



Exam : 156-315

Title : Check Point Security Administration
NGX II (156-315.1)

Ver : 11-24-2008

QUESTION 1:

You work a network administrator for Certkiller .com. 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 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 2:

Certkiller .com has many VPN-1 Edge gateways at various branch offices, to allow VPN-1 SecureClient users to access Certkiller .com resources. For security reasons, Certkiller .com's Secure 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

Explanation:

This configuration option can be found in the properties window under Advanced Settings > VPN Routing for a Star Community VPN Object (see screenshot)

From the help file on this properties page:

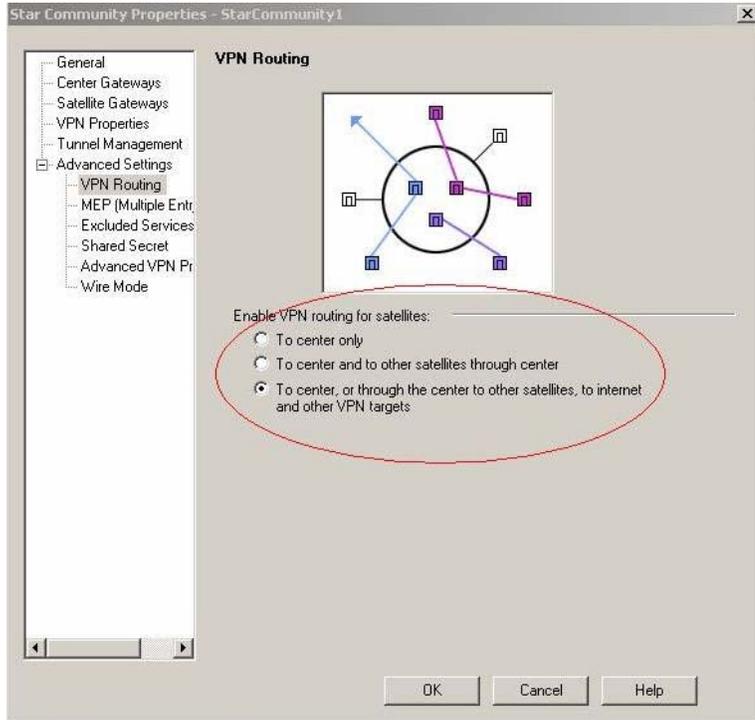
Three options are available:

* To center only. No VPN routing actually occurs. Only connections between the Satellite Gateways and Central Gateway go through the VPN tunnel. Other connections are routed in the normal way

* To center and to other satellites through center. Use VPN routing for connection between satellites. Every packet passing from a Satellite Gateway to another Satellite Gateway is routed

through the Central Gateway. Connection between Satellite Gateways and Gateways that do not belong to the community are routed in the normal way.

* To center, or through the center to other satellites, to internet and other VPN targets. Use VPN routing for every connection a Satellite Gateway handles. Packets sent by a Satellite Gateway pass through the VPN tunnel to the Central Gateway before being routed to the destination address.



QUESTION 3:

You are preparing to configure your VoIP Domain Gatekeeper object.
Which two other object 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 4:

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 Queing

Answer: D

Explanation:

Bandwidth Allocation and Rules

A rule can specify three factors to be applied to bandwidth allocation for classified connections:

Weight

Weight is the relative portion of the available bandwidth that is allocated to a rule.

To calculate what portion of the bandwidth the connections matched to a rule receive, use the following formula:

$$\text{this rule's portion} = \frac{\text{this rule's weight}}{\text{total weight of all rules with open connections}}$$

For example, if this rule's weight is 12 and the total weight of all the rules under which connections are currently open is 120, then all the connections open under this rule are allocated 12/120 (or 10%) of the available bandwidth.

In practice, a rule may get more than the bandwidth allocated by this formula, if other rules are not using their maximum allocated bandwidth.

Unless a per connection limit or guarantee is defined for a rule, all connections under a rule receive equal weight.

Allocating bandwidth according to weights ensures full utilization of the line even if a specific class is not using all of its bandwidth. In such a case, the left over bandwidth is divided among the remaining classes in accordance with their relative weights. Units are configurable, see "Defining QoS Global Properties" on page 94.

Default Rule

Chapter 4 Basic QoS Policy Management 35

Guarantees

A guarantee allocates a minimum bandwidth to the connections matched with a rule.

Guarantees can be defined for:

the sum of all connections within a rule

A total rule guarantee reserves a minimum bandwidth for all the connections under a rule combined. The actual bandwidth allocated to each connection depends on the number of open connections that match the rule. The total bandwidth allocated to the rule can be no less than the guarantee, but the more connections that are open, the less bandwidth each one receives.

individual connections within a rule

A per connection guarantee means that each connection that matches the particular rule is guaranteed a minimum bandwidth.

Although weights do in fact guarantee the bandwidth share for specific connections,

only a guarantee allows you to specify an absolute bandwidth value.

Limits

A limit specifies the maximum bandwidth that is assigned to all the connections together. A limit defines a point beyond which connections under a rule are not allocated bandwidth, even if there is unused bandwidth available.

Limits can also be defined for the sum of all connections within a rule or for individual connections within a rule.

QUESTION 5:

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. MacOS X

Answer: A

Explanation:

RedHat 8 is also not currently supported according to the docs, but A is the most correct answer..

http://www.checkpoint.com/products/downloads/vpn-1_clients_datasheet.pdf

QUESTION 6:

You want to upgrade a SecurePlatform NG with Application Intelligence (AI) 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. VNP-1 and FireWall-1
- C. SecurePlatform NGX R60
- D. SVN Foundation
- E. VPN-1 Pro/Express NGX R60

Answer: C

Explanation:

SmartCenter Upgrade on SecurePlatform R54, R55 and Later Versions

Upgrading to NGX R60 over a SecurePlatform operating system requires updating both operating system and software products installed. SecurePlatform users should follow the relevant SecurePlatform upgrade process.

The process described in this section will result with an upgrade of all components

(Operating System and software packages) in a single upgrade process. No further upgrades are required.

Refer to NGX R60 SecurePlatform Guide for additional information.

If a situation arises in which a revert to your previous configuration is required refer to "Revert to your Previous Deployment" on page 52 for detailed information.

Using a CD ROM

The following steps depict how to upgrade SecurePlatform R54 and later versions using a CD ROM drive.

1 Log into SecurePlatform (Expert mode is not necessary).

2 Apply the SecurePlatform NGX R60 upgrade package:

```
# patch add cd.
```

3 At this point you will be asked to verify the MD5 checksum.

4 Answer the following question:

Do you want to create a backup image for automatic revert? Yes/No

If you select Yes, a Safe Upgrade will be performed.

Safe Upgrade automatically takes a snapshot of the entire system so that the entire system (operating system and installed products) can be restored if something goes wrong during the Upgrade process (for example, hardware incompatibility). If the Upgrade process detects a malfunction, it will automatically revert to the Safe Upgrade image.

When the Upgrade process is complete, upon reboot you will be given the option to manually choose to start the SecurePlatform operating system using the upgraded version image or using the image prior to the Upgrade process.

QUESTION 7:

Exhibit:

```
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 exhibit displays the cphaprob state command output from a New Mode High Availability cluster member.

Which machine has the highest priority?

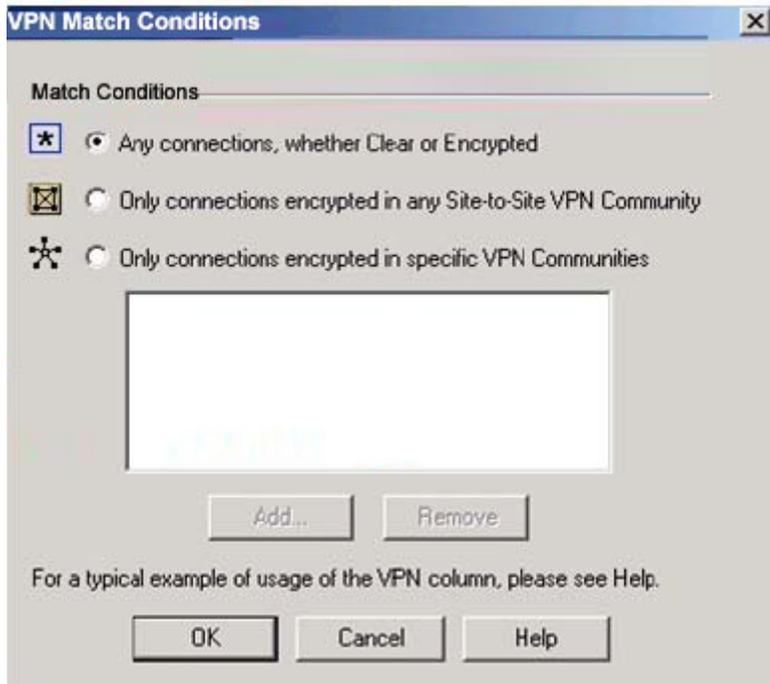
- A. 192.168.1.2, since its number is 2.
- B. 192.168.1.1, because its number is 1.
- C. This output does not indicate which machine has the highest priority.
- D. 192.168.1.2, because its stats is active

Answer: B

Reference: ClusterXL.pdf page 76

QUESTION 8:

Exhibit:



Certkiller 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. Certkiller sees the screen displayed in the exhibit.

What is the problem?

- A. Jack must enable `directional_match(true)` in the `object_5_0.c` file on SmartCenter server.
- B. Jack must enable Advanced Routing on each Security Gateway
- C. Jack must enable VPN Directional Match on the VPN Advanced screen, in Global properties.
- D. Jack must enable a dynamic-routing protocol, such as OSPF, on the Gateways.
- E. Jack must enable VPN Directional Match on the gateway object's VPN tab.

Answer: C

Reference: VPN.pdf page 145

QUESTION 9:

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 each QoS rule.

Answer: A

Reference: R60 CheckPointQoS.pdf page 94

QUESTION 10:

Certkiller is the Security Administrator for Certkiller .com. Certkiller .com FTP servers have old hardware and software. Certain FTP commands cause the FTP servers to malfunction. Upgrading the FTP Servers is not an option this time. Which of the following options will allow Certkiller to control which FTP commands pass through the Security Gateway protecting the FTP servers?

- A. Global Properties->Security Server ->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

Reference: Surf to that location in Smart Dashboard

QUESTION 11:

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>All-GwToGw
- B. Communities>Communities
- C. Internal_clear>External_Clear
- D. Internal_clear>Communities
- E. Internal_clear>All_communities

Answer: E

Explanation:

The ability to configure the directional match suggested in this question firstly depends on VPN Directional Match being enable in the Global Properties VPN Advanced screen. When this is enabled you have the Directional Match Condition available on the VPN column of the rule base (see screenshot).

'A' is not correct because you want traffic for all communities, not just the Gateway-to-Gateway traffic.

'B' is not a valid option.

'C' is not correct because you don't want a directional match for traffic outside the community.

'D' is not a valid option

'E' is a directional match for traffic between local domains within the community and all communities



Configurable Objects in a Direction

FIGURE 4-2 below lists all the objects that can be configured in a direction. This includes three new objects created for Directional VPN:

FIGURE 4-2 Objects List

Name of Object	Meaning
SiteToSiteVPN	Regular Star/Mesh Community
Remote_Access_Community	Remote Access community
Any Traffic	Any traffic
All_GwToGw	All Gateway to Gateway traffic
All_Communities	All communities (new object)
External_clear	For traffic outside the community
Internal_clear	For traffic between local domains within the community

QUESTION 12:

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?

- Highlight the suspicious connection in SmartView Tracker>Active mode. Block the connection using Tools>Block Intruder menu. Use the active mode to confirm that the suspicious connection does not reappear.
- 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 does not reappear.
- Highlight the suspicious connection in SmartView Tracker>Active mode. Block the connection using Tools>Block Intruder menu. Use the active mode to confirm that the suspicious connection is dropped.
- 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: C

Explanation:

Block Intruder

SmartView Tracker allows you to terminate an active connection and block further connections from and to specific IP addresses. Proceed as follows:

1Select the connection you wish to block by clicking it in the Active mode's Records pane.

2From the Tools menu, select Block Intruder.

The Block Intruder window is displayed.

3In Blocking Scope, select the connections that you would like to block:

Block all connections with the same source, destination and service - block the selected connection or any other connection with the same service, source or destination.

Block access from this source - block access from this source. Block all connections that are coming from the machine specified in the Source field.

Block access to this destination - block access to this destination. Block all connections that are headed to the machine specified in the Destination field.

4In Blocking Timeout, select one of the following:

Indefinite blocks all further access

For... minutes blocks all further access attempts for the specified number of minutes

5In Force this blocking, select one of the following:

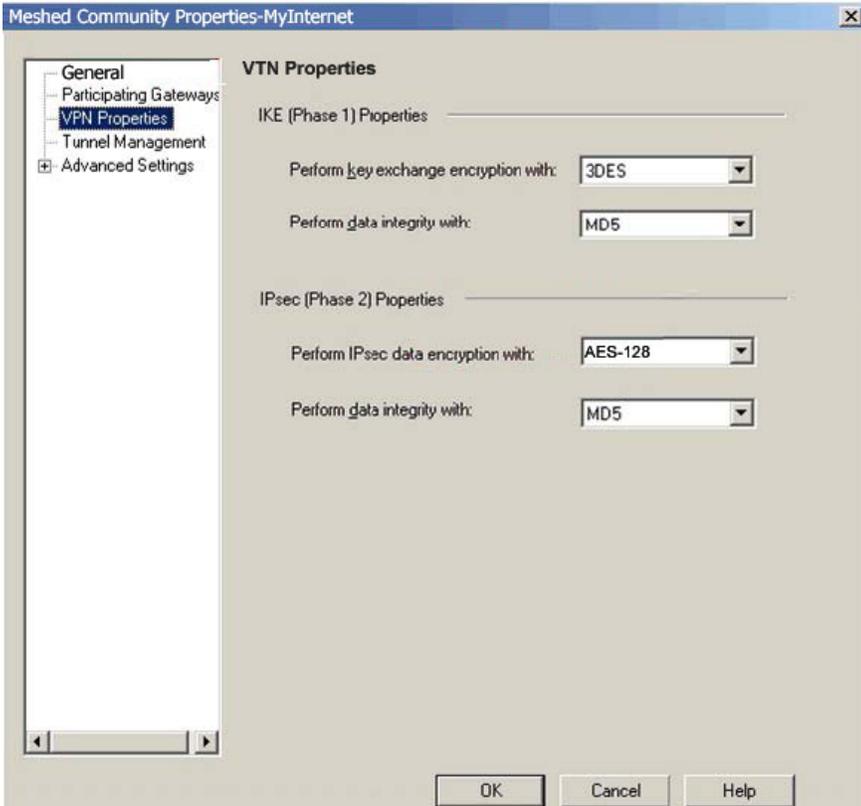
Only on... blocks access attempts through the indicated VPN-1 Pro module.

On any VPN-1 & FireWall-1 Module blocks access attempts through all VPN-1 Pro modules defined as gateways or hosts on the Log Server.

6Click OK.

QUESTION 13:

Exhibit:



Certkiller is using a mesh VPN Community to create a site-to-site VPN. The VPN properties in this mesh Community is displayed in the exhibit. Which of the following statements are true?

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

Answer: C

QUESTION 14:

Exhibit:



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

- A. Yes, these machines are configured correctly for a ClusterXL 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, al cluster must have an even number of machines.
- E. No, ClusterXL is not supported on Red Hat Linux.

Answer: C

Explanation:

Extract from Check Point Security Administration NGX II 1.1 Student Handbook page 436:

The following restrictions apply to Cluster XL configurations:

1. Only NGX Gateways running on the same operating system can be synchronized.
2. NGX Gateways must be on the same version and feature pack.
3. The Gateways must have the same Policy installed.
4. The SmartCenter Server of a ClusterXL Gateway cannot be running on the same host as a gateway cluster object (made up of a group of Gateways with many properties in common). A distributed environment is required.

QUESTION 15:

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?

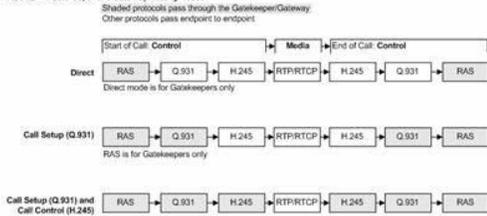
- A. Direct
- B. Direct and Call Setup
- C. Call Setup
- D. Call Setup and Call Control

Answer: A

Explanation:

From the help section:

FIGURE 1-4 Gatekeeper and Gateway Routing Modes



- **Direct** is for Gatekeepers only and not for Gateways. Only the RAS signals pass through the Gatekeeper. All other signalling (Q.931 and H.245) as well as the RTP/RTCP media passes directly endpoint to endpoint.
- **Call Setup (Q.931)** is where RAS (used only by Gatekeepers) and Q.931 pass through the Gatekeeper/Gateway. H.245 and the RTP/RTCP media pass endpoint to endpoint.
- **Call Setup (Q.931) and Call Control (H.245)** is where RAS (for a Gatekeeper only), Q.931 and H.245 pass through the Gatekeeper/Gateway. Only the RTP/RTCP media passes endpoint to endpoint.

Getting here - Manage > Network Objects > New > VoIP Domain > VoIP Domain H.323 Gatekeeper

QUESTION 16:

Certkiller is concerned that a denial-of-service (DoS) attack may affect her VPN Communities. She decides to implement IKE DoS protection. Jack needs to minimize the performance impact of implementing this new protection. Which of the following configurations is MOST appropriate for Mrs. Bill?

- Set Support IKE DoS protection from identified source to "Puzzles", and Support IKE DoS protection from unidentified source to "Stateless"
- Set Support IKE DoS protection from identified source, and Support IKE DoS protection from unidentified source to "Puzzles"
- Set Support IKE DoS protection from identified source to "Stateless", and Support IKE DoS protection from unidentified source to "Puzzles".
- Set Support IKE DoS protection from identified source, and "Support IKE DoS protection" from unidentified source to "Stateless".
- Set Support IKE DoS protection from identified source to "Stateless", and Support IKE DoS protection from unidentified source to "None".

Answer: D

Explanation:

From the online HELP for NGX R60, (see screen capture below)

The options for DOS on IKE for both identified and unidentified connections are...

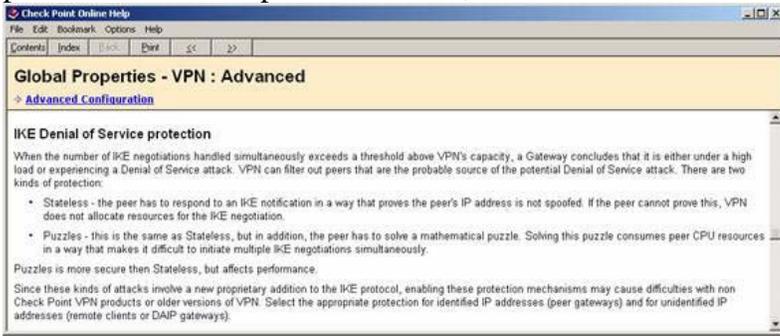
Puzzles - best protection, but performance intensive

Stateless - less protection, but not as performance intensive

None - no protection for DOS on IKE

Therefore, answer C will have impact on "unidentified" IKE connections. To provide

protection with less performance hit, use 'stateless' so answer D is correct, not C.



QUESTION 17:

You have a production implementation of Management High Availability, at Version VPN-1 NG with application Intelligence R55.

You must upgrade two SmartCenter Servers to VPN-1.

What is the correct procedure?

- A. 1. Synchronize the two SmartCenter 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 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: A

Explanation:

Management High Availability

Upgrade the Management High Availability Servers

- 1 Synchronize the Standby SmartCenter Servers (SCSs) with the Active SCS by selecting Synchronize in the Policy > Management High Availability window.
 - 2 Upgrade all the SCSs in the organization.
 - 3 Login to SmartDashboard via the Active SCS. For each Standby SCS, change the software version in Check Point Products listbox of its network objects window.
 - 4 Synchronize the Standby SCSs with the Active SCS. The synchronization status is expected to be collision. This occurs on account of the Upgrade operation.
 - 5 Make sure that you select the Active SCS as the dominant SCS, in order that all the Standby SCSs will be overwritten. Once again, synchronize the remaining Standby SCSs to the Active SCS.
- Not D: You can not sync NGX with NG.

QUESTION 18:

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 primary SmartCenter Server

Answer: E

QUESTION 19:

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 Key Revocation
- B. Perfect Forward Secrecy
- C. MD5 Hash Completion
- D. SH1 Hash Completion
- E. DES Key Reset

Answer: B

QUESTION 20:

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 21:

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

- A. Change the cluster mode to Unicast on the cluster object. Reinstall the Security Policy.
- B. Restart 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 projects. 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 22:

Certkiller is notified by blacklist.org that her site has been reported as a spam relay, due to her SMTP server being unprotected. Mrs. Bill 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 Jack's corporate domain.

Answer: E

Explanation:

The following screen shot is from the Check Point Secure knowledge base.

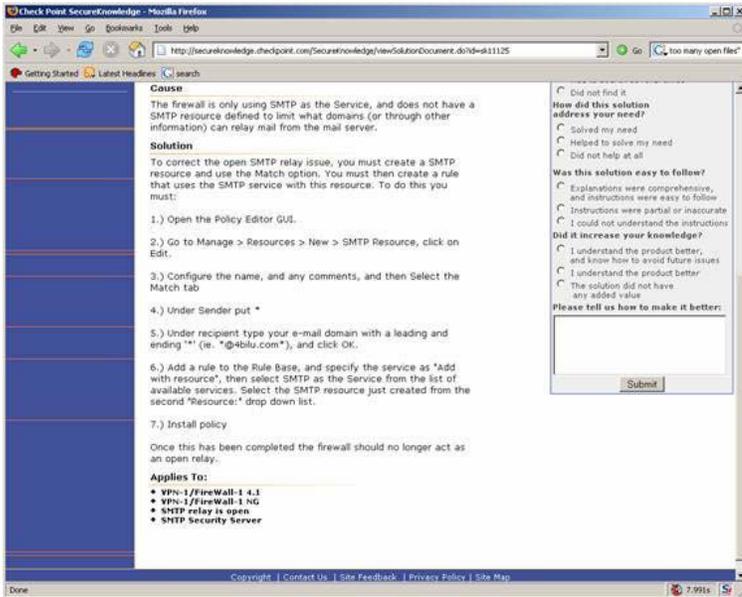
It states that

"To correct the open SMTP relay issue, you must create a SMTP resource and use the Match option. You must then create a rule that uses the SMTP service with this resource."

"Under recipient type your e-mail domain with a leading and ending '*' (ie. *@4bilu.com*), and click OK."

"Once this has been completed the firewall should no longer act as an open relay."

Therefore, you are using a match resource on the corporate domain, not filtering which makes the correct answer E.



QUESTION 23:

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 24:

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

A. The standard three-packet IKE Phase 1 exchange is replaced by a six-packet exchange.

B. The standard six-packet IKE Phase 2 exchange is replaced by a three-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 a twelve-packet exchange.

Answer: D

QUESTION 25:

Which of the following commands shows full synchronization status?

A. `cphaprob -i list`

B. `chpastop`

C. `fw ctl pstat`

D. `cphaprob -a if`

E. `fw hastat`

Answer: C

Explanation:

Monitoring Synchronization (`fw ctl pstat`)

To monitor the synchronization mechanism on ClusterXL or third-party OPSEC certified clustering products, run the following command on a cluster member:

The output of this command is a long list of statistics for the VPN-1 Pro Gateway. At

the end of the list there is a section called "Synchronization" that applies per Gateway Cluster member. Many of the statistics are counters that can only increase. A typical output is as follows:

The meaning of each line in this printout is explained below.

This line must appear if synchronization is configured. It indicates that new sync is working (as opposed to old sync from version 4.1).

If sync is unable to either send or receive packets, there is a problem. Sync may be temporarily unable to send or receive packets during boot, but this should not happen during normal operation. When performing full sync, sync packet reception may be interrupted.

fw ctl pstat

Version: new

Status: Able to Send/Receive sync packets

Sync packets sent:

total : 3976, retransmitted : 0, retrans reqs : 58, acks : 97

Sync packets received:

total : 4290, were queued : 58, dropped by net : 47

retrans reqs : 0, received 0 acks

retrans reqs for illegal seq : 0

Callback statistics: handled 3 cb, average delay : 1, max delay : 2

Delta Sync memory usage: currently using XX KB mem

Callback statistics: handled 322 cb, average delay : 2, max delay : 8

Number of Pending packets currently held: 1

Packets released due to timeout: 18

Version: new

Status: Able to Send/Receive sync packets

Sync packets sent:

total : 3976, retransmitted : 0, retrans reqs : 58, acks : 97

Monitoring Synchronization (fw ctl pstat)

90

The total number of sync packets sent is shown. Note that the total number of sync packets is non-zero and increasing.

The cluster member sends a retransmission request when a sync packet is received out of order. This number may increase when under load.

Acks are the acknowledgements sent for received sync packets, when an

acknowledgement was requested by another cluster member.

The total number of sync packets received is shown. The queued packets figure increases when a sync packet is received that complies with one of the following conditions:

1 The sync packet is received with a sequence number that does not follow the previously processed sync packet.

2 The sync packet is fragmented. This is done to solve MTU restrictions.

This figure never decreases. A non-zero value does not indicate a problem.

The dropped by net number may indicate network congestion. This number may increase slowly under load. If this number increases too fast, a networking error may interfere with the sync protocol. In that case, check the network.

This message refers to the number of received retransmission requests, in contrast to the transmitted retransmission requests in the section above. When this number grows very fast, it may indicate that the load on the machine is becoming too high for sync to handle.

Acks refer to the number of acknowledgements received for the "cb request" sync

packets, which are sync packets with requests for acknowledgments.

Retrans reqs for illegal seq displays the number of retransmission requests for

packets which are no longer in this member's possession. This may indicate a sync problem.

Callback statistics relate to received packets that involve Flush and Ack. This

statistic only appears for a non-zero value.

Sync packets received:

total : 4290, were queued : 58, dropped by net : 47

retrans reqs : 0, received 0 acks

retrans reqs for illegal seq : 0

Callback statistics: handled 3 cb, average delay : 1, max delay : 2

Starting the Cluster Member

Chapter 6 Monitoring and Troubleshooting Gateway Clusters 91

The callback average delay is how much the packet was delayed in this member until it was released when the member received an ACK from all the other members. The delay happens because packets are held until all other cluster members have acknowledged reception of that sync packet.

This figure is measured in terms of numbers of packets. Normally this number should be small (~1-5). Larger numbers may indicate an overload of sync traffic, which causes connections that require sync acknowledgements to suffer slight latency.

In a heavily loaded system, the cluster member may drop synchronization updates sent from another cluster member.

Delta Sync memory usage only appears for a non-zero value.

Delta sync requires

requires memory only while full sync is occurring. Full sync happens when the system goes up- after reboot for example. At other times, Delta sync requires no memory because Delta sync updates are applied immediately. For information about Delta sync

Number of Pending packets currently held only appears for a non-zero value.

ClusterXL prevents out-of-state packets in non-sticky connections. It does this by holding packets until a SYN-ACK is received from all other active cluster members. If for some reason a SYN-ACK is not received, VPN-1 Pro on the cluster member will

not release the packet, and the connection will not be established.
Packets released due to timeout only appears for a non-zero value. If the Number of Pending Packets is large (more than 100 pending packets), and the number of Packets released due to timeout is small, you should take action to reduce the number of pending packets.
dropped updates as a result of sync overload: 0
Delta Sync memory usage: currently using XX KB mem
Number of Pending packets currently held: 1
Packets released due to timeout: 18
Reference: R60 ClusterXL.pdf page 90

QUESTION 26:

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 27:

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 28:

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

- A. Dropped VoIP traffic is logged, but accepted VoIP traffic is not logged.
- B. VoIP protocol-specific log fields are not included in SmartView 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

Explanation:

Help file:

Logging Modifiers

- **Log every authenticated HTTP connection** specifies that a log entry should be generated for every authenticated HTTP connection.
- **Log VoIP connection** generates additional log entries for every VoIP connection. The additional log entries for SIP contain information about the user (SIP URL, for example, "fred@bloggs.com"). The additional log entries for H.323 contain information about the phone numbers.

Community Default Rule

- **Log Traffic** specifies whether or not to log traffic, by choosing either Log (the default setting) or None from the drop-down list.



Getting here - Policy > Global Properties > Log and Alert

QUESTION 29:

Exhibit:

```
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
```

The exhibit is a cphaprob state command output from a ClusterXL New mode high Availability member.

When a member 192.168.1.2 fails over and restarts, which member will become 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 30:

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

Point QoS?

- A. Turn "per rule guarantees" into "peer connection guarantees".
- B. Install Check Point QoS 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

Explanation:

The complete section 'Optimizing Check Point QOS' on page 402 of the NGX II 1.1 book states:

Check Point QoS performance can be improved by following the suggestions below:

- * Upgrade to the newest Check Point QoS version available
- * Install Check Point QoS only on the external interfaces of the QoS Module. Unless you are using limits for inbound traffic, installing Check Point QoS only in the outbound direction will provide you the most functionality and improvements.
- * Put more frequent rules at the top of your Rule Base. You can use SmartView Monitor to analyze how much a rule is used.
- * Turn per-connection limits into per-rule limits.
- **Turn per-connection guarantees into per-rule guarantees.

QUESTION 31:

How would you configure a rule in a Security Policy to allow SIP traffic from end point Net_A to 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/VoIP_any/accept
- D. Net_A/Net_B/VoIP /accept

Answer: A

Explanation:

SIP Based Communications without a Proxy

If the SIP environment does not include proxies, only one rule is require. To configure a Policy that will enable traffic from one SIP environment without a proxy to another, you must create a rule that allows the services sip or sip_any traffic from network object (or IP address range) to the other. The following Rule Base is an example of the configuration for this scenario:"

NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
VoIP Traffic SIP Rule	net_rome_VoIP	net_toronto_VoIP	Any Traffic	sip	accept	Log

Be aware that if the question mentioned a single proxy on one side of the transmission the rule would define a VoIP domain SIP object, for example:

NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
VoIP Traffic SIP Rule	net_rome_VoIP	toronto_SIP_VoIP	Any Traffic	UDP sip_any	accept	Log

If the question mentioned dual proxies, one on each side of the transmission the rule would look like this:

NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
VoIP Traffic SIP Rule	rome_SIP_VoIP	toronto_SIP_VoIP	Any Traffic	UDP sip_any	accept	Log

Reference: Check Point Security Administration NGX II 1.1, page 348

QUESTION 32:

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. Runt cpstop on one member, while leaving the other member running. Upgrade one member at a time, and reboot after upgrade.
4. Reinstasll 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 33:

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

- A. Run the command vpn tu on the Security Gateway, and choose the option "Delete all IPSec+IKE SAs for ALL peers and users".
- B. Run the command vpn 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 command vpn tu on the Security Gateway, and choose the option "Delete all IPSec SAs for ALL peers and users".

Answer: C

Explanation:

Not A: The question is how to tear down a specific VPN tunnel.

Reference. See Checkpoint PDF file named Checkpoint_NGX_CLI_Guide.pdf on page 129.

QUESTION 34:

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 agreements
- * 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 requirements?

A. Processor 1.1 GHz

RAM: 512 MB

Hard disk: 10 GB

OS: Windows 2000 Workstation

B. Processor 2.0 GHz

RAM: 512 MB

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 GHz

RAM: 256 MB

Hard disk: 20 GB

OS: Windows 2000 Server

Answer: E

QUESTION 35:

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 36:

Certkiller has configured a Common Internet File System (CIFS) resource to allow access to the public partition of Certkiller .com's file server, on \\ Certkiller 13\logigame\files\public. Mrs. Bill 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 37:

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

- A. The related end-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 38:

You have two Nokia Appliances: one IP530 and on IP380. Both appliances have

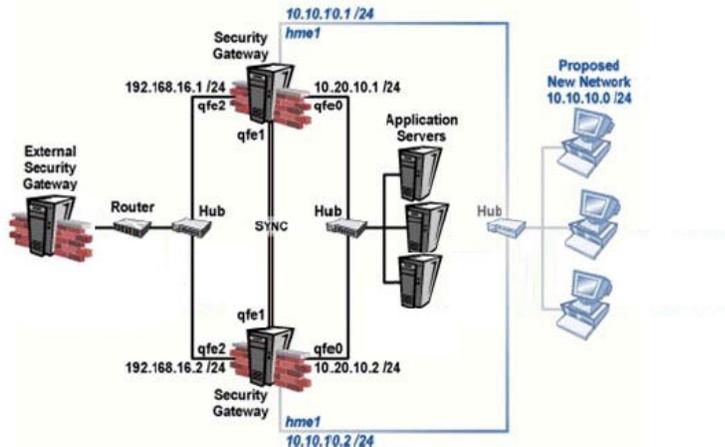
IPSO 3.9 and VPN-1 Pro NGX installed in a distributed deployment.
Can they be members of a gateway cluster?

- A. No, because the Gateway versions must 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 39:

Exhibit:



You work as a network administrator at Certkiller .com. Your network includes ClusterXL running Multicast mode on two members, as shown in this topology exhibit.

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 the ifconfig 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 via cpconfig.
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

Explanation: It looks like Solaris OS therefore should be ifconfig command not sysconfig.

QUESTION 40:

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: C

Explanation:

From the Help file:

Tell me about the fields...

Use sharing method based on

-IPs, Ports, SPIs (default) provides the best sharing distribution, and is recommended for use. It is the least "sticky" sharing configuration.

-IPs, Ports should be used only if problems arise when distributing IPSec packets to a few machines although they have the same source and destination IP addresses.

-IPs should be used only if problems arise when distributing IPSec packets or different port packets to a few machines although they have the same source and destination IP addresses. It is the most "sticky" sharing configuration, in other words, it increases the probability that a certain connection will pass through a single cluster member on both inbound and outbound directions.

Getting here - Gateway Cluster Properties > ClusterXL > Advanced

QUESTION 41:

Exhibit:

```
MEMBER Certkiller1:
HOST      NAME      ID      #VALS    #PEAK    #SLINKS
localhost connections 8158    1553     1560     800

[expert@ Certkiller2]# fw tab -t connections -s

MEMBER Certkiller2:
HOST      NAME      ID      #VALS    #PEAK    #SLINKS
localhost connections 8158    800      1001     800
```

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 exhibit is the fw tab -t connections -s output from both members.

Is State synchronization working properly between the two members?

- A. Members Certkiller 1 and Certkiller 2 are synchronized, because ID for both members are identical in the connection table
- B. The connections-table output is incomplete. You must run the cphaprob state command, to determine if members Certkiller 1 and Certkiller 2 are synchronized.
- C. Members Certkiller 1 and Certkiller 2 are not synchronized, because #PEAK for both members is not close in the connections table.
- D. Members Certkiller 1 and Certkiller 2 are synchronized, because #SLINKS are identical in the connections table.
- E. Members Certkiller 1 and Certkiller 2 are not synchronized, because #VALS in the connection table are not close.

Answer: E

Explanation:

Debugging State Synchronization

To monitor the synchronization mechanism on ClusterXL or third-party OPSEC certified clustering products, run the following commands on a cluster member.

FW TAB -T CONNECTIONS -S

One quick test to verify if State Synchronization is working properly is by running the fw tab -t connections -s command from cluster members. If the #VALS numbers are very close between cluster members, cluster members are synchronizing properly.

Here is a sample output of fw tab -t connections -s:

```
HOST NAME ID #VALS #PEAK #SLINKS
localhost connections 8158 4 22 4
```

If the #VALS numbers are very close between cluster members, it is safe to say State Synchronization is working properly.

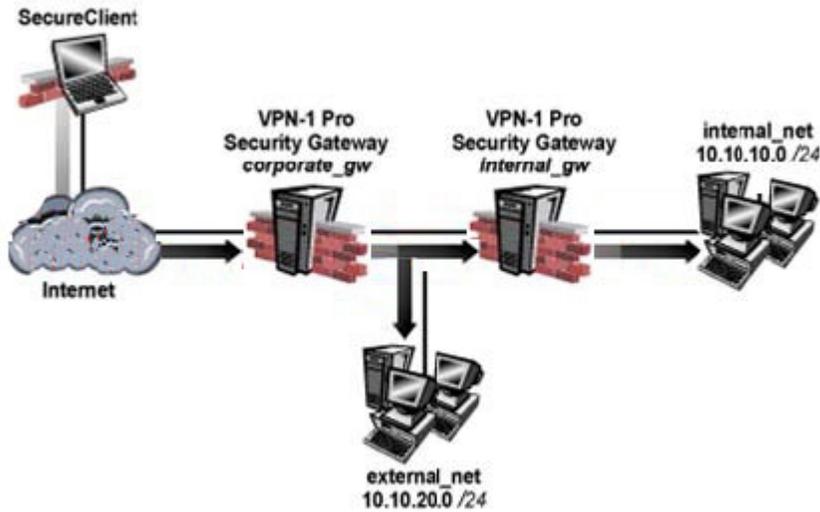
The key line is "If the #VALS numbers are very close between cluster members, it is safe to say State Synchronization is working properly."

Reference.

http://www.checkpoint.com/services/education/training/samples/ClusterXL_Sample_Chapter.pdf

QUESTION 42:

Exhibit:



The exhibit illustrates how a VPN-1 SecureClient user tries to establish a VPN host 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

Explanation:

For the remote-access client to make it through to the internal-net, he must first connect to the corporate_gw. From there, he must route and have access to talk with the internal_gw or he will never get into the internal net. Answer A does not include the internal_gw in the "external vpn domain", so the connection would never make it in! Just like the "internal gateway vpn domain" does NOT include the gateway protecting it, the "external gateway vpn domain" does not need the corporate_gw either.

QUESTION 43:

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

- A. The guarantee of a sub-rule cannot be greater than the guarantee defined for the rule

above it.

B. If the guarantee is defined in a sub-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 a QoS rule, the limit must be smaller than the guarantee.

Answer: E

QUESTION 44:

You plan to install a VPN-1 Pro Gateway for VPN-1 NGX at Certkiller .com's headquarters. You have a single Sun SPARC Solaris 9 machines 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 primary SmartCenter Server

B. Policy Server and primary SmartCenter Server

C. ClusterXL and SmartCenter Server

D. VPN-1 Pro Gateway

E. SmartCenter Server

Answer: A

QUESTION 45:

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 standby SmartCenter Server starts for the first time.

Answer: A

QUESTION 46:

Your primary SmartCenter Server is installed on a SecrePlatform 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 a spare machine. Add the new machine to the same network as the primary Server.

Answer: A

Explanation: Based on deploying a management HA, it has to be in a distributed environment so it seems answer "A" would be the answer.

QUESTION 47:

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

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

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

Certkiller 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

Explanation: A very good explanation to this exact scenario is given in the CheckPoint training manual Check Point Security Administration NGX II 1.1 (rev RSNGX001.1) on pages 121 and 122 in the section CVP inspection.

QUESTION 48:

You must set up SIP with 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 object:

- * Network object: SIP-net 172.16.100.0/24
 - * SIP-gateway: 172.16.100.100
 - * VoIP Domain Object: VoIP_domain_A
 1. End-point domain: SIP-net
 2. VoIP gateway installed at: SIP-gateway host object
- How should you configure the rule`?

- A. SIP-Gateway/Net_B/sip_any/accept
- B. VoIP_domain/Net_B/sip/accept
- C. SIP-Gateway/Net_B/sip/accept
- D. VoIP_domain_A/Net_B/sip_any; and sip/accept
- E. VoIP_Gateway_A/Net_B/sip_any/accept

Answer: A

Explanation:

Not E: VoIP_Gateway_A" is not actually referenced in the question.

QUESTION 49:

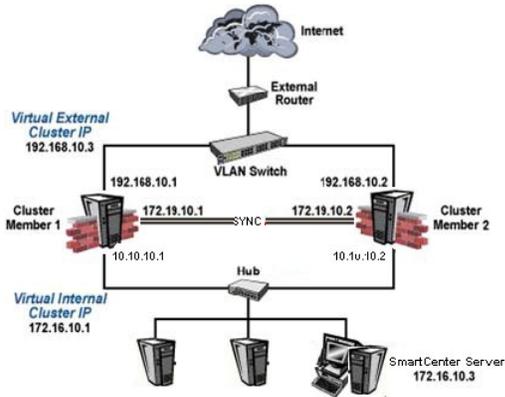
How does a standby SmartCenter Server receive logs from all Security Gateways, when an active SmartCenter Server fails over?

- A. The remote Gateways must set up SIC with the secondary SmartCenter 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 Server screen (from the Logs and Master 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 50:

Exhibit:



You are preparing a lab for a ClusterXL environment, with the topology shown in the exhibit.

- * Vip internal cluster IP = 172.16.10.1; Vip external cluster IP = 192.168.10.3
- * Cluster Member 1: four NICs, three enabled: qfe0: 192.168.10.1/24, qfe1: 10.10.10.1/24, qfe2: 172.16.10.1/24
- * Cluster Member 2: five NICs, three enabled: hme0: 192.168.10.2/24, eth1: 10.10.10.2/24, eth2: 172.16.10.2/24
- * Member Network tab on internal-cluster interfaces: 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 10.10.01.0 network. 172.19.10.0 is the synchronization network. What is the problem with this configuration?

- A. The SmartCenter Pro Server cannot be in synchronization network.
- B. There is no problem with 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 51:

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 new interface on each Gateway.

2. Remove the newly added network from the current VPN domain in 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 network to each peer's VTI interface..

C. 1. Add a new interface on each Gateway.

2. Add the newly added network into the existingVPN 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 existingVPN domain for each Gateway.

3. Create VTIs on each Gateway, 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

Answer: B

Explanation:

In the VPN NGX (R60) Route Based VPN Deployments Documentation (August 30,2005) on page 7 it states that

"The order between the two VPN routing methods is simply set by the order of the VPN routing decisions. First, the Domain Based VPN routing tables are consulted, to determine the proper origin and/or target VPN gateway for the traffic. If no Domain Based VPN routing applies, the IP routing table is consulted, to determine whether the traffic is routed through a VPN Tunnel Interface." (see screen print below)

For this reason, you must 'remove' the new network from the VPN domain or you will never be able to 'test' the route-based VPN feature. Secondly, you must add the static routes, (enabling advanced routing is only for dynamic routing) Therefore, answer C is incorrect and answer B is the correct answer.

Note: This assumes as the question states that the "newly added network" does not have

any VPN's currently running on it. VPN's not on this network will continue to run.

New VPN-1 Pro Concepts — Combining Route Based VPN and Domain Based VPN

Combining Route Based VPN and Domain Based VPN

It is important to note that Route Based VPN has not replaced Domain Based VPN or made it obsolete, but rather it expands the possibilities of configuring a VPN. In fact, the two methods can be used simultaneously. This is particularly useful during migration periods. The governing principal is that Domain Based VPN takes precedence over Route Based VPN. Consequently, whatever is routed into a certain IPsec tunnel based on Domain Based VPN configuration is not changed by the definition of Route Based VPN. In other words, routing through VPN Tunnel Interfaces can only apply to traffic that is not covered by the definition of VPN Domains, and that would otherwise go in the clear.

The order between the two VPN routing methods is simply set by the order of the VPN routing decisions. First, the Domain Based VPN routing tables are consulted, to determine the proper origin and/or target VPN gateway for the traffic. If no Domain Based VPN routing applies, the IP routing table is consulted, to determine whether the traffic is routed through a VPN Tunnel Interface.

For example, if two gateways have their respective VPN Domains defined, the two gateways will always route traffic between those VPN Domains through the community tunnel that connects between them, regardless of whether VPN Tunnel Interfaces were defined or not. Adding VPN Tunnel Interfaces can be used at first to serve additional traffic that is not handled by Domain Based VPN. This way, an OSPF daemon can be set up to work over a VPN Tunnel Interface while Domain Based VPN is still active. Since OSPF uses multicast for communication, it can only work with VPN Tunnel Interfaces. Once OSPF adjacency is established between the two gateways, routing information can be exchanged. After verifying that the routing information is correct, one could gradually remove parts of the VPN Domains definition, to allow Route Based VPN to take affect.

QUESTION 52:

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 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 53:

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 54:

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 55:

You plan to incorporate OPSEC servers, such as Websense and Trend Micro, to do content filtering.

Which segments 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

Explanation:

Deploying OPSEC Servers

OPSEC solutions, such as CVP and UFP servers are deployed on dedicated servers.

These servers are typically either placed in the DMZ, or on a private network segment.

This allows fast, secure connections between the CVP servers and the VPN-1 Pro Gateway.

Performing scanning at the network perimeter is both safer and more efficient than performing the scanning at the desktop or the application servers.

FTP, HTTP & SMTP servers are typically placed in the DMZ - Checkpoint help depicts dedicated subnet for CVP 7 UFP servers.

QUESTION 56:

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 exist to match the rejected traffic.
- B. The number of guaranteed connections is exceeded. The rule's 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's sub-rules exceeds the guarantee in the rule itself.

Answer: B

Explanation:

QoS rules with the track field set to Log can generate the following types of log events: QoS rejects a connection when the number of guaranteed connections is exceeded, and/or when the rule's action properties are not set to accept additional connections.
359, accel_ccse_ngx

QUESTION 57:

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

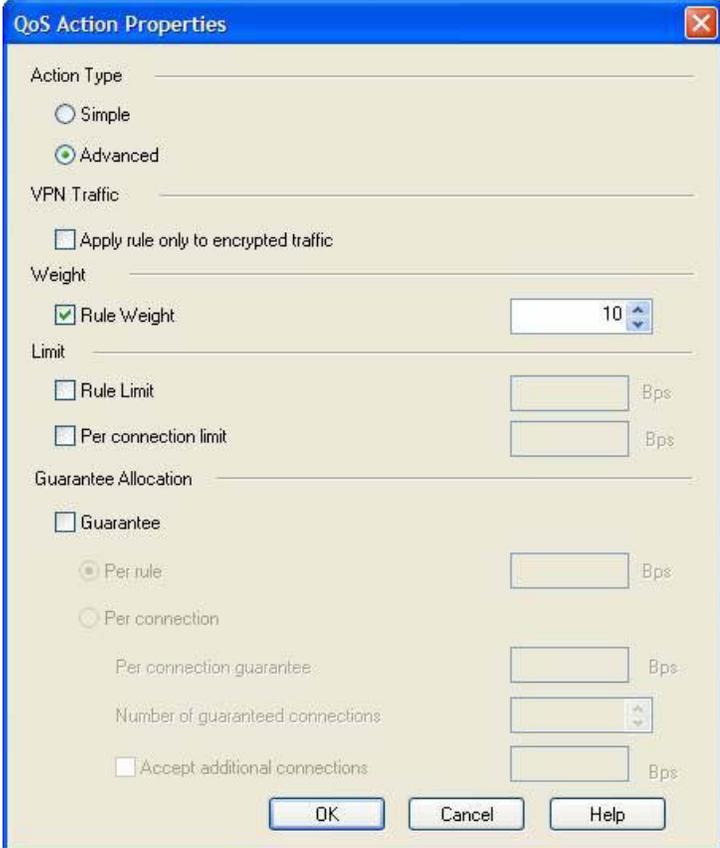
Answer: A

Explanation:

Create a new policy package and compare.
QOS Action Properties for QOS Express



QoS Action Properties for QoS Traditional



QUESTION 58:

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 59:

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 60:

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.

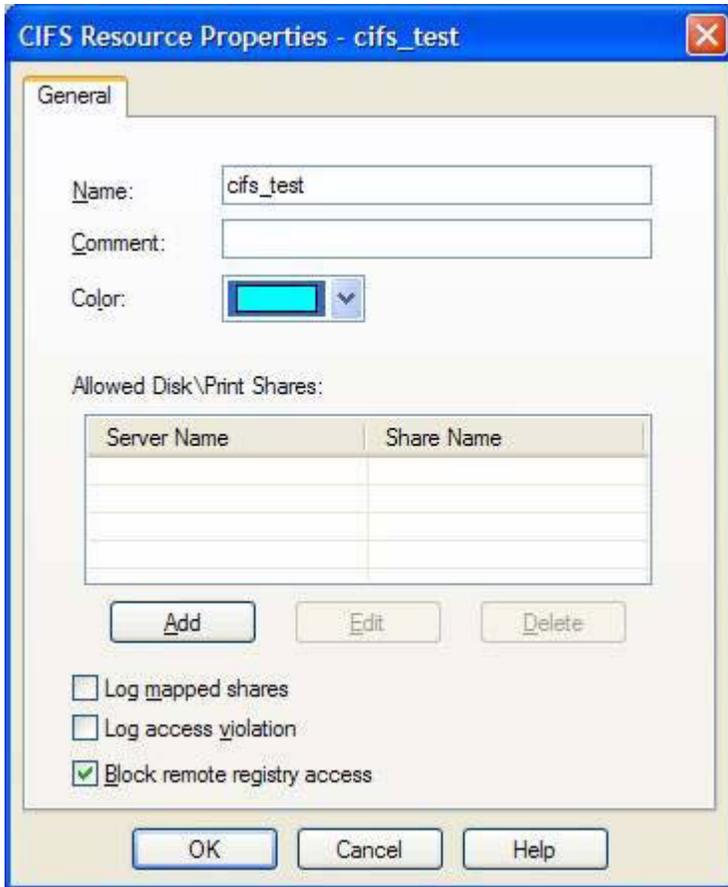
Which of the following services is NOT provided by a CIFS resource?

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

Answer: A

Explanation:

Create a new CIFS resource.



The other options are displayed in the screenshot.

QUESTION 61:

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. DiffServ rule
- C. Guaranteed per connection
- D. Weighted Fair Queuing
- E. Guaranteed per VoIP rule

Answer: A

Explanation:

In Check Points PDF CheckPoint_R61_QoS_UserGuide.pdf, on page 95, paragraph 4 it says "FloodGate-1 Low Latency Queuing makes it possible to define special Classes of Service for "delay sensitive" applications like voice and video."

This we believe indicates that Low Latency Classes is the best option.

QUESTION 62:

Certkiller is a Security Administrator preparing to implement a VPN solution for her multi-site organization Certkiller .com. To comply with industry regulations, Mrs. Bill'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 Jack 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 63:

Your current VPN-1 NG Application Intelligence (AI) 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 AI 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 NGX SmartCenter Server license, using the new machine's IP address. Request a new local license for the NGX VPN-1 Pro Gateway.
- B. Request a VPN-1 NGX SmartCenter Server license, using the new machine's IP address. Request a new central license for the NGX VPN-1 Pro Gateway.
- C. Request a new VPN-1 NGX SmartCenter Server license, using the NG with AI 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 AI SmartCenter Server IP address. Request a new central license for the NGX VPN-1 Pro Gateway, licenses for the existing SmartCenter Server IP address.

Answer: C

QUESTION 64:

Certkiller is a Security Administrator for Certkiller .com. Certkiller .com has two sites using pre-shared secrets in its VPN. The two sites are Boston and New York. Jack has just been informed that a new office is opening in Houston, and she 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 New York Security Gateway. Mrs. Bill decides to switch from a pre-shared secrets to Certificates issued by the Internal Certificate Authority (ICA). After creating the Houston gateway object with the proper VPN domain, what are Certkiller's remaining steps?

1. Disable "Pre-shared Secret" on the Boston and New York gateway objects.
2. Add the Houston gateway object into the New York and Boston's mesh VPN Community.
3. Manually generate ICA Certificates for all three Security Gateways.
4. Configure "Traditional mode VPN configuration" in the Houston 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: C

Explanation: VPN routing is done through simple vpns not traditional, therefore the answer is C.

QUESTION 65:

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

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

Answer: B

QUESTION 66:

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

Explanation:

Security	Authentication	Content Security
Telnet	Yes	No
rlogin	Yes	No
FTP	Yes	Yes
HTTP	Yes	Yes
SMTP	No	Yes

Reference: Page 105 of the Check Point Security Administration NGX II 1.1

QUESTION 67:

Certkiller .com has two headquarters, one in Los Angeles and one in Mumbai. Each headquarter includes several branch offices. The branch office only need to communicate with the headquarter 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?

VNP communities comprised of:

- A. two star and one mesh community; each start Community is set up for each site, with headquarter as the center of the Community, and branches as satellites. The mesh Communities are between Mumbai and Los Angeles headquarters.
- B. Three mesh Communities: one for Los Angeles and its branches, one for Mumbai headquarters and its branches, and one for Los Angeles and Mumbai headquarters.
- C. Two mesh Communities, one for each headquarters; and one start Community, in which Los Angeles is the center of the Community and Mumbai is the satellite.
- D. Two mesh Communities, one for each headquarters; and one start Community, in which Mumbai is the center of the Community and Los Angeles is the satellite.

Answer: A

QUESTION 68:

Certkiller wants to protect internal users from malicious Java code, but Jack does not want to strop Java scripts.

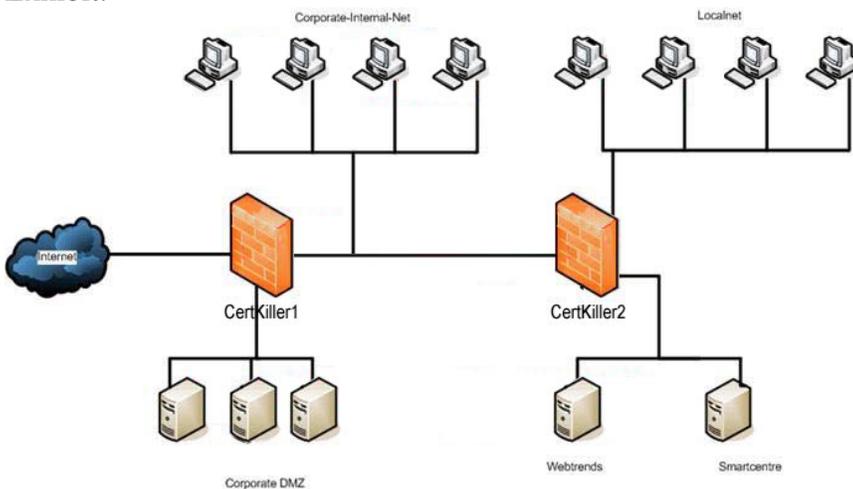
Which is the best configuration option?

- 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 strop ActiveX tags
- D. Use the URI resource to strop applet tags
- E. Use the URI resource to strop script tags

Answer: A

QUESTION 69:

Exhibit:



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 Certkiller 1 and Certkiller 2 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 the message "content security is not reachable".

What is the problem, and how do you fix it?

A. The connection from Certkiller 2 to the internal WebTrends server is not allowed in the Policy.

Fix: Add a rule in Certkiller 1's Policy to allow source WebTrendsServer, destination Certkiller 2, service TCP port 18182, and action accept.

B. The connection from Certkiller 2 to the WebTrends server is not allowed in the Policy.

Fix: Add a rule in Certkiller 2's Policy with Source Certkiller 2, destination WebTrends server, service TCP port 18182, and action accept.

C. The connection from Certkiller 1 to the internal WebTrends server is not allowed in the Policy.

Fix: Add a rule in Certkiller 2's Policy with source WebTrendsServer, destination

Certkiller 1, service TCP port 18182, and action accept.

D. The connection from Certkiller 1 to the internal WebTrends server is not allowed in the Policy.

Fix: Add a rule in Certkiller 2's Policy with source Certkiller 1, destination WebTrends server, service TCP port 18182, and action accept.

E. The connection from Certkiller 1 to the internal WebTrends server is not allowed in the Policy.

Fix: Add a rule in Certkiller 1's Policy to allow source Certkiller 1, destination WebTrends server, service TCP port 18182, and action accept.

Answer: B

Explanation:

Not C,D,E because the connection to WebTrends must get through FW named Certkiller 2.

No A because only FW named Certkiller 2 must have the rules enabled on.

You must add a rule as consequence of disabling Control connection in global Properties.

QUESTION 70:

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

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

Answer: A, C

QUESTION 71:

Which service type does NOT invoke a Security Server?

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

Answer: D

Explanation:

NGX II 1.1 book P/N 701768 page 105.

Telnet, rlogin, FTP, HTTP, SMTP are Security Servers. CIF is not.
Also on page 123 of NGX II 1.1 book P/N 701768 - the first line reads:
"CIFS resources do not invoke Security Servers"

QUESTION 72:

You have two Nokia Appliances one IP530 and one IP380. Both Appliances have IPSO 39 and VPN-1 Pro NGX installed in a distributed deployment Can they be members of a gateway cluster?

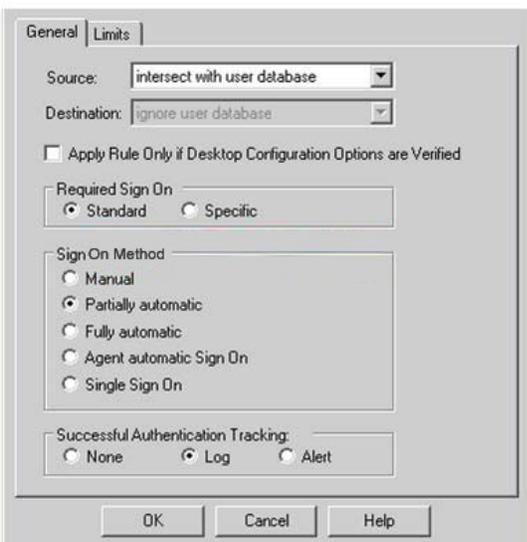
- A. No, because the Gateway versions must not be the same on both security gateways
- B. Yes, as long as they have the same IPSO version and the same VPN-1 Pro version
- C. No, because members of a security gateway cluster must be installed as stand-alone deployments
- D. Yes, because both gateways 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 IP530orIP380.)

Answer: B

QUESTION 73:

Review the following rules and note the Client Authentication Action properties screen, as shown in the exhibit.

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1		Customers@Any	* Any	* Any Traffic	TCP http TCP ftp TCP telnet	Client Auth	Log
2		* Any	* Any	* Any Traffic	* Any	drop	Log



After being authenticated by the Security Gateway when a user starts an HTTP connection to a Web site the user tries to FTP to another site using the command

line. What happens to the user?
The....

- A. FTP session is dropped by the implicit Cleanup Rule.
- B. User is prompted from the FTP site only, and does not need to enter username and password for the Client Authentication.
- C. FTP connection is dropped by rule 2.
- D. FTP data connection is dropped, after the user is authenticated successfully.
- E. User is prompted for authentication by the Security Gateway again.

Answer: B

QUESTION 74:

What is the command to see the licenses of the Security Gateway Certkiller from your SmartCenter Server?

- A. print Certkiller
- B. fw licprint Certkiller
- C. fw tab -t fwlic Certkiller
- D. cplic print Certkiller
- E. fw lic print Certkiller

Answer: D

Explanation:

cplic print - prints details of Check Point licenses on the local machine. On a Module, this command will print all licenses that are installed on the local machine - both Local and Central licenses.

P456, .

NG COMMAND LINE INTERFACE

Advanced Technical Reference Guide - NG FP3

QUESTION 75:

Ophelia is the security Administrator for a shipping company. Her company uses a custom application to update the distribution database. The custom application includes a service used only to notify remote sites that the distribution database is malfunctioning. The perimeter Security Gateways Rule Base includes a rule to accept this traffic. Ophelia needs to be notified, via a text message to her cellular phone, whenever traffic is accepted on this rule. Which of the following options is MOST appropriate for Ophelia's requirement?

- A. User-defined alert script
- B. Logging implied rules
- C. SmartViewMonitor

- D. Pop-up API
- E. SNMP trap

Answer: A

QUESTION 76:

Choose the BEST sequence for configuring user management on SmartDashboard, for use with an LDAP server:

- A. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP server using an OPSEC application.
- B. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object.
- C. Enable LDAP in Global Properties, configure a host-node object for the LDAP Server, and configure a server object for the LDAP Account Unit.
- D. Configure a server object for the LDAP Account Unit, and create an LDAP resource object.
- E. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties.

Answer: C

Explanation:

'A' is incorrect because you do not create an LDAP Server using an OPSEC Application. The LDAP server is a host node. Also not that the question asks for the BEST sequence. Logically, the first thing to do when configuring LDAP is to enable it in Global Properties.

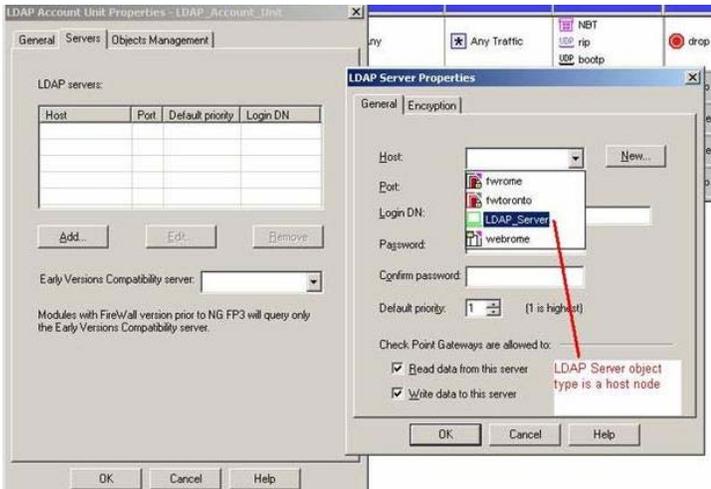
'B' is incorrect because you cannot create an LDAP Resource Object.

'C' is correct. Logic says you enable LDAP in Global Properties first, then create the host node that will be defined on the LDAP Account Unit properties window as the LDAP Server and then create the LDAP Account unit as a Server object not an OPSEC Application. See screenshot.

'D' is incorrect because you cannot create an LDAP Resource Object.

'E' is incorrect because Workstation is not the correct object name for an LDAP server, it is a host

node.



QUESTION 77:

Which of the following is the final step in an NGXbackup?

- A. Test restoration in a non-production environment, using the upgrade_import command
- B. Move the *.tgz file to another location
- C. Run the upgrade_export command
- D. Copy the conf directory to another location
- E. Run the cpstop command

Answer: B

Explanation:

In a production environment, copy this file to a safe off-site archive, and destroy the original.

427, Check Point Security Administration NGX I Student Handbook

QUESTION 78:

Which mechanism is used to export Check Point logs to third party applications?

- A. OPSE
- B. CPLogManager
- C. LEA
- D. SmartViewTracker
- E. ELA

Answer: C

Explanation; Check Point has made an API (Application Programming Interface) available for these companies to use to communicate with Check Point's product line. The

SDK (Software Development Kit) requires knowledge of the C programming language. The SDK contains software to integrate with the following interfaces:

- ? CVP The Content Vectoring Protocol allows antivirus solutions to talk to FireWall-1.
- ? UFP The URI Filtering Protocol allows Web filtering to integrate.
- ? LEA The Log Export API enables you to export log files to third-party log servers.
- ? ELA The Event Logging API allows Check Point to receive logs from third-party software.

338, Configuring Check Point NGX VPN-1/FireWall-1, Syngress, 1597490318

QUESTION 79:

In NGX, what happens if a Distinguished Name (ON) is NOT found in LADP?

- A. NGX takes the common-name value from the Certificate subject, and searches the LADP account unit for a matching user id
- B. NGX searches the internal database for the username
- C. The Security Gateway uses the subject of the Certificate as the ON for the initial lookup
- D. If the first request fails or if branches do not match, NGX tries to map the identity to the user id attribute
- E. When users authenticate with valid Certificates, the Security Gateway tries to map the identities with users registered in the external LADP user database

Answer: D

Explanation:

Retrieving Information from a SmartDirectory (LDAP) server

When a Gateway requires user information for authentication purposes, it searches for this information in three different places:

- 1 The first place that is queried is the internal users database.
- 2 If the specified user is not defined in this database, the Gateway queries the SmartDirectory (LDAP) servers defined in the Account Unit one at a time, and according to their priority. If for some reason the query against a specified SmartDirectory (LDAP) server fails, for instance the SmartDirectory (LDAP) connection is lost, the SmartDirectory (LDAP) server with the next highest priority is queried. If there is more than one Account Unit, the Account Units are queried concurrently. The results of the query are either taken from the first Account Unit to meet the conditions, or from all the Account Units which meet the conditions. The choice between taking the result of one Account Unit as opposed to many is a matter of Gateway configuration.
- 3 If the information still cannot be found, the Gateway uses the external users template to see if there is a match against the generic profile. This generic profile has the default attributes applied to the specified user.

QUESTION 80:

Which command allows you to view the contents of an NGX table?

- A. fw tab -s <tablename>-
- B. fw tab -t <tablename>-
- C. fw tab -u <tablename>-
- D. fw tab -a <tablename>-
- E. fw tab -x <tablename>-

Answer: B

QUESTION 81:

Jack's project is to define the backup and restore section of his organization's disaster recovery plan for his organization's distributed NGX installation. Jack must meet the following required and desired objectives.

- * Required Objective The security policy repository must be backed up no less frequent~ than every 24 hours
 - * Desired Objective The NGX components that enforce the Security Policies should be backed up no less frequently than once a week
 - * Desired Objective Back up NGX logs no less frequently than once a week
- Jack's disaster recovery plan is as follows. See exhibit.

1. Use the cron utility to run the upgrade export command each night on the SmartCenter Servers. Configure the organization's routine backup to back up the files created by the upgrade export command
2. Configure the SecurePlatform backup utility to backup the SecurityGateways every Saturday night
3. Use the cron utility to run the upgrade export command each Saturday night on the Log Servers. Configure an automatic, nightly logswitch. Configure the organization's routine backup software to backup the switched logs every night

Jack's plan:

- A. Meets the required objective but does not meet either desired objective
- B. Does not meet the required objective
- C. Meets the required objective and only one desired objective
- D. Meets the required objective and both desired objectives

Answer: D

Explanation: Logs can be viewed after exported.

QUESTION 82:

The following is cphaprobstate command output from a New Mode High Availability cluster member:

Number	Unique IP Addresses	Assigned Load	State
1 <local>	192.168.1.1	0%	down
2	192.168.1.2	100%	active

Which 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 83:

What do you use to view an NGX Security Gateway's status, including CPU use, amount of virtual memory, percent of free hard-disk space, and version?

- A. SmartLSM
- B. SmartViewTracker
- C. SmartUpdate
- D. SmartViewMonitor
- E. SmartViewStatus

Answer: D

QUESTION 84:

Which of the following commands is used to restore NGX configuration information?

- A. cpcontig
- B. cpinfo-i
- C. restore
- D. fwm dbimport
- E. upgrade_import

Answer: E

QUESTION 85:

Eric wants to see all URLs' full destination path in the SmartView Tracker logs, not just the fully qualified domain name of the web servers. For Example, the information field of a log entry displays the URL <http://hp.msn.com/css/home/hpcl1012.css>. How can Eric best customize SmartView Tracker to see the logs he wants? Configure the URI resource, and select

- A. "transparent" as the connection method
- B. "tunneling" as the connection method
- C. "optimize URL logging"; use the URI resource in the rule, with action "accept"
- D. "Enforce URI capability"; use the URI resource in the rule, with action "accept"

Answer: C

QUESTION 86:

Which of the following commands shows full synchronization status?

- A. cphaprob -i list
- B. cphastop
- C. fw ctl pstat
- D. cphaprob -a if
- E. fw hastat

Answer: C

QUESTION 87:

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 88:

If you are experiencing LDAP issues, which of the following should you check?

- A. Secure Internal Communications(SIC)
- B. VPN tunneling
- C. Overlapping VPN Domains
- D. NGX connectivity
- E. VPN Load Balancing

Answer: D

QUESTION 89:

How can you reset the password of the Security Administrator, which was created during initial installation of the SmartCenter Server on SecurePlatform?

- A. Launch cpcontig and select "Administrators"
- B. Launch SmartDashboard, click the admin user account, and overwrite the existing

Check Point Password

- C. Type `cpm -a`, and provide the existing administration account name. Reset the Security Administrator's password
- D. Export the user database into an ASCII file with `fwm dbexport`. Open this file with an editor, and delete the "Password" portion of the file Then log in to the account without password. You will be prompted to assign a new password
- E. Launch `cpconfig` and delete the Administrator's account. Recreate the account with the same name

Answer: E

Explanation:

We have validated that Administrator account created during initial installation can not be managed by SmartDashboard.



This is the account we have created during installation.
The only way you can reset the password following instruction on answer E.

QUESTION 90:

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

- A. IPS0 3.9
- B. Windows XP SP2
- C. Windows 2000 Professional
- D. RedHat Linux 7 0
- E. MacOS X

Answer: A

QUESTION 91:

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

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

Answer: D

QUESTION 92:

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. On~ the patch utility is upgraded using this command
- E. Only the OS

Answer: B

QUESTION 93:

Amanda is compiling traffic statistics for Certkiller .com's Internet activity during production hours. How could she use SmartView Monitor to find this information?
By

- A. using the "Traffic Counters" settings and SmartView Monitor to generate a graph showing the total HTTP traffic for the day
- B. -monitoring each specific user's Web traffic use.
- C. Viewing total packets passed through the Security Gateway
- D. selecting the "Tunnels" view, and generating a report on the statistics
- E. configuring a Suspicious Activity Rule which triggers an alert when HTTP traffic passes through the Gateway

Answer: A

QUESTION 94:

A Security Administrator is notified that some long-lasting Telnet connections to a mainframe are dropped every time after an hour. The Administrator suspect that the the Security Gateway might be blocking these connections. As she reviews the Smart Tracker the Administrator sees the packet is dropped with the error "Unknown established connection". How can she resolve this problem without

causing other security issues?

Choose the BEST answer. She can:

- A. increase the session time-out in the mainframe's Object Properties
- B. create a new TCP service object on port 23, and increase the session time-out for this object She only uses this new object in the rule that allows the Telnet connections to the mainframe
- C. increase the session time-out in the Service Properties of the Telnet service
- D. increase the session time-out in the Global Properties
- E. ask the mainframe users to reconnect every time this error occurs

Answer: B

Explanation; It is better to change the "Session Timeout" for a specific service than to set it globally for ALL Services.

Checkpoint KBase:

To specify a timeout for a TCP service that is different from the global TCP timeout (defined in the Stateful Inspection page of the Global Properties window), proceed as follows:

1. Open the TCP Service Properties window for the specific service.
2. Click "Advanced".
3. In the Advanced TCP Service Properties window, select "Other".
4. Specify the timeout.
5. Install the policy.

QUESTION 95:

Certkiller is the Security Administrator for a software-development company. To isolate the corporate network from the developer's network, Certkiller installs an internal Security Gateway. Jack wants to optimize the performance of this Gateway. Which of the following actions is most likely to improve the Gateway's performance?

- A. Remove unused Security Policies from Policy Packages
- B. Clear all Global Properties check boxes, and use explicit rules
- C. Use groups within groups in the manual NAT Rule Base
- D. Put the least-used rules at the top of the Rule Base
- E. Use domain objects in rules, where possible

Answer: A

QUESTION 96:

Certkiller is the Security Administrator for a chain of grocery stores. Each grocery store is protected by a Security Gateway. Certkiller is generating a report for the information-technology audit department. The report must include the name of the Security Policy installed on each remote Security Gateway, the date and time the

Security Policy was installed, and general performance statistics (CPU Use, average CPU time, active real memory, etc.).

Which SmartConsole application should Certkiller use to gather this information?

- A. SmartUpdate
- B. SmartView Status
- C. SmartView Tracker
- D. SmartLSM
- E. SmartView Monitor

Answer: E

QUESTION 97:

How can you reset Secure Internal Communications (SIC) between a SmartCenter Server and Security Gateway?

- A. Run the command `fwm sic_reset` to reinitialize the Internal Certificate Authority (ICA) of the SmartCenter Server. Then retype the activation key on the Security-Gateway from SmartDashboard
- B. From `cpconfig` on the SmartCenter Server, choose the Secure Internal Communication option and retype the activation key Next, retype the same key in the gateway object in SmartDashboard and reinitialize Secure Internal Communications (SIC)
- C. From the SmartCenter Server's command line type `fw putkey -p <shared key>- <IP Address of SmartCenter Server>-`.
- D. From the SmartCenter Server's command line type `fw putkey -p <shared key>- <IP Address of security Gateway>-`.
- E. Re-install the Security Gateway

Answer: B

QUESTION 98:

Which NGX feature or command allows Security Administrators to revert to earlier versions of the Security Policy without changing object configurations?

- A. `upgrade_export/upgrade_import`
- B. Policy Package management
- C. `fwm dbexport/fwm dbimport`
- D. `cpconfig`
- E. Database Revision Control

Answer: B

QUESTION 99:

Certkiller is the Security Administrator for Certkiller .com's large geographically distributed network. The internet connection at one of her remote sites failed during the weekend, and the Security Gateway logged locally for over 48 hours. Certkiller is concerned that the logs may have consumed most of the free space on the Gateway's hard disk.

Which SmartConsole application should Certkiller use, to view the percent of free hard-disk space on the remote Security Gateway?

- A. SmartView Status
- B. SmartView Tracker
- C. SmartUpdate
- D. SmartView Monitor
- E. SmartLSM

Answer: D

QUESTION 100:

What is a Consolidation Policy?

- A. The collective name of the Security Policy, Address Translation, and SmartDefense Policies
- B. The specific Policy used by Eventia Reporter to configure log-management practices
- C. The state of the Policy once installed on a Security Gateway
- D. A Policy created by Eventia Reporter to generate logs
- E. The collective name of the logs generated by Eventia Reporter

Answer: B

QUESTION 101:

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

- A. Change the cluster mode to Unicast 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 reenable 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