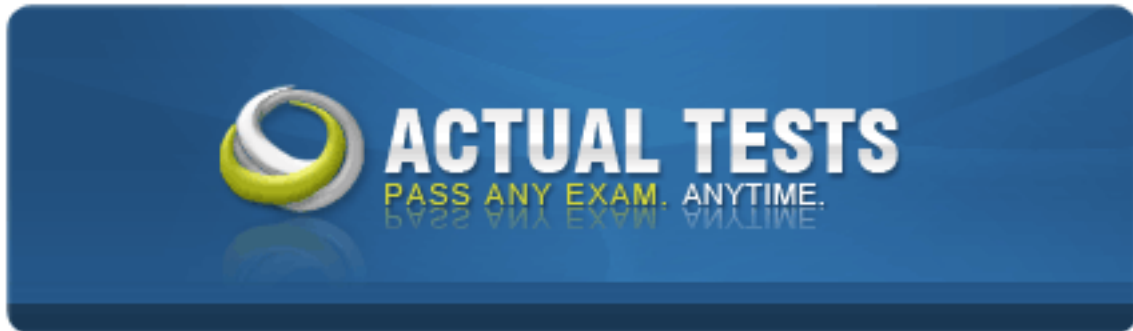


Checkpoint 156-915



156-915 Accelerated CCSE NGX (156-915.1)

Practice Test

Version 1.8

QUESTION NO: 1

When restoring NGX using the upgrade import command, which of the following items are NOT restored?

- A. Security Policies
- B. Global properties
- C. Licenses
- D. User groups
- E. Route tables

Answer: E

QUESTION NO: 2

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

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

Answer: D

QUESTION NO: 3

Your organization's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. How would you request and apply the license? Request a central license:

- A. using the remote Gateway's IP address. Apply the license locally with the cplic put command.
- B. for the Gateways' IP address. Apply the license on the Smart Center Server with the cprlic put command.
- C. using the remote Gateway's IP address. Attach the license to the remote Gateway via Smart Update.
- D. using your Smart Center Server's IP address. Attach the license to the remote Gateway via Smart Update

E. using the Smart Center Server's IP address. Apply the license locally on the remote Gateway with the cplic put command.

Answer: D

QUESTION NO: 4

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

Answer: B

QUESTION NO: 5

Eric wants to see all URLs' full destination paths in the Smart View Tracker logs, not just the fully qualified domain name of the Web servers. For example, the information filed of a log entry displays the URL `http://hp.msn.com/css/home/hpcl1012.css`. How can Eric best customize Smart View 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 URL capability"; use the URI resource in the rule, with action "accept"

Answer: C

QUESTION NO: 6

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



- A. Steve must enable `directional_match(true)` in the `objectes_5_0.C` file on Smart Center Server.
- B. Steve must enable Advanced Routing on each Security Gateway.
- C. Steve must enable VPN Directional Match on the VPN Advanced screen, in Global properties.
- D. Steve must enable a dynamic-routing protocol, such as OSPF, on the Gateways.
- E. Steve must enable VPN Directional Match on the gateway object's VPN tab.

Answer: C

QUESTION NO: 7

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

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

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

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

Answer: E

QUESTION NO: 8

After importing the NGX schema into an LDAP server, what should you enable? Schema checking

- A. Encryption
- B. User Authority
- C. Connect Control
- D. Secure Internal Communications

Answer: A

QUESTION NO: 9

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

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

Answer: A

QUESTION NO: 10

How can you unlock an administrator's account, which was been locked due to SmartCenter Access settings in Global Properties?

- A. Type `fwm lock_admin -ua` from the command line of the Smart Center Server.
- B. Clear the "locked" box of the user's General Properties in Smart Dashboard.
- C. Type `fwm unlock_admin -ua` from the command line of the Smart Center Server
- D. Type `fwm unlock_admin -ua` from the command line of the Security Gateway.
- E. Delete the file `admin.lock` in the `$FWDIR/tmp/directory` of the Smart Center Server.

Answer: A

QUESTION NO: 11

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

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

Answer: B

QUESTION NO: 12

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

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

E. An object to represent the call manager. AND an object to represent the host on which the transmission router is installed.

Answer: C

QUESTION NO: 13

In Smart View Tracker, which rule shows when a packet is dropped due to anti-spoofing?

- A. Rule 0
- B. Cleanup Rule
- C. Rule 1
- D. Rule 999
- E. Stealth Rule

Answer: A

QUESTION NO: 14

Your NGX Enterprise Smart Center Server is working normally. However, you must reinstall the Smart Center Server, but keep the Smart Center Server configuration (for example, all Security Policies, database, etc.) How would you reinstall the Server and keep its configuration?

- A. 1 .Run the latest upgrade_export utility to export the configuration 2.Keep the exported file in the same location. 3.Use Smart Update to reinstall the Smart Center Server. 4.Run upgrade import to import the configuration.
- B. 1 .Run the latest upgrade_export utility to export the configuration 2.Leave the exported, tgzfile in \$ FWDIR.
3.Install the primary Smart Center Server on top of the configuration 4.Run upgrade import to import the configuration.
- C. 1. Insert the NGX CD-ROM, and select the option to export the configuration into a.tgzfile
2. Transfer the .tgzfiel to another networked maching.
3. Uninstall all NGX packages, and reboot.
4. Use the NGX CD-ROM to select the upgrade import option to import the configuration.
- D. 1. Download the latest upgrade_export utility, and run it from \$FWDIR\bin to export the confirguration into a.tgzfile.
2. Transfer the .tgzfile to another network machine.
3. Uninstall all NGX packages and reboot.
4. Install a new primary Smart Center Server.
5. Run upgrade import to import the configuration

Answer: D

QUESTION NO: 15

Jeremy manages sites in Tokyo, Calcutta and Dallas, from his office in Chicago. He is trying to create a report for management, detailing the current software level of each Security Gateway. He also wants to create a proposal outline, listing the most cost-effective way to upgrade his Gateways. Which two Smart Console applications should Jeremy use, to create his report and outline?

- A. Smart LSM and Smart Update
- B. Smart Dashboard and Smart LSM
- C. Smart Dashboard and Smart View Tracker
- D. Smart View Monitor and Smart Update
- E. Smart View Tracker and Smart View Monitor

Answer: D

QUESTION NO: 16

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

- A. From the SmartCenter Server's command line type `fw putkey-p <shared key> <IP Address of SmartCenter Server>`.
- B. From the SmartCenter Server's command line type `fw putkey-p <shared key> <IP Address of Security Gateway>`.
- C. 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 Smart Dashboard.
- D. From `cpconfig` on the Smart Center Server, choose the Secure Internal Communication option and retype the activation key. Next, retype the same key in the gateway object in Smart Dashboard and reinitialize Secure Internal Communications (SIC).
- E. Use Smart Update to retype the activation key of the Security Gateway.

Answer: D

QUESTION NO: 17

Select the correct statement about Secure Internal Communications (SIC) Certificates? SIC Certificates:

- A. for NGX Security Gateways are created during the SmartCenter Server installation.
- B. for the SmartCenter Server are created during the SmartCenter Server installation
- C. are used for securing internal network communications between the SmartView Tracker and an OPSEC device.
- D. decrease network security by securing administrative communication among the SmartCenter Servers and the Security Gateway.
- E. uniquely identify Check Point enable machines; they have the same function as Authentication Certificates.

Answer: B

QUESTION NO: 18

Nelson is a consultant. He is at a customer's site reviewing configuration and logs as part of a security audit. Nelson sees logs accepting POP3 traffic, but he does not see a rule allowing POP3 traffic in the Rule Base.

Which of the following is the most likely cause? The POP3:

- A. service is a VPN-1 Control Connection
- B. rule is hidden
- C. service is accepted in Global Properties
- D. service cannot be controlled by NGX
- E. rule is disabled

Answer: B

QUESTION NO: 19

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

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

Answer: D

QUESTION NO: 20

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

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

Answer: D

QUESTION NO: 21

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. interna_clear > All_GwToGw
- B. Communities > Communities
- C. Internal_clear > External_Clear
- D. Internal_clear > Communities
- E. internal clear>All communities

Answer: E

QUESTION NO: 22

How do you view a Security Administrator's activities, using Smart Console tools? With:

- A. User Monitor
- B. Smart View Monitor using the Administrator Activity filter
- C. Smart View Tracker in Log mode
- D. Smart View Tracker in Audit mode
- E. Smart View Status

Answer: D

QUESTION NO: 23

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: A

QUESTION NO: 24

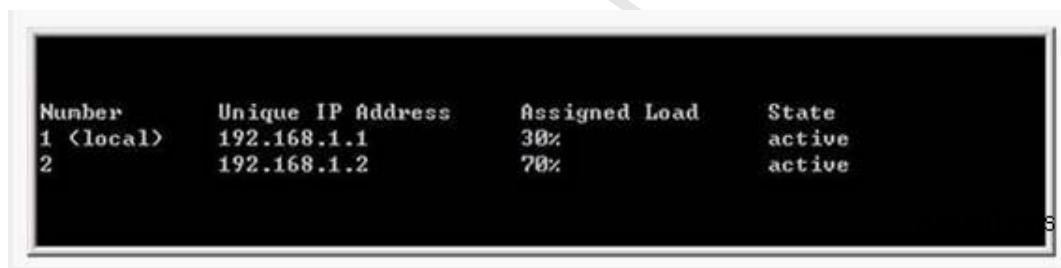
Which operating system is not supported by VPN-1 Secure Client?

- A. IPSO 3.9
- B. Windows XP SP2
- C. Windows 2000 Professional
- D. RedHat Linux 7.0
- E. MacOSX

Answer: A

QUESTION NO: 25

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



```
Number      Unique IP Address  Assigned Load  State
1 <local>    192.168.1.1       30%           active
2           192.168.1.2       70%           active
```

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

Answer: C

QUESTION NO: 26

You want to establish a VPN, using Certificates. Your VPN will exchange Certificates with an external partner.

Which of the following activities should you do first?

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

Answer: E

QUESTION NO: 27

Your SmartCenter Server fails and does not reboot. One of your remote Security Gateways managed by the SmartCenter Server reboots. What happens to that remote Gateway after reboot?

- A. Since the SmartCenter Server is not available, the remote Gateway cannot fetch the Security Policy. Therefore, no traffic is allowed through the Gateway.
- B. Since the SmartCenter Server is not available, the remote Gateway cannot fetch the Security Policy. Therefore, all traffic is allowed through the Gateway.
- C. The remote Gateway fetches the last installed Security Policy locally, and passes traffic normally. The Gateway will log locally, since the SmartCenter Server is not available.
- D. Since the SmartCenter Server is not available to the remote Gateway, fetching the Security Policy and logging will both fail.
- E. Since the SmartCenter Server is not available, the remote Gateway uses the local Security Policy, but does not log traffic.

Answer: C

QUESTION NO: 28

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

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

Answer: B

QUESTION NO: 29

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

```
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
```

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

Answer: B

QUESTION NO: 30

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

- A. OPSE
- B. CPLogManager
- C. LEA
- D. Smart View Tracker
- E. ELA

Answer: C

QUESTION NO: 31

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



```
Command Prompt
C:> arp -

Interface: 10.4.8.108 on Interface 0x4

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

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

Answer: C

QUESTION NO: 32

When you find a suspicious connection from a problematic host, you want to block everything from that whole network, not just the host. You want to block this for an hour, but you do not want to add any rules to the Rule Base. How do you achieve this?

- A. Create a Suspicious Activity rule in Smart View Tracker.
- B. Create a Suspicious Activity Rule in Smart View.
- C. Create an "FW SAM" rule in Smart View Monitor.
- D. Select "block intruder" from the Tools menu in the Smart View Tracker

Answer: B

QUESTION NO: 33

You create two Policy Packages for two NGX Security Gateways. For the first Policy Package, you selected security and Address Translation and QoS Policy. For the second Policy Package, you selected Security and Address Translation and Desktop Security Policy. In the first Policy Package, you enabled host-based port scan from the Smart Defense tab. You save and install the policy to the relevant Gateway object. How is the port scan configured on the second Policy Package's SmartDefense tab?

- A. Host-based port scan is disabled by default.
- B. Host-based port scan is enabled, because SmartDefense settings are global.

- C. Host-based port scan is enabled but it is not highlighted
- D. There is no Smart Defense tab in the second Policy Package.

Answer: B

QUESTION NO: 34

With Smart Dashboard's Smart Directory, you can create NGX user definitions on a(n)_____Server.

- A. NT Domain
- B. LDAP
- C. Provider-1
- D. SecureID
- E. Radius

Answer: B

QUESTION NO: 35

How can you prevent delay-sensitive applications, such as video and voice traffic, from being dropped due to long queue using 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

QUESTION NO: 36

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 frequently 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. Administrators should be able to view backed up logs in Smart View Tracker.

Jack's disaster recovery plan is as follows:

1. Use the cron utility to run the upgrade_export command each night on the Smart Center Servers. Configure the organization's routine backup software to back up the files created by the upgrade_export command.
2. Configure the Secure Poatform backup utility to back up the Security Gateway 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 logexport, Configure the organization's routine backup software to backup the exported logs every night.

Jack's plan:

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

Answer: C

QUESTION NO: 37

What does schema checking do?

- A. Authenticates users attempting to access resources protected by an NGX Security Gateway.
- B. Verifies that every object class, and its associated attributes, is defined in the directory schema.
- C. Maps LDAP objects to objects in the NGX objects_5_0.c file.
- D. Verifies the Certificate Revocation List for Certificate validity.
- E. Provides topology downloads for Secu Remote and Secure Client users authenticated by an LDAP Server.

Answer: B

QUESTION NO: 38

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

- A. Turn "per rule guarantees" into "per connection guarantees".
- B. Install Checkpoint 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

QUESTION NO: 39

Jill is about to test some rule and object changes suggested in an NGX newsgroup. Which backup and restore solution should Jill use, to ensure she can most easily restore her Security Policy to its previous configuration, after testing the changes?

- A. Secure Platform backup utilities
- B. Manual copies of the \$FWDIR/conf directory
- C. upgrade_export and upgrade import commands
- D. Policy Package management
- E. Database Revision Control

Answer: E

QUESTION NO: 40

When you hide a rule in a Rule Base, how can you disable the rule?

- A. Open the Rule Menu, and select Hide and view hidden rules. Select the rule, right-click, and select Disable.
- B. Uninstall the Security Policy, and then disable the rule.
- C. When a rule is hidden, it is automatically disabled. You do not need to disable the rule again.
- D. Run cpstop and cpstart on the SmartCenter Server, then disable the rule.
- E. Clear Hide from Rules drop-down menu, then right-click and select "Disable Rule (s)".

Answer: E

QUESTION NO: 41

How are cached usernames and passwords cleared from the memory of an NGX Security Gateway?

- A. Usernames and passwords only clear from memory after they time out.
- B. By retrieving LDAP user information, using the fw fetchldap command.
- C. By using the Clear User Cache button in Smart Dashboard.
- D. By installing a Security Policy
- E. By pushing new user information from the LDAP server.

Answer: D

QUESTION NO: 42

What is the proper command for exporting users in LDAP format?

- A. fw dbexport-f c: \temp\users.txt
- B. fw dbimport-f c: \temp\users.ldif-l -s "o=YourCity.com, c=YourCountry"
- C. fw dbimport-f c:\temp\users.ldap
- D. fw dbexport-f c: \temp\users.ldap-l-s
- E. fw dbexport-f c. \temp\users.ldif-l -s "o=YourCity.com. c=YourCountry"

Answer: E

QUESTION NO: 43

Anna is working in a large hospital, together with three other Security Administrators. Which Smart Console tool should she use to check changes to rules or object properties other administrators made?

- A. Smart Dashboard
- B. Smart View Tracker
- C. Eventia Tracker
- D. Eventia Monitor
- E. SmartView Monitor

Answer: B

QUESTION NO: 44

Doug wants to know who installed a Security Policy blocking all traffic from the corporate network. Which Smart View Tracker selection is best suited for this?

- A. Records pane
- B. Active tab
- C. custom filter
- D. log connections
- E. Audit tab

Answer: E

QUESTION NO: 45

You have a production implementation of Management High Availability, at version VPN-1 NG with Application Intelligence R55. You must upgrade your two Smart Center Servers to VPN-1 NGX. 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 Servers host objects version to VPN-1 NGX
5. Synchronize the Servers again.
- B. 1. Synchronize the two SmartCenter Servers
2. Perform an advanced upgrade on the primary SmartCenter Server.
3. Upgrade the secondary SmartCenter Server
4. Configure both SmartCenter Server host objects to version VPN-1 NGX.
5. Synchronize the Servers again.
- C. 1. Perform an advanced upgrade on the primary SmartCenter Server.
2. Configure the primary Perform SmartCenter Server host object to version VPN-1 NGX.
3. Synchronize the primary with the secondary SmartCenter Server.
4. Upgrade the secondary SmartCenter Server.
5. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
6. Synchronize the Servers again.
- D. 1. Synchronize the two SmartCenter Servers.
2. Perform an advanced upgrade on the primary SmartCenter Server.
3. Configure the primary SmartCenter Server host object to version VPN-1 NGX.
4. Synchronize the two Servers again.
5. Upgrade the secondary SmartCenter Server.
6. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
7. Synchronize the Servers again.

Answer: B

QUESTION NO: 46

Katie is the Security Administrator for an insurance company. Her manager gives Katie the following requirements for controlling DNS traffic:

Required Result #1: Accept domain-name over-TCP traffic (zone transfer traffic).

Required Result #2: Log domain-name over-TCP traffic (zone transfer traffic).

Desired Result #1: Accept domain-name over-UDP traffic (queries traffic).

Desired Result #2: Do not log domain-name over-UDP traffic (queries traffic).

Desired Result #3: Do not clutter the Rule Base by creating explicit rules for traffic that can be controlled using Global Properties.

Katie makes the following configuration changes, and installs the Security Policy:

1. She selects the box "Accept Domain Name over TCP (Zone Transfer)" in Global Properties.
2. She selects the box "Accept Domain Name over UDP (Queries)" in Global Properties.
3. She selects the box "Log Implied Rules" in Global Properties.

Does Katie's solution meet the required and desired results?

- A. The solution meets the required results, and one of the desired results
- B. The solution meets all required results, and none of the desired results
- C. The solution meets the required results, and two of the desired results
- D. The solution meets all required and desired results.
- E. The solution does not meet the required results.

Answer: C

QUESTION NO: 47

You have blocked an IP address via the Block Intruder feature of SmartView Tracker. How can you see the addresses you have blocked?

- A. In SmartView Status click the Blocked Intruder tab.
- B. Run `fwm blocked_view`
- C. Run `fwsmam-va`
- D. Run `fwmtab-tsam_blocked_ips`.
- E. In SmartView Tracker, click the Active tab, and the actively blocked connections display.

Answer: D

QUESTION NO: 48

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

- A. `cd patch add`
- B. `fwm upgrade_tool`
- C. `cppkg add`
- D. `patch add`
- E. `patch add cd`

Answer: E

QUESTION NO: 49

How does ClusterXL Unicast mode handle new traffic?

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

Answer: B

QUESTION NO: 50

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

How do you upgrade to VPN-1 NGX?

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

on the NG with AI R55 Security Gateway.

Answer: A

QUESTION NO: 51

Herman is attempting to configure a site-to-site VPN with one of his firm's business partners. Herman thinks Phase 2 negotiations are failing. Which SmartConsole application should Herman use to confirm his suspicions?

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

Answer: B

QUESTION NO: 52

Your company has two headquarters, one in London, one in New York. Each headquarters includes several branch offices. The branch offices ONLY need to communicate with the headquarters in their country, not with each other, and only the headquarters need to communicate directly. Which configuration meets the criteria? VPN Communities comprised of:

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

Answer: B

QUESTION NO: 53

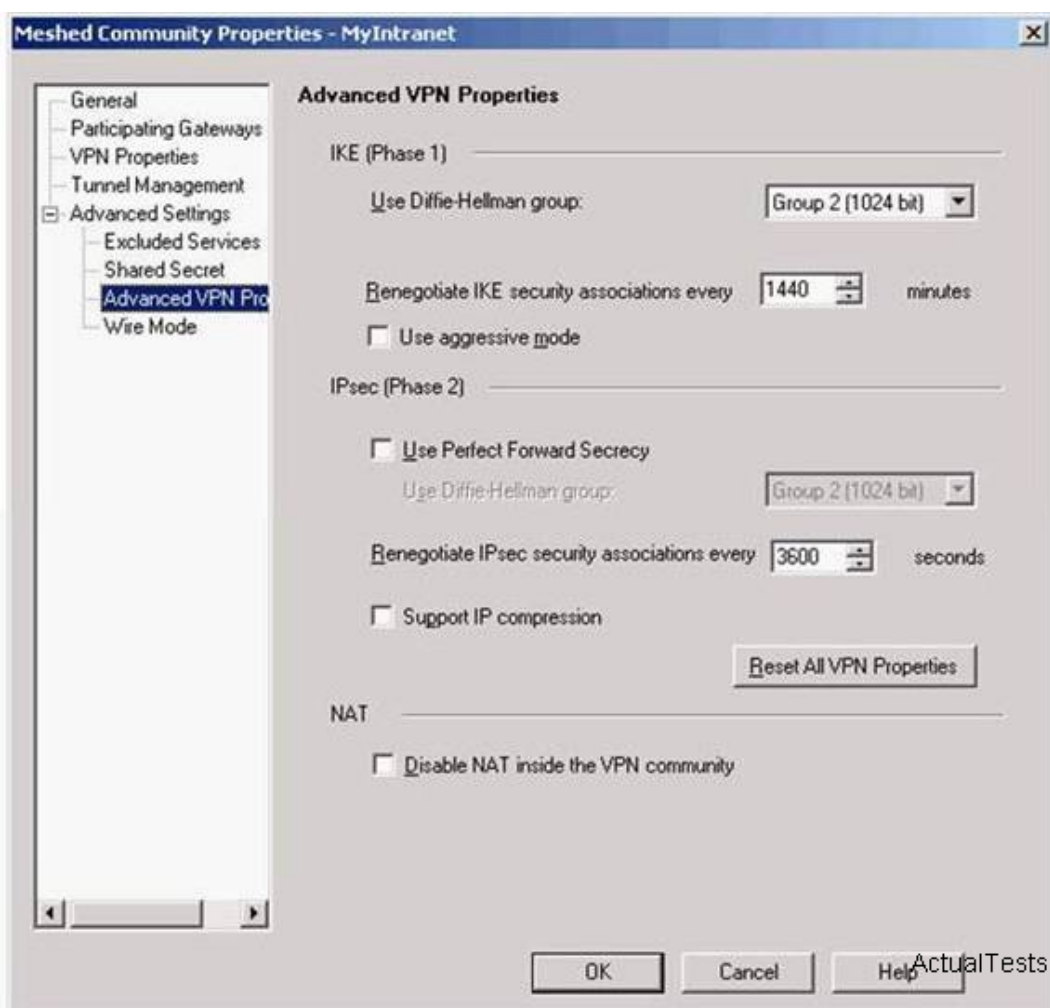
Which of these changes to a Security Policy optimizes Security Gateway performance?)

- A. Using domain objects in rules when possible
- B. Using groups within groups in the manual NAT Rule Base
- C. Putting the least-used rule at the top of the Rule Base.
- D. Logging rules as much as possible.
- E. Removing old or unused Security Policies from Policy Packages.

Answer: E

QUESTION NO: 54

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



What can Stephanie do to achieve her goal?

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

Answer: D

QUESTION NO: 55

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 NO: 56

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

QUESTION NO: 57

When you use the Global Properties' default settings, which type of traffic will be dropped, if no explicit rule allows the traffic?

- A. Firewall logging and ICA key-exchange information.
- B. Outgoing traffic origination from the Security Gateway.
- C. RIP traffic
- D. Smart Update connection
- E. IKE and RDP traffic

Answer: C

QUESTION NO: 58

Andrea has created a new gateway object that she will be managing at a remote location. She attempts to install the Security Policy to the new gateway object, but the object does not appear in the "install on" box. Which of the following is the most likely cause?

- A. Andrea has created the object using "New Check Point > VPN-1 Edge Embedded Gateway".
- B. Andrea created the gateway object using the "New Check Point > Externally Managed VPN Gateway" option from the Network Objects dialog box.
- C. Andrea has not configured anti-spoofing on the interfaces on the gateway object.
- D. Andrea has not configured Secure Internal Communications (SIC) for the object.
- E. Andrea created the Object using "New Check Point > VPN-1 Pro/Express Security Gateway" option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

Answer: B

QUESTION NO: 59

Use manages a distributed NGX installation for a large bank. Use needs to know which Security Gateways have licenses that will expire within the next 30 days. Which Smart Console application should Use use to gather this information?

- A. Smart View Monitor
- B. Smart Update
- C. Smart Dashboard
- D. Smart View Tracker
- E. Smart View Status

Answer: B

QUESTION NO: 60

How do you configure an NGX Security Gateway's kernel memory settings, without manually modifying the configuration files in \$FWDIR/lib? By configuring:

- A. the settings on the gateway object's Capacity Optimization screen.
- B. the settings on the Global Properties Capacity Optimization screen.
- C. the settings on the Gateway object's Advanced screen.
- D. the settings on the SmartCenter Server object's Advanced screen.
- E. SmartDefense Kernel Defender options

Answer: A

QUESTION NO: 61

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

```
Required interfaces: 3
Required secured interfaces: 1
eth00UP (sync, secured) multicast
eth1 UP non sync (non secured) multicast
eth2 UP non sync (non secured), multicast
Virtual cluster interfaces: 3
eth0 192.168.1.3
eth1 172.28.108.3
eth2 10.4.8.3
```

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

Answer: D

QUESTION NO: 62

David is a consultant for a software deployment company. David is working at a customer's site this week. David's task is to create a map of the customer's VPN tunnels, including down and destroyed tunnels. Which Smart Console application will provide David with the information needed to create this map?

- A. Smart Update
- B. Smart View Monitor
- C. Smart LSM
- D. Smart View Tracker

E. Smart View Status

Answer: B

QUESTION NO: 63

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

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

Answer: D

QUESTION NO: 64

Mary is the IT auditor for a bank. One of her responsibilities is reviewing the Security Administrator activity and comparing it to the change log. Which application should Mary use to view Security Administrator activity?

- A. NGX cannot display Security Administrator activity.
- B. Smart View Tracker in Real-Time Mode.
- C. Smart View Tracker in Audit Mode.
- D. Smart View Tracker in Log Mode
- E. Smart View Tracker in Active Mode

Answer: C

QUESTION NO: 65

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

QUESTION NO: 66

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

- A. ICMPPort Unreachable
- B. TCP keep alive
- C. IKE Key Exchange
- D. ICMP Destination Unreachable
- E. UDP keep alive

Answer: E

QUESTION NO: 67

Mary is recently hired as the Security Administrator for a public relations company. Mary's manager has asked her to investigate ways to improve the performance of the firm's perimeter Security Gateway. Mary must propose a plan based on the following required and desired results:

Required Result#1: Do not purchase new hardware.

Required Result#2: Use configuration changes that do not reduce security.

Desired Result#1: Reduce the number of explicit rules in the Rule Base.

Desired Result#2: Reduce the volume of logs.

Desired Result#3: Improve the Gateway's performance.

Proposed Solution:

Mary recommends the following changes to the Gateway's configuration:

Replace all domain objects with network and group objects.

Check "Log implied rules" and "Accept ICMP requests" in Global Properties.

Use Global Properties, instead of explicit rules, to control ICMP, VRRR, and RIP.

Does Mary's proposed solution meet the required and desired results?

- A. The solution meets all required and desired results.
- B. The solution meets all required results, and one of the desired results.
- C. The solution meets all required results, and two of the desired results.
- D. The solution meets all required results, and none of the desired results.
- E. The solution does not meet the required results.

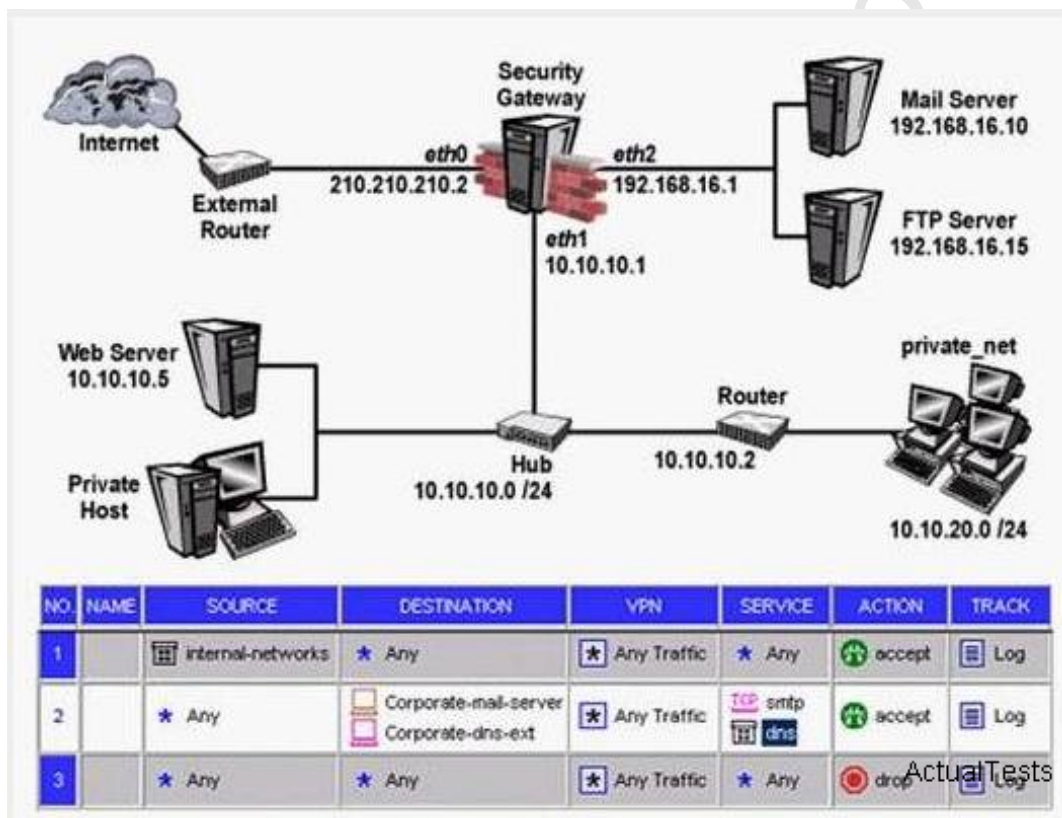
Answer: B

QUESTION NO: 68

You create implicit and explicit rules for the following network. The group object "internal-networks" includes networks 10.10.10.0 and 10.10.20.0. Assume

"Accept ICMP requests" is enabled as before last in the Global Properties.

Based on these rules, what happens if you Ping from host 10.10.10.5 to a host on the Internet, by IP address? ICMP will be:



- A. dropped by rule 0
- B. dropped by rule 2, the Cleanup Rule.
- C. accepted by rule 1.
- D. dropped by the last implicit rule.
- E. accepted by the implicit rule

Answer: C

QUESTION NO: 69

What is a requirement for setting up Management High Availability?

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

Answer: E

QUESTION NO: 70

You are a Security Administrator preparing to implement a VPN solution for his multisite organization. To comply with industry regulations, Your'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

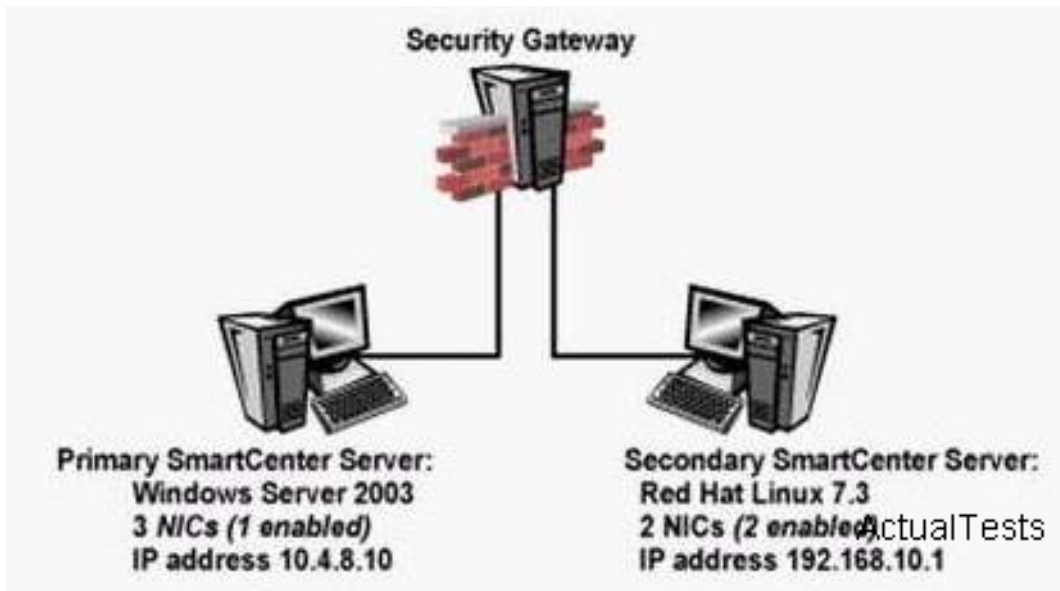
What is the most appropriate setting You should choose?

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

Answer: D

QUESTION NO: 71

The following configuration is for VPN-1 NGX:



Is this configuration correct for Management High Availability (HA)?

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

Answer: A

QUESTION NO: 72

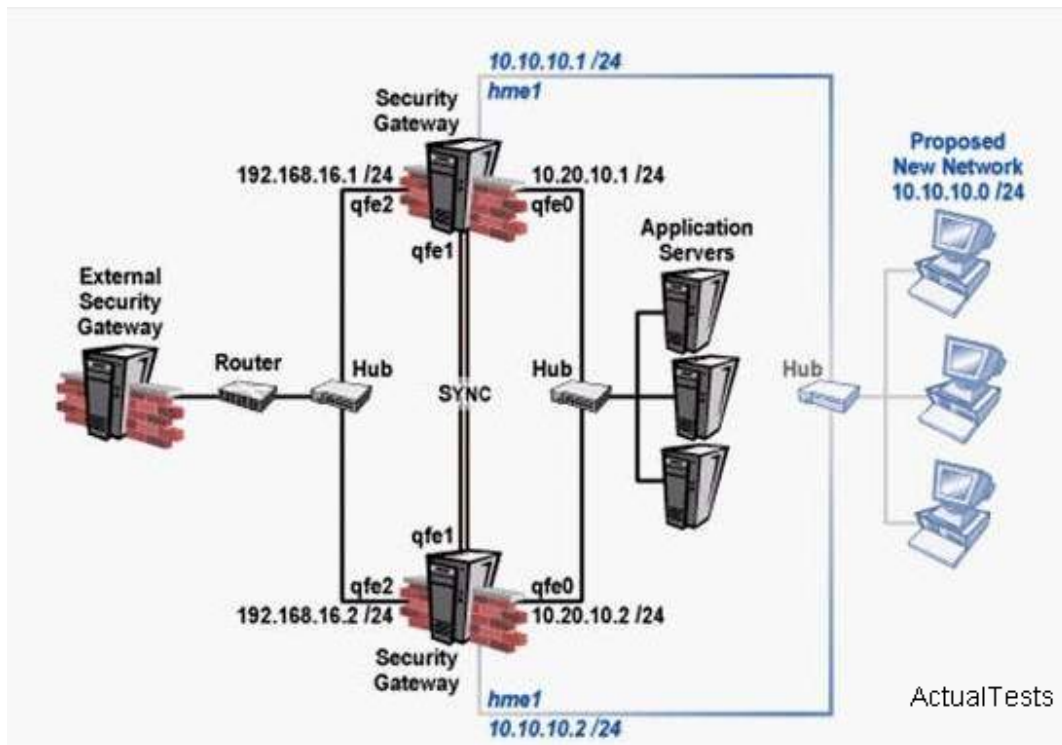
Your standby Smart Center Server's status is collision. What does that mean, and how do you synchronize the Server and its peer?

- A. The standby and active Servers have two Internal Certificate Authority (ICA) Certificates. Uninstall and reinstall the standby Server.
- B. The peer Server detected a keep-alive packet from the standby Server.
- C. The peer Server has not been properly synchronized. Manually synchronize both Servers again.
- D. The peer Server is more up-to-date. Manually synchronize both Servers again.
- E. The active Smart Center Server and its peer have different Security Policies and databases. Manually synchronize the Servers, and decide which Server's configuration to overwrite.

Answer: E

QUESTION NO: 73

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



- A. By running the cphaprob state command on both members.
- B. By running the cphaprob -a if command on both members.
- C. By running the cphaprob -r list command on both members
- D. By running the fw ctl iflist command on both members
- E. By running the cpconfig command on both members

Answer: B

QUESTION NO: 74

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

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

Answer: D

QUESTION NO: 75

Shauna is troubleshooting a Security Gateway that is dropping all traffic whenever the most recent Security Policy is installed. Working at the Security Gateway. Shauna needs to uninstall the Policy, but keep the processes running so she can see if there is an issue with the Gateway's firewall tables. Which of the following commands will do this?

- A. fwdbload 10.1.1.5
- B. fw unload 10.1.1.5
- C. cprestart
- D. fw tab -x -u
- E. cpstop

Answer: B

QUESTION NO: 76

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

The diagram shows three Cluster Members with the following configurations:

- Cluster Member 1:** OS: SecurePlatform, NIC(s): QuadCard, Installed Check Point product: VPN-1 Pro Gateway, Version: NGX.
- Cluster Member 2:** OS: Microsoft Windows 2000, NIC(s): Four, Intel 3Com Gigabit Ethernet cards, Installed Check Point product: VPN-1 Pro Gateway, Version: NGX.
- Cluster Member 3:** OS: Red Hat Linux 7.3, NIC(s): Four, Intel 3Com FastEtherLink 10/100 cards, Installed Check Point product: VPN-1 Pro Gateway, Version: NGX.

ActualTests

- 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, a cluster must have an even number of machines.

Answer: C

QUESTION NO: 77

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

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

Answer: B

QUESTION NO: 78

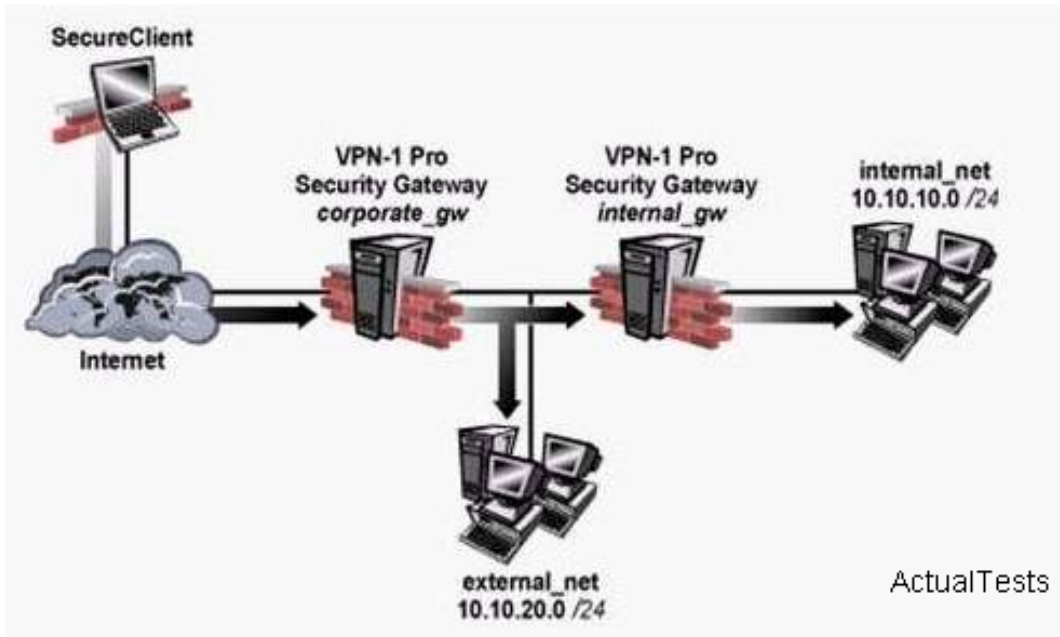
Which NGX feature or command allows Security Administrators to revert to earlier versions of the Security Policy without changing object configurations?

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

Answer: B

QUESTION NO: 79

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



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

Answer: D

QUESTION NO: 80

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 a 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 NO: 81

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

- A. Only VPN-1 Pro Security Gateway
- B. Both the operating system (OS) and all Check Point products
- C. All products, except the Policy Server
- D. Only the patch utility is upgraded using this command
- E. Only the OS

Answer: B

QUESTION NO: 82

Jane needs to back up the routing, interface, and DNS configuration information from her NGX Secure Platform Pro Security Gateway. Which backup-and-restore solution do you recommend for Jane?

- A. Database Revision Control
- B. Manual copies of the \$FWDIR/ conf directory
- C. upgrade_export and upgrade import commands
- D. Secure Platform backup utilities
- E. Policy Package management

Answer: D

QUESTION NO: 83

Eric wants to see all URLs? full destination paths in the Smart View 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/hpc11012.ess. How can Eric best customize Smart View 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 UPI resource in the rule, with action "accept"

Answer: C

QUESTION NO: 84

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: A

QUESTION NO: 85

You have locked yourself out of SmartDashboard with the rules you just installed on your stand alone Security Gateway. Now you cannot access the SmartCenter Server or any SmartConsole tools via SmartDashboard. How can you reconnect to SmartDashboard?

- A. Run cpstop on the SmartCenter Server.
- B. Run fw unlocklocal on the SmartCenter Server.
- C. Run fw unloadlocal on the Security Gateway
- D. Delete the \$ fwdir/database/manage.lockfile and run cprestart.
- E. Run fw uninstall localhost on the Security Gateway.

Answer: C

QUESTION NO: 86

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

- A. Launch cpconfig 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

QUESTION NO: 87

How does ClusterXL Unicast mode handle new traffic?

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

Answer: B

QUESTION NO: 88

By default, when you click file > Switch Active File from SmartView Tracker, the SmartCenter Server.

- A. Opens a new window with a previously saved log file.
- B. Purges the current log file, and starts a new log file.
- C. Purges the current log, and prompts you for the new log's mode.
- D. Saves the current log file, names the log file by date and time, and starts a new log file.
- E. Prompts you to enter a filename, then saves the log file.

Answer: D

QUESTION NO: 89

Alex is the Security Administrator for a large, geographically distributed network. The internet connection at one of his remote sites failed during the weekend, and the Security Gateway logged locally for over 48 hours. Alex is concerned that the logs may have consumed most of the free space on the Gateway's hard disk. Which SmartConsole application should Alex 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 NO: 90

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

- A. OPSE
- B. CPLogManager
- C. LEA
- D. SmartView Tracker
- E. ELA

Answer: C

QUESTION NO: 91

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 NO: 92

You want 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. VPN-1 and Firewall-1
- C. SecurePlatform NGX R60
- D. SVN Foundation
- E. VPN-1 Pro/Express NGXR60

Answer: C

QUESTION NO: 93

Choose the BEST sequence for configuring user management on SmartDashboard, for use with and LDAP server.

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

Answer: A

QUESTION NO: 94

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

General Limits

Source: intersect with user database

Destination: ignore user database

Apply Rule Only if Desktop Configuration Options are Verified

Required Sign On

Standard Specific

Sign On Method

Manual

Partially automatic

Fully automatic

Agent automatic Sign On

Single Sign On

Successful Authentication Tracking:

None Log Alert

OK Cancel Help

ActualTests

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 that FTP site only, and does not need to enter username and password for 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 NO: 95

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

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

Answer: C

QUESTION NO: 96

Select the correct statement about Secure Internal Communications (SIC) Certificates? SIC Certificates:

- A. for the SmartCenter Server are created during the SmartCenter Server configuration.
- B. decrease network security by securing administrative communication among the SmartCenter Servers and the Security Gateway.
- C. for NGX Security Gateways are created during the SmartCenter Server installation.
- D. uniquely identify Check Point enabled machines; they have the same function as VPN Certificates.

Answer: D

QUESTION NO: 97

What is the command to see the licenses of the Security Gateway FWDALLAS from you SmartCenter Server?

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

Answer: A

QUESTION NO: 98

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

- A. cpconfig
- B. cpinfo-i
- C. restore
- D. fwm dbimport
- E. upgrade import

Answer: E

QUESTION NO: 99

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 SmartDashboard 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 ???ji?Cp <shared key> <IP Address of SmartCenter Server>`.
- D. From the SmartCenter Server's command line type `fw putkey ???ji?Cp <shared key> <IP Address of Security Gateway>`.
- E. RE. install the Security Gateway.

Answer: B

QUESTION NO: 100

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



	Cluster Member 1	OS: SecurePlatform NIC(s): QuadCard Installed Check Point product: VPN-1 Pro Gateway Version: NGX
	Cluster Member 2	OS: Microsoft Windows 2000 NIC(s): Four, Intel 3Com Gigabit Ethernet cards Installed Check Point product: VPN-1 Pro Gateway Version: NGX
	Cluster Member 3	OS: Red Hat Linux 7.3 NIC(s): Four, Intel 3Com FastEtherLink 10/100 cards Installed Check Point product: VPN-1 Pro Gateway Version: NGX

ActualTests

- 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, a cluster must have an even numbers of machines.
- E. No, ClusterXL is not supported on Red Hat Linux.

Answer: C

QUESTION NO: 101

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

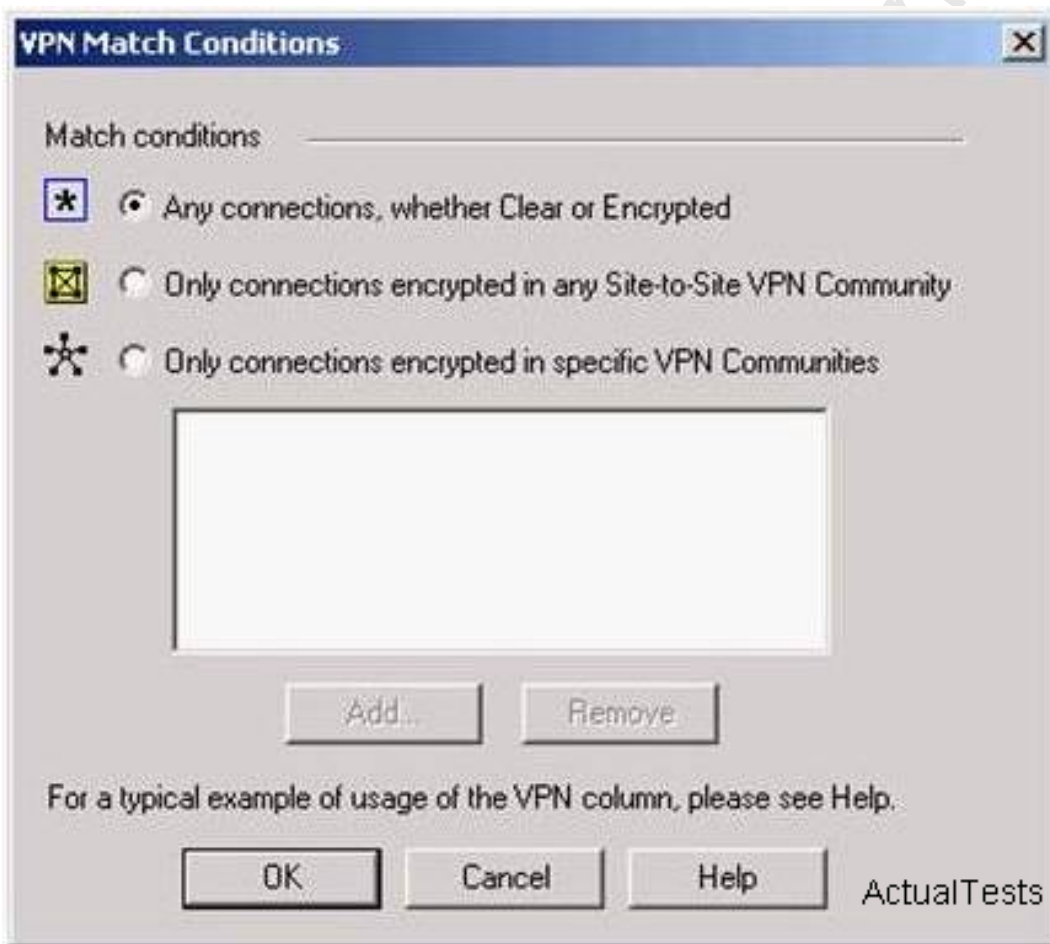
- A. Two star and one mesh Community, each star Community is set up for each site, with headquarters as the center of the Community, and branches as satellites The mesh Communities are between the New York and London headquarters

- B. three mesh Communities: one for London headquarters and its branches, one for New York headquarters and its branches, and one for London and New York headquarters.
- C. two mesh Communities, one for each headquarters and their branch offices; and one star Community, in which London is the center of the Community and New York is the satellite.
- D. two mesh Communities, one for each headquarters and their branch offices; and one star Community, where New York is the center of the Community and London is the satellite.

Answer: A

QUESTION NO: 102

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



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

Answer: C

QUESTION NO: 103

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 10. The H.323 rule includes a per-connection guarantee of 384 Kbps, and a per-connection allowed in the Action properties. If traffic passing through the Qos Module matches both rules .which of the following statements is true?

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

Answer: B

QUESTION NO: 104

Jordan's company is streaming training videos provided by a third party on the Internet. Jordan configures NGX so that each department ONLY views Webcasts specific to its department. Jordan created and configured the multicast groups for all interfaces, and configures them to "Drop all multicast except those whose destination is in the list". However, no multicast transmissions are coming from the Internet. What is a possible cause for the connection problem?

- A. The Multicast Rule is below the Stealth Rule. NGX can only pass multicast traffic, if the Multicast Rule is above the Stealth Rule.
- B. Jordan did not create the necessary "to and through" Rules, defining how NGX will handle the multicast traffic.
- C. Multicast groups are configured improperly on the external interface properties of the Security Gateway object.
- D. Anti-spoofing is enabled. NGX cannot pass multicast traffic, if anti-spoofing is enabled.
- E. NGX does not support multicast routing protocols and streaming media through the Security Gateway.

Answer: B

QUESTION NO: 105

Mary is recently hired as the Security Administrator for a public relations company. Mary's manager has asked her to investigate ways to improve the performance of the firm's perimeter

Security Gateway. Mary must propose a plan based on the following required and desired results:

Required Result #1: Do not purchase new hardware.

Required Result #2: Use configuration changes that do not reduce security.

Desired Result #1: Reduce the number of explicit rules in the Rule Base.

Desired Result #2: Reduce the volume of logs.

Desired Result #3: Improve the Gateway's performance.

Proposed Solution:

Mary recommends the following changes to the Gateway's configuration:

Replace all domain objects with network and group objects.

Stop logging Domain Name over UDP (queries).

Use Global Properties, instead of explicit rules, to control ICMP, VRRP, and RIP.

Does Mary's proposed solution meet the required and desired results?

- A. The solution meets the required results, and two of the desired results.
- B. The solution does not meet the required results.
- C. The solution meets all required results, and none of the desired results.
- D. The solution meets all required and desired results.
- E. The solution meets the required results, and one of the desired results.

Answer: D

QUESTION NO: 106

Carol is the Security Administrator for a chain of grocery stores. Each grocery store is protected by a Security Gateway. Carol 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 data and time the Security Policy was installed, and general performance statistics (CPU Use, average CPU time, active real memory, ect.).

Which SmartConsole application should Carol use to gather this information?

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

Answer: E

QUESTION NO: 107

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: E

QUESTION NO: 108

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 7.0
- E. MacOSX

Answer: A

QUESTION NO: 109

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 NO: 110

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

- A. Low latency class
- B. DiffServrule

- C. guaranteed per connection
- D-Weighted Fair queuing
- E. guaranteed per VOIP rule

Answer: A

QUESTION NO: 111

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

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

Answer: B

QUESTION NO: 112

You are trying to enter a new user, group, or organizational unit on an LDAP server, and you encounter the error "violates schema". To provide the BEST long-term security, you should:

- A. Import the schema, and enable schema checking
- B. Turn off schema checking, and restart the LDAP server.
- C. Turn off schema checking, and restart the SmartCenter Server.
- D. Restart the server E. Recover the corrupt database.

Answer: A

QUESTION NO: 113

You users defined in a Windows 2000 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule

in NGX?

- A. All Users
- B. A group with generic* user
- C. External-user group
- D. LDAP account-unit group
- E. LDAP group

Answer: E

QUESTION NO: 114

John is the Security Administrator for a public hospital. New health-care legislation requires logging for all traffic accepted through the perimeter Security Gateway. What must John do, to ensure implied rules meet the new requirement?

- A. Use the "Implicit Rules" predefined query in SmartView Tracker.
- B. Install the "View Implicit Rules" package using SmartUpdate.
- C. Check the "Log Implied Rules Globally" box on the NGX Gateway object.
- D. Set the position of all implicit rules to "Before Last".
- E. Check the "Log Implied Rules" box in Global Properties

Answer: E

QUESTION NO: 115

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 NO: 116

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

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

Answer: B

QUESTION NO: 117

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

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

Answer: B

QUESTION NO: 118

Sonny is the Security Administrator for a company with a large call center. The management team in the center is concerned that employees may be installing and attempting to use peer-to-peer file sharing utilities, during their lunch breaks. The call center's network is protected by an internal Security Gateway, which is configured to drop peer-to-peer file sharing traffic. Which application should Sonny use, to determine the number of packets dropped by each Gateway?

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

Answer: B

QUESTION NO: 119

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

- A. NGX takes the common-name value from the Certificate subject, and searches the LDAP 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 DN 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 LDAP user database.

Answer: B

QUESTION NO: 120

Which of the following is the final step in an NGX backup?

- A. Test restoration in a non-production environment, using the upgradeimport 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: A

QUESTION NO: 121

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 Queueing
- E. Low Latency Queueing

Answer: D

QUESTION NO: 122

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

- A. Turn "per rule guarantees" into "per connection guarantees".
- B. Install Checkpoint 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

QUESTION NO: 123

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

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

Answer: D

QUESTION NO: 124

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_Cleat
- D. Internal_clear > Communities
- E. internal clear>All communities

Answer: E

QUESTION NO: 125

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 frequently 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:

1. Use the cron utility to run the upgrade_export command each night on the SmartCenter Servers. Configure the organization's routine backup software to back up the files created by the upgrade_export command.
2. Configure the SecurePlanform backup utility to back up the Security Gateways 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 back up the switched logs every night.

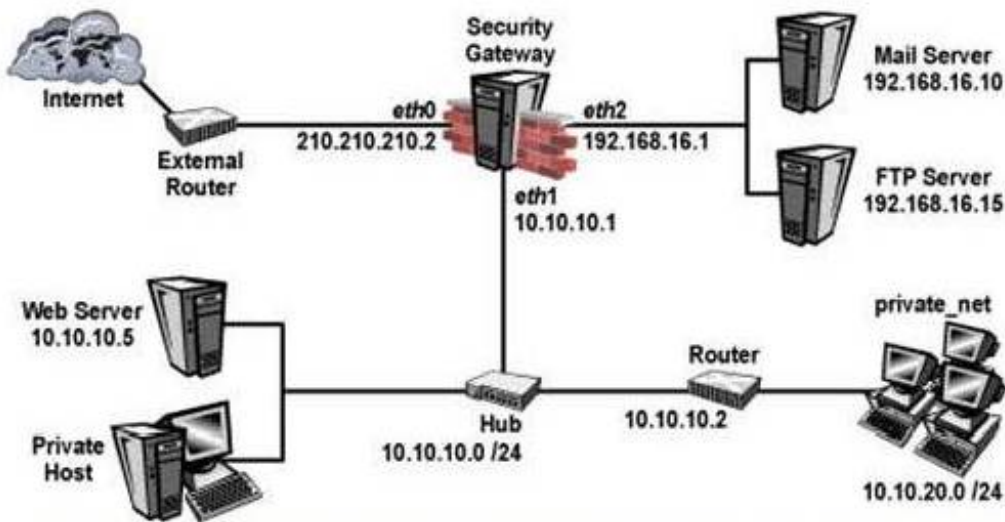
Jack's plan:

- 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

QUESTION NO: 126

As a Security Administrator, you must configure anti-spoofing on Security Gateway interfaces, to protect your internal networks. What is the correct anti-spoofing setting on interface ETH1 in this network diagram?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1		internal-networks	Any	Any Traffic	Any	accept	Log
2		Any	Corporate-mail-server Corporate-dns-ext	Any Traffic	smtp dns	accept	Log
3		Any	Any	Any Traffic	Any	drop	Log

NOTE: In the DMZ, mail server 192.168.16.10 is statically translated to the object "mail_valid", with IP address 210.210.210.3. The FTP server 192.168.16.15 is statically translated to the object "ftp_vaild", with IP address 210.210.210.5

- A. A group object that includes the 10.10.0.0/16 and 192.168.16.0/24 networks, and mail_valid and ftp_valid host objects.
- B. A group object that includes the 10.10.20.0/24 and 10.10.10.0/24 networks.
- C. A group object that includes the 10.10.0.0/16 network object, mail_valid host, and ftp_valid host object
- D. A group object that includes the 192.168.16.0/24 and 10.10.0.0/16 networks.
- E. A group object that includes the 10.10.10.0/24 and 192.168.16.0/24 networks

Answer: B

QUESTION NO: 127

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 Gateway's 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. Smart View Monitor
- D. Pop-up API
- E. SNMP trap

Answer: A

QUESTION NO: 128

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

```
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
```

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 NO: 129

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 VPN Tunnel Interfaces (VTI) on each gateway object, to point to the other two peers. 4.Add static routes on three Gateways, to route the new network to each peer's VTI interface.
- C. 1 .Add a new interface on each Gateway.
2.Add the newly added network into the existing VPN Domain for each Gateway. 3.Create VTIs on

each gateway object, to point to the other two peers. 4.Enable advanced routing on all three Gateways.

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

2.Add the newly added network into the existing VPN Domain for each gateway object.

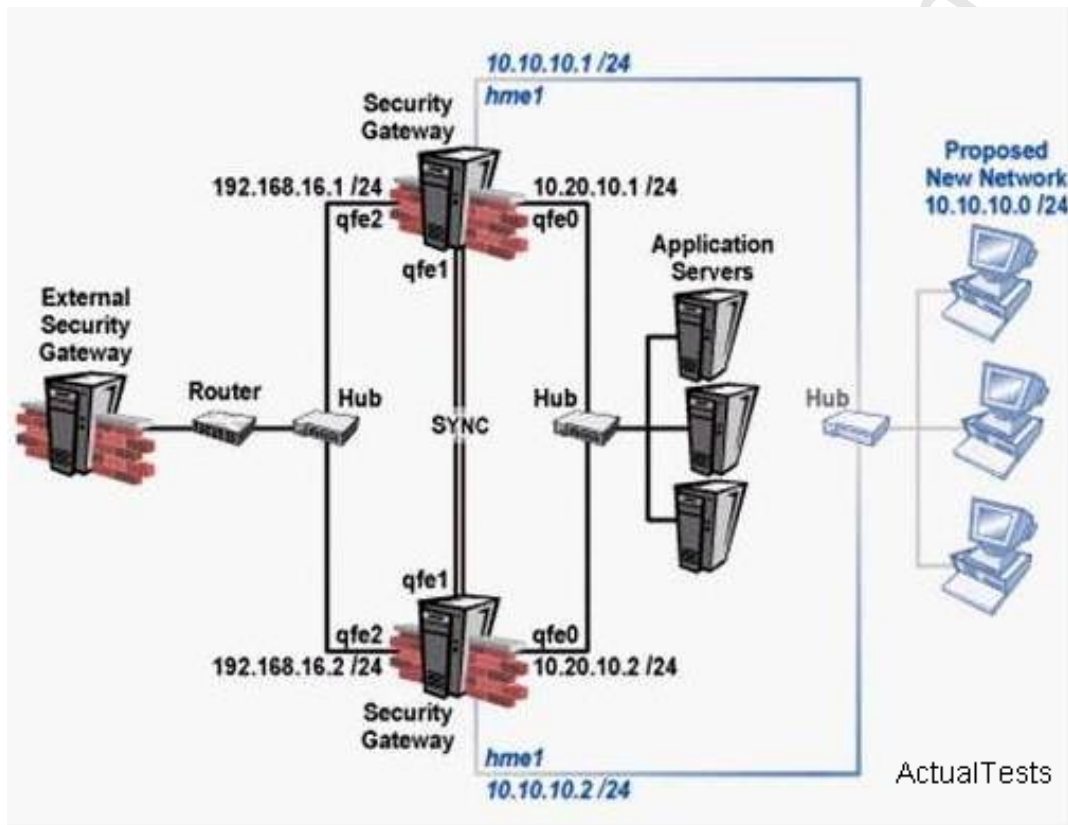
3.Create VTIs on each gateway object, to point to the other two peers.

9.Add static routes on three Gateways, to route the new networks to each peer's VTI interface.

Answer: B

QUESTION NO: 130

You network includes ClusterXL running Multicast mode on two members, as shown in this topology:



Your network is expanding, and you need to add new interfaces: 10.10.10.1/24 on Member A, and 10.10.10.2/24 on Member B. The virtual IP address for interface 10.10.10.0/24 is 10.10.10.3. What is the correct procedure to add these interfaces?

A. 1 .Use 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.Reenable "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.

e. 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 topology in the cluster object for the cluster and both members. 4. Install the Security Policy

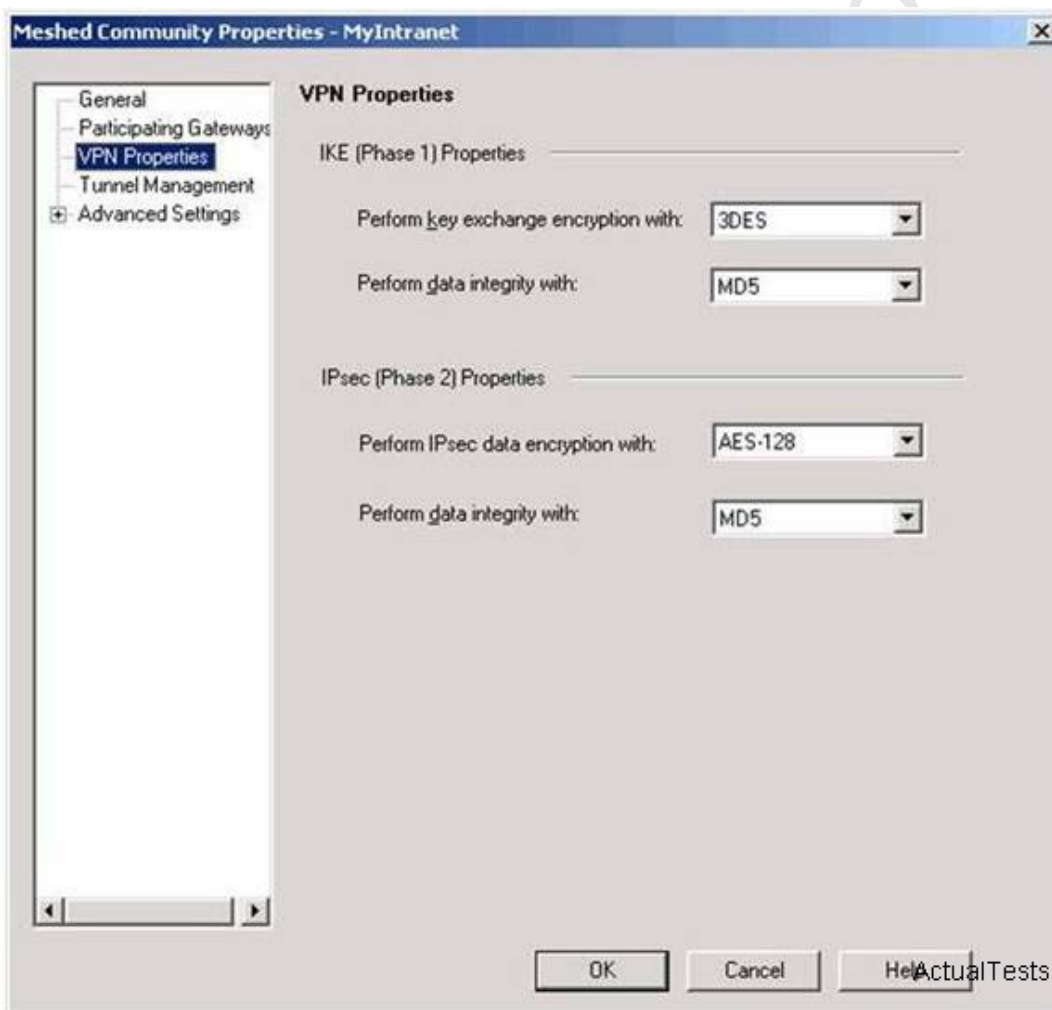
D. 1. Use sysconfig to configure the new interfaces on both members.

2. Update the topology in the cluster object for the cluster and both members. 3. Install the Security Policy.

Answer: C

QUESTION NO: 131

Jacob is using a mesh VPN Community to create a site-to-site VPN. The VPN properties in this mesh Community display in this graphic:



Which of the following statements is TRUE?

A. If Jacob changes the setting, "Perform key exchange encryption with" from "3DES" to "DES", he will enhance the VPN Community's security and reduce encryption overhead.

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

Answer: C

QUESTION NO: 132

Frank wants to know why users on the corporate network cannot receive multicast transmission from the Internet. An NGX Security Gateway protects the corporate network from the Internet. Which of the following is a possible cause for the connection problem?

- A. NGX does not support multicast routing protocols and streaming media through the Security Gateway.
- B. Frank did not install the necessary multicast license with SmartUpdate, when he upgraded to NGX.
- C. The Multicast Rule is below the Stealth Rule. NGX can only pass multicast traffic, if the Multicast Rule is above the Stealth Rule.
- D. Multicast restrictions are not configured properly on the corporate internal network interface properties of the Security Gateway object.
- E. Anti-spoofing is enabled. NGX cannot pass multicast traffic, if anti-spoofing is enabled.

Answer: D

QUESTION NO: 133

Gail is the Security Administrator for a marketing firm. Gail is working with the networking team, to troubleshoot user complaints regarding access to audio-streaming material from the Internet. The networking team asks Gail to check the object and rule configuration settings for the perimeter Security Gateway. Which SmartConsole application should Gail use to check these objects and rules?

- A. SmartViewMonitor
- B. SmartUpdate
- C. SmartView Tracker
- D. SmartDashboard
- E. SmartView Status

Answer: D

QUESTION NO: 134

When you hide a rule in a Rule Base, how can you then disable the rule?

- A. Open the Rule Menu, and select Hide and view hidden rules. Select the rule, right-click, and select Disable.
- B. Uninstall the Security Policy, and then disable the rule.
- C. When a rule is hidden, it is automatically disabled. You do not need to disable the rule again.
- D. Run cpstop and cpstart on the SmartCenter Server, then disable the rule.
- E. Clear Hide from Rules drop-down menu, then right-click and select "Disable Rule (s)".

Answer: E

QUESTION NO: 135

Which of these changes to a Security Policy optimizes Security Gateway performance?

- A. Using domain objects in rules when possible.
- B. Using groups within groups in the manual NAT Rule Base.
- C. Putting the least-used rule at the top of the Rule Base.
- D. Logging rules as much as possible.
- E. Removing old or unused Security Policies from Policy Packages.

Answer: E

QUESTION NO: 136

One of your remote Security Gateways suddenly stops sending logs, and you cannot install the Security Policy on the Gateway. All other remote Security Gateways are logging normally to the SmartCenter Server, and Policy installation is not affected. When you click the Test SIC status button in the problematic gateway object, you receive error message "unknown". What is the problem?

- A. The remote Gateway's IP address has changed, which invalidates the SIC Certificate.
- B. The Security Gateway is NG with Application Intelligence, and the SmartCenter Server is NGX.
- C. The Internal Certificate Authority for the SmartCenter object has been removed from objects_5_0.C
- D. The time on the SmartCenter Server's clock has changed, which invalidates the remote Gateway's Certificate.

E. There is no connection between the SmartCenter Server and the remote Gateway. Rules or routing may block the connection.

Answer: E

QUESTION NO: 137

A Security Administrator is notified that some long-lasting Telnet connections to a mainframe are dropped every time after an hour. The Administrator suspects that 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 timeout in the mainframe's Object Properties.
- B. create a new TCP service object on port 23, and increase the session timeout for this object. She only uses this new object in the rule that allows the Telnet connections to the mainframe.
- C. increase the session timeout in the Service Properties of the Telnet service.
- D. increase the session timeout in the Global Properties.
- E. ask the mainframe users to reconnect every time this error occurs.

Answer: B

QUESTION NO: 138

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. SHA1 Hash Completion

Answer: B

QUESTION NO: 139

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

- A. Guarantee Allocation
- B. Rule weight

- C. Apply rule only to encrypted traffic
- D. Rule limit
- E. Rule guarantee

Answer: A

QUESTION NO: 140

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. SmartView Tracker
- C. SmartUpdate
- D. SmartView Monitor
- E. SmartView Status.

Answer: D

QUESTION NO: 141

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 Queueing
- E. Limits

Answer: C

QUESTION NO: 142

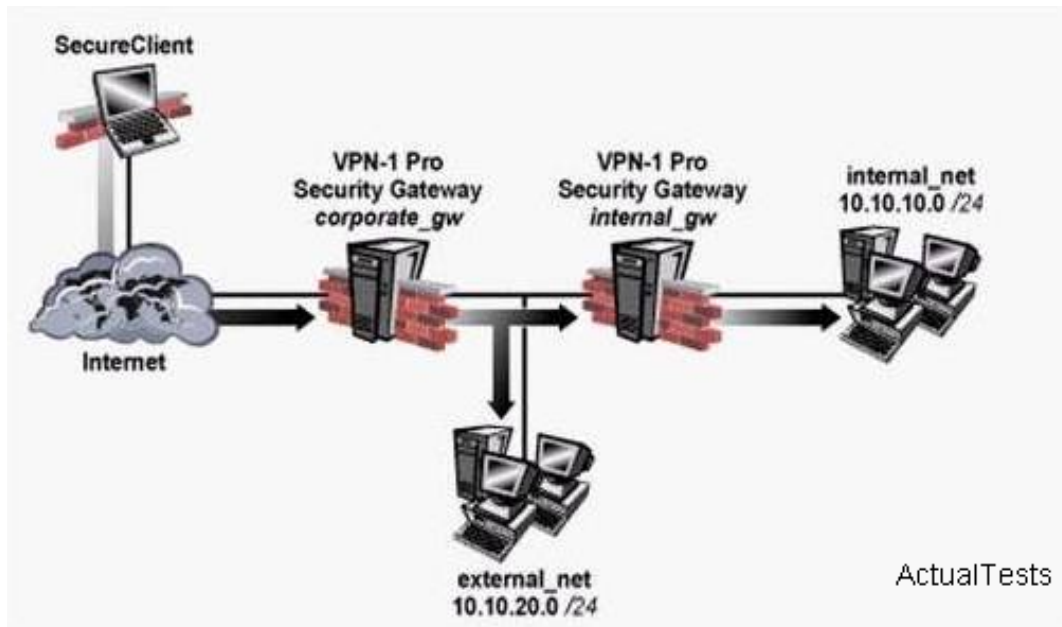
Where can a Security Administrator adjust the unit of measurement (bps, Kbps or Bps), for Check Point QoS bandwidth?

- 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

QUESTION NO: 143

The following diagram illustrates how a VPN-1 SecureClient user tries to establish a VPN with hosts in the external_net and internal_net from the Internal.



How is the Security Gateway VPN Domain created?

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

Answer: D

QUESTION NO: 144

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 NO: 145**

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

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

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

Answer: A**QUESTION NO: 146**

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

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

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

Answer: D

QUESTION NO: 147

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 Servers screen (from the Logs and Masters tree on the gateway object's General Properties screen), add the secondary SmartCenter Server object as the additional log server. Reinstall the Security Policy.
- D. Create a Check Point host object to represent the standby SmartCenter Server. Then select "Secondary SmartCenter Server" and Log Server", from the list of Check Point Products on the General properties screen.
- E. The secondary Server's host name and IP address must be added to the Masters file, on the remote Gateways.

Answer: C

QUESTION NO: 148

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

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

Answer: A

QUESTION NO: 149

Larry is the Security Administrator for a software development company. To isolate the corporate network from the developers' network, Larry installs an internal Security Gateway. Larry 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 NO: 150

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

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

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

Answer: D

QUESTION NO: 151

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

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

Answer: A

QUESTION NO: 152

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 a 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 NO: 153

When you change an implicit rule's order from "last" to "first" in Global Properties, how do you make the change effective?

- A. Close SmartDashboard, and reopen it.
- B. Select install database from the Policy menu.
- C. Select save from the file menu.
- D. Reinstall the Security Policy
- E. Run fw fetch from the security Gateway.

Answer: D

QUESTION NO: 154

Which NGX component displays the number of packets accepted, rejected, and dropped on a specific Security Gateway, in real time?

- A. Reporting Module
- B. Eventia Reporter

- C. Smart Update
- D. Smart View Status
- E. Smart View Monitor

Answer: A

QUESTION NO: 155

The following is cphaprob state command output from a ClusterXL New mode High Availability member:

```
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
```

When 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 member's state will be standby
- D. Both members' state will be active

Answer: B

QUESTION NO: 156

State Synchronization is enable on both members in a cluster, and the Security Policy is successfully installed. No protocols or services have been unselected for "selective sync". The following is the fw tab -t connections -s output from both members:

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

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

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

Is State Synchronization working properly between the two members?

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

Answer: E

QUESTION NO: 157

Amanda is compiling traffic statistics for her company'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 statics.
- E. configuring a Suspicious Activity Rule which triggers an alert when HTTP traffic pssses through the Gateway.

Answer: A

QUESTION NO: 158

By default, a standby Smart Center Server is automatically synchronized by an active Smart Center 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 Smart Center Server, for the first time.
- E. The standby Smart Center Server starts for the first time.

Answer: A

QUESTION NO: 159

Ben is the Security Administrator for a university. Ben configured and installed a new Security Policy this morning. An hour after installing the new Security Policy. Ben began receiving complaints that Internet access was very slow. Ben called his Internet Service Provider, who asked Ben how much virtual memory his Security Gateway had. Which Smart Console application should Ben use to answer this question?

- A. Smart View Tracker
- B. Smart LSM
- C. Smart Updae
- D. Smart View Monitor
- E. Smart View Status

Answer: D

QUESTION NO: 160

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 reenale 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