Cisco 642-825

CISCO 642-825 ISCW - Implementing Secure Converged Wide Area Networks

Practice Test

Version 2.1

QUESTION NO: 1

What technology must be enabled as a prerequisite to running MPLS on a Cisco router?

A. process switching
B. CEF switching
C. fast switching
D. cache driven switching
E. routing-table driven switching

Answer: B

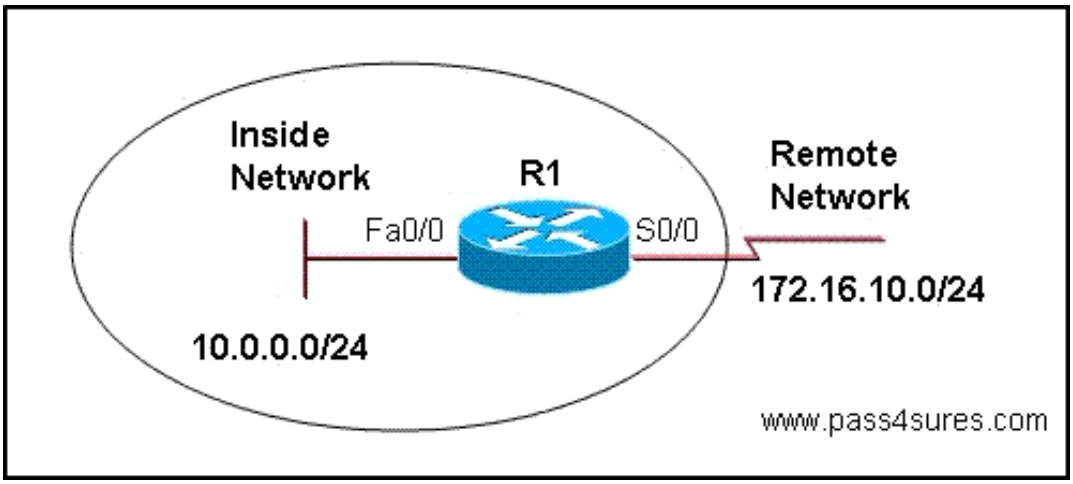
Explanation:
Configuring Cisco Express Forwarding
To enable MPLS, you must first enable Cisco Express Forwarding (CEF) switching.

Reference: "CCNP ISCW Portable Command Guide" By Scott Empson, Hans Roth.
http://www.ciscopress.com/articles/article.asp?p=1180984

QUESTION NO: 2

Refer to the exhibit.

Which ACL configuration will prevent a DoS TCP SYN attack from a spoofed source into the internal network?



A. R1(config)# access-list 120 deny icmp any any echo log
R1(config)# access-list 120 deny icmp any any redirect log
R1(config)# access-list 120 permit icmp any 10.0.0.0 0.0.0.255
R1(config)# interface Serial0/0
R1(config-if)# ip access-group 120 in
B. R1(config)# access-list 120 permit tcp any 172.16.10.0 0.0.0.255 established
R1(config)# access-list 120 deny ip any any log

R1(config)# interface FastEthernet0/0
R1(config-if)# ip access-group 120 in
C. R1(config)# access-list 120 deny ip any host 10.0.0.255 log
R1(config)# access-list 120 permit ip any 10.0.0.0 0.0.0.255 log
R1(config)# interface Serial0/0
R1(config-if)# ip access-group 120 in
D. R1(config)# access-list 120 deny udp 10.0.0.0 0.0.255.255 host 255.255.255.255 eq 512
R1(config)# interface Serial0/0
R1(config-if)# ip access-group 120 in

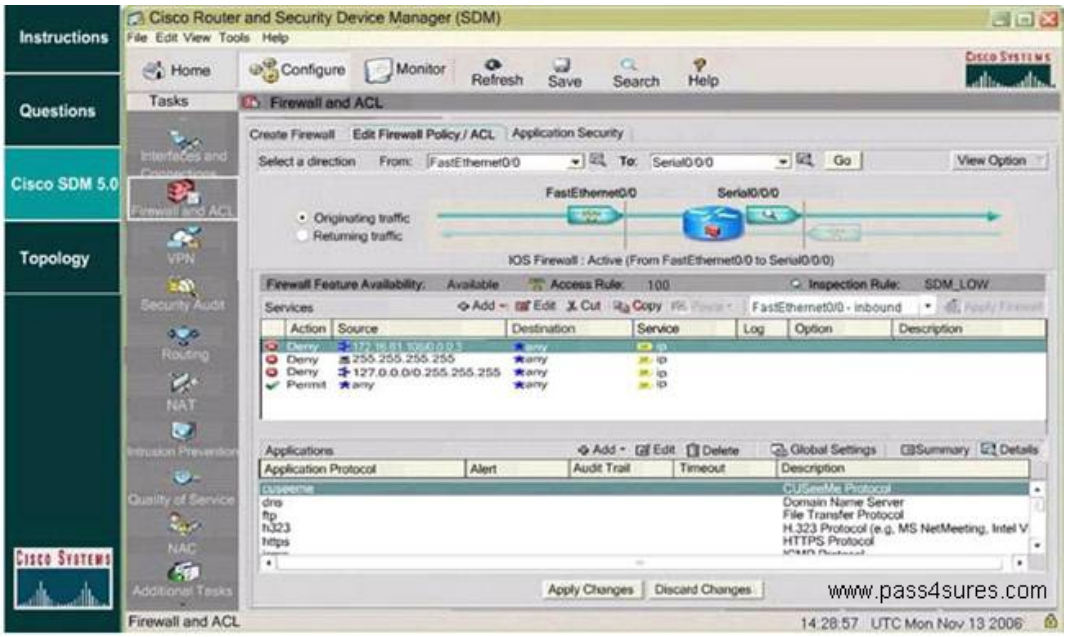
Answer: B

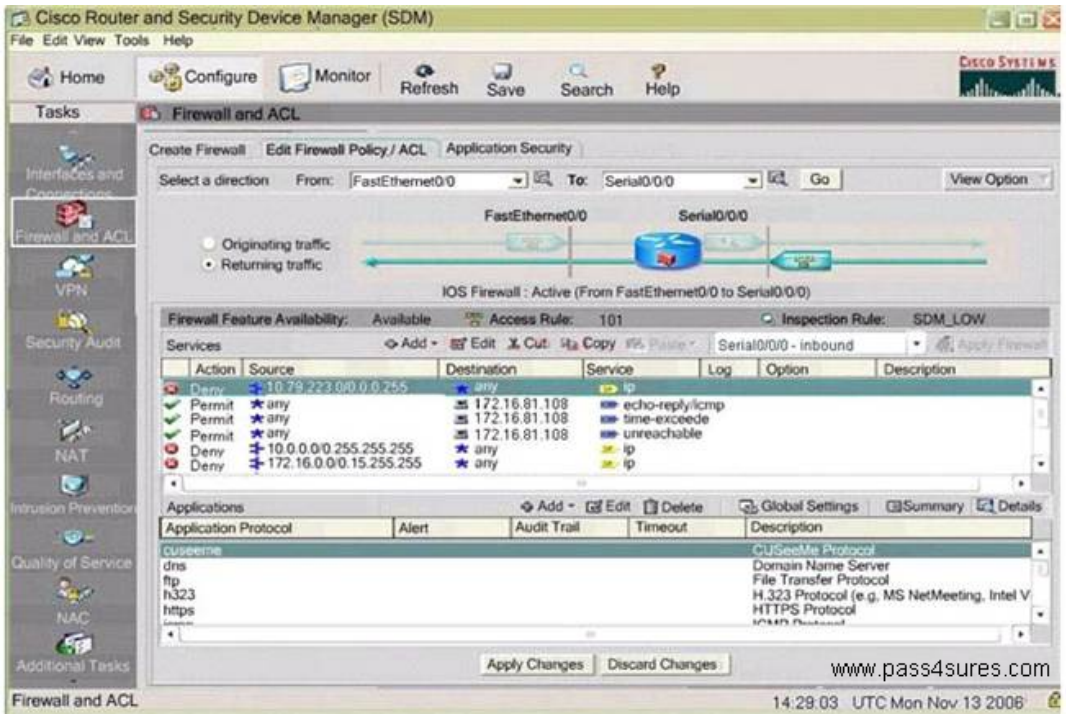
Explanation:
The TCP SYN Attack
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN ACK before the connection is established. This is referred to as the "TCP three-way handshake."
While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.
The TCP SYN attack exploits this design by having an attacking source host generate TCP SYN packets with random source addresses toward a victim host. The victim destination host sends a SYN ACK back to the random source address and adds an entry to the connection queue. Since the SYN ACK is destined for an incorrect or non-existent host, the last part of the "three-way handshake" is never completed and the entry remains in the connection queue until a timer expires, typically for about one minute. By generating phony TCP SYN packets from random IP addresses at a rapid rate, it is possible to fill up the connection queue and deny TCP services (such as e-mail, file transfer, or WWW) to legitimate users.
There is no easy way to trace the originator of the attack because the IP address of the source is forged.
In this example, this type of attack could be stopped since we are allowing only traffic that was originated by the internal (fa0/0) network destined to the R1 branch network with the use of the "established" keyword.

QUESTION NO: 3

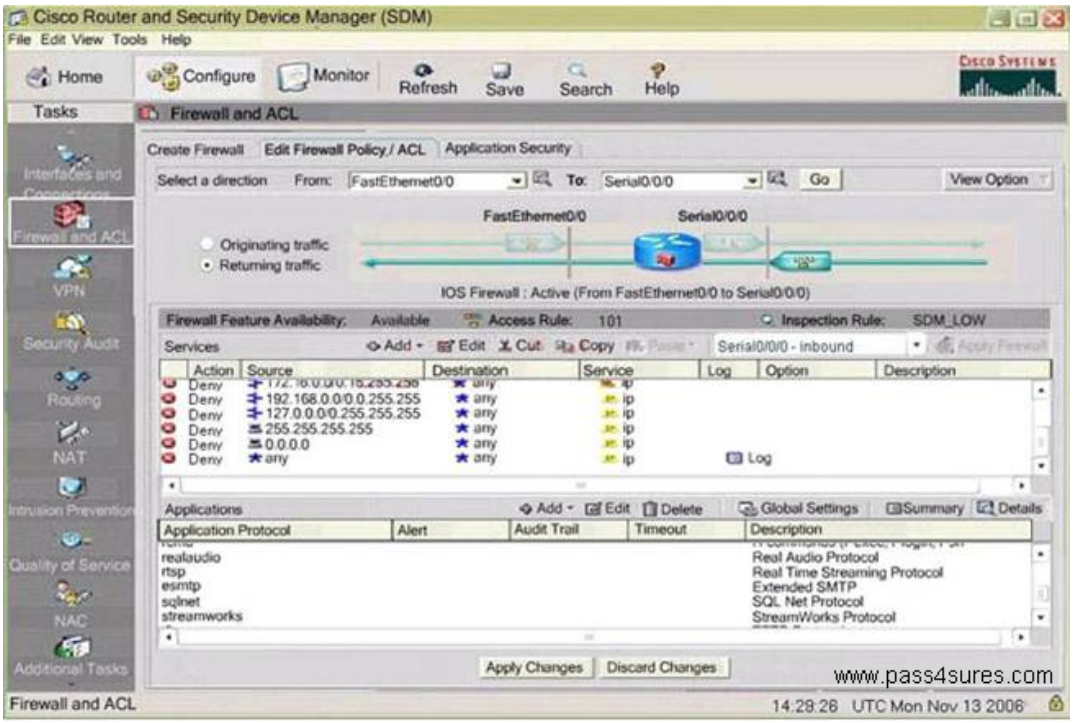
This item contains several questions that you must answer. You can view these questions by clicking on the Questions button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the SDM and the topolgy, neither of which is currently visible.

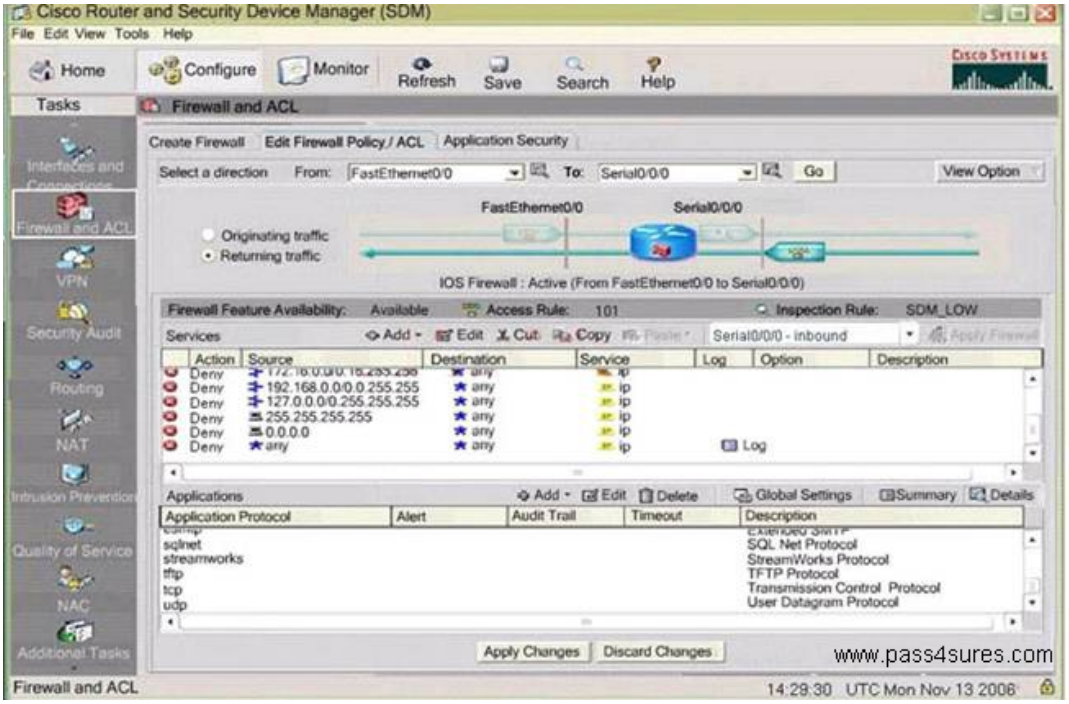
To gain access to either the topology or the SDM, click on the button to left side of the screen that corresponds to the section you wish to access. When you have finished viewing the topolgy or the SDM, you can return to your questions by clicking on the Questions button to the left.

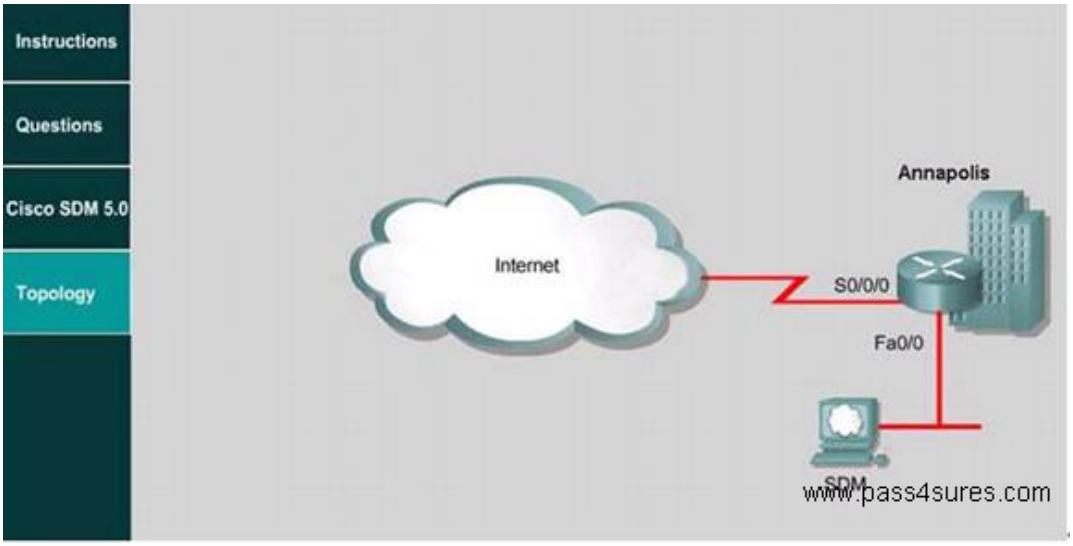





Cisco Router and Security Device Manager (SDM)
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Select a direction
From: FastEthernet0/0
To: Serial0/0/0
Go
View Option
FastEthernet0/0
Serial0/0/0
Originating traffic
Returning traffic
IOS Firewall : Active (From FastEthernet0/0 to Serial0/0/0)
Firewall Feature Availability: Available
Access Rule: 101
Inspection Rule: SDM_LOW
Services
Add
Edit
Cut
Copy
Serial0/0/0 - inbound
Action
Source
Destination
Service
Log
Option
Description
Deny 192.168.0.0/0.0.255.255 any ip
Deny 127.0.0.0/0.255.255.255 any ip
Deny 255.255.255.255 any ip
Deny 0.0.0.0 any ip
Deny any any ip
Log
Applications
Add
Edit
Delete
Global Settings
Summary
Details
Application Protocol
Alert
Audit Trail
Timeout
Description
cuseeme
CUSeeMe Protocol
dns
Domain Name Server
ftp
File Transfer Protocol
h323
H.323 Protocol (e.g. MS NetMeeting, Intel V
https
HTTPS Protocol
Apply Changes
Discard Changes
www.pass4sures.com
Firewall and ACL
14:29:11 UTC Mon Nov 13 2006


Cisco Router and Security Device Manager (SDM)
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Select a direction
From: FastEthernet0/0
To: Serial0/0/0
Go
View Option
FastEthernet0/0
Serial0/0/0
Originating traffic
Returning traffic
IOS Firewall : Active (From FastEthernet0/0 to Serial0/0/0)
Firewall Feature Availability: Available
Access Rule: 101
Inspection Rule: SDM_LOW
Services
Add
Edit
Cut
Copy
Serial0/0/0 - inbound
Action
Source
Destination
Service
Log
Option
Description
Deny 192.168.0.0/0.0.255.255 any ip
Deny 127.0.0.0/0.255.255.255 any ip
Deny 255.255.255.255 any ip
Deny 0.0.0.0 any ip
Deny any any ip
Log
Applications
Add
Edit
Delete
Global Settings
Summary
Details
Application Protocol
Alert
Audit Trail
Timeout
Description
realaudio
Real Audio Protocol
rtsp
Real Time Streaming Protocol
esmtp
Extended SMTP
sqlnet
SQL Net Protocol
streamworks
StreamWorks Protocol
Apply Changes
Discard Changes
www.pass4sures.com
Firewall and ACL
14:29:26 UTC Mon Nov 13 2006





Off Shore Industries is a large worldwide sailing charter. The company has recently upgraded its Internet connectivity. As a recent addition to the network engineering team, you have been tasked with documenting the active Firewall configurations on the Annapolis router using the Cisco Router and Security Device Manager (SDM) utility. Using the SDM output from Firewall and ACL Tasks under the Configure tab, answer the following questions:

Which two statements would be true for a permissible incoming TCP packet on an untrusted Interface in this configuration? (Choose two.)

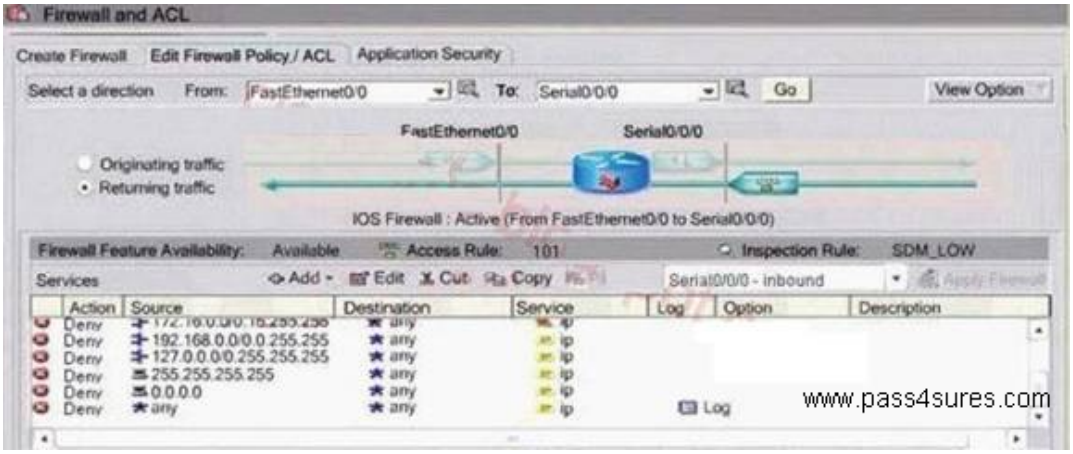
A. The session originated from a trusted Interface
B. The application is not specified within the inspection rule SDM_LOW.
C. The session originated from an untrusted interface
D. The packet has a source address of 10.79.233.186
E. The packet has a source address of 172.16.81.108
F. The packet has a source address of 198.133.219.135

Answer: A,F

Explanation:

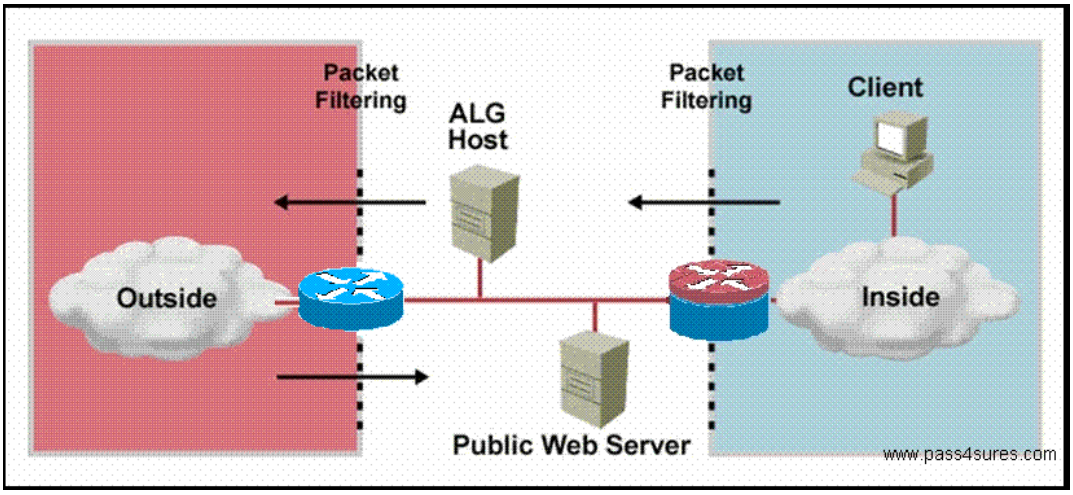
According to the question, after configuring CBAC, the TCP traffic on the untrusted interface can be divided into two types: 1. The inspected return traffic from the intranet is permitted by the state table, so C is right. 2. The TCP traffic permitted by the ACL comes from external network, so E is right.

The direction of ACL101 is from S0/0/0 to f0/0, which only allows the echo- reply/ icmp, time-exceede, unreachable services of the destination address of 172.16.81.108, denies any IP data packets from 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 224.0.0.0/4, 240.0.0.0/4 and 10.79.223/24, as well as adds log to any access. As to the address 172.16.81.108, only part of the ICMP packets are allowed. The address 198.133.219.135 is first initiated from the inside network. If an address of 198.133.219.135 is received from the outside network it should be directely dropped.



QUESTION NO: 4

Refer to the exhibit. What is the name given to the security zone occupied by the public web server?

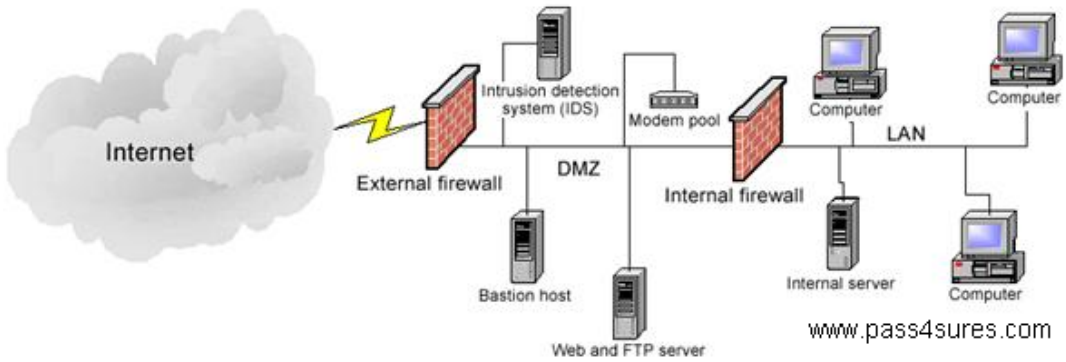


A. proxy network
B. ALG
C. DMZ
D. multiple DMZs
E. extended proxy network
F. protected subnet

Answer: C

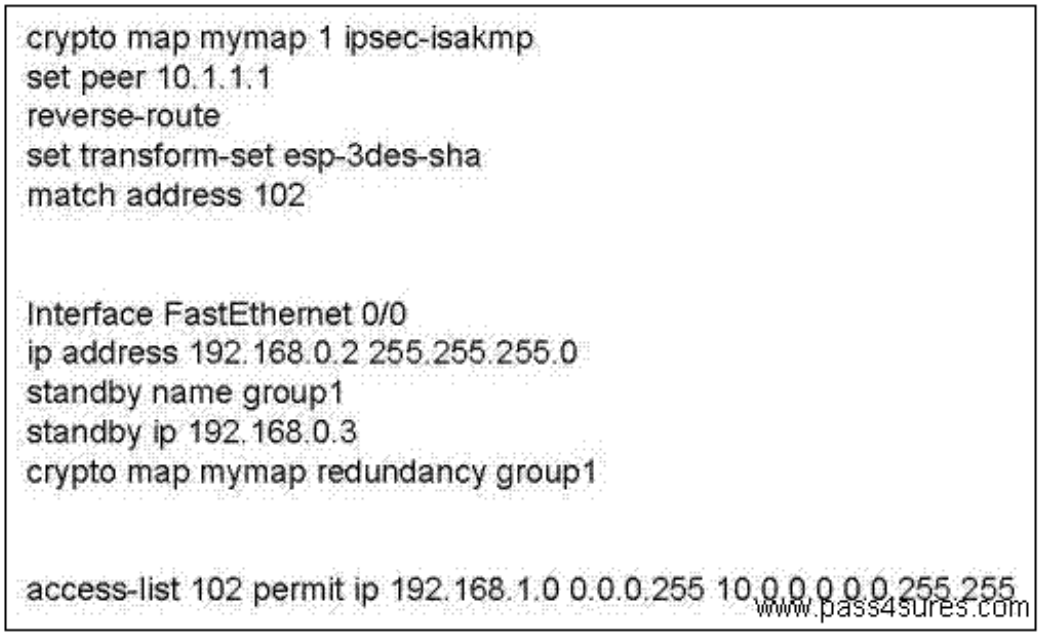
Explanation:
A DMZ, short for demilitarized zone, is a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.
Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. The term comes from military use, meaning a buffer area between two enemies.

A DMZ is the most common and secure firewall topology. It is often referred to as a screened subnet. A DMZ creates a secure space between your Internet and your network, as shown in the figure below:



QUESTION NO: 5

Refer to the exhibit. What are the two options that are used to provide High Availability IPsec? (Choose two.)



A. IPsec Stateful Switchover (SSO)
B. Dynamic Crypto Map
C. IPsec Backup Peerings
D. Dual Router Mode (DRM) IPsec
E. RRI
F. HSRP

Answer: E,F

Explanation:
Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities. This is configured using the "reverse-route" command.
The Hot Standby Router Protocol (HSRP) provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits. This is done by logically grouping one or more routers into a single virtual gateway, and HSRP is configured using the "standby" configuration commands.

QUESTION NO: 6

What are three options for viewing Security Device Event Exchange (SDEE) messages in Security Device Manager (SDM)? (Choose three.)

A. to view SDEE status messages
B. to view SDEE actions
C. to view SDEE statistics
D. to view SDEE alerts
E. to view SDEE keepalive messages
F. to view all SDEE messages

Answer: A,D,F

Explanation:
SDEE Messages
This window lists the SDEE messages received by the router. SDEE messages are generated when there are changes to Cisco IOS IPS configuration.
SDEE Messages
Choose the SDEE message type to display:

All- SDEE error, status, and alert messages are shown.

Error-Only SDEE error messages are shown.

Status-Only SDEE status messages are shown.

Alerts-Only SDEE alert messages are shown.

Reference:
http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/IPS.html#wp1083698

QUESTION NO: 7

Refer to the exhibit. What Cisco feature generated the configuration?