact to zoning or policy
B. drop
C. apply default policy
D. no policy lookup (pass)
Answer: (SHOW ANSWER)

NEW QUESTION: 27
When AAA login autnentication 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. krb5
B. group RADIUS
C. group TACACS+
D. local
E. enable
F. if-authenticated
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which statement describes how the sender of the message is verified when asymmetric encryption is used?
The sender encrypts the message using the sender's public key, and the receiver
A. decrypts the message using the receiver's private key.
The sender encrypts the message using the receiver's private key, and the receiver
B. decrypts the message using the sender's private key.
The sender encrypts the message using the sender's private key, and the receiver
C. decrypts the message using the sender's public key.
D. decrypts the message using the receiver's public key.
The sender encrypts the message using the receiver's public key, and the receiver
E. decrypts the message using the sender's public key.
The sender encrypts the message using the receiver's public key, and the receiver
Answer: E (LEAVE A REPLY)

NEW QUESTION: 29
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. at the entry point into the data center
B. at remote branch offices
C. inside the firewall of the corporate headquarters Internet connection
D. outside the firewall of the corporate headquarters Internet connection
Answer: (SHOW ANSWER)

NEW QUESTION: 30
What are two primary attack methods of VLAN hopping? (Choose two).
A. double tagging
B. VOIP hopping
C. Switch spoofing
D. CAM-table overflow
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 31
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 10.1.129.0 0.0.0.255 eq www 192.168.1.10 0.0.0.0 eq www
C. access-list 101 permit tcp 10.1.128.0 0.0.1.255 eq 3030 192.168.1.0 0.0.0.15 eq www
D. access-list 101 permit ip host 10.1.129.100 eq 3030 host 192.168.1.100 eq 80
E. access-list 101 permit tcp host 192.168.1.10 eq 80 10.1.0.0 0.0.255.255 eq 3030
F. access-list 101 permit tcp 192.168.1.10 0.0.0.0 eq 80 10.1.0.0 0.0.255.255
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which tjpe of Cisco IOS access control list is identified by 100 to 199 and 2000 to 2699?
A. named

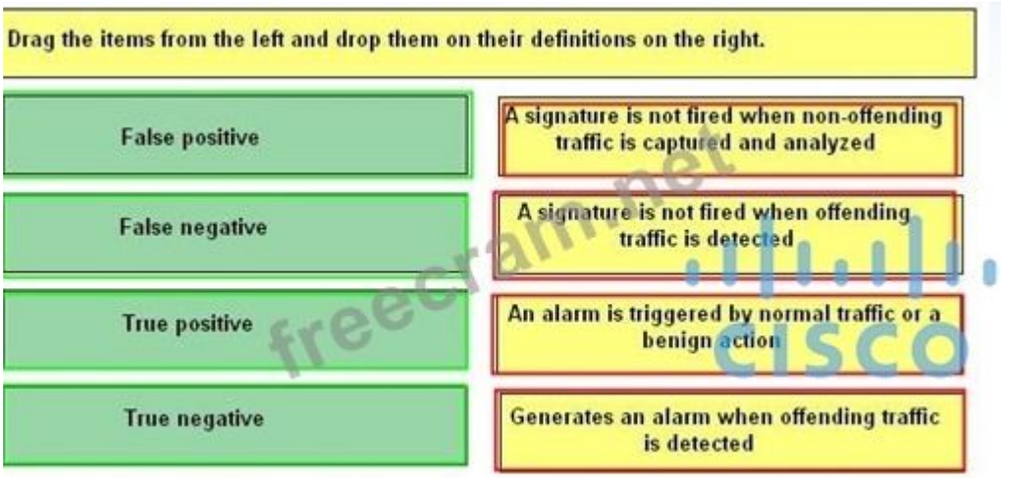
B. extended

C. standard

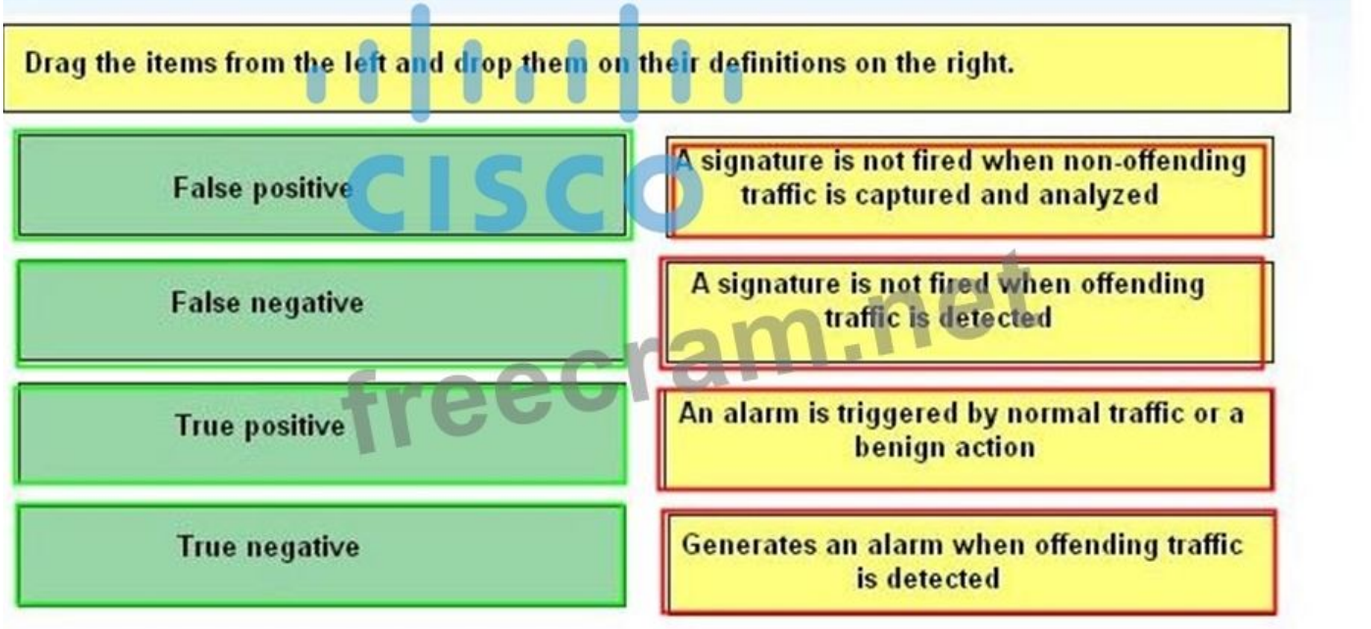
D. IPv4 for 100 to 199 and IPv6 for 2000 to 2699

Answer: (SHOW ANSWER)

NEW QUESTION: 33



Select and Place:



Answer:

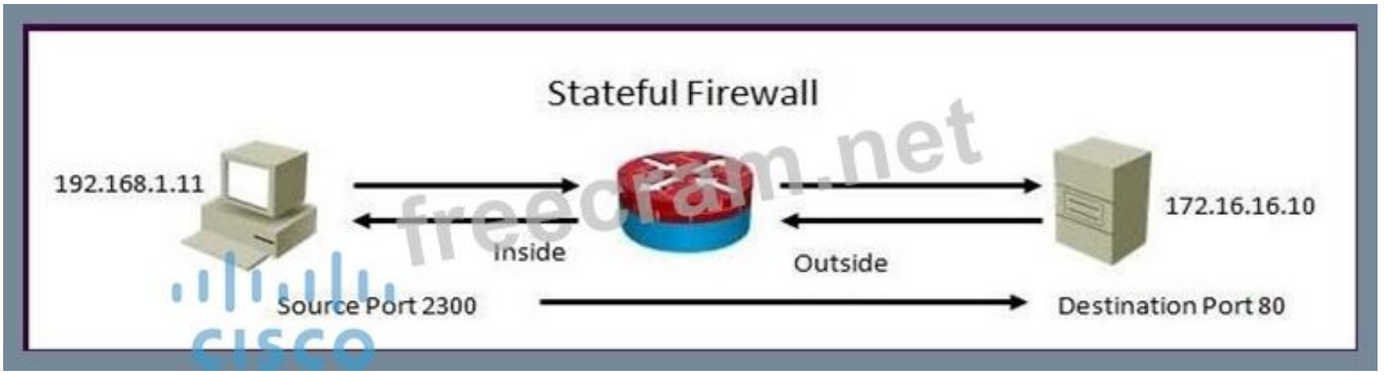
NEW QUESTION: 34
Which item is the great majority of software vulnerabilities that have been discovered?
A. Heap overflows
B. Stack vulnerabilities
C. Software overflows
D. Buffer overflows
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which technology provides an automated digital certificate management system for use with IPsec?
A. Digital Signature Algorithm
B. Public key infrastructure
C. Internet Key Exchange
D. ISAKMP
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which two statements about SSL-based VPNs are true? (Choose two.)
A. The authentication process uses hashing technologies.
B. Both client and clientless SSL VPNs require special-purpose client software to be installed on the client machine.
C. SSL VPNs and IPsec VPNs cannot be configured concurrently on the same router.
D. Asymmetric algorithms are used for authentication and key exchange.
E. The application programming interface can be used to modify extensively the SSL client software for use in special applications.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which type of network masking is used when Cisco IOS access control lists are configured?
A. extended subnet masking
B. standard subnet masking
C. wildcard masking
D. priority masking
Answer: (SHOW ANSWER)

NEW QUESTION: 38
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 ip host 172.16.16.10 eq 80 host 192.168.1.0 0.0.0.255 eq 2300
D. permit tcp any eq 80 host 192.168.1.11 eq 2300
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which type of firewall technology is considered the versatile and commonly used firewall technology?
A. application layer firewall
B. adaptive layer firewall
C. static packet filter firewall
D. stateful packet filter firewall
E. proxy firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which two features are supported by Cisco IronPort Security Gateway? (Choose two.)
A. HTTP and HTTPS scanning

B. outbreak intelligence
C. DDoS protection
D. email encryption
E. spam protection
Answer: (SHOW ANSWER)

NEW QUESTION: 41
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. inbound traffic initiated from the outside to the inside
B. outbound traffic initiated from the inside to the DMZ
C. inbound traffic initiated from the outside to the DMZ
D. HTTP return traffic originating from the inside network and returning via the outside interface
E. HTTP return traffic originating from the DMZ network and returning via the inside interface
F. HTTP return traffic originating from the outside network and returning via the inside interface
G. outbound traffic initiated from the DMZ to the outside
H. HTTP return traffic originating from the inside network and returning via the DMZ interface
I. inbound traffic initiated from the DMZ to the inside
J. outbound traffic initiated from the inside to the outside
Answer: B,D,G,H,J (LEAVE A REPLY)

NEW QUESTION: 42
Which two services are provided by IPsec? (Choose two.)
A. Confidentiality
B. Data Integrity
C. Authentication Header
D. Internet Key Exchange
E. Encapsulating Security Payload
Answer: (SHOW ANSWER)

NEW QUESTION: 43
What is the purpose of a trunk port?
A. A trunk port connects multiple hubs together to increase bandwitch.
B. A trunk port provides a physical link specifically for a VPN.
C. A trunk port carries traffic for multiple VLANS.
D. A trunk port separates VLAN broadcast domains.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Which option describes the purpose of Diffie-Hellman?
A. used to verity the identity of the peer
B. used between the initiator and the responder to establish a basic security policy
C. used to establish a symmetric shared key via a public key exchange process
D. used for asymmetric public key encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which option is a characteristic of the RADIUS protocol?
A. combines authentication and authorization in one process
B. uses TCP
C. offers multiprotocol support
D. supports bi-directional challenge
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which three statements about the IPsec ESP modes of operation are true? (Choose three.)
A. Tunnel mode is used between two security gateways.
B. Transport mode leaves the original IP header in the clear.
C. Tunnel mode only encrypts and authenticates the data.
D. Tunnel mode is used between a host and a security gateway.
E. Transport mode authenticates the IP header.
Answer: (SHOW ANSWER)

NEW QUESTION: 47
How are Cisco IOS access control lists processed?
A. The global ACL is matched first before the interlace ACL.
B. The best match ACL is matched first.
C. Permit ACL entries are matched first before the deny ACL entries.
D. Standard ACLs are processed first.
E. ACLs are matched from top down.

Answer: (SHOW ANSWER)

NEW QUESTION: 48
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 176.16.80.0 255.255.252.0
C. permit 172.16.80.0 255.255.240.0
D. permit 172.16.80.0 0.0.248.255
E. permit 172.16.80.0 255.255.248.0
F. permit 172.16.80.0 0.0.7.255
Answer: (SHOW ANSWER)

NEW QUESTION: 49
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. Log all messages to the system buffer so that they can be displayed when accessing the router.
B. Use SSH to access your syslog information.
C. Enable the highest level of syslog function available to ensure that all possible event messages are logged.
D. Synchronize clocks on the network with a protocol such as Network Time Protocol.
Answer: (SHOW ANSWER)

NEW QUESTION: 50

Instruction

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

Scenario

You are the security adminstrator for a small company. You needs 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

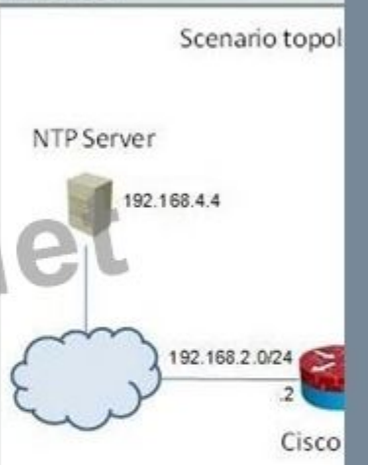
Create a new Access Rule
- Name: Inbound
- Type: Extended Rule

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

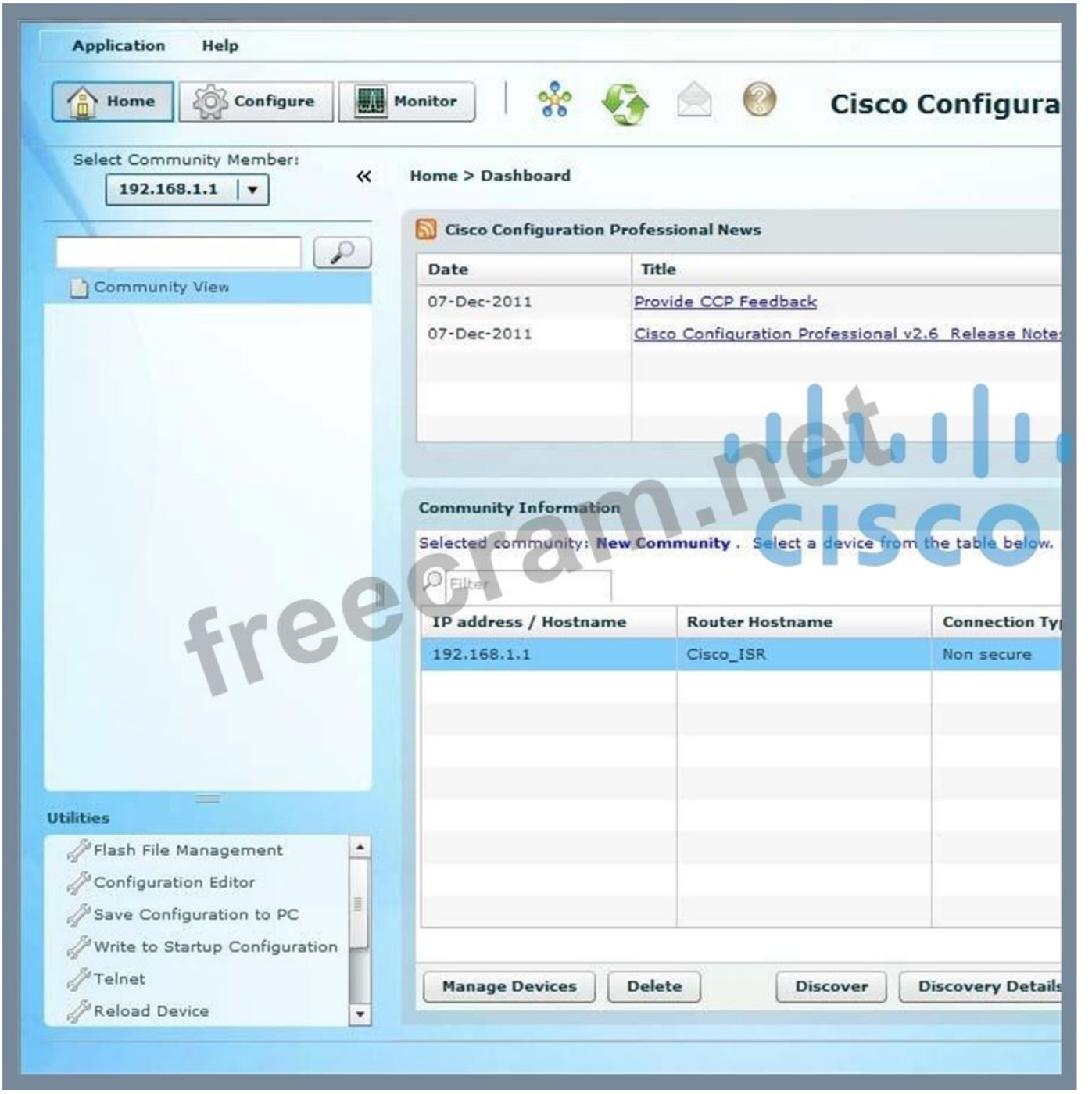
Add an additional Rule Entry to the Access Rule
- Permit any source to the 10.0.2.0/24 network for protocol 80

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



Instruction | Scenario | TOPOLOGY

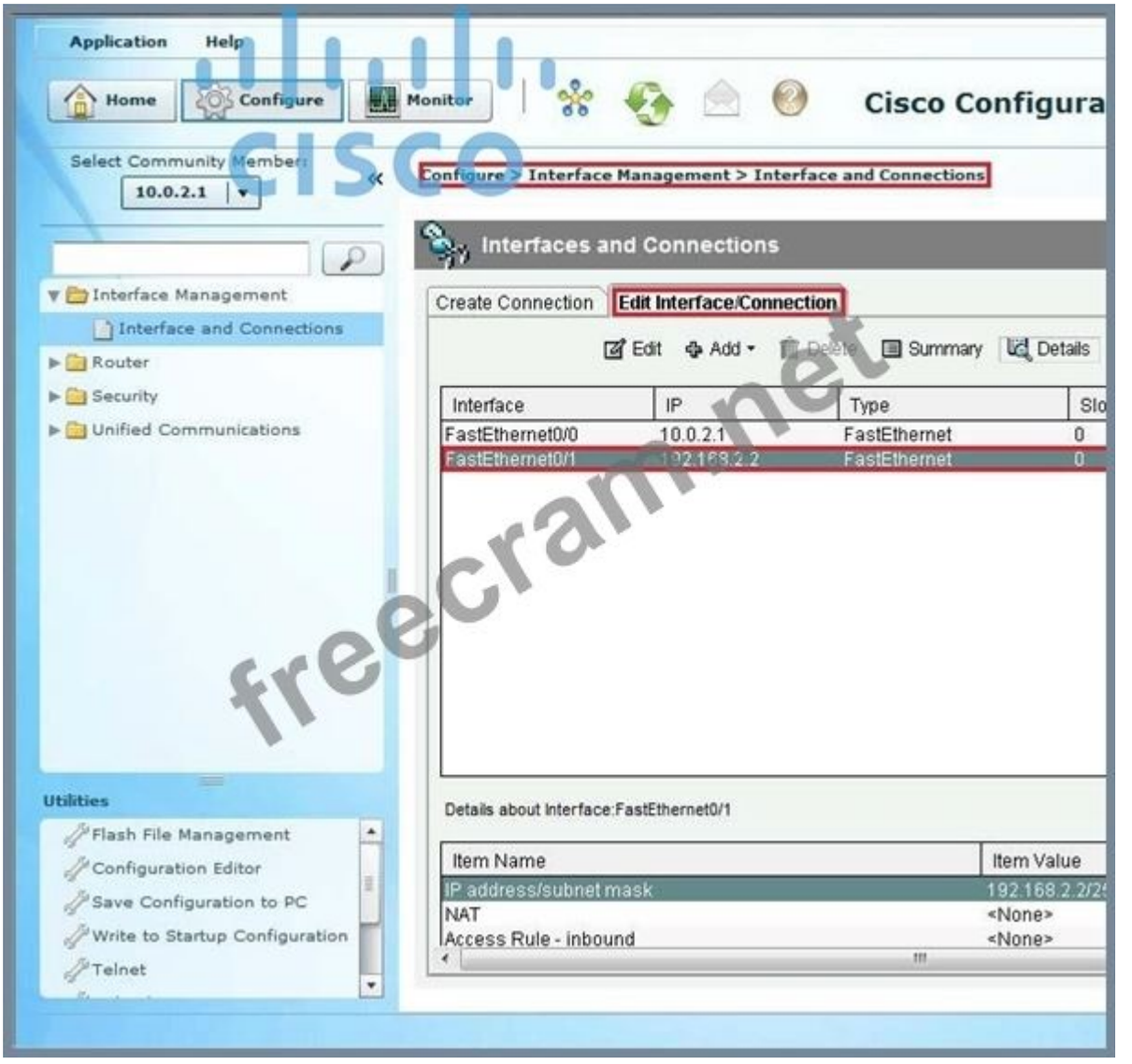


A.

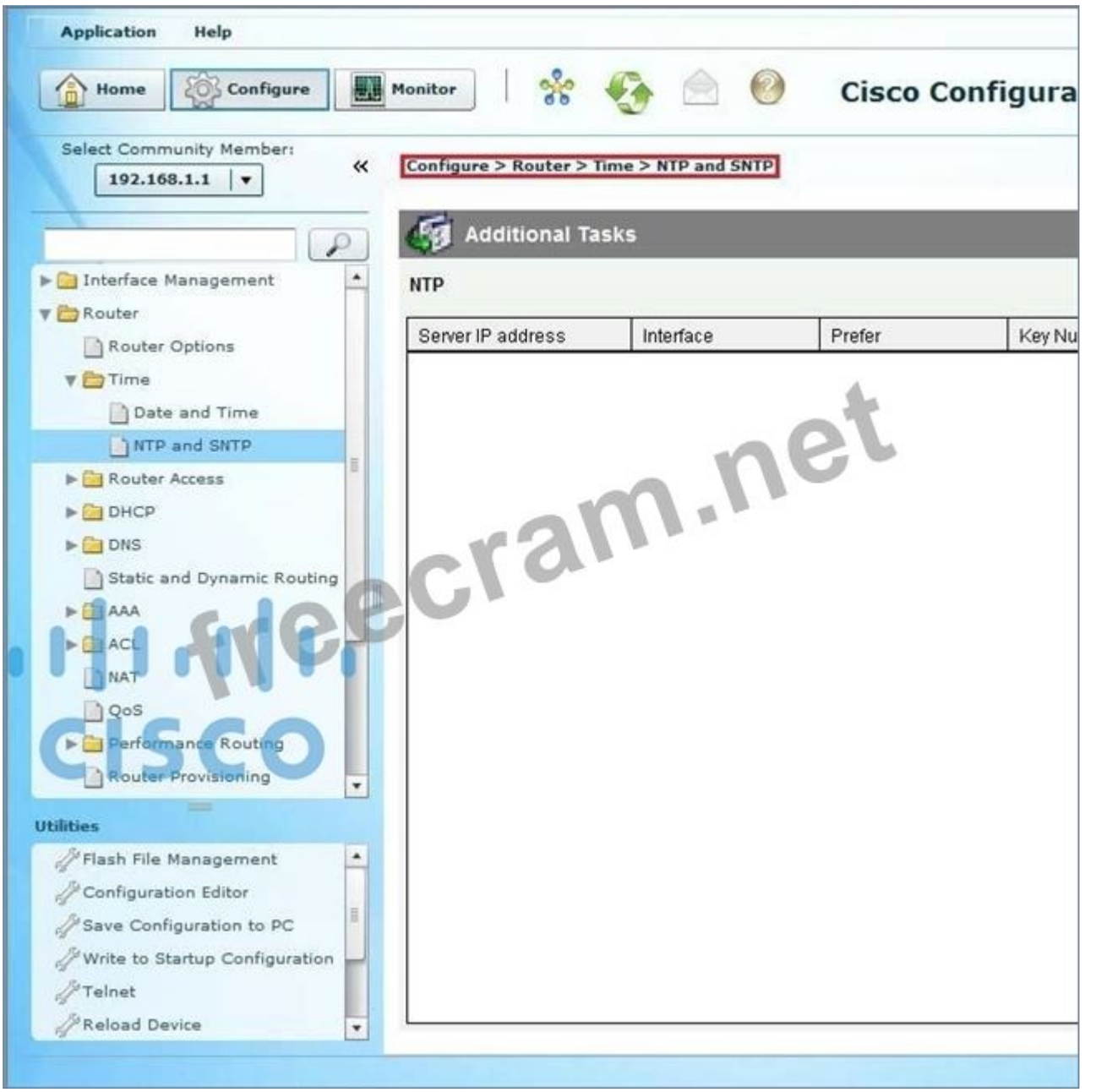
Answer:

Explanation/Reference:

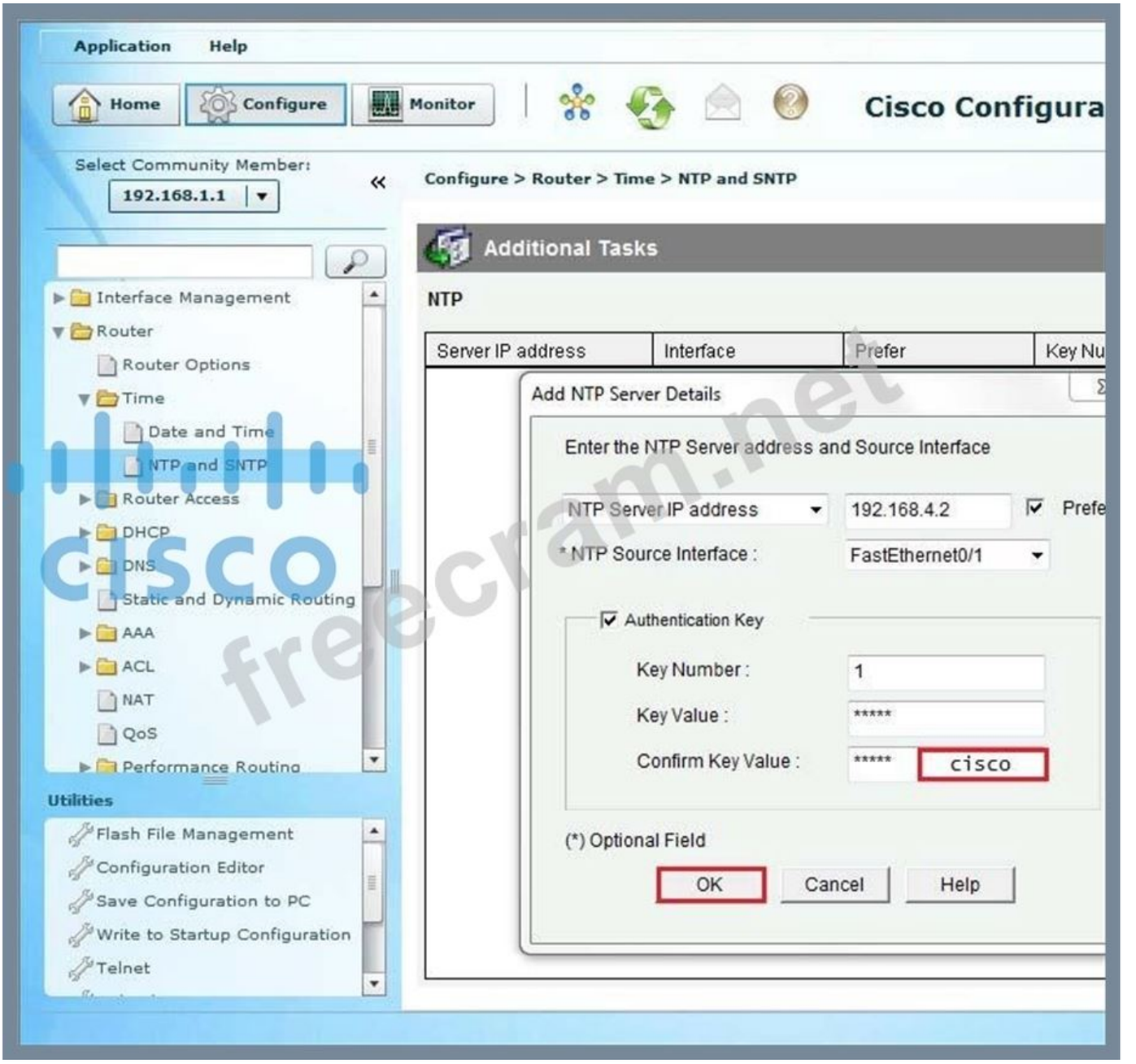
First step you need to know which interface is belong to OUTSIDE. To check this navigate to Configure>Interface Management>Interface and Connections and click on Edit Interface/ Connection to see which interface is belong to OUTSIDE by checking IP addresses assigned. In out case OUTSIDE interface is FastEthernet0/1. Note it!



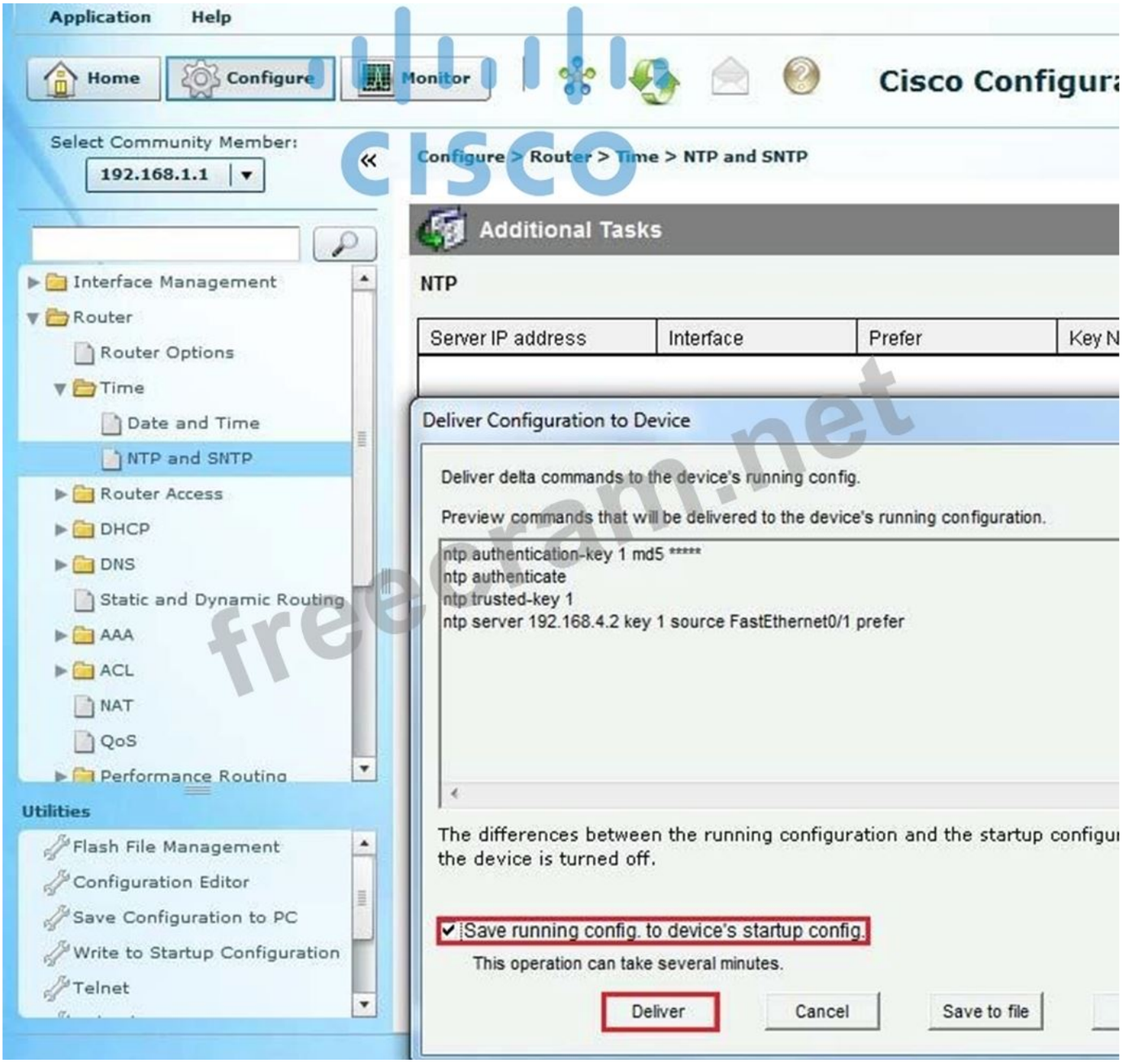
To configure NTP you have to navigate to Configure>Router>Time>NTP and SNMP and click on "Add.." button



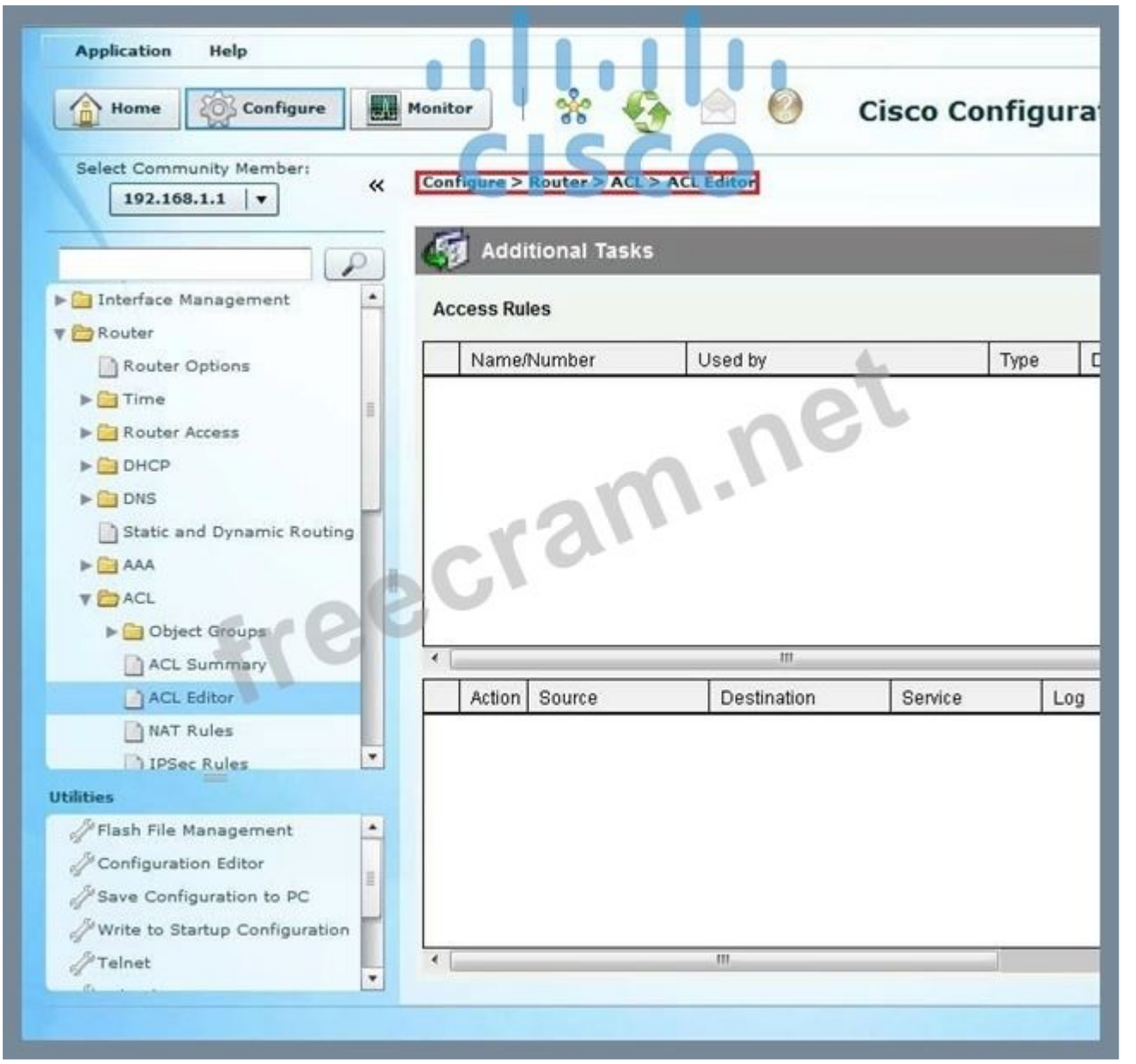
Enter the NTP Server IP, choose interface, type key number, value and click on "Prefer" and Ok.



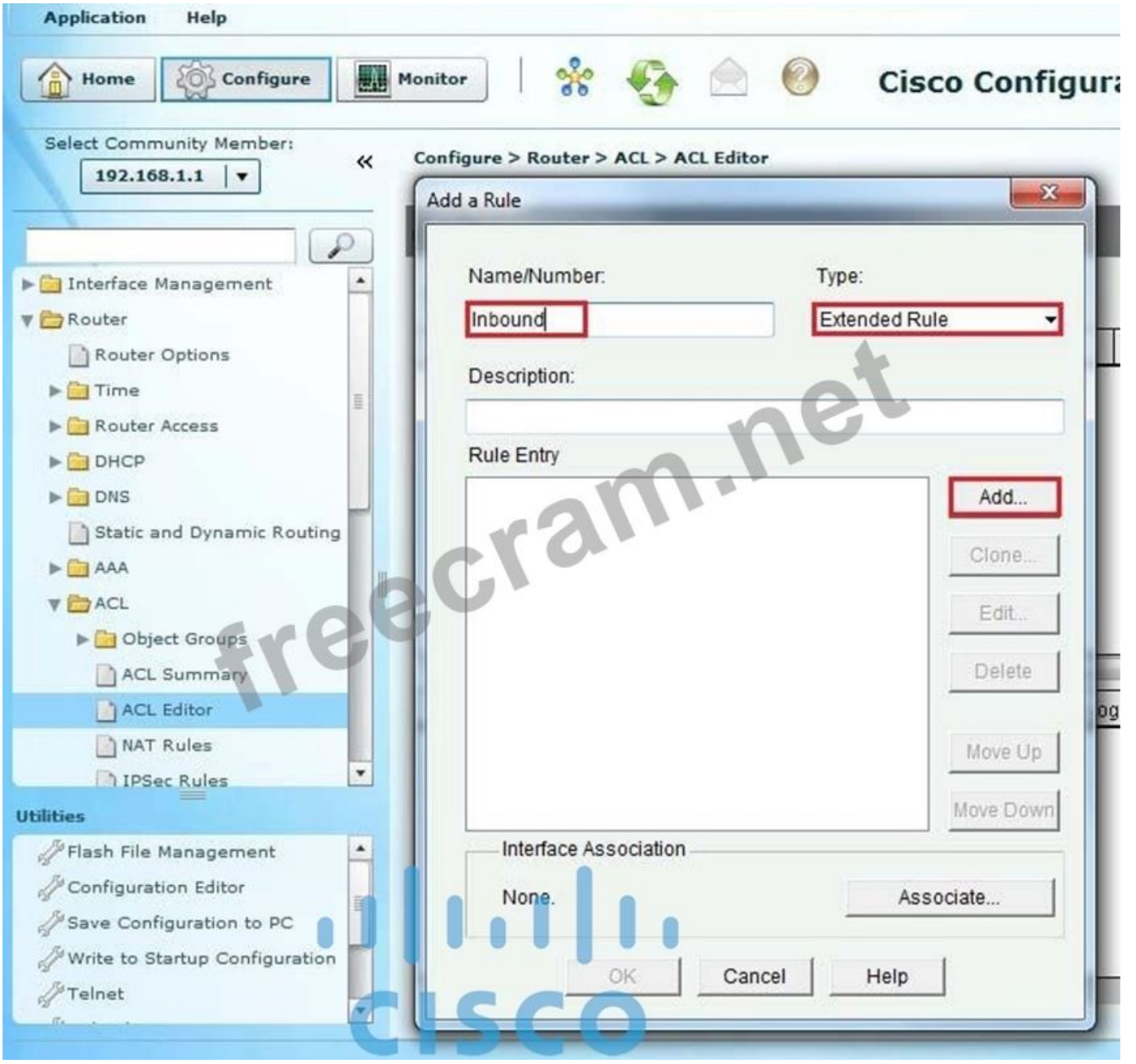
After save configuration file and click on "Deliver".



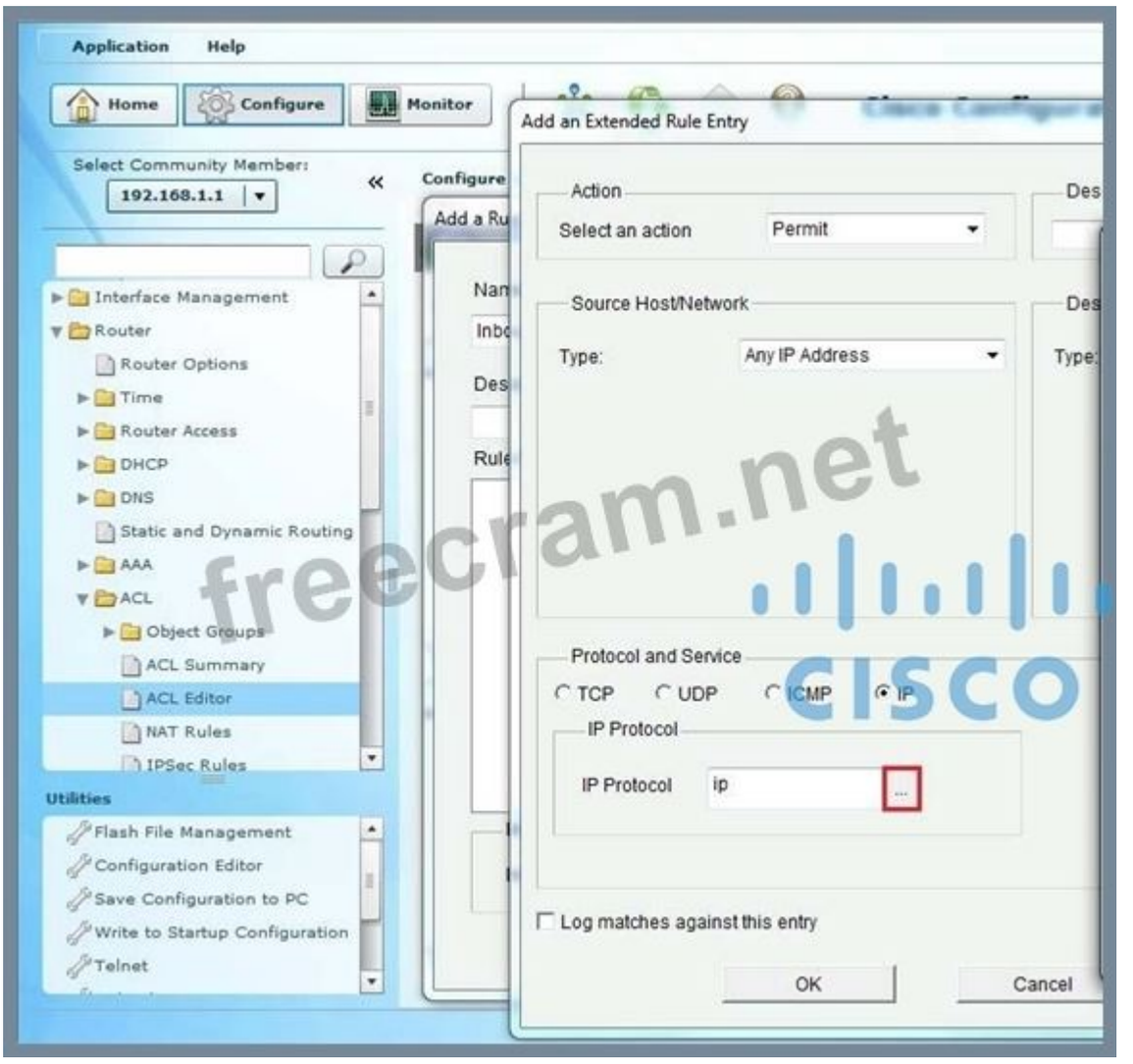
To configure Access Rules you have to go to Configure>Router>ACL>ACL Editor and click on "Add..." button.



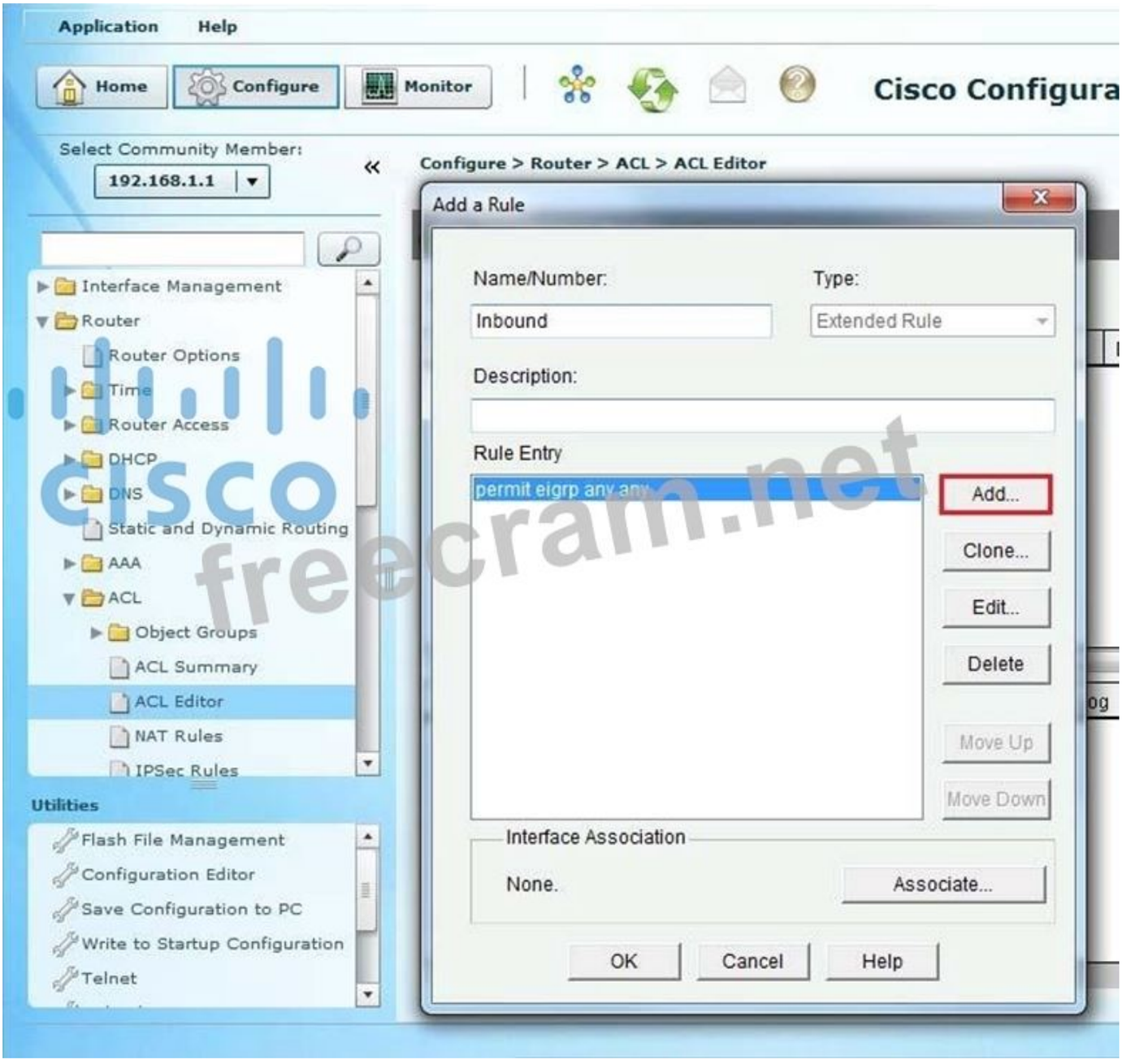
Enter name as "Inbound", make sure it is Extended ACL and click on "Add..."



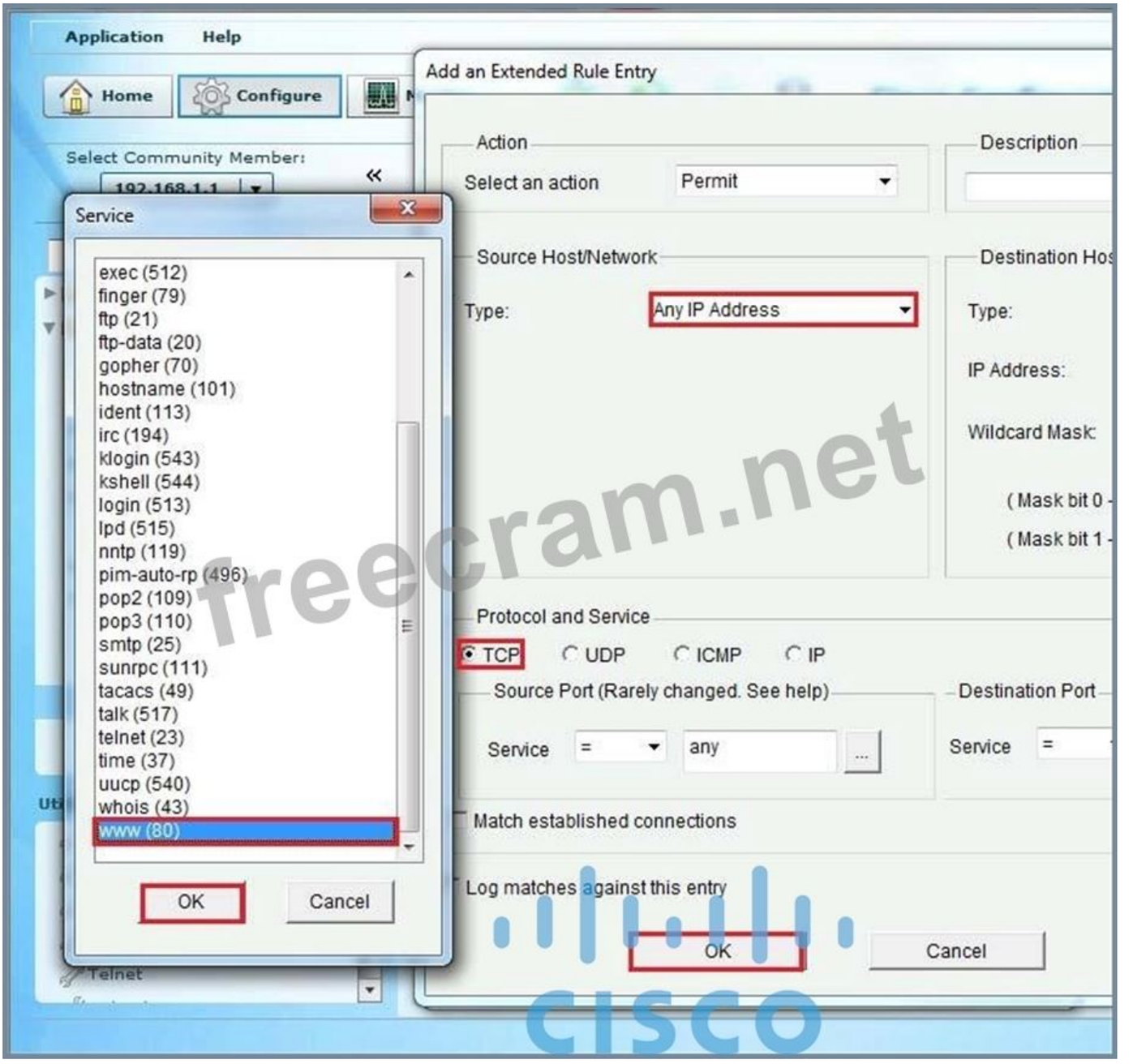
After check "Action", make sure it is "Permit" (it is default state in CCP), live source and destination as "Any" (it is default state in CCP). Then navigate to "Protocol and Service" and choose "EIGRP" as a protocol. Click "Ok".



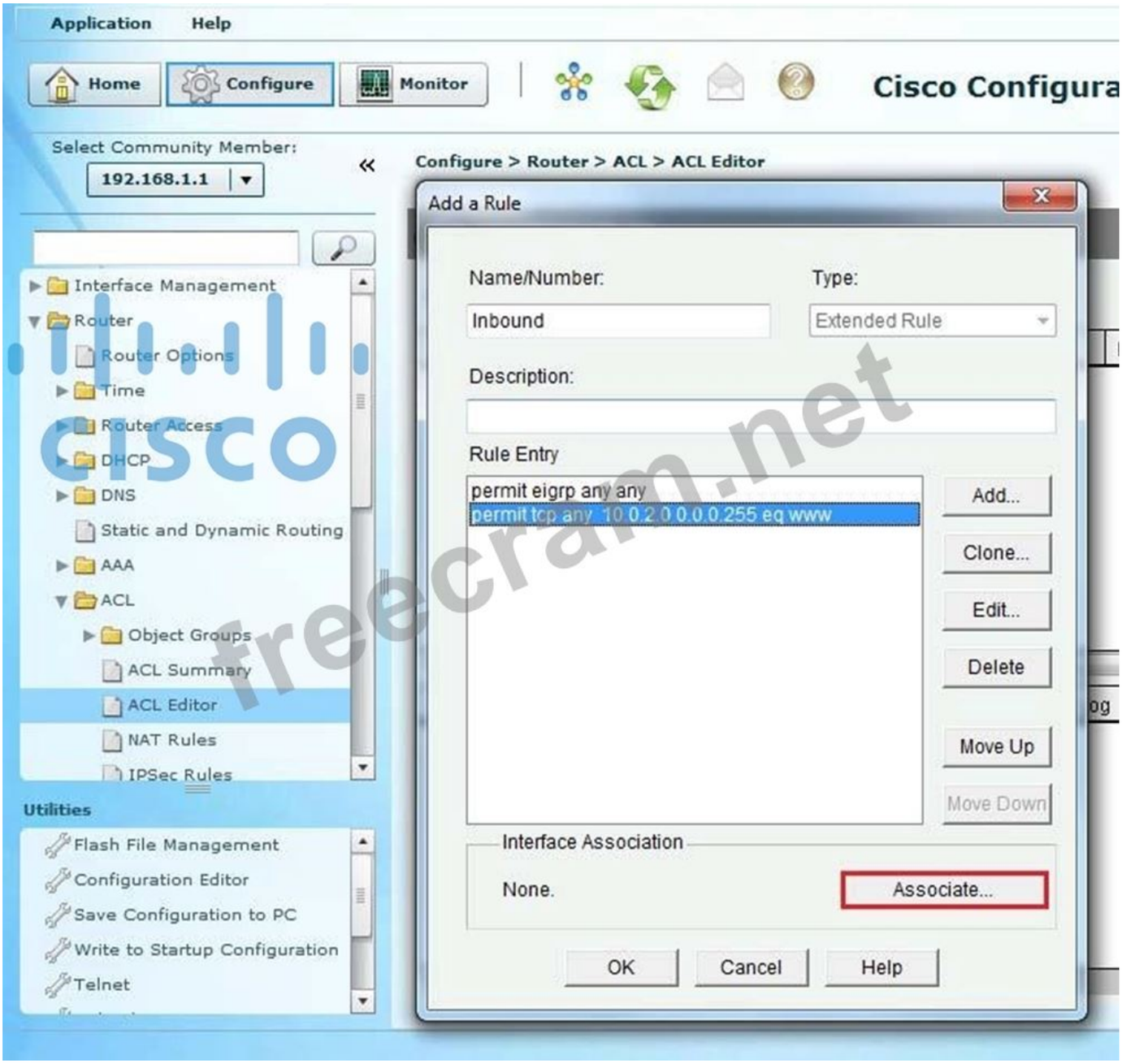
After click "Add..." now create another ACL to permit "HTTP" traffic.



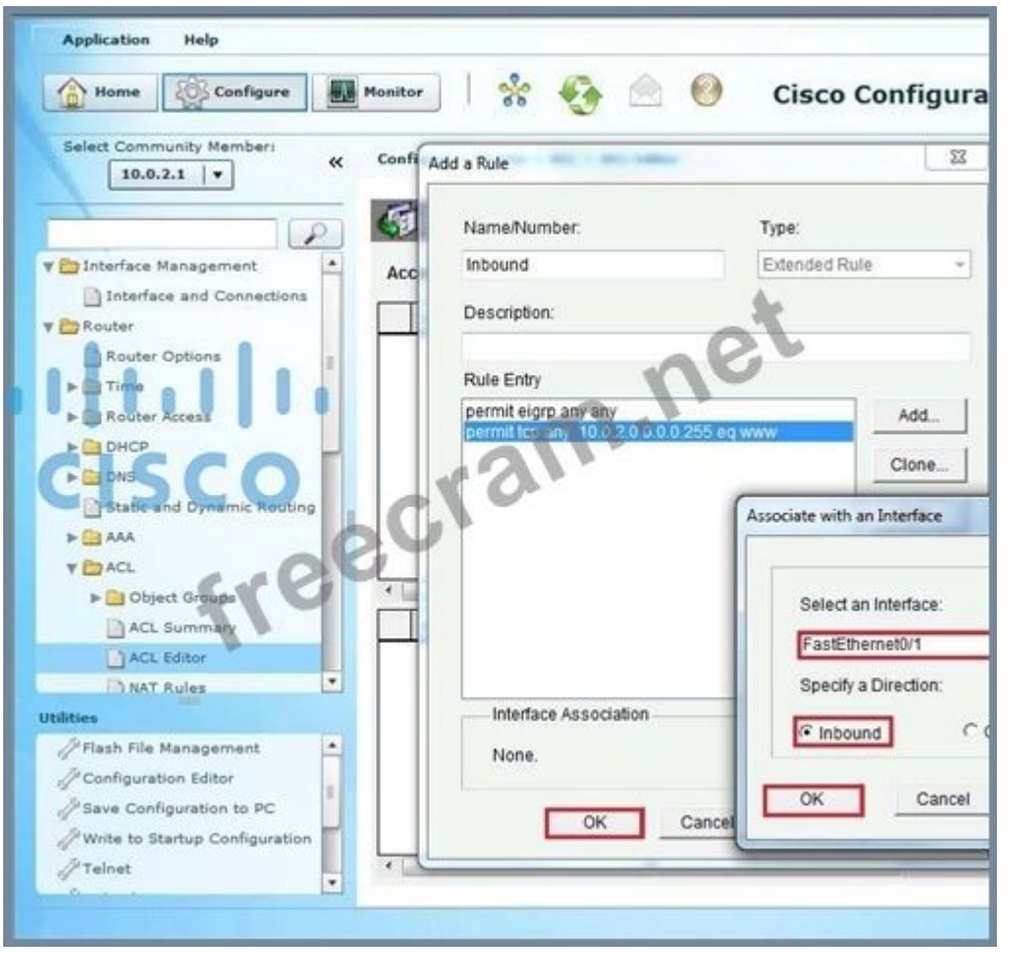
Make sure "Action" is "Permit" (it is default state in CCP), live source as "Any" . In destination section choose " A Network" as a "Type", put appropriate IP address and wildcard mask. Navigate to "Protocol and Service", select "TCP", source port live as "Any" (it is default state in CCP) but destination port we have to change for "80". Click on Service box and pick up in the end of list www(80). Click "Ok" in both windows.



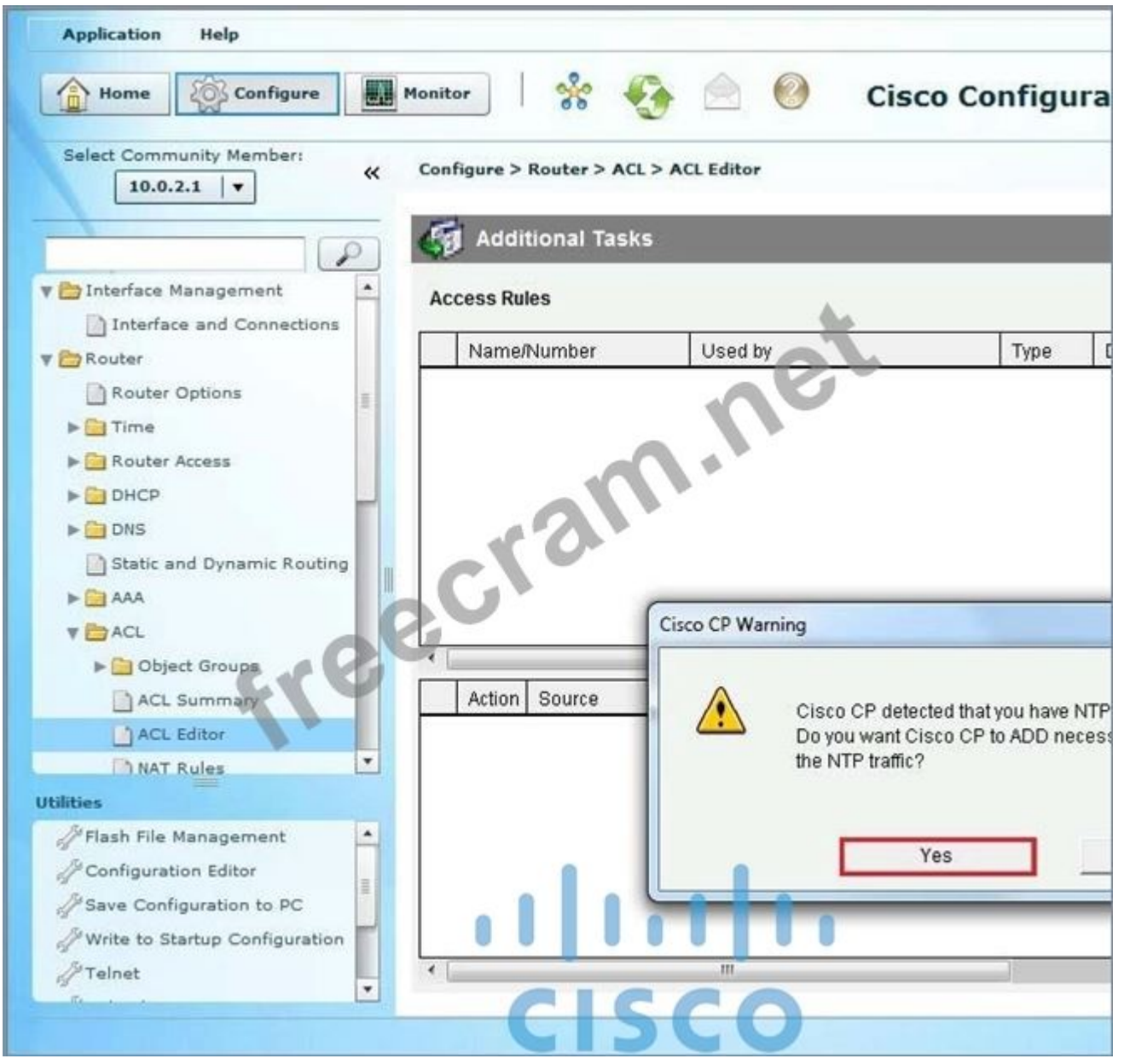
Now we have to associate our ACL rules to the OUTSIDE interface with INBOUND direction. Click on "Associate..".



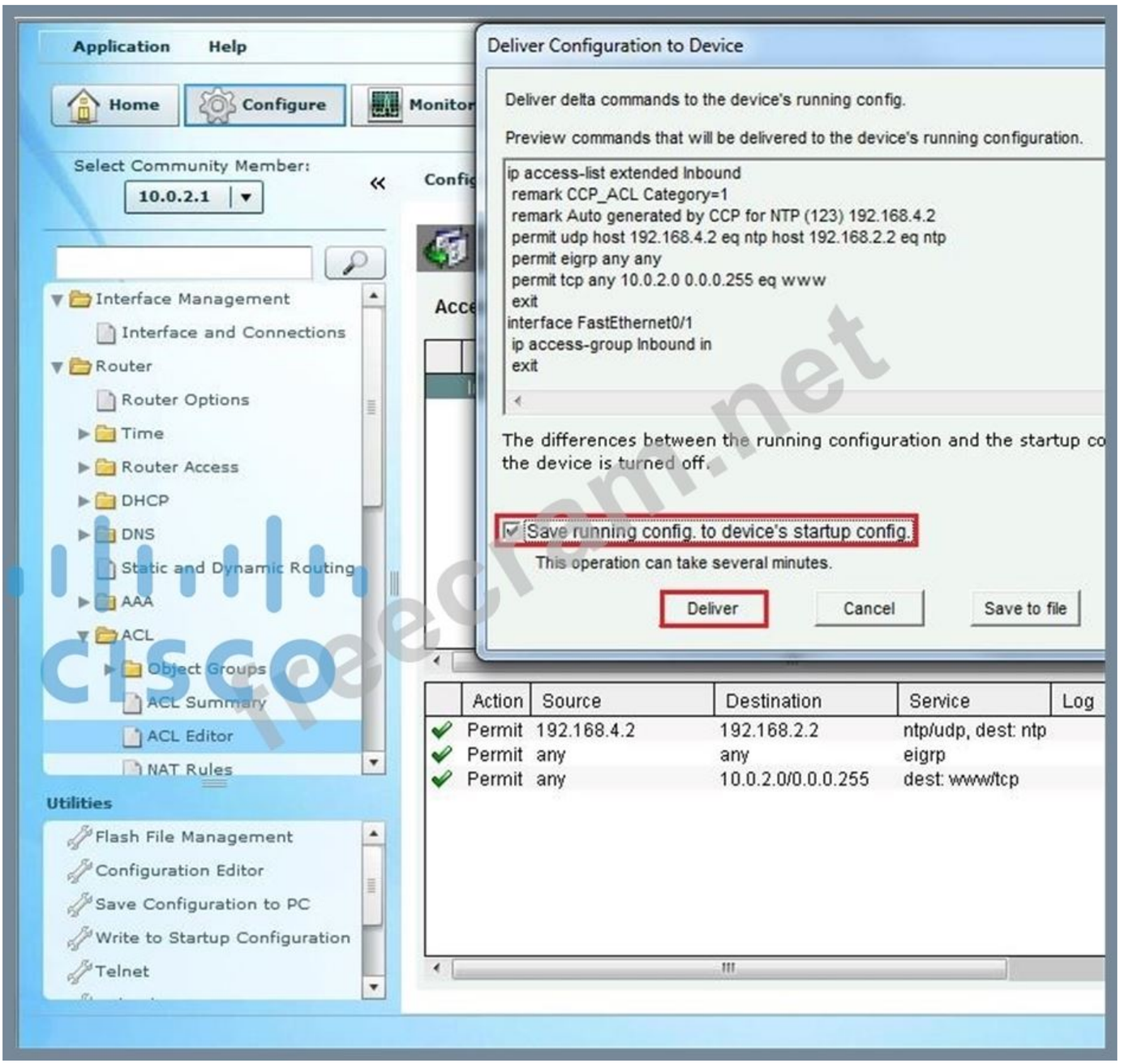
Early we discovered that our OUTSIDE interface is FastEthernet0/1. Choose from list FastEthernet0/1, specify a destination as "Inbound". Click "Ok".

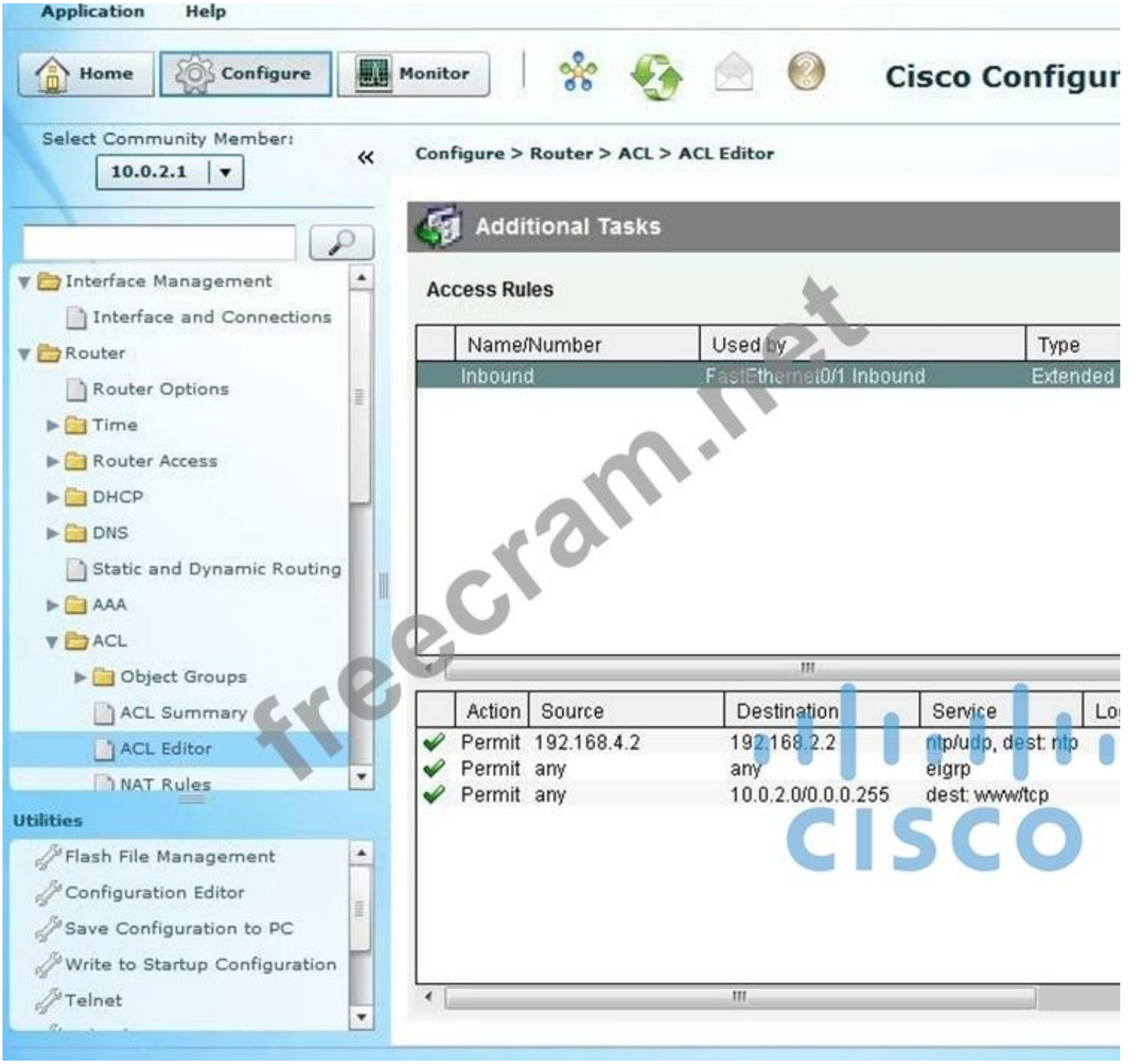


You will get this Cisco CP Warning. Requirements says that we have to add entry rule to allow NTP traffic. Click "Yes".



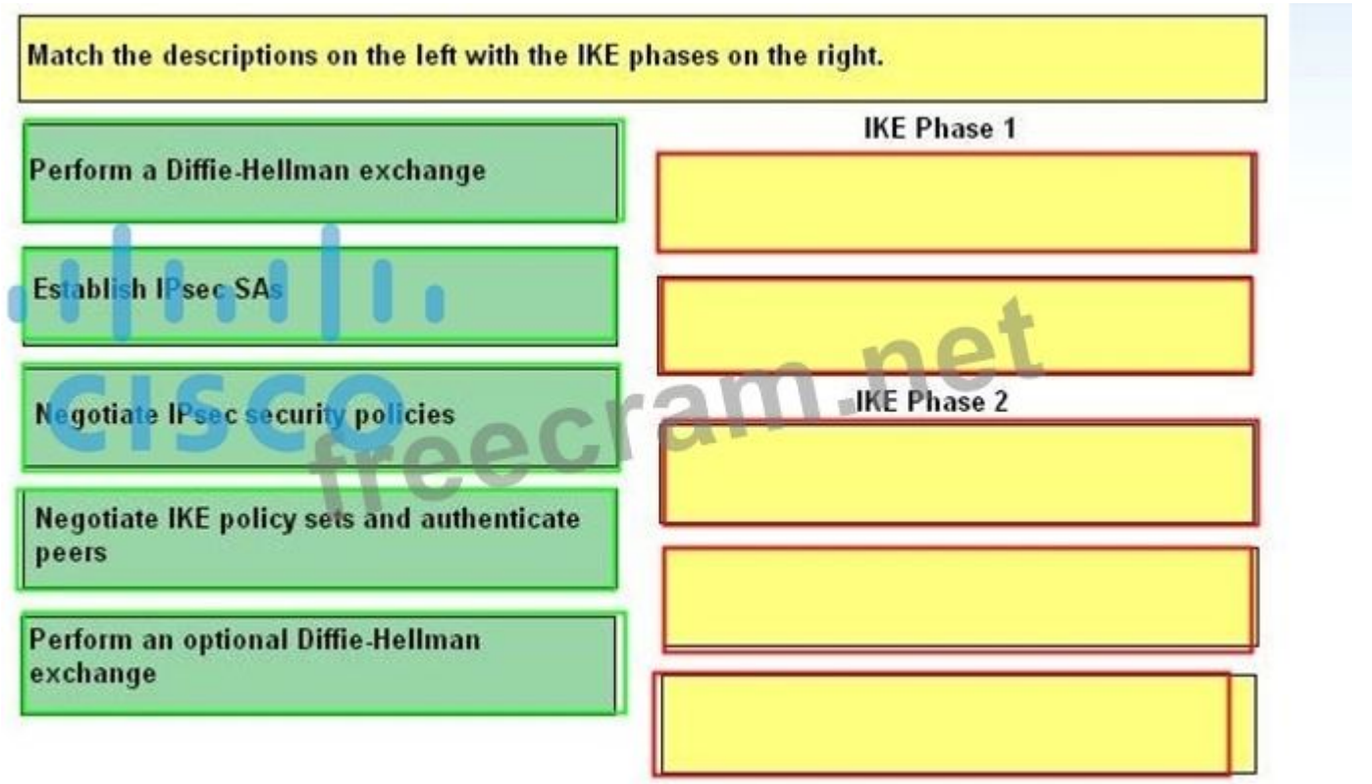
Final step save the configuration and click "Deliver.


Application
Help
Home
Configure
Monitor
Select Community Member:
10.0.2.1
Interface Management
Interface and Connections
Router
Router Options
Time
Router Access
DHCP
DNS
Static and Dynamic Routing
AAA
ACL
Object Groups
ACL Summary
ACL Editor
NAT Rules
Utilities
Flash File Management
Configuration Editor
Save Configuration to PC
Write to Startup Configuration
Telnet
Deliver Configuration to Device
Deliver delta commands to the device's running config.
Preview commands that will be delivered to the device's running configuration.
ip access-list extended Inbound
remark CCP_ACL Category=1
remark Auto generated by CCP for NTP (123) 192.168.4.2
permit udp host 192.168.4.2 eq ntp host 192.168.2.2 eq ntp
permit eigrp any any
permit tcp any 10.0.2.0 0.0.0.255 eq www
exit
interface FastEthernet0/1
ip access-group Inbound in
exit
The differences between the running configuration and the startup co
the device is turned off.
Save running config. to device's startup config.
This operation can take several minutes.
Deliver
Cancel
Save to file
Action
Source
Destination
Service
Log
Permit
192.168.4.2
192.168.2.2
ntp/udp, dest: ntp
Permit
any
any
eigrp
Permit
any
10.0.2.0/0.0.0.255
dest: www/tcp

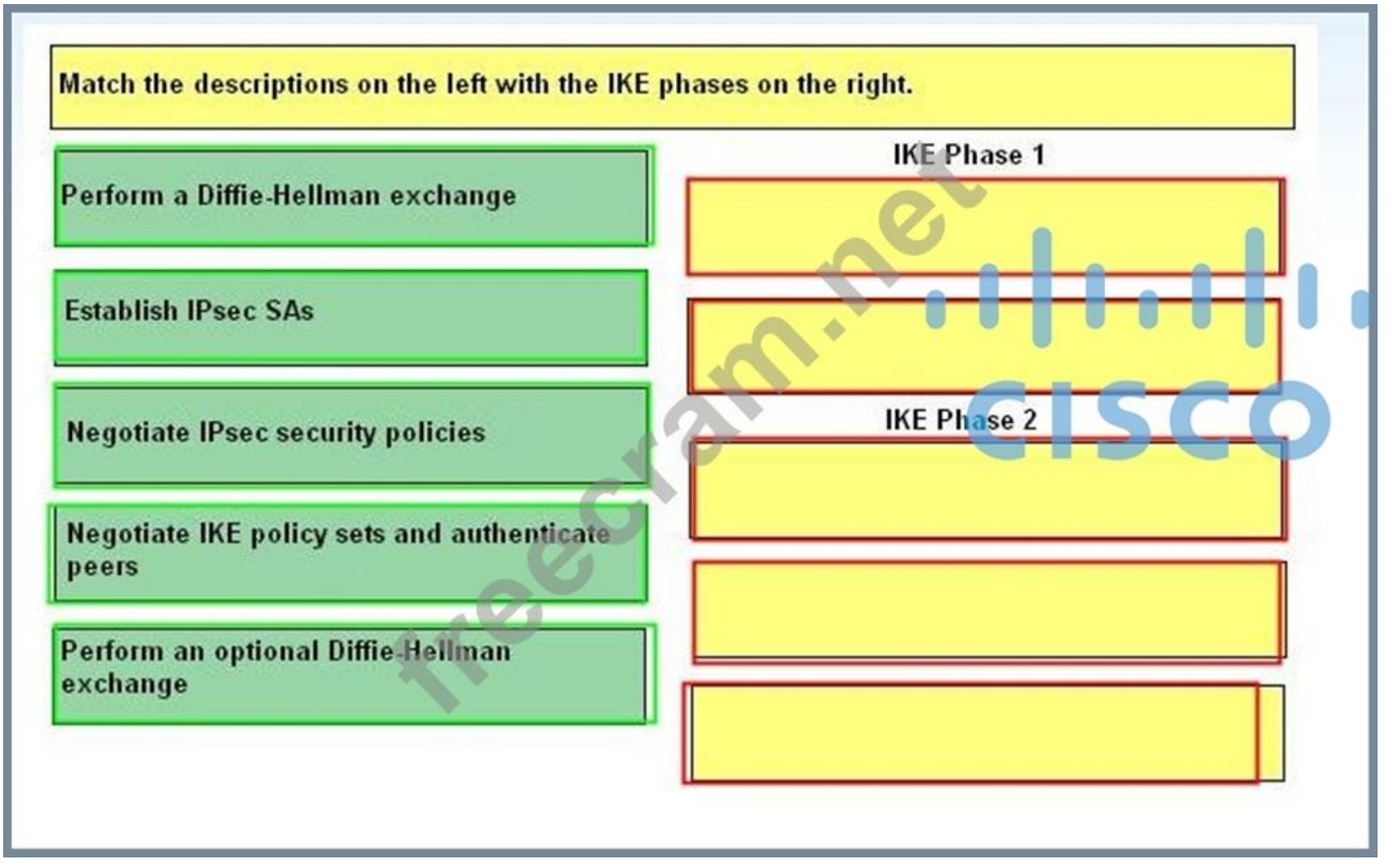


Exam D

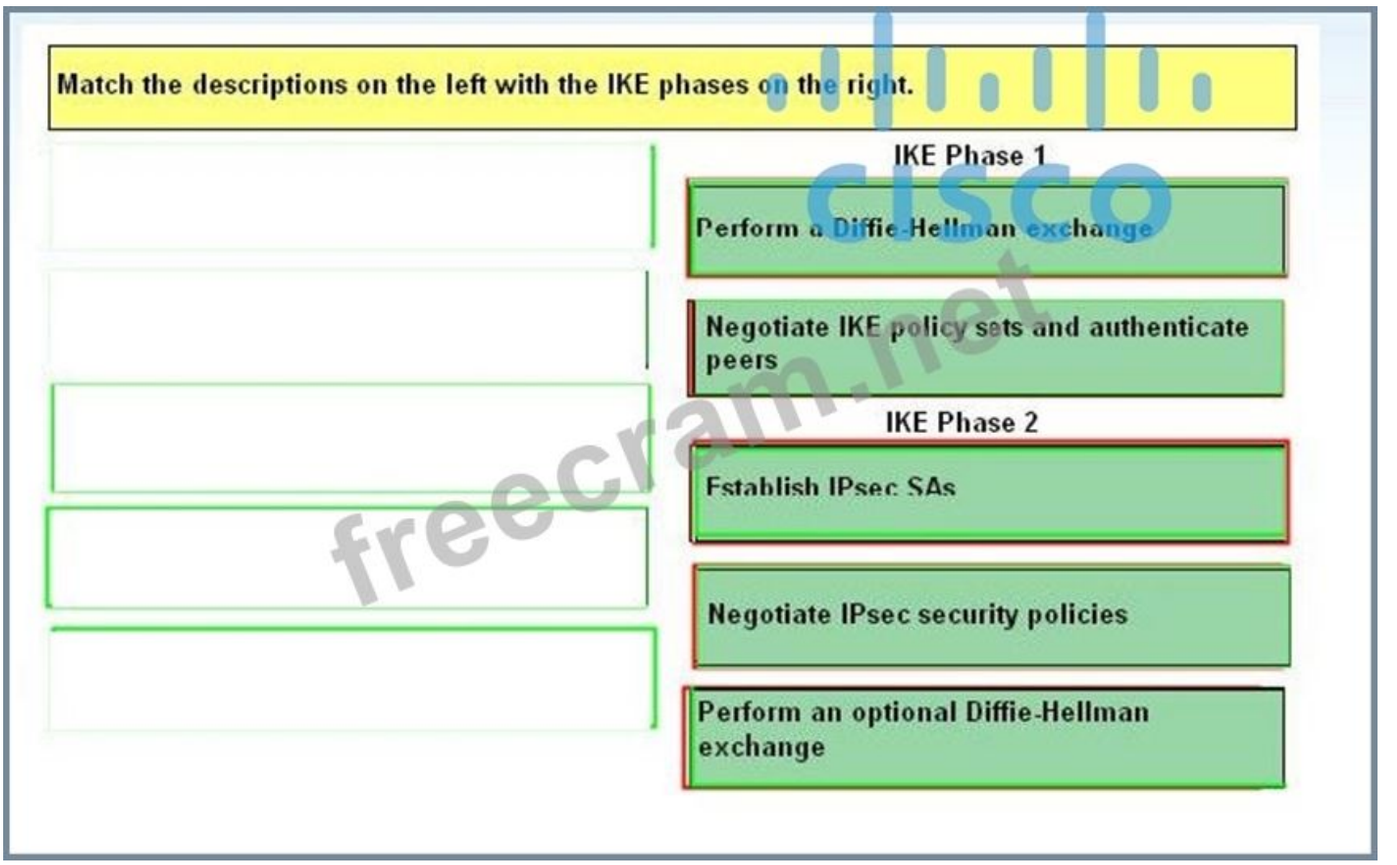
NEW QUESTION: 51



Select and Place:



Answer:



NEW QUESTION: 52
Which characteristic is the foundation of Cisco Self-Defending Network technology?
A. secure network platform
B. threat control and containment
C. policy management
D. secure connectivity
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Which three options are common examples of AAA implementation on Cisco routers? (Choose three.)
A. securing the router by locking down all unused services
B. tracking Cisco NetFlow accounting statistics
C. authenticating administrator access to the router console port, auxiliary port, and vty ports
D. implementing PKI to authenticate and authorize IPsec VPN peers using digital certificates
E. authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
F. performing router commands authorization using TACACS+
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Which statement about control plane policing is true?

A. Control Plane Policing classifies traffic into three categories to intercept malicious traffic.
B. Control Plane Policing allows Qos filtering to protect the control plane against Dos attacks.
C. Control Plane Policing intercepts and classifies all traffic.
D. Control Plane Policing allows ACL-based filtering to protect the control plane against Dos attacks.
Answer: (SHOW ANSWER)

NEW QUESTION: 55
When STP mitigation features are configured, where should the root guard feature be deployed?
A. on all switch ports
B. Root guard should be configured globally on the switch.
C. toward ports that connect to switches that should not be the root bridge
D. toward user-facing ports
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Which statement about asymmetric encryption algorithms is true?
A. They use different keys for encryption and decryption of data.
B. They use the same key for encryption and decryption of data.
C. They use different keys for decryption but the same key for encryption of data.
D. They use the same key for decryption but different keys for encryption of data.
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Which three statements about TACAS+ are true? (Choose three)
A. TACAS+ uses UDP port 1645 and 1812.
B. TACAS+ encrypts the entire packet.
C. TACAS+ is a Cisco proprietary technology.
D. TACAS+ encrypts only the password in the Access-Request packet.
E. TACAS+ is an open standard.
F. TACAS+ uses TCP port 49.
Answer: (SHOW ANSWER)

NEW QUESTION: 58
When a network transitions from IPV4 to IPV6, how many bits does the address expand to?
A. 128 bits
B. 96 bits
C. 64 bits
D. 156 bits
Answer: (SHOW ANSWER)

NEW QUESTION: 59
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. unretired and enabled
B. successfully complied and unretired
C. unretired
D. enabled
E. successfully complied
F. successfully complied and enabled
G. enabled, unretired and successfully complied
Answer: (SHOW ANSWER)

NEW QUESTION: 60
security control is defense in depth?
A. risk analysis
B. botnet mitigation
C. threat mitigation
D. overt and covert channels
Answer: (SHOW ANSWER)

NEW QUESTION: 61
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: (SHOW ANSWER)
Explanation/Reference:

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.

NEW QUESTION: 62
Which type of Layer 2 attack causes a switch to flood all incoming traffic to all ports?
A. STP attack
B. CAM overflow attack
C. VLAN hopping attack
D. MAC spoofing attack
Answer: (SHOW ANSWER)

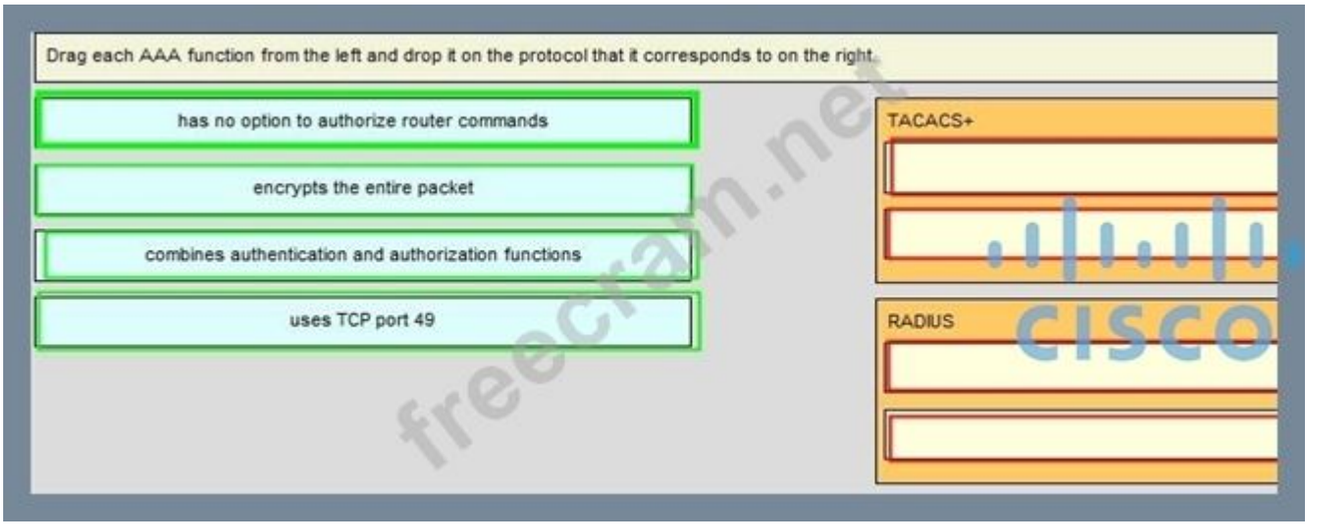
NEW QUESTION: 63
You suspect that an attacker in your network has configured a rogue Layer 2 device to intercept traffic from multiple VLANs, which allows the attacker to capture potentially sensitive data. Which two methods will help to mitigate this type of activity? (Choose two.)
A. Turn off all trunk ports and manually configure each VLAN as required on each port
B. Disable DTP on ports that require trunking
C. Set the native VLAN on the trunk ports to an unused VLAN

D. Place unused active ports in an unused VLAN

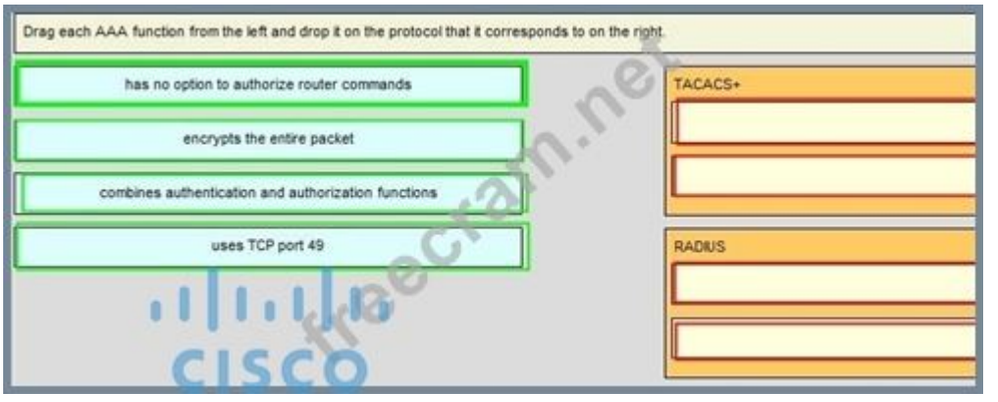
E. Secure the native VLAN, VLAN 1 with encryption

Answer: (SHOW ANSWER)

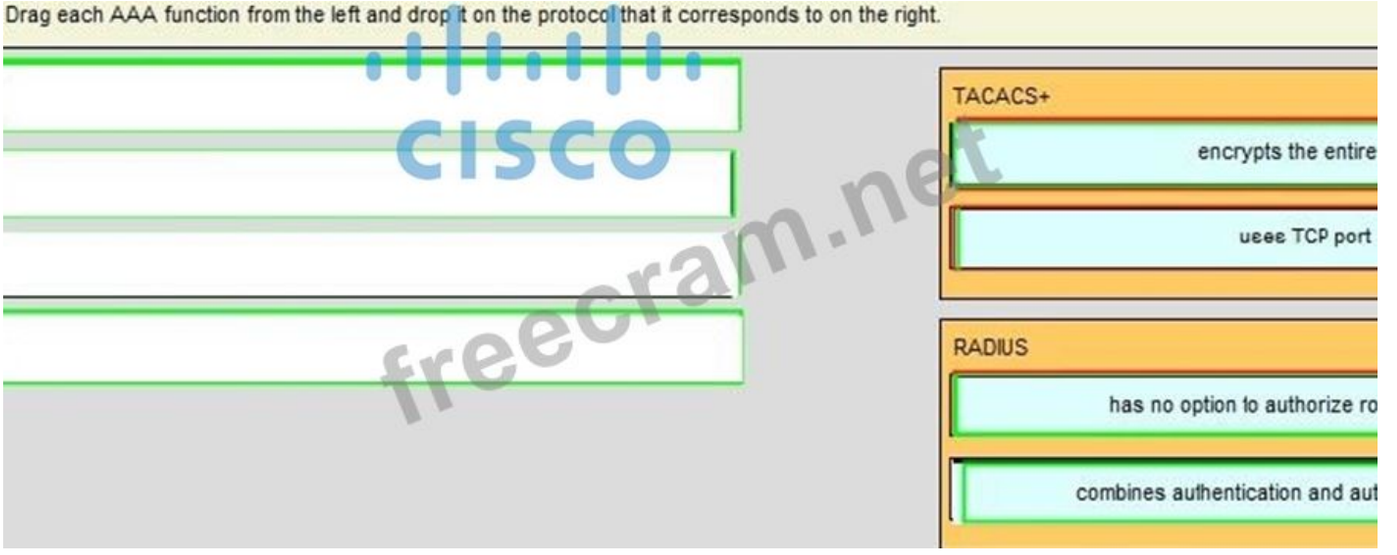
NEW QUESTION: 64



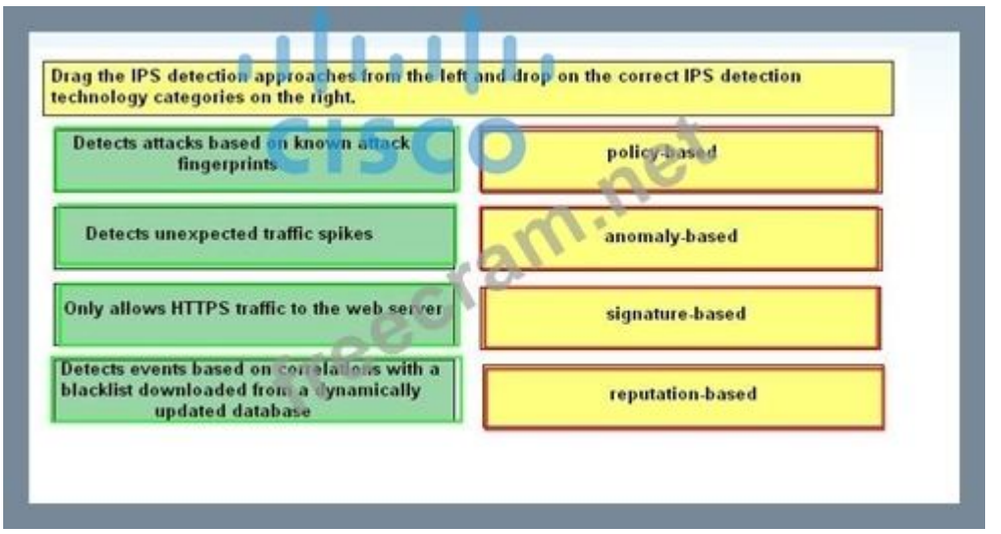
Select and Place:



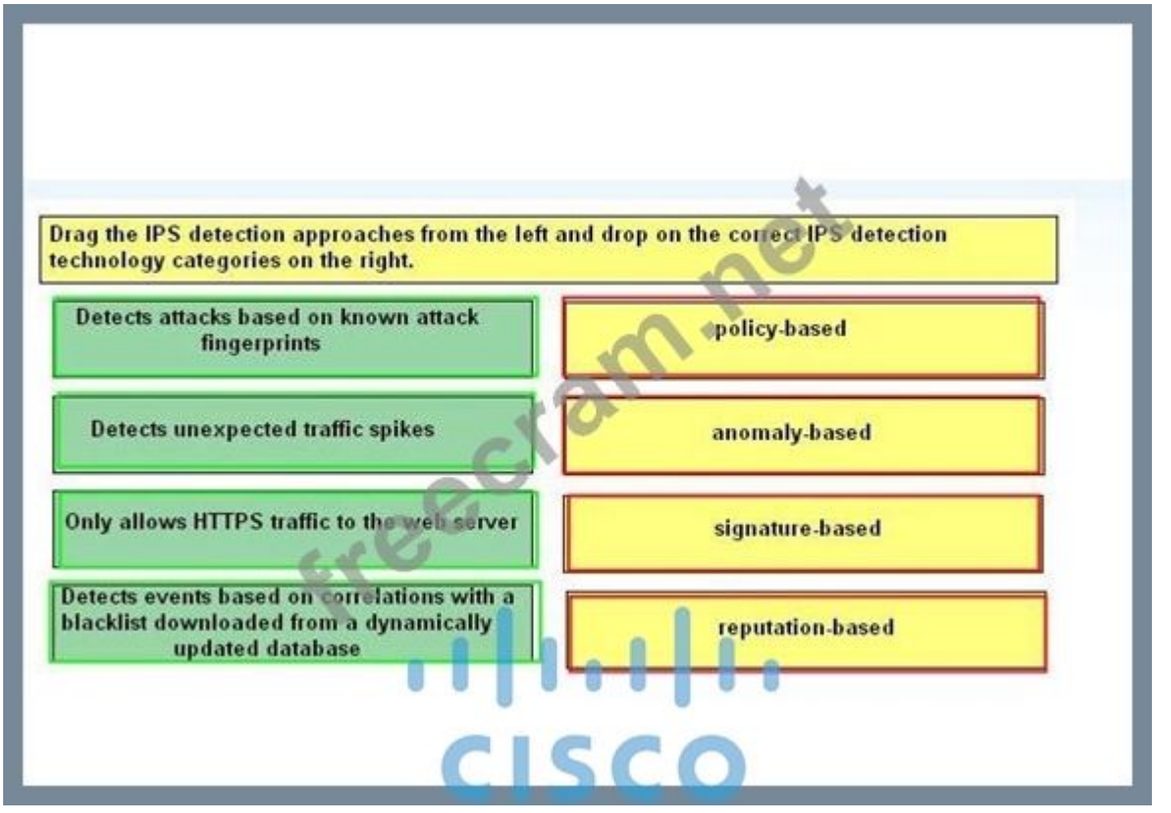
Answer:



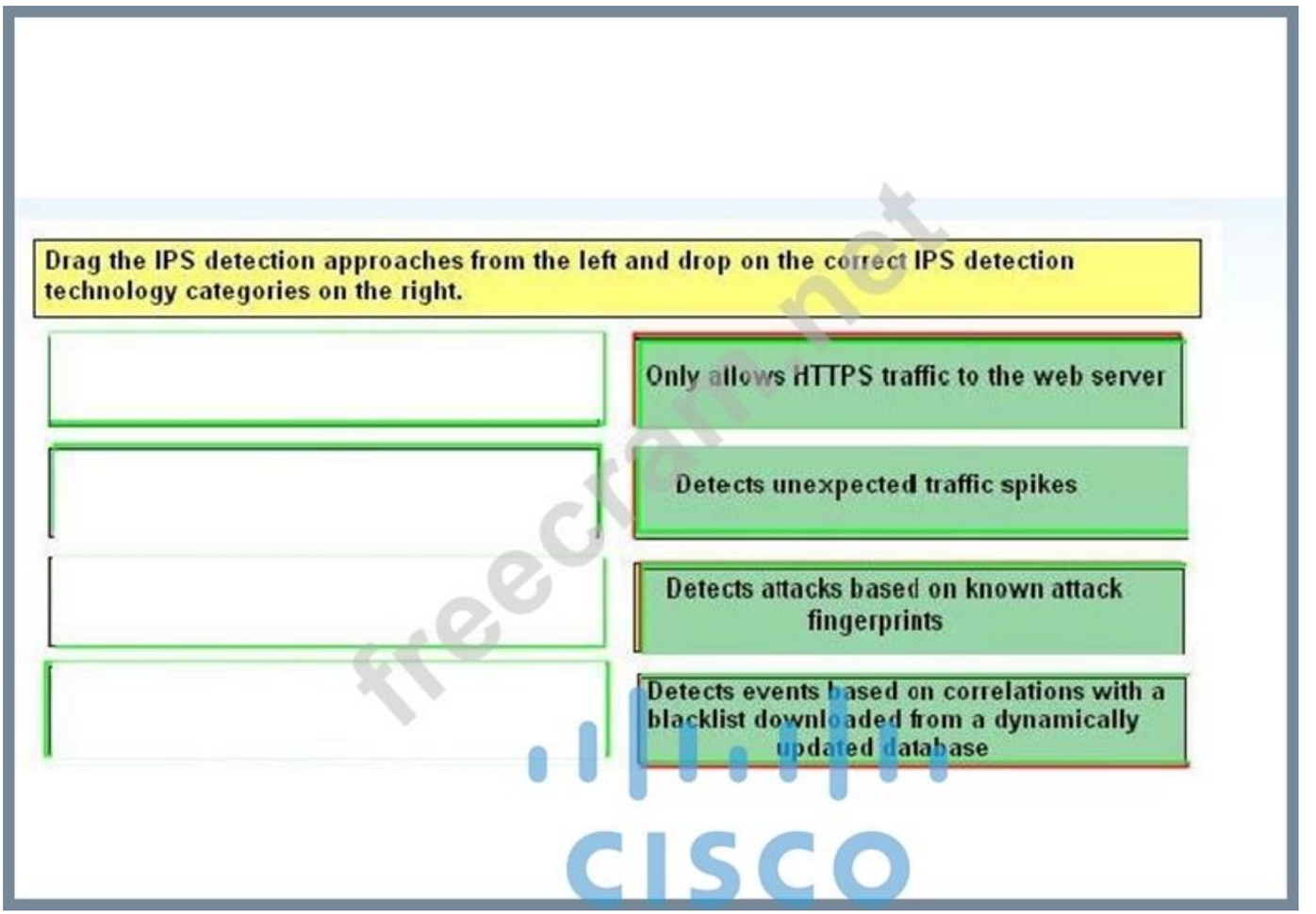
NEW QUESTION: 65



Select and Place:



Answer:



NEW QUESTION: 66
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 IKE policy
D. the pre-shared key
E. the interesting traffic (the traffic to be protected)
F. the IPsec transform-set
Answer: (SHOW ANSWER)

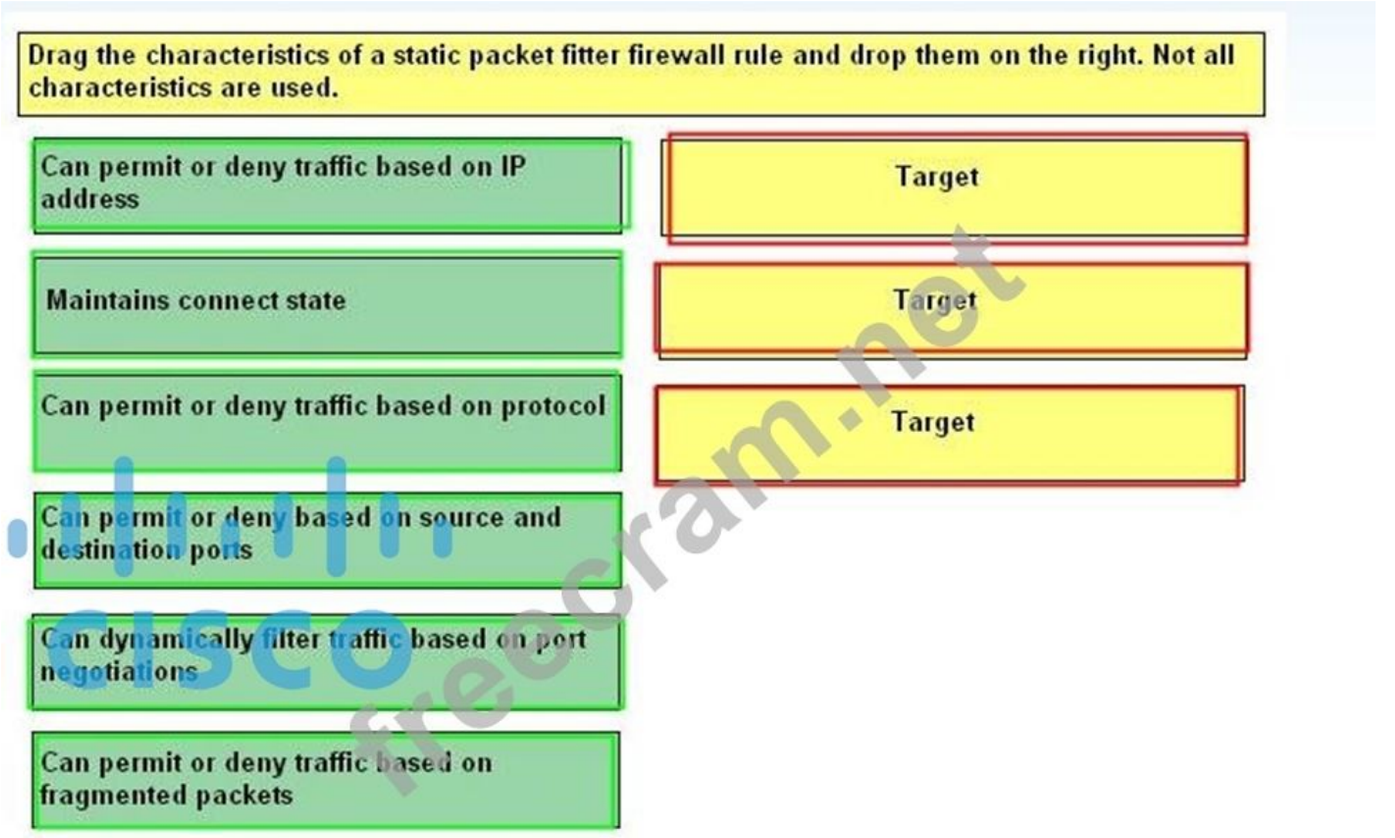
NEW QUESTION: 67
When configuring role-based CLI on a Cisco router, which step is performed first?
A. Log in to the router as the root user.
B. Create a parser view called "root view."
C. Enable role-based CLI globally on the router using the privileged EXEC mode Cisco IOS command.
D. Enable the root 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: (SHOW ANSWER)
Explanation
DRAG DROP

NEW QUESTION: 68
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 AIP-SSM
D. Cisco IOS IPS
Answer: (SHOW ANSWER)

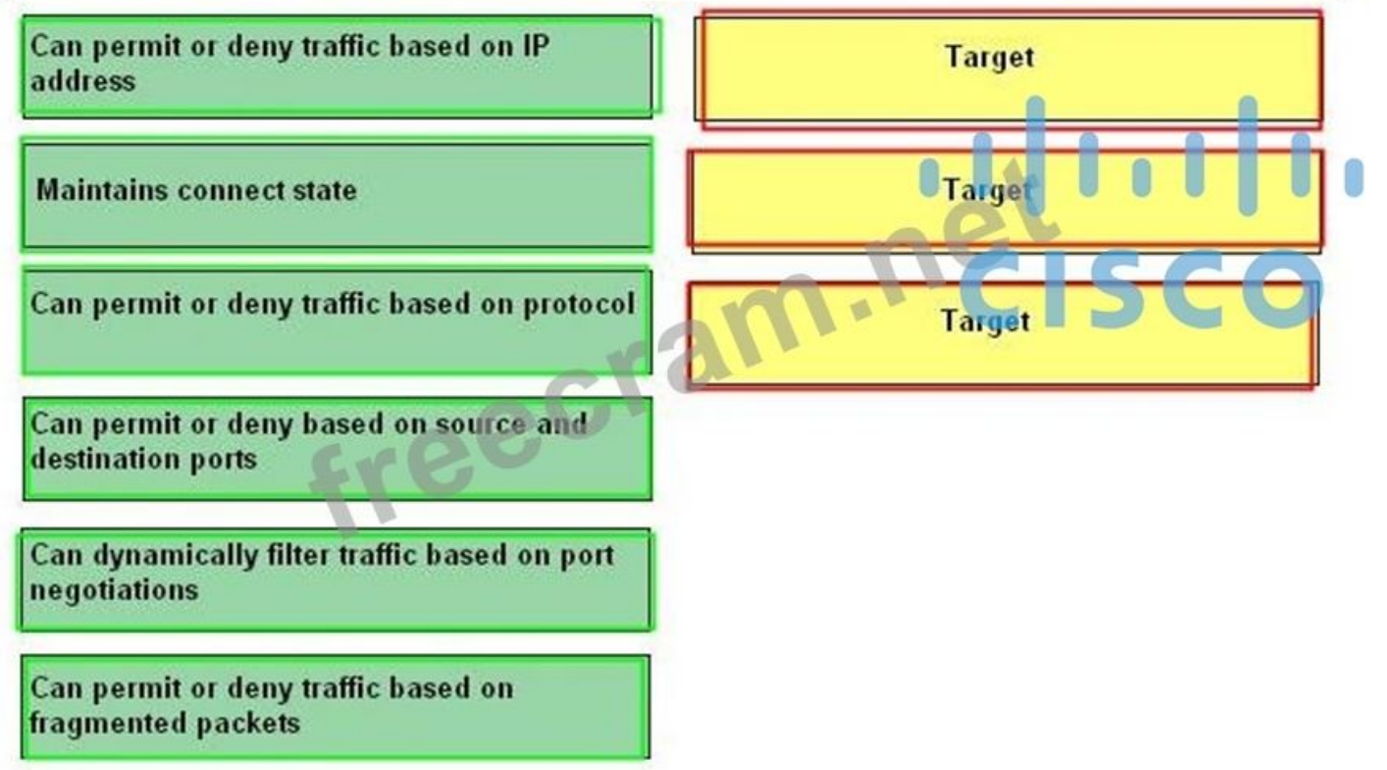
NEW QUESTION: 69
What is the best way to prevent a VLAN hopping attack?
A. Physically secure data closets.
B. Encapsulate trunk ports with IEEE 802.1Q.
C. Enable BDPU guard.
D. Disable DTP negotiations.
Answer: (SHOW ANSWER)

NEW QUESTION: 70

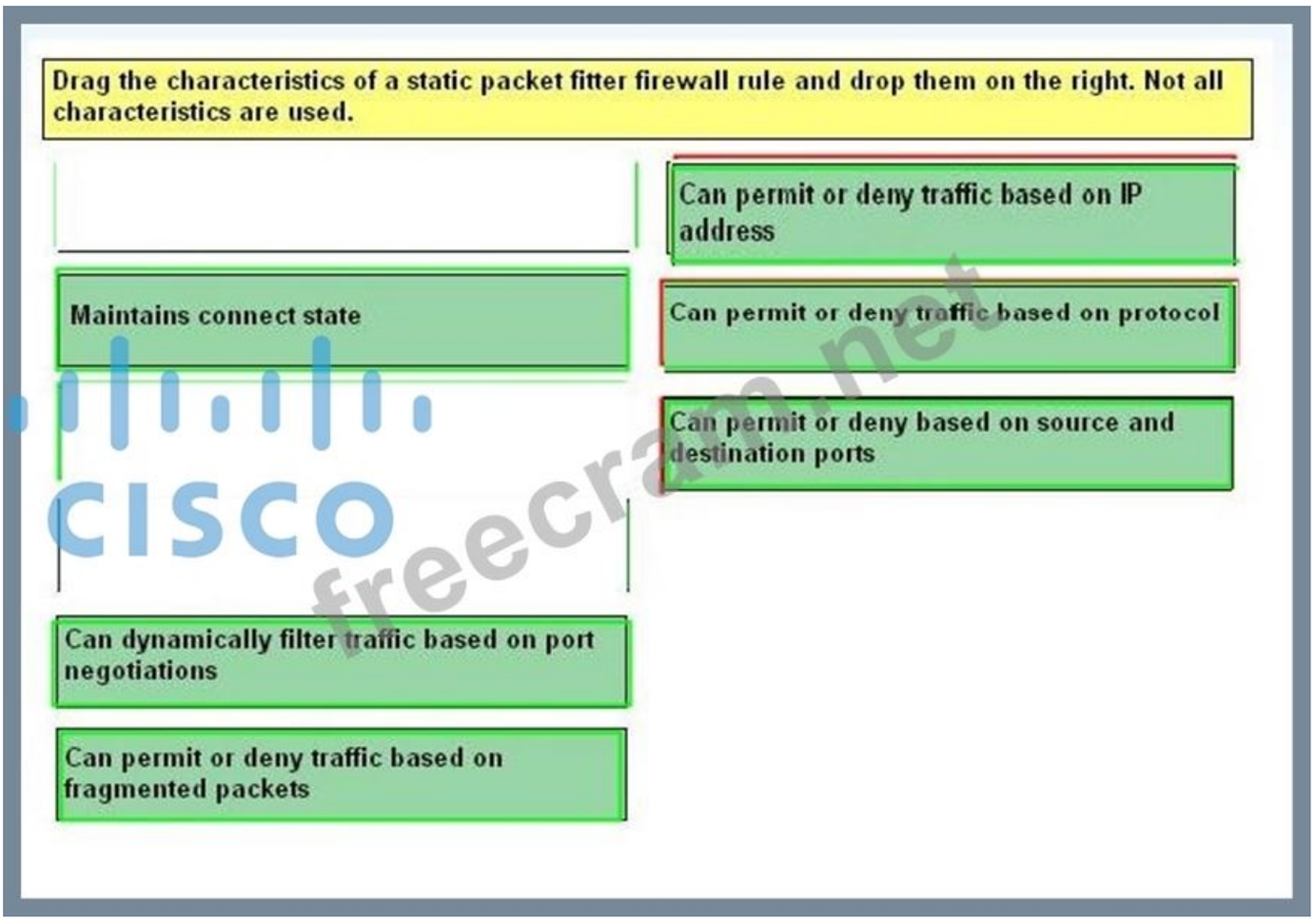


Select and Place:

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



Answer:



NEW QUESTION: 71
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: (SHOW ANSWER)
Explanation

NEW QUESTION: 72
Which step is important to take when implementing secure network management?
A. Implement management plane protection using routing protocol authentication.
B. Implement SNMP with read/write access for troubleshooting purposes.
C. Implement in-band management whenever possible.
D. Synchronize clocks on hosts and devices.
E. Implement telnet for encrypted device management access.
Answer: (SHOW ANSWER)

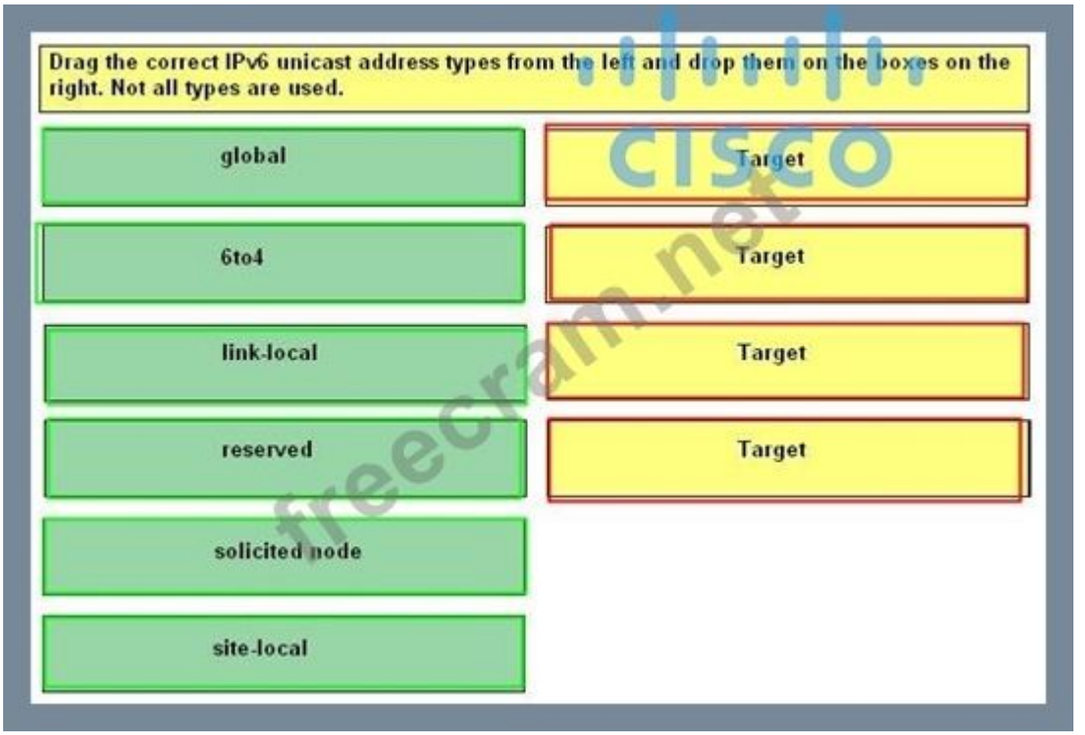
NEW QUESTION: 73
Which statement about an access control list that is applied to a router interface is true?
A. It filters pass-through and router-generated traffic.
B. It filters traffic in the inbound and outbound directions.
C. It only filters traffic that passes through the router.
D. An empty ACL blocks all traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which statement best represents the characteristics of a VLAN?
A. A VLAN is a logical broadcast domain that can span multiple physical LAN segments.
B. A VLAN provides individual port security.
C. Ports in a VLAN will not share broadcasts amongst physically separate switches.
D. A VLAN can only connect across a LAN within the same building.
Answer: (SHOW ANSWER)

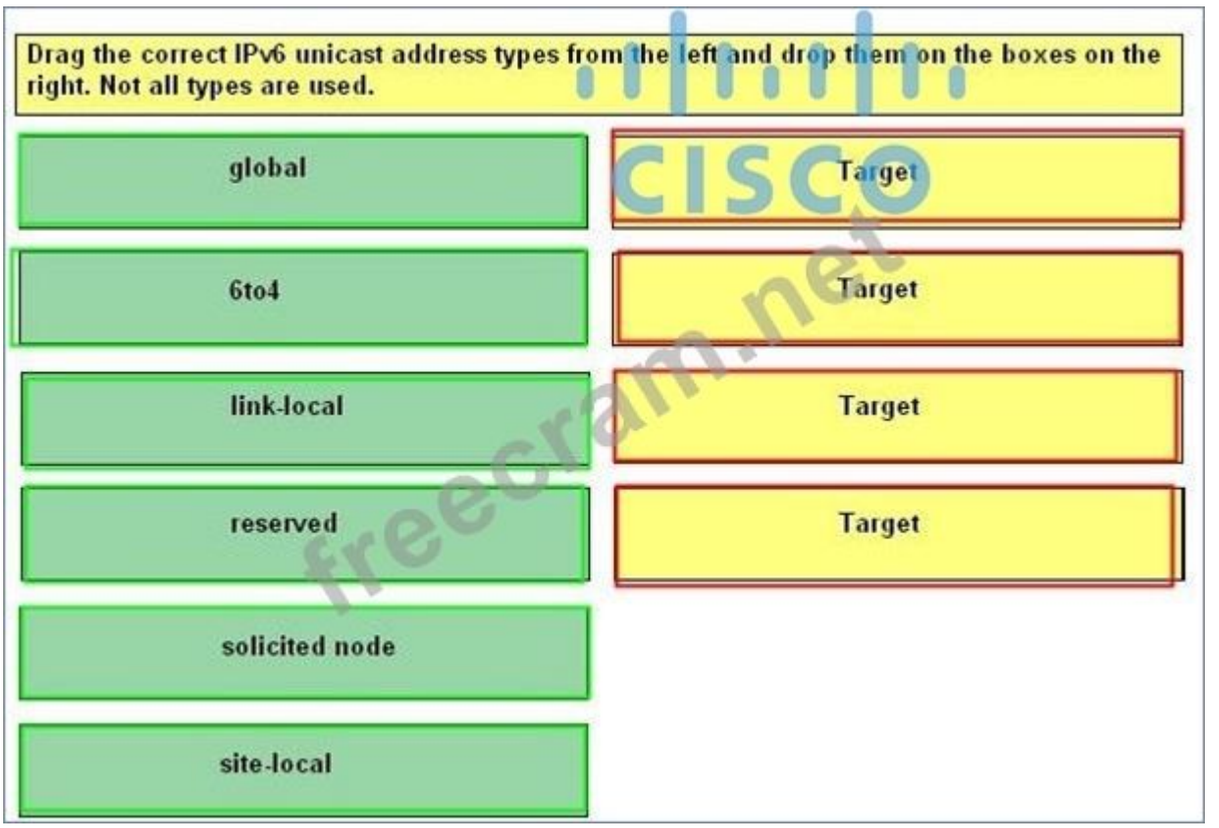
NEW QUESTION: 75
Which two considerations about secure network management are important? (Choose two.)
A. off-site storage
B. accurate time stamping
C. Do not use a loopback interface for device management access.
D. Use RADIUS for router commands authorization.
E. log tampering
F. encrjption algorithm strength
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Under which higher-level policy is a VPN security policy categorized?
A. compliance policy.
B. remote access policy.
C. corporate WAN policy.
D. DLP policy.
E. application policy.
Answer: (SHOW ANSWER)

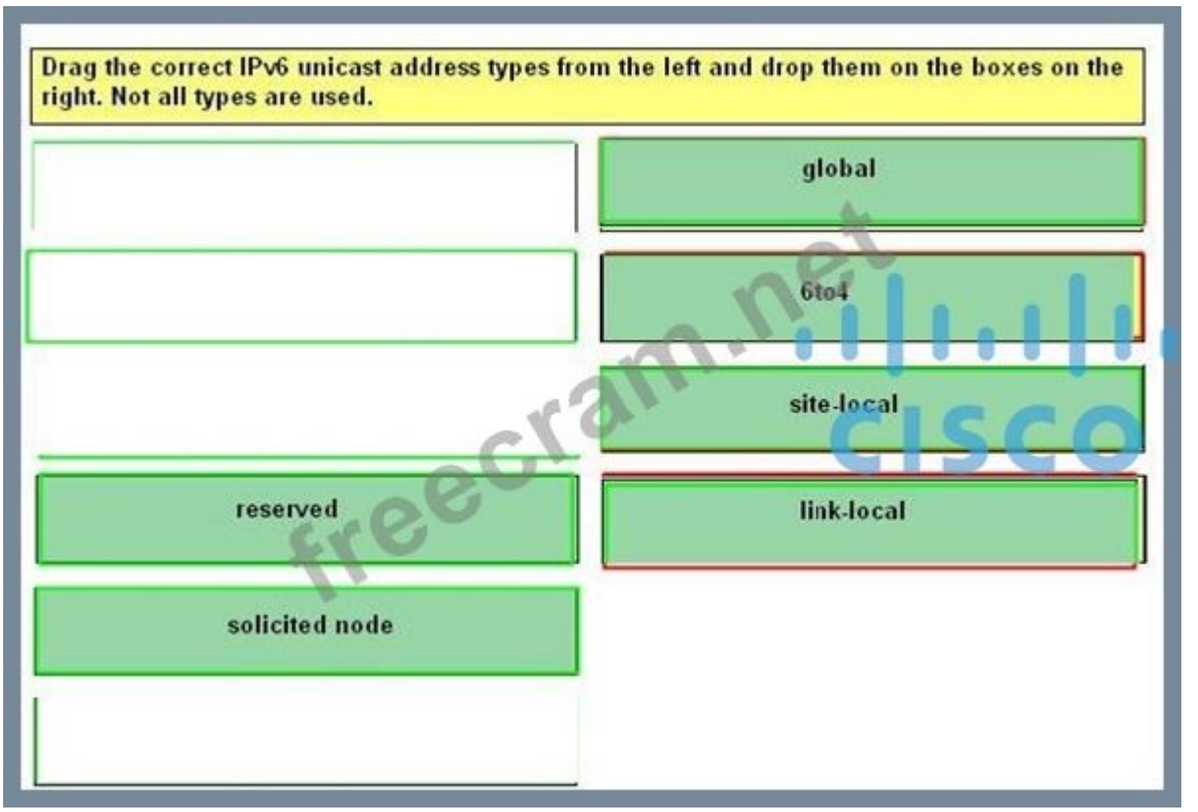
NEW QUESTION: 77



Select and Place:



Answer:



NEW QUESTION: 78
Which two statements about IPV6 access list are true? (Choose two).
A. IPV6 access list support wildcard masks.
B. IPV6 access list support extended access lists.
C. IPV6 access list support standard access lists.
D. IPV6 access list support numbered access lists.
E. IPV6 access list support named access lists.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
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: (SHOW ANSWER)

NEW QUESTION: 80
Which command enables Cisco IOS image resilience?
A. secure boot-running-config
B. secure boot-image
C. secure boot-<IOS image filename>
D. secure boot-start

Answer: (SHOW ANSWER)

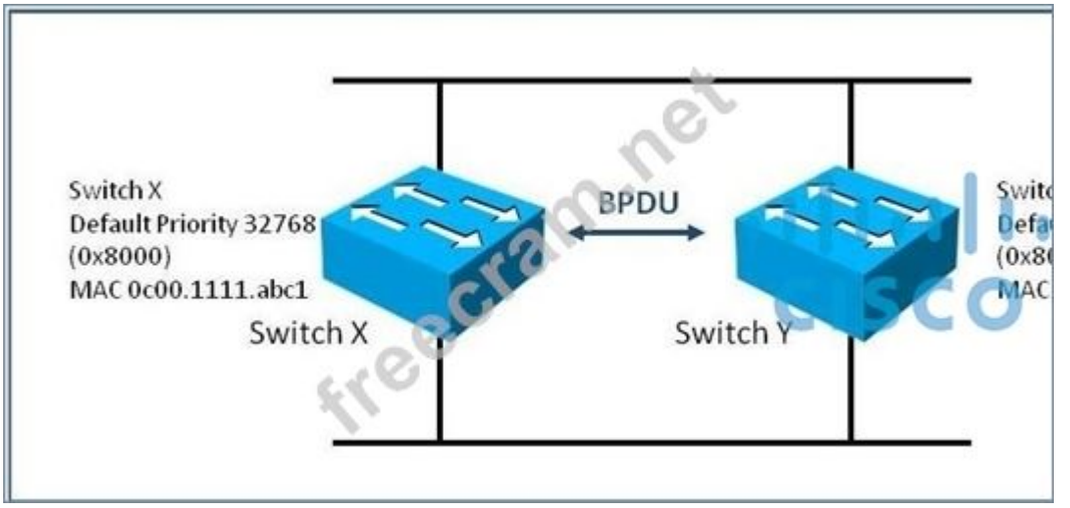
NEW QUESTION: 81
Refer to the exhibit. You are a network manager for your organization. You are looking at your Syslog server reports. Based on the Syslog message shown, which two statements are true? (Choose two.)

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

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: (SHOW ANSWER)
Explanation

NEW QUESTION: 82
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. connection profile
B. IP address pool
C. SSL VPN interlace
D. user authentication
E. group policy
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Refer to exhibit:



Which switch is designated as the root bridge in this topology?
A. SwitchY
B. It depends on which switch came on line first.

C. SwitchX

D. Neither switch would assume the role of root bridge because they have the same default priority.

Answer: (SHOW ANSWER)

NEW QUESTION: 84

Which statement about PVLAN Edge is true?

A. The switch does not forward any traffic from one protected port to any other protected port.

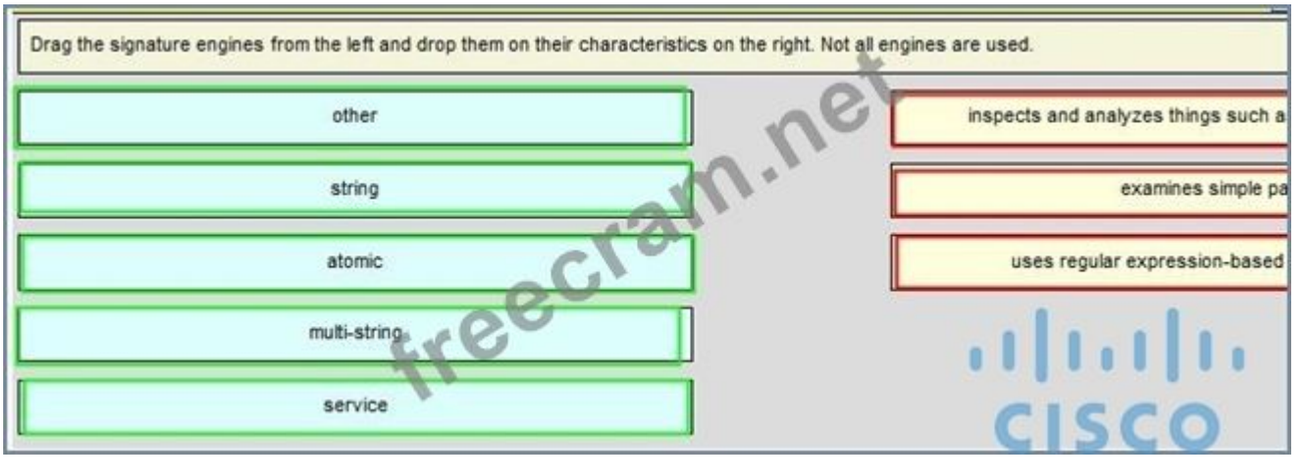
B. By default, when a port policy error occurs, the switchport shuts down.

C. PVLAN Edge can be configured to restrict the number of MAC addresses that appear on a single port.

D. The switch only forwards traffic to ports within the same VLAN Edge.

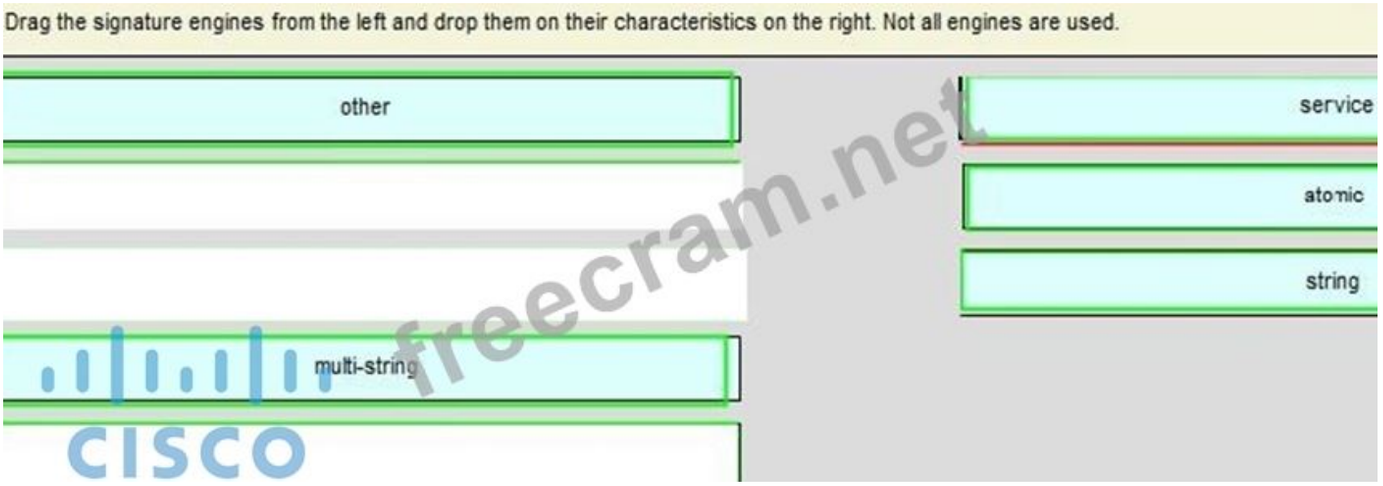
Answer: (SHOW ANSWER)

NEW QUESTION: 85



Select and Place:

Answer:



NEW QUESTION: 86
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 10 percent
B. Roughly 50 percent
C. Roughly 75 percent
D. Roughly 66 percent
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which AAA feature can automate record keeping within a network?
A. TACACS+
B. Accounting
C. Authorization
D. Authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which lype of intrusion prevention technology is the primary tipe used by the Cisco IPS security appliances?
A. NetFlow anomaly-based
B. profile-based
C. rule-based
D. signature-based
E. protocol analysis-based
Answer: (SHOW ANSWER)

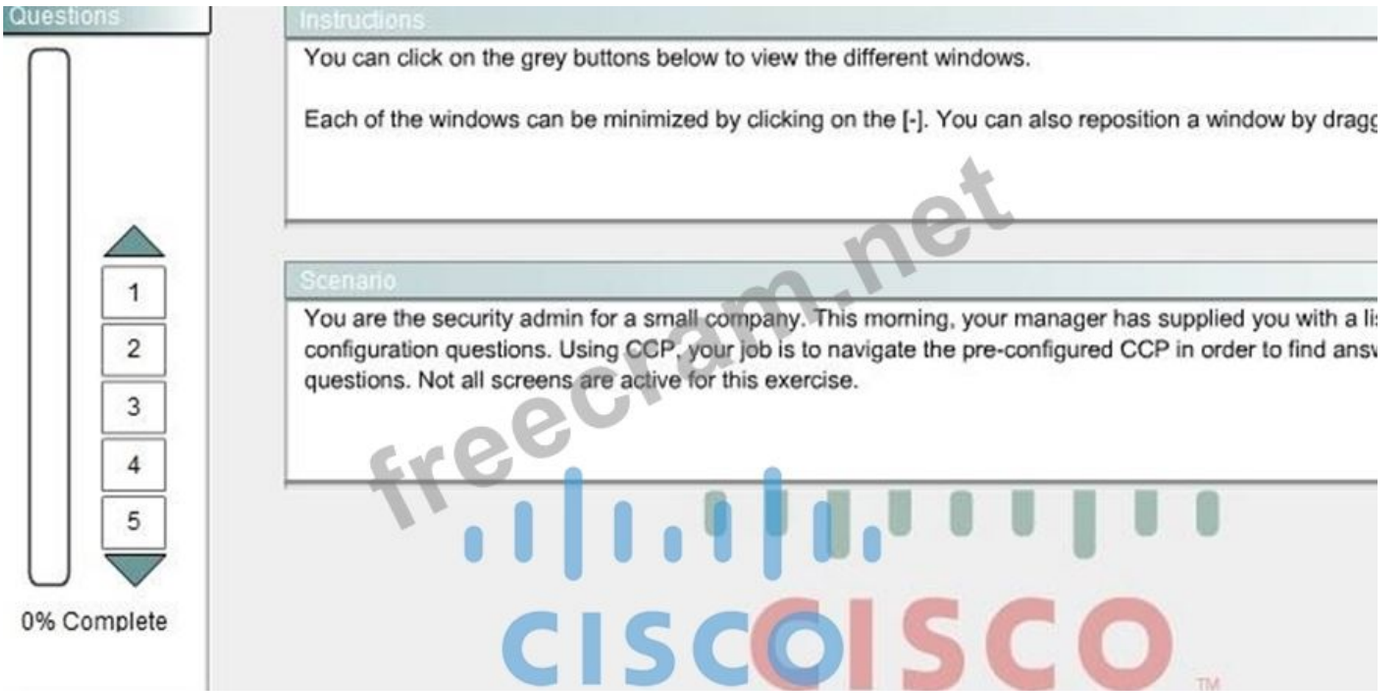
NEW QUESTION: 89
Which statement correctly describes the function of a private VLAN?
A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains.

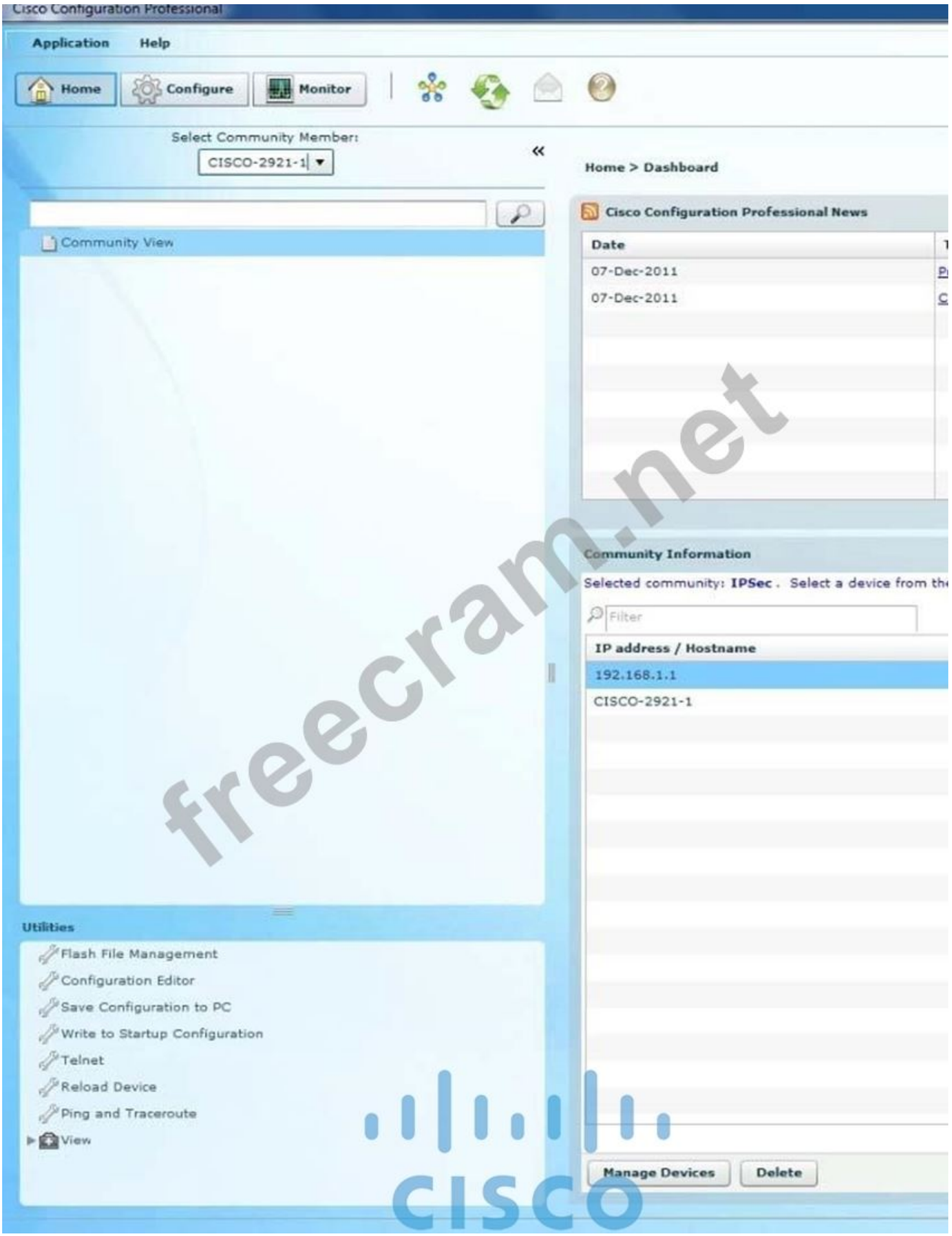
B. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomains.
C. A private VLAN enables the creation of multiple VLANs using one broadcast domain.
D. A private VLAN combines the Layer 2 broadcast domain of many VLANs into one major broadcast domain.
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 90
Which option is a characteristic of a stateful firewall?
A. allows modification of security rule sets in real time to allow return traffic
B. can analyze traffic at the application layer
C. supports user authentication
D. will allow outbound communication, but return traffic must be explicitly permitted
Answer: (SHOW ANSWER)

NEW QUESTION: 91
When Cisco IOS zone-based policy firewall is configured, which three actions can be applied to a traffic class? (Choose three.)
A. pass
B. queue
C. inspect
D. shape
E. drop
F. police
Answer: (SHOW ANSWER)

NEW QUESTION: 92


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 dragg
Scenario
You are the security admin for a small company. This morning, your manager has supplied you with a li
configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answ
questions. Not all screens are active for this exercise.
freecram.net
CISCO
CISCO

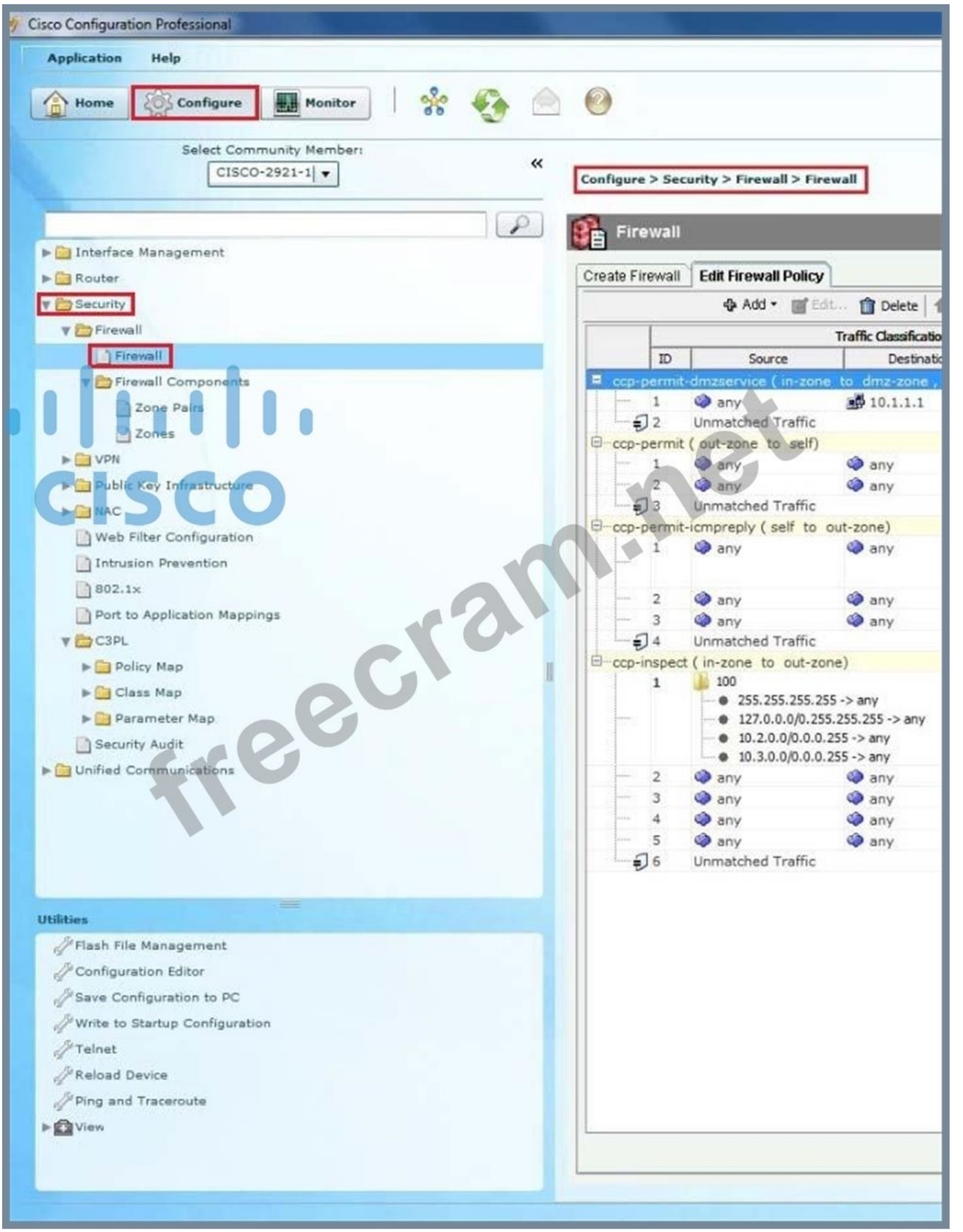


Which four properties are included in the inspection Cisco Map OUT_SERVICE? (Choose four)

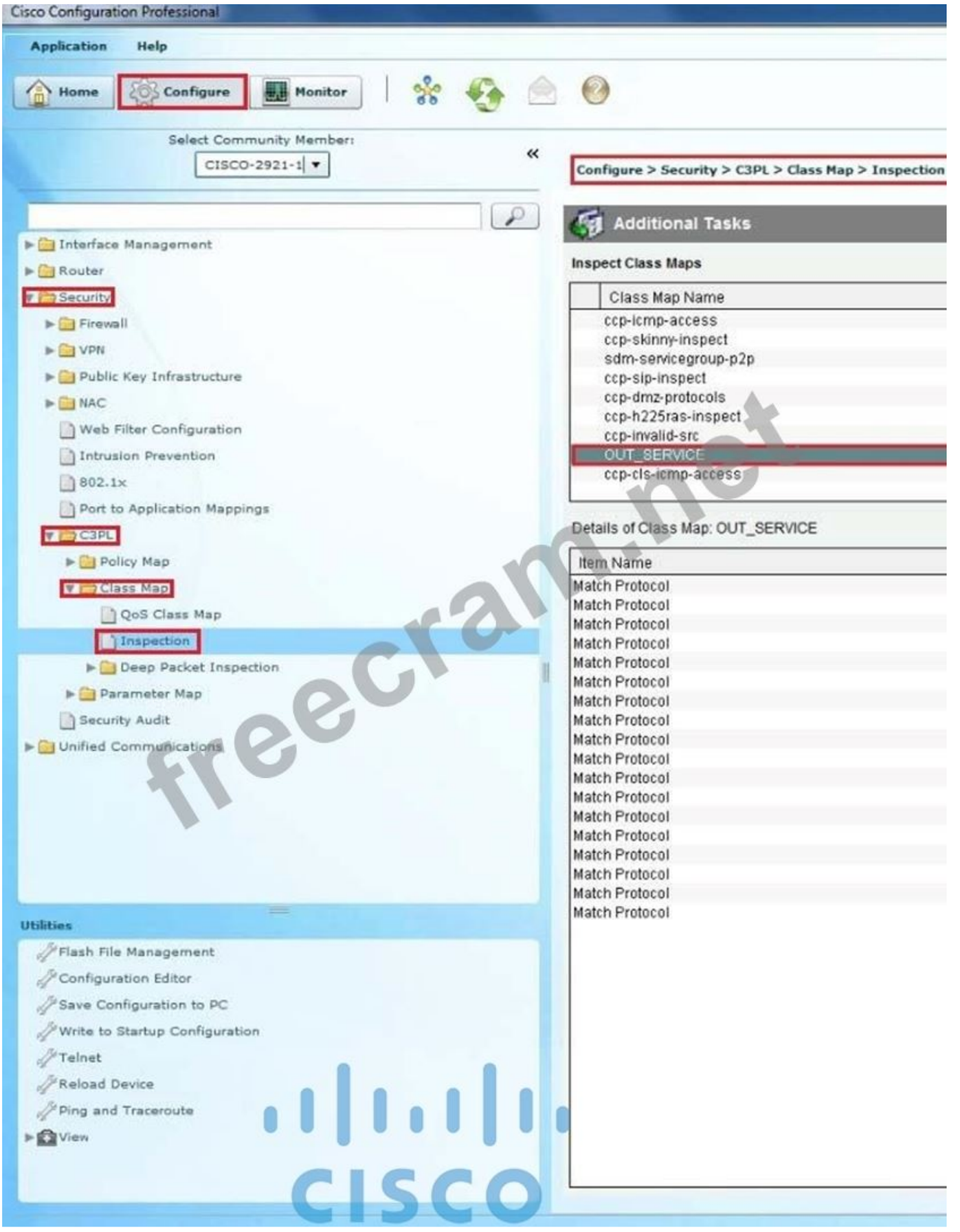
A. FTP

B. HTTP

C. HTTPS
D. SMTP
E. P2P
F. ICMP
Answer: (SHOW ANSWER)
Explanation/Reference:
First option:



Second option:



NEW QUESTION: 93

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 FastEthernet0/0
ip address 192.168.32.13 255.255.255.0
ip access-group IOS in
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: 192.168.15.36 destination port 80
D. destination ip address: 192.168.15.66 destination port: 8080
E. destination ip address: 192.168.15.63 destination port: 80
F. destination ip address: 192.168.15.40 destination port: 21
Answer: (SHOW ANSWER)

NEW QUESTION: 94
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: (SHOW ANSWER)
Explanation

NEW QUESTION: 95
Which two countermeasures can mitigate STP root bridge attacks?(Choose two).

A. BPDU filtering
B. Layer 2 PDU rate limiter
C. Root guard
D. BPDU guard
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 96
Which two protocols enable Cisco Configuration Professional to pull IPS alerts from a Cisco ISP router?
(Choose two.)
A. TFTP
B. FTP
C. SDEE
D. SSH
E. syslog
F. HTTPS
Answer: (SHOW ANSWER)

NEW QUESTION: 97
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 enable SNMP version3.
B. One-Step Lockdown can enable DHCP snooping.
C. One-Step Lockdown can disable unused ports.
D. One-Step Lockdown can enable IP Cisco Express Forwarding.
E. One-Step Lockdown can disable the TCP small servers service.
F. One-Step Lockdown can set the enable secret password.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
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 then network-based IPS.
F. Host-based IPS deployment requires less planning than network-based IPS.
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 99
Which three modes of access can be delivered by SSL VPN? (Choose three.)
A. TLS tunnel mode
B. TLS transport mode
C. full tunnel client
D. clientless
E. thin client
F. IPsec SSL
Answer: (SHOW ANSWER)

NEW QUESTION: 100
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 a TFTP server.
E. The running Cisco IOS image is encrypted and then automatically backed up to the NVRAM.
Answer: (SHOW ANSWER)

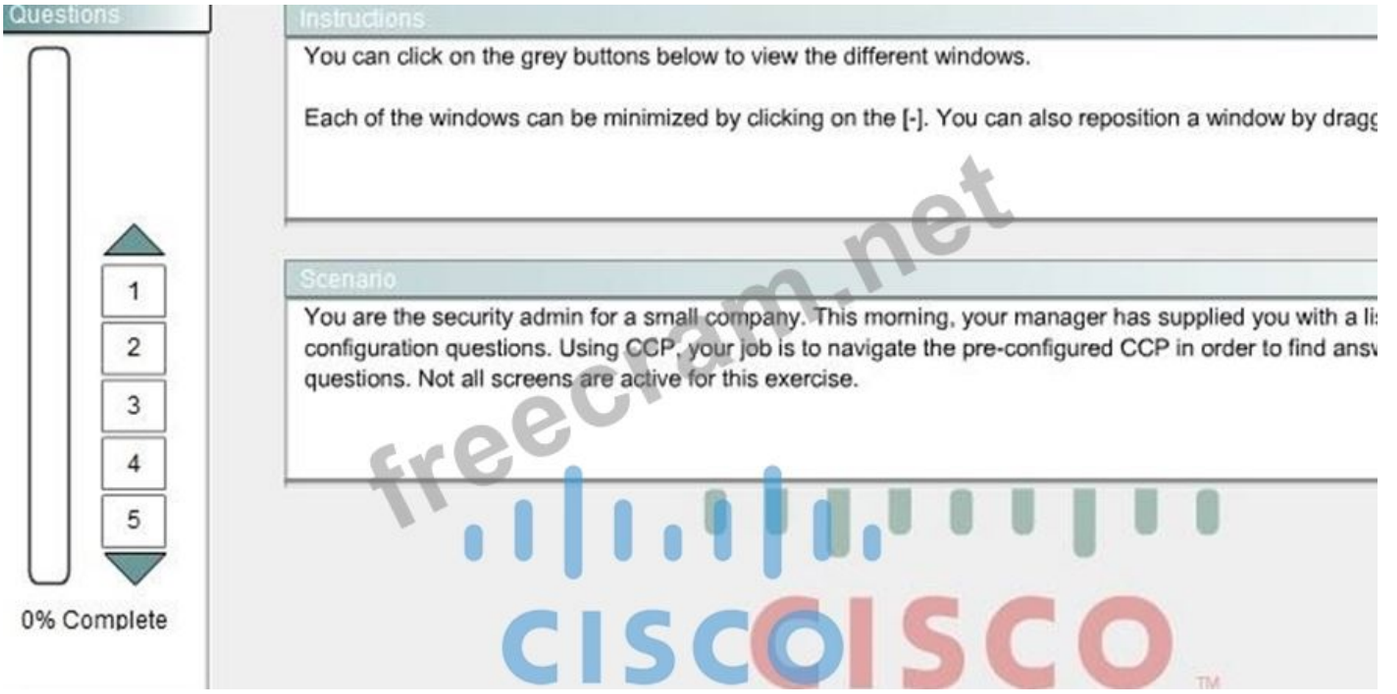
NEW QUESTION: 101
Which two options represent a threat to the physical installation of an enterprise network? (Choose two.)
A. surveillance camera
B. change control
C. electrical power
D. computer room access
E. security guards
Answer: (SHOW ANSWER)

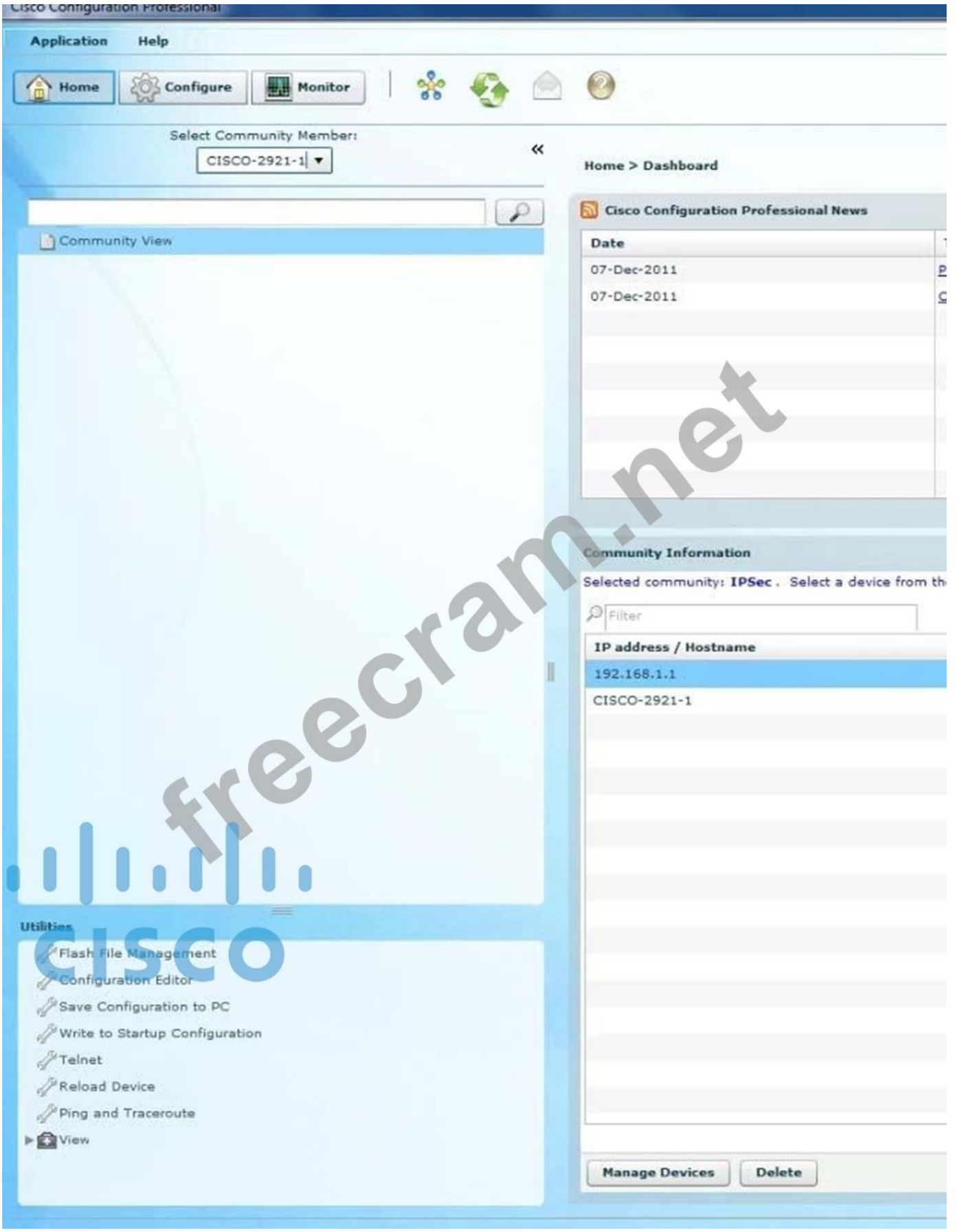
NEW QUESTION: 102
Which type of attack can be prevented by setting the native VLAN to an unused VLAN?
A. MAC-address spoofing
B. Denial-of-service attacks
C. CAM-table overflow
D. VLAN-hopping attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 103
In which type of Layer 2 attack does an attacker broadcast BDPUs with a lower switch priority?

A. CAM overflow attack
B. MAC spooling attack
C. VLAN hopping attack
D. STP attack
Answer: (SHOW ANSWER)

NEW QUESTION: 104





What NAT address will be assigned by ACL 1?

A. 192.168.1.0/25

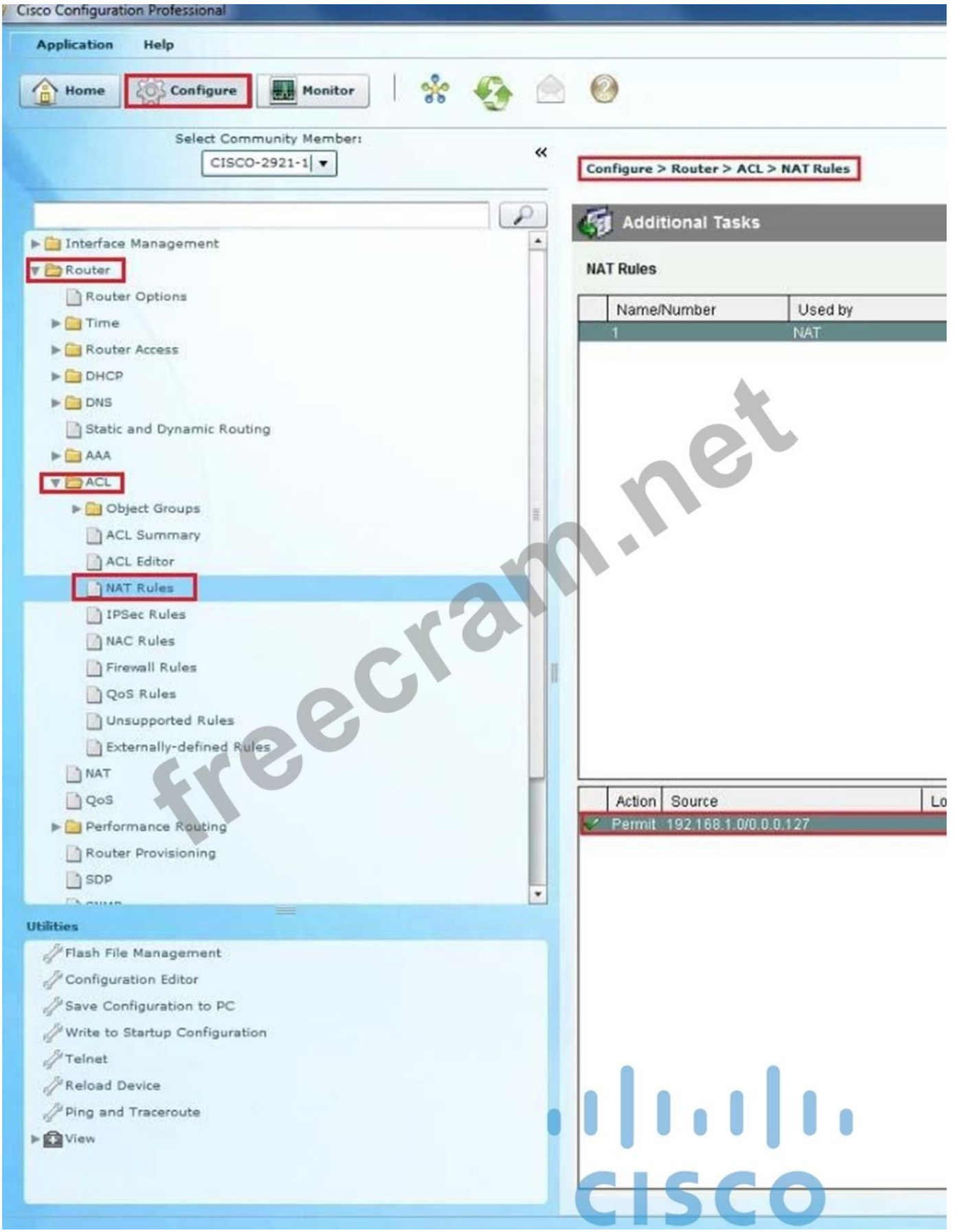
B. GlobalEthernet0/0 interface address.

C. 172.25.223.0/24

D. 10.0.10.0/24

Answer: (SHOW ANSWER)

Explanation/Reference:



NEW QUESTION: 105

Which option is a feature of Cisco ScanSafe technology?

A. consistent cloud-based policy
B. RSA Email DLP
C. DDoS protection
D. spam protection
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Which description of the Diffie-Heliman protocol is true?
A. It uses asymmetrical encryption to provide authentication over an unsecured communications channel.
B. It is used within the IKE Phase 1 exchange to provide peer authentication.
C. It uses symmetrical encryption to provide data confidentiality over an unsecured communications channel.
D. It is a data integrity algorithm that is used within the IKE exchanges to guarantee the integrity of the message of the IKE exchanges.
E. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Which two types of access lists can be used for sequencing? (Choose Two).
A. dynamic
B. standard
C. extended
D. relfexive
Answer: (SHOW ANSWER)

NEW QUESTION: 108
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 generate a persistent self-signed identity certificate for the ISR so administrators can authenticate the ISP when accessing it using Cisco Configuration Professional

C. used to enable asymmetric encryption on IPsec and SSL VPNs
D. used during the DH exchanges on IPsec VPNs
E. used to veritythe digital signature of the IPS signature file
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Which router management feature provides for the ability to configure multiple administrative views?
A. virtual routing and forwarding
B. role-based CLI
C. parser view view name
D. secure config privilege {level}
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
On which protocol number does Encapsulating Security Payload operate?
A. 47
B. 06
C. 50
D. 51
Answer: (SHOW ANSWER)

NEW QUESTION: 111
What does level 5 in this enable secret global configuration mode command indicate?
router(config)#enable secret level 5 password
A. The enable secret password is hashed using MD5.
B. The enable secret password is hashed using SHA.
C. Set the enable secret command to privilege level 5.
D. The enable secret password is for accessing exec privilege level 5.
E. The enable secret password is encrypted using Cisco proprietary level 5 encryption.
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Which command verifies phase 2 of an IPSEC VPN on a Cisco router?
A. Show crypto engine connection active
B. Show crypto isakmp sa
C. Show crypto map
D. Show crypto ipsec sa
Answer: (SHOW ANSWER)

NEW QUESTION: 113

Which two options are symmetric-key algorithms that are recommended by Cisco? (Choose two).
A. Twofish
B. Triple Data Encryption Standard
C. Advanced Encryption Standard
D. Blowfish
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 114
Which option is a key difference between Cisco IOS interface ACL configurations and Cisco ASA appliance interface ACL configurations?
A. The Cisco ASA appliance interface ACL also applies to traffic directed to the IP addresses of the Cisco ASA appliance interfaces.
B. The Cisco ASA appliance does not support standard ACL. The Cisco ASA appliance only support extended ACL.
C. Cisco IOS supports interface ACL and also global ACL. Global ACL is applied to all interfaces.
D. The Cisco IOS interface ACL has an implicit permit-all rule at the end of each interface ACL.
E. The Cisco ASA appliance interface ACL configurations use netmasks instead of wildcard masks.
Answer: (SHOW ANSWER)

NEW QUESTION: 115
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. Specile the signature file and the Cisco public key.
C. Specify the configuration location and select the category of signatures to be applied to the selected interface(s).
D. Add or remove IPS alerts actions based on the risk rating.
E. Select the traffic flow direction that should be applied by the IPS rule.
F. Select the IPS bypass mode (fail-open or fail-close).
Answer: (SHOW ANSWER)

NEW QUESTION: 116
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: (SHOW ANSWER)

Explanation

NEW QUESTION: 117
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: (SHOW ANSWER)
Explanation

NEW QUESTION: 118
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 192.168.8.4 255.255.255.224 192.168.8.32 255.255.255.192
C. permit esp 192.168.8.0.0.0.3 192.168.8.32 0.0.0.31
D. permit esp 192.168.8.4 0.0.0.31 192.168.8.32 0.0.0.31
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Which two characteristics of the TACACS+ protocol are true? (Choose two.)
A. separates AAA functions
B. encrypts the body of every packet
C. is an open RFC standard protocol
D. uses UDP ports 1645 or 1812
E. offers extensive accounting capabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which two options are two of the built-in features of IPv6? (Choose two.)
A. VLSM
B. mobile IP
C. native IPsec
D. controlled broadcasts
E. NAT
Answer: (SHOW ANSWER)

NEW QUESTION: 121
Which three statements about the Cisco ASA appliance are true? (Choose three.)

A. An SSM is required on the Cisco ASA appliance to support Botnet Traffic Eiltering.
B. The Cisco ASA appliance has no default MPE configurations.
C. The Cisco ASA appliance supports Active/Active or Active/Standby failover.
D. The Cisco ASA appliance uses security contexts to virtually partition the ASA into multiple virtual firewalls.
E. The DMZ interface(s) on the Cisco ASA appliance most typically use a security level between 1 and 99.
F. The Cisco ASA appliance supports user-based access control using 802.lx.
Answer: (SHOW ANSWER)

NEW QUESTION: 122
Which security measure must you take for native VLANs on a trunk port?
A. Native VLANs for trunk ports should be tagged with 802.IQ.
B. The native VLAN for trunk ports should be VLAN 1.
C. Native VLANs for trunk ports should never be used anywhere else on the switch.
D. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
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: (SHOW ANSWER)
Explanation

NEW QUESTION: 124
Which network security framework is used to set up access control on Cisco Appliances?

A. TACACS+
B. RADIUS
C. NAS
D. AAA
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Which statement describes a best practice when configuring trunking on a switch port?
A. Limit the allowed VLAN(s) on the trunk to the native VLAN only.
B. Enable encryption on the trunk port.
C. Enable authentication and encryption on the trunk port.
D. Disable double tagging by enabling DTP on the trunk port.
E. Configure an unused VLAN as the native VLAN.
Answer: (SHOW ANSWER)

NEW QUESTION: 126
The host A layer 2 port is configured in VLAN5 on switch1, and the host B port is configured in VLAN10 on switch1. Which two actions you can take to enable the two communicate with each other? (Choose two).
A. Configure inter-VLAN routing.
B. Connect the hosts directly through a router.
C. Configure switched virtual interfaces.
D. Connect the hosts directly through a hub.
Answer: (SHOW ANSWER)

NEW QUESTION: 127
Which three items are Cisco best-practice recommendations for securing a network? (Choose three).
A. Require strong passwords, and enable password expiration.
B. Routinely apply patches to operating systems and applications.
C. Deploy HIPS software on all end-user workstations.
D. Disable uneeded services and ports on hosts.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 128
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: (SHOW ANSWER)
Explanation

NEW QUESTION: 129
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: (SHOW ANSWER)
Explanation/Reference:
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.

NEW QUESTION: 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: (SHOW ANSWER)
Explanation

NEW QUESTION: 131
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 (LEAVE A REPLY)
Explanation

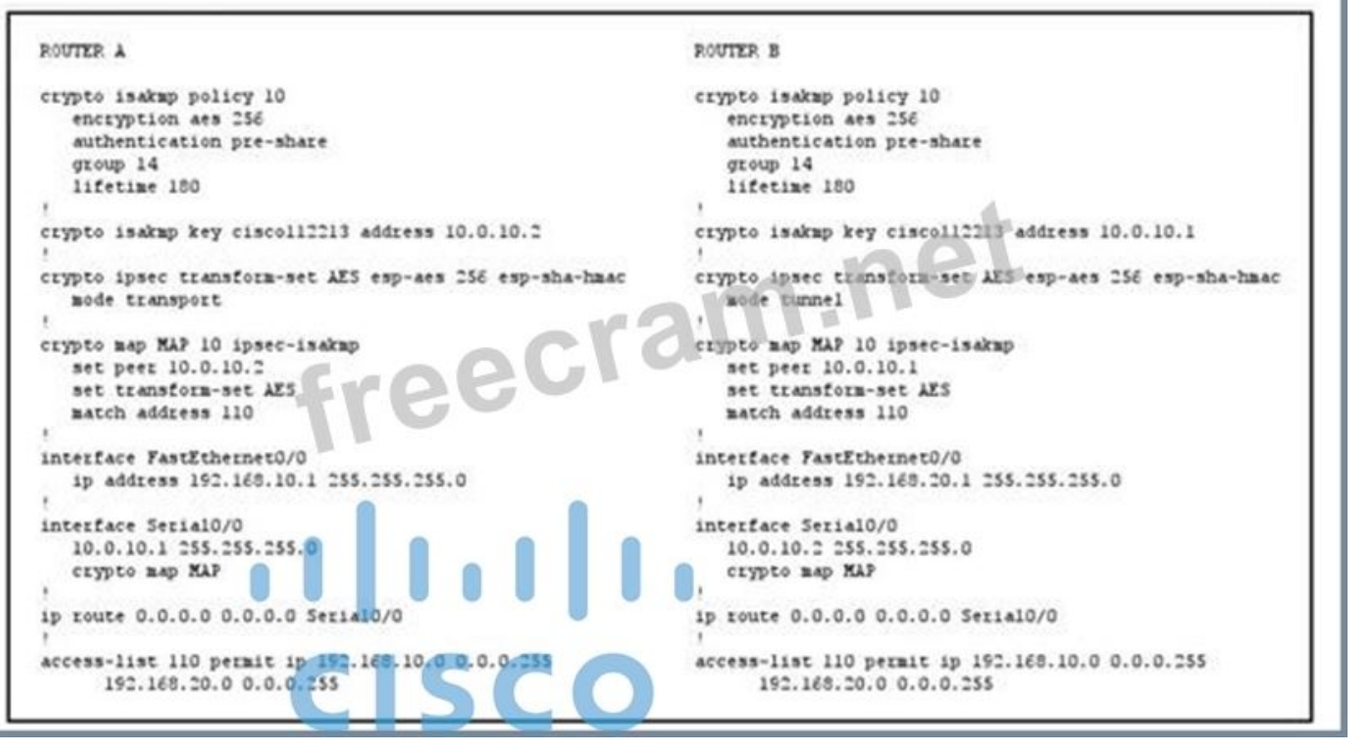
NEW QUESTION: 132
Which three statements about applying access control lists to a Cisco router are true? (Choose three.)
A. Place generic ACL entries at the top of the ACL to filter general traffic and thereby reduce "noise" on the network.
B. ACLs always search for the most specific entry before taking any filtering action.
C. If an access list is applied but it is not configured, all traffic passes.
D. Router-generated packets cannot be filtered by ACLs on the router.
E. Place more specific ACL entries at the top of the ACL.
Answer: (SHOW ANSWER)

NEW QUESTION: 133
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: (SHOW ANSWER)

NEW QUESTION: 134
Which statement describes how VPN traffic is encrypted to provide confidentiality when using asymmetric encryption?
A. The sender encrypts the data using the receiver's public key, and the receiver decrypts the data using the receiver's private 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 sender's private key, and the receiver decrypts the data using the sender's public key.
E. The sender encrypts the data using the receiver's private key, and the receiver decrypts the data using the receiver's public 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: (SHOW ANSWER)

NEW QUESTION: 135

Refer to the exhibit.



```
ROUTER A

crypto isakmp policy 10
   encryption aes 256
   authentication pre-share
   group 14
   lifetime 180
!
crypto isakmp key ciscol12213 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
```

```
ROUTER B

crypto isakmp policy 10
   encryption aes 256
   authentication pre-share
   group 14
   lifetime 180
!
crypto isakmp key ciscol12213 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
```


Which two changes must you make to given IOS site-to-site VPN configuration to enable the routers to form a connection? (Choose two).

A. Configure the access list on Router B to mirror Router A.

B. Configure the tunnel modes on the two routers to match.

C. Configure a valid route on Router A.

D. Configure Route B's ISAKMP policy to match the policy on Router A.

Answer: (SHOW ANSWER)

NEW QUESTION: 136

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

A. 2001::150c::41b1:45a3:041d

B. 2001:0:150c::41b1:45a3:41d

C. 2001:0:150c:0::41b1:45a3:04d1

D. 2001:150c::41b1:45a3::41d

Answer: B (LEAVE A REPLY)

NEW QUESTION: 137
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: (SHOW ANSWER)
Explanation

NEW QUESTION: 138
Which two options are advantages of an application layer firewall? (Choose two.)
A. provides high-performance filtering
B. authenticates individuals
C. supports a large number of applications
D. authenticates devices
E. makes DoS attacks difficult
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 139
Which type of NAT would you configure if a host on the external network required access to an internal host?
A. dynamic outside NAT
B. NAT overload
C. static NAT
D. outside global NAT
Answer: (SHOW ANSWER)

NEW QUESTION: 140
Which three applications comprise Cisco Security Manager? (Choose three)
A. Event Viewer
B. Syslog Monitor
C. Packet Tracer
D. Device Manager
E. Configuration Manager
F. Report Manager

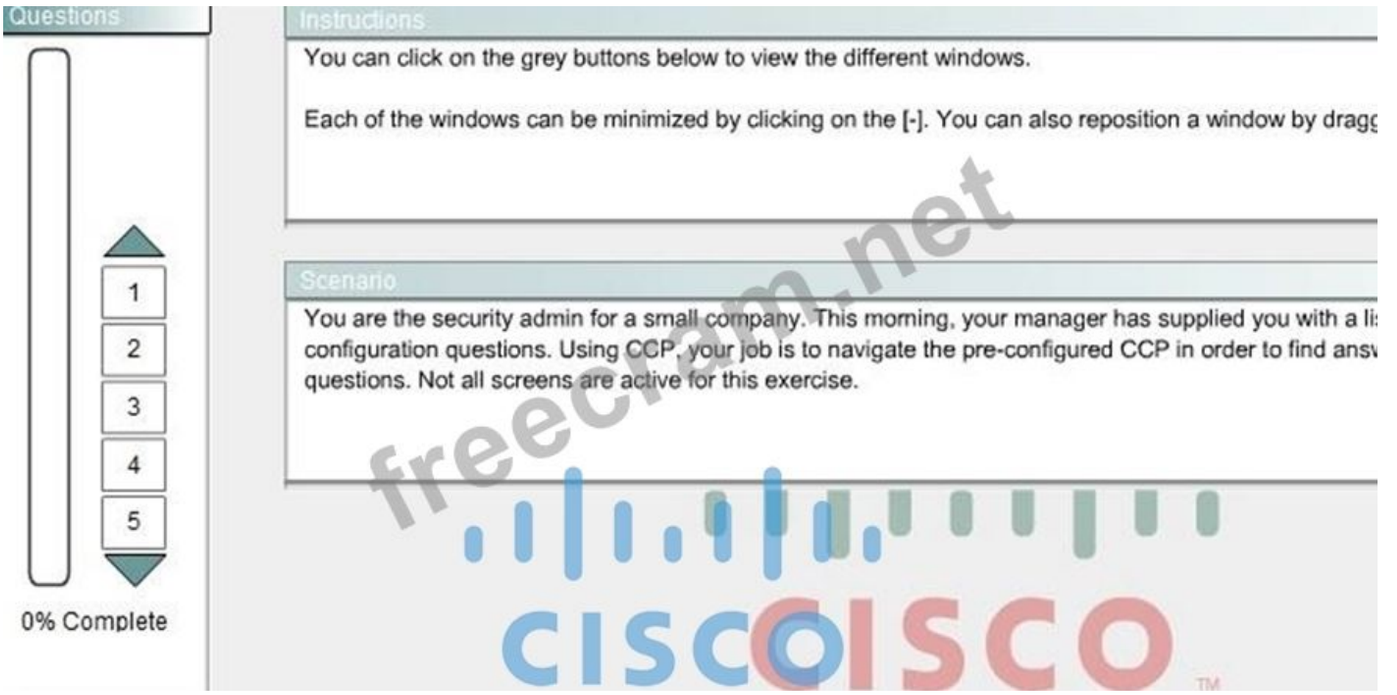
Answer: (SHOW ANSWER)

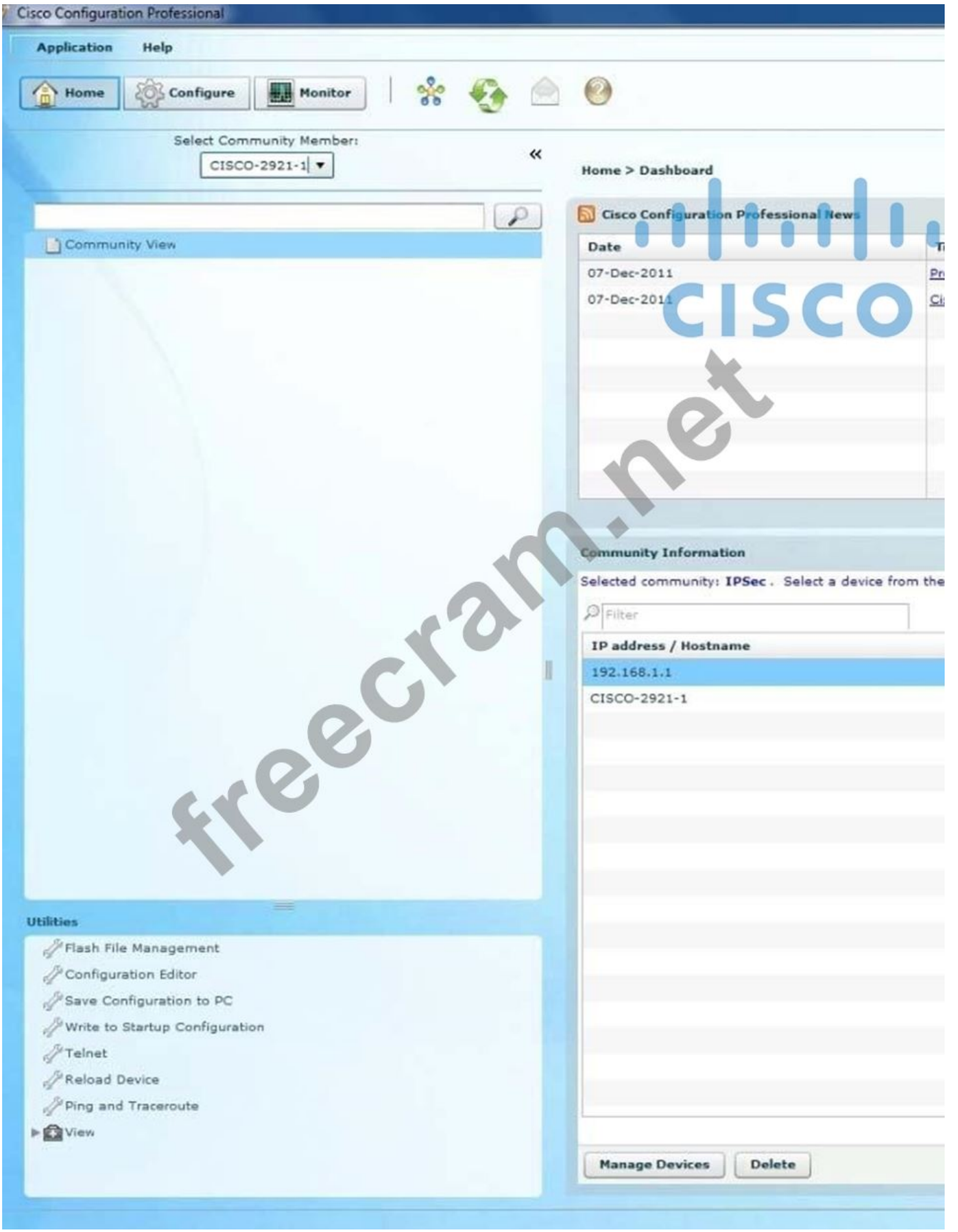
NEW QUESTION: 141
Which priorit is most important when you plan out access control lists?
A. Build ACLs based upon your security policy.
B. Always test ACLs in a small, controlled production environment before you roll it out into the larger production network.
C. Place deny statements near the top of the ACL to prevent unwanted traffic from passing through the router.
D. Always put the ACL closest to the source of origination.
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Refer to CISCO IOS Zone-Based Policy Firewall, where will the inspection policy be applied?
A. to the zone
B. to the interface
C. to the global service policy
D. to the zone-pair
Answer: (SHOW ANSWER)

NEW QUESTION: 143
For what purpose is the Cisco ASA appliance web launch SSL VPN feature used?
A. to enable users to login to a web portal to download and launch the AnyConnect client
B. to enable single-sign-on so the SSL VPN users need only log in once
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 split tunneling when using clientless SSL VPN access
Answer: (SHOW ANSWER)

NEW QUESTION: 144


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 dragg
Scenario
You are the security admin for a small company. This morning, your manager has supplied you with a li
configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answ
questions. Not all screens are active for this exercise.
freecram.net
CISCO
CISCO



Which Class Map is used by the INBOUND Rule?

A. SERVICE_IN

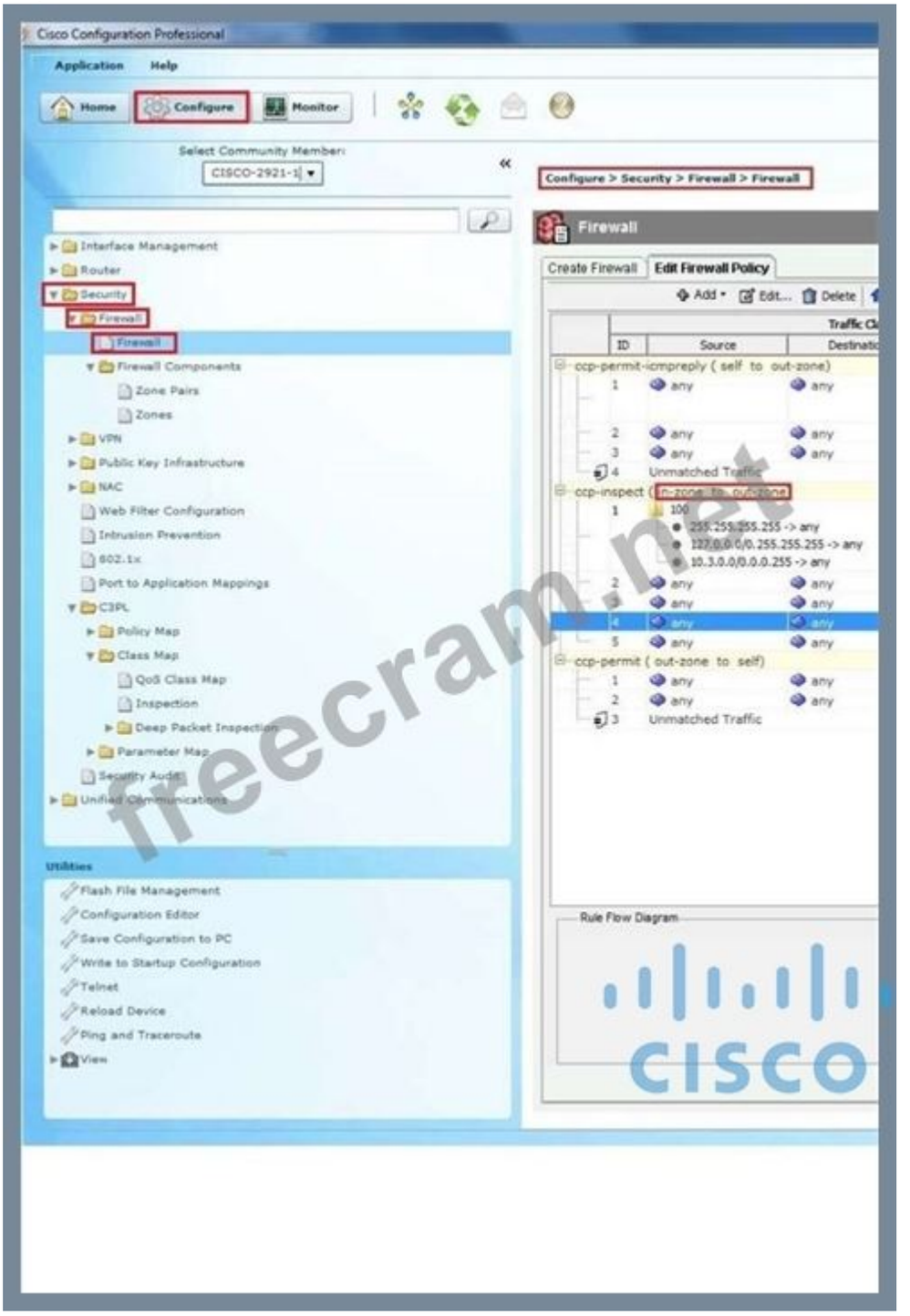
B. Class-map-ccp-cls-2

C. Ccp-cts-2

D. Class-map SERVICE_IN

Answer: (SHOW ANSWER)

Explanation/Reference:



NEW QUESTION: 145

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 the phone.

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 a web page.
Answer: (SHOW ANSWER)

NEW QUESTION: 146
Which type of NAT is used where you translate multiple internal IP addresses to a single global, routable IP address?
A. policy NAT
B. policy PAT
C. dynamic PAT
D. dynamic NAT
E. static NAT
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Refer to the exhibit:

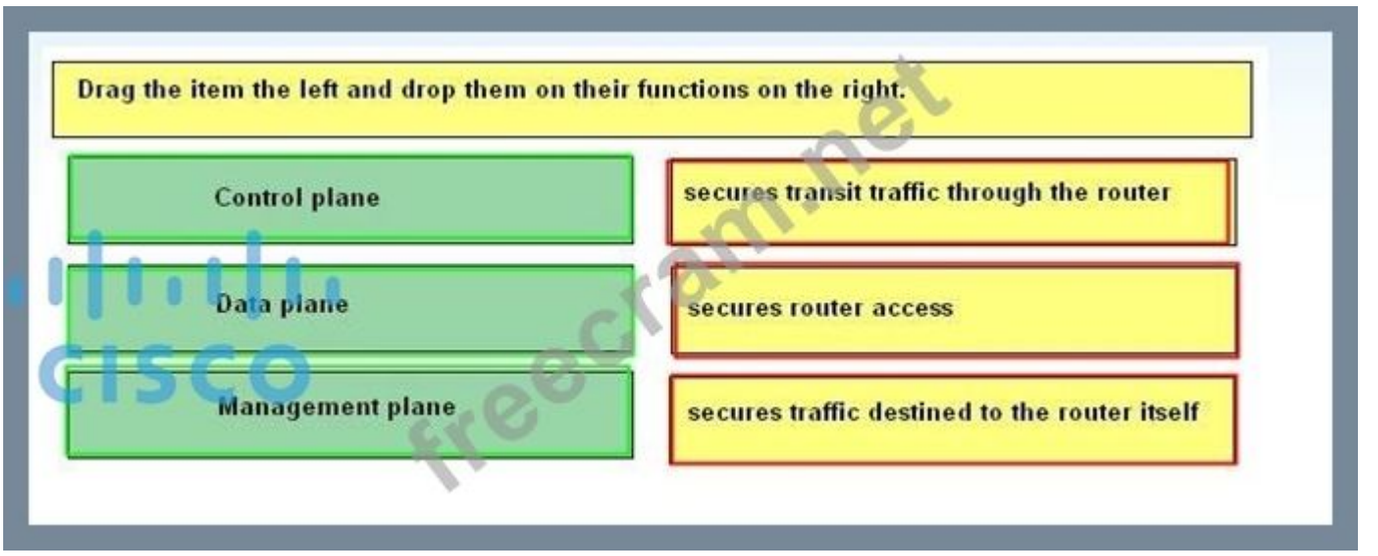
```
router#sh run | include username

username test secret 5 $1$knm.$GOGQBIL8TK77P0LWxvX4O0
```

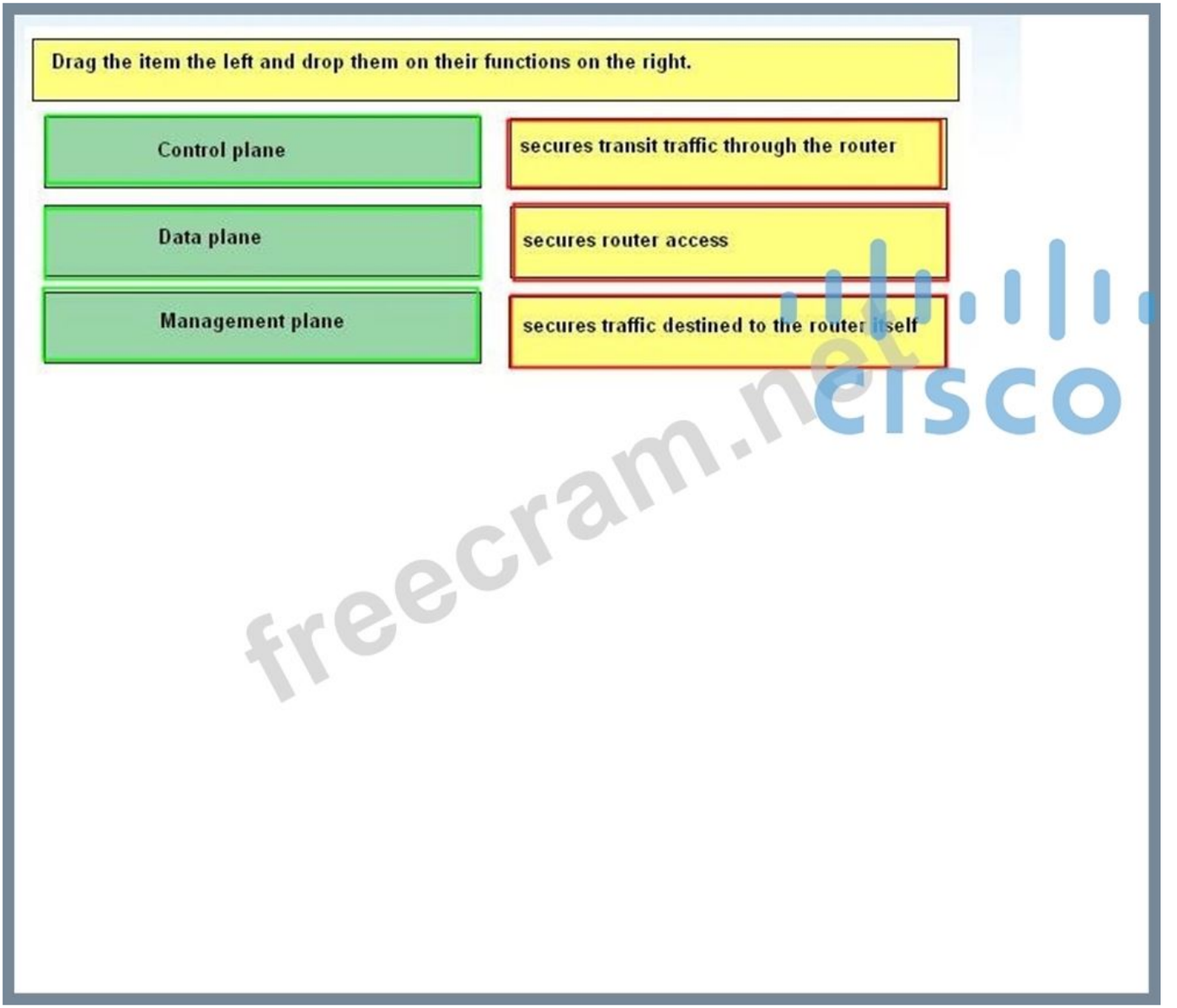
What does the option secret 5 in the username global configuration mode command indicate about the user password?
A. It is encrypted using DH group 5.
B. It is encrypted using the service password-encryption command.
C. It is hashed using a proprietary Cisco hashing algorithm.
D. It is hashed using SHA.
E. It is encrypted using a proprietary Cisco encryption algorithm.
F. It is hashed using MD5.
Answer: (SHOW ANSWER)

NEW QUESTION: 148
Which one of the following items may be added to a password stored in MD5 to make it more secure?
A. Rainbow table
B. Cryptotext
C. Ciphertext
D. Salt
Answer: (SHOW ANSWER)

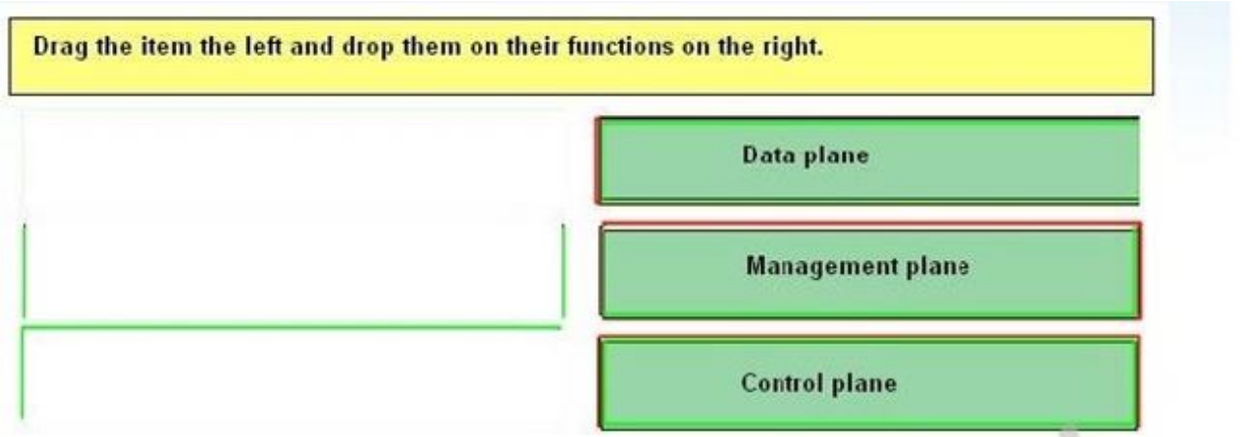
NEW QUESTION: 149



Select and Place:



Answer:



NEW QUESTION: 150

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

A. secret password for the root user

B. aaa new-model command

C. usernames and passwords

D. multiple privilege levels

E. HTTP and/or HTTPS server

F. TACACS+ server group

Answer: (SHOW ANSWER)

NEW QUESTION: 151

In which two modes can Cisco Configuration Professional Security Audit operate? (Choose two)

A. One-Step Lockdown

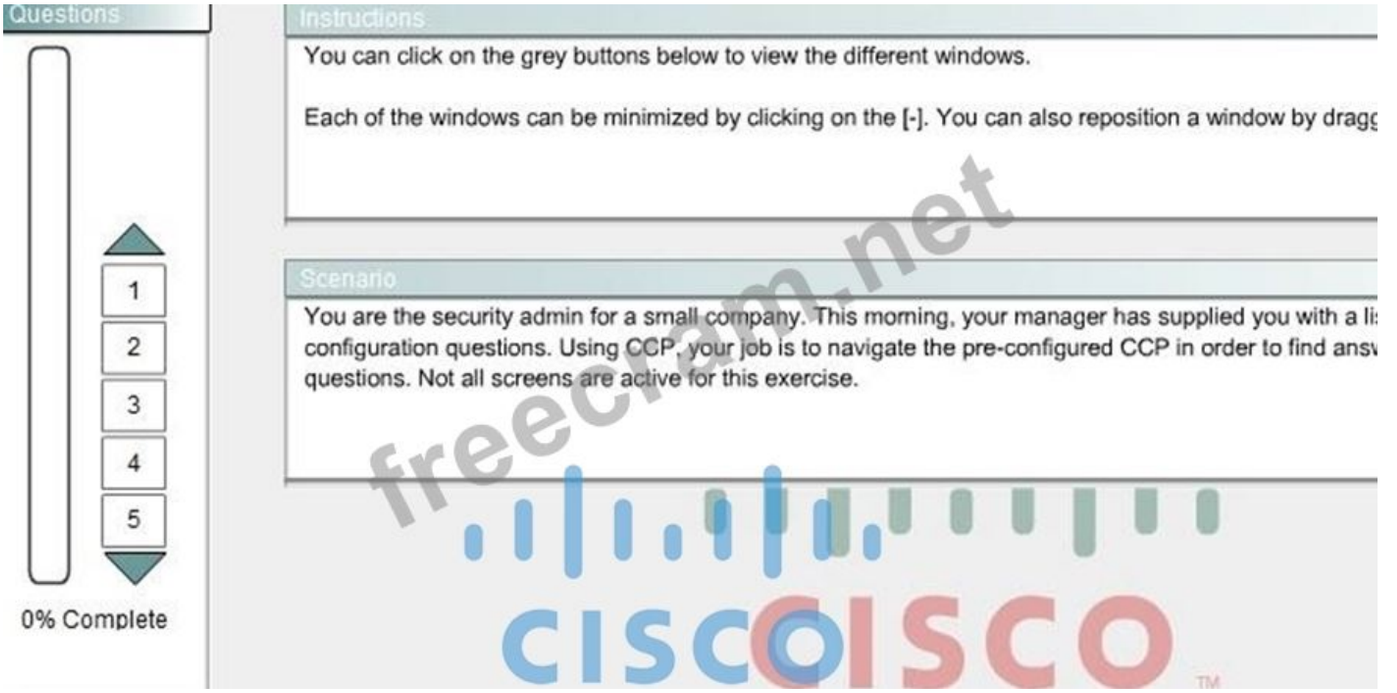
B. Security Audit wizard

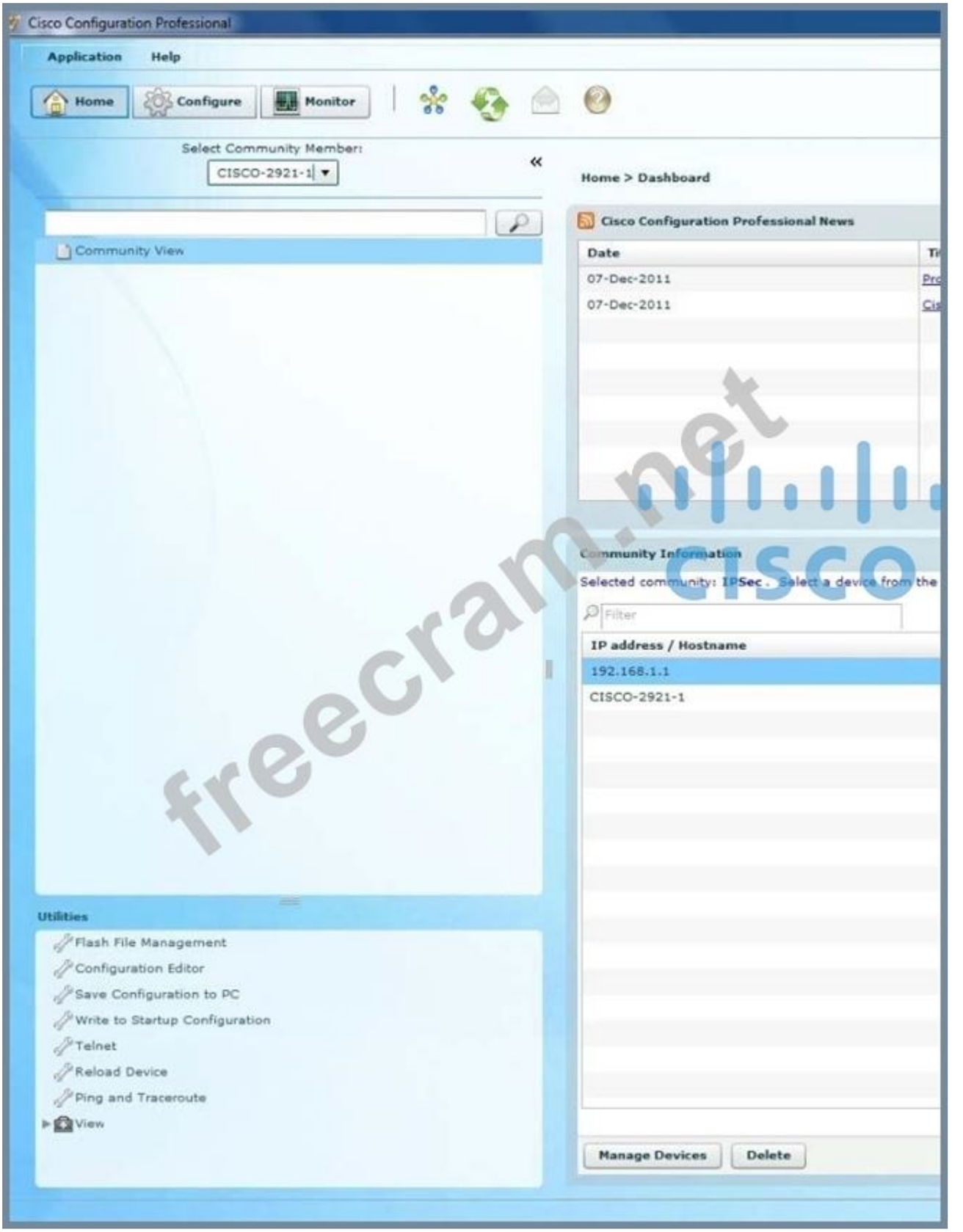
C. AutoSecure

D. Lockdown

Answer: (SHOW ANSWER)

NEW QUESTION: 152





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

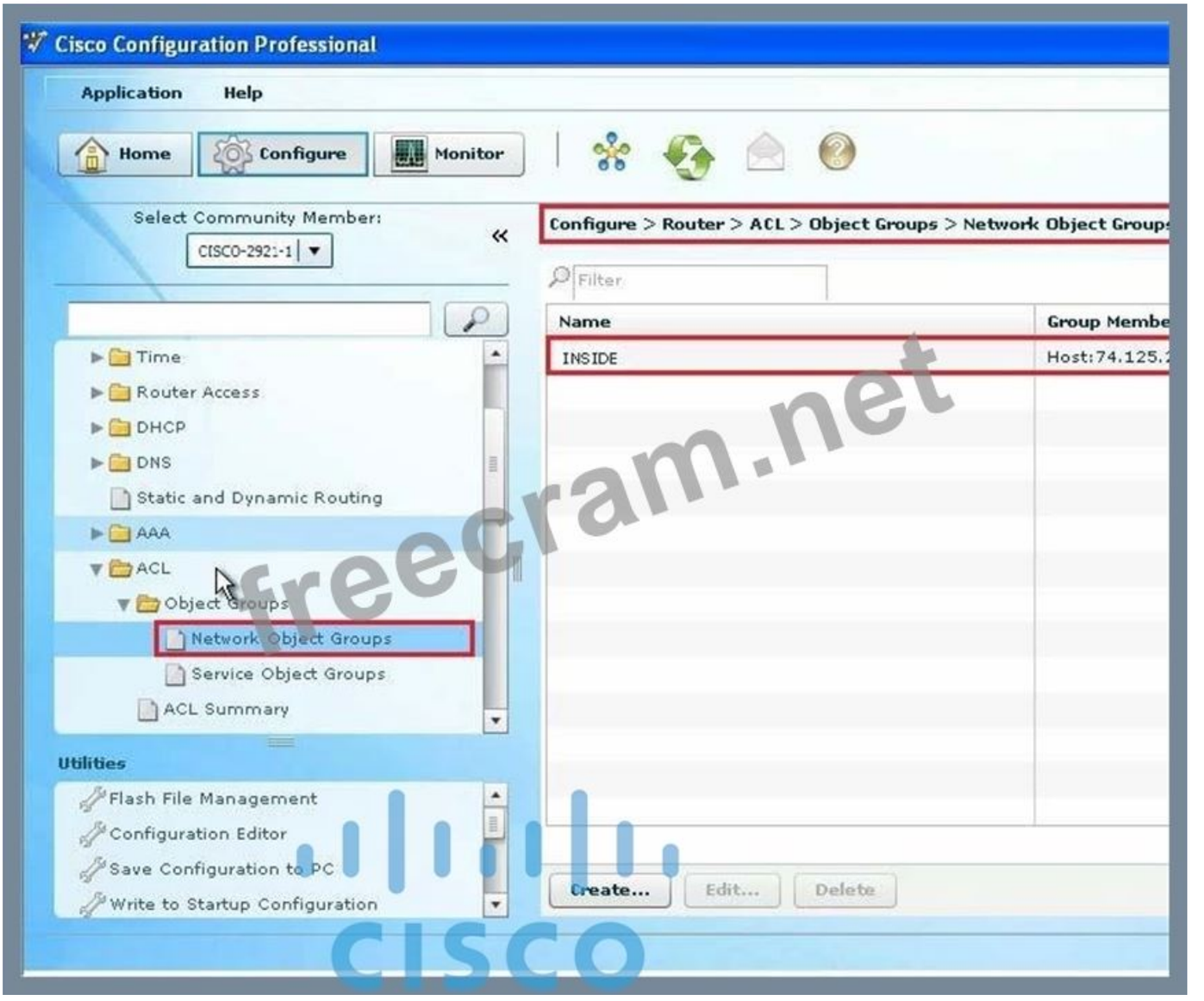
C. Host 74.125.224.176

D. Network 10.0.10.0/24

E. Host 74.125.224.179

Answer: (SHOW ANSWER)

Explanation/Reference:



NEW QUESTION: 153

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 11 deny host 172.16.0.1

D. access-list 101 deny ip any any

Answer: (SHOW ANSWER)

NEW QUESTION: 154

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

A. trojan horse attack

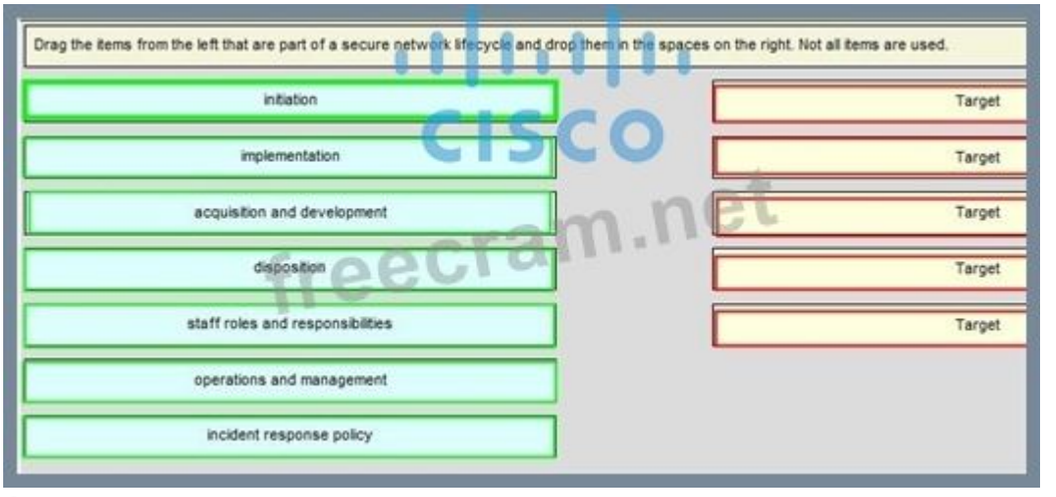
B. pharming attack

C. day zero attack
D. man-in-the-middle attack
E. denial of service attack
Answer: (SHOW ANSWER)

NEW QUESTION: 155
Which option can be used to authenticate the IPsec peers during IKE Phase 1?
A. ACS
B. Diffie-Hellman Nonce
C. pre-shared key
D. integrily check value
E. XAUTH
F. AH
Answer: (SHOW ANSWER)

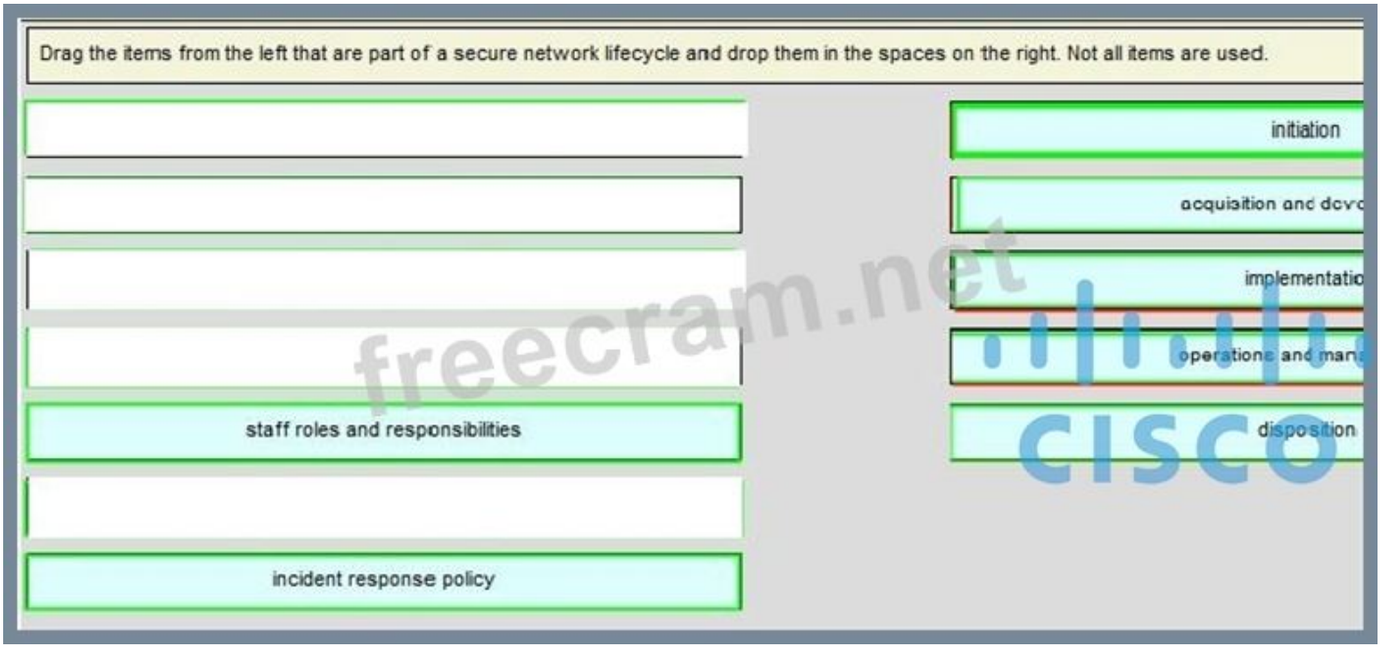
NEW QUESTION: 156
Which Cisco IOS command will verify authentication between a router and a AAA server?
A. test aaa group
B. aaa new-model
C. debug aaa authentication
D. test aaa accounting
Answer: (SHOW ANSWER)

NEW QUESTION: 157



Select and Place:

Answer:



Explanation/Reference:
LABORATORIOS

NEW QUESTION: 158
Which option represents a step that should be taken when a security policy is developed?
A. Determine device risk scores.
B. Perform quantitative risk analysis.
C. Implement a security monitoring system.
D. Perform penetration testing.
Answer: (SHOW ANSWER)

NEW QUESTION: 159

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 commands 15 start-stop tacacs+

B. aaa accounting connection start-stop tacacs+

C. aaa accounting system start-stop tacacs+

D. aaa accounting network start-stop tacacs+

E. aaa accounting exec start-stop tacacs+

Answer: (SHOW ANSWER)

NEW QUESTION: 160

Information about a managed device. Is 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: (SHOW ANSWER)

NEW QUESTION: 161

Refer to the exhibit:

Which traffic is permitted by this ACL?

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

B. 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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 162

Which IPsec transform set provides the strongest protection?

A. crypto ipsec transform-set 1 esp-3des esp-sha-hmac

B. crypto ipsec transform-set 5 esp-des esp-sha-hmac

C. crypto ipsec transform-set 2 esp-3des esp-md5-hmac

D. crypto ipsec transform-set 4 esp-aes esp-md5-hmac

E. crypto ipsec transform-set 3 esp-aes 256 esp-sha-hmac

F. crypto ipsec transform-set 6 esp-des esp-md5-hmac

Answer: (SHOW ANSWER)

NEW QUESTION: 163

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. The IPsec transform set uses SHA for data confidentiality.

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

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

D. Traffic matched by ACL 110 is encrypted.

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 164

Under which option do you create a AAA authentication policy in Cisco Configuration Professional?

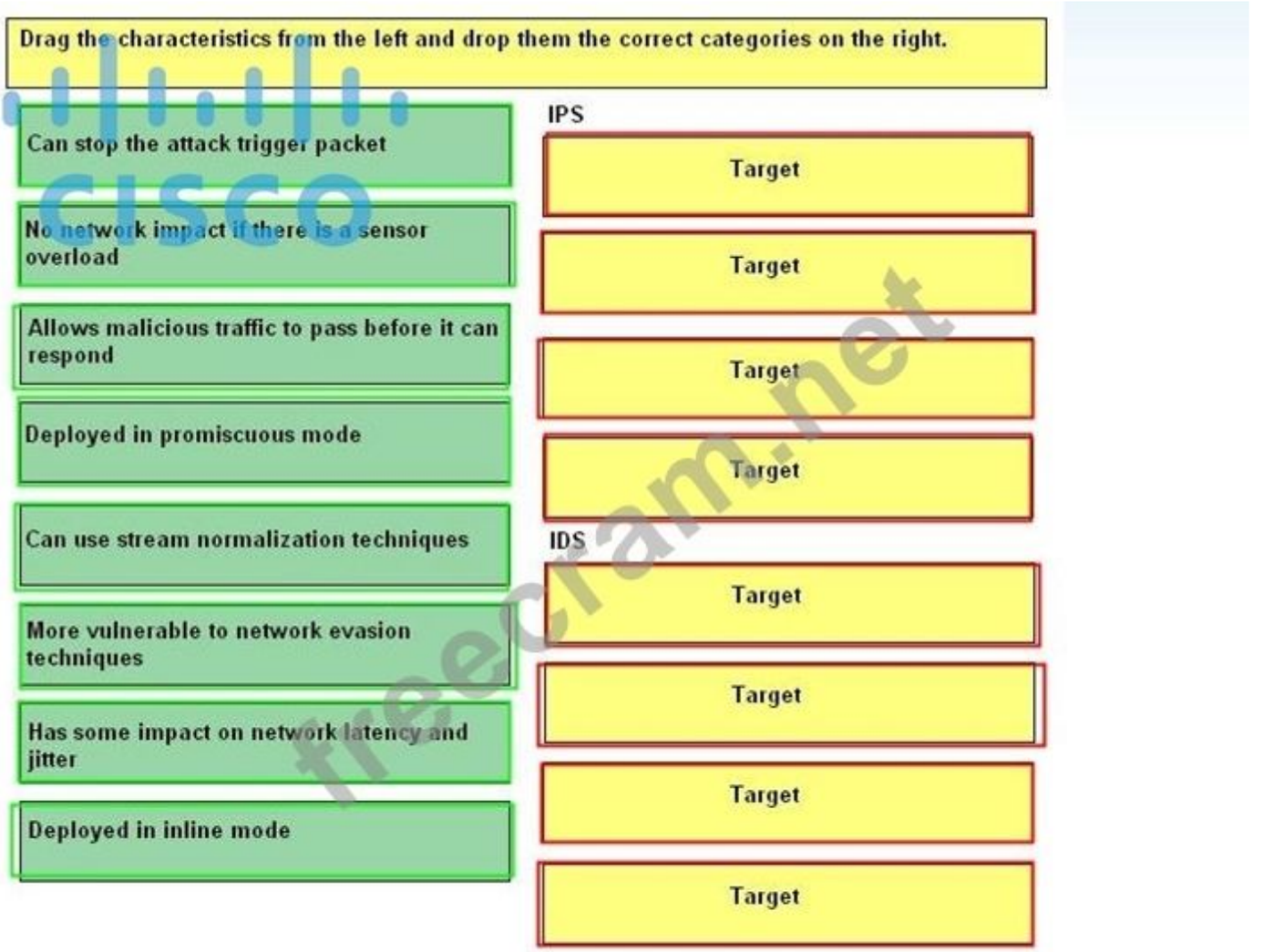
A. Authentication Policies

B. AAA Servers and Groups

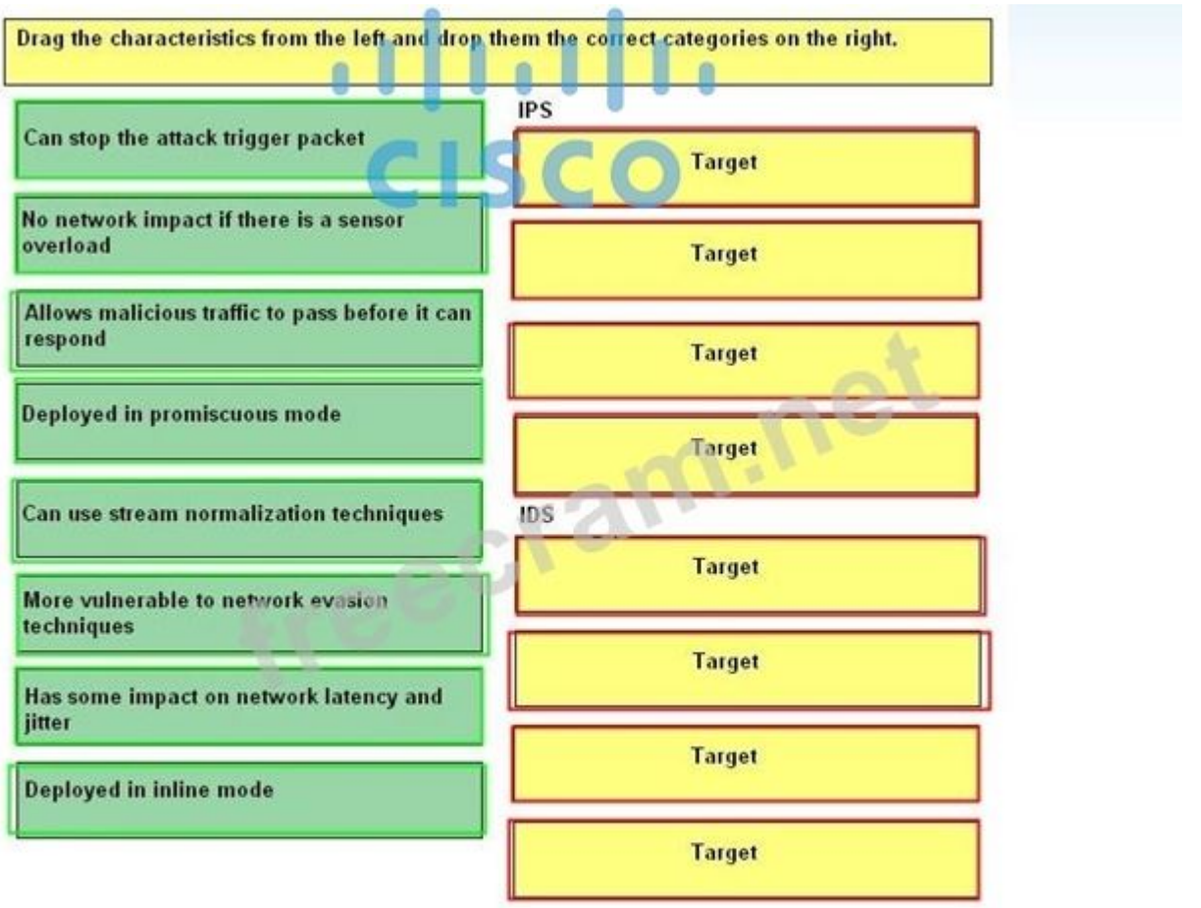
C. AAA Summary
D. Authentication Policies-Login
Answer: (SHOW ANSWER)

NEW QUESTION: 165
Which four types of VPN are supported using Cisco ISRs and Cisco ASA appliances? (Choose four.)
A. SSL full-tunnel client remote-access VPNs
B. IPsec site-to-site VPNs
C. IPsec clientless remote-access VPNs
D. SSL site-to-site VPNs
E. SSL clientless remote-access VPNs
F. IPsec client remote-access VPNs
Answer: A,B,E,F (LEAVE A REPLY)

NEW QUESTION: 166



Select and Place:



Answer:

NEW QUESTION: 167
Which three statements about RADIUS are true? (Choose three)
A. RADIUS encrypts only the password in the Access-Request packet.
B. RADIUS is a Cisco proprietary technology.
C. RADIUS uses TCP port 49.
D. RADIUS uses UDP ports 1645 or 1812.

E. RADIUS encrypts the entire packet.

F. RADIUS is an open standard.

Answer: (SHOW ANSWER)

NEW QUESTION: 168

Select and Place:

Answer:

NEW QUESTION: 169

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: (SHOW ANSWER)

Explanation/Reference:

Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP.

NEW QUESTION: 170

Which two pieces of information should you acquire before you troubleshoot an STP loop? (Choose two).

A. topology of the switched network
B. location of the root bridge
C. topology of the routed network
D. number of switches in the network
Answer: (SHOW ANSWER)

NEW QUESTION: 171

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: (SHOW ANSWER)
Explanation

NEW QUESTION: 172

Which type of management reporting is defined by separating management traffic from production traffic?
A. in-band
B. SSH
C. IPsec encrypted
D. out-of-band
Answer: (SHOW ANSWER)