Checkpoint 156-915-65

ACTUAL TESTS

PASS ANY EXAM. ANYTIME.

156-915.65 Accelerated CCSE NGX R65

Practice Test

Version 2.1

QUESTION NO: 1

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

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

Answer: C

QUESTION NO: 2

A security audit has determined that your unpatched web application server is revealing the fact that it accesses a SQL server. You believe that you have enabled the proper SmartDefense setting but would like to verily this fact using SmartView Tracker. Which of the following entries confirms the proper blocking of this leaked information to an attacker?

A. "Fingerprint Scrambling: Changed [SQL] to [Perl]"
B. "HTTP response spoofing: remove signature [SQL Server]"
C. "Concealed HTTP response [SQL Server]. (Error Code WSE0160003)"
D. "ASCII Only Response Header detected: SQL"

Answer: C

QUESTION NO: 3

Your online bookstore has customers connecting to a variety of Web servers to place or change orders, and check order status. You ran penetration tests through the Security Gateway, to determine if the Web servers were protected from a recent series of cross-site scripting attacks. The penetration testing indicated the Web servers were still vulnerable. You have checked every box in the Web Intelligence tab, and installed the Security Policy. What else might you do to reduce the vulnerability?

A. Configure the Security Gateway protecting the Web servers as a Web server.
B. Check the "Products > Web Server" box on the host node objects representing your Web servers.
C. Configure resource objects as Web servers, and use them in the rules allowing HTTP traffic to the Web servers.
D. The penetration software you are using is malfunctioning and is reporting a false-positive.

Answer: C

QUESTION NO: 4

Where is it necessary to configure historical records in SmartView Monitor to generate Express reports in Eventia Reporter?

A. In SmartDashboard, the SmartView Monitor page in the VPN-1 Security Gateway object
B . In Eventia Reporter, under Express > Network Activity
C. In Eventia Reporter, under Standard > Custom
D. In SmartView Monitor, under Global Properties > Log and Masters

Answer: A

QUESTION NO: 5 CORRECT TEXT

Where do you enable popup alerts for SmartDefense settings that have detected suspicious activity?

A . In SmartView Monitor, select Tools > Alerts
B . In SmartView Tracker, select Tools > Custom Commands

Answer: A

QUESTION NO: 6

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

A. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
B. MEP Gateways must be managed by the sameSmartCenter Server.
C. MEP VPN Gateways cannot be geographically separated machines.
D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

Answer: A

QUESTION NO: 7

Which Check Point product is used to create and save changes to a Log Consolidation Policy?

A. Eventia Reporter Client
B. SmartDashboard Log Consolidator
C. SmartCenterServer
D. Eventia Reporter Server

Answer: B

QUESTION NO: 8

Which of the following would NOT be a reason for beginning with a fresh installation of VPN-1 NGX R65, instead of upgrading a previous version to VPN-1 NGX R65?

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

Answer: B

QUESTION NO: 9

How do you block some seldom-used FTP commands, such as CWD, and FIND from passing through the Gateway?

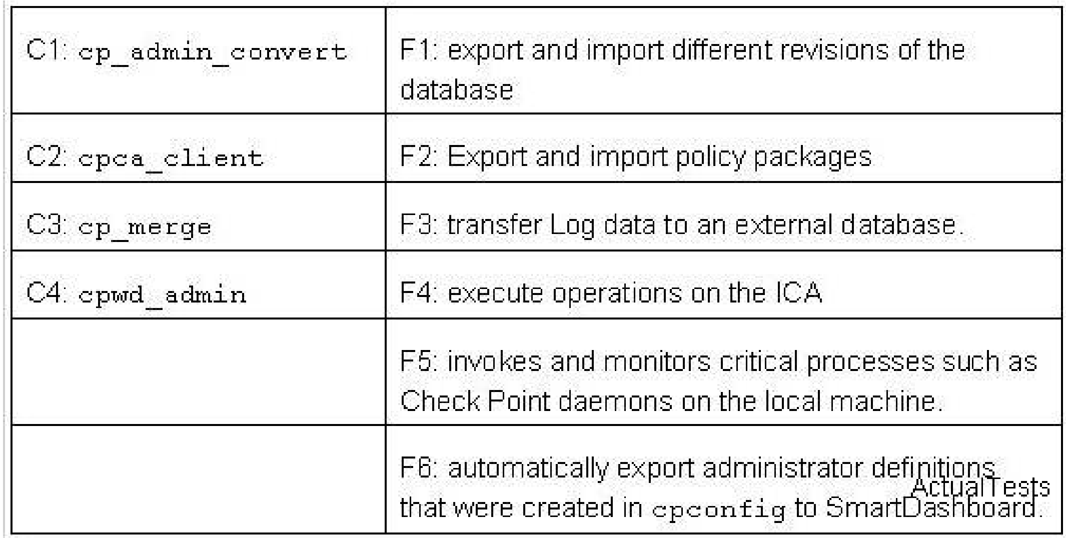
A . Use FTP Security Server settings in SmartDefense.

A. Add the restricted commands to theaftpd.conf file in the SmartCenter Server.
B. Configure the restricted FTP commands in the Security Servers screen of the Global properties.
C. Enable FTP Bounce checking inSmartDefense.

Answer: A

QUESTION NO: 10

Match each of the following commands to their correct function. Each command only has one function listed



C1: `cp_admin_convert`	F1: export and import different revisions of the database
C2: `cpca_client`	F2: Export and import policy packages
C3: `cp_merge`	F3: transfer Log data to an external database.
C4: `cpwd_admin`	F4: execute operations on the ICA
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in `cpconfig` to SmartDashboard.

A. C1>F6; C2>F4; C3>F2; C4>F5
B. C1>F4; C2>F6; C3>F3; C4>F2
C. C1>F2; C2>F4; C3>F1; C4>F5
D. C1>F2; C2>F1; C3>F6; C4>F4

Answer: A

QUESTION NO: 11

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

A. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
B. MEP Gateways must be managed by the sameSmartCenter Server.
C. MEP VPN Gateways cannot be geographically separated machines.
D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

Answer: A

QUESTION NO: 12

How do you block some seldom-used FTP commands, such as CWD, and FIND from passing through the Gateway?

A. Use FTP Security Server settings inSmartDefense
B. Add the restricted commands to theaftpd.conf file in the SmartCenter Server.
C. Configure the restricted FTP commands in the Security Servers screen of the Global properties.
D. Enable FTP Bounce checking inSmartDefense.

Answer: A

QUESTION NO: 13

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

A. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
B. MEP Gateways must be managed by the sameSmartCenter Server.
C. MEP VPN Gateways cannot be geographically separated machines.
D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

Answer: A

QUESTION NO: 14

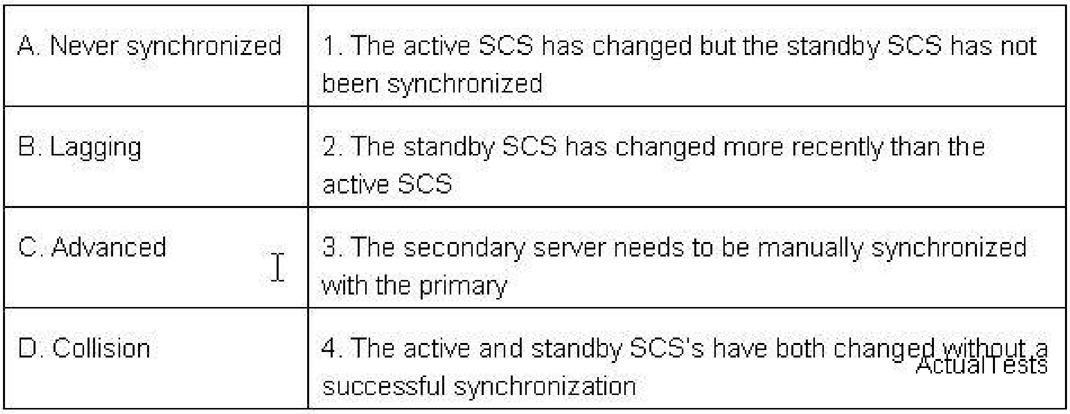
Which NGX R65 logs can you configure to send to DShield.org?

A. SNMP and account logs
B. Alert and user-defined alert logs
C. Account and alert logs
D. Audit and alert logs

Answer: B

QUESTION NO: 15

Match the Best Management High Availability synchronization-status descriptions for your SmartCenter Server (SCS)



A. Never synchronized	1. The active SCS has changed but the standby SCS has not been synchronized
B. Lagging	2. The standby SCS has changed more recently than the active SCS
C. Advanced	3. The secondary server needs to be manually synchronized with the primary
D. Collision	4. The active and standby SCS's have both changed without a successful synchronization

A. A3.B 1.C2.D4
B. A4.B3.C 1.D2
C. A3.B2.C 1.D4
D. A3.B 1.C4.D2

Answer: A

QUESTION NO: 16

The customer has a small Check Point installation which includes one Window XP workstation working as SmartConsole one Solaris server working as SmartCenter, and a third server running SecurePlatform working as Security Gateway. This is an example of:

A. Hybrid Installation
B. Unsupported configuration
C. Stand-Alone Installation
D. Distributed Installation

Answer: A

QUESTION NO: 17

Which VPN-1 NGX R65 component displays the number of packets accepted, rejected, and dropped on a specific Security Gateway, in real time?

A. SmarrViewMonitor
B. SmarrView Status
C. SmartUpdate
D. Eventia Analyzer

Answer: D

QUESTION NO: 18

SmartDefense profiles are:

A. Files that take 3MB of RAM from the user console machine.
B. Able to be cloned, but only from the command line.
C. Configurable up to 20 for all VPN-1 R65 Gateways and above.
D. Configurable from either theSmartDefense tab or from the Gateway itself.

Answer: D

QUESTION NO: 19

What is a Consolidation Policy?

A. A global Policy used to share a common enforcement policy for multiple similar Security Gateways
B. The collective name of the logs generated byEventia Reporter
C. The collective name of the Security Policy, Address Translation, andSmartDefense Policies
D. The specific Policy written inSmartDashboard to configure which log data is stored in the Eventia Reporter database

Answer: D

QUESTION NO: 20

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

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

Select the BEST response for the synchronization sequence. Choose One:

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

Answer: C

QUESTION NO: 21

Match the ClusterXL Modes with their configurations

A. A2.B3.C4.D 1

B. A2.B3.C 1.D4

C. A3,B2,C4,D 1

D. A3.B2.C 1.D4

Answer: D

QUESTION NO: 22

What is a Consolidation Policy?

A. A global Policy used to share a common enforcement policy for multiple similar Security Gateways

B. The collective name of the logs generated byEventia Reporter

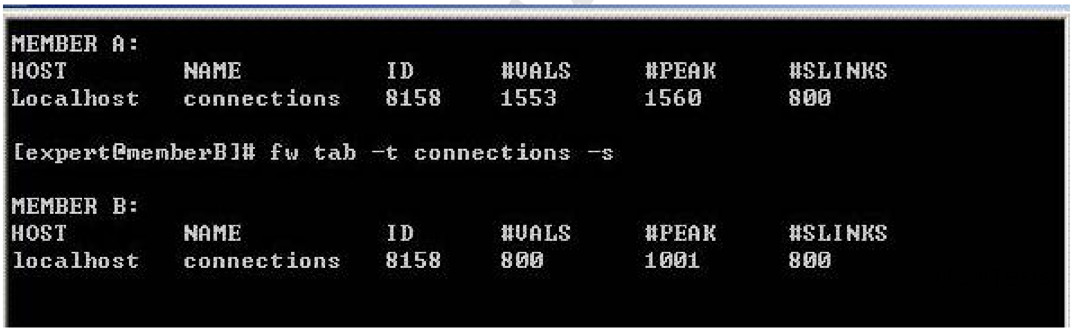
C. The collective name of the Security Policy, Address Translation, andSmartDefense Policies

D. The specific Policy written inSmartDashboard to configure which log data is stored in the Eventia Reporter database

Answer: D

QUESTION NO: 23

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



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

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

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

A. Members A and B are synchronized, because #SLINKS are identical in the connections table.

B. Members A and B are not synchronized, because #VALS in the connections table are not close.

C. Members A and B are not synchronized, because #PEAKfor both members is not close in the connections table.

D. Members A and B are synchronized, because ID for both members is identical in the connections table.

Answer: B

QUESTION NO: 24

Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?

A . VTIs are supported on SecurePlatform

A. VTIS cannot share IP addresses
B. VTIs can use an already existing physical-interface IP address
C. VTIS are assigned only local addresses, not remote addresses

Answer: A

QUESTION NO: 25

Which of the following is NOT supported with Office Mode?

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

Answer: D

QUESTION NO: 26

Central License management allows a Security Administrator to perform which of the following functions?

(1) Check for expired licenses.
(2) Sort licenses and view license properties.
(3) Attach both NGX Central and Local licenses to a remote module.
(4) Delete both NGX Local licenses and Central licenses from a remote module.
(5) Add or remove a license to or from the license repository.
(6) Attach and/or delete only NGX Central licenses to a remote module (not Local licenses).

A. 1,2,3,4,&5
B. 1.2.5.&6
C. 2,3,4,&5
D. 2,5,&6

Answer: A

QUESTION NO: 27

You are the Security Administrator for a university. The university's FTP servers have old hardware and software. Certain FTP commands cause the FTP servers to malfunction. Upgrading the FTP servers is not an option at this time. Where can you define Blocked FTP Commands passing through the Security Gateway protecting the FTP servers?

A. SmartDefense > Application Intelligence > FTP > FTP Security Server
B. Rule Base > Action Field > Properties
C. FTP Service Object > Advanced > Blocked FTP Commands
D. Global Properties > Security Server > Allowed FTP Commands

Answer: A

QUESTION NO: 28

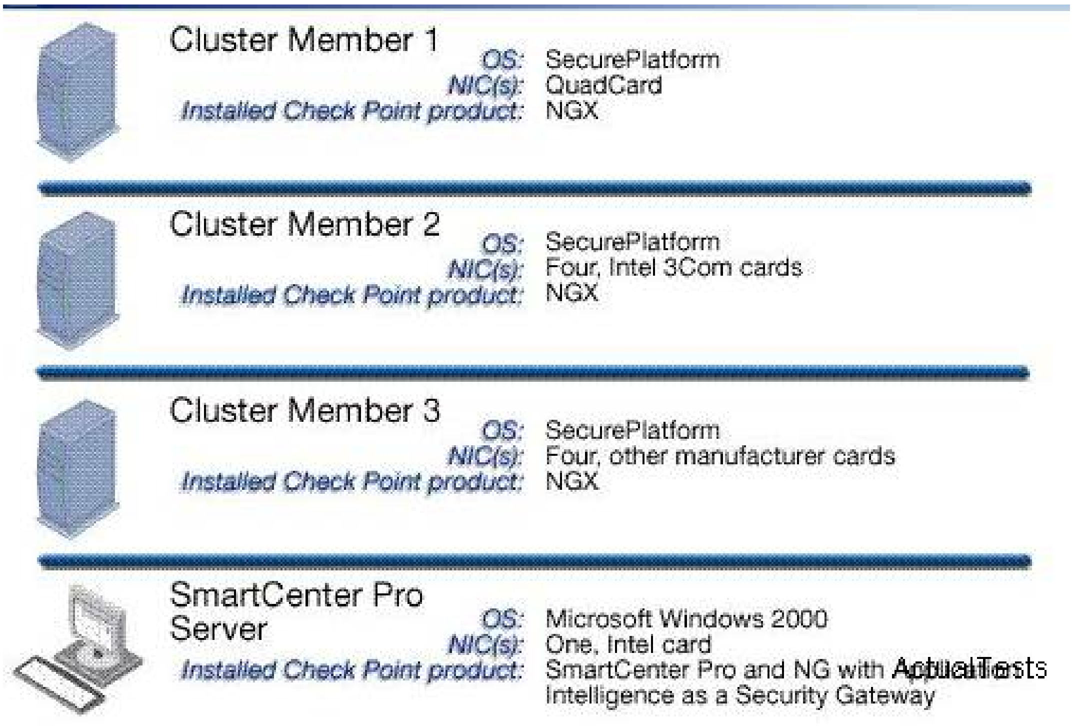
You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use three machines with the following configurations: Cluster Member 1: OS: SecurePlatform, NICs: QuadCard, memory: 512 MB, Security Gateway, version: VPN-1 NGX R65 and primary SmartCenter Server installed, version: VPN-1 NGX R65 Cluster Member 2: OS: SecurePlatform, NICs: 4 Intel 3Com, memory: 512 MB, Security Gateway only, and version: VPN-1 NGX R65 Cluster Member 3: OS: SecurePlatform, NICs: 4 other manufacturers, memory: 256 MB, Security Gateway only, and version: VPN-1 NGX R65

A. No, the Security Gateway cannot be installed on theSmartCenter Pro Server.
B. No, theSmartCenter Pro Server is not running the same operating system as the cluster members.
C. Yes, these machines are configured correctly for aClusterXL deployment.
D. No, Cluster Member 3 does not have the required memory.

Answer: A

QUESTION NO: 29

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



Cluster Member 1
OS: SecurePlatform
NIC(s): QuadCard
Installed Check Point product: NGX

Cluster Member 2
OS: SecurePlatform
NIC(s): Four, Intel 3Com cards
Installed Check Point product: NGX

Cluster Member 3
OS: SecurePlatform
NIC(s): Four, other manufacturer cards
Installed Check Point product: NGX

SmartCenter Pro Server
OS: Microsoft Windows 2000
NIC(s): One, Intel card
Installed Check Point product: SmartCenter Pro and NG with Application Intelligence as a Security Gateway

A. No, all machines in a cluster must be running on the same OS.

B. Yes, these machines are configured correctly for aClusterXL deployment.

C. No,QuadCards are not supported with ClusterXL.

D. No, a cluster may only have two members.

Answer: A

QUESTION NO: 30

When synchronizing clusters, which of the following statements is NOT true?

A. Client Auth or Session Auth connections through a cluster member will be lost if the cluster member fails.

B. The state of connections using resources ismaintaineci by a Security Server, so these connections cannot be synchronized.

C. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization

D. Only cluster members running on the same OS platform can be synchronized.

Answer: A

QUESTION NO: 31

Where is it necessary to configure historical records in SmartView Monitor to generate Express reports in Eventia Reporter?

A. In SmartDashboard.the SmartView Monitor page in the VPN-1 Security Gateway object
B. InEventia Reporter, under Express > Network Activity
C. InEventia Reporter, under Standard > Custom
D. InSmartView Monitor, under Global Properties > Log and Masters

Answer: A

QUESTION NO: 32

Which utility allows you to configure the DHCP service on SecurePlatform from the command line?

A. WebUI
B. cpconfig
C. ifconfig
D. sysconfig

Answer: D

QUESTION NO: 33

Which Check Point product is used to create and save changes to a Log Consolidation Policy?

A. Eventia Reporter Client
B. SmartDashboard Log Consolidator
C. SmartCenterServer
D. Eventia Reporter Server

Answer: B

QUESTION NO: 34

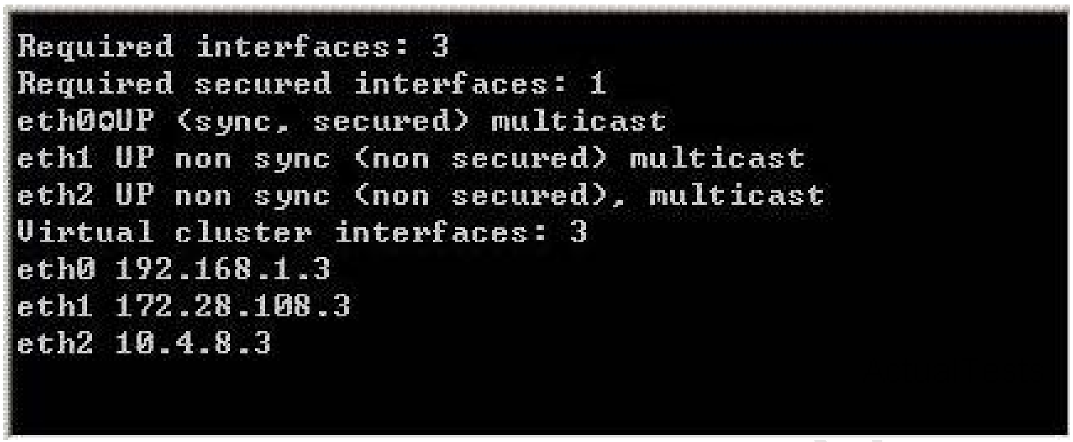
Which of the following statements about file-type recognition in Content Inspection is TRUE?

A. A scan failure will only occur if the antivirus engine fails to initialize.
B. Antivirus status is monitored usingSmartView Tracker.
C. The antivirus engine acts as a proxy, caching the scanned file before delivering it to the client.
D. All file types are considered "at risk", and are not subject to the whims of the Administrator or the Security Policy

Answer: C

QUESTION NO: 35

An NGXR65 HA 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 VIP address is 172.28.108.3 and the internal cluster VIP 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. The cphaprob if command output displays shows:What is causing the State Synchronization problem?



```
Required interfaces: 3
Required secured interfaces: 1
eth0oUP (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. The synchronization network has been defined as "Network Objective: Cluster + 1st sync" with an IP address 192.168.1.3 defined in the NGX cluster object's topology. This configuration is supported in NGX and therefore the above screenshot is not relevant to the sync problem.
B. The synchronization interface on the individual NGX cluster member object's Topology tab is enabled with "Cluster Interface". Disable this setting.
C. The synchronization network has a cluster VIP address (192.168.1.3) defined in the NGX cluster object's topology. Remove the 192.168.1.3 VIP interface from the cluster topology.
D. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.

Answer: A

QUESTION NO: 36

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN-1 Power 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?

A. Usecpprod_util to reconfigure the primary SmartCenter Server to become the secondary on the VPN-1 Power Gateway. Install a new primary SmartCenter Server on the spare machine and set to "standby". Synchronize the "active" secondary to the "standby" primary in order to migrate the configuration.
B. Install the secondary Server on the spare machine. Add the new machine to any network routable to the primary Server. Synchronize the machines.

C. You cannot configure Management HA, when either the primary or secondarySmartCenter Server is running on a VPN-1 Pro Gateway.
D. Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server. Synchronize the machines.

Answer: C

QUESTION NO: 37

What must a public hospital Security Administrator do to comply with new health-care legislation requirements for logging all traffic accepted through the perimeter Security Gateway?

A. Define two log servers on the VPN-1 NGX R65 Gateway object. Enable "Log Implied Rules" on the first log server. Enable "Log Rule Base" on the second log server. UseEventia Reporter to merge the two log server records into the same database for HIPPA log audits.
B. Install the "View Implicit Rules" package usingSmartUpdate.
C. In Global Properties > Reporting Tools check the box "Enable tracking all rules (including rules marked as 'None' in the Track column). Send these logs to a secondary log server for a complete logging history Use your normal log server for standard logging for troubleshooting.
D. Check the "Log Implied Rules Globally" box on the VPN-1 NGX R65 Gateway object.

Answer: C

QUESTION NO: 38

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

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

Select the BEST response for the synchronization sequence. Choose One:

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

Answer: C

QUESTION NO: 39

Which of the following commands is a CLI command for VPN-1 NGX R65?

A. fw shutdown
B. fwprint
C. fw tab -u
D. fw merge

Answer: C

QUESTION NO: 40

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

A. Simulate the license-upgrade process.
B. Perform the actual license-upgrade process.
C. View the status of currently installed licenses.
D. View the licenses in theSmartUpdate License Repository.

Answer: D

QUESTION NO: 41

What tools CANNOT be launched from SmartUpdate NGX R65?

A. cpinfo
B. SecurePlatform WebUI
C. snapshot
D. Nokia Voyager

Answer: C

QUESTION NO: 42

Your VPN-1 NGX R65 primary SmartCenter Server is installed on SecurePlatform. You plan to schedule the SmartCenter Server to run fw logswitch automatically every 48 hours. How do you create this schedule?

A. Create a time object, and add 48 hours as the interval. Select that time object's Global Properties > Logs and Masterswindow, to schedule a logswitch.
B. Create a time object, and add 48 hours as the interval. Open the Security Gateway object's Logs and Masterswindow, enable "Schedule log switch", and select the time object.
C. Create a time object, and add 48 hours as the interval. Open the primarySmartCenter Server object's Logs and Masters window, enable "Schedule log switch", and select the Time object.
D. On aSecurePlatform SmartCenter Server, this can only be accomplished by configuring the fw logswitch command via the cron utility.

Answer: C

QUESTION NO: 43

What must a public hospital Security Administrator do to comply with new health-care legislation requirements for logging all traffic accepted through the perimeter Security Gateway?

A. Define two log servers on the VPN-1 NGX R65 Gateway object. Enable "Log Implied Rules" on the first log server. Enable "Log Rule Base" on the second log server. UseEventia Reporter to merge the two log server records into the same database for HIPPA log audits.
B. Install the "View Implicit Rules" package usingSmartUpdate.
C. In Global Properties > Reporting Tools check the box "Enable tracking all rules (including rules marked as 'None' in the Track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.
D. Check the "Log Implied Rules Globally" box on the VPN-1 NGX R65 Gateway object.

Answer: C

QUESTION NO: 44

You plan to migrate an NG with Application Intelligence (AI) R55 SmartCenter Server on Windows to VPN-1 NGX R65. You also plan to upgrade four VPN-1 Pro Gateways at remote offices, and one local VPN-1 Pro Gateway at your company's headquarters. The SmartCenter Server configuration must be migrated. What is the correct procedure to migrate the configuration?

A. 1. Upgrade the five remote Gateways viaSmartUpdate.
2. Upgrade the SmartCenter Server, using the NGX R65 CD.
B. 1. From the VPN-1 NGX R65 CD on theSmartCenter Server, select "Upgrade".
2. Reboot after installation and upgrade all licenses via SmartUpdate.
3. Reinstall all gateways using NGX R65 and install a policy.
C. 1. From the VPN-1 NGX R65 CD in theSmartCenter Server, select "Export".
2. Install VPN-1 NGX R65 on a new PC using the option "Installation using imported configuration".

3. Reboot after installation and upgrade all licenses via SmartUpdate.
4. Upgrade software on all five remote Gateways via SmartUpdate.
D. 1.Copy the $FWDIR\conf directory from the SmartCenter Server.
2. Save directory contents to another file server.
3. Uninstall the SmartCenter Server, and install a new SmartCenter Server.
4. Move the saved directory contents to $FWDIR\conf replacing the default installation files.
5. Reinstall all gateways using VPN-1 NGX R65 and install a Security Policy.

Answer: C

QUESTION NO: 45

How should Check Point packages be uninstalled?

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

Answer: C

QUESTION NO: 46

Which is the BEST configuration option to protect internal users from malicious Java code, without stripping Java scripts?

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

Answer: B

QUESTION NO: 47

You are working in a large hospital, together with three other Security Administrators. How do you use SmartConsole to check changes to rules or object properties other administrators made?

A. Eventia Monitor
B. SmartView Monitor
C. Eventia Tracker

D. SmartView Tracker

Answer: D

QUESTION NO: 48

Which operating system is not supported by SecureClient?

A. MacOSX
B. Windows XP SP2
C. Windows 2003 Professional
D. IPSO 3.9

Answer: D

QUESTION NO: 49

In SmartDashboard, you configure 45 MB as the required free hard-disk space to accommodate logs. What can you do to keep old log files, when free space falls below 45 MB?

A. Do nothing. Old logs are deleted, until free space is restored.
B. Do nothing. TheSmartCenter Server automatically copies old logs to a backup server before purging.
C. Use thefwm logexport command to export the old log files to other location.
D. Configure a script to runfw logswitch and SCP the output file to a separate file server.

Answer: D

QUESTION NO: 50

What happens when you select File > Export from the SmartView Tracker menu?

A. Exported log entries are deleted from fw.log.
B. Current logs are exported to anew'.log file.
C. Exported log entries are still viewable inSmartView Tracker.
D. Logs in fw.log are exported to a file that can be opened by Microsoft Excel

Answer: D

QUESTION NO: 51

You plan to migrate an NG with Application Intelligence (Al) R55 SmartCenter Server on Windows to VPN-1 NGX R65. You also plan to upgrade four VPN-1 Pro Gateways at remote offices, and one local VPN-1 Pro Gateway at your company's headquarters. The SmartCenter Server configuration must be migrated. What is the correct procedure to migrate the configuration?

A. 1. Upgrade the five remote Gateways viaSmartUpdate.
2. Upgrade the SmartCenter Server, using the NGX R65 CD.
B. 1. From the VPN-1 NGX R65 CD on theSmartCenter Server, select "Upgrade".
2 Reboot after installation and upgrade all licenses via SmartUpdate.
3. Reinstall all gateways using NGX R65 and install a policy.
C. 1. From the VPN-1 NGX R65 CD in theSmartCenter Server, select "Export".
2. Install VPN-1 NGX R65 on a new PC using the option "Installation using imported configuration".
3. Reboot after installation and upgrade all licenses via SmartUpdate.
4. Upgrade software on all five remote Gateways via SmartUpdate.
D. 1.Copy the $FWDIR\conf directory from the SmartCenter Server.
2. Save directory contents to another file server.
3. Uninstall the SmartCenter Server, and install a new SmartCenter Server.
4. Move the saved directory contents to $FWDIR\conf replacing the default installation files.
5. Reinstall all gateways using VPN-1 NGX R65 and install a Security Policy.

Answer: C

QUESTION NO: 52

When launching SmartDashboard, what information is required to log into VPN-1 NGX R65?

A. User Name, Password,SmartCenter Server IP
B. User Name,SmartCenter Server IP, certificate fingerprint file
C. Password,SmartCenter Server IP. LDAP Server
D. Password,SmartCenter Server IP

Answer: B

QUESTION NO: 53

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

A. upgrade_mgmt
B. fwinstall_mgmt

C. fwm upgrade_tool
D. patch addcd

Answer: D

QUESTION NO: 54

Which SmartView Tracker mode allows you to read the SMTP email body sent from the Chief Executive Officer (CEO)?

A. Log Tab
B. Display Capture Action
C. This is not aSmartView Tracker feature
D. Account Query

Answer: B

QUESTION NO: 55

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

A. Connectivity between the NGX gateway and LDAP server
B. Secure Internal Communications (SIC)
C. VPN Load Balancing
D. Overlapping VPN Domains

Answer: C

QUESTION NO: 56

Which SmartConsole component can Administrators use to track remote administrative activities?

A. SmartView Tracker
B. TheWebUI
C. Eventia Reporter
D. SmartView Monitor

Answer: B

QUESTION NO: 57

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

A. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
B. MEP Gateways must be managed by the sameSmartCenter Server.
C. MEP VPN Gateways cannot be geographically separated machines.
D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

Answer: A

QUESTION NO: 58

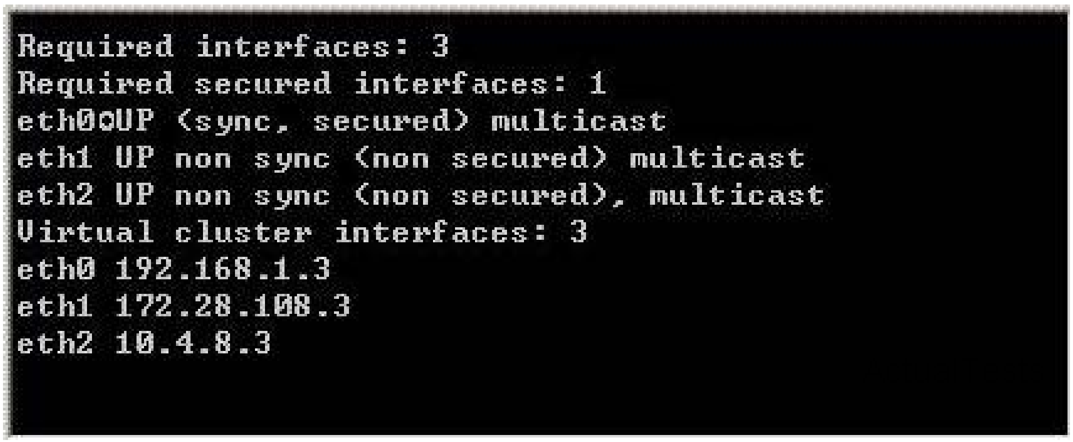
Where can an administrator configure the notification action in the event of a policy install time change?

A. SmartDashboard: Policy Package Manager
B. SmartView Tracker: Audit Log
C. SmartView Monitor: Global Thresholds
D. SmartDashboard: Security Gateway Object: Advanced Properties Tab

Answer: C

QUESTION NO: 59

An NGXR65 HA 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 VIP address is 172.28.108.3 and the internal cluster VIP 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. The cphaprob if command output displays shows:What is causing the State Synchronization problem?



```
Required interfaces: 3
Required secured interfaces: 1
eth0OUP (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. The synchronization network has been defined as "Network Objective: Cluster + 1st sync" with an IP address 192.168.1.3 defined in the NGX cluster object's topology. This configuration is supported in NGX and therefore the above screenshot is not relevant to the sync problem.
B. The synchronization interface on the individual NGX cluster member object's Topology tab is enabled with "Cluster Interface". Disable this setting.
C. The synchronization network has a cluster VIP address (192.168.1.3) defined in the NGX cluster object's topology. Remove the 192.168.1.3 VIP interface from the cluster topology.
D. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.

Answer: A

QUESTION NO: 60

In a Management High Availability (HA) configuration, you can configure synchronization to occur automatically, when
(1) The Security Policy is installed.
(2) The Security Policy is saved.
(3) The Security Administrator logs in to the secondary SmartCenter Server, and changes its status to active.
(4) A scheduled event occurs.
(5) The user database is installed.

Select the BEST response for the synchronization sequence. Choose One:

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

Answer: C

QUESTION NO: 61

You have a High Availability ClusterXL configuration. Machines are not synchronized. What happens to connections on failover?

A. It is not possible to configure High Availability that is not synchronized.
B. Connections cannot be established until cluster members are fully synchronized.
C. Old connections are lost but can be reestablished.
D. Old connections are lost and but are automatically recovered whenever the failed machine recovers.

Answer: C

QUESTION NO: 62

Your online bookstore has customers connecting to a variety of Web servers to place or change orders, and check order status. You ran penetration tests through the Security Gateway, to determine if the Web servers were protected from a recent series of cross-site scripting attacks. The penetration testing indicated the Web servers were still vulnerable. You have checked every box in the Web Intelligence tab, and installed the Security Policy. What else might you do to reduce the vulnerability?

A. Configure the Security Gateway protecting the Web servers as a Web server.
B. The penetration software you are using is malfunctioning and is reporting a false-positive.
C. Check the "Web Intelligence" box in theSmartDefense > HTTP Protocol Inspection.
D. Check the "Products > Web Server" box on the host node objects representing your Web servers.

Answer: C

QUESTION NO: 63

Which of the following is the most critical step in a SmartCenter Server NGX R65 backup strategy?

A. Perform a full system tape backup of both theSmartCenter and Security Gateway machines.
B. Run thecpstop command prior to running the upgrade_export command
C. Using theupgradejmport command, attempt to restore the SmartCenter Server to a non-production system
D. Move the *.tgzupgrade_export file to an off site location via ftp.

Answer: C

QUESTION NO: 64

In a VPN-1NGX R65 ClusterXL Load Sharing configuration, which type of ARP related problem sometimes forces the use of Unicast Mode (Pivot) configuration due to incompatibility on some adjacent routers and switches?

A. Multicast MAC address response to a RARP request
B. MGCP MAC address response to a Multicast IP request
C. Unicast MAC address response to a Multicast IP request

D. Multicast MAC address response to aUnicast IP request

Answer: D

QUESTION NO: 65

In SmartDashboard, you configure 45 MB as the required free hard-disk space to accommodate logs. What can you do to keep old log files, when free space falls below 45 MB?

A. Do nothing. Old logs are deleted, until free space is restored.
B. Do nothing. TheSmartCenter Server automatically copies old logs to a backup server before purging.
C. Use thefwm logexport command to export the old log files to other location.
D. Configure a script to runfw logswitch and SCP the output file to a separate file server.

Answer: D

QUESTION NO: 66

How do you verify a VPN Tunnel Interface (VTI) is configured properly?

A. vpn shell display interface detailed <VTI name>
B. vpn shell show interface detailed <VTI name*
C. vpn shell display <VTI name> detailed
D. vpn shell show<VTI name> detailed

Answer: B

QUESTION NO: 67

Where do you enable popup alerts for SmartDefense settings that have detected suspicious activity?

A. In SmartView Monitor, select Tools > Alerts
B. In SmartView Tracker, select Tools > Custom Commands
C. In SmartDashboard, edit the Gateway object, select SmartDefense > Alerts
D. In SmartDashboard, select Global Properties > Log and Alert > Alert Commands

Answer: A

QUESTION NO: 68

What action can be run from SmartUpdate NGX R65?

A. mds_backup
B. cpinfo
C. upgrade_export
D. remote uninstall verifier

Answer: B

QUESTION NO: 69

Which of the following would NOT be a function of the Check Point license-upgrade tool?

A. Upgrade locally managed licenses.
B. Simulate the license-upgrade process.
C. Manually upgrade a specific license.
D. View the status of the currently installed licenses.

Answer: C

QUESTION NO: 70

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

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

Select the BEST response for the synchronization sequence. Choose One:

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

Answer: C

QUESTION NO: 71

How do you use SmartView Monitor to compile traffic statistics for your company's Internet activity during production hours?

A. Use the "Traffic Counters" settings andSmartView Monitor to generate a graph showing the total HTTP traffic for the day
B. Select the "Tunnels" view, and generating a report on the statistics
C. View total packets passed through the Security Gateway
D. Configure a Suspicious Activity Rule which triggers an alert when HTTP traffic passes through the Gateway

Answer: A

QUESTION NO: 72

How do you recover communications between your SmartCenter Server and Security Gateway if you "lock" yourself out via a rule or policy mis-configuration?

A. cpstop
B. fw unload policy
C. fw delete all.all
D. fwunloadlocal

Answer: D

QUESTION NO: 73

Which command is used to uninstall the Security Policy directly from the Security Gateway?

A. fwm unload.local
B. fw kill policy
C. cpstop
D. fwunloadlocal

Answer: D

QUESTION NO: 74

You have two NOKIA Appliances: one IP530 and one IP380. Both appliances have IPSO 3.9 and NGX R65 VPN-1 Power installed in a distributed deployment. Can they be members of a Gateway Cluster?

A . No, because the appliances must be of the same model (both should be IP530 or IP380)

A. NO, because NOKIA does not have a cluster option.
B. Yes, as long as they have the same IPSO and VPN-1 versions.
C. NO, because the Security Gateways must be installed in a stand-alone installation.

Answer: C

QUESTION NO: 75

Your organization has many VPN-1 Edge Gateways at various branch offices, to allow 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;orthrougnthe center to other satellites, then to the Internet and other VPN targets
D. To the center only

Answer: C

QUESTION NO: 76

Your bank's distributed VPN-1 NGX R65 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

A. SmartUpdate
B. SmartView Tracker
C. SmartDashboard
D. SmartPortal

Answer: D

QUESTION NO: 77

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

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

Answer: C

QUESTION NO: 78

A marketing firm's networking team is trying to troubleshoot user complaints regarding access to audio-streaming material from the Internet. The networking team asks you to check the object and rule configuration settings for the perimeter Security Gateway. Which SmartConsole application should you use to check these objects and rules?

A. SmartViewTracker
B. SmartView Status
C. SmartView Monitor
D. SmartDashboard

Answer: B

QUESTION NO: 79

A third shift Security Administrator configured and installed a new Security Policy early this morning. When you arrive, he tells you that he has been receiving complaints that Internet access is very slow. You suspect the Security Gateway virtual memory might be the problem. How would you check this using SmartConsole?

A. SmartViewMonitor
B. SmartView Tracker
C. Eventia Analyzer
D. This information can only be viewed withfw ctl pstat command from the CLI.

Answer: A

QUESTION NO: 80

Which SmartView Tracker mode allows you to read the SMTP email body sent from the Chief Executive Officer (CEO)?

A. Log Tab
B. Display Capture Action
C. This is not aSmartView Tracker feature
D. Account Query

Answer: B

QUESTION NO: 81

The command fw fetch causes the:

A. SmartCenter Server to retrieve the debug logs of the target Security Gateway
B. Security Gateway to retrieve the user database information from the tables on theSmartCenter Server.
C. SmartCenter Server to retrieve the IP addresses of the target Security Gateway
D. Security Gateway to retrieve the compiled policy and inspect code from theSmartCenter Server and install it to the kernel

Answer: D

QUESTION NO: 82

Your bank's distributed VPN-1 NGX R65 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

A. Smartupdate
B. SmartView Tracker
C. SmartDashboard
D. SmartPortal

Answer: D

QUESTION NO: 83

When configuring Port Scanning, which level of sensitivity detects more than 100 inactive ports are tried for a period of 30 seconds?

A. LOW
B. High
C. None. Such a level does not exist.
D. Medium

Answer: D

QUESTION NO: 84

How do you define a service object for a TCP port range?

A. Manage Services, New Other, Provide name and define Protocol: x-y
B. Manage Services, New TCP, Provide name and define Port: x-y
C. Manage Services, New Other, Provide name and define Protocol: 17, Range: x-y
D. Manage Services, New Group, Provide name and Add all service ports for range individually to the group object

Answer: B

QUESTION NO: 85

You plan to migrate an NG with Application Intelligence (AI) R55 SmartCenter Server on Windows to VPN-1 NGX R65. You also plan to upgrade four VPN-1 Pro Gateways at remote offices, and one local VPN-1 Pro Gateway at your company's headquarters. The SmartCenter Server configuration must be migrated. What is the correct procedure to migrate the configuration?

A. 1. Upgrade the five remote Gateways via SmartUpdate.
2. Upgrade the SmartCenter Server, using the NGX R65 CD.
B. 1. From the VPN-1 NGX R65 CD on theSmartCenter Server, select "Upgrade".
2. Reboot after installation and upgrade all licenses via SmartUpdate.
3. Reinstall all gateways using NGX R65 and install a policy.
C. 1. From the VPN-1 NGX R65 CD in theSmartCenter Server, select "Export".
2. Install VPN-1 NGX R65 on a new PC using the option "Installation using imported configuration".
3. Reboot after installation and upgrade all licenses via SmartUpdate.
4. Upgrade software on all five remote Gateways via SmartUpdate.
D. 1.Copy the $FWDIR\conf directory from the SmartCenter Server.
2. Save directory contents to another file server.
3. Uninstall the SmartCenter Server, and install a new SmartCenter Server.
4. Move the saved directory contents to $FWDIR\conf replacing the default installation files.
5. Reinstall all gateways using VPN-1 NGX R65 and install a Security Policy.

Answer: C

QUESTION NO: 86

How do you recover communications between your SmartCenter Server and Security Gateway if you "lock" yourself out via a rule or policy mis-configuration?

A. cpstop
B. fw unload policy
C. fw delete all.all
D. fwunloadlocal

Answer: D

QUESTION NO: 87

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

A . Check Point Gateway

A. SmartCenterServer
B. SmartConsole
C. SmartUpdate upgrading/patching

Answer: A,C

Explanation:
When configuring VPN High Availability (HA) with MEP, which of the following is correct?

A. The decision on which MEP Security Gatewavto use is made on the remote gateway's side (non-MEP side).
B. MEP Gateways must be managed by the same SmartCenter Server.
C. MEP VPN Gateways cannot be geographically separated machines.
D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

QUESTION NO: 88

Which of the following is the most critical step in a SmartCenter Server NGX R65 backup strategy?

A. Perform a full system tape backup of both the SmartCenter and Security Gateway machines.
B. Run thecpstop command prior to running the upgrade_export command
C. Using theupgradejmport command, attempt to restore the SmartCenter Server to a non-production system
D. Move the *.tgzupgrade_export file to an off site location via ftp.

Answer: C

QUESTION NO: 89

The Web Filtering Policy can be configured to monitor URLs in order to:

A. Log sites that are currently being blocked.
B. Log sites from blocked categories.
C. Alert the Administrator to block a suspicious site.
D. Block sites only once.

Answer: B

QUESTION NO: 90

Your online bookstore has customers connecting to a variety of Web servers to place or change orders, and check order status. You ran penetration tests through the Security Gateway, to determine if the Web servers were protected from a recent series of cross-site scripting attacks. The penetration testing indicated the Web servers were still vulnerable. You have checked every box in the Web Intelligence tab, and installed the Security Policy. What else might you do to reduce the vulnerability?

A. Configure the Security Gateway protecting the Web servers as a Web server.
B. Check the "Products > Web Server" box on the host node objects representing your Web servers.
C. Configure resource objects as Web servers, and use them in the rules allowing HTTP traffic to the Web servers.
D. The penetration software you are using is malfunctioning and is reporting a false-positive.

Answer: C

QUESTION NO: 91

Upon checking SmartView Monitor, you find the following Critical Problem notification.What is the reason?

A. Version mismatch between theSmartCenter Server and Security Gateway
B. NO Secure Internal Communications established between theSmartCenter Server and Security Gateway
C. Time not synchronized between theSmartCenter Server and Security Gateway
D. No Security Policy installed on the Security Gateway

Answer: D

QUESTION NO: 92

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN.1 Power 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?

A. Usecpprod_util to reconfigure the primary SmartCenter Server to become the secondary on the VPN-1 Power Gateway. Install a new primary SmartCenter Server on the spare machine and set to "standby". Synchronize the "active" secondary to the "standby" primary in order to migrate the configuration.
B. Install the secondary Server on the spare machine. Add the new machine to any network routable to the primary Server. Synchronize the machines.
C. You cannot configure Management HA, when either the primary or secondarySmartCenter Server is running on a VPN-1 Pro Gateway.
D. Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server. Synchronize the machines.

Answer: C

QUESTION NO: 93

You have two NOKIA Appliances: one IP530 and one IP380. Both appliances have IPSO 3.9 and NGX R65 VPN-1 Power installed in a distributed deployment. Can they be members of a Gateway Cluster?

A. No, because the appliances must be of the same model (both should be IP530 or IP380).
B. NO, because NOKIA does not have a cluster option.
C. Yes, as long as they have the same IPSO and VPN-1 versions.
D. NO, because the Security Gateways must be installed in a stand-alone installation.

Answer: C

QUESTION NO: 94

When configuring Port Scanning, which level of sensitivity detects more than 100 inactive ports are tried for a period of 30 seconds?

A. LOW
B. High
C. None. Such a level does not exist.
D. Medium

Answer: D

QUESTION NO: 95 CORRECT TEXT

You are administering your company's Clientless VPN connections. How many Security Servers should you be running to support 750 active users? A. 3 B. 7 C. 5 D. 1

Answer: C

QUESTION NO: 96

How do you view a Security Administrator's activities, using SmartConsole tools?

A. SmartView Tracker in Log mode
B. Eventia Suite
C. SmartView Monitor using the Administrator Activity filter
D. SmartView Tracker in Audit mode

Answer: D

QUESTION NO: 97

The Check Point ClusterXL mode must synchronize the physical interface IP and MAC addresses on all clustered interfaces

A. New Mode HA
B. Legacy Mode HA
C. Multicast Mode Load Sharing
D. Pivot Mode Load Sharing

Answer: B

QUESTION NO: 98

Which of the following is TRUE concerning unnumbered VPN Tunnel Interfaces (VTIs)?

A. VTIs cannot be assigned a proxy interface
B. Local IP addresses are not configured, remote IP addresses are configured
C. VTIs are only supported onSecurePlatform
D. VTI specific additional local and remote IP addresses are not configured

Answer: D

QUESTION NO: 99

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

A. assld
B. fwd
C. fwm
D. cpp

Answer: B

QUESTION NO: 100

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

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

Answer: D

QUESTION NO: 101

Which of the following is NOT supported with Office Mode?

A. SSL Network Extender
B. L2TP
C. SecureClient

D. Transparent Mode

Answer: D

QUESTION NO: 102

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

A. Exchange exportedCAkeys and uses them to create a new server object to represent your partner's Certificate Authority (CA).
B. Manually import your partner's Access Control List.
C. Manually import your partner's Certificate Revocation List.
D. Create a new logical-server object to represent your partner's CA.

Answer: A

QUESTION NO: 103

You are establishing a ClusterXL environment, with the following topology: VIP internal cluster IP = 172.16.10.3; VIP external cluster IP = 192.168.10.3 ClusterMember1:4NICs,3enabled: hme(): 192.168.10.1/24, hmel: 10.10.10.1/24, qfe2: 172.16.10.1/24 Cluster Member 2: 5 NICs, 3 enabled; hme3: 192.168.10.2/24, hmel: 10.10.10.2/24, hme2: 172.16.10.2/24 External interfaces 192.168.10.1 and 192.168.10.2 connect to a VLAN switch. The upstream router connects to the same VLAN switch. Internal interfaces 172.16.10.1 and 172.16.10.2 connect to a hub. 10.10.10.0 is the synchronization network. The SmartCenter Server is located on the internal network with IP 172.16.10.3. What is the problem with this configuration?

A. There is an IP address conflict.
B. Cluster members cannot use the VLAN switch. They must use hubs.
C. The Cluster interface names must be identical across all cluster members.
D. The SmartCenter Server must be in the dedicated synchronization network, not the internal network.

Answer: A

QUESTION NO: 104

Which utility allows you to configure the DHCP service on SecurePlatform from the command line?

A. WebUI

B. cpconfig
C. ifconfig
D. sysconfig

Answer: D

QUESTION NO: 105 CORRECT TEXT

Where do you enable popup alerts for SmartDefense settings that have detected suspicious activity?

A . In SmartView Monitor, select Tools > Alerts
B . In SmartView Tracker, select Tools > Custom Commands

Answer: A

QUESTION NO: 106

You have three Gateways in a mesh community. Each gateway's VPN Domain is their internal network as defined on the Topology tab setting "All IP Addresses behind Gateway based on Topology information." You want to test the route-based VPN, so you created VTIs among the Gateways and created static route entries for the VTIs. However, when you test the VPN, you find out the VPN still go through the regular domain IPSec tunnels instead of the routed VTI tunnels. What is the problem and how do you make the VPN to use the VTI tunnels?

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

Answer: D

QUESTION NO: 107

You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use four machines with the following configurations: Cluster Member 1: OS: SecurePlatform, NICs:

QuadCard, memory: 512 MB, Security Gateway only, and version: VPN-1 NGX R65
Cluster Member 2: OS: SecurePlatform, NICs: 4 Intel 3Com, memory: 512 MB, Security Gateway only, and version: VPN-1 NGX R65 Cluster Member 3: OS: SecurePlatform, NICs: 4 other manufacturers, memory: 256 MB, Security Gateway only, and version: VPN-1 NGX R65
SmartCenter Server: MS Windows 2000, NIC: Intel NIC (1), Security Gateway and primary SmartCenter Server installed, version: VPN-1 NGX R65 Are these machines correctly configured for a ClusterXL deployment?

A. No, Cluster Member 3 does not have the required memory.
B. NO, the Security Gateway cannot be installed on theSmartCenter Pro Server.
C. Yes, these machines are configured correctly for aClusterXL deployment.
D. NO, theSmartCenter Pro Server is not running the same operating system as the cluster members.

Answer: C

QUESTION NO: 108

Which of the following statements about file-type recognition in Content Inspection is TRUE?

A. A scan failure will only occur if the antivirus engine fails to initialize.
B. Antivirus status is monitored usingSmartView Tracker.
C. The antivirus engine acts as a proxy, caching the scanned file before delivering it to the client.
D. All file types are considered "at risk", and are not subject to the whims of the Administrator or the Security Policy

Answer: C

QUESTION NO: 109

What is a Consolidation Policy?

A. A global Policy used to share a common enforcement policy for multiple similar Security Gateways
B. The collective name of the logs generated byEventia Reporter
C. The collective name of the Security Policy, Address Translation, andSmartDefense Policies
D. The specific Policy written inSmartDashboard to configure which log data is stored in the Eventia Reporter database

Answer: D

QUESTION NO: 110

A third shift Security Administrator configured and installed a new Security Policy early this morning. When you arrive, he tells you that he has been receiving complaints that Internet access is very slow. You suspect the Security Gateway virtual memory might be the problem. How would you check this using SmartConsole?

A. SmartView Monitor
B. SmartView Tracker
C. Eventia Analyzer
D. This information can only be viewed withfw ctl pstat command from the CLI.

Answer: A

QUESTION NO: 111

What port is used for communication to the User Center with SmartUpdate?

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

Answer: C

QUESTION NO: 112

Which VPN-1 NGX R65 component displays the number of packets accepted, rejected, and dropped on a specific Security Gateway, in real time?

A. SmartView Monitor
B. SmartView Status
C. SmartUpdate
D. Eventia Analyzer

Answer: D

QUESTION NO: 113

Which command line interface utility allows the administrator to verify the name and timestamp of the Security Policy currently installed on a firewall module?

A. fwver
B. fw stat
C. fw ctl pstat
D. cpstatfwd

Answer: B

QUESTION NO: 114

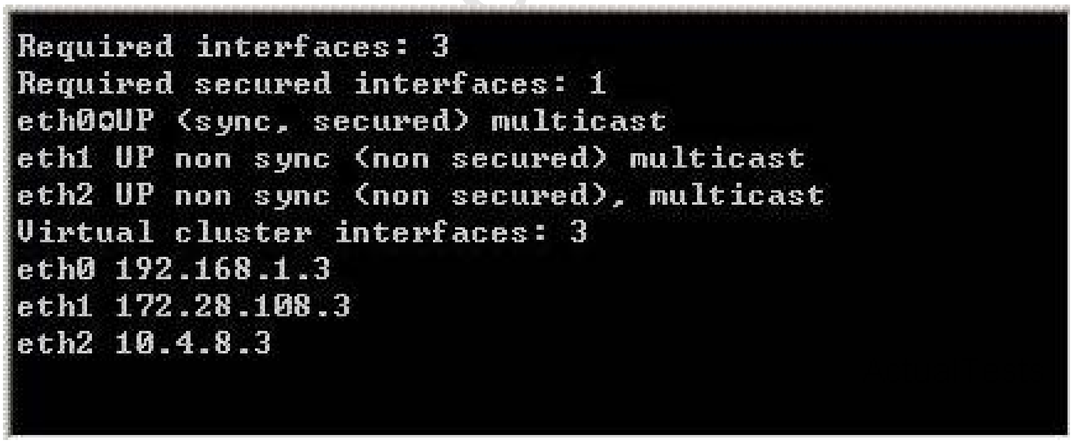
If you are experiencing LDAP issues, which of the following should you check?

A. Connectivity between the NGX gateway and LDAP server
B. Secure Internal Communications (SIC)
C. VPN Load Balancing
D. Overlapping VPN Domains
Overlapping VPN Domains

Answer: D

QUESTION NO: 115

An NGXR65 HA 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 VIP address is 172.28.108.3 and the internal cluster VIP 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. The cphaprob if command output displays shows:What is causing the State Synchronization problem?



```
Required interfaces: 3
Required secured interfaces: 1
eth0OUP (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. Overlapping VPN Domains
Overlapping VPN Domains
B. The synchronization network has been defined as "Network Objective: Cluster + 1st sync" with an IP address 192.168.1.3 defined in the NGX cluster object's topology. This configuration is supported in NGX and therefore the above screenshot is not relevant to the sync problem.

C. The synchronization interface on the individual NGX cluster member object's Topology tab is enabled with "Cluster Interface". Disable this setting.
D. The synchronization network has a cluster VIP address (192.168.1.3) defined in the NGX cluster object's topology. Remove the 192.168.1.3 VIP interface from the cluster topology.
E. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.

Answer: A

QUESTION NO: 116

The Check Point Security Gateway's virtual machine (kernel) exists between which two layers of the OSI model?

A. Physical and Data Link layers
B. Application and Presentation layers
C. Network and Data Link layers
D. Session and Network layers

Answer: B

QUESTION NO: 117

Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?

A. VTIS are supported onSecurePlatform
B. VTIS cannot share IP addresses
C. VTIs can use an already existingphysical.interface IP address
D. VTIS are assigned only local addresses, not remote addresses

Answer: A

QUESTION NO: 118

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

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

Answer: B

QUESTION NO: 119

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

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

Answer: A

QUESTION NO: 120

Which of the following would NOT be a reason for beginning with a fresh installation of VPN.1 NGX R65, instead of upgrading a previous version to VPN.1 NGX R65?

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

Answer: B

QUESTION NO: 121

Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Why?

A. Users must use theSecuRemote Client, to use the User Authentication Rule.
B. YOU have forgotten to place the User Authentication Rule before the Stealth Rule.
C. You checked the "cache password on desktop" option in Global Properties.
D. Another rule that accepts HTTP without authentication exists in the Rule Base.

Answer: B

QUESTION NO: 122

Match the Best Management High Availability synchronization.status descriptions for your SmartCenter Server (SCS)

A. A3.B 1.C2.D4
B. A4.B3.C 1.D2
C. A3.B2.C 1.D4
D. A3.B 1.C4.D2

Answer: A

QUESTION NO: 123

When you check "Web Server" in a host.node object, what happens to the host?

A. The Web server daemon is enabled on the host.
B. More granular controls are added to the host, in addition to Web Intelligence tab settings.
C. You can specify allowed ports in the Web server'snode.object properties. You then do not need to list all allowed ports in the Rule Base
D. SmartDefense Web Intelligence is enabled to check on the host.

Answer: B

QUESTION NO: 124

Where do you enable popup alerts for SmartDefense settings that have detected suspicious activity?

A. In SmartView Monitor, select Tools > Alerts
B. In SmartView Tracker, select Tools > Custom Commands
C In SmartDashboard, edit the Gateway object, select SmartDefense > Alerts
D. In SmartDashboard, select Global Properties > Log and Alert > Alert Commands

Answer: A

QUESTION NO: 125

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

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

Answer: B

QUESTION NO: 126

Where is it necessary to configure historical records in SmartView Monitor to generate Express reports in Eventia Reporter?

A. In SmartDashboard, the SmartView Monitor page in the VPN-1 Security Gateway object
B. InEventia Reporter, under Express > Network Activity
C. InEventia Reporter, under Standard > Custom
D. InSmartView Monitor, under Global Properties > Log and Masters

Answer: A

QUESTION NO: 127

What command displays the version of an already installed Security Gateway?

A. cpstat-gw
B. fw printver
C. fwver
D. fw stat

Answer: C

QUESTION NO: 128

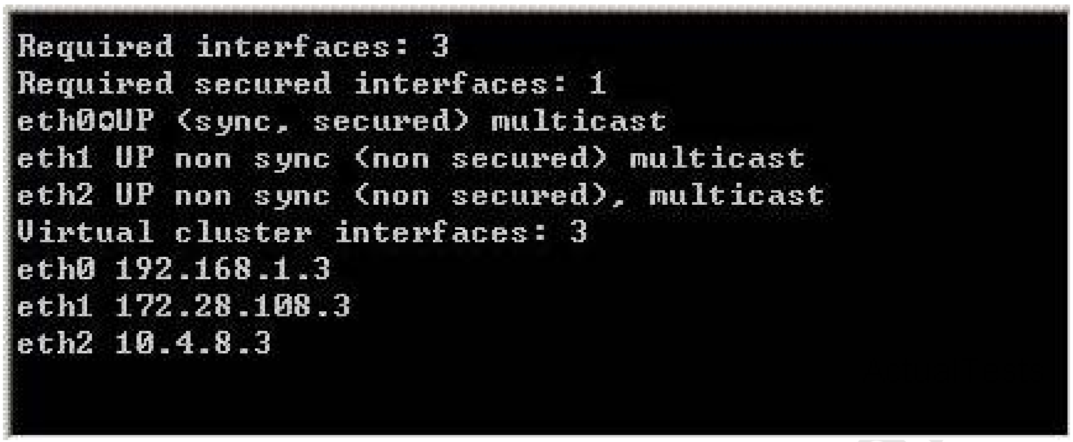
When configuring VPN High Availability (HA) with MEP, which of the following is correct?

A. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
B. MEP Gateways must be managed by the sameSmartCenter Server.
C. MEP VPN Gateways cannot be geographically separated machines.
D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

Answer: A

QUESTION NO: 129

An NGXR65 HA 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 VIP address is 172.28.108.3 and the internal cluster VIP 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. The cphaprob if command output displays shows:What is causing the State Synchronization problem?



```
Required interfaces: 3
Required secured interfaces: 1
eth0oUP (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. The synchronization network has been defined as "Network Objective: Cluster + 1st sync" with an IP address 192.168.1.3 defined in the NGX cluster object's topology. This configuration is supported in NGX and therefore the above screenshot is not relevant to the sync problem.
B. The synchronization interface on the individual NGX cluster member object's Topology tab is enabled with "Cluster Interface". Disable this setting.
C. The synchronization network has a cluster VIP address (192.168.1.3) defined in the NGX cluster object's topology. Remove the 192.168.1.3 VIP interface from the cluster topology.
D. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.

Answer: A

QUESTION NO: 130

Which utility allows you to configure the DHCP service on SecurePlatform from the command line?

A. WebUI
B. cpconfig
C. ifconfig
D. sysconfig

Answer: D

QUESTION NO: 131

Multi-Corp wants to implement IKE DoS protection to prevent a denial-of-service (DoS) attack from paralyzing its VPN Communities. Jerry needs to minimize the performance impact of implementing this new protection. Which of the following configurations would BEST enable this new protection with minimal impact to the organization?

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

Answer: C

QUESTION NO: 132

You are concerned that your company's servers might be vulnerable to an attack where a client fools a server into sending large amounts of data, using small packets. Which SmartDefense option should you use to protect the servers?

A. Network Security > Denial of Service > Non-TCP Flooding
B. Network Security > Denial of Service > LAND
C. Network Security > IP and ICMP > Block Null Payload ICMP
D. Network Security > TCP > Small PMTU

Answer: D

QUESTION NO: 133

Your organization's disaster recovery plan needs an update to the backup and restore section to realize the benefits of the new distributed VPN-1 NGX R65 installation. You want to document a plan to 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 Your disaster recovery plan is as follows:? 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? Configure the SecurePlatform backup utility to back up the Security Gateways every Saturday night? 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. Upon evaluation, your plan:

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

Answer: D

QUESTION NO: 134

Which of the following generates an Eventia Report from its SQL database?

A. SmartCenterServer
B. SmartDashboard Log Consolidator
C. Eventia Reporter Client
D. Eventia Reporter Server

Answer: D

QUESTION NO: 135

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. Exchange exported CA keys and uses them to create a new server object to represent your partner's Certificate Authority (CA).
B. Manually import your partner's Access Control List.
C. Manually import your partner's Certificate Revocation List.
D. Create a new logical-server object to represent your partner's CA.

Answer: A

QUESTION NO: 136

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

A. Members A and B are synchronized, because #SLINKS are identical in the connections table.
B. Members A and B are not synchronized, because #VALS in the connections table are not close.
C. Members A and B are not synchronized, because #PEAKfor both members is not close in the connections table.

D. Members A and B are synchronized, because ID for both members is identical in the connections table.

Answer: B

QUESTION NO: 137

Which command would provide the most comprehensive diagnostic information to Check Point Technical Support?

A. cpinfo date.cpinfo.txt
B. cpstat> date.cpstat.txt
C. netstat > date.netstat.txt
D. diag

Answer: A

QUESTION NO: 138

Antivirus protection on a VPN-1 Gateway is available for all of the following protocols, EXCEPT

A. POP3
B. TELNET
C. HTTP
D. FTP

Answer: B

QUESTION NO: 139

How do you define a service object for a TCP port range?

A. Manage Services, New Other, Provide name and define Protocol: x-y
B. Manage Services, New TCP, Provide name and define Port: x-y
C. Manage Services, New Other, Provide name and define Protocol: 17, Range: x-y
D. Manage Services, New Group, Provide name and Add all service ports for range individually to the group object

Answer: B

QUESTION NO: 140

How do you define a service object for a TCP port range?

A. Manage Services, New Other, Provide name and define Protocol: x-y
B. Manage Services, New TCP, Provide name and define Port: x-y
C. Manage Services, New Other, Provide name and define Protocol: 17, Range: x-y
D. Manage Services, New Group, Provide name and Add all service ports for range individually to the group object

Answer: B

QUESTION NO: 141

Your online bookstore has customers connecting to a variety of Web servers to place or change orders, and check order status. You ran penetration tests through the Security Gateway, to determine if the Web servers were protected from a recent series of cross-site scripting attacks. The penetration testing indicated the Web servers were still vulnerable. You have checked every box in the Web Intelligence tab, and installed the Security Policy. What else might you do to reduce the vulnerability?

A. Configure the Security Gateway protecting the Web servers as a Web server.
B. The penetration software you are using is malfunctioning and is reporting a false-positive.
C. Check the "Web Intelligence" box in theSmartDefense > HTTP Protocol Inspection.
D. Check the "Products > Web Server" box on the host node objects representing your Web servers.

Answer: C

QUESTION NO: 142

What is a Consolidation Policy?

A. A global Policy used to share a common enforcement policy for multiple similar Security Gateways
B. The collective name of the logs generated byEventia Reporter
C. The collective name of the Security Policy, Address Translation, andSmartDefense Policies
D. The specific Policy written inSmartDashboard to configure which log data is stored in the Eventia Reporter database

Answer: D

QUESTION NO: 143

How do you use SmartView Monitor to compile traffic statistics for your company's Internet activity during production hours?

A. Use the "Traffic Counters" settings andSmartView Monitor to generate a graph showing the total HTTP traffic for the day
B. Select the "Tunnels" view, and generating a report on the statistics
C. View total packets passed through the Security Gateway
D. Configure a Suspicious Activity Rule which triggers an alert when HTTP traffic passes through the Gateway

Answer: A

QUESTION NO: 144

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

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

Answer: B

QUESTION NO: 145

Which command line interface utility allows the administrator to verify the name and timestamp of the Security Policy currently installed on a firewall module?

A. fwver
B. fw stat
C. fw ctl pstat
D. cpstatfwd

Answer: B

QUESTION NO: 146

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

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

A. 1.3.4.S6
B. 1 &4
C. 4.5.S6
D. 2,4,5,&6

Answer: D

QUESTION NO: 147

How do you view a Security Administrator's activities, using SmartConsole tools?

A. SmartView Tracker in Log mode
B. Eventia Suite
C. SmartView Monitor using the Administrator Activity filter
D. SmartView Tracker in Audit mode

Answer: D

QUESTION NO: 148

Which SmartView Tracker mode allows you to read the SMTP email body sent from the Chief Executive Officer (CEO)?

A. Log Tab
B. Display Capture Action
C. This is not aSmartView Tracker feature
D. Account Query

Answer: B

QUESTION NO: 149

Which of the following statements about the Port Scanning feature of SmartDefense is TRUE?

A. When a port scan is detected, only a log isissued ?never an alert.
B. The Port Scanning feature actively blocks the scanning, and sends an alert to SmartView Monitor.
C. A typical scan detection is when more than 500 open inactive ports are open for a period of 120 seconds.
D. Port Scanning does not blockscanning, it detects port scans with one of three levels of detection sensitivity

Answer: D

QUESTION NO: 150

You plan to migrate an NG with Application Intelligence (Al) R55 SmartCenter Server on Windows to VPN-1 NGX R65. You also plan to upgrade four VPN-1 Pro Gateways at remote offices, and one local VPN-1 Pro Gateway at your company's headquarters. The SmartCenter Server configuration must be migrated. What is the correct procedure to migrate the configuration?

A. 1. Upgrade the five remote Gateways via SmartUpdate.
2. Upgrade the SmartCenter Server, using the NGX R65 CD.
B. 1. From the VPN-1 NGX R65 CD on theSmartCenter Server, select "Upgrade".
2. Reboot after installation and upgrade all licenses via SmartUpdate.
3. Reinstall all gateways using NGX R65 and install a policy.
C. 1. From the VPN-1 NGX R65 CD in theSmartCenter Server, select "Export".
2. Install VPN-1 NGX R65 on a new PC using the option "Installation using imported configuration".
3. Reboot after installation and upgrade all licenses via SmartUpdate.
4. Upgrade software on all five remote Gateways via SmartUpdate.
D. 1.Copy the $FWDIR\conf directory from the SmartCenter Server.
2. Save directory contents to another file server.
3. Uninstall the SmartCenter Server, and install a new SmartCenter Server.
4. Move the saved directory contents to $FWDIR\conf replacing the default installation files.
5. Reinstall all gateways using VPN-1 NGX R65 and install a Security Policy.

Answer: C

QUESTION NO: 151

What is the command in SecurePlatform Expert shell used to add routes without the use of sysconfig or the WebUI?

A. ifroute

B. ifconfig
C. sysconfig route
D. ip route

Answer: D

QUESTION NO: 152

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

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

Answer: B

QUESTION NO: 153

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

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

Answer: B

QUESTION NO: 154

Which of the following would NOT be a function of the Check Point license-upgrade tool?

A. Upgrade locally managed licenses.
B. Simulate the license-upgrade process.
C. Manually upgrade a specific license.
D. View the status of the currently installed licenses.

Answer: C

QUESTION NO: 155

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

A. Multi-connection support for VPN-1 cluster members
B. Support for Performance Pack acceleration
C. Support for all VPN deployments (except those with third-party VPN peers)
D. Support forSecureClient/SecuRemote/SSL Network Extender encrypted connections

Answer: D

QUESTION NO: 156

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

A. Connectivity between the NGX gateway and LDAP server
B. Secure Internal Communications (SIC)
C. VPN Load Balancing
D. Overlapping VPN Domains

Answer: C

QUESTION NO: 157

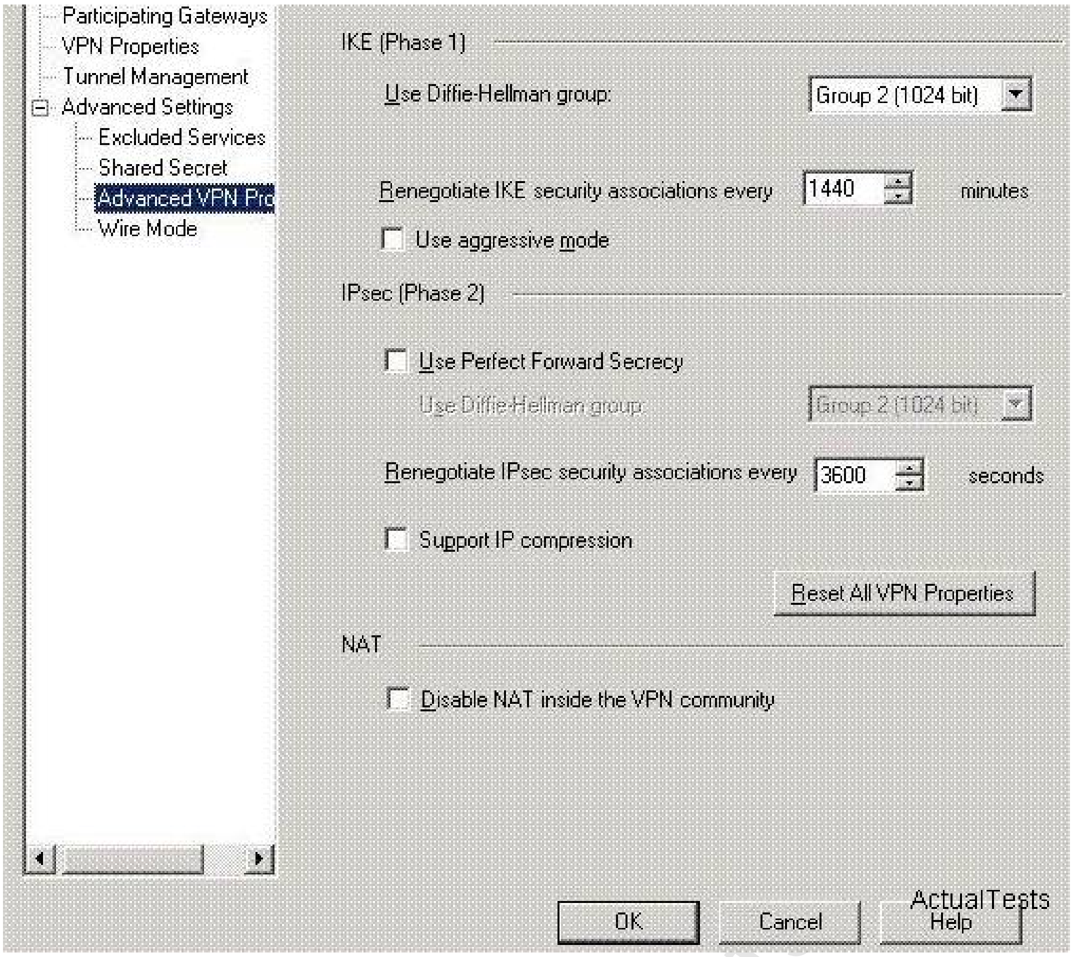
Which Check Point product is used to create and save changes to a Log Consolidation Policy?

A. Eventia Reporter Client
B. SmartDashboard Log Consolidator
C. SmartCenterServer
D. Eventia Reporter Server

Answer: B

QUESTION NO: 158

Look at the Advanced Properties screen exhibit. What settings can you change to reduce the encryption overhead and improve performance for your mesh VPN Community?



IKE (Phase 1)

Use Diffie-Hellman group: Group 2 (1024 bit)

Renegotiate IKE security associations every 1440 minutes

□ Use aggressive mode

IPsec (Phase 2)

□ Use Perfect Forward Secrecy

Use Diffie-Hellman group: Group 2 (1024 bit)

Renegotiate IPsec security associations every 3600 seconds

□ Support IP compression

NAT

□ Disable NAT inside the VPN community

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

Answer: B

QUESTION NO: 159

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

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

Answer: C

QUESTION NO: 160

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN-1 Power 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?

A. Usecpprod_util to reconfigure the primary SmartCenter Server to become the secondary on the VPN-1 Power Gateway. Install a new primary SmartCenter Server on the spare machine and set to "standby". Synchronize the "active" secondary to the "standby" primary in order to migrate the configuration.
B. Install the secondary Server on the spare machine. Add the new machine to any network routable to the primary Server. Synchronize the machines.
C. You cannot configure Management HA, when either the primary or secondarySmartCenter Server is running on a VPN-1 Pro Gateway.
D. Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server. Synchronize the machines.

Answer: C

QUESTION NO: 161

The Check Point ClusterXL mode must synchronize the physical interface IP and MAC addresses on all clustered interfaces

A. New Mode HA
B. Legacy Mode HA
C. Multicast Mode Load Sharing
D. Pivot Mode Load Sharing

Answer: B

QUESTION NO: 162

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

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

Answer: C

QUESTION NO: 163

Which utility allows you to configure the DHCP service on SecurePlatform from the command line?

A. WebUI
B. cpconfig
C. ifconfig
D. sysconfig

Answer: D

QUESTION NO: 164

A VPN Tunnel Interface (VTI) is defined on SecurePlatform Pro as: vpn shell interface add numbered 10.10.0.1 10.10.0.2 madrid.cp What do you know about this VTI?

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

Answer: B

QUESTION NO: 165

The customer has a small Check Point installation which includes one Window XP workstation working as SmartConsole one Solaris server working as SmartCenter, and a third server running SecurePlatform working as Security Gateway. This is an example of:

A Hybrid Installation

A. Unsupported configuration
B. Stand-Alone Installation
C. Distributed Installation

Answer: A

QUESTION NO: 166

Your bank's distributed VPN-1 NGX R65 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

A. SmartUpdate
B. SmartViewTracker
C. SmartDashboard
D. SmattPortal

Answer: D

QUESTION NO: 167

Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?

A VTIs are supported on SecurePlatform

A. VTIS cannot share IP addresses
B. VTIs can use an already existing physical-interface IP address
C. VTIS are assigned only local addresses, not remote addresses

Answer: A

QUESTION NO: 168

Your VPN-1 NGX R65 primary SmartCenter Server is installed on SecurePlatform. You plan to schedule the SmartCenter Server to run fw logswitch automatically every 48 hours. How do you create this schedule?

A. Create a time object, and add 48 hours as the interval. Select that time object's Global Properties > Logs and Masterswindow, to schedule a logswitch.
B. Create a time object, and add 48 hours as the interval. Open the Security Gateway object's Logs and Masterswindow, enable "Schedule log switch", and select the time object.
C. Create a time object, and add 48 hours as the interval. Open the primarySmartCenter Server object's Logs and Masters window, enable "Schedule log switch", and select the Time object.
D. On aSecurePlatform SmartCenter Server, this can only be accomplished by configuring the fw logswitch command via the cron utility.

Answer: C

QUESTION NO: 169

Central License management allows a Security Administrator to perform which of the following functions?

(1) Check for expired licenses.
(2) Sort licenses and view license properties.
(3) Attach both NGX Central and Local licenses to a remote module.
(4) Delete both NGX Local licenses and Central licenses from a remote module.
(5) Add or remove a license to or from the license repository.
(6) Attach and/or delete only NGX Central licenses to a remote module (not Local licenses).

A. 1,2,3,4,&5
B. 1.2.5.&6
C. 2,3,4,&5
D. 2. 5. &6

Answer: A

QUESTION NO: 170

Which utility allows you to configure the DHCP service on SecurePlatform from the command line?

A. WebUI
B. cpconfig
C. ifconfig
D. sysconfig

Answer: D

QUESTION NO: 171

Which VPN-1 NGX R65 component displays the number of packets accepted, rejected, and dropped on a specific Security Gateway, in real time?

A. SmartUpdate
B. SmartView Monitor
C. SmartView Status
D. Eventia Analyzer

Answer: B

QUESTION NO: 172

Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?

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

Answer: A

QUESTION NO: 173

Which of the following is the most critical step in a SmartCenter Server NGX R65 backup strategy?

A. Perform a full system tape backup of both theSmartCenter and Security Gateway machines.
B. Run thecpstop command prior to running the upgrade_export command
C. Using theupgradejmport command, attempt to restore the SmartCenter Server to a non-production system
D. Move the *.tgzupgrade_export file to an off site location via ftp.

Answer: C

QUESTION NO: 174

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

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

Answer: B

QUESTION NO: 175

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

A. 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.

B. Add the secondarySmartCenter Server object as a backup log server in the "Log Servers" window (under the "Logs and Masters" tab on the Gateway object). Reinstall the Security Policy.
C. The secondary Server's host name and IP address must be added to the Masters file on the remote Gateways.
D. Create a Check Point host object to represent the standbySmartCenter Server. Then select "Secondary SmartCenter Server" and "Log Server", from the list of Check Point Products on the General Properties window.

Answer: B

QUESTION NO: 176

A marketing firm's networking team is trying to troubleshoot user complaints regarding access to audio-streaming material from the Internet. The networking team asks you to check the object and rule configuration settings for the perimeter Security Gateway. Which SmartConsole application should you use to check these objects and rules?

A. SmartViewTracker
B. SmartView Status
C. SmartView Monitor
D. SmartDashboard

Answer: B

QUESTION NO: 177

Which of the following statements about the Port Scanning feature of SmartDefense is TRUE?

A. When a port scan is detected, only a log isissued ?never an alert.
B. The Port Scanning feature actively blocks the scanning, and sends an alert to SmartView Monitor.
C. A typical scan detection is when more than 500 open inactive ports are open for a period of 120 seconds.
D. Port Scanning does not blockscanning, it detects port scans with one of three levels of detection sensitivity

Answer: D

QUESTION NO: 178

What must a public hospital Security Administrator do to comply with new health-care legislation requirements for logging all traffic accepted through the perimeter Security Gateway?

A. Define two log servers on the VPN-1 NGX R65 Gateway object. Enable "Log Implied Rules" on the first log server. Enable "Log Rule Base" on the second log server. UseEventia Reporter to merge the two log server records into the same database for HIPPA log audits.
B. Install the "View Implicit Rules" package usingSmartUpdate.
C. In Global Properties > Reporting Tools check the box "Enable tracking all rules (including rules marked as 'None' in the Track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.
D. Check the "Log Implied Rules Globally" box on the VPN-1 NGX R65 Gateway object.

Answer: C

QUESTION NO: 179

When launching SmartDashboard, what information is required to log into VPN-1 NGX R65?

A. User Name, Password,SmartCenter Server IP
B. User Name,SmartCenter Server IP, certificate fingerprint file
C. Password,SmartCenter Server IP, LDAP Server
D. Password,SmartCenter Server IP

Answer: B

QUESTION NO: 180

SmartDefense profiles are:

A. Files that take 3MB of RAM from the user console machine.
B. Able to be cloned, but only from the command line.
C. Configurable up to 20 for all VPN-1 R65 Gateways and above.
D. Configurable from either theSmartDefense tab or from the Gateway itself.

Answer: D

QUESTION NO: 181

Which specific VPN-1 NGX R65 GUI would you use to view the length of time a TCP connection was open?

A. SmartView Tracker
B. SmartView Status
C. SmartLSM

D. SmartView Monitor

Answer: A

QUESTION NO: 182

Users are not prompted for authentication when they access their Web servers, even though you ave created an HTTP rule via User Authentication. Why?

A. Users must use theSecuRemote Client, to use the User Authentication Rule.
B. YUhave forgotten to place the User Authentication Rule before the Stealth Rule.
C. You checked the "cache password on desktop" option in Global Properties.
D. Another rule that accepts HTTP without authentication exists in the Rule Base.

Answer: B

QUESTION NO: 183

When synchronizing clusters, which of the following statements is NOT true?

A. User Authentication connections will be lost by the cluster.
B. Only cluster members running on the same OS platform can be synchronized.
C. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization
D. An SMTP resource connection using CVP will be maintained by the cluster.

Answer: D

QUESTION NO: 184

SmartView Tracker logs the following Security Administrator activities, EXCEPT

A. Administrator login and logout.
B. Object creation, deletion, and editing.
C. Tracking SLA compliance.
D. Rule Base changes.

Answer: C

QUESTION NO: 185

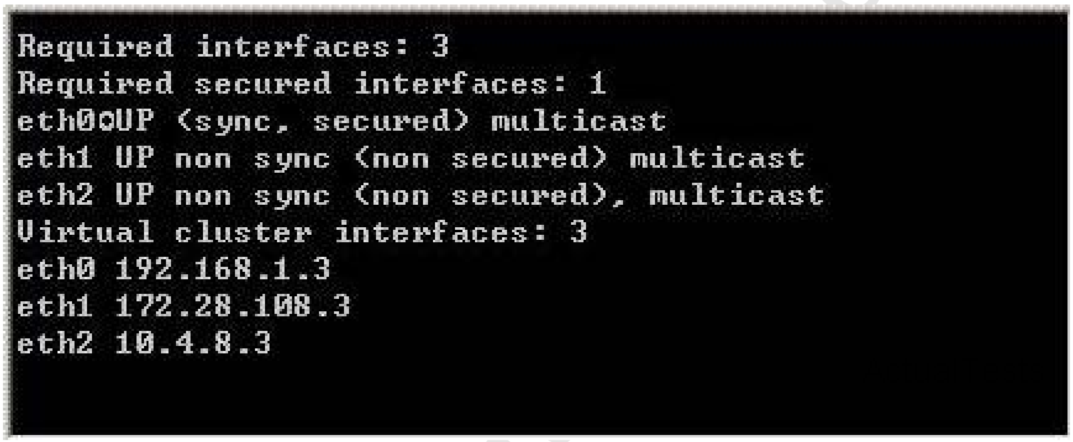
What information is found in the SmartView Tracker audit log?

A. SIC revoke certificate event
B. Number of concurrent IKE negotiations
C. Destination IP address
D. Most accessed Rule Base rule

Answer: A

QUESTION NO: 186

An NGXR65 HA 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 VIP address is 172.28.108.3 and the internal cluster VIP 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. The cphaprob if command output displays shows:What is causing the State Synchronization problem?



```
Required interfaces: 3
Required secured interfaces: 1
eth0oUP (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. The synchronization network has been defined as "Network Objective: Cluster + 1st sync" with an IP address 192.168.1.3 defined in the NGX cluster object's topology. This configuration is supported in NGX and therefore the above screenshot is not relevant to the sync problem.
B. The synchronization interface on the individual NGX cluster member object's Topology tab is enabled with "Cluster Interface". Disable this setting.
C. The synchronization network has a cluster VIP address (192.168.1.3) defined in the NGX cluster object's topology. Remove the 192.168.1.3 VIP interface from the cluster topology.
D. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.

Answer: A

QUESTION NO: 187

What must a public hospital Security Administrator do to comply with new health-care legislation requirements for logging all traffic accepted through the perimeter Security Gateway?

A. Define two log servers on the VPN-1 NGX R65 Gateway object. Enable "Log Implied Rules" on the first log server. Enable "Log Rule Base" on the second log server. UseEventia Reporter to merge the two log server records into the same database for HIPPA log audits.
B. Install the "View Implicit Rules" package usingSmartUpdate.
C. In Global Properties > Reporting Tools check the box "Enable tracking all rules (including rules marked as 'None' in the Track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.
D. Check the "Log Implied Rules Globally" box on the VPN-1 NGX R65 Gateway object.

Answer: C

QUESTION NO: 188

You want to upgrade a cluster with two members to VPN-1 NGX R65. 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. 1,3,2,4
B. 2,3, 1,4
C. 2,4,3, 1
D. 3,2, 1,4

Answer: B

QUESTION NO: 189

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

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

Answer: A

QUESTION NO: 190

Your network includes a SecurePlatform machine running NG with Application Intelligence (Al) R55. This configuration acts as both the primary SmartCent Server and VPN-1 Pro Gateway. You add one machine, so you can implement VPN-1 NGX R65 in a distributed environment. The new machine is an Intel CoreDuo processor, with 2 GB RAM and a 500-GB hard drive. How do you use these two machines to successfully migrate the NG with Al R55 configuration?

A. 1. On the existing machine, export the NG with Al R55 configuration to a network share.
2. Insert the NGXR65 CD-ROM in the old machine. Install the NGXR65 Security Gateway only while reinstalling the SecurePlatform OS over the to of the existing installation. Complete sysconfig.
4. On the new machine, install SecurePlatform as the primary SmartCenter Server only.
5. Transfer the exported .tgzfile into the new machine, import the configuration, and then reboot.
6. Open SmartDashboard, change the Gateway object to the new version, and reset SIC for the Gateway object.
B. 1. Export the configuration on the existing machine to a network share.
2. Uninstall the Security Gateway from the existing machine, using sysconfig.
3. Insert the NGX R65 CD-ROM, and run the patch add cd command to upgrade the SmartCenter Server to VPN-1 NGX R65.
4. Select "upgrade with imported file", and reboot.
5. Install a new NGX R65 Security Gateway as the only module on the new machine, and reset SIC to the new Gateway.
C. 1. Export the configuration on the existing machine to a tape drive.
2. Uninstall the SmartCenter Server from the existing machine, using sysconfig.
3. Insert the NGX R65 CD-ROM, run the patch add cd command to upgrade the existing machine to the NGX R65 Security Gateway, and reboot.
4. Install a new primary SmartCenter Server on the new machine.
5. Change the gateway object to the new version, and reset SIC.
D. 1. Export the configuration on the existing machine as a backup only.
2. Edit $FWDIR\product.conf on the existing machine, to disable the Pro gateway package.
3. Reboot the existing machine.
4. Perform an in-place-upgrade on the SmartCenter using the command "patch add cd".
5. On the new machine, install SecurePlatform as the NGX R65 Security Gateway only.
6. Run sysconfig to complete the configuration.
7. From SmartDashboard, reconfigure the Gateway object to the new version, and reset SIC.

Your company enforces a strict change control policy, which of the following would be best to quickly drop an attacker's specific active connection?
E. Change the Rule Base and install the policy to all security gateways

F. SAM ?Block Intruder feature of SmartView Tracker
G. Intrusion Detection System (IDS)policy install
H. SAM ?Suspicious Activity Rules feature of SmartView Monitor

Answer: B

QUESTION NO: 191

You are concerned that your company's servers might be vulnerable to an attack where a client fools a server into sending large amounts of data, using small packets. Which SmartDefense option should you use to protect the servers?

A. Network Security > Denial of Service > Non-TCP Flooding
B. Network Security > Denial of Service > LAND
C. Network Security > IP and ICMP > Block Null Payload ICMP
D. Network Security > TCP > Small PMTU

Answer: D

QUESTION NO: 192

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

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

Select the BEST response for the synchronization sequence. Choose One:

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

Answer: C

QUESTION NO: 193

Which of the following is NOT true for Management High Availability (HA)?

A. The HA SmartCenter Servers must all be the same OS and OS Service Pack
B. The HA SmartCenter Servers must all be the same Check Point Version
C. If the activeSmartCenter Server is down, a standby SmartCenter Servers needs to become active in order to be able to edit and install the Security Policy
D. The HA SmartCenter Servers are synchronized so matching data is maintained and ready to be used.

Answer: A

QUESTION NO: 194

A marketing firm's networking team is trying to troubleshoot user complaints regarding access to audio-streaming material from the Internet. The networking team asks you to check the object and rule configuration settings for the perimeter Security Gateway. Which SmartConsole application should you use to check these objects and rules?

A. SmartViewTracker
B. SmartView Status
C. SmartView Monitor
D. SmartDashboard

Answer: B

QUESTION NO: 195

The Check Point Security Gateway's virtual machine (kernel) exists between which two layers of the OSI model?

A. Physical and Data Link layers
B. Application and Presentation layers
C. Network and Data Link layers
D. Session and Network layers

Answer: B

QUESTION NO: 196

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

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

Answer: C

QUESTION NO: 197

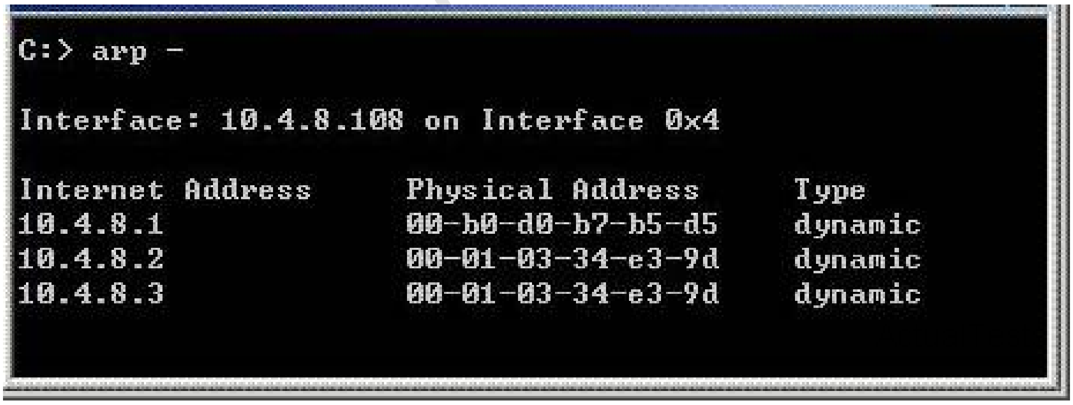
When synchronizing clusters, which of the following statements is NOT true?

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

Answer: A

QUESTION NO: 198

An internal host 10.4.8.108 successfully pings its Legacy Mode Cluster and receives replies. The following is the ARP table from the internal Windows host 10.4.8.108. Based on this information, what is the active cluster member's IP address?According to the output, which member is the standby machine?



```
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
```

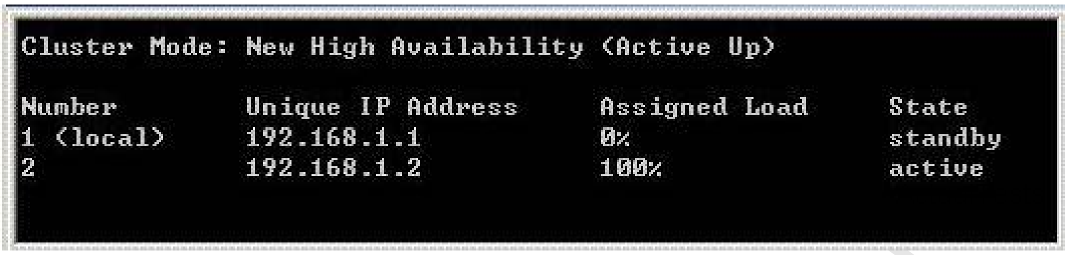
A. 10.4.8.2
B. 10.4.8.3
C. The active cluster member's IP address cannot be determined by thisarp cache

D. 10.4.8.1

Answer: C

QUESTION NO: 199

The following is cphaprob state command output from one New Mode High Availability ClusterXL cluster member:Which member will be active after member 192.168.1.2 fails over and is rebooted?



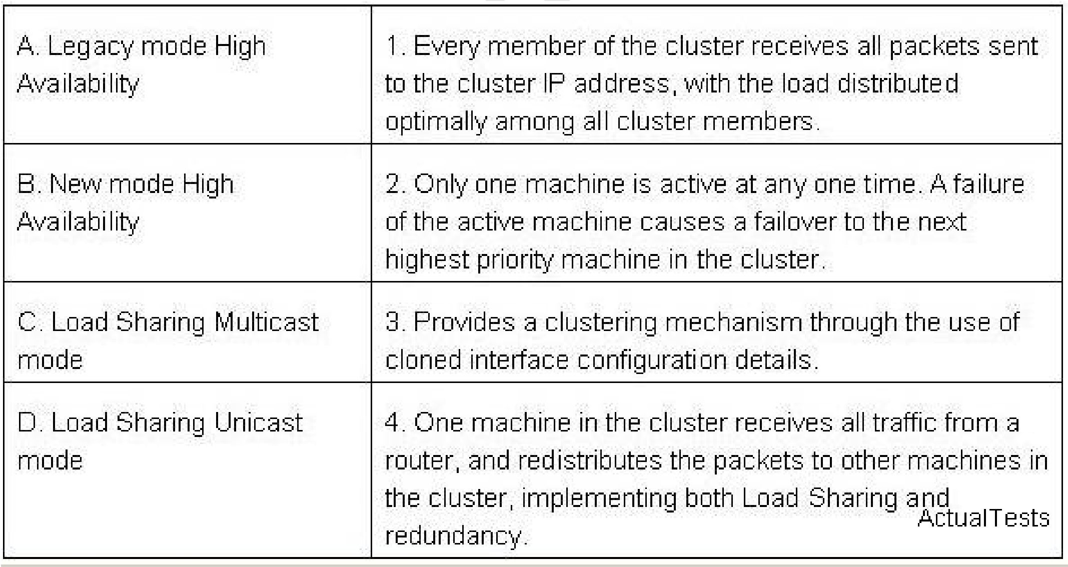
```
Cluster Mode: New High Availability (Active Up)

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

A. Both members' state will be collision.
B. 192.168.1.1
C. 192.168.1.2
D. Both members' state will be active.

Answer: B

QUESTION NO: 200

Match the ClusterXL Modes with their configurations



A. Legacy mode High Availability	1. Every member of the cluster receives all packets sent to the cluster IP address, with the load distributed optimally among all cluster members.
B. New mode High Availability	2. Only one machine is active at any one time. A failure of the active machine causes a failover to the next highest priority machine in the cluster.
C. Load Sharing Multicast mode	3. Provides a clustering mechanism through the use of cloned interface configuration details.
D. Load Sharing Unicast mode	4. One machine in the cluster receives all traffic from a router, and redistributes the packets to other machines in the cluster, implementing both Load Sharing and redundancy.

A. A2.B3.C4.D 1
B. A2.B3.C 1.D4

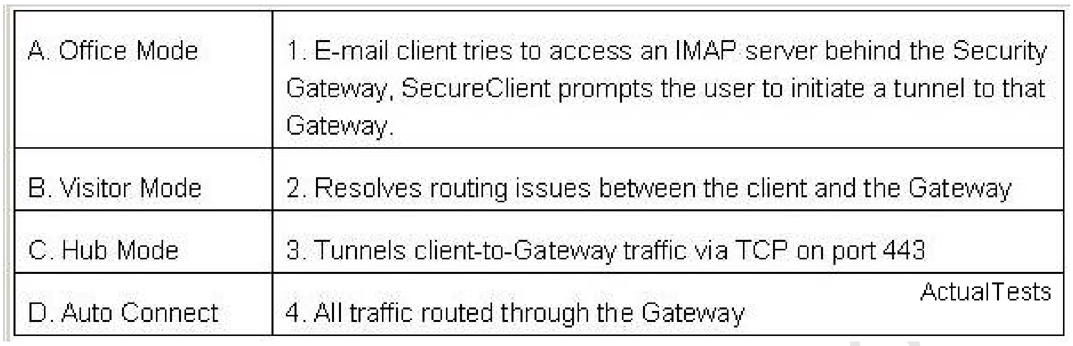
C. A3,B2,C4,D 1

D. A3.B2.C 1.D4

Answer: D

QUESTION NO: 201

Match the remote-access VPN Connection mode features with their descriptions:



A. Office Mode	1. E-mail client tries to access an IMAP server behind the Security Gateway, SecureClient prompts the user to initiate a tunnel to that Gateway.
B. Visitor Mode	2. Resolves routing issues between the client and the Gateway
C. Hub Mode	3. Tunnels client-to-Gateway traffic via TCP on port 443
D. Auto Connect	4. All traffic routed through the Gateway

ActualTests

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

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

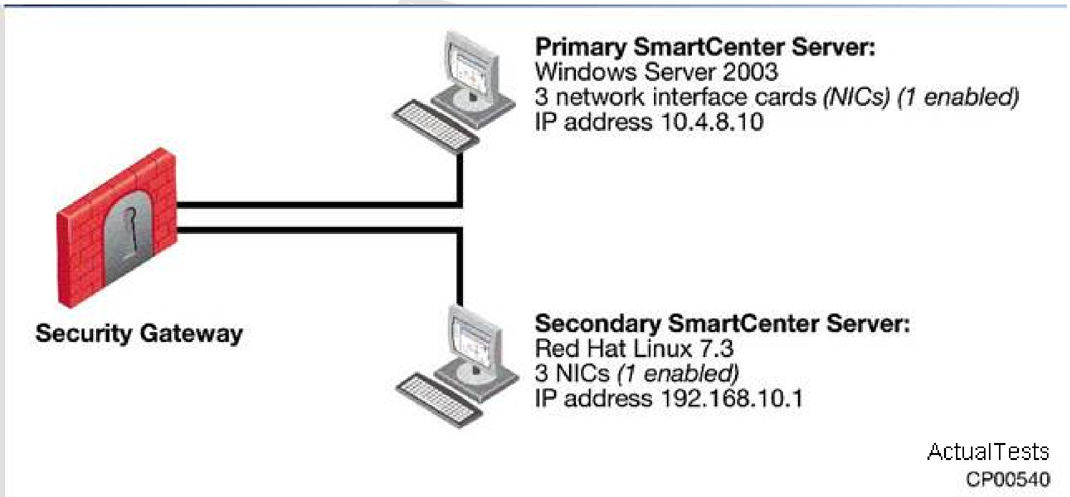
C. A 2,B 4,C 3,D 1

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

Answer: B

QUESTION NO: 202

The following configuration is for VPN-1 NGX R65:Is this configuration correct for Management High Availability?



A. No, theSmartCenter Servers must be installed on the same operating system.

B. No, the SmartCenter Servers do not have the same number of NICs.

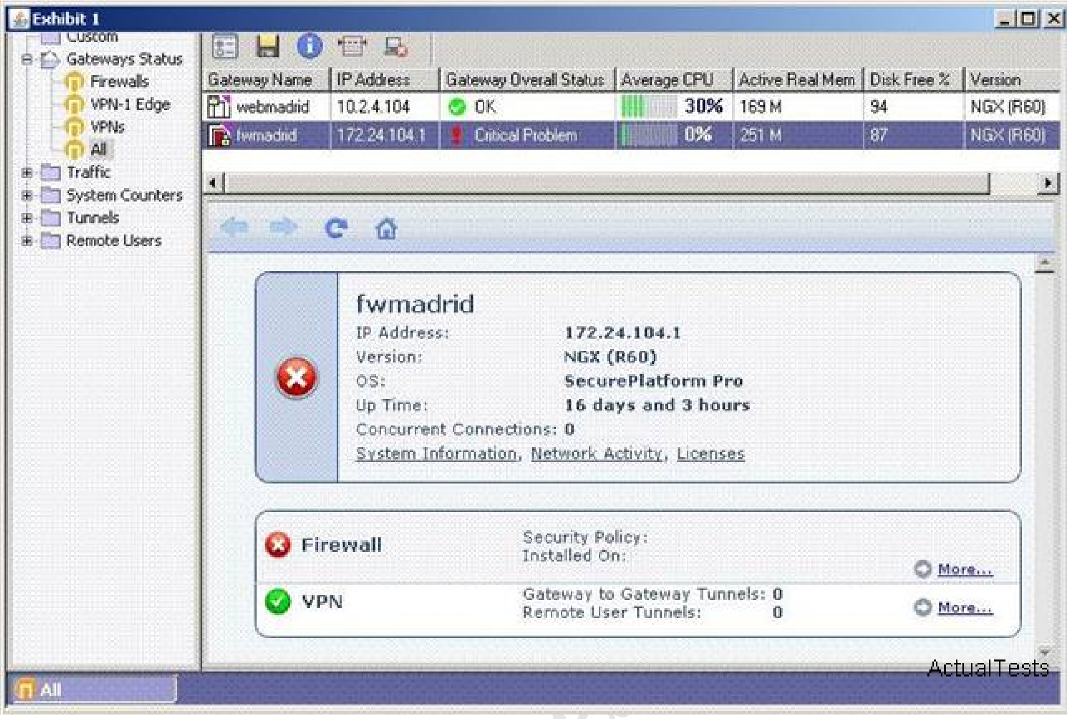
C. No, an NGXR65SmartCenter Server cannot run on Red Hat Linux 7.3.

D. NO, theSmartCenter Servers must reside on the same network.

Answer: A

QUESTION NO: 203

Upon checking SmartView Monitor, you find the following Critical Problem notification.What is the reason?



Gateway Name	IP Address	Gateway Overall Status	Average CPU	Active Real Mem	Disk Free %	Version
webmadrid	10.2.4.104	OK	30%	169 M	94	NGX (R60)
fwmadrid	172.24.104.1	Critical Problem	0%	251 M	87	NGX (R60)

fwmadrid

IP Address: 172.24.104.1

Version: NGX (R60)

OS: SecurePlatform Pro

Up Time: 16 days and 3 hours

Concurrent Connections: 0

System Information, Network Activity, Licenses

Firewall — Security Policy: Installed On: More...

VPN — Gateway to Gateway Tunnels: 0 Remote User Tunnels: 0 More...

A. Version mismatch between theSmartCenter Server and Security Gateway

B. NO Secure Internal Communications established between the SmartCenter Server and Security Gateway

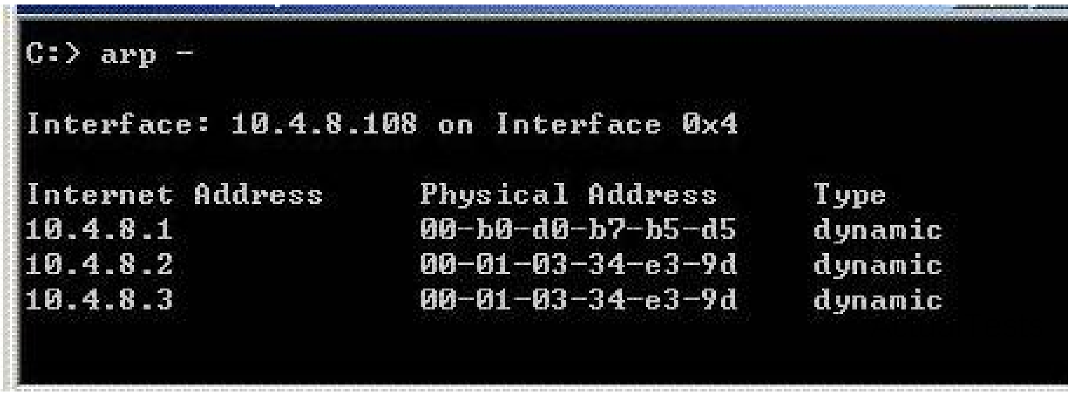
C. Time not synchronized between theSmartCenter Server and Security Gateway

D. No Security Policy installed on the Security Gateway

Answer: D

QUESTION NO: 204

In New Mode HA, the internal cluster IP VIP 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:According to the output, which member is the standby machine?



```
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. 10.4.8.1

B. The standby machine cannot be determined by this test.

C. 10.4.8.2

D. 10.4.8.3

Answer: A