Checkpoint 156-315

156-315.65 Check Point Security Administration NGX II R65

Practice Test

Version 3.1

QUESTION NO: 1

The following is cphaprob state command output from a ClusterXL New mode High Availability memberWhen member 192.168.1.2 fails over and restarts, which member will become active?

```
Cluster Mode: New High Availability (Active Up)

Number          Unique IP Address      Assigned Load      State
1 (local)       192.168.1.1            0%                 standby
2               192.168.1.2            100%               active
```

A. 192.168.1.2
B. 192.168.1 1
C. Both members' state will be standby
D. Both members' state will be active

Answer: B

QUESTION NO: 2

What is the command to upgrade a SecurePlatform NG with Application Intelligence (AI) R55 SmartCenter Server to VPN-1 NGX using a CD?

A. cd patch add
B. fwm upgrade_tool
C. cppkg add
D. patchadd
E. patch addcd

Answer: E

QUESTION NO: 3

You have a production implementation of Management High Availability, at version VPN-1 NG with Application Intelligence R55. You must upgrade your two SmartCenter Servers to VPN-1 NGX. What is the correct procedure?

A. 1. Synchronize the twoSmartCenter Servers.
2. Upgrade the secondary SmartCenter Server.
3. Upgrade the primary SmartCenter Server.
4. Configure both SmartCenter Server host objects version to VPN-1 NGX.
5. Synchronize the Servers again.
B. 1. Synchronize the two SmartCenter Servers.
2. Perform an advanced upgrade on the primary SmartCenter Server.

3. Upgrade the secondary SmartCenter Server.
4. Configure both SmartCenter Server host objects to version VPN-1 NGX.
5. Synchronize the Servers again.

C. 1. Perform an advanced upgrade on the primary SmartCenter Server.
2. Configure the primary SmartCenter Server host object to version VPN-1 NGX.
3. Synchronize the primary with the secondary SmartCenter Server.
4. Upgrade the secondary SmartCenter Server.
5. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
6. Synchronize the Servers again.

D. 1. Synchronize the two SmartCenter Servers.
2. Perform an advanced upgrade on the primary SmartCenter Server.
3. Configure the primary SmartCenter Server host object to version VPN-1 NGX.
4. Synchronize the two Servers again.
5. Upgrade the secondary SmartCenter Server.
6. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
7. Synchronize the Servers again.

Answer: B

QUESTION NO: 4

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN-1 Pro Gateway. You want to implement Management High Availability (HA). You have a spare machine to configure as the secondary SmartCenter Server. How do you configure the new machine to be the standby SmartCenter Server, without making any changes to the existing primary SmartCenter Server? (Changes can include uninstalling and reinstalling.)

A. You cannot configure Management HA, when either the primary or secondary SmartCenter Server is running on a VPN-1 Pro Gateway.
B. The new machine cannot be installed as the Internal Certificate Authority on its own.
C. The secondary Server cannot be installed on a SecurePlatform Pro machine alone.
D. Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server.

Answer: A

QUESTION NO: 5

You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use four machines with the following configurations:

Cluster Member 1: OS: SecurePlatform, NICs: QuadCard, memory: 256 MB, Security Gateway

version: VPN-1 NGX
Cluster Member 2: OS: SecurePlatform, NICs: four Intel 3Com, memory: 512 MB, Security Gateway version: VPN-1 NGX
Cluster Member 3: OS: SecurePlatform, NICs: four other manufacturers, memory: 128 MB, Security Gateway version: VPN-1 NGX
SmartCenter Pro Server: MS Windows Server 2003, NIC: Intel NIC (one), Security Gateway and primary SmartCenter Server installed version: VPN-1 NGX
Are these machines correctly configured for a ClusterXL deployment?

A. No, theSmartCenter Pro Server is not using the same operating system as the cluster members.
B. Yes, these machines are configured correctly for aClusterXL deployment.
C. No, Cluster Member 3 does not have the required memory.
D. No, the SmartCenter Pro Server has only one NIC.

Answer: B

QUESTION NO: 6

You set up a mesh VPN Community, so your internal networks can access your partner's network, and vice versa. Your Security Policy encrypts only FTP and HTTP traffic through a VPN tunnel. All other traffic among your internal and partner networks is sent in clear text. How do you configure the VPN Community?

A. Disable "accept all encrypted traffic", and put FTP and HTTP in the Excluded services in the Community object. Add a rule in the Security Policy for services FTP and http, with the Community object in the VPN field.
B. Disable "accept all encrypted traffic" in the Community, and add FTP and HTTP services to the Security Policy, with that Community object in the VPN field.
C. Enable "accept all encrypted traffic", but put FTP and HTTP in the Excluded services in the Community. Add a rule in the Security Policy, with services FTP and http, and the Community object in the VPN field.
D. Put FTP and HTTP in the Excluded services in the Community object. Then add a rule in the Security Policy to allow Any as the service, with the Community object in the VPN field.

Answer: B

QUESTION NO: 7

How does a standby SmartCenter Server receive logs from all Security Gateways, when an active SmartCenter Server fails over?

A. The remote Gateways must set up SIC with the secondarySmartCenter Server, for logging.
B. Establish Secure Internal Communications (SIC) between the primary and secondary Servers. The secondary Server can then receive logs from the Gateways, when the active Server fails over.
C. On the Log Servers screen (from the Logs and Masters tree on the gateway object's General Properties screen), add the secondary SmartCenter Server object as the additional log server. Reinstall the Security Policy.
D. Create a Check Point host object to represent the standby SmartCenter Server. Then select "Secondary SmartCenter Server" and Log Server", from the list of Check Point Products on the General properties screen.
E. The secondary Server's host name and IP address must be added to the Masters file, on the remote Gateways.

Answer: C

QUESTION NO: 8

You want only RAS signals to pass through H.323 Gatekeeper and other H.323 protocols, passing directly between end points. Which routing mode in the VoIP Domain Gatekeeper do you select?

A. Direct
B. Direct and Call Setup
C. Call Setup
D. Call Setup and Call Control

Answer: A

QUESTION NO: 9

Which component functions as the Internal Certificate Authority for VPN-1 NGX?

A. VPN-1 Certificate Manager
B. SmartCenterServer
C. SmartLSM
D. Policy Server
E. Security Gateway

Answer: B

QUESTION NO: 10

:
You are configuring the VoIP Domain object for a Skinny Client Control Protocol (SCCP)

environment protected by VPN-1 NGX. Which VoIP Domain object type can you use?

A. CallManager
B. Gatekeeper
C. Gateway
D. Proxy
E. Transmission Router

Answer: A

QUESTION NO: 11

What type of packet does a VPN-1 SecureClient send to its Policy Server, to report its Secure Configuration Verification status?

A. ICMPPort Unreachable
B. TCPkeep alive
C. IKE Key Exchange
D. ICMP Destination Unreachable
E. UDPkeep alive

Answer: E

QUESTION NO: 12

Which Security Servers can perform Content Security tasks, but CANNOT perform authentication tasks?

A. Telnet
B. FTP
C. SMTP
D. HTTP

Answer: C

QUESTION NO: 13

Which Security Server can perform content-security tasks, but CANNOT perform authentication tasks?

A. FTP

B. SMTP
C. Telnet
D. HTTP
E. rlogin

Answer: B

QUESTION NO: 14

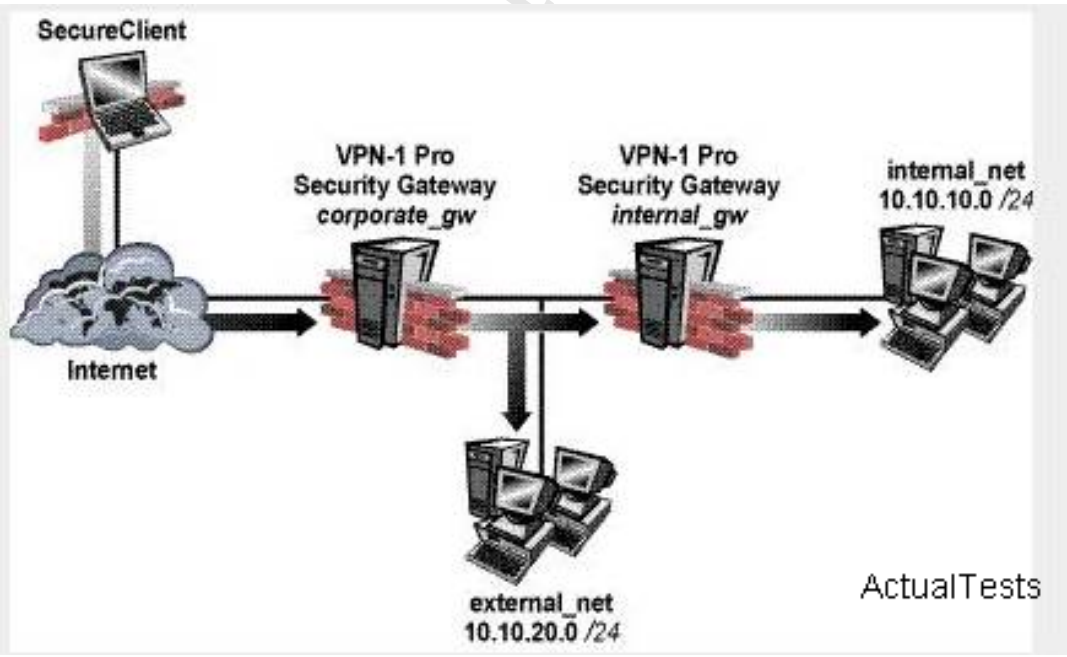
You want VPN traffic to match packets from internal interfaces. You also want the traffic to exit the Security Gateway, bound for all sitE. to-site VPN Communities, including Remote Access Communities. How should you configure the VPN match rule?

A. internal_clear > AII_GwToGw
B. Communities > Communities
C. Internal_clear > External_Clear
D. Internal_clear > Communities
E. internal clear>All communities

Answer: E

QUESTION NO: 15

The following diagram illustrates how a VPN-1 SecureClient user tries to establish a VPN with hosts in the external_net and internal_net from the Internet. How is the Security Gateway VPN Domain created?



A. Internal Gateway VPN Domain = internal_net;
External VPN Domain = external net + external gateway object + internal_net.
B. Internal Gateway VPN Domain = internal_net.
External Gateway VPN Domain = external_net + internal gateway object
C. Internal Gateway VPN Domain = internal_net;
External Gateway VPN Domain = internal_net + external_net
D. Internal Gateway VPN Domain = internal_net.
External Gateway VPN Domain = internal VPN Domain + internal gateway object + external_net

Answer: D

QUESTION NO: 16

A cluster contains two members, with external interfaces 172.28.108.1 and 172.28.108.2. The internal interfaces are 10.4.8.1 and 10.4.8.2. The external cluster's IP address is 172.28.108.3, and the internal cluster's IP address is 10.4.8.3. The synchronization interfaces are 192.168.1.1 and 192.168.1.2. The Security Administrator discovers State Synchronization is not working properly, cphaprob if command output displays as follows:What is causing the State Synchronization problem?

```
Required interfaces: 3
Required secured interfaces: 1
eth0 UP (sync, secured) multicast
eth1 UP non sync (non secured) multicast
eth2 UP non sync (non secured), multicast
Virtual cluster interfaces: 3
eth0 192.168.1.3
eth1 172.28.108.3
eth2 10.4.8.3
```

A. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.
B. Interfaces 192.168.1.1 and 192.168.1.2 have defined 192.168.1.3 as asuB. interface.
C. The synchronization interface on the cluster member object's Topology tab is enabled with "Cluster Interface". Disable this interface.
D. The synchronization network has a cluster, with IP address 192.168.1.3 defined in the gateway-cluster object. Remove the 192.168.1.3 VIP interface from the cluster topology.

Answer: D

QUESTION NO: 17

How can you completely tear down a specific VPN tunnel in an intranet IKE VPN deployment?

A. Run the commandvpn tu on the Security Gateway, and choose the option "Delete all IPSec+IKE SAs for ALL peers and users".
B. Run the commandvpn tu on the SmartCenter Server, and choose the option "Delete all IPSec+IKE SAs for ALL peers and users".
C. Run the command vpn tu on the Security Gateway, and choose the option "Delete all IPSec+IKE SAs for a given peer (GW)".
D. Run the command vpn tu on the Security Gateway, and choose the option "Delete all IPSec SAs for a given user (Client)".
E. Run the commandvpn tu on the Security Gateway, and choose the option "Delete all IPSec SAs for ALL peers and users".

Answer: C

QUESTION NO: 18

How can you prevent delay-sensitive applications, such as video and voice traffic, from being dropped due to long queues when using a Check Point QoS solution?

A. Low latency class
B. DiffServrule
C. guaranteed per connection
D. Weighted Fair Queuing
E. guaranteed per VoIP rule

Answer: A

QUESTION NO: 19

You are preparing to deploy a VPN-1 Pro Gateway for VPN-1 NGX. You have five systems to choose from for the new Gateway, and you must conform to the following requirements:

Operating-system vendor's license agreement
Check Point's license agreement
Minimum operating-system hardware specification
Minimum Gateway hardware specification
Gateway installed on a supported operating system (OS)

Which machine meets ALL of the following requirements?

A. Processor: 1.1 GHz RAM: 512MB Hard disk: 10 GB OS: Windows 2000 Workstation
B. Processor: 2.0 GHz RAM: 512MB Hard disk: 10 GB OS: Windows ME

C. Processor: 1.5 GHz RAM: 256 MB Hard disk: 20 GB OS: Red Hat Linux 8.0
D. Processor: 1.67 GHz RAM: 128 MB Hard disk: 5 GB OS: FreeBSD
E. Processor 2.2 GHzRAM: 256 MB Hard disk: 20 GB OS: Windows 2000 Server

Answer: E

QUESTION NO: 20

Which of the following actions is most likely to improve the performance of Check Point QoS?

A. Turn "per rule guarantees" into "per connection guarantees".
B. Install CheckpointQoS only on the external interfaces of the QoS Module.
C. Put the most frequently used rules at the bottom of the QoS Rule Base.
D. Turn "per rule limits" into "per connection limits".
E. Define weights in the Default Rule in multiples of 10.

Answer: B

QUESTION NO: 21

In a Management High Availability (HA) configuration, you can configure synchronization to occur automatically, when:

1 The Security Policy is installed.
2.The Security Policy is saved.
3.The Security Administrator logs in to the secondary SmartCenter Server, and changes its status to active.
4.A scheduled event occurs.
5.The user database is installed.

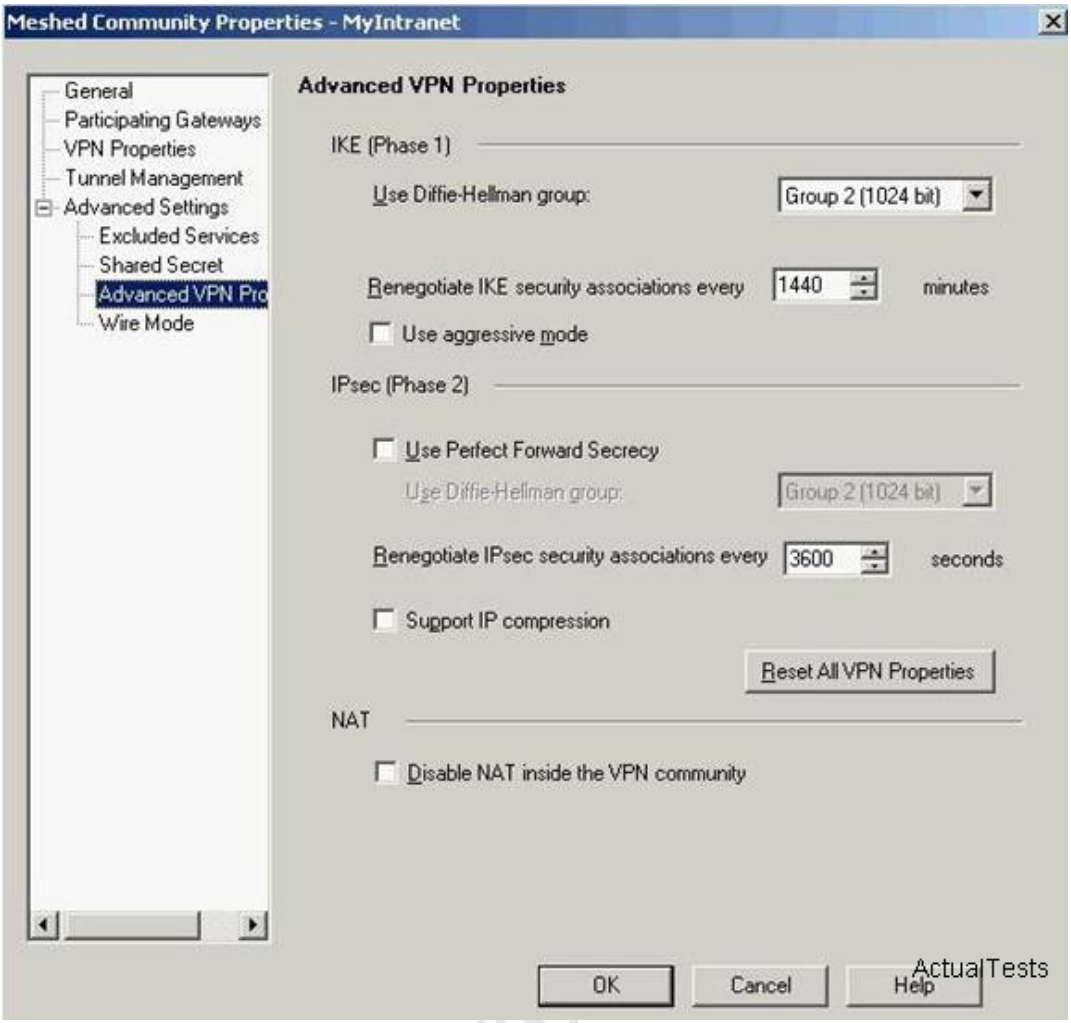
Select the BEST response for the synchronization sequence. Choose one.

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

Answer: E

QUESTION NO: 22

Stephanie wants to reduce the encryption overhead and improve performance for her mesh VPN Community. The Advanced VPN Properties screen below displays adjusted page settings:What can Stephanie do to achieve her goal?

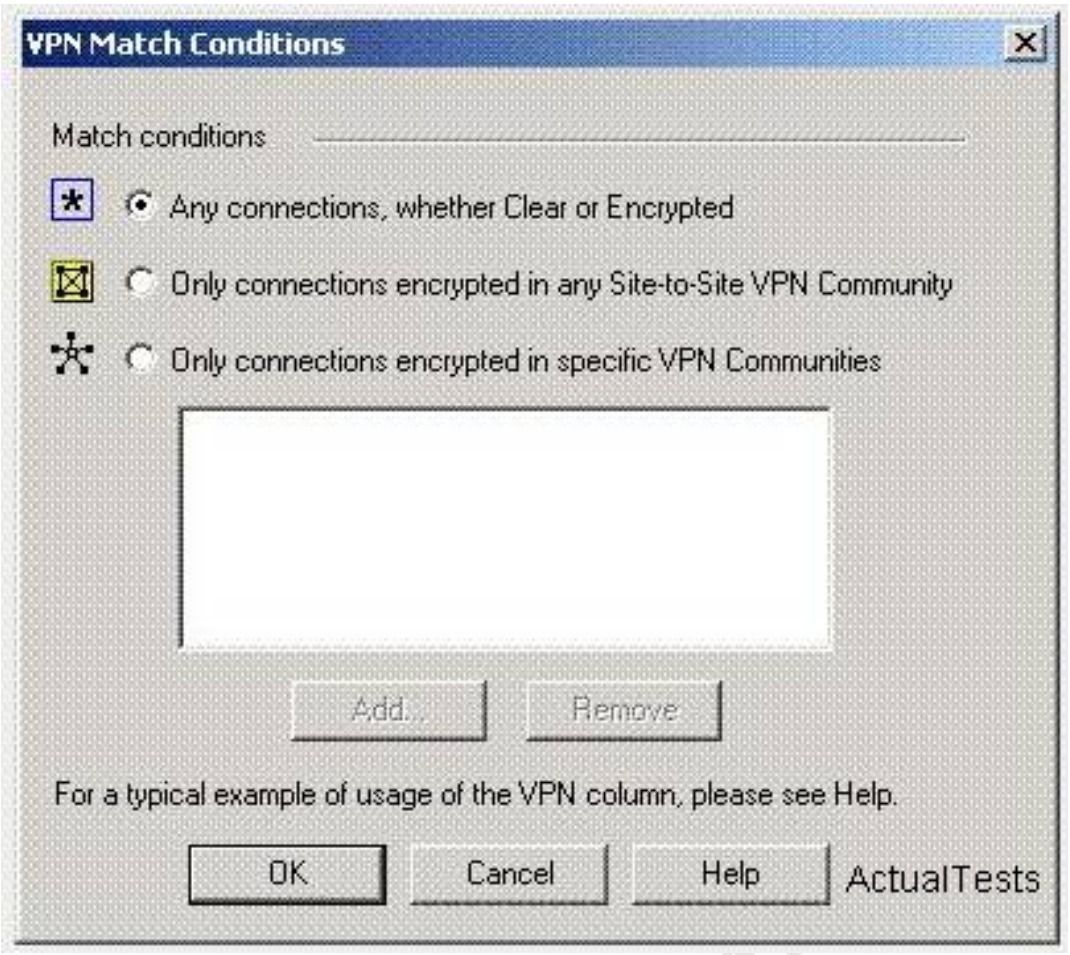


A. Check the box "Use Perfect Forward Secrecy".
B. Change the setting "UseDiffiE. Hellman group" to "Group 5 (1536 bit)".
C. Check the box "Use aggressive mode".
D. Check the box "Support IP compression"
E. Reduce the setting "Renegotiate IKE security associations every" to "720".

Answer: D

QUESTION NO: 23

Steve tries to configure Directional VPN Rule Match in the Rule Base. But the Match column does not have the option to see the Directional Match. Steve sees the following screen. What is the problem?



A. Steve must enabledirectional_match(true) in the objects_5_0.C file on SmartCenter Server.
B. Steve must enable Advanced Routing on each Security Gateway.
C. Steve must enable VPN Directional Match on the VPN Advanced screen, in Global properties.
D. Steve must enable a dynamiC. routing protocol, such as OSPF, on the Gateways.
E. Steve must enable VPN Directional Match on the gateway object's VPN tab.

Answer: C

QUESTION NO: 24

Jerry is concerned that a denial-oF. service (DoS) attack may affect his VPN Communities. He decides to implement IKE DoS protection. Jerry needs to minimize the performance impact of implementing this new protection. Which of the following configurations is MOST appropriate for Jerry?

A. Set Support IKEDoS protection from identified source to "Puzzles", and Support IKE DoS protection from unidentified source to "Stateless".
B. Set Support IKE Dos Protection from identified source, and Support IKEDoS protection from unidentified source to "Puzzles".
C. Set Support IKE DoS protection from identified source to "Stateless," and Support IKE DoS protection from unidentified source to "Puzzles".

D. Set "Support IKE DoS protection" from identified source, and "Support IKE DoS protection" from unidentified source to "Stateless".
E. Set Support IKEDoS protection from identified source to "Stateless", and Support IKE DoS protection from unidentified source to "None".

Answer: D

QUESTION NO: 25

Where can a Security Administrator adjust the unit of measurement (bps, Kbps or Bps), for Check Point QoS bandwidth?

A. Global Properties
B. QoS Class objects
C. Check Point gateway object properties
D. $CPDIR/conf/qos_props.pf
E. Advanced Action options in eachQoS rule

Answer: A

QUESTION NO: 26

You are configuring the VoIP Domain object for an H.323 environment, protected by VPN-1 NGX. Which VoIP Domain object type can you use?)

A. Transmission Router
B. Gatekeeper
C. Call Manager
D. Proxy
E. Call Agent

Answer: B

QUESTION NO: 27

Problems sometimes occur when distributing IPSec packets to a few machines in a Load Sharing Multicast mode cluster, even though the machines have the same source and destination IP addresses. What is the best Load Sharing method for preventing this type of problem?

A. Load Sharing based on IP addresses, ports, and serial peripheral interfaces (SPI)
B. Load Sharing based on SPIs only

C. Load Sharing based on IP addresses only
D. Load Sharing based on SPIs and ports only
E. Load Sharing based on IP addresses and ports

Answer: E

QUESTION NO: 28

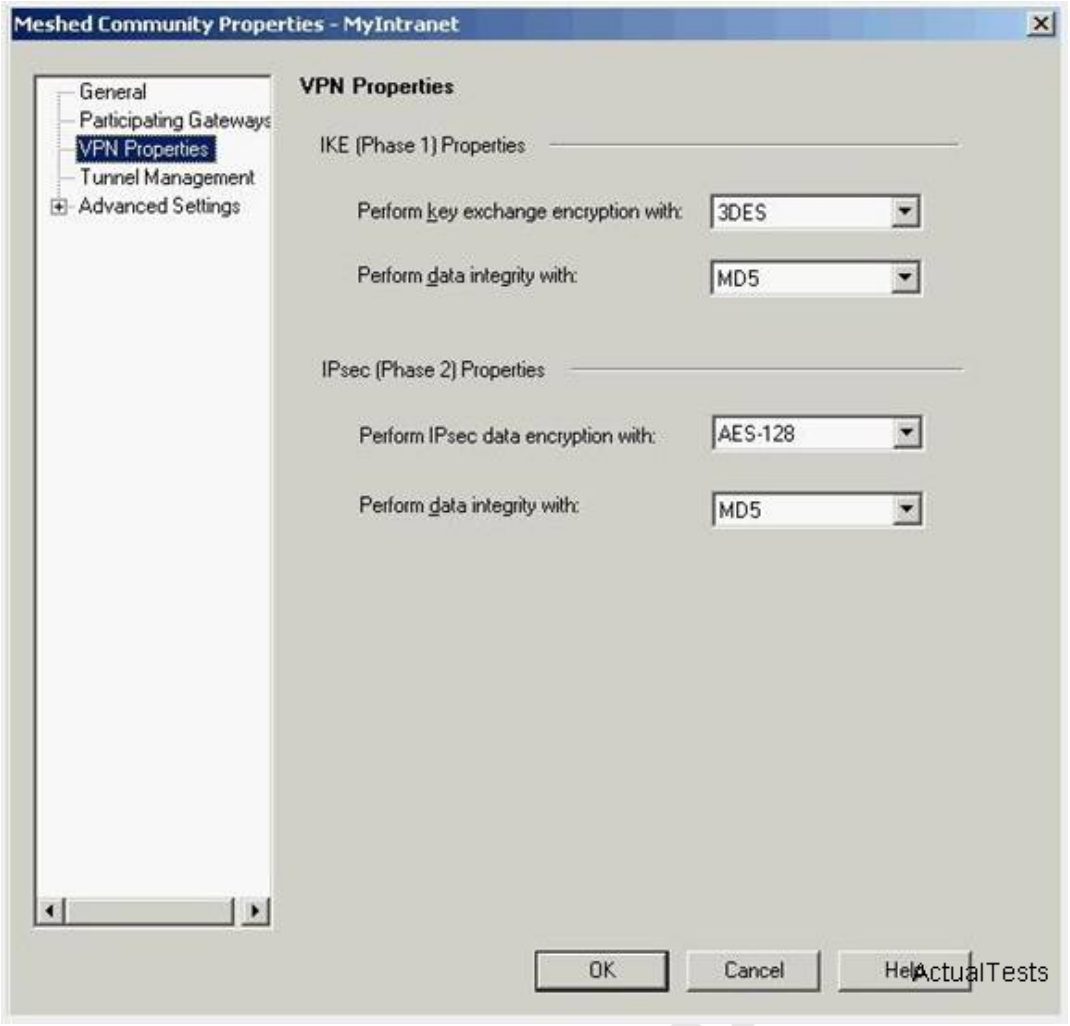
Problems sometimes occur when distributing IPSec packets to a few machines in a Load Sharing Multicast mode cluster, even though the machines have the same source and destination IP addresses. What is the best Load Sharing method for preventing this type of problem?

A. Load Sharing based on IP addresses, ports, and serial peripheral interfaces (SPI)
B. Load Sharing based on SPIs only
C. Load Sharing based on IP addresses only
D. Load Sharing based on SPIs and ports only
E. Load Sharing based on IP addresses and ports

Answer: E

QUESTION NO: 29

Jacob is using a mesh VPN Community to create a sitE. to-site VPN. The VPN properties in this mesh Community display in this graphic:Which of the following statements is TRUE?



A. If Jacob changes the setting, "Perform key exchange encryption with" from "3DES" to "DES", he will enhance the VPN Community's security and reduce encryption overhead.
B. Jacob must change thedatA. integrity settings for this VPN Community. MD5 is incompatible with AES.
C. If Jacob changes the setting "Perform IPSec data encryption with" from "AES-128" to "3DES", he will increase the encryption overhead.
D. Jacob's VPN Community will perform IKE Phase 1 key-exchange encryption, using the longest key VPN-1 NGX supports.

Answer: C

QUESTION NO: 30

Rachel is the Security Administrator for a university. The university's FTP servers have old hardware and software. Certain FTP commands cause the FTP servers to malfunction. Upgrading the FTP servers is not an option at this time. Which of the following options will allow Rachel to control which FTP commands pass through the Security Gateway protecting the FTP servers?

A. Global Properties > Security Server > Allowed FTP Commands

B. SmartDefense > Application Intelligence > FTP Security Server
C. Rule Base > Action Field > Properties
D. Web Intelligence > Application Layer > FTP Settings
E. FTP Service Object > Advanced > Blocked FTP Commands

Answer: B

QUESTION NO: 31

You want to establish a VPN, using Certificates. Your VPN will exchange Certificates with an external partner. Which of the following activities should you do first?

A. Manually import your partner's Access Control List.
B. Exchange a shared secret, before importing Certificates.
C. Create a new logical-server object, to represent your partner's CA.
D. Manually import your partner's Certificate Revocation List.
E. Exchange exportedCAkeys and use them to create a new server object, to represent your partner's Certificate Authority (CA).

Answer: E

QUESTION NO: 32

You are reviewing SmartView Tracker entries, and see a Connection Rejection on a Check Point QoS rule. What causes the Connection Rejection?

A. No QOS rule exists to match the rejected traffic.
B. The number of guaranteed connections is exceeded. The rule's action properties are not set to accept additional connections.
C. The Constant Bit Rate for a Low Latency Class has been exceeded by greater than 10%, and the Maximal Delay is set below requirements.
D. Burst traffic matching the Default Rule is exhausting the Check Point QoS global packet buffers.
E. The guarantee of one of the rule'ssuB. rules exceeds the guarantee in the rule itself.

Answer: B

QUESTION NO: 33

Wayne configures an HTTP Security Server to work with the content vectoring protocol to screen forbidden sites. He has created a URI resource object using CVP with the following settings:

Use CVP
Allow CVP server to modify content
Return data after content is approved

He adds two rules to his Rule Base: one to inspect HTTP traffic going to known forbidden sites, the other to allow all other HTTP traffic.

Wayne sees HTTP traffic going to those problematic sites is not prohibited.

What could cause this behavior?

A. The Security Server Rule is after the general HTTP Accept Rule.
B. The Security Server is not communicating with the CVP server.
C. The Security Server is not configured correctly.
D. The Security Server is communicating with the CVP server, but no restriction is defined in the CVP server.

Answer: A

QUESTION NO: 34

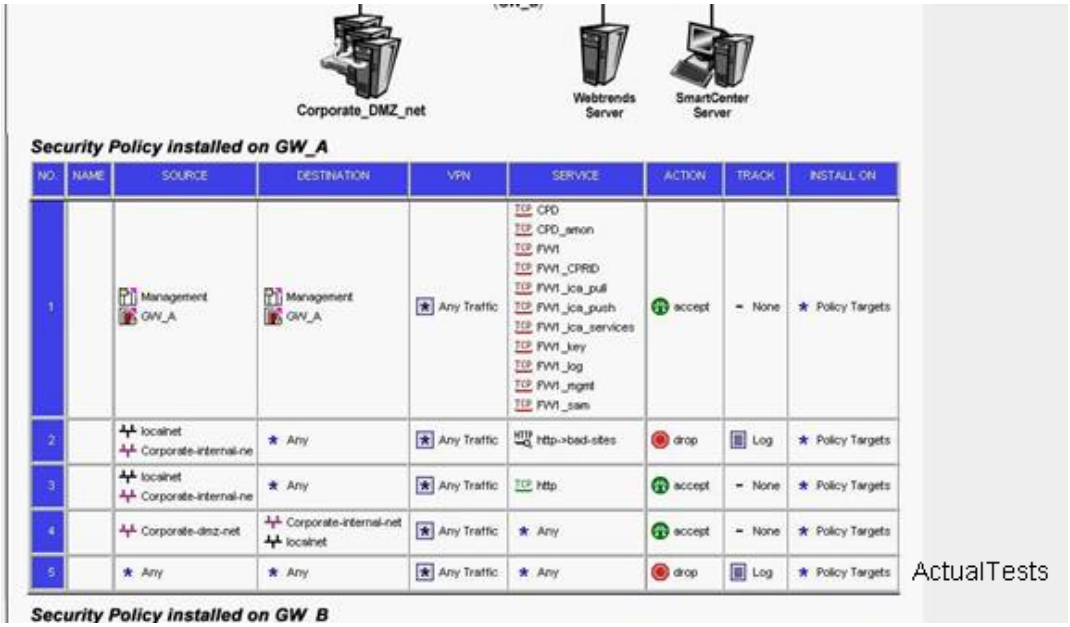
You have two Nokia Appliances: one IP530 and one IP380. Both Appliances have IPSO 3.9 and VPN-1 Pro NGX installed in a distributed deployment. Can they be members of a gateway cluster?

A. No, because the Gateway versions must not be the same on both security gateways
B. Yes, as long as they have the same IPSO version and the same VPN-1 Pro version
C. No, because members of a security gateway cluster must be installed as stanD. alone deployments
D. Yes, because both gateways are from Nokia, whether they have the same VPN-1 PRO version or not
E. No, because the appliances must be of the same model (Both should be IP530 or IP380.)

Answer: B

QUESTION NO: 35

You want to block corporatE. internal-net and localnet from accessing Web sites containing inappropriate content. You are using WebTrends for URL filtering. You have disabled VPN-1 Control connections in the Global properties. Review the diagram and the Security Policies for GW_A and GW_B in the exhibit provided.



Corporate users and localnet users receive message "Web cannot be displayed". In SmartView Tracker, you see the connections are dropped with message "content security is not reachable". What is the problem, and how do you fix it?

A. The connection from GW_B to the internalWebTrends server is not allowed in the Policy.
Fix: Add a rule in GW_A's Policy to allow source WebTrends Server, destination GW_B, service TCP port 18182, and action accept.
B. The connection from GW_B to theWebTrend server is not allowed in the Policy.
Fix: Add a rule in GW_B's Policy with Source GW_B, destination WebTrends server, service TCP port 18182, and action accept.
C. The connection from GW_Ato the WebTrends server is not allowed in the Policy.
Fix: Add a rule in GW_B's Policy with source WebTrends server, destination GW_A, service TCP port 18182, and action accept.
D. The connection from GW_A to the WebTrends server is not allowed in the Policy.
Fix: Add a rule in GW_B's Policy with source GW_A, destination: WebTrends server, service TCP port 18182, and action accept.
E. The connection from GW_A to the WebTrends server is not allowed in the Policy.
Fix: Add a rule in GW_A's Policy to allow source GW_A, destination WebTrends server, service TCP port 18182, and action accept.

Answer: E

QUESTION NO: 36

VPN-1 NGX includes a resource mechanism for working with the Common Internet File System (CIFS). However, this service only provides a limited level of actions for CIFS security. Which of the following services is NOT provided by a CIFS resource?

A. Log access shares
B. Block Remote Registry Access
C. Log mapped shares
D. Allow MS print shares

Answer: D

QUESTION NO: 37

Your organization has many VPN-1 Edge gateways at various branch offices, to allow VPN-1 SecureClient users to access company resources. For security reasons, your organization's Security Policy requires all Internet traffic initiated behind the VPN-1 Edge gateways first be inspected by your headquarters' VPN-1 Pro Security Gateway. How do you configure VPN routing in this star VPN Community?

A. To the Internet and other targets only
B. To the center and other satellites, through the center
C. To the center only
D. To the center; or through the center to other satellites, then to the Internet and other VPN targets

Answer: D

QUESTION NO: 38

Which Check Point QoS feature is used to dynamically allocate relative portions of available bandwidth?

A. Guarantees
B. Differentiated Services
C. Limits
D. Weighted Fair Queuing
E. Low Latency Queuing

Answer: D

QUESTION NO: 39

You are reviewing SmartView Tracker entries, and see a Connection Rejection on a Check Point QoS rule. What causes the Connection Rejection?

A. No QOS rule exists to match the rejected traffic.
B. The number of guaranteed connections is exceeded. The rule's action properties are not set to accept additional connections.
C. The Constant Bit Rate for a Low Latency Class has been exceeded by greater than 10%, and the Maximal Delay is set below requirements.
D. Burst traffic matching the Default Rule is exhausting the Check Point QoS global packet buffers.
E. The guarantee of one of the rule'ssuB. rules exceeds the guarantee in the rule itself.

Answer: B

QUESTION NO: 40

Robert has configured a Common Internet File System (CIFS) resource to allow access to the public partition of his company's file server, on \\erisco\goldenapple\files\public. Robert receives reports that users are unable to access the shared partition, unless they use the file server's IP address. Which of the following is a possible cause?

A. Mapped shares do not allow administrative locks.
B. The CIFS resource is not configured to use Windows name resolution.
C. Access violations are not logged.
D. Remote registry access is blocked.
E. Null CIFS sessions are blocked.

Answer: B

QUESTION NO: 41

In a Load Sharing Unicastmode scenario, the internal-cluster IP address is 10.4.8.3. The internal interfaces on two members are 10.4.8.1 and 10.4.8.2. Internal host 10.4.8.108 Pings 10.4.8.3, and receives replies. The following is the ARP table from the internal Windows host 10.4.8.108: c:> arp According to the output, which member is the Pivot?

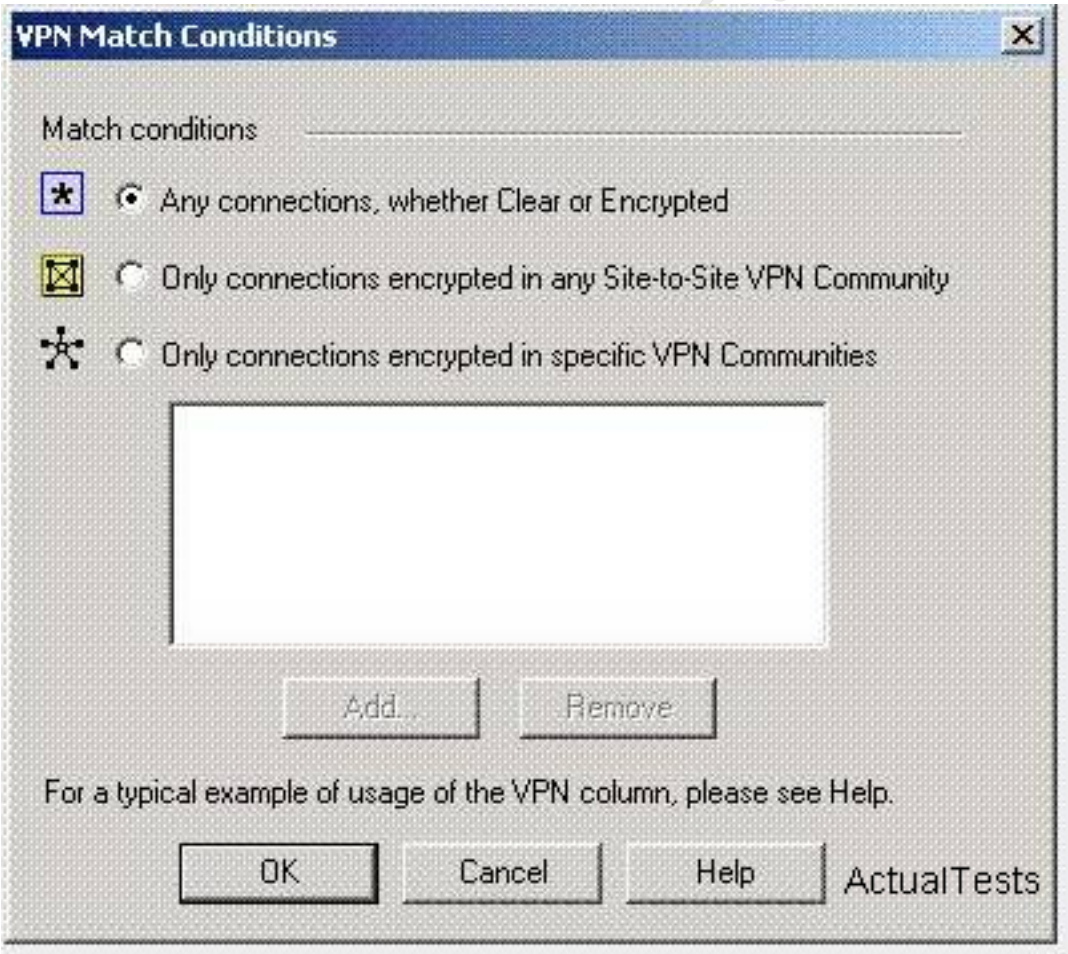
```
C:> arp -

Interface: 10.4.8.108 on Interface 0x4

Internet Address      Physical Address      Type
10.4.8.1              00-b0-d0-b7-b5-d5     dynamic
10.4.8.2              00-01-03-34-e3-9d     dynamic
10.4.8.3              00-01-03-34-e3-9d     dynamic
```

A. 10.4.8.108
B. 10.4.8.3
C. 10.4.8.2
D. 10.4.8.1

Answer: C

QUESTION NO: 42

Steve tries to configure Directional VPN Rule Match in the Rule Base. But the Match column does not have the option to see the Directional Match. Steve sees the following screen. What is the problem?



A. Steve must enabledirectional_match(true) in the objects_5_0.C file on SmartCenter Server.

B. Steve must enable Advanced Routing on each Security Gateway.
C. Steve must enable VPN Directional Match on the VPN Advanced screen, in Global properties.
D. Steve must enable a dynamiC. routing protocol, such as OSPF, on the Gateways.
E. Steve must enable VPN Directional Match on the gateway object's VPN tab.

Answer: C

QUESTION NO: 43

You want to create an IKE VPN between two VPN-1 NGX Security Gateways, to protect two networks. The network behind one Gateway is 10.15.0.0/16, and network 192.168.9.0/24 is behind the peer's Gateway. Which type of address translation should you use, to ensure the two networks access each other through the VPN tunnel?

A. Manual NAT
B. Static NAT
C. Hide NAT
D. None
E. Hide NAT

Answer: D

QUESTION NO: 44

Jennifer wants to protect internal users from malicious Java code, but she does not want to strip Java scripts. Which is the BEST configuration option?

A. Use the URI resource to block Java code
B. Use CVP in the URI resource to block Java code
C. Use the URI resource to strip ActiveX tags
D. Use the URI resource to strip applet tags
E. Use the URI resource to strip script tags

Answer: A

QUESTION NO: 45

Your VPN Community includes three Security Gateways. Each Gateway has its own internal network defined as a VPN Domain. You must test the VPN-1 NGX routE. based VPN feature, without stopping the VPN. What is the correct order of steps?

A. 1. Add a new interface on each Gateway.
2. Remove the newly added network from the current VPN Domain for each Gateway.
3. Create VTIs on each Gateway, to point to the other two peers
4. Enable advanced routing on all three Gateways.
B. 1. Add a hew interface on each Gateway.
2. Remove the newly added network from the current VPN Domain in each gateway object.
3. Create VPN Tunnel Interfaces (VTI) on each gateway object, to point to the other two peers.
4. Add static routes on three Gateways, to route the new network to each peer's VTI interface.
C. 1. Add a new interface on each Gateway.
2. Add the newly added network into the existing VPN Domain for each Gateway.
3. Create VTIs on each gateway object, to point to the other two peers.
4. Enable advanced routing on all three Gateways.
D. 1. Add a new interface on each Gateway.
2. Add the newly added network into the existing VPN Domain for each gateway object.
3. Create VTIs on each gateway object, to point to the other two peers.
4. Add static routes on three Gateways, to route the new networks to each peer's VTI interface.

Answer: B

QUESTION NO: 46

Which Security Server can perform authentication tasks, but CANNOT perform content security tasks?

A. Telnet
B. HTTP
C. rlogin
D. FTP
E. SMTP

Answer: C

QUESTION NO: 47

You are running a VPN-1 NG with Application Intelligence R54 SecurePlatform VPN-1 Pro Gateway. The Gateway also serves as a Policy Server. When you run patch add cd from the NGX CD, what does this command allow you to upgrade?

A. Only VPN-1 Pro Security Gateway
B. Both the operating system (OS) and all Check Point products
C. All products, except the Policy Server

D. Only the patch utility is upgraded using this command
E. Only the OS

Answer: B

QUESTION NO: 48

Which type of service should a Security Administrator use in a Rule Base to control access to specific shared partitions on target machines?

A. Telnet
B. CIFS
C. HTTP
D. FTP
E. URI

Answer: B

QUESTION NO: 49

Assume an intruder has compromised your current IKE Phase 1 and Phase 2 keys. Which of the following options will end the intruder's access, after the next Phase 2 exchange occurs?

A. Phase 3 KeyRevocation
B. Perfect Forward Secrecy
C. MD5 Hash Completion
D. SHA1 Hash Completion
E. DES Key Reset

Answer: B

QUESTION NO: 50

You want only RAS signals to pass through H.323 Gatekeeper and other H.323 protocols, passing directly between end points. Which routing mode in the VoIP Domain Gatekeeper do you select?

A. Direct
B. Direct and Call Setup
C. Call Setup
D. Call Setup and Call Control

Answer: A

QUESTION NO: 51

Your organization has many VPN-1 Edge gateways at various branch offices, to allow VPN-1 SecureClient users to access company resources. For security reasons, your organization's Security Policy requires all Internet traffic initiated behind the VPN-1 Edge gateways first be inspected by your headquarters' VPN-1 Pro Security Gateway. How do you configure VPN routing in this star VPN Community?

A. To the Internet and other targets only
B. To the center and other satellites, through the center
C. To the center only
D. To the center; or through the center to other satellites, then to the Internet and other VPN targets

Answer: D

QUESTION NO: 52

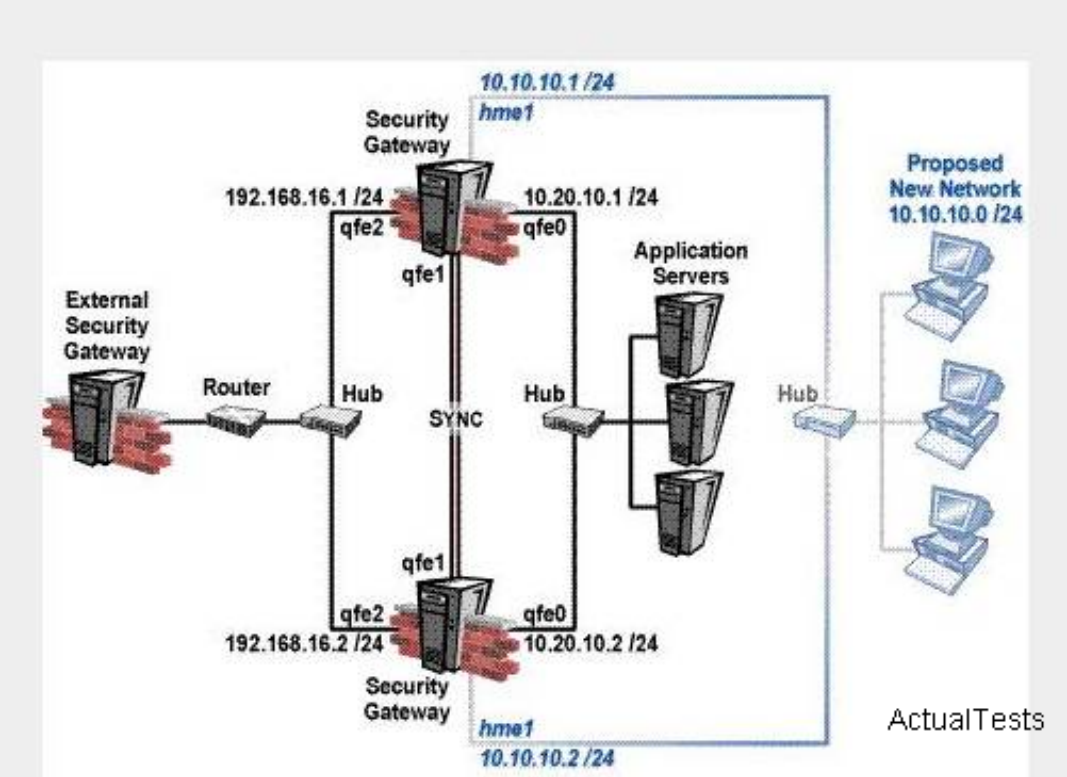
How would you configure a rule in a Security Policy to allow SIP traffic from end point Net_Ato end point Net_B, through an NGX Security Gateway?

A. Net_A/Net_B/sip/accept
B. Net_A/Net_B/sip and sip_any/accept
C. Net_A/Net_B/VolP_any/accept
D. Net_A/Net_BM3lP/accept

Answer: A

QUESTION NO: 53

After you add new interfaces to this cluster, how can you check if the new interfaces and associated virtual IP address are recognized by ClusterXL?



A. By running thecphaprob state command on both members
B. By running the cphaproB. a if command on both members
C. By running the cphaproB. I list command on both members
D. By running the fw ctl iflist command on both members
E. By running thecpconfig command on both members

Answer: B

QUESTION NO: 54

How does ClusterXL Unicast mode handle new traffic?

A. The pivot machine receives and inspects all new packets, and synchronizes the connections with other members.
B. Only the pivot machine receives all packets. It runs an algorithm to determine which member should process the packets.
C. All members receive all packets. The SmartCenter Server decides which member will process the packets. Other members simply drop the packets.
D. All cluster members process all packets, and members synchronize with each other.

Answer: B

QUESTION NO: 55

Barak is a Security Administrator for an organization that has two sites using prE. shared secrets in its VPN. The two sites are Oslo and London. Barak has just been informed that a new office is opening in Madrid, and he must enable all three sites to connect via the VPN to each other. Three Security Gateways are managed by the same SmartCenter Server, behind the Oslo Security Gateway. Barak decides to switch from prE. shared secrets to Certificates issued by the Internal Certificate Authority (ICA). After creating the Madrid gateway object with the proper VPN Domain, what are Barak's remaining steps?

1 .Disable "PrE. Shared Secret" on the London and Oslo gateway objects.
2.Add the Madrid gateway object into the Oslo and London's mesh VPN Community.
3.Manually generate ICA Certificates for all three Security Gateways.
4.Configure "Traditional mode VPN configuration" in the Madrid gateway object's VPN screen.
5.Reinstall the Security Policy on all three Security Gateways.

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

Answer: A

QUESTION NO: 56

Which Check Point QoS feature allows a Security Administrator to define special classes of service for delay-sensitive applications?

A. Weighted Fair Queuing
B. Limits
C. Differentiated Services
D. Low Latency Queuing
E. Guarantees

Answer: D

QUESTION NO: 57

You have an internal FTP server, and you allow downloading, but not uploading. Assume Network Address Translation is set up correctly, and you want to add an inbound rule with: Source: Any Destination: FTP server Service: an FTP resource object.
How do you configure the FTP resource object and the action column in the rule to achieve this goal?

A. Enable only the "Get" method in the FTP Resource Properties, and use this method in the rule, with action accept.
B. Enable only the "Get" method in the FTP Resource Properties and use it in the rule, with action drop.
C. Enable both "Put" and "Get" methods in the FTP Resource Properties and use them in the rule, with action drop.
D. Disable "Get" and "Put" methods in the FTP Resource Properties and use it in the rule, with action accept.
E. Enable only the "Put" method in the FTP Resource Properties and use it in the rule, with action accept.

Answer: A

QUESTION NO: 58

You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use three machines with the following configurations:Are these machines correctly configured for a ClusterXL deployment?

A. Yes, these machines are configured correctly for aClusterXL deployment.
B. No,QuadCards are not supported with ClusterXL.
C. No, all machines in a cluster must be running on the same OS.
D. No, a cluster must have an even number of machines.
E. No,ClusterXL is not supported on Red Hat Linux.

Answer: C

QUESTION NO: 59

Damon enables an SMTP resource for content protection. He notices that mail seems to slow down on occasion, sometimes being delivered late. Which of the following might improve throughput performance?

A. Configuring the SMTP resource to bypass the CVP resource
B. Increasing the Maximum number of mail messages in the Gateway's spool directory
C. Configuring the Content Vector Protocol (CVP) resource to forward the mail to the internal SMTP server, without waiting for a response from the Security Gateway
D. Configuring the CVP resource to return the mail to the Gateway
E. Configuring the SMTP resource to only allow mail with Damon's company's domain name in the header

Answer: C

QUESTION NO: 60

You configure a Check Point QoS Rule Base with two rules: an HTTP rule with a weight of 40, and the Default Rule with a weight of 10. If the only traffic passing through your QoS Module is HTTP traffic, what percent of bandwidth will be allocated to the HTTP traffic?

A. 10%
B. 100%
C. 40%
D. 80%
E. 50%

Answer: B

QUESTION NO: 61

You configure a Check Point QoS Rule Base with two rules: an HTTP rule with a weight of 40, and the Default Rule with a weight of 10. If the only traffic passing through your QoS Module is HTTP traffic, what percent of bandwidth will be allocated to the HTTP traffic?

A. 10%
B. 100%
C. 40%
D. 80%
E. 50%

Answer: B

QUESTION NO: 62

Which of the following actions is most likely to improve the performance of Check Point QoS?

A. Turn "per rule guarantees" into "per connection guarantees".
B. Install CheckpointQoS only on the external interfaces of the QoS Module.
C. Put the most frequently used rules at the bottom of the QoS Rule Base.
D. Turn "per rule limits" into "per connection limits".
E. Define weights in the Default Rule in multiples of 10.

Answer: B

QUESTION NO: 63

Robert has configured a Common Internet File System (CIFS) resource to allow access to the public partition of his company's file server, on \\erisco\goldenapple\files\public. Robert receives reports that users are unable to access the shared partition, unless they use the file server's IP address. Which of the following is a possible cause?

A. Mapped shares do not allow administrative locks.
B. The CIFS resource is not configured to use Windows name resolution.
C. Access violations are not logged.
D. Remote registry access is blocked.
E. Null CIFS sessions are blocked.

Answer: B

QUESTION NO: 64

What is the consequence of clearing the "Log VoIP Connection" box in Global Properties?

A. Dropped VoIP traffic is logged, but accepted VoIP traffic is not logged.
B. VoIP protocol-specific log fields are not included inSmartView Tracker entries.
C. The log field setting in rules for VoIP protocols are ignored.
D. IP addresses are used, instead of object names, in log entries that reference VoIP Domain objects.
E. The SmartCenter Server stops importing logs from VoIP servers.

Answer: B

QUESTION NO: 65

Your VPN Community includes three Security Gateways. Each Gateway has its own internal network defined as a VPN Domain. You must test the VPN-1 NGX routE. based VPN feature, without stopping the VPN. What is the correct order of steps?

A. 1. Add a new interface on each Gateway.
2. Remove the newly added network from the current VPN Domain for each Gateway.
3. Create VTIs on each Gateway, to point to the other two peers
4. Enable advanced routing on all three Gateways.
B. 1. Add a hew interface on each Gateway.
2. Remove the newly added network from the current VPN Domain in each gateway object.
3. Create VPN Tunnel Interfaces (VTI) on each gateway object, to point to the other two peers.
4. Add static routes on three Gateways, to route the new network to each peer's VTI interface.
C. 1. Add a new interface on each Gateway.
2. Add the newly added network into the existing VPN Domain for each Gateway.
3. Create VTIs on each gateway object, to point to the other two peers.
4. Enable advanced routing on all three Gateways.
D. 1. Add a new interface on each Gateway.
2. Add the newly added network into the existing VPN Domain for each gateway object.
3. Create VTIs on each gateway object, to point to the other two peers.
4. Add static routes on three Gateways, to route the new networks to each peer's VTI interface.

Answer: B

QUESTION NO: 66

VPN-1 NGX includes a resource mechanism for working with the Common Internet File System (CIFS). However, this service only provides a limited level of actions for CIFS security. Which of the following services is provided by a CIFS resource?

A. Allow Unixfile sharing.
B. Allow MS print shares
C. Logging Mapped Shares
D. Access Violation logging.

Answer: C

QUESTION NO: 67

Your company has two headquarters, one in London, one in New York. Each headquarters includes several branch offices. The branch offices only need to communicate with the headquarters in their country, not with each other, and only the headquarters need to communicate directly. What is the BEST configuration for VPN Communities among the branch

offices and their headquarters, and between the two headquarters? VPN Communities comprised of:

A. two star and one mesh Community; each star Community is set up for each site, with headquarters as the center of the Community, and branches as satellites. The mesh Communities are between the New York and London headquarters
B. three mesh Communities: one for London headquarters and its branches, one for New York headquarters and its branches, and one for London and New York headquarters.
C. twomesh Communities, one for each headquarters and their branch offices; and one star Community, in which London is the center of the Community and New York is the satellite.
D. twomesh Communities, one for each headquarters and their branch offices; and one star Community, where New York is the center of the Community and London is the satellite.

Answer: A

QUESTION NO: 68

You are preparing to configure your VoIP Domain Gatekeeper object. Which two other objects should you have created first?

A. An object to represent the IP phone network, AND an object to represent the host on which the proxy is installed
B. An object to represent the PSTN phone network, AND an object to represent the IP phone network
C. An object to represent the IP phone network, AND an object to represent the host on which the gatekeeper is installed
D. An object to represent the Q.931 service origination host, AND an object to represent the H.245 termination host
E. An object to represent the call manager, AND an object to represent the host on which the transmission router is installed

Answer: C

QUESTION NO: 69

Yoav is a Security Administrator preparing to implement a VPN solution for his multi-site organization. To comply with industry regulations, Yoav's VPN solution must meet the following requirements:

Portability: Standard
Key management: Automatic, external PKI
Session keys: Changed at configured times during a connection's lifetime

Key length: No less than 128-bit
Data integrity: Secure against inversion and brutE. force attacks

What is the most appropriate setting Yoav should choose?

A. IKE VPNs: AES encryption for IKE Phase 1, and DES encryption for Phase 2; SHA1 hash
B. IKE VPNs: SHA1 encryption for IKE Phase 1, and MD5 encryption for Phase 2; AES hash
C. IKE VPNs: CAST encryption for IKE Phase 1, and SHA1 encryption for Phase 2; DES hash
D. IKE VPNs: AES encryption for IKE Phase 1, and AES encryption for Phase 2; SHA1 hash
E. IKE VPNs: DES encryption for IKE Phase 1, and 3DES encryption for Phase 2; MD5 hash

Answer: D

QUESTION NO: 70

Assume an intruder has compromised your current IKE Phase 1 and Phase 2 keys. Which of the following options will end the intruder's access, after the next Phase 2 exchange occurs?

A. Phase 3 KeyRevocation
B. Perfect Forward Secrecy
C. MD5 Hash Completion
D. SHA1 Hash Completion
E. DES Key Reset

Answer: B

QUESTION NO: 71

Which of the following commands shows full synchronization status?

A. cphaproB. i list
B. cphastop
C. fw ctl pstat
D. cphaproB. a if
E. fwhastat

Answer: A

QUESTION NO: 72

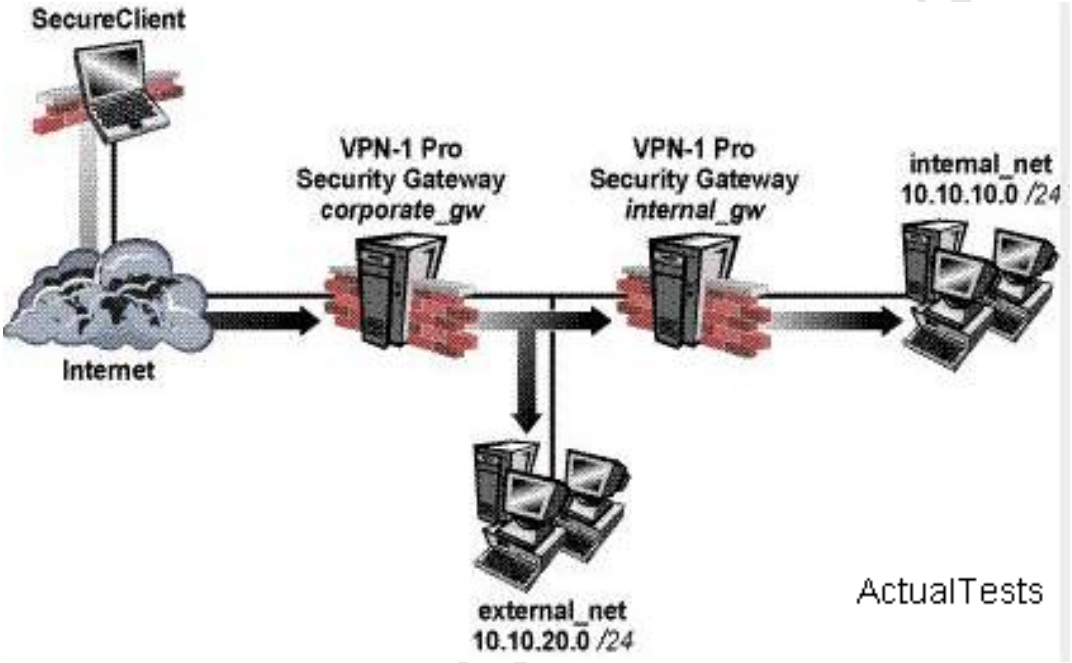
In a distributed VPN-1 Pro NGX environment, where is the Internal Certificate Authority (ICA) installed?

A. On the Security Gateway
B. Certificate Manager Server
C. On the Policy Server
D. On the Smart View Monitor
E. On the primarySmattCenter Server

Answer: E

QUESTION NO: 73

The following diagram illustrates how a VPN-1 SecureClient user tries to establish a VPN with hosts in the external_net and internal_net from the Internet. How is the Security Gateway VPN Domain created?



A. Internal Gateway VPN Domain = internal_net;
External VPN Domain = external net + external gateway object + internal_net.
B. Internal Gateway VPN Domain = internal_net.
External Gateway VPN Domain = external_net + internal gateway object
C. Internal Gateway VPN Domain = internal_net;
External Gateway VPN Domain = internal_net + external_net
D. Internal Gateway VPN Domain = internal_net.
External Gateway VPN Domain = internal VPN Domain + internal gateway object + external_net

Answer: D

QUESTION NO: 74

You must set up SIP with a proxy for your network. IP phones are in the 172.16.100.0 network. The Registrar and proxy are installed on host 172.16.100.100. To allow handover enforcement for outbound calls from SIP-net to network Net_B on the Internet, you have defined the following objects:

Network object: SIP-net: 172.16.100.0/24
SIP-gateway: 172.16.100.100
VoIP Domain object: VolP_domain_A
1 .EnD. point domain: SIP-net
2.VoIP gateway installed at: SIP-gateway host object

How would you configure the rule?

A. SIP- G ateway/N et_B/s i p_a ny/a c c e pt
B. VolP_domain_A/Net_B/sip/accept
C. SIP-Gateway/Net_B/sip/accept
D. VolP_domain_A/Net_B/sip_any, and sip/accept
E. VolP_Gateway_MJet_B/sip_any/accept

Answer: B

QUESTION NO: 75

What is the behavior of ClusterXL in a High Availability environment?

A. Both members respond to the virtual IP address, and both members pass traffic when using their physical addresses.
B. Both members respond to the virtual IP address, but only the active member is able to pass traffic.
C. The active member responds to the virtual IP address.nd both members pass traffic when using their physical addresses.
D. The active member responds to the virtual IP address.nd is the only member that passes traffic
E. The passive member responds to the virtual IP address, and both members route traffic when using their physical addresses.

Answer: D

QUESTION NO: 76

Which Check Point QoS feature marks the Type of Service (ToS) byte in the IP header?

A. Guarantees
B. Low Latency Queuing
C. Differentiated Services
D. Weighted Fair Queuing
E. Limits

Answer: C

QUESTION NO: 77

You plan to incorporate OPSEC servers, such as Websense and Trend Micro, to do content filtering. Which segment is the BEST location for these OPSEC servers, when you consider Security Server performance and data security?

A. On the Security Gateway
B. Internal network, where users are located
C. On the Internet
D. DMZ network, where application servers are located
E. Dedicated segment of the network

Answer: E

QUESTION NO: 78

How can you completely tear down a specific VPN tunnel in an intranet IKE VPN deployment?

A. Run the commandvpn tu on the Security Gateway, and choose the option "Delete all IPSec+IKE SAs for ALL peers and users".
B. Run the commandvpn tu on the SmartCenter Server, and choose the option "Delete all IPSec+IKE SAs for ALL peers and users".
C. Run the command vpn tu on the Security Gateway, and choose the option "Delete all IPSec+IKE SAs for a given peer (GW)".
D. Run the command vpn tu on the Security Gateway, and choose the option "Delete all IPSec SAs for a given user (Client)".
E. Run the commandvpn tu on the Security Gateway, and choose the option "Delete all IPSec SAs for ALL peers and users".

Answer: C

QUESTION NO: 79

The following rule contains an FTP resource object in the Service field:

Source: local_net
Destination: Any
Service: FTP-resource object
Action: Accept

How do you define the FTP Resource Properties > Match tab to prevent internal users from receiving corporate files from external FTP servers, while allowing users to send files?

A. Enable "Put" and "Get" methods.
B. Disable the "Put" method globally.
C. Enable the "Put" method only on the Match tab.
D. Enable the "Get" method on the Match tab.
E. Disable "Get" and "Put" methods on the Match tab.

Answer: C

QUESTION NO: 80

The following rule contains an FTP resource object in the Service field:
Source: local_net Destination: Any Service: FTP-resource object Action: Accept

How do you define the FTP Resource Properties > Match tab to prevent internal users from sending corporate files to external FTP servers, while allowing users to retrieve files?

A. Enable the "Get" method on the match tab
B. Disable "Get" and "Put" methods on the Match tab.
C. Enable the "Put" and "Get" methods.
D. Enable the "Put" method only on the match tab.
E. Disable the "Put" method globally.

Answer: A

QUESTION NO: 81

You have an internal FTP server, and you allow uploading, but not downloading. Assume Network Address Translation (NAT) is set up correctly and you want to add an inbound rule with:

Source: Any
Destination: FTP server
Service: an FTP resource object.

How do you configure the FTP resource object and the action column in the rule to achieve this goal?

A. Disable "Get" and "Put" methods in the FTP Resource Properties and use them in the rule, with action accept.
B. Enable both "Put" and "Get" methods in the FTP Resource Properties and use them in the rule, with action drop.
C. Enable only the "Get" method in the FTP Resource Properties and use this method in the rule, with action accept.
D. Enable only the "Put" method in the FTP Resource Properties and use this method in the rule, with action drop.
E. Enable only "Put" method in the FTP Resource Properties and use this method in the rule, with action accept.

Answer: E

QUESTION NO: 82

In a distributed VPN-1 Pro NGX environment, where is the Internal Certificate Authority (ICA) installed?

A. On the Security Gateway
B. Certificate Manager Server
C. On the Policy Server
D. On the Smart View Monitor
E. On the primarySmattCenter Server

Answer: E

QUESTION NO: 83

VPN-1 NGX supports VoIP traffic in all of the following environments, EXCEPT which environment?

A. H.323
B. SIP
C. MEGACO
D. SCCP
E. MGCP

Answer: C

QUESTION NO: 84

Where can a Security Administrator adjust the unit of measurement (bps, Kbps or Bps), for Check Point QoS bandwidth?

A. Global Properties
B. QoS Class objects
C. Check Point gateway object properties
D. $CPDIR/conf/qos_props.pf
E. Advanced Action options in eachQoS rule

Answer: A

QUESTION NO: 85

Cody is notified by blacklist.org that his site has been reported as a spam relay, due to his SMTP Server being unprotected. Cody decides to implement an SMTP Security Server, to prevent the server from being a spam relay. Which of the following is the most efficient configuration method?

A. Configure the SMTP Security Server to perform MX resolving.
B. Configure the SMTP Security Server to perform filtering, based on IP address and SMTP protocols.
C. Configure the SMTP Security Server to work with an OPSEC based product, for content checking.
D. Configure the SMTP Security Server to apply a generic "from" address to all outgoing mail.
E. Configure the SMTP Security Server to allow only mail to or from names, within Cody's corporate domain.

Answer: E

QUESTION NO: 86

You want to upgrade a SecurePlatform NG with Application Intelligence (Al) R55 Gateway to SecurePlatform NGX R60 via SmartUpdate. Which package is needed in the repository before upgrading?

A. SVN Foundation and VPN-1 Express/Pro
B. VPN-1 and Firewall-1
C. SecurePlatform NGX R60
D. SVN Foundation 3 E. VPN-1 Pro/Express NGXR60

Answer: C

QUESTION NO: 87

You configure a Check Point QoS Rule Base with two rules: an H.323 rule with a weight of 10, and the Default Rule with a weight of 10. The H.323 rule includes a per-connection guarantee of 384 Kbps, and a per-connection limit of 512 Kbps. The per-connection guarantee is for four connections, and no additional connections are allowed in the Action properties. If traffic passing through the QoS Module matches both rules, which of the following statements is true?

A. Neither rule will be allocated more than 10% of available bandwidth.
B. The H.323 rule will consume no more than 2048 Kbps of available bandwidth.
C. 50% of available bandwidth will be allocated to the H.323 rule.
D. 50% of available bandwidth will be allocated to the Default Rule.
E. Each H.323 connection will receive at least 512 Kbps of bandwidth.

Answer: B

QUESTION NO: 88

Your current stanD. alone VPN-1 NG with Application Intelligence (Al) R55 installation is running on SecurePlatform. You plan to implement VPN-1 NGX in a distributed environment, where the existing machine will be the VPN-1 Pro Gateway. An additional machine will serve as the SmartCenter Server. The new machine runs on a Windows Server 2003. You need to upgrade the NG with Al R55 SmartCenter Server configuration to VPN-1 NGX.
How do you upgrade to VPN-1 NGX?

A. Insert the NGX CD in the existingNGwithAI R55 SecurePlatform machine, and answer yes to backup the configuration. Copy the backup file to the Windows Server 2003. Continue the upgrade process. Reboot after upgrade is finished. After SecurePlatform NGX reboots, run sysconfig, select VPN-1 Pro Gateway, and finish the sysconfig process. Reboot again. Use the NGX CD to install the primary SmartCenter on the Windows Server 2003. Import the backup file.
B. Run the backup command in the existingSecurePlatform machine, to create a backup file. Copy the file to the Windows Server 2003. Uninstall all Check Point products on SecurePlatform by running rpm CPsuitE. R55 command. Reboot. Install new VPN-1 NGX on the existing SecurePlatform machine. Run sysconfig, select VPN-1 Pro Gateway, and reboot. Use VPN-1 NGX CD to install primary SmartCenter Server on the Windows Server 2003. Import the backup file.
C. Copy the $FWDIR\conf and $FWDIR\lib files from the existing SecurePlatform machine. Create a tar.gzfile, and copy it to the Windows Server 2003. Use VPN-1 NGX CD on the existing SecurePlatform machine to do a new installation. Reboot. Run sysconfig and select VPN-1 Pro Gateway. Reboot. Use the NGX CD to install the primary SmartCenter Server on the Windows Server 2003. On the Windows Server 2003, run upgradejmport command to import $FWDIR\conf

and $FWDIR\lib from the SecurePlatform machine.
D. Run backup command on the existing SecurePlatform machine to create a backup file. Copy the file to the Windows Server 2003. Uninstall the primary SmartCenter Server package from NG with Al R55 SecurePlatform using sysconfig. Reboot. Install the NGX primary SmartCenter Server and import the backup file. Open the NGX SmartUpdate, and select "upgrade all packages" on the NG with Al R55 Security Gateway.

Answer: A

QUESTION NO: 89

If you check the box "Use Aggressive Mode", in the IKE Properties dialog box:

A. The standardthreE. packet IKE Phase 1 exchange is replaced by a six-packet exchange.
B. The standard six-packet IKE Phase 2 exchange is replaced by athreE. packet exchange.
C. The standard threE. packet IKE Phase 2 exchange is replaced by a six-packet exchange.
D. The standard six-packet IKE Phase 1 exchange is replaced by a threE. packet exchange.
E. The standard six-packet IKE Phase 1 exchange is replaced by atwelvE. packet exchange.

Answer: D

QUESTION NO: 90

DShield is a Check Point feature used to block which of the following threats?

A. Cross Site Scripting
B. SQL injection
C. DDOS
D. Buffer overflows
E. Trojan horses

Answer: C

QUESTION NO: 91

You must set up SIP with a proxy for your network. IP phones are in the 172.16.100.0 network. The Registrar and proxy are installed on host 172.16.100.100. To allow handover enforcement for outbound calls from SIP-net to network Net_B on the Internet, you have defined the following objects:

Network object: SIP-net: 172.16.100.0/24
SIP-gateway: 172.16.100.100

VoIP Domain object: VolP_domain_A
1 .EnD. point domain: SIP-net
2.VoIP gateway installed at: SIP-gateway host object

How would you configure the rule?

A. SIP-Gateway/Net_B/sip/accept
B. VolP_Gateway_MJet_B/sip/accept
C. SIP-Gateway/Net_B/sip_any/accept
D. VolP_domain_A/Net_B/sip_any, and sip/accept
E. VolP_domain A/Net_B/sip_any/accept

Answer: E

QUESTION NO: 92

Which of the following commands shows full synchronization status?

A. cphaproB. i list
B. cphastop
C. fw ctl pstat
D. cphaproB. a if
E. fwhastat

Answer: A

QUESTION NO: 93

How do you control the maximum mail messages in a spool directory?

A. In the Security Server window in Global Properties
B. In SmartDefense SMTP settings
C. In the smtp.conf file on the SmartCenter Server
D. In the gateway object's SMTP settings in the Advanced window
E. In the SMTP resource object

Answer: D

QUESTION NO: 94

Your company has two headquarters, one in London, one in New York. Each headquarters includes several branch offices. The branch offices ONLY need to communicate with the

headquarters in their country, not with each other, and only the headquarters need to communicate directly. Which configuration meets the criteria? VPN Communities comprised of:

A. three mesh Communities: one forLondon headquarters and its branches, one for New York headquarters and its branches, and one for London and New York headquarters.
B. three star Communities: first betweenNew York headquarters and its branches, the second between London headquarters and its branches, the third between New York and London headquarters.
C. twomesh and one star Community; each mesh Community is set up for each site, with mesh Communities between their branches. The star Community has New York as the headquarters and London as its satellite.
D. twomesh Communities for each headquarters and their branch offices; and one star Community, in which London is the center of the Community and New York is the satellite.

Answer: B

QUESTION NO: 95

Greg is creating rules and objects to control VoIP traffic in his organization, through a VPN-1 NGX Security Gateway. Greg creates VoIP Domain SIP objects to represent each of his organization's three SIP gateways. Greg then creates a simple group to contain the VoIP Domain SIP objects. When Greg attempts to add the VoIP Domain SIP objects to the group, they are not listed. What is the problem?

A. The relatedenD. points domain specifies an address range.
B. VoIP Domain SIP objects cannot be placed in simple groups.
C. The installed VoIP gateways specify host objects.
D. The VoIP gateway object must be added to the group, before the VoIP Domain SIP object is eligible to be added to the group.
E. The VoIP Domain SIP object's name contains restricted characters.

Answer: B

QUESTION NO: 96

You plan to install a VPN-1 Pro Gateway for VPN-1 NGX at your company's headquarters. You have a single Sun SPARC Solaris 9 machine for VPN-1 Pro enterprise implementation. You need this machine to inspect traffic and keep configuration files. Which Check Point software package do you install?

A. VPN-1 Pro Gateway and primarySmartCenter Server

B. Policy Server and primary SmartCenter Server
C. ClusterXL and SmartCenter Server
D. VPN-1 Pro Gateway
E. SmartCenter Server

Answer: A

QUESTION NO: 97

```
Cluster Mode:New High Availability (Active Up)

Number        Unique IP Address     Assigned Load     State
1 (local)     192.168.1.1           0%                down
2             192.168.1.2           100%              active
```

The following is cphaprob state command output from a New Mode High Availability cluster memberWhich machine has the highest priority?

A. 192.168.1.2, since its number is 2
B. 192.168.1.1, because its number is 1
C. This output does not indicate which machine has the highest priority.
D. 192.168.1.2, because its state is active

Answer: B

QUESTION NO: 98

You are preparing to configure your VoIP Domain Gatekeeper object. Which two other objects should you have created first?

A. An object to represent the IP phone network, AND an object to represent the host on which the proxy is installed
B. An object to represent the PSTN phone network, AND an object to represent the IP phone network
C. An object to represent the IP phone network, AND an object to represent the host on which the gatekeeper is installed
D. An object to represent the Q.931 service origination host, AND an object to represent the H.245 termination host
E. An object to represent the call manager, AND an object to represent the host on which the transmission router is installed

Answer: C

QUESTION NO: 99

How would you configure a rule in a Security Policy to allow SIP traffic from end point Net_Ato end point Net_B, through an NGX Security Gateway?

A. Net_A/Net_EWolP_any/accept
B. Net_A/Net_B/sip and sip_any/accept
C. Net_A/Net_EWolP/accept
D. Net_A/Net_B/sip_any/accept

Answer: D

QUESTION NO: 100

You want VPN traffic to match packets from internal interfaces. You also want the traffic to exit the Security Gateway, bound for all sitE. to-site VPN Communities, including Remote Access Communities. How should you configure the VPN match rule?

A. internal_clear > AII_GwToGw
B. Communities > Communities
C. lnternal_clear > External_Clear
D. lnternal_clear > Communities
E. internal clear>All communities

Answer: E

QUESTION NO: 101

Which service type does NOT invoke a Security Server?

A. HTTP
B. FTP
C. Telnet
D. CIFS
E. SMTP

Answer: D

QUESTION NO: 102

When Load Sharing Multicast mode is defined in a ClusterXL cluster object, how are packets being handled by cluster members?

A. All cluster members process all packets, and members synchronize with each other.
B. All members receive all packets. TheSmartCenter Server decides which member will process the packets. Other members simply drop the packets.
C. Only one member at a time is active. The active cluster member processes all packets.
D. All members receive all packets. An algorithm determines which member processes packets, and which member drops packets.

Answer: D

QUESTION NO: 103

Your current VPN-1 NG with Application Intelligence (Al) R55 stanD. alone VPN-1 Pro Gateway and SmartCenter Server run on SecurePlatform. You plan to implement VPN-1 NGX in a distributed environment, where the existing machine will be the SmartCenter Server, and a new machine will be the VPN-1 Pro Gateway only. You need to migrate the NG with Al R55 SmartCenter Server configuration, including such items as Internal Certificate Authority files, databases, and Security Policies.

How do you request a new license for this VPN-1 NGX upgrade?

A. Request a VPN-1 NGXSmartCenter Server license, using the new machine's IP address. Request a new local license forthe NGX VPN-1 Pro Gateway.
B. Request a VPN-1 NGXSmartCenter Server license, using the new machine's IP address. Request a new central license forthe NGX VPN-1 Pro Gateway.
C. Request a new VPN-1 NGX SmartCenter Server license, using the NG with Al SmartCenter Server IP address. Request a new central license for the NGX VPN-1 Pro Gateway.
D. Request a VPN-1 NGX SmartCenter Server license, using the NG with Al SmartCenter Server IP address. Request a new central license forthe NGX VPN-1 Pro Gateway, licensed forthe existing SmartCenter Server IP address.

Answer: D

QUESTION NO: 104

Yoav is a Security Administrator preparing to implement a VPN solution for his multi-site organization. To comply with industry regulations, Yoav's VPN solution must meet the following requirements:

Portability: Standard
Key management: Automatic, external PKI
Session keys: Changed at configured times during a connection's lifetime
Key length: No less than 128-bit

Data integrity: Secure against inversion and brutE. force attacks

What is the most appropriate setting Yoav should choose?

A. IKE VPNs: AES encryption for IKE Phase 1, and DES encryption for Phase 2; SHA1 hash
B. IKE VPNs: SHA1 encryption for IKE Phase 1, and MD5 encryption for Phase 2; AES hash
C. IKE VPNs: CAST encryption for IKE Phase 1, and SHA1 encryption for Phase 2; DES hash
D. IKE VPNs: AES encryption for IKE Phase 1, and AES encryption for Phase 2; SHA1 hash
E. IKE VPNs: DES encryption for IKE Phase 1, and 3DES encryption for Phase 2; MD5 hash

Answer: D

QUESTION NO: 105

Jerry is concerned that a denial-oF. service (DoS) attack may affect his VPN Communities. He decides to implement IKE DoS protection. Jerry needs to minimize the performance impact of implementing this new protection. Which of the following configurations is MOST appropriate for Jerry?

A. Set Support IKEDoS protection from identified source to "Puzzles", and Support IKE DoS protection from unidentified source to "Stateless".
B. Set Support IKE Dos Protection from identified source, and Support IKEDoS protection from unidentified source to "Puzzles".
C. Set Support IKE DoS protection from identified source to "Stateless," and Support IKE DoS protection from unidentified source to "Puzzles".
D. Set "Support IKE DoS protection" from identified source, and "Support IKE DoS protection" from unidentified source to "Stateless".
E. Set Support IKEDoS protection from identified source to "Stateless", and Support IKE DoS protection from unidentified source to "None".

Answer: D

QUESTION NO: 106

What is a requirement for setting up Management High Availability?

A. AllSmartCenter Servers must reside in the same Local Area Network (LAN).
B. AllSmartCenter Servers must have the same amount of memory.
C. You can only have one Secondary SmartCenter Server.
D. All SmartCenter Servers must have the BIOS release.
E. AllSmartCenter Servers must have the same operating system.

Answer: E

QUESTION NO: 107

What is the consequence of clearing the "Log VoIP Connection" box in Global Properties?

A. Dropped VoIP traffic is logged, but accepted VoIP traffic is not logged.
B. VoIP protocol-specific log fields are not included inSmartView Tracker entries.
C. The log field setting in rules for VoIP protocols are ignored.
D. IP addresses are used, instead of object names, in log entries that reference VoIP Domain objects.
E. The SmartCenter Server stops importing logs from VoIP servers.

Answer: B

QUESTION NO: 108

Which of the following TCP port numbers is used to connect the VPN-1 Gateway to the Content Vector Protocol (CVP) server?

A. 18182
B. 18180
C. 18181
D. 17242
E. 1456

Answer: C

QUESTION NO: 109

Which operating system is NOT supported by VPN-1 SecureClient?

A. IPSO 3.9
B. Windows XP SP2
C. Windows 2000 Professional
D. RedHat Linux 8.0
E. MacOSX

Answer: A

QUESTION NO: 110

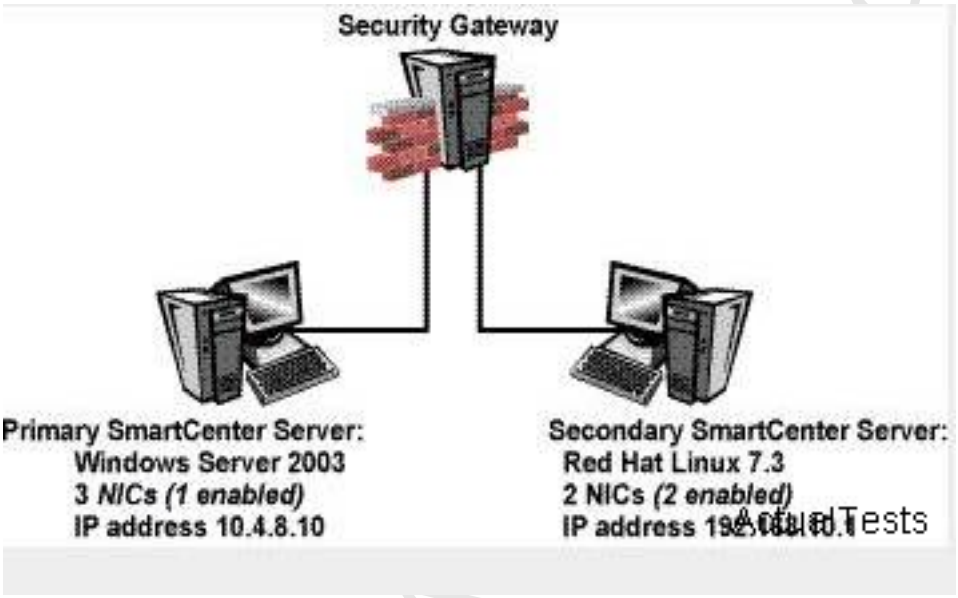
If you check the box "Use Aggressive Mode", in the IKE Properties dialog box:

A. The standardthreE. packet IKE Phase 1 exchange is replaced by a six-packet exchange.
B. The standard six-packet IKE Phase 2 exchange is replaced by athreE. packet exchange.
C. The standard threE. packet IKE Phase 2 exchange is replaced by a six-packet exchange.
D. The standard six-packet IKE Phase 1 exchange is replaced by a threE. packet exchange.
E. The standard six-packet IKE Phase 1 exchange is replaced by atwelvE. packet exchange.

Answer: D

QUESTION NO: 111

The following configuration is for VPN-1 NGX:Is this configuration correct for Management High Availability (HA)?



A. No, theSmartCenter Servers must be installed on the same operating system.
B. No, a VPN-1 NGXSmartCenter Server cannot run on Red Hat Linux 7.3.
C. No, the SmartCenter Servers must reside on the same network.
D. No, A VPN-1 NGX SmartCenter Server can only be in a Management HA configuration, if the operating system is Solaris.
E. No, theSmartCenter Servers do not have the same number of NICs.

Answer: A

QUESTION NO: 112

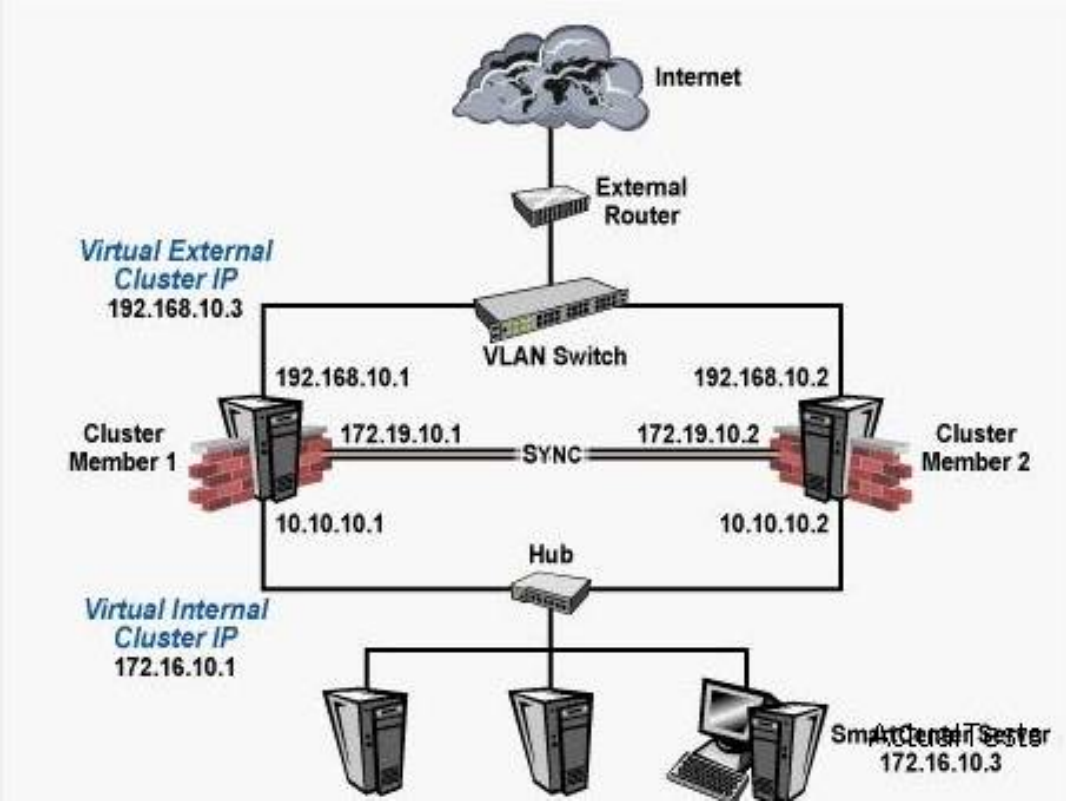
Which operating system is NOT supported by VPN-1 SecureClient?

A. IPSO 3.9
B. Windows XP SP2
C. Windows 2000 Professional
D. RedHat Linux 8.0
E. MacOSX

Answer: A

QUESTION NO: 113

You are preparing a lab for a ClusterXL environment, with the following topology:
Vip internal cluster IP = 172.16.10.1; Vip external cluster IP = 192.168.10.3
Cluster Member 1: four NICs, three enabled: qfeO: 192.168.10.1/24, qfel: 10.10.10.1/24, qfe2: 172.16.10.1/24
Cluster Member 2: five NICs, three enabled; hmeO: 192.168.10.2/24, ethi: 10.10.10.2/24, eth2: 172.16.10.2/24
Member Network tab on internal-cluster interface: is 10.10.10.0, 255.255.255.0
SmartCenter Pro Server: 172.16.10.3
External interfaces 192.168.10.1 and 192.168.10.2 connect to a Virtual Local Area Network (VLAN) switch. The upstream router connects to the same VLAN switch. Internal interfaces 10.10.10.1 and 10.10.10.2 connect to a hub. There is no other machine in the 10.10.10.0 network. 172.19.10.0 is the synchronization network. What is the problem with this configuration?



A. The SmartCenter Pro Server cannot be in the synchronization network.

B. There is no problem with this configuration. It is correct.
C. Members do not have the same number of NICs.
D. The internal network does not have a third cluster member.
E. Cluster members cannot use the VLAN switch. They must use hubs.

Answer: B

QUESTION NO: 114

Which VPN Community object is used to configure VPN routing within the SmartDashboard?

A. Star
B. Mesh
C. Remote Access
D. Map

Answer: A

QUESTION NO: 115

You have a production implementation of Management High Availability, at version VPN-1 NG with Application Intelligence R55. You must upgrade your two SmartCenter Servers to VPN-1 NGX. What is the correct procedure?

A. 1. Synchronize the twoSmartCenter Servers.
2. Upgrade the secondary SmartCenter Server.
3. Upgrade the primary SmartCenter Server.
4. Configure both SmartCenter Server host objects version to VPN-1 NGX.
5. Synchronize the Servers again.
B. 1. Synchronize the two SmartCenter Servers.
2. Perform an advanced upgrade on the primary SmartCenter Server.
3. Upgrade the secondary SmartCenter Server.
4. Configure both SmartCenter Server host objects to version VPN-1 NGX.
5. Synchronize the Servers again.
C. 1. Perform an advanced upgrade on the primary SmartCenter Server.
2. Configure the primary SmartCenter Server host object to version VPN-1 NGX.
3. Synchronize the primary with the secondary SmartCenter Server.
4. Upgrade the secondary SmartCenter Server.
5. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
6. Synchronize the Servers again.
D. 1. Synchronize the two SmartCenter Servers.
2. Perform an advanced upgrade on the primary SmartCenter Server.

3. Configure the primary SmartCenter Server host object to version VPN-1 NGX.
4. Synchronize the two Servers again.
5. Upgrade the secondary SmartCenter Server.
6. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
7. Synchronize the Servers again.

Answer: B

QUESTION NO: 116

Cody is notified by blacklist.org that his site has been reported as a spam relay, due to his SMTP Server being unprotected. Cody decides to implement an SMTP Security Server, to prevent the server from being a spam relay. Which of the following is the most efficient configuration method?

A. Configure the SMTP Security Server to perform MX resolving.
B. Configure the SMTP Security Server to perform filtering, based on IP address and SMTP protocols.
C. Configure the SMTP Security Server to work with an OPSEC based product, for content checking.
D. Configure the SMTP Security Server to apply a generic "from" address to all outgoing mail.
E. Configure the SMTP Security Server to allow only mail to or from names, within Cody's corporate domain

Answer: E

QUESTION NO: 117

You want to upgrade a cluster with two members to VPN-1 NGX. The SmartCenter Server and both members are version VPN-1/Firewall-1 NG FP3, with the latest Hotfix. What is the correct upgrade procedure?

1. Change the version, in the General Properties of the gateway-cluster object.
2. Upgrade the SmartCenter Server, and reboot after upgrade.
3. Run cpstop on one member, while leaving the other member running. Upgrade one member at a time, and reboot after upgrade.
4. Reinstall the Security Policy.

A. 3,2, 1,4
B. 2,4,3, 1
C. 1,3,2,4
D. 2,3, 1,4

E. 1,2,3,4

Answer: D

QUESTION NO: 118

By default, a standby SmartCenter Server is automatically synchronized by an active SmartCenter Server, when:

A. The Security Policy is installed.
B. The Security Policy is saved.
C. The user database is installed.
D. The Security Administrator logs in to the standby SmartCenter Server, for the first time.
E. The standbySmartCenter Server starts for the first time.

Answer: A

QUESTION NO: 119

VPN-1 NGX supports VoIP traffic in all of the following environments, except which environment?

A. H509-D
B. SIP
C. MGCP
D. H.323
E. SCCP

Answer: A

QUESTION NO: 120

You receive an alert indicating a suspicious FTP connection is trying to connect to one of your internal hosts. How do you block the connection in real time and verify the connection is successfully blocked?

A. Highlight the suspicious connection in SmartView Tracker > Active mode. Block the connection using the Tools > Block Intruder menu. Use the Active mode to confirm that the suspicious connection does not reappear.
B. Highlight the suspicious connection in SmartView Tracker > Log mode. Block the connection using Tools > Block Intruder menu. Use Log mode to confirm that the suspicious connection does not reappear.

C. Highlight the suspicious connection in SmartView Tracker > Active mode. Block the connection using Tools > Block Intruder menu. Use Active mode to confirm that the suspicious connection is dropped.
D. Highlight the suspicious connection in SmartView Tracker > Log mode. Block the connection using Tools > Block Intruder menu. Use the Log mode to confirm that the suspicious connection is dropped.

Answer: A

QUESTION NO: 121

Which of the following QoS rulE. action properties is an Advanced action type, only available in Traditional mode?

A. Guarantee Allocation
B. Rule weight
C. Apply rule only to encrypted traffic
D. Rule limit
E. Rule guarantee

Answer: A

QUESTION NO: 122

Which OPSEC server is used to prevent users from accessing certain Web sites?

A. LEA
B. URI
C. UFP
D. AMON
E. CVP

Answer: C

QUESTION NO: 123

Regarding QoS guarantees and limits, which of the following statements is FALSE? ~>

A. The guarantee of asuB. rule cannot be greater than the guarantee defined for the rule above it.
B. If a guarantee is defined in asuB. rule, a guarantee must be defined for the rule above it.
C. A rule guarantee must not be less than the sum defined in the guarantees' suB. rules.

D. If both a rule and per-connection limit are defined for a rule, the per-connection limit must not be greater than the rule limit.
E. If both a limit and guarantee per rule are defined in aQoS rule, the limit must be smaller than the guarantee.

Answer: E

QUESTION NO: 124

Wayne configures an HTTP Security Server to work with the content vectoring protocol to screen forbidden sites. He has created a URI resource object using CVP with the following settings:

Use CVP
Allow CVP server to modify content
Return data after content is approved
He adds two rules to his Rule Base: one to inspect HTTP traffic going to known forbidden sites, the other to allow all other HTTP traffic.
Wayne sees HTTP traffic going to those problematic sites is not prohibited.

What could cause this behavior?

A. The Security Server Rule is after the general HTTP Accept Rule.
B. The Security Server is not communicating with the CVP server.
C. The Security Server is not configured correctly.
D. The Security Server is communicating with the CVP server, but no restriction is defined in the CVP server.

Answer: A

QUESTION NO: 125

Greg is creating rules and objects to control VoIP traffic in his organization, through a VPN-1 NGX Security Gateway. Greg creates VoIP Domain SIP objects to represent each of his organization's three SIP gateways. Greg then creates a simple group to contain the VoIP Domain SIP objects. When Greg attempts to add the VoIP Domain SIP objects to the group, they are not listed. What is the problem?

A. The relatedenD. points domain specifies an address range.
B. VoIP Domain SIP objects cannot be placed in simple groups.
C. The installed VoIP gateways specify host objects.
D. The VoIP gateway object must be added to the group, before the VoIP Domain SIP object is eligible to be added to the group.

E. The VoIP Domain SIP object's name contains restricted characters.

Answer: B

QUESTION NO: 126

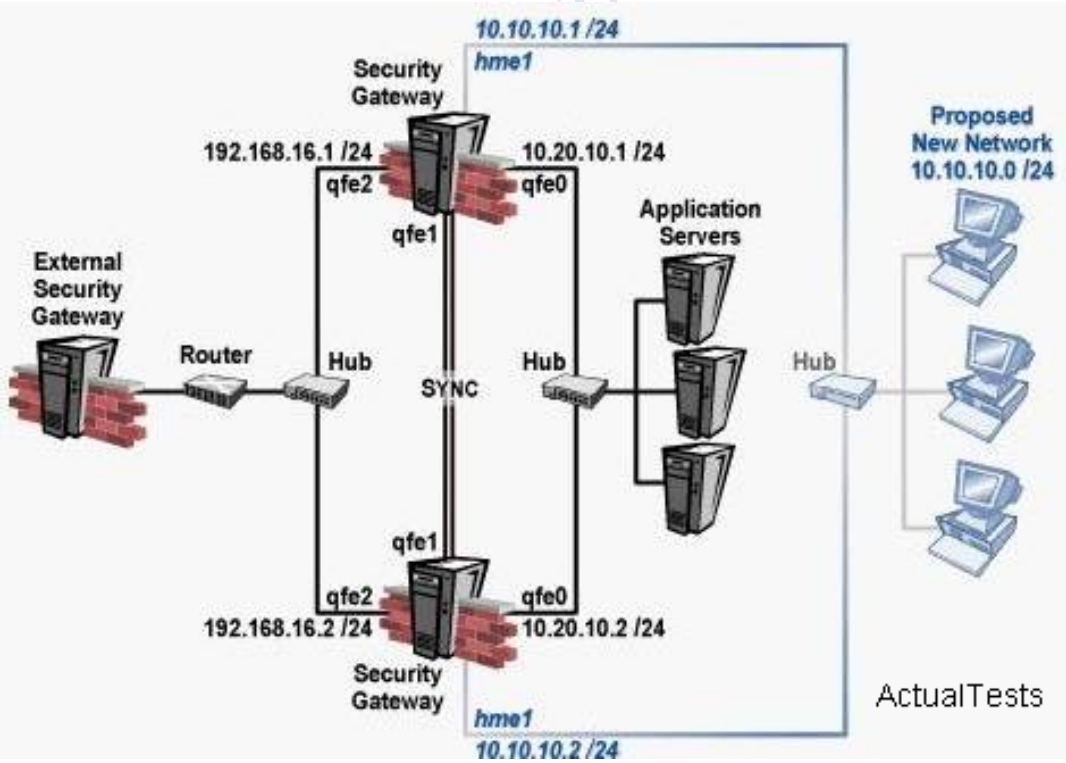
How does ClusterXL Unicast mode handle new traffic?

A. The pivot machine receives and inspects all new packets, and synchronizes the connections with other members.
B. Only the pivot machine receives all packets. It runs an algorithm to determine which member should process the packets.
C. All members receive all packets. The SmartCenter Server decides which member will process the packets. Other members simply drop the packets.
D. All cluster members process all packets, and members synchronize with each other.

Answer: B

QUESTION NO: 127

Your network includes ClusterXL running Multicast mode on two members, as shown in this topology:Your network is expanding, and you need to add new interfaces: 10.10.10.1/24 on Member A, and 10.10.10.2/24 on Member B. The virtual IP address for interface 10.10.10.0/24 is 10.10.10.3. What is the correct procedure to add these interfaces?



A. 1. Use theifconfig command to configure and enable the new interface.
2. Run cpstop and cpstart on both members at the same time.
3. Update the topology in the cluster object for the cluster and both members.
4. Install the Security Policy.
B. 1. Disable "Cluster membership" from one Gateway viacpconfig.
2. Configure the new interface via sysconfig from the "non-member" Gateway.
3. RE. enable "Cluster membership" on the Gateway.
4. Perform the same step on the other Gateway.
5. Update the topology in the cluster object for the cluster and members.
6. Install the Security Policy.
C. 1. Run cpstop on one member, and configure the new interface via sysconfig.
2. Run cpstart on the member. Repeat the same steps on another member.
3. Update the new topology in the cluster object for the cluster and members.
4. Install the Security Policy.
D. 1. Use sysconfig to configure the new interfaces on both members.
2. Update the topology in the cluster object for the cluster and both members.
3. Install the Security Policy.

Answer: C

QUESTION NO: 128

Barak is a Security Administrator for an organization that has two sites using prE. shared secrets in its VPN. The two sites are Oslo and London. Barak has just been informed that a new office is opening in Madrid, and he must enable all three sites to connect via the VPN to each other. Three Security Gateways are managed by the same SmartCenter Server, behind the Oslo Security Gateway. Barak decides to switch from prE. shared secrets to Certificates issued by the Internal Certificate Authority (ICA). After creating the Madrid gateway object with the proper VPN Domain, what are Barak's remaining steps?

1 .Disable "PrE. Shared Secret" on the London and Oslo gateway objects.
2.Add the Madrid gateway object into the Oslo and London's mesh VPN Community.
3.Manually generate ICA Certificates for all three Security Gateways.
4.Configure "Traditional mode VPN configuration" in the Madrid gateway object's VPN screen.
5.Reinstall the Security Policy on all three Security Gateways.

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

Answer: A

QUESTION NO: 129

You are configuring the VoIP Domain object for a SIP environment, protected by VPN-1 NGX. Which VoIP Domain object type can you use?

A. Call Manager
B. Gateway
C. Call Agent
D. Gatekeeper
E. Proxy

Answer: E

QUESTION NO: 130

When you add a resource service to a rule, which ONE of the following actions occur?

A. VPN-1SecureClient users attempting to connect to the object defined in the Destination column of the rule will receive a new Desktop Policy from the resource.
B. All packets that match the resource in the rule will be dropped.
C. All packets matching the resource service rule are analyzed or authenticated, based on the resource properties.
D. Users attempting to connect to the destination of the rule will be required to authenticate.
E. All packets matching that rule are either encrypted or decrypted by the defined resource.

Answer: C

QUESTION NO: 131

How can you prevent delay-sensitive applications, such as video and voice traffic, from being dropped due to long queues when using a Check Point QoS solution?

A. Low latency class
B. DiffServrule
C. guaranteed per connection
D. Weighted Fair Queuing
E. guaranteed per VoIP rule

Answer: A

QUESTION NO: 132

To change an existing ClusterXL cluster object from Multicast to Unicast mode, what configuration change must be made?

A. Change the cluster mode toUnicast on the cluster object Reinstall the Security Policy.
B. Reset Secure Internal Communications (SIC) on the cluster-member objects. Reinstall the Security Policy.
C. Run cpstop and cpstart, to rE. enable High Availability on both objects. Select Pivot mode in cpconfig.
D. Change the cluster mode to Unicast on the cluster-member object.
E. Switch the internal network's default Security Gateway to the pivot machine's IP address.

Answer: A

QUESTION NO: 133

State Synchronization is enabled on both members in a cluster, and the Security Policy is successfully installed. No protocols or services have been unselected for "selective sync". The following is the fw taB. t connections -s output from both members: Is State Synchronization working properly between the two members?

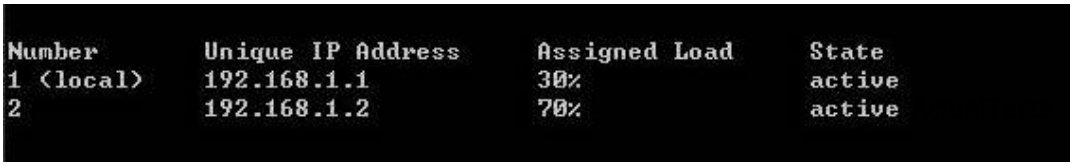
```
MEMBER A:
HOST        NAME          ID      #VALS     #PEAK     #SLINKS
Localhost   connections   8158    1553      1560      800

[expert@memberB]# fw tab -t connections -s

MEMBER B:
HOST        NAME          ID      #VALS     #PEAK     #SLINKS
localhost   connections   8158    800       1001      800
```

A. Members A and B are synchronized, because ID for both members is identical in the connections table.
B. The connections-table output is incomplete. You must run thecphaprob state command, to determine if members A and B are synchronized.
C. Members A and B are not synchronized, because #PEAKfor both members is not close in the connections table.
D. Members A and B are synchronized, because #SLINKS are identical in the connections table.
E. Members A and B are not synchronized, because #VALS in the connections table are not close.

Answer: E

QUESTION NO: 134

From the following output of cphaprob state, which ClusterXL mode is this?



A. Load Balancing Mode
B. Multicast mode
C. Unicastmode
D. New mode
E. Legacy mode

Answer: C

QUESTION NO: 135

You configure a Check Point QoS Rule Base with two rules: an H.323 rule with a weight of 10, and the Default Rule with a weight of 10. The H.323 rule includes a per-connection guarantee of 384 Kbps, and a per-connection limit of 512 Kbps. The per-connection guarantee is for four connections, and no additional connections are allowed in the Action properties. If traffic passing through the QoS Module matches both rules, which of the following statements is true?

A. Neither rule will be allocated more than 10% of available bandwidth.
B. The H.323 rule will consume no more than 2048 Kbps of available bandwidth.
C. 50% of available bandwidth will be allocated to the H.323 rule.
D. 50% of available bandwidth will be allocated to the Default Rule.
E. Each H.323 connection will receive at least 512 Kbps of bandwidth.

Answer: B

QUESTION NO: 136

You plan to migrate a VPN-1 NG with Application Intelligence (AI) R55 SmartCenter Server to VPN-1 NGX. You also plan to upgrade four VPN-1 Pro Gateways at remote offices, and one local VPN-1 Pro Gateway at your company's headquarters. The SmartCenter Server configuration must be migrated. What is the correct procedure to migrate the configuration?

A. Upgrade theSmartCenter Server and the five remote Gateways via SmartUpdate, at the same time.
B. 1.Copy the $FWDIR\conf directory from the SmartCenter Server.
2. Save directory contents to another directory.

3. Uninstall the SmartCenter Server, and install a new SmartCenter Server.
4. Move directory contents to $FWDIR\conf.
5. Reinstall all gateways using NGX and install a policy.

C. 1. From the VPN-1 NGX CD in the SmartCenter Server, select "advance upgrade".
2. After importing the SmartCenter configuration into the new NGX SmartCenter, reboot.
3. Upgrade all licenses and software on all five remote Gateways via SmartUpdate.

D. 1. Upgrade the five remote Gateways via SmartUpdate.
2. Upgrade the SmartCenter Server, using the VPN-1 NGX CD.

E. 1. Upgrade theSmartCenter Server, using the VPN-1 NGX CD. 2. Reinstall and update the licenses of the five remote Gateways.

Answer: C

QUESTION NO: 137

Which Security Server can perform content-security tasks, but CANNOT perform authentication tasks?

A. FTP
B. SMTP
C. Telnet
D. HTTP
E. rlogin

Answer: B

QUESTION NO: 138

You are configuring the VoIP Domain object for an H.323 environment, protected by VPN-1 NGX. Which VoIP Domain object type can you use?

A. Transmission Router
B. Gatekeeper
C. Call Manager
D. Proxy
E. Call Agent

Answer: B

QUESTION NO: 139

Your network traffic requires preferential treatment by other routers on the network, in addition to the QoS Module, which Check Point QoS feature should you use?

A. Guarantees
B. Limits
C. Differentiated Services
D. Weighted Fair Queuing
E. Low Latency Queuing

Answer: C

QUESTION NO: 140

When upgrading to NGX R65, which Check Point products do not require a license upgrade to be current?

A. VPN-1 NGX (R64) and later
B. VPN-1 NGX (R60) and later
C. VPN-1 NG with Application Intelligence (R54) and later
D. None, all versions require a license upgrade

Answer: B

QUESTION NO: 141

Which of these components does NOT require a VPN-1 NGX R65 license?

A. SmartConsole
B. Check Point Gateway
C. SmartCenter Server
D. SmartUpdate upgrading/patching

Answer: A

QUESTION NO: 142

Which of the following is a TRUE statement concerning contract verification?

A. Your contract file is stored on the User Center and fetched by the Gateway as needed.
B. Your contract file is stored on theSmartConsole and downloaded to the SmartCenter Server.
C. Your contract file is stored on theSmartConsole and downloaded to the Gateway.

D. Your contract file is stored on theSmartCenter Server and downloaded to the Security Gateway.

Answer: D

QUESTION NO: 143

Your current VPN-1 NG with Application Intelligence (AI) R55 stand-alone VPN-1 Pro Gateway and
SmartCenter Server runs on SecurePlatform. You plan to implement VPN-1 NGX R65 in a distributed
environment, where the new machine will be the SmartCenter Server, and the existing machine will be the
VPN-1 Pro Gateway only. You need to migrate the NG with AI R55 SmartCenter Server configuration,
including licensing.

How do you handle licensing for this NGX R65 upgrade?

A. Request an NGX R65SmartCenter Server license, using the new server's IP address. Request a new
central NGX R65 VPN-1 Gateway license also licensed to the new SmartCenter Server's IP address.
B. Leave the current license on the gateway to be upgraded during the software upgrade. Purchase a new
license for the VPN-1 NGX R65 SmartCenter Server.
C. Request an NGX R65SmartCenter Server license, using the existing gateway machine's IP address.
Request a new local license for the NGX R65 VPN-1 Gateway using the new server's IP address.
D. Request an NGX R65SmartCenter Server license, using the new server's IP address. Request a new
central NGX R65 VPN-1 Gateway license for the existing gateway server's IP address.

Answer: A

QUESTION NO: 144

You are running the license_upgrade tool on your SecurePlatform Gateway. Which of the following can you NOT do with the upgrade tool?

A. Simulate the license-upgrade process.
B. View the licenses in theSmartUpdate License Repository.

C. Perform the actual license-upgrade process.
D. View the status of currently installed licenses.

Answer: B

QUESTION NO: 145

What action can be run from SmartUpdate NGX R65?

A. remote_uninstall_verifier
B. upgrade_export
C. mds_backup
D. cpinfo

Answer: D

QUESTION NO: 146

What tools CANNOT be launched from SmartUpdate NGX R65?

A. cpinfo
B. SecurePlatform Web UI
C. Nokia Voyager
D. snapshot

Answer: D

QUESTION NO: 147

Choose all correct statements. SmartUpdate, located on a VPN-1 NGX SmartCenter Server, allows you
to:

(1) Remotely perform a first time installation of VPN-1 NGX on a new machine
(2) Determine OS patch levels on remote machines
(3) Update installed Check Point and any OPSEC certified software remotely
(4) Update installed Check Point software remotely
(5) Track installed versions of Check Point and OPSEC products
(6) Centrally manage licenses

A. 4, 5, & 6

B. 2, 4, 5, & 6
C. 1 & 4
D. 1, 3, 4, & 6

Answer: B

QUESTION NO: 148

You are a Security Administrator preparing to deploy a new HFA (Hotfix Accumulator) to ten Security
Gateways at five geographically separated locations. What is the BEST method to implement this HFA?

A. Send a Certified Security Engineer to each site to perform the update
B. UseSmartUpdate to install the packages to each of the Security Gateways remotely
C. Use a SSH connection to SCP the HFA to each Security Gateway. Once copied locally, initiate a
remote installation command and monitor the installation progress with SmartView Monitor.
D. Send a CDROM with the HFA to each location and have local personnel install it

Answer: B

QUESTION NO: 149

You are using SmartUpdate to fetch data and perform a remote upgrade of an NGX Security Gateway.
Which of the following statements is FALSE?

A. IfSmartDashboard is open during package upload and upgrade, the upgrade will fail.
B. A remote installation can be performed without the SVN Foundation package installed on a remote NG
with Application Intelligence Security Gateway
C. SmartUpdate can query the SmartCenter Server and VPN-1 Gateway for product information
D. SmartUpdate can query license information running locally on the VPN-1 Gateway

Answer: B

QUESTION NO: 150

What port is used for communication to the UserCenter with SmartUpdate?

A. HTTP
B. HTTPS
C. TCP 8080
D. CPMI

Answer: B

QUESTION NO: 151

What physical machine must have access to the UserCenter public IP when checking for new packages
with SmartUpdate?

A. VPN-1 Security Gateway getting the new upgrade package
B. SmartUpdate installed SmartCenter Server PC
C. SmartUpdate Repository SQL database Server
D. SmartUpdate GUI PC

Answer: D

QUESTION NO: 152

What action CANNOT be run from SmartUpdate NGX R65?

A. Get all Gateway Data
B. Reboot gateway
C. Preinstall verifier...
D. Fetch sync status

Answer: D

QUESTION NO: 153

You want to upgrade an NG with Application Intelligence R55 Security Gateway running on SecurePlatform to VPN-1 NGX R65 via SmartUpdate. Which package(s) is(are) needed in the Repository prior to upgrade?

A. SecurePlatform NGX R65 package
B. VPN-1 Power/UTM NGX R65 package
C. SecurePlatform and VPN-1 Power/UTM NGX R65 packages
D. SVN Foundation and VPN-1 Power/UTM packages

Answer: A

QUESTION NO: 154

Why should the upgrade_export configuration file (.tgz) be deleted after you complete the import process?

A. It will prevent a future successfulupgrade_export since the .tgz file cannot be overwritten.
B. It will conflict with any future upgrades run fromSmartUpdate.
C. SmartUpdate will start a new installation process if the machine is rebooted.
D. It contains your security configuration, which could be exploited.

Answer: D

QUESTION NO: 155

Concerning these products: SecurePlatform, VPN-1 Pro Gateway, UserAuthority Server, Nokia OS, UTM-1, Eventia Reporter, and Performance Pack, which statement is TRUE?

A. All but the Nokia OS can be upgraded to VPN-1 NGX R65 withSmartUpdate.
B. All but Performance Pack can be upgraded to VPN-1 NGX R65 withSmartUpdate.
C. All can be upgraded to VPN-1 NGX R65 withSmartUpdate.
D. All but the UTM-1 can be upgraded to VPN-1 NGX R65 withSmartUpdate.

Answer: C

QUESTION NO: 156

If a SmartUpdate upgrade or distribution operation fails on SecurePlatfom, how is the system recovered?

A. SecurePlatform will reboot and automatically revert to the last snapshot version prior to upgrade.
B. The Administrator must remove the rpm packages manually, and reattempt the upgrade.
C. The Administrator can only revert to a previously created snapshot (if there is one) with the command
cprinstall snapshot <object name> <filename>.
D. The Administrator must reinstall the last version via the command cprinstall revert <object name> <file name>.

Answer: A

QUESTION NO: 157

Identify the correct step performed by SmartUpdate to upgrade a remote Security Gateway.

A. After selecting "Packages: Add... from CD", the entire contents of the CD are copied to the packages
directory on the selected remote Security Gateway.
B. After selecting "Packages: Add... from CD", the entire contents of the CD are copied to the Package
Repository on the SmartCenter Server.
C. After selecting "Packages: Add... from CD", the selected package is copied to the packages directory on
the selected remote Security Gateway.
D. After selecting "Packages: Add... from CD", the selected package is copied to the Package Repository
on the SmartCenter Server.

Answer: D

QUESTION NO: 158

Identify the correct step performed by SmartUpdate to upgrade a remote Security Gateway.

A. After selecting "Packages > Distribute..." and choosing the target gateway, the selected package is
copied from the Package Repository on the SmartCenter to the Security Gateway but the installation IS
NOT performed.
B. After selecting "Packages > Distribute..." and choosing the target gateway, theSmartUpdate wizard
walks the Administrator through a Distributed Installation.
C. After selecting "Packages > Distribute..." and choosing the target gateway, the selected package is
copied from the Package Repository on the SmartCenter to the Security Gateway and the installation IS
performed.
D. After selecting "Packages > Distribute..." and choosing the target gateway, the selected package is
copied from the CDROM of the SmartUpdate PC directly to the Security Gateway and the installation IS
performed.

Answer: A

QUESTION NO: 159

What happens in relation to the CRL cache after a cpstop;spstart has been initiated?

A. The gateway continues to use the old CRL even if it is not valid, until a new CRL is cached
B. The gateway continues to use the old CRL, as long as it is valid.
C. The gateway issues a crl_zap on startup, which empties the cache and forces Certificate retrieval.
D. The gateway retrieves a new CRL on startup, then discards the old CRL as invalid.

Answer: B

QUESTION NO: 160

Public-key cryptography is considered which of the following?

A. two-key/symmetric
B. one-key/asymmetric
C. two-key/asymmetric
D. one-key/symmetric

Answer: C

QUESTION NO: 161

What is the greatest benefit derived from VPNs compared to frame relay, leased lines any other types of dedicated networks?

A. lower cost
B. stronger authentication
C. Less failure/downtime
D. Greater performance

Answer: A

QUESTION NO: 162

What is the bit size of DES?

A. 56
B. 112
C. 168
D. 128
E. 32
F. 64

Answer: A

QUESTION NO: 163

In cryptography, the Rivest, Shamir, Adelman (RSA) scheme has which of the following? Select all that apply.

A. A symmetric-cipher system
B. A secret-key encryption-algorithm system
C. A public-key encryption-algorithm system
D. An asymmetric-cipher system

Answer: C,D

QUESTION NO: 164

Which of the following are supported with the office mode? Select all that apply.

A. SecureClient
B. L2TP
C. Transparent Mode
D. Gopher
E. SSL Network Extender

Answer: A,B,E

QUESTION NO: 165

Which network port does PPTP use for communication?

A. 1723/tcp
B. 1723/udp
C. 25/udp
D. 25/tco

Answer: A

QUESTION NO: 166

VPN access control would fall under which VPN component?

A. QoS
B. Performance
C. Management
D. Security

Answer: D

QUESTION NO: 167

In ClusterXL, which of the following processes are defined by default as critical devices?

A. fwm
B. cphad
C. fw.d
D. fwd.proc

Answer: B

QUESTION NO: 168

If a digital signature is used to achieve both data-integrity checking and verification of sender, digital signatures are only used when implementing:

A. A symmetric-encryption algorithm
B. CBL-DES
C. Triple DES
D. An asymmetric-encryption algorithm

Answer: D

QUESTION NO: 169

Which of the following is supported with Office Mode?

A. SecuRemote
B. SecureClient
C. SSL Network Extender
D. Connect Mode

Answer: A

QUESTION NO: 170

When synchronizing clusters, which of the following statements are true?
Select all that apply.

A. Only cluster members running on the same OS platform can be synchronized.
B. Client Auth or Session Auth connections through a cluster member will be lost of the cluster member fails.
C. The state of connections using resources is maintained by a Security Server, so these connections cannot be synchronized.
D. In the case of a failover, accounting information on the failed member may be lost despite a properly

Answer: A,B,C

QUESTION NO: 171

VPN traffic control would fall under which VPN component?

A. Performance
B. Management
C. Security
D. QoS

Answer: D

QUESTION NO: 172

Which of the following is an example of the hash function?

A. DES and CBC
B. DAC and MAC
C. SHA and 3DES
D. MD5 and SHA-1

Answer: D

QUESTION NO: 173

When configuring site-to-site VPN High Availability (HA) with MEP, which of the following is correct?

A. MEP Gateways cannot be geographically separated machines.
B. The decision on which MEP Gateway to use is made on the MEP Gateway's side of the tunnel.
C. MEP Gateways must be managed by the same SmartCenter Server.
D. If one MEP Security Gateway fails, the connection is lost and the backup Gateway picks up the next connection.

Answer: D

QUESTION NO: 174

Consider the following actions that VPN-1 NGX can take when it control packets. The Policy Package has been configured for Traditional Mode VPN. Identify the options that includes the available actions. Select four.

A. Allow
B. Reject
C. Client auth
D. Decrypt
E. Accept
F. Drop
G. Encrypt
H. Hold
I. Proxy

Answer: B,E,F,G

QUESTION NO: 175

Which of the following is a supported Sticky Decision function of Sticky Connections for Load Sharing?

A. Multi-connection support for VPN-1 cluster members
B. Support for SecureClient/SecuRemote/SSL Network Extended encrypted connections.
C. Support for all VPN deployments (except those with third-party VPN peers)

D. Support for Performance Pack acceleration

Answer: D

QUESTION NO: 176

Which of the following does IPSec use during IPSec key negotiation?

A. IPSec SA
B. RSA Exchange
C. ISAKMP SA
D. Diffie-Hellman exchange

Answer: D

QUESTION NO: 177

Which of the following SSL Network Extender server-side prerequisites are correct? Select all that apply.

A. The VPN1-Gateway must be configured to work with Visitor Mode
B. The specific VPN-1 Security Gateway must be configured as a member of the VPN-1 Remote Access Community.
C. There are distinctly separate access rules required for SecureClient users vs. SSL Network Extender users.
D. To use Integrity Clientless Security (ICS), you must install the ICS server or configuration tool.

Answer: A,B,D

QUESTION NO: 178

After installing VPN-1 Pro NGQ R65, you discover that one port on your Intel Quad NIC on the Security Gateway is not fetched by a get topology request. What is the most likely cause and solution?

A. The NIC is faulty. Replace it and reinstall.
B. Make sure the driver for you particular NIC is available, and reinstall. You will be prompted for the driver.
C. If an interface is not configured, it is not recognized. Assign an IP and subnet mask using the Web UI,
D. Your NIC driver is installed but was not recognized. Apply the latest SecurePlatform R65 Hotfix Accumulator (HFA).

Answer: C

QUESTION NO: 179

Which of the following provides a unique user ID for a digital Certificate?

A. Username
B. User-message digest
C. User e-mail
D. User organization

Answer: B

QUESTION NO: 180

For object-based VPN routing to succeed, what must be configured?

A. A single rule in the Rule Base must cover traffic in both directions, inbound and outbound on the central (HUB) Security Gateway.
B. No rules need to be created, implied rules that cover inbound and outbound traffic on the central (HUB) Gateway are already in place from Policy > Properties > Accept VPN-1 Control Connections.
C. At least two rules in the Rule Base must created, one to cover traffic inbound and the other to cover traffic outbound on the central (HUB) Security Gateway.
D. VPN routing is not configured in the Rule Base or Community objects. Only the native-routing mechanism on each Gateway can direct the traffic via its VTI configured interfaces.

Answer: C

QUESTION NO: 181

What proprietary Check Point protocol is the basis of the functionality of Check Point ClusterXL inter-module communication?

A. RDP
B. IPSec
C. CCP
D. HA OPCODE
E. CKPP

Answer: C

QUESTION NO: 182

Which of the following is part of the PKI? Select all that apply.

A. User certificate
B. Attribute Certificate
C. Certificate Revocation Lists
D. Public-key certificate

Answer: A,C,D

QUESTION NO: 183

Which of the following are valid PKI architectures?

A. mesh architecture
B. Bridge architecture
C. Gateway architecture
D. Hierarchical architecture

Answer: A,C,D

QUESTION NO: 184

Which of the following are valid reasons for beginning with a fresh installation VPN-1 NGX R65, instead of upgrading a previous version to VPN-1 NGX R65? Select all that apply.

A. You see a more logical way to organize your rules and objects
B. You want to keep your Check Point configuration.
C. Your Security Policy includes rules and objects whose purpose you do not know.
D. Objects and rules' naming conventions have changed over time.

Answer: A,C,D

QUESTION NO: 185

Public keys and digital certificates provide which of the following? Select three.

A. nonrepudiation

B. Data integrity
C. Availability
D. Authentication

Answer: A,B,D

QUESTION NO: 186

Which of the following uses the same key to decrypt as it does to encrypt?

A. dynamic encryption
B. Certificate-based encryption
C. static encryption
D. Symmetric encryption
E. Asymmetric encryption

Answer: D

QUESTION NO: 187

Which of the following happen when using Pivot Mode in ClusterXL? Select all that apply.

A. The Pivot forwards the packet to the appropriate cluster member.
B. The Security Gateway analyzes the packet and forwards it to the Pivot.
C. The packet is forwarded through the same physical interface from which it originally came, not on the sync interface.
D. The Pivot's Load Sharing decision function decides which cluster member should handle the packet.

Answer: A,C,D

QUESTION NO: 188

Central License management allows a Security Administrator to perform which of the following? Select all that apply.

A. Attach and/or delete only NGX Central licenses to a remote module (not Local licenses)
B. Check for expired licenses
C. Add or remove a license to or from the license repository
D. Sort licenses and view license properties
E. Delete both NGX Local licenses and Central licenses from a remote module

F. Attach both NGX Central and Local licenses to a remote moduel

Answer: A,B,C,D

QUESTION NO: 189

How should Check Point packages be uninstalled?

A. In the same order in which the installation wrapper initially installed from.
B. In the opposite order in which the installation wrapper initially installed them.
C. In any order, CPsuite must be the last package uninstalled
D. In any order as long as all packages are removed

Answer: B

QUESTION NO: 190

You have three Gateways in a mesh community. Each gateway's VPN Domain is their internal network as defined on the Topology tab setting "All IP Addresses behind Gateway based on Topology information."

You want to test the route-based VPN, so you created VTIs among the Gateways and created static route entries for the VTIs. However, when you test the VPN, you find out the VPN still go through the regular domain IPsec tunnels instead of the routed VTI tunnels.

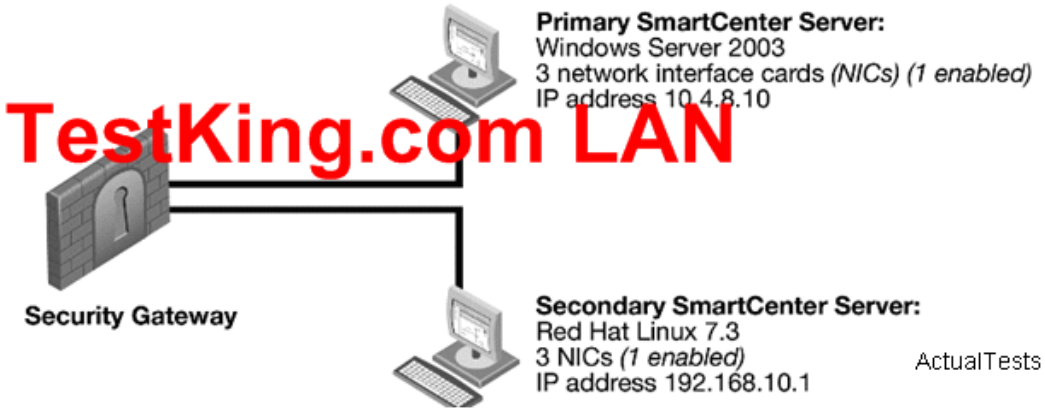
What is the problem and how do you make the VPN to use the VTI tunnels?

A. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, remove the Gateways out of the mesh community and replace with a star community.
B. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, use an empty group object as each Gateway's VPN Domain
C. Route-based VTI takes precedence over the Domain VPN. To Make the VPN go through VTI, use dynamic-routing protocol like OSPF or BGP to route the VTI address to the peer instead of static routes.
D. Route-based VTI takes precedence over the Domain VPN. Troubleshoot the static route entries to insure that they are correctly pointing to the VTI gateway IP.

Answer: B

QUESTION NO: 191

The following configuration is for VPN-1 NGX 65.
:Is this configuration correct for Management High Availability (HA)?



A. No, a NGX 65SmartCenter Server cannot run on Red Hat Linux 7.3.
B. No, theSmartCenter Servers must be installed on the same operating system.
C. No, theSmartCenter Servers must reside on the same network.
D. No, theSmartCenter Servers do not have the same number of NICs.

Answer: B

QUESTION NO: 192

When distributing IPSec packets to gateways in a Load Sharing Multicast mode cluster, which valid Load Sharing method will consider VPN information in the decision function?

A. Load Sharing based on SPIs
B. Load Sharing based on ports, VTI, and IP addresses
C. Load Sharing based on IP addresses, ports, and serial peripheral interfaces.
D. Load Sharing based on IP addresses, ports, and security parameter indexes.

Answer: D

QUESTION NO: 193

Which encryption scheme provides in-place encryption?

A. DES
B. SKIP
C. AES
D. IKE

Answer: B

QUESTION NO: 194

Which of the following can be said about numbered VPN Tunnel Interfaces (VTIs)?

A. VTIs are assigned only local addresses, not remote addresses
B. VTIs cannot share IP addresses
C. VTIs cannot use an already existing physical-interface IP address
D. VTIs are only supported on Nokia IPSO

Answer: A

QUESTION NO: 195

What is the command to upgrade an NG with Application Intelligence R55 SmartCenter running on SecurePlatform to VPN-1 NGX R65?

A. fw install_mgmt
B. upgrade_mgmt
C. patch add cd
D. fwm upgrade_tool

Answer: C

QUESTION NO: 196

What can be said about RSA algorithms? Select all that apply.

A. Long keys can be used in RSA for enhances security
B. Short keys can be used for RSA efficiency.
C. RSA is faster to compute than DES
D. RSA's key length is variable.

Answer: A,B,D

QUESTION NO: 197

By default Check Point High Availability components send updates about their state every...

A. 1 second

B. 2 seconds
C. 5 seconds
D. 0.1 seconds
E. 0.5 seconds

Answer: D

QUESTION NO: 198

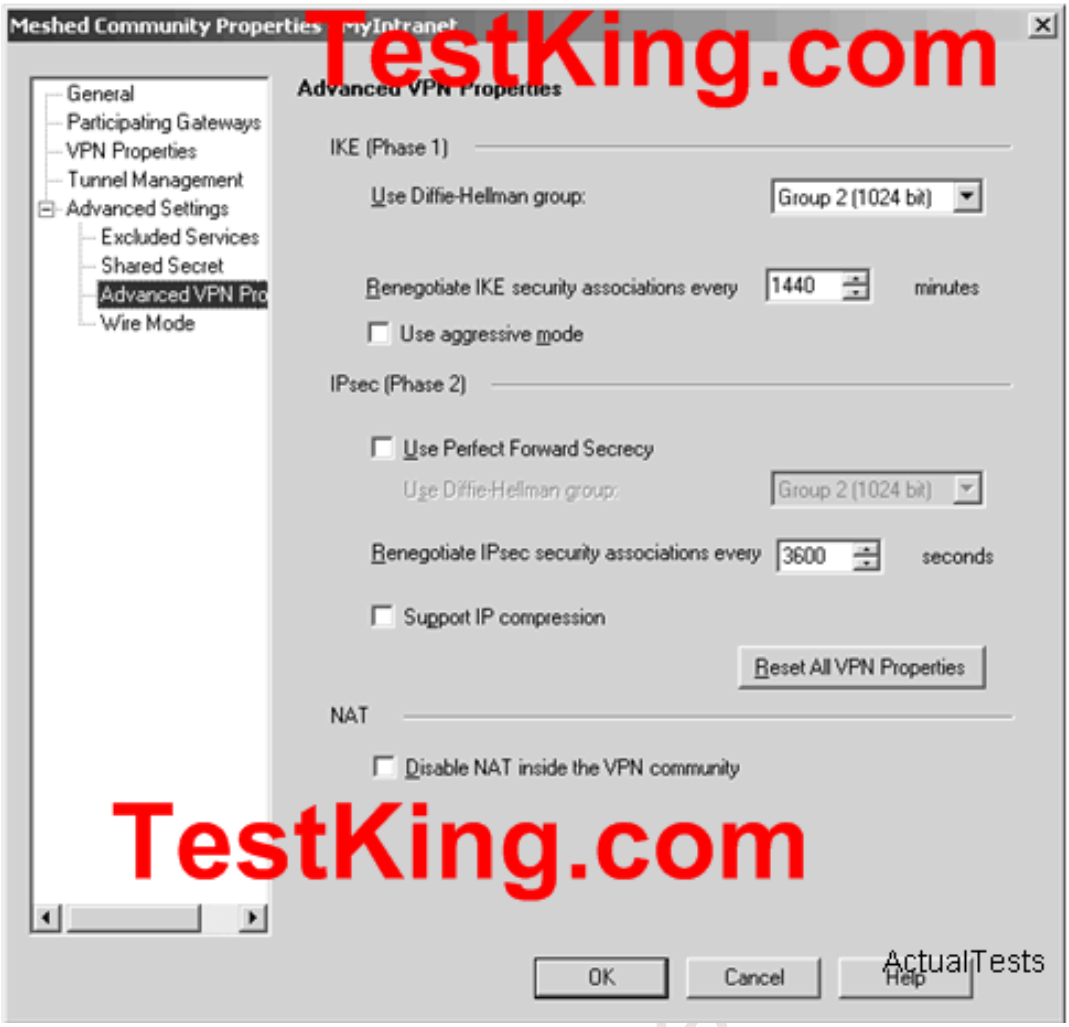
What is the most typical type of configuration for VPNs with several externally managed Gateways?

A. star community
B. mesh community
C. domain community
D. Hybrid community
E. SAT community

Answer: A

QUESTION NO: 199

Exhibit:



You study the Advanced Properties exhibit carefully. What settings can you change to reduce the encryption overhead and improve performance for your mesh VPN Community?

A. Change the "Renegotiate IPsec security associations every 3600 seconds" to 7200
B. Check the box "Use aggressive mode"
C. Change the box "Use Perfect Forward Secrecy"
D. Change the setting "Use Diffie-Hellman group:" to "Group 5 (1536 bit)"

Answer: A

QUESTION NO: 200

A VPN Tunnel Interface (VTI) is defined on SecurePlatform Pro as:

vpn shell interface add numbered 10.10.0.1 10.10.0.2 Helsinki.cp

What do you know about this VTI?

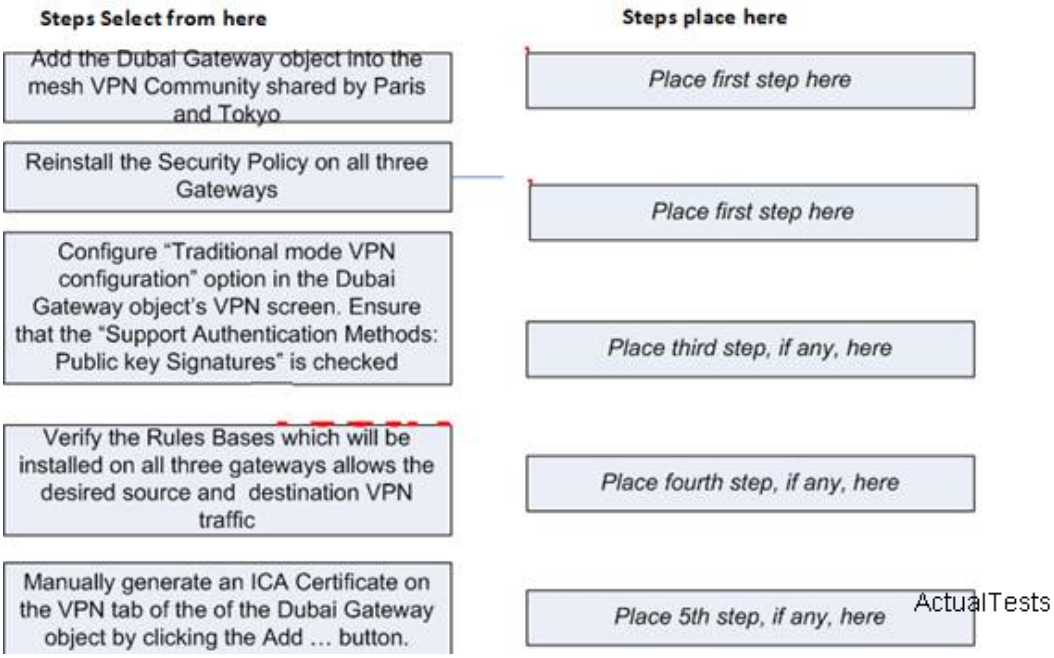
A. The VTI name is "Helsinki.cp"

B. The local Gateway's object name is "Helsinki.cp"
C. The peer Security Gateway's name is "Helsinki.cp"
D. 10.10.0.1 is the local Gateway's internal interface, and 10.10.0.2 is the internal interface of the remote Gateway

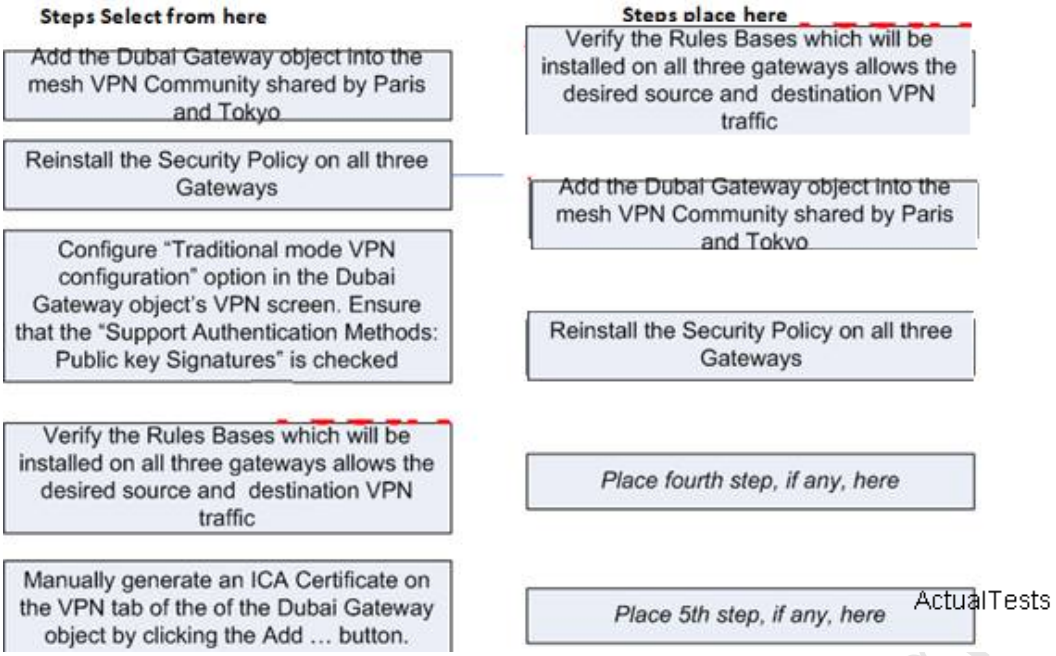
Answer: C

QUESTION NO: 201 DRAG DROP

TestKing.com has two sites using certificates-based VPN issued by the ICA. The two sites, Tokyo and Paris, are configured using a simplified VPN policy. You are trying to integrate a new office opening in New Delhi. You must enable all three sites to connect via the VPN to each other. Three Security Gateways are managed by the same SmartCenter Server behind the Paris Security Gateway.
After creating the Dubai Gateway object with the proper VPN domain, what must you do?



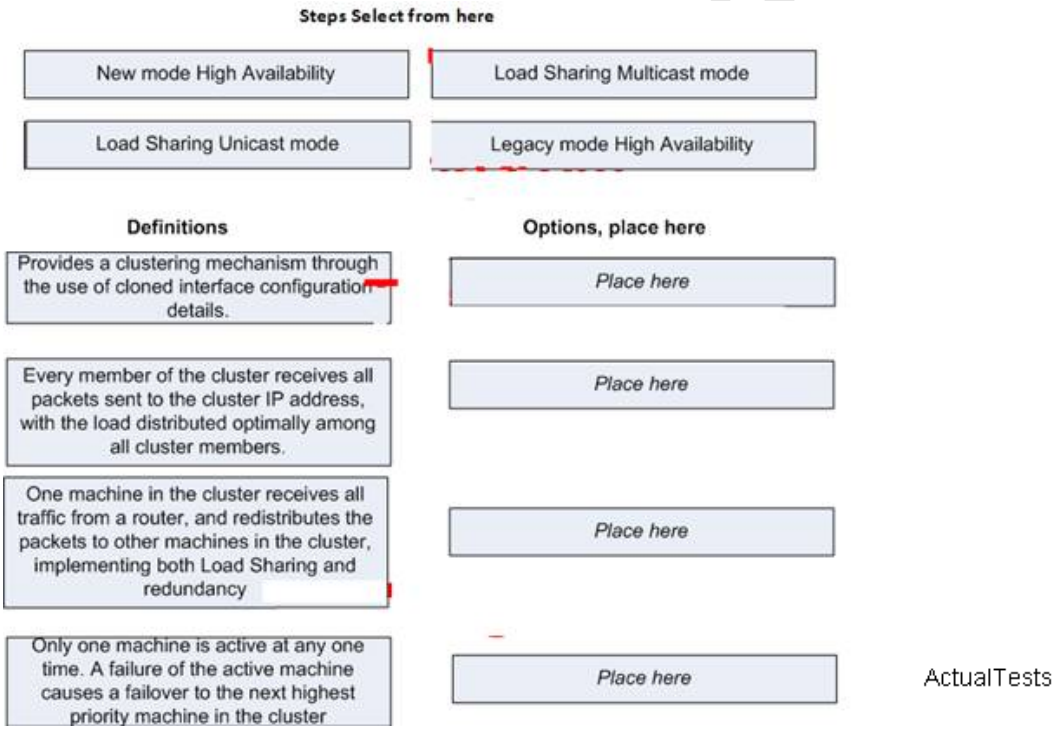
Answer:



ActualTests

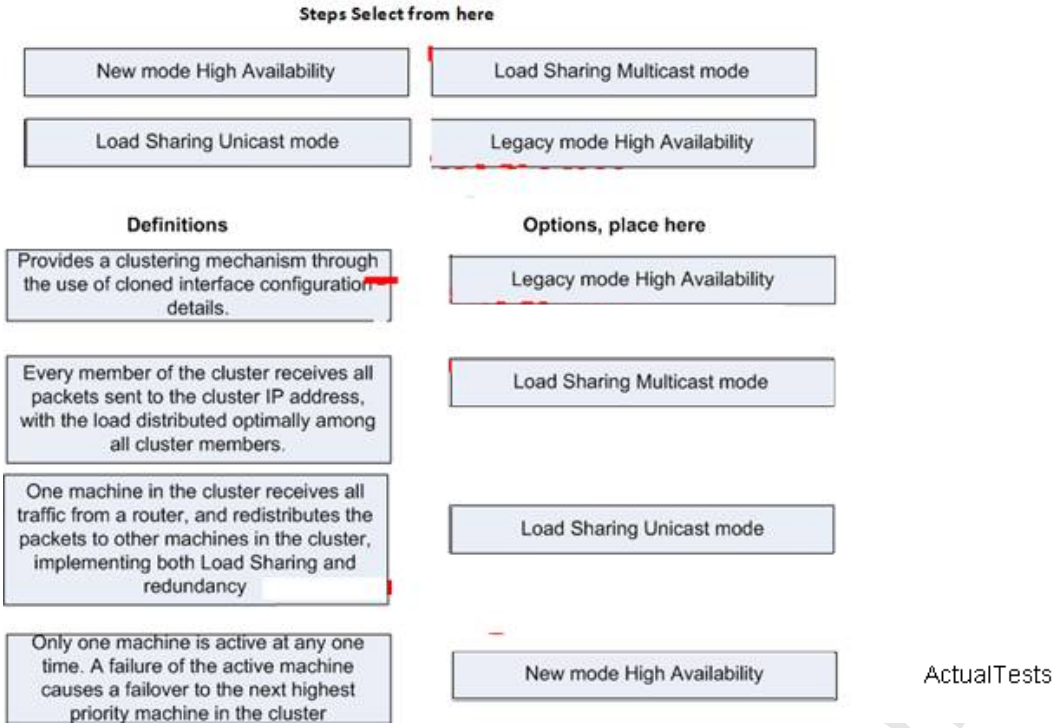
QUESTION NO: 202 DRAG DROP

Match the ClusterXL Modes with their configurations.



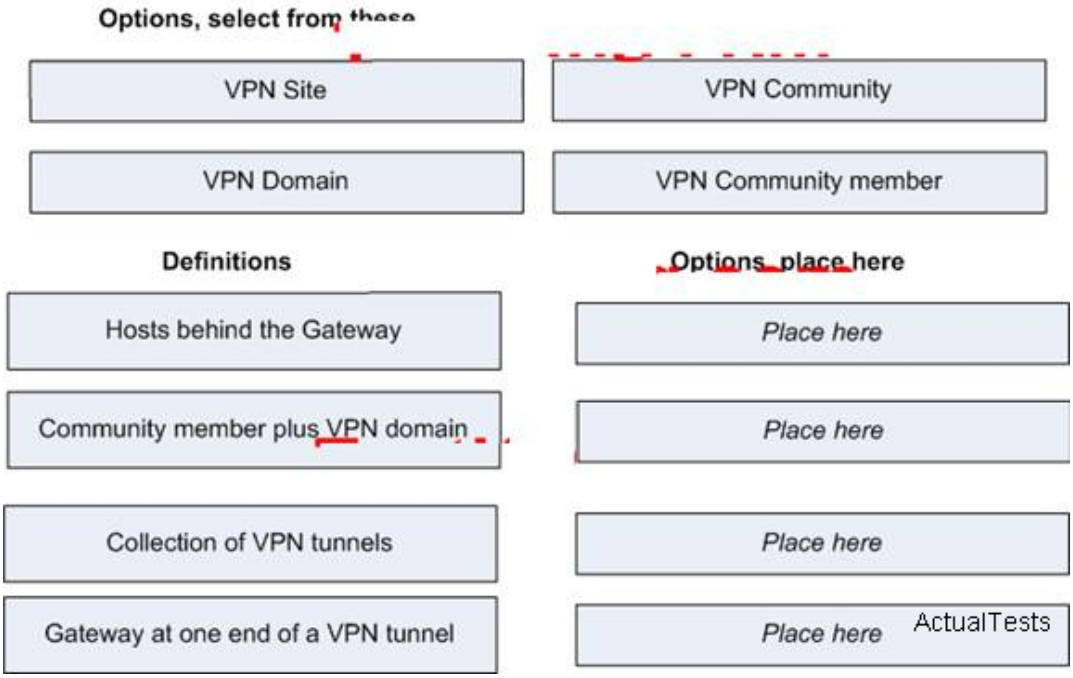
ActualTests

Answer:

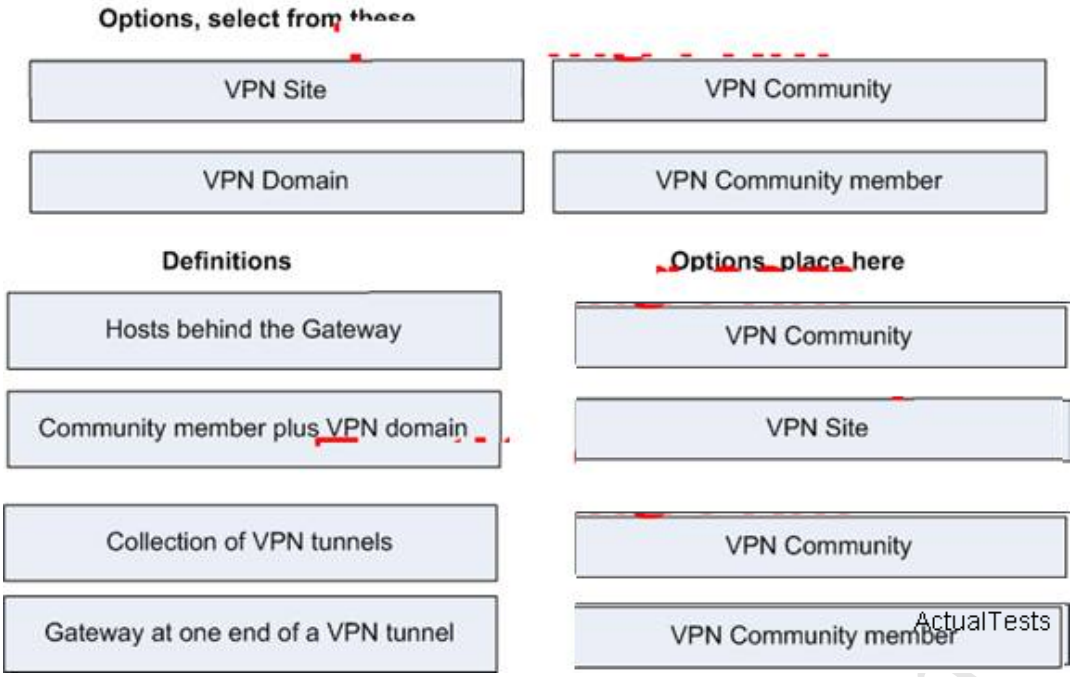


QUESTION NO: 203 DRAG DROP

Match the Terms with their definitions.

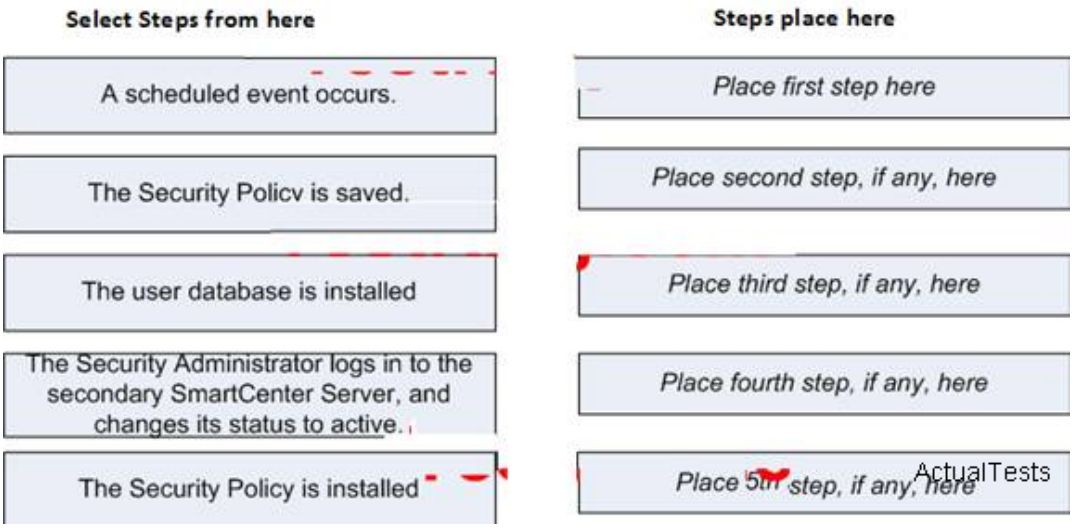


Answer:

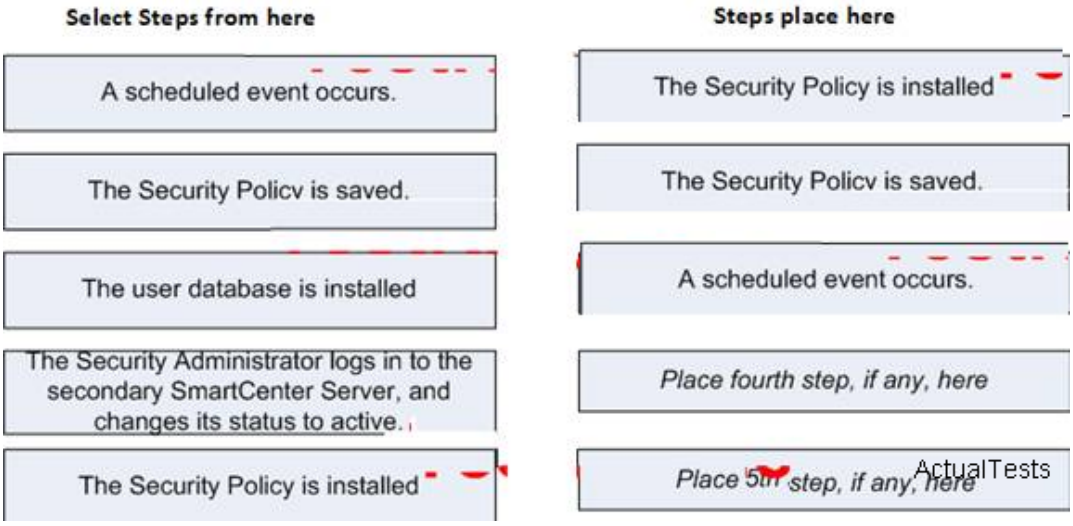


QUESTION NO: 204 DRAG DROP

In a Management High Availability (HA) configuration, you can configure synchronization to occur automatically. Select the best response for the synchronization sequence.

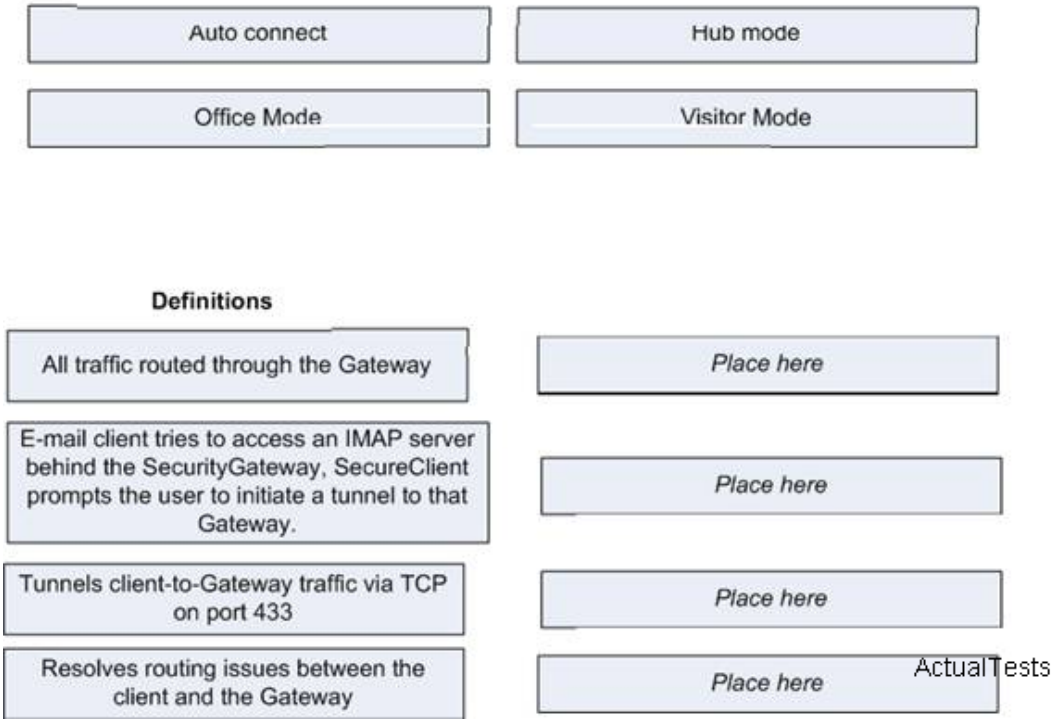


Answer:

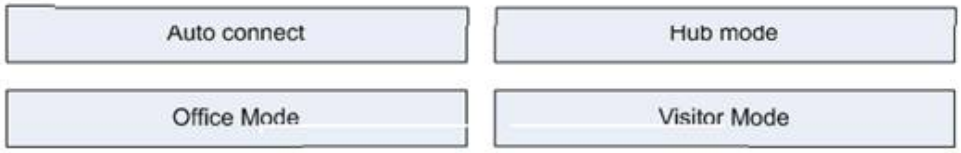


QUESTION NO: 205 DRAG DROP

Match the remote-access VPN connection mode features with their descriptions.



Answer:



Definitions

All traffic routed through the Gateway	Hub mode
E-mail client tries to access an IMAP server behind the SecurityGateway, SecureClient prompts the user to initiate a tunnel to that Gateway.	Auto connect
Tunnels client-to-Gateway traffic via TCP on port 433	Visitor Mode
Resolves routing issues between the client and the Gateway	Office Mode