Vendor: EXIN

Exam Code: SCNS

Exam Name: SCNS Tactical Perimeter Defense

Version: Demo

QUESTION NO: 1

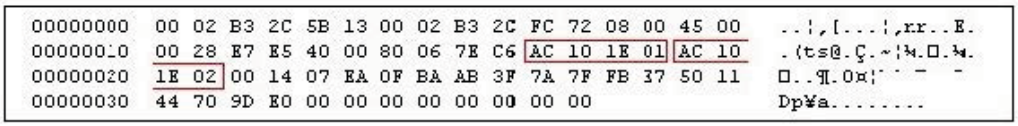
As per the specifications of the RFC on TCP, identify from the list below the correct order of the Control
Bits in the TCP header from the left to the right (i.e., in the order they are sent):

A. PSH, URG, ACK, RST, SYN, FIN
B. SYN, FIN, ACK, PSH, RST, URG
C. ACK, SYN, FIN, URG, PSH, RST
D. URG, ACK, PSH, RST, SYN, FIN
E. FIN, SYN, URG, ACK, PSH, RST

Answer: D

QUESTION NO: 2

Network Monitor was run on a Windows Server 2003. The exhibit shows the actual contents of a Network
Monitor capture file.



What are the IP addresses of the source and destination hosts involved in this communication? To help you determine the two hosts, they have been outlined within the captured content.

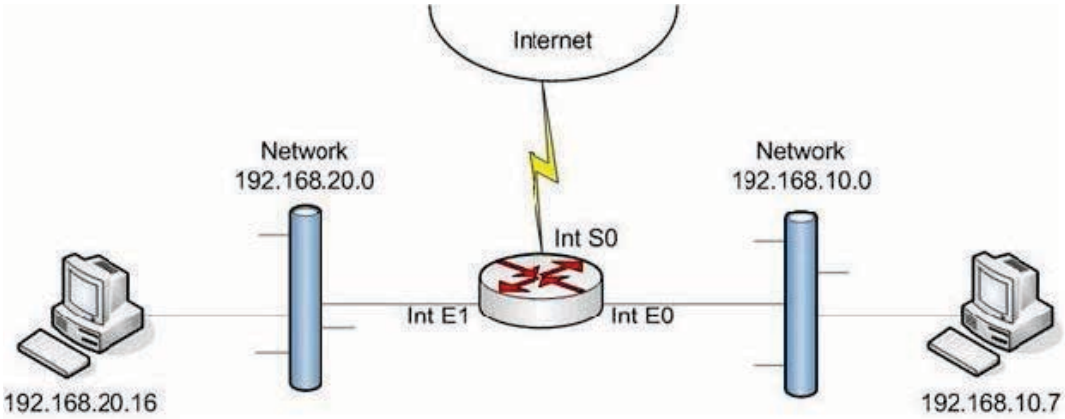
A. 10.18.10.211 & 10.18.71.12
B. 10.28.33.131 & 10.28.64.20
C. 172.16.30.1 & 172.16.30.2
D. 17.26.30.1 & 19.26.30.2
E. 212.168.15.1 & 192.168.15.2

Answer: C

QUESTION NO: 3

The exhibit shows a router with three interfaces E0, E1 and S0. Interfaces E0 and E1 are connected to internal networks 192.168.10.0 and 192.168.20.0 respectively and interface S0 is connected to the Internet.

The objective is to allow only network 192.168.20.0 to access e-commerce Web sites on the Internet, while allowing all internal hosts to access resources within the internal network. From the following, select all the access list statements that are required to make this possible.



A. access-list 113 permit tcp 192.168.20.0 0.0.0.255 any eq 80
B. access-list 113 permit tcp 192.168.20.0 0.0.0.255 any eq 53
C. access-list 113 permit tcp 192.168.20.0 0.0.0.255 any eq 443
D. access-list 113 permit tcp 192.168.20.0 0.0.0.255 any lt 1023
E. int S0, ip access-group 113 in F.
int E1, ip access-group 113 in G.
int S0, ip access-group 113 out

Answer: A,B,C,G

QUESTION NO: 4

What is the function of the following configuration fragment?

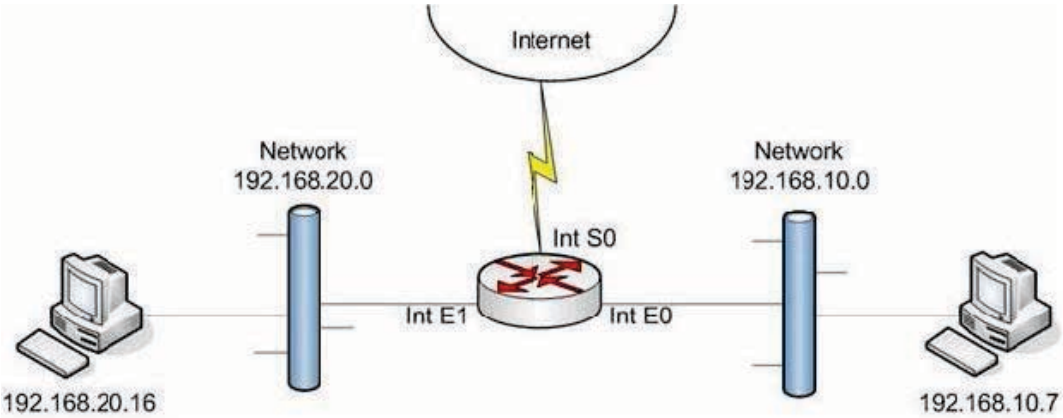
Router#configure terminal
Router(config)#line vty 0 4
Router(config-line)#transport input ssh telnet
Router(config-line)#^Z
Router#

A. The router will attempt to use SSH first, then use Telnet
B. The router will attempt to use Telnet first, then use SSH
C. The router will accept only SSH on VTY 0 4
D. The router will accept both Telnet and SSH connections
E. The router will accept only Telnet on VTY 0 4

Answer: D

QUESTION NO: 5

The exhibit shows a router with three interfaces E0, E1 and S0. Interfaces E0 and E1 are connected to internal networks 192.168.10.0 and 192.168.20.0 respectively and interface S0 is connected to the Internet.



The objective is to allow two hosts, 192.168.20.16 and 192.168.10.7 access to the Internet while all other hosts are to be denied Internet access. All hosts on network 192.168.10.0 and 192.168.20.0 must be allowed to access resources on both internal networks. From the following, select all the access list statements that are required to make this possible.

A. access-list 53 permit 192.168.20.16 0.0.0.0
B. access-list 80 permit 192.168.20.16 0.0.0.0
C. access-list 53 deny 0.0.0.0 255.255.255.255
D. access-list 80 permit 192.168.10.7 0.0.0.0
E. int S0, ip access-group 53 out
F. int S0, ip access-group 80 out

Answer: B,D,F

QUESTION NO: 6

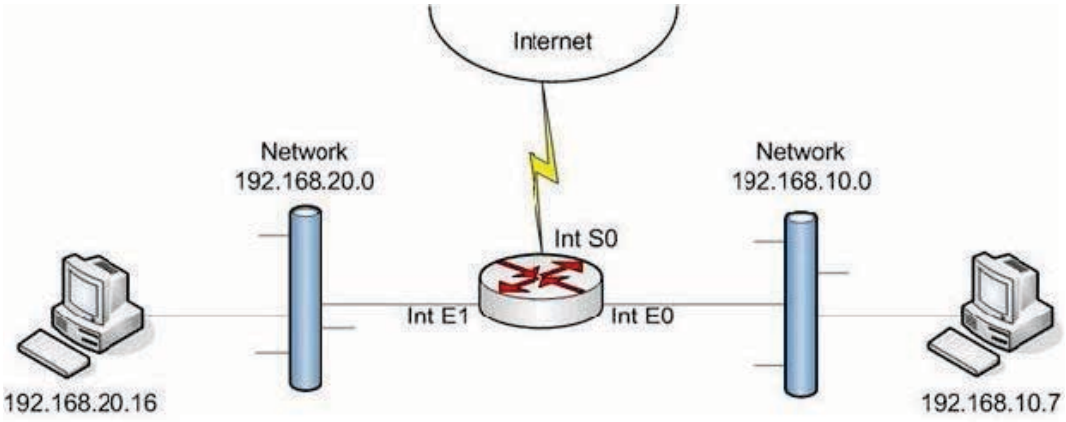
You are going to migrate the Cisco routers in your network from RIPv1 to RIPv2. What is a security advantage that RIPv2 provides over RIPv1?

A. RIPv2 encrypts all of the router updates
B. RIPv2 encrypts all the payloads in router updates
C. RIPv2 provides for authentication using Smart Cards and Kerberos
D. RIPv2 provides for authentication using NTLMv2
E. RIPv2 allows for authentication of updates

Answer: E

QUESTION NO: 7

The exhibit shows a router with three interfaces E0, E1 and S0. Interfaces E0 and E1 are connected to internal networks 192.168.10.0 and 192.168.20.0 respectively and interface S0 is connected to the Internet.



The objective is to allow host 192.168.10.7 access to the Internet via ftp and deny access to the Internet to everyone else while allowing them to access resources amongst themselves. From the following, select all the access list statements that are required to make this possible.

A. access-list 153 permit tcp 192.168.10.7 0.0.0.0 any eq ftp
B. access-list 21 permit ip 192.168.10.7 0.0.0.0 any eq ftp
C. access-list 21 deny 0.0.0.0 255.255.255.255
D. int S0, ip access-group 21 out
E. int S0, ip access-group 153 out
F. int E1, ip access-group 153 in

Answer: A,E

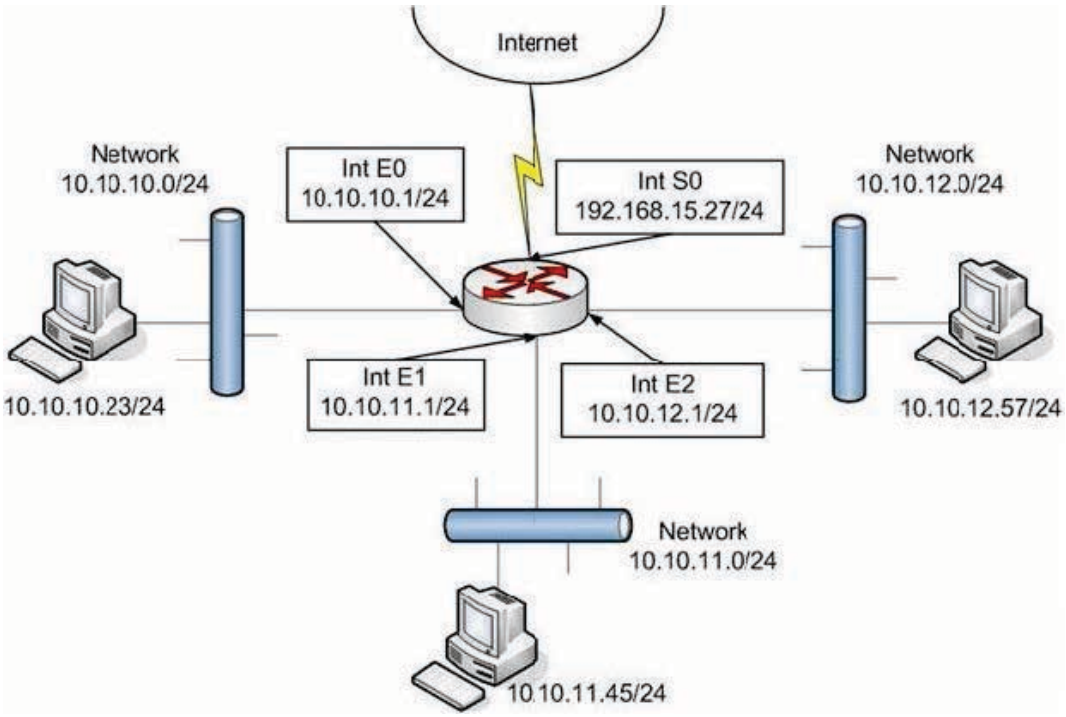
QUESTION NO: 8

You are configuring the Access Lists for your new Cisco Router. The following are the commands that are entered into the router for the list configuration.

Router(config)#access-list 131 deny tcp 10.10.0.0 0.0.255.255 0.0.0.0 255.255.255.255 eq 23
Router(config)#access-list 131 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
Router(config)#interface Serial 0
Router(config-if)#ip access-group 131 out

Based on this configuration, and using the exhibit, select the answers that identify what the list will

accomplish.



A. Block all FTP Data traffic to the Internet
B. Block all FTP Control traffic to the Internet
C. Block all SMTP traffic to the Internet
D. Permit all non-Telnet traffic to the Internet
E. Block all Telnet traffic to the Internet

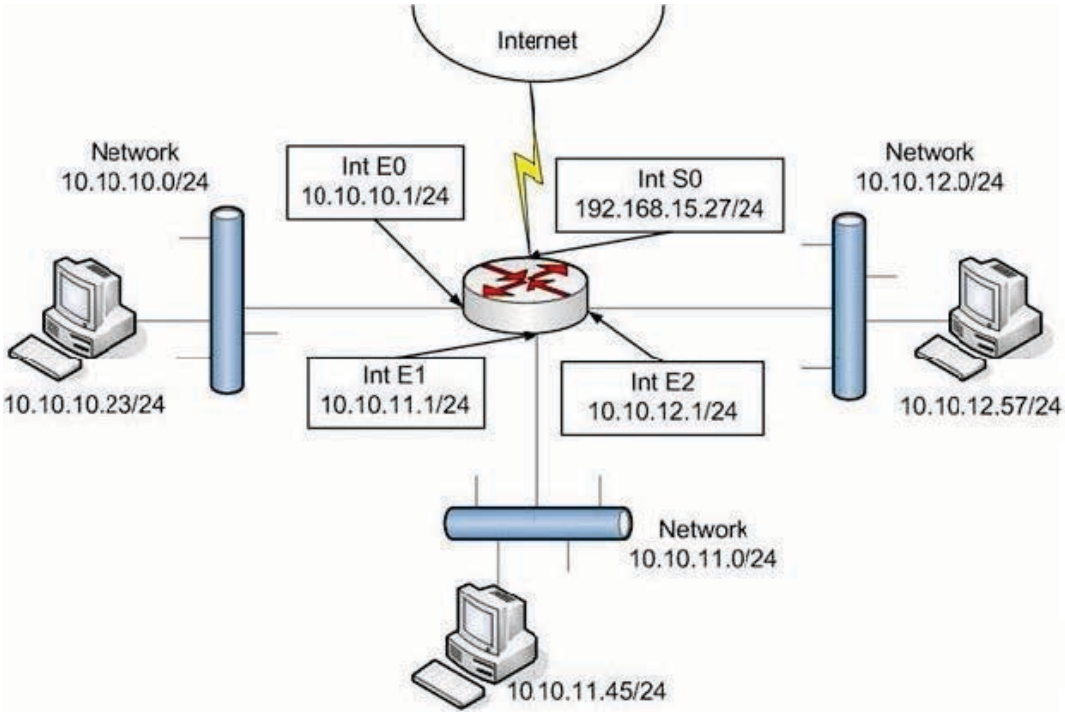
Answer: D,E

QUESTION NO: 9

You are configuring the Access Lists for your new Cisco Router. The following are the commands that are entered into the router for the list configuration.

Router(config)#access-list 171 permit tcp 10.10.0.0 0.0.255.255 any eq 80
Router(config)#access-list 171 deny tcp 0.0.0.0 255.255.255.255 10.10.0.0 0.0.255.255 eq 80
Router(config)#access-list 171 deny tcp any any eq 23
Router(config)#access-list 171 permit tcp 10.10.0.0 0.0.255.255 any eq 20
Router(config)# access-list 171 permit tcp 10.10.0.0 0.0.255.255 any eq 21

Based on this configuration, and using the exhibit, select the answers that identify how the router will deal with network traffic.



A. Permit WWW traffic to the Internet
B. Deny WWW traffic to the internal networks
C. Deny all Telnet traffic
D. Permit FTP traffic to the Internet
E. Permit FTP traffic to the internal networks

Answer: A,D,E

QUESTION NO: 10

You are configuring a L2TP solution between your office and your primary branch office. The CEO has requested a report on the benefits of using this technology. Which of the following benefits does L2TP (with IPSec) provide?

A. Bandwidth Management
B. Encryption
C. User Authentication
D. Packet Authentication
E. Key Management

Answer: B,D,E

QUESTION NO: 11

As you analyze the settings of the Secure Server (Require Security) IPSec policy in Windows Server

2003, you are looking at the options available for encryption and integrity. Which of the following answers presents a legitimate combination for encryption and integrity in the IPSec policy?

A. Encryption: SHA1, Integrity: 3DES
B. Encryption: 3DES, Integrity: SHA1
C. Encryption: RSA, Integrity: MD5
D. Encryption: MD5, Integrity: RSA
E. Encryption: SHA1, Integrity: MD5

Answer: B

QUESTION NO: 12

You are configuring a new custom IPSec policy on your Windows Server 2003 machine. On the rules tab, you find the three default options under the IP Filter List. What are these three default options?

A. All TCP Traffic
B. All UDP Traffic
C. All IP Traffic
D. All ICMP Traffic
E. <Dynamic>

Answer: C,D,E

QUESTION NO: 13

During an analysis of your IPSec implementation, you capture traffic with Network Monitor. You are verifying that IP is properly identifying AH. When you look into IP, what protocol ID would IP identify with AH?

A. Protocol ID 0x800 (800)
B. Protocol ID 0x6 (6)
C. Protocol ID 0x15 (21)
D. Protocol ID 0x33 (51)
E. Protocol ID 0x1 (1)

Answer: D

QUESTION NO: 14

You are designing a new IPSec implementation for your organization, and are trying to determine your security needs. You need to clearly understand the implementation choices, before you make any changes to the network. Which of the following describes what transport and tunnel modes protect using IPSec?

A. In transport mode, IPSec protects upper-layer protocols.
B. In transport mode, IPSec protects just the TCP header.
C. In tunnel mode, IPSec protects the upper-layer protocols.
D. In transport mode, IPSec protects the entire IP packet.
E. In tunnel mode, IPSec protects the entire IP packet.
F. In tunnel mode, IPSec protects just the IP header.

Answer: A,E

QUESTION NO: 15

If you wish to implement IPSec between two branch offices of your organization, and wish for this to include the encryption of the full packet, which implementation would meet your needs?

A. ESP in Transport Mode
B. AH in Transport Mode
C. ESP in Tunnel Mode
D. AH in Tunnel Mode
E. Combination of both AH and ESP in Transport Mode

Answer: C

QUESTION NO: 16

In your current organization, you have been given the task of implementing the IPSec solution. All your servers are running Windows Server 2003, so you wish to use the built in policies. What are the three default IPSec policies in Windows Server 2003?

A. Server (Require Security)
B. Server (Request Security)
C. Client (Respond Only)
D. Client (Request Security)
E. Server (Respond Only)

Answer: A,B,C

QUESTION NO: 17

You have clients that are connected to your network via a VPN. What is the internetwork environment that connects the VPN Client to the VPN Server called?

A. VPN Tunnel
B. Ethernet Tunnel
C. Internet Pipe
D. Transit Network
E. Session Pipe

Answer: D

QUESTION NO: 18

To verify that your PPTP implementation is working as you intended, you sniff the network after the implementation has been completed. You are looking for specific values in the captures that will indicate to you the type of packets received. You analyze the packets, including headers and payload. PPTP works at which layer of the OSI model?

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

Answer: B

QUESTION NO: 19

You are the firewall administrator for your company and you have just learned that the Server administrators are gearing up support an L2TP based VPN solution. You are told to be sure that your firewall rule sets will not hinder the performance of the VPN. Which port, from the following list, will you have to allow through the firewall?

A. TCP 1701
B. UDP 1701
C. TCP 443
D. UDP 443
E. TCP 1601

Answer: B

QUESTION NO: 20

After you implemented your IPSec solution, you wish to run some tests to verify functionality. Which of the following provides confidentiality and authentication when implementing IPSec?

A. Authentication Header
B. Encapsulating Security Payload
C. Security Associations
D. Security Authentications
E. Encapsulating Delimiters

Answer: B

QUESTION NO: 21

Your network is going to implement a new IPSec solution. Which of the following IPSec components is used to define the security environment in which the two hosts communicate?

A. Management Tools
B. Security Association API
C. IPSec Driver
D. IP Policy Agent
E. IP Security Policy and Security Association

Answer: E

QUESTION NO: 22

You are the firewall administrator at your company and the network administrators have decided to implement a PPTP VPN solution, which of these ports would you need to allow through the firewall to allow these VPN sessions into your network?

A. 1723
B. 2397
C. 5273
D. 4378
E. 7135

Answer: A