

100% Money Back Guarantee

Vendor: CheckPoint

Exam Code: 156-315.13

Exam Name: Check Point Certified Security Expert

Version: Demo

Topic 1, Volume A

QUESTION NO: 1

Control connections between the Security Management Server and the Gateway are not encrypted by the VPN Community. How are these connections secured?

- A. They are encrypted and authenticated using SIC.
- B. They are not encrypted, but are authenticated by the Gateway
- C. They are secured by PPTP
- D. They are not secured.

Answer: D

Explanation:

QUESTION NO: 2

If Bob wanted to create a Management High Availability configuration, what is the minimum number of Security Management servers required in order to achieve his goal?

- A. Three
- B. Two
- C. Four
- D. One

Answer: D

Explanation:

QUESTION NO: 3

David wants to manage hundreds of gateways using a central management tool.

What tool would David use to accomplish his goal?

- A. SmartProvisioning
- B. SmartBlade
- C. SmartDashboard
- D. SmartLSM

Answer: B

Explanation:

QUESTION NO: 4

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

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

- A. New mode
- B. Multicast mode
- C. Legacy mode
- D. Unicast mode

Answer: D

Explanation:

QUESTION NO: 5

Which of the following is NOT a feature of ClusterXL?

- A. Enhanced throughput in all ClusterXL modes (2 gateway cluster compared with 1 gateway)
- B. Transparent failover in case of device failures
- C. Zero downtime for mission-critical environments with State Synchronization
- D. Transparent upgrades

Answer: C

Explanation:

QUESTION NO: 6

In which case is a Sticky Decision Function relevant?

- A. Load Sharing - Unicast
- B. Load Balancing - Forward

- C. High Availability
- D. Load Sharing - Multicast

Answer: C

Explanation:

QUESTION NO: 7

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

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

Answer: C

Explanation:

QUESTION NO: 8

You have pushed a policy to your firewall and you are not able to access the firewall. What command will allow you to remove the current policy from the machine?

- A. fw purge policy
- B. fw fetch policy
- C. fw purge active
- D. fw unload local

Answer: D

Explanation:

QUESTION NO: 9

How do you verify the Check Point kernel running on a firewall?

- A. fw ctl get kernel

- B. fw ctl pstat
- C. fw kernel
- D. fw ver -k

Answer: D

Explanation:

QUESTION NO: 10

The process _____ compiles \$FWDIR/conf/*.W files into machine language.

- A. fw gen
- B. cpd
- C. fwd
- D. fwm

Answer: A

Explanation:

QUESTION NO: 11

Which of the following is NOT part of the policy installation process?

- A. Code compilation
- B. Code generation
- C. Initiation
- D. Validation

Answer: D

Explanation:

QUESTION NO: 12

When, during policy installation, does the atomic load task run?

- A. It is the first task during policy installation.
- B. It is the last task during policy installation.
- C. Before CPD runs on the Gateway.

D. Immediately after fwm load runs on the SmartCenter.

Answer: B

Explanation:

QUESTION NO: 13

What process is responsible for transferring the policy file from SmartCenter to the Gateway?

- A. FWD
- B. FWM
- C. CPRID
- D. CPD

Answer: D

Explanation:

QUESTION NO: 14

What firewall kernel table stores information about port allocations for Hide NAT connections?

- A. NAT_dst_any_list
- B. host_ip_addrs
- C. NAT_src_any_list
- D. fwx_alloc

Answer: D

Explanation:

QUESTION NO: 15

Where do you define NAT properties so that NAT is performed either client side or server side?

- A. In SmartDashboard under Gateway setting
- B. In SmartDashboard under Global Properties > NAT definition
- C. In SmartDashboard in the NAT Rules
- D. In file \$DFWDIR/lib/table.def

Answer: B

Explanation:

QUESTION NO: 16

The process _____ is responsible for all other security server processes run on the Gateway.

- A. FWD
- B. CPLMD
- C. FWM
- D. CPD

Answer: A

Explanation:

QUESTION NO: 17

The process _____ is responsible for GUIClient communication with the SmartCenter.

- A. FWD
- B. FWM
- C. CPD
- D. CPLMD

Answer: B

Explanation:

QUESTION NO: 18

The process _____ is responsible for Policy compilation.

- A. FWM
- B. Fwcmp
- C. CPLMD
- D. CPD

Answer: A

Explanation:

QUESTION NO: 19

The process _____ is responsible for Management High Availability synchronization.

- A. CPLMD
- B. FWM
- C. Fwsync
- D. CPD

Answer: B

Explanation:

QUESTION NO: 20

_____ is the called process that starts when opening SmartView Tracker application.

- A. logtrackerd
- B. fwlogd
- C. CPLMD
- D. FWM

Answer: C

Explanation:

QUESTION NO: 21

Anytime a client initiates a connection to a server, the firewall kernel signals the FWD process using a trap. FWD spawns the _____ child service, which runs the security server.

- A. FWD
- B. FWSD
- C. In.httpd
- D. FWSSD

Answer: D

Explanation:

QUESTION NO: 22

Security server configuration settings are stored in _____ .

- A. \$FWDIR/conf/AMT.conf
- B. \$FWDIR/conf/fwrl.conf
- C. \$FWDIR/conf/fwauthd.conf
- D. \$FWDIR/conf/fwopsec.conf

Answer: C

Explanation:

QUESTION NO: 23

User definitions are stored in _____ .

- A. \$FWDIR/conf/fwmuser
- B. \$FWDIR/conf/users.NDB
- C. \$FWDIR/conf/fwauth.NDB
- D. \$FWDIR/conf/fwusers.conf

Answer: C

Explanation:

QUESTION NO: 24

Jon is explaining how the inspection module works to a colleague. If a new connection passes through the inspection module and the packet matches the rule, what is the next step in the process?

- A. Verify if the packet should be moved through the TCP/IP stack.
- B. Verify if any logging or alerts are defined.
- C. Verify if the packet should be rejected.
- D. Verify if another rule exists.

Answer: B

Explanation:

QUESTION NO: 25

Which of the following statements accurately describes the `upgrade_export` command?

- A.** Used primarily when upgrading the Security Management Server, `upgrade_export` stores all object databases and the conf directories for importing to a newer version of the Security Gateway.
- B.** Used when upgrading the Security Gateway, `upgrade_export` includes modified files, such as in the directories `/lib` and `/conf`.
- C.** `upgrade_export` is used when upgrading the Security Gateway, and allows certain files to be included or excluded before exporting.
- D.** `upgrade_export` stores network-configuration data, objects, global properties, and the database revisions prior to upgrading the Security Management Server.

Answer: A

Explanation:

QUESTION NO: 26

What are you required to do before running `upgrade_export`?

- A.** Run a `cpstop` on the Security Gateway.
- B.** Run `cpconfig` and set yourself up as a GUI client.
- C.** Run a `cpstop` on the Security Management Server.
- D.** Close all GUI clients.

Answer: D

Explanation:

QUESTION NO: 27

A snapshot delivers a complete backup of SecurePlatform. The resulting file can be stored on servers or as a local file in `/var/CPsnapshot/snapshots`. How do you restore a local snapshot named `MySnapshot.tgz`?

- A.** As Expert user, type command `snapshot - R` to restore from a local file. Then, provide the correct file name.

- B. As Expert user, type command `revert --file MySnapshot.tgz`.
- C. As Expert user, type command `snapshot -r MySnapshot.tgz`.
- D. Reboot the system and call the start menu. Select option Snapshot Management, provide the Expert password and select [L] for a restore from a local file. Then, provide the correct file name.

Answer: B

Explanation:

QUESTION NO: 28

What is the primary benefit of using `upgrade_export` over either `backup` or `snapshot`?

- A. The commands `backup` and `snapshot` can take a long time to run whereas `upgrade_export` will take a much shorter amount of time.
- B. `upgrade_export` will back up routing tables, hosts files, and manual ARP configurations, where `backup` and `snapshot` will not.
- C. `upgrade_export` has an option to backup the system and SmartView Tracker logs while `backup` and `snapshot` will not.
- D. `upgrade_export` is operating system independent and can be used when `backup` or `snapshot` is not available.

Answer: D

Explanation:

QUESTION NO: 29

Your R7x-series Enterprise Security Management Server is running abnormally on Windows Server 2003 R2. You decide to try reinstalling the Security Management Server, but you want to try keeping the critical Security Management Server configuration settings intact (i.e., all Security Policies, databases, SIC, licensing etc.) What is the BEST method to reinstall the Server and keep its critical configuration?

- A) Run `cpstop` on one member, and configure the new interface via `sysconfig`.
2. Run `cpstart` on the cluster member. Repeat the same steps on another member.
 3. Update the new topology in the cluster object from SmartDashboard.
 4. Install the Security Policy.

B)

1. Use the `ifconfig` command to configure and enable the new interface on both members.
2. Run `cprestart` on both members.
3. Update the topology in the cluster object for the cluster and both members.
4. Install the Security Policy.

C)

1. Use `sysconfig` to configure the new interfaces on both members.
2. Update the topology in the cluster object.
3. Install the Security Policy.

D)

1. Disable "Cluster membership" from one gateway via `cpconfig`.
2. Configure the new interface via `sysconfig` from the "non-member" Gateway.
3. Re-enable "Cluster membership" on the Gateway.
4. Perform the same steps on the other Gateway.
5. Update the topology in the cluster object.
6. Install the Security Policy.

- A. Exhibit A
- B. Exhibit B
- C. Exhibit C
- D. Exhibit D

Answer: B

Explanation:

QUESTION NO: 30

Your primary Security Management Server runs on GAIa. What is the easiest way to back up your Security Gateway R76 configuration, including routing and network configuration files?

- A. Using the native GAIa back up utility from command line or in the Web-based user interface.
- B. Using the command `upgrade_export`.
- C. Run the command `pre_upgrade_verifier` and save the file *.tgz to the directory `c:/temp`.
- D. Copying the directories `$FWDIR/conf` and `$FWDIR/lib` to another location.

Answer: A

Explanation:

QUESTION NO: 31

You need to back up the routing, interface, and DNS configuration information from your R76 SecurePlatform Security Gateway. Which backup-and-restore solution do you use?

- A. SecurePlatform back up utilities

- B. Manual copies of the directory \$FWDIR/conf
- C. Database Revision Control
- D. Commands upgrade_export and upgrade_import

Answer: A

Explanation:

QUESTION NO: 32

Which of the following methods will provide the most complete backup of an R76 configuration?

- A. Database Revision Control
- B. Policy Package Management
- C. Copying the directories \$FWDIR/conf and \$CPDIR/conf to another server
- D. upgrade_export command

Answer: D

Explanation:

QUESTION NO: 33

Which of the following commands can provide the most complete restore of an R76 configuration?

- A. upgrade_import
- B. fwm dbimport -p <export file>
- C. cpconfig
- D. cpinfo -recover

Answer: A

Explanation:

QUESTION NO: 34

When restoring R76 using the command upgrade_import, which of the following items are NOT restored?

- A. Global properties
- B. Route tables

- C. Licenses
- D. SIC Certificates

Answer: B

Explanation:

QUESTION NO: 35

Your organization's disaster recovery plan needs an update to the backup and restore section to reap the benefits of the new distributed R76 installation. Your plan must meet the following required and desired objectives:

Required Objective: The Security Policy repository must be backed up no less frequently than every 24 hours.

Desired Objective: The R76 components that enforce the Security Policies should be backed up at least once a week.

Desired Objective: Back up R76 logs at least once a week.

Your disaster recovery plan is as follows:

- Use the utility `cron` to run the command `upgrade_export` each night on the Security Management Servers.
- Configure the organization's routine back up software to back up the files created by the command `upgrade_export`.
- Configure the SecurePlatform back up utility to back up the Security Gateways every Saturday night.
- Use the utility `cron` to run the command `upgrade_export` each Saturday night on the log servers.
- Configure an automatic, nightly `logswitch`.
- Configure the organization's routine back up software to back up the switched logs every night.

Upon evaluation, your plan:

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

Answer: B

Explanation:

QUESTION NO: 36

You are running a R76 Security Gateway on SecurePlatform. In case of a hardware failure, you have a server with the exact same hardware and firewall version installed. What backup method could be used to quickly put the secondary firewall into production?

- A. upgrade_export
- B. manual backup
- C. snapshot
- D. backup

Answer: C

Explanation:

QUESTION NO: 37

Before upgrading SecurePlatform, you should create a backup. To save time, many administrators use the command backup. This creates a backup of the Check Point configuration as well as the system configuration.

An administrator has installed the latest HFA on the system for fixing traffic problems after creating a backup file. There is a mistake in the very complex static routing configuration. The Check Point configuration has not been changed. Can the administrator use a restore to fix the errors in static routing?

- A. The restore is not possible because the backup file does not have the same build number (version).
- B. The restore is done by selecting Snapshot Management from the SecurePlatform boot menu.
- C. The restore can be done easily by the command restore and selecting the appropriate backup file.
- D. A back up cannot be restored, because the binary files are missing.

Answer: C

Explanation:

QUESTION NO: 38

You intend to upgrade a Check Point Gateway from R65 to R76. To avoid problems, you decide to back up the Gateway. Which approach allows the Gateway configuration to be completely backed up into a manageable size in the least amount of time?

- A. snapshot
- B. database revision
- C. backup
- D. upgrade_export

Answer: D

Explanation:

QUESTION NO: 39

Your R76 enterprise Security Management Server is running abnormally on Windows 2008 Server. You decide to try reinstalling the Security Management Server, but you want to try keeping the critical Security Management Server configuration settings intact (i.e., all Security Policies, databases, SIC, licensing etc.) What is the BEST method to reinstall the Server and keep its critical configuration?

- A.**
 1. Create a database revision control backup using the SmartDashboard
 2. Create a compressed archive of the *FWDIR*\ conf and »FWDiR8\lib directories and copy them to another networked machine.
 3. Uninstall all R70 packages via Add/Remove Programs and reboot.
 4. Install again as a primary Security Management Server using the R70 CD.
 5. Reboot and restore the two archived directories over the top of the new installation, choosing to overwrite existing files.
- B.**
 1. Download the latest upgrade_export utility and run it from a c; \temp directory to export the configuration into a . tgz file
 2. Skip any upgarde__verification warnings since you are not upgrading
 3. Transfer the . tgz file to another networked machine
 4. Download and run the cpclean utility and reboot
 5. Use the R70 CD-ROM to select the uuarade import ootion to import the confiauration
- C.**
 1. Download the latest upgrade__expoct utility and run it from a \temp directory to export the configuration into a . tgz file
 2. Perform any requested upgcade__veri£ic«tion suggested steps
 3. Uninstall all R70 packages via Add/Remove Programs and reboot
 4. Use SmartUpdate to reinstall the Security Management Server and reboot
 5. Transfer the tgz file back to the local \temp
 6. Run upgrade__import to import the configuration
- D.**
 1. Insert the F70 CD-ROM, and select the option to export the configuration using the latest

upgrade utilities

2. Perform any requested upgrade_verification suggested steps and re-export the configuration if needed
3. Save the export " tgz file to a local c: \temp directory
4. Uninstall all R70 packages via Add/Remove Programs and reboot
5. Install again using the R70 CD-ROM as a primary Security Management Server and reboot
6. Run upgrade_import to import the configuration

Answer: C

Explanation:

QUESTION NO: 40

True or false? After creating a snapshot of a Windows 2003 SP2 Security Management Server, you can restore it on a SecurePlatform R76 Security Management Server, except you must load interface information manually.

- A. True, but only when the snapshot file is restored to a SecurePlatform system running R76.20.
- B. False, you cannot run the Check Point snapshot utility on a Windows gateway.
- C. True, but only when the snapshot file is restored to a SecurePlatform system running R76.10.
- D. False, all configuration information conveys to the new system, including the interface configuration settings.

Answer: B

Explanation:

QUESTION NO: 41

Check Point recommends that you back up systems running Check Point products. Run your back ups during maintenance windows to limit disruptions to services, improve CPU usage, and simplify time allotment. Which back up method does Check Point recommend before major changes, such as upgrades?

- A. snapshot
- B. upgrade_export
- C. backup
- D. migrate export

Answer: A

Explanation:

QUESTION NO: 42

Check Point recommends that you back up systems running Check Point products. Run your back ups during maintenance windows to limit disruptions to services, improve CPU usage, and simplify time allotment. Which back up method does Check Point recommend every couple of months, depending on how frequently you make changes to the network or policy?

- A. backup
- B. migrate export
- C. upgrade_export
- D. snapshot

Answer: A

Explanation:

QUESTION NO: 43

Check Point recommends that you back up systems running Check Point products. Run your back ups during maintenance windows to limit disruptions to services, improve CPU usage, and simplify time allotment. Which back up method does Check Point recommend anytime outside a maintenance window?

- A. backup
- B. migrate export
- C. backup_export
- D. snapshot

Answer: B

Explanation:

QUESTION NO: 44

Snapshot is available on which Security Management Server and Security Gateway platforms?

- A. Solaris
- B. Windows 2003 Server
- C. Windows XP Server
- D. SecurePlatform

Answer: D

Explanation:

QUESTION NO: 45

The file snapshot generates is very large, and can only be restored to:

- A. The device that created it, after it has been upgraded
- B. Individual members of a cluster configuration
- C. Windows Server class systems
- D. A device having exactly the same Operating System as the device that created the file

Answer: D

Explanation:

QUESTION NO: 46

Restoring a snapshot-created file on one machine that was created on another requires which of the following to be the same on both machines?

- A. Windows version, objects database, patch level, and interface configuration
- B. Windows version, interface configuration, and patch level
- C. State, SecurePlatform version, and patch level
- D. State, SecurePlatform version, and objects database

Answer: C

Explanation:

QUESTION NO: 47

When restoring a Security Management Server from a backup file, the restore package can be retrieved from which source?

- A. HTTP server, FTP server, or TFTP server
- B. Disk, SCP server, or TFTP server
- C. Local folder, TFTP server, or FTP server
- D. Local folder, TFTP server, or Disk

Answer: C

Explanation:

QUESTION NO: 48

When upgrading Check Point products in a distributed environment, in which order should you upgrade these components?

1 GUI Client

2 Security Management Server

3 Security Gateway

A. 3, 2, 1

B. 1, 2, 3

C. 3, 1, 2

D. 2, 3, 1

Answer: D

Explanation:

QUESTION NO: 49

When using migrate to upgrade a Secure Management Server, which of the following is included in the migration?

A. SmartEvent database

B. SmartReporter database

C. classes.C file

D. System interface configuration

Answer: C

Explanation:

QUESTION NO: 50

Typically, when you upgrade the Security Management Server, you install and configure a fresh R76 installation on a new computer and then migrate the database from the original machine.

When doing this, what is required of the two machines? They must both have the same:

- A. Products installed.
- B. Interfaces configured.
- C. State.
- D. Patch level.

Answer: A

Explanation:

QUESTION NO: 51

Typically, when you upgrade the Security Management Server, you install and configure a fresh R76 installation on a new computer and then migrate the database from the original machine. Which of the following statements are TRUE?

- A. Both machines must have the same number of interfaces installed and configured before migration can be attempted.
- B. The new machine may not have more Check Point products installed than the original Security Management Server.
- C. All product databases are included in the migration.
- D. The Security Management Server on the new machine must be the same or greater than the version on the original machine.

Answer: D

Explanation:

QUESTION NO: 52

Typically, when you upgrade the Security Management Server, you install and configure a fresh R76 installation on a new computer and then migrate the database from the original machine. What is the correct order of the steps below to successfully complete this procedure?

- 1) Export databases from source.
- 2) Connect target to network.
- 3) Prepare the source machine for export.
- 4) Import databases to target.

5) Install new version on target.

6) Test target deployment.

A. 6, 5, 3, 1, 4, 2

B. 3, 1, 5, 4, 2, 6

C. 5, 2, 6, 3, 1, 4

D. 3, 5, 1, 4, 6, 2

Answer: D

Explanation:

QUESTION NO: 53

During a Security Management Server migrate export, the system:

A. Creates a backup file that includes the SmartEvent database.

B. Creates a backup file that includes the SmartReporter database.

C. Creates a backup archive for all the Check Point configuration settings.

D. Saves all system settings and Check Point product configuration settings to a file.

Answer: C

Explanation:

QUESTION NO: 54

If no flags are defined during a back up on the Security Management Server, where does the system store the *.tgz file?

A. /var/opt/backups

B. /var/backups

C. /var/CPbackup/backups

D. /var/tmp/backups

Answer: C

Explanation:

QUESTION NO: 55

Which is NOT a valid option when upgrading Cluster Deployments?

- A. Full Connectivity Upgrade
- B. Fast path Upgrade
- C. Minimal Effort Upgrade
- D. Zero Downtime

Answer: B

Explanation:

QUESTION NO: 56

In a zero downtime firewall cluster environment what command do you run to avoid switching problems around the cluster.

- A. cphaconf set mc_relod
- B. cphaconf set clear_subs
- C. cphaconf set_ccp broadcast
- D. cphaconf set_ccp multicast

Answer: C

Explanation:

QUESTION NO: 57

In a "zero downtime" scenario, which command do you run manually after all cluster members are upgraded?

- A. cphaconf set_ccp broadcast
- B. cphaconf set clear_subs
- C. cphaconf set mc_relod
- D. cphaconf set_ccp multicast

Answer: D

Explanation:

QUESTION NO: 58

Which command provides cluster upgrade status?

- A. cphaprob status
- B. cphaprob ldstat
- C. cphaprob fcustat
- D. cphaprob tablestat

Answer: C

Explanation:

QUESTION NO: 59

John is upgrading a cluster from NGX R65 to R76. John knows that you can verify the upgrade process using the pre-upgrade verifier tool. When John is running Pre-Upgrade Verification, he sees the warning message:

Title: Incompatible pattern.

What is happening?

- A. R76 uses a new pattern matching engine. Incompatible patterns should be deleted before upgrade process to complete it successfully.
- B. Pre-Upgrade Verification process detected a problem with actual configuration and upgrade will be aborted.
- C. Pre-Upgrade Verification tool only shows that message but it is only informational.
- D. The actual configuration contains user defined patterns in IPS that are not supported in R76. If the patterns are not fixed after upgrade, they will not be used with R76 Security Gateways.

Answer: D

Explanation:

QUESTION NO: 60

Which command would you use to save the interface information before upgrading a GAIa Gateway?

- A. netstat -rn > [filename].txt
- B. ipconfig -a > [filename].txt
- C. ifconfig > [filename].txt

D. cp /etc/sysconfig/network.C [location]

Answer: C

Explanation:

QUESTION NO: 61

Which command would you use to save the routing information before upgrading a SecurePlatform Gateway?

A. cp /etc/sysconfig/network.C [location]

B. netstat -rn > [filename].txt

C. ifconfig > [filename].txt

D. ipconfig -a > [filename].txt

Answer: A

Explanation:

QUESTION NO: 62

Which command would you use to save the routing information before upgrading a Windows Gateway?

A. ipconfig -a > [filename].txt

B. ifconfig > [filename].txt

C. cp /etc/sysconfig/network.C [location]

D. netstat -rn > [filename].txt

Answer: D

Explanation:

QUESTION NO: 63

Which command would you use to save the interface information before upgrading a Windows Gateway?

A. cp /etc/sysconfig/network.C [location]

B. ipconfig -a > [filename].txt

- C. ifconfig > [filename].txt
- D. netstat -rn > [filename].txt

Answer: B

Explanation:

QUESTION NO: 64

When upgrading a cluster in Full Connectivity Mode, the first thing you must do is see if all cluster members have the same products installed. Which command should you run?

- A. fw fcu
- B. cphaprob fcustat
- C. cpconfig
- D. fw ctl conn -a

Answer: D

Explanation:

QUESTION NO: 65

A Minimal Effort Upgrade of a cluster:

- A. Is only supported in major releases (R70 to R71, R71 to R76).
- B. Is not a valid upgrade method in R76.
- C. Treats each individual cluster member as an individual gateway.
- D. Upgrades all cluster members except one at the same time.

Answer: C

Explanation:

QUESTION NO: 66

A Zero Downtime Upgrade of a cluster:

- A. Upgrades all cluster members except one at the same time.
- B. Is only supported in major releases (R70 to R71, R71 to R76).
- C. Treats each individual cluster member as an individual gateway.

D. Is not a valid upgrade method in R76.

Answer: A

Explanation:

QUESTION NO: 67

A Full Connectivity Upgrade of a cluster:

- A. Treats each individual cluster member as an individual gateway.
- B. Upgrades all cluster members except one at the same time.
- C. Is only supported in minor version upgrades (R70 to R71, R71 to R76).
- D. Is not a valid upgrade method in R76.

Answer: C

Explanation:

QUESTION NO: 68

A Fast Path Upgrade of a cluster:

- A. Upgrades all cluster members except one at the same time.
- B. Treats each individual cluster member as an individual gateway.
- C. Is not a valid upgrade method in R76.
- D. Is only supported in major releases (R70 to R71, R75 to R76).

Answer: C

Explanation:

QUESTION NO: 69

How does Check Point recommend that you secure the sync interface between gateways?

- A. Configure the sync network to operate within the DMZ.
- B. Secure each sync interface in a cluster with Endpoint.
- C. Use a dedicated sync network.
- D. Encrypt all sync traffic between cluster members.

Answer: C

Explanation:

QUESTION NO: 70

How would you set the debug buffer size to 1024?

- A. Run fw ctl set buf 1024
- B. Run fw ctl kdebug 1024
- C. Run fw ctl debug -buf 1024
- D. Run fw ctl set int print_cons 1024

Answer: C

Explanation:

QUESTION NO: 71

Steve is troubleshooting a connection problem with an internal application. If he knows the source IP address is 192.168.4.125, how could he filter this traffic?

- A. Run fw monitor -e "accept dsrc=192.168.4.125;"
- B. Run fw monitor -e "accept dst=192.168.4.125;"
- C. Run fw monitor -e "accept ip=192.168.4.125;"
- D. Run fw monitor -e "accept src=192.168.4.125;"

Answer: D

Explanation:

QUESTION NO: 72

Check Point support has asked Tony for a firewall capture of accepted packets. What would be the correct syntax to create a capture file to a filename called monitor.out?

- A. Run fw monitor -e "accept;" -f monitor.out
- B. Run fw monitor -e "accept;" -c monitor.out
- C. Run fw monitor -e "accept;" -o monitor.out
- D. Run fw monitor -e "accept;" -m monitor.out

Answer: C

Explanation:

QUESTION NO: 73

What is NOT a valid LDAP use in Check Point SmartDirectory?

- A. Retrieve gateway CRL's
- B. External users management
- C. Enforce user access to internal resources
- D. Provide user authentication information for the Security Management Server

Answer: C

Explanation:

QUESTION NO: 74

There are several SmartDirectory (LDAP) features that can be applied to further enhance SmartDirectory (LDAP) functionality, which of the following is NOT one of those features?

- A. High Availability, where user information can be duplicated across several servers
- B. Support multiple SmartDirectory (LDAP) servers on which many user databases are distributed
- C. Encrypted or non-encrypted SmartDirectory (LDAP) Connections usage
- D. Support many Domains under the same account unit

Answer: D

Explanation:

QUESTION NO: 75

Choose the BEST sequence for configuring user management in SmartDashboard, using an LDAP server.

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

D. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object.

Answer: C

Explanation:

QUESTION NO: 76

The User Directory Software Blade is used to integrate which of the following with a R76 Security Gateway?

- A. LDAP server
- B. RADIUS server
- C. Account Management Client server
- D. UserAuthority server

Answer: A

Explanation:

QUESTION NO: 77

Your users are defined in a Windows 2008 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R76?

- A. LDAP group
- B. External-user group
- C. A group with a generic user
- D. All Users

Answer: A

Explanation:

QUESTION NO: 78

Which of the following commands do you run on the AD server to identify the DN name before configuring LDAP integration with the Security Gateway?

- A. query ldap -name administrator
- B. dsquery user -name administrator
- C. ldapquery -name administrator
- D. cpquery -name administrator

Answer: B

Explanation:

QUESTION NO: 79

In SmartDirectory, what is each LDAP server called?

- A. Account Server
- B. Account Unit
- C. LDAP Server
- D. LDAP Unit

Answer: B

Explanation:

QUESTION NO: 80

What is the default port number for standard TCP connections with the LDAP server?

- A. 398
- B. 636
- C. 389
- D. 363

Answer: C

Explanation:

QUESTION NO: 81

What is the default port number for Secure Sockets Layer connections with the LDAP Server?

- A. 363
- B. 389

- C. 398
- D. 636

Answer: D

Explanation:

QUESTION NO: 82

When defining an Organizational Unit, which of the following are NOT valid object categories?

- A. Domains
- B. Resources
- C. Users
- D. Services

Answer: A

Explanation:

QUESTION NO: 83

When defining SmartDirectory for High Availability (HA), which of the following should you do?

- A. Replicate the same information on multiple Active Directory servers.
- B. Configure Secure Internal Communications with each server and fetch branches from each.
- C. Configure a SmartDirectory Cluster object.
- D. Configure the SmartDirectory as a single object using the LDAP cluster IP. Actual HA functionality is configured on the servers.

Answer: A

Explanation:

QUESTION NO: 84

The set of rules that governs the types of objects in the directory and their associated attributes is called the:

- A. LDAP Policy
- B. Schema

- C. Access Control List
- D. SmartDatabase

Answer: B

Explanation:

QUESTION NO: 85

When using SmartDashboard to manage existing users in SmartDirectory, when are the changes applied?

- A. Instantaneously
- B. At policy installation
- C. Never, you cannot manage users through SmartDashboard
- D. At database synchronization

Answer: A

Explanation:

QUESTION NO: 86

Where multiple SmartDirectory servers exist in an organization, a query from one of the clients for user information is made to the servers based on a priority. By what category can this priority be defined?

- A. Gateway or Domain
- B. Location or Account Unit
- C. Location or Domain
- D. Gateway or Account Unit

Answer: D

Explanation:

QUESTION NO: 87

Each entry in SmartDirectory has a unique _____ ?

- A. Distinguished Name

- B. Organizational Unit
- C. Port Number Association
- D. Schema

Answer: A

Explanation:

QUESTION NO: 88

With the User Directory Software Blade, you can create R76 user definitions on a(n) _____ Server.

- A. SecureID
- B. LDAP
- C. NT Domain
- D. Radius

Answer: B

Explanation:

QUESTION NO: 89

Which describes the function of the account unit?

- A. An Account Unit is the Check Point account that SmartDirectory uses to access an (LDAP) server
- B. An Account Unit is a system account on the Check Point gateway that SmartDirectory uses to access an (LDAP) server
- C. An Account Unit is the administration account on the LDAP server that SmartDirectory uses to access to (LDAP) server
- D. An Account Unit is the interface which allows interaction between the Security Management server and Security Gateways, and the SmartDirectory (LDAP) server.

Answer: D

Explanation:

QUESTION NO: 90

An organization may be distributed across several SmartDirectory (LDAP) servers. What provision

do you make to enable a Gateway to use all available resources? Each SmartDirectory (LDAP) server must be:

- A. a member in the LDAP group.
- B. a member in a group that is associated with one Account Unit.
- C. represented by a separate Account Unit.
- D. represented by a separate Account Unit that is a member in the LDAP group.

Answer: C

Explanation:

QUESTION NO: 91

Which is NOT a method through which Identity Awareness receives its identities?

- A. GPO
- B. Captive Portal
- C. AD Query
- D. Identity Agent

Answer: A

Explanation:

QUESTION NO: 92

If using AD Query for seamless identity data reception from Microsoft Active Directory (AD), which of the following methods is NOT Check Point recommended?

- A. Leveraging identity in Internet application control
- B. Identity-based auditing and logging
- C. Basic identity enforcement in the internal network
- D. Identity-based enforcement for non-AD users (non-Windows and guest users)

Answer: D

Explanation:

QUESTION NO: 93

When using Captive Portal to send unidentified users to a Web portal for authentication, which of the following is NOT a recommended use for this method?

- A. Identity-based enforcement for non-AD users (non-Windows and guest users)
- B. For deployment of Identity Agents
- C. Basic identity enforcement in the internal network
- D. Leveraging identity in Internet application control

Answer: C

Explanation:

QUESTION NO: 94

Identity Agent is a lightweight endpoint agent that authenticates securely with Single Sign-On (SSO). Which of the following is NOT a recommended use for this method?

- A. When accuracy in detecting identity is crucial
- B. Identity based enforcement for non-AD users (non-Windows and guest users)
- C. Protecting highly sensitive servers
- D. Leveraging identity for Data Center protection

Answer: B

Explanation:

QUESTION NO: 95

Which of the following access options would you NOT use when configuring Captive Portal?

- A. Through the Firewall policy
- B. From the Internet
- C. Through all interfaces
- D. Through internal interfaces

Answer: B

Explanation:

QUESTION NO: 96

Where do you verify that SmartDirectory is enabled?

- A. Global properties > Authentication> Use SmartDirectory(LDAP) for Security Gateways is checked
- B. Gateway properties > Smart Directory (LDAP) > Use SmartDirectory(LDAP) for Security Gateways is checked
- C. Gateway properties > Authentication> Use SmartDirectory(LDAP) for Security Gateways is checked
- D. Global properties > Smart Directory (LDAP) > Use SmartDirectory(LDAP) for Security Gateways is checked

Answer: D

Explanation:

QUESTION NO: 97

Remote clients are using IPSec VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?

- A. vpnd
- B. cpvpnd
- C. fwm
- D. fwd

Answer: A

Explanation:

QUESTION NO: 98

Remote clients are using SSL VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?

- A. vpnd
- B. cpvpnd
- C. fwm
- D. fwd

Answer: B

Explanation:

QUESTION NO: 99

Which of the following is NOT a LDAP server option in SmartDirectory?

- A. Novell_DS
- B. Netscape_DS
- C. OPSEC_DS
- D. Standard_DS

Answer: D

Explanation:

QUESTION NO: 100

An Account Unit is the interface between the _____ and the _____.

- A. Users, Domain
- B. Gateway, Resources
- C. System, Database
- D. Clients, Server

Answer: D

Explanation:

Topic 2, Volume B

QUESTION NO: 101

Which of the following is a valid Active Directory designation for user John Doe in the Sales department of AcmeCorp.com?

- A. Cn=john_doe,ou=Sales,ou=acmecorp,dc=com
- B. Cn=john_doe,ou=Sales,ou=acme,ou=corp,dc=com
- C. Cn=john_doe,dc=Sales,dc=acmecorp,dc=com
- D. Cn=john_doe,ou=Sales,dc=acmecorp,dc=com

Answer: D

Explanation:

QUESTION NO: 102

Which of the following is a valid Active Directory designation for user Jane Doe in the MIS department of AcmeCorp.com?

- A. Cn= jane_doe,ou=MIS,DC=acmecorp,dc=com
- B. Cn= jane_doe,ou=MIS,cn=acmecorp,dc=com
- C. Cn=jane_doe,ou=MIS,dc=acmecorp,dc=com
- D. Cn= jane_doe,ou=MIS,cn=acme,cn=corp,dc=com

Answer: C

Explanation:

QUESTION NO: 103

Which utility or command is useful for debugging by capturing packet information, including verifying LDAP authentication?

- A. fw monitor
- B. ping
- C. um_core enable
- D. fw debug fwm

Answer: A

Explanation:

QUESTION NO: 104

You can NOT use SmartDashboard's SmartDirectory features to connect to the LDAP server. What should you investigate?

1. Verify you have read-only permissions as administrator for the operating system.
2. Verify there are no restrictions blocking SmartDashboard's User Manager from connecting to the LDAP server.
3. Check that the Login Distinguished Name configured has root (Administrator) permission (or at least write permission) in the access control configuration of the LDAP server.

- A. 1 and 3
- B. 2 and 3
- C. 1 and 2
- D. 1, 2, and 3

Answer: B

Explanation:

QUESTION NO: 105

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

- A. Secure Internal Communications (SIC)
- B. Domain name resolution
- C. Overlapping VPN Domains
- D. Connectivity between the R76 Gateway and LDAP server

Answer: D

Explanation:

QUESTION NO: 106

How are cached usernames and passwords cleared from the memory of a R76 Security Gateway?

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

Answer: D

Explanation:

QUESTION NO: 107

When an Endpoint user is able to authenticate but receives a message from the client that it is unable to enforce the desktop policy, what is the most likely scenario?

- A. The user's rights prevent access to the protected network.

- B. A Desktop Policy is not configured.
- C. The gateway could not locate the user in SmartDirectory and is allowing the connection with limitations based on a generic profile.
- D. The user is attempting to connect with the wrong Endpoint client.

Answer: D

Explanation:

QUESTION NO: 108

When using a template to define a SmartDirectory, where should the user's password be defined?
In the:

- A. Template object
- B. VPN Community object
- C. User object
- D. LDAP object

Answer: C

Explanation:

QUESTION NO: 109

When configuring an LDAP Group object, which option should you select if you want the gateway to reference the groups defined on the LDAP server for authentication purposes?

- A. All Account-Unit's Users
- B. Only Group in Branch
- C. Group Agnostic
- D. OU Accept and select appropriate domain

Answer: B

Explanation:

QUESTION NO: 110

When configuring an LDAP Group object, which option should you select if you do NOT want the gateway to reference the groups defined on the LDAP server for authentication purposes?

- A. OU Accept and select appropriate domain
- B. Only Sub Tree
- C. Only Group in Branch
- D. Group Agnostic

Answer: B

Explanation:

QUESTION NO: 111

When configuring an LDAP Group object, which option should you select if you want the gateway to reference the groups defined on the LDAP server for authentication purposes?

- A. Only Group in Branch
- B. Only Sub Tree
- C. OU Auth and select Group Name
- D. All Account-Unit's Users

Answer: A

Explanation:

QUESTION NO: 112

The process that performs the authentication for SmartDashboard is:

- A. fwm
- B. vpnd
- C. cvpnd
- D. cpd

Answer: A

Explanation:

QUESTION NO: 113

The process that performs the authentication for Remote Access is:

- A. cpd

- B. vpnd
- C. fwm
- D. cvpnd

Answer: B

Explanation:

QUESTION NO: 114

The process that performs the authentication for SSL VPN Users is:

- A. cvpnd
- B. cpd
- C. fwm
- D. vpnd

Answer: A

Explanation:

QUESTION NO: 115

The process that performs the authentication for legacy session authentication is:

- A. cvpnd
- B. fwm
- C. vpnd
- D. fwssd

Answer: D

Explanation:

QUESTION NO: 116

While authorization for users managed by SmartDirectory is performed by the gateway, the authentication is mostly performed by the infrastructure in which of the following?

- A. ldapd
- B. cpauth

- C. cpShared
- D. ldapauth

Answer: B

Explanation:

QUESTION NO: 117

When troubleshooting user authentication, you may see the following entries in a debug of the user authentication process. In which order are these messages likely to appear?

- A. make_au, au_auth, au_fetchuser, au_auth_auth, cpLdapCheck, cpLdapGetUser
- B. cpLdapGetUser, au_fetchuser, cpLdapCheck, make_au, au_auth, au_auth_auth
- C. make_au, au_auth, au_fetchuser, cpLdapGetUser, cpLdapCheck, au_auth_auth
- D. au_fetchuser, make_au, au_auth, cpLdapGetUser, au_auth_auth, cpLdapCheck

Answer: C

Explanation:

QUESTION NO: 118

Which of the following is NOT a ClusterXL mode?

- A. Multicast
- B. Legacy
- C. Broadcast
- D. New

Answer: C

Explanation:

QUESTION NO: 119

In an R76 Cluster, some features such as VPN only function properly when:

- A. All cluster members have the same policy
- B. All cluster members have the same Hot Fix Accumulator pack installed
- C. All cluster members' clocks are synchronized

D. All cluster members have the same number of interfaces configured

Answer: C

Explanation:

QUESTION NO: 120

In ClusterXL R76; when configuring a cluster synchronization network on a VLAN interface what is the supported configuration?

- A. It is supported on VLAN tag 4095
- B. It is supported on VLAN tag 4096
- C. It is supported on the lowest VLAN tag of the VLAN interface
- D. It is not supported on a VLAN tag

Answer: C

Explanation:

QUESTION NO: 121

Which process is responsible for delta synchronization in ClusterXL?

- A. fw kernel on the security gateway
- B. fwd process on the security gateway
- C. cpd process on the security gateway
- D. Clustering process on the security gateway

Answer: A

Explanation:

QUESTION NO: 122

Which process is responsible for full synchronization in ClusterXL?

- A. fwd on the Security Gateway
- B. fw kernel on the Security Gateway
- C. Clustering on the Security Gateway
- D. cpd on the Security Gateway

Answer: A

Explanation:

QUESTION NO: 123

Which process is responsible for kernel table information sharing across all cluster members?

- A. fwd daemon using an encrypted TCP connection
- B. CPHA using an encrypted TCP connection
- C. fw kernel using an encrypted TCP connection
- D. cpd using an encrypted TCP connection

Answer: A

Explanation:

QUESTION NO: 124

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

- A. The user data base is installed.
- B. The standby Security Management Server starts for the first time.
- C. The Security Policy is installed.
- D. The Security Policy is saved.

Answer: C

Explanation:

QUESTION NO: 125

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

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

Answer: D

Explanation:

QUESTION NO: 126

_____ is a proprietary Check Point protocol. It is the basis for Check Point ClusterXL inter-module communication.

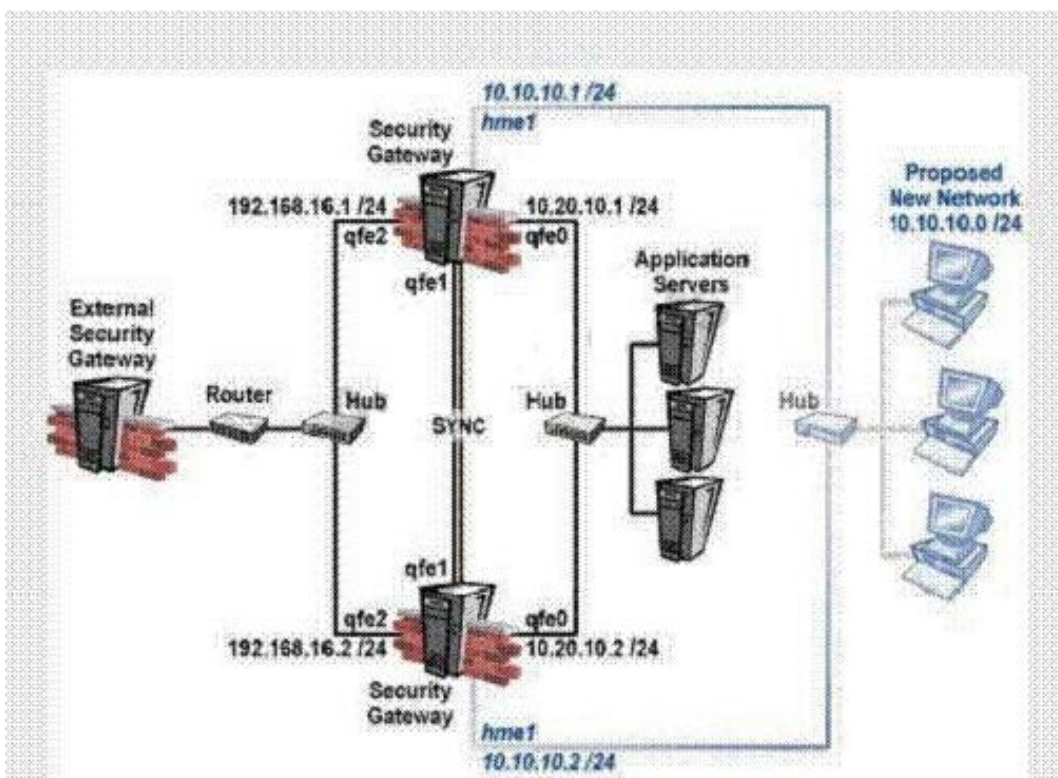
- A. HA OP CODE
- B. RDP
- C. CKPP
- D. CCP

Answer: D

Explanation:

QUESTION NO: 127

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



- A. By running the command `cphaprob state` on both members
- B. By running the command `cpconfig` on both members
- C. By running the command `cphaprob -l list` on both members
- D. By running the command `cphaprob -a if` on both members

Answer: D

Explanation:

QUESTION NO: 128

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 all VPN deployments (except those with third-party VPN peers)
- C. Support for SecureClient/SecuRemote/SSL Network Extender encrypted connections
- D. Support for Performance Pack acceleration

Answer: C

Explanation:

QUESTION NO: 129

Included in the customer's network are some firewall systems with the Performance Pack in use. The customer wishes to use these firewall systems in a cluster (Load Sharing mode). He is not sure if he can use the Sticky Decision Function in this cluster. Explain the situation to him.

- A. Sticky Decision Function is not supported when employing either Performance Pack or a hardware-based accelerator card. Enabling the Sticky Decision Function disables these acceleration products.
- B. ClusterXL always supports the Sticky Decision Function in the Load Sharing mode.
- C. The customer can use the firewalls with Performance Pack inside the cluster, which should support the Sticky Decision Function. It is just necessary to enable the Sticky Decision Function in the SmartDashboard cluster object in the ClusterXL page, Advanced Load Sharing Configuration window.
- D. The customer can use the firewalls with Performance Pack inside the cluster, which should support the Sticky Decision Function. It is just necessary to configure it with the `clusterXL_SDF_enable` command.

Answer: A

Explanation:

QUESTION NO: 130

A connection is said to be Sticky when:

- A. The connection information sticks in the connection table even after the connection has ended.
- B. A copy of each packet in the connection sticks in the connection table until a corresponding reply packet is received from the other side.
- C. A connection is not terminated by either side by FIN or RST packet.
- D. All the connection packets are handled, in either direction, by a single cluster member.

Answer: D

Explanation:

QUESTION NO: 131

How does a cluster member take over the VIP after a failover event?

- A. Broadcast storm
- B. iflist -renew
- C. Ping the sync interface
- D. Gratuitous ARP

Answer: D

Explanation:

QUESTION NO: 132

Check Point Clustering protocol, works on:

- A. UDP 500
- B. UDP 8116
- C. TCP 8116
- D. TCP 19864

Answer: B

Explanation:

QUESTION NO: 133

A customer is calling saying one member's status is Down. What will you check?

- A. cphaprob list (verify what critical device is down)
- B. fw ctl pstat (check sync)
- C. fw ctl debug -m cluster + forward (forwarding layer debug)
- D. tcpdump/snoop (CCP traffic)

Answer: A

Explanation:

QUESTION NO: 134

A customer calls saying that a Load Sharing cluster shows drops with the error First packet is not SYN. Complete the following sentence. I will recommend:

- A. turning on SDF (Sticky Decision Function)
- B. turning off SDF (Sticky Decision Function)
- C. changing the load on each member
- D. configuring flush and ack

Answer: A

Explanation:

QUESTION NO: 135

Which of the following commands can be used to troubleshoot ClusterXL sync issues?

- A. fw debug cxl connections > file_name
- B. fw tab -s -t connections > file_name
- C. fw tab -u connections > file_name
- D. fw ctl -s -t connections > file_name

Answer: B

Explanation:

QUESTION NO: 136

Which of the following commands shows full synchronization status?

- A. fw hastat
- B. cphaprob -i list
- C. cphaprob -a if
- D. fw ctl iflist

Answer: B

Explanation:

QUESTION NO: 137

Which of the following commands shows full synchronization status?

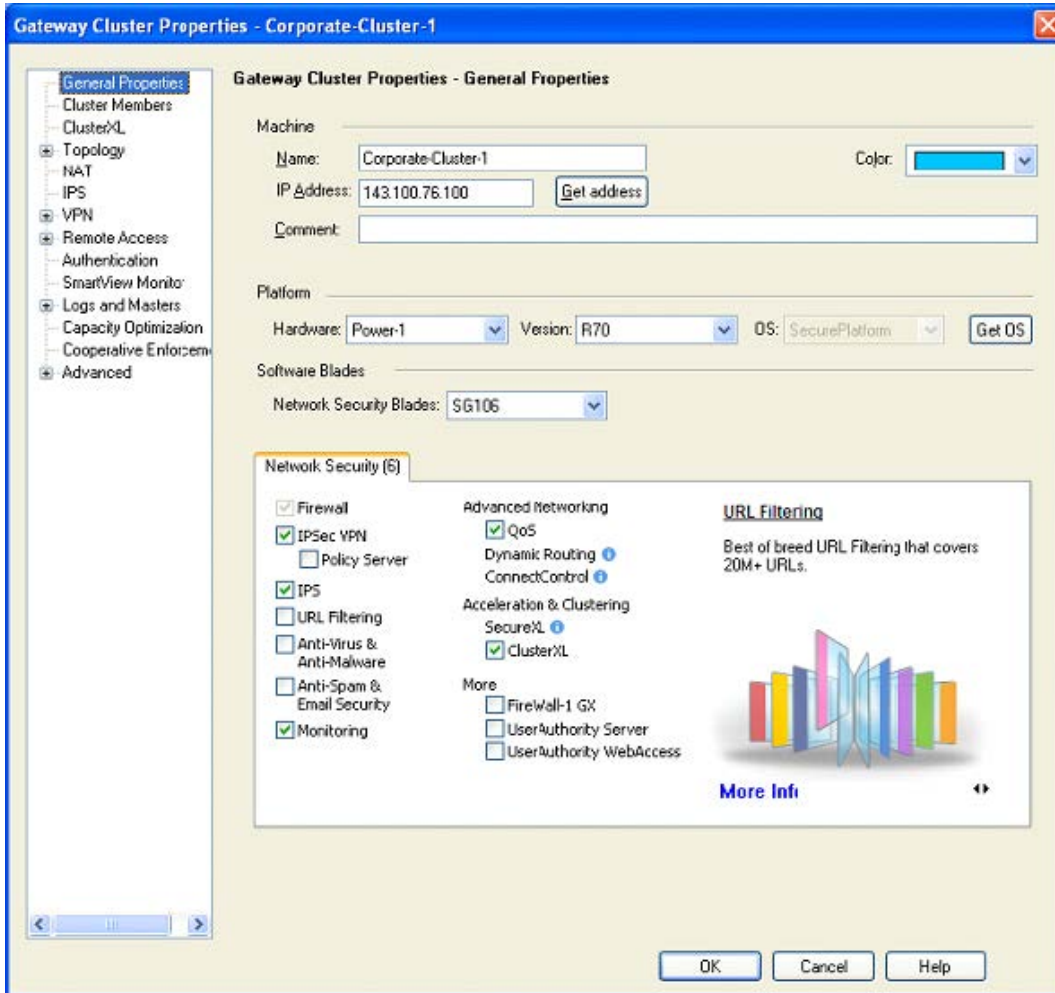
- A. cphaprob -a if
- B. fw ctl iflist
- C. fw hastat
- D. fw ctl pstat

Answer: D

Explanation:

QUESTION NO: 138

John is configuring a new R76 Gateway cluster but he can not configure the cluster as Third Party IP Clustering because this option is not available in Gateway Cluster Properties.



What's happening?

- A. Third Party Clustering is not available for R76Security Gateways.
- B. John is not using third party hardware as IP Clustering is part of Check Point's IP Appliance.
- C. ClusterXL needs to be unselected to permit 3rd party clustering configuration.
- D. John has an invalid ClusterXL license.

Answer: C

Explanation:

QUESTION NO: 139

In ClusterXL, _____ is defined by default as a critical device.

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

Answer: A

Explanation:

QUESTION NO: 140

In ClusterXL, _____ is defined by default as a critical device.

- A. fw.d
- B. protect.exe
- C. PROT_SRV.EXE
- D. Filter

Answer: D

Explanation:

QUESTION NO: 141

Refer to Exhibit below:

Mode	Configuration
A. Legacy Mode High Availability	1. Every member of the cluster receives all packets sent to the cluster IP address, which the load distributed optimally among all cluster members
B. New Mode High Availability	2. Only one machine is active at any 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 the other machines in the cluster, implementing both load sharing and redundancy

Match the ClusterXL modes with their configurations.

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

Answer: D

Explanation:

QUESTION NO: 142

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

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

Answer: D

Explanation:

QUESTION NO: 143

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

- A.** User Authentication connections will be lost by the cluster.
- B.** An SMTP resource connection using CVP will be maintained by the cluster.
- 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: B

Explanation:

QUESTION NO: 144

When a failed cluster member recovers, which of the following actions is NOT taken by the recovering member?

- A.** It will try to take the policy from one of the other cluster members.
- B.** It will not check for any updated policy and load the last installed policy with a warning message

- indicating that the Security Policy needs to be installed from the Security Management Server.
- C.** If the Security Management Server has a newer policy, it will be retrieved, else the local policy will be loaded.
 - D.** It compares its local policy to the one on the Security Management Server.

Answer: B

Explanation:

QUESTION NO: 145

Organizations are sometimes faced with the need to locate cluster members in different geographic locations that are distant from each other. A typical example is replicated data centers whose location is widely separated for disaster recovery purposes. What are the restrictions of this solution?

- A.** There are no restrictions.
- B.** There is one restriction: The synchronization network must guarantee no more than 150 ms latency (ITU Standard G.114).
- C.** There is one restriction: The synchronization network must guarantee no more than 100 ms latency.
- D.** There are two restrictions: 1. The synchronization network must guarantee no more than 100ms latency and no more than 5% packet loss. 2. The synchronization network may only include switches and hubs.

Answer: D

Explanation:

QUESTION NO: 146

You are the MegaCorp Security Administrator. This company uses a firewall cluster, consisting of two cluster members. The cluster generally works well but one day you find that the cluster is behaving strangely. You assume that there is a connectivity problem with the cluster synchronization cluster link (cross-over cable). Which of the following commands is the best for testing the connectivity of the crossover cable?

- A.** telnet <IP address of the synchronization interface on the other cluster member>
- B.** ifconfig -a
- C.** ping <IP address of the synchronization interface on the other cluster member>
- D.** arping <IP address of the synchronization interface on the other cluster member>

Answer: D

Explanation:

QUESTION NO: 147

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

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

Answer: C

Explanation:

QUESTION NO: 148

What command will allow you to disable sync on a cluster firewall member?

- A. fw ctl syncstat stop
- B. fw ctl setsync off
- C. fw ctl setsync 0
- D. fw ctl syncstat off

Answer: B

Explanation:

QUESTION NO: 149

When using ClusterXL in Load Sharing, what is the default method?

- A. IPs, Ports, SPIs
- B. IPs
- C. IPs, Ports
- D. IPs, SPIs

Answer: A

Explanation:

QUESTION NO: 150

If ClusterXL Load Sharing is enabled with state synchronization enabled, what will happen if one member goes down?

- A. The connections are dropped as Load Sharing does not support High Availability.
- B. The processing of all connections handled by the faulty machine is dropped, so all connections need to be re-established through the other machine(s).
- C. There is no state synchronization on Load Sharing, only on High Availability.
- D. The processing of all connections handled by the faulty machine is immediately taken over by the other member(s).

Answer: D

Explanation:

QUESTION NO: 151

In the following cluster configuration; if you reboot sglondon_1 which device will be active when sglondon_1 is back up and running? Why?

- A. Sglondon_1, because it is up again, sglondon_2 took over during reboot
- B. Sglondon_2 because I has highest IP
- C. Sglondon_2 because it has highest priority
- D. Sglondon_1 because it the first configured object with the lowest IP

Answer: C

Explanation:

QUESTION NO: 152

What is a "sticky" connection?

- A. A Sticky Connection is one in which a reply packet returns through the same gateway as the original packet.
- B. A Sticky Connection is a VPN connection that remains up until you manually bring it down.

C. A Sticky Connection is a connection that remains the same.

D. A Sticky Connection is a connection that always chooses the same gateway to set up the initial connection.

Answer: A

Explanation:

QUESTION NO: 153

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

A. 1. Use the ifconfig command to configure and enable the new interface.

2. Run cpstop and cpstart on both members at the same time.

3. Update the topology in the cluster object for the cluster and both members.

4. Install the Security Policy.

B. 1. Disable "Cluster membership" from one Gateway via cpconfig.

2. Configure the new interface via sysconfig from the "non-member" Gateway.

3. RE. enable "Cluster membership" on the Gateway.

4. Perform the same step on the other Gateway.

5. Update the topology in the cluster object for the cluster and members.

6. Install the Security Policy.

C. 1. Run cpstop on one member, and configure the new interface via sysconfig.

2. Run cpstart on the member. Repeat the same steps on another member.

3. Update the new topology in the cluster object for the cluster and members.

4. Install the Security Policy.

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

2. Update the topology in the cluster object for the cluster and both members.

3. Install the Security Policy.

Answer: C

Explanation:

QUESTION NO: 154

Match the Best Management High Availability synchronization-status descriptions for your Security Management Server (SMS):

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

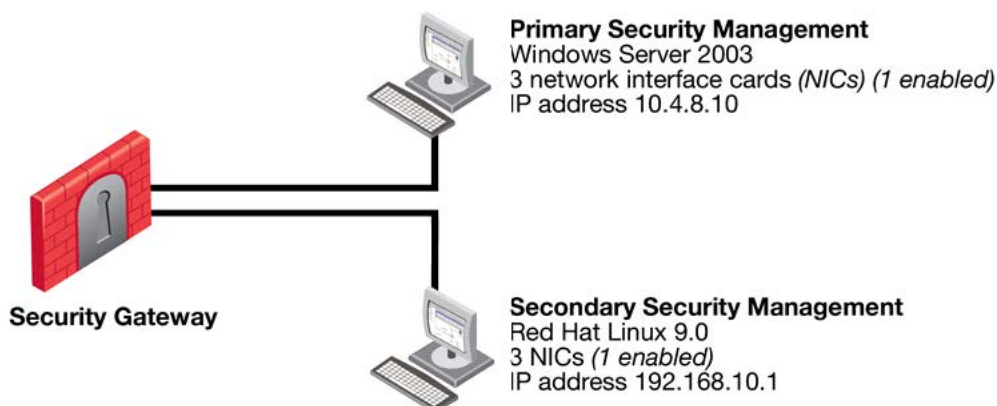
- A. A - 3, B - 1, C - 2, D - 4
- B. A - 3, B - 1, C - 4, D - 2
- C. A - 4, B - 3, C - 1, D - 2
- D. A - 3, B - 2, C - 1, D - 4

Answer: A

Explanation:

QUESTION NO: 155

Review the R76 configuration.



Is it correct for Management High Availability?

- A. No, the Security Management Servers must reside on the same network.
- B. No, the Security Management Servers must be installed on the same operating system.
- C. No, the Security Management Servers do not have the same number of NICs.
- D. No, a R71 Security Management Server cannot run on Red Hat Linux 9.0.

Answer: B

Explanation:

QUESTION NO: 156

Check Point New Mode HA is a(n) _____ solution.

- A. primary-domain
- B. hot-standby
- C. acceleration
- D. load-balancing

Answer: B

Explanation:

QUESTION NO: 157

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

- A. The active member responds to the virtual address and is the only member that passes traffic.
- B. The active member responds to the virtual address and, using sync network forwarding, both members pass traffic.
- C. Both members respond to the virtual address but only the active member is able to pass traffic.
- D. Both members respond to the virtual address and both members pass traffic.

Answer: A

Explanation:

QUESTION NO: 158

Review the cphaprob state command output from one New Mode High Availability ClusterXL cluster member.

```
Cluster Mode: New High Availability <Active Up>
Number      Unique IP Address    Assigned Load    State
1 <local>   192.168.1.1         0%              standby
2           192.168.1.2         100%           active
```

Which member will be active after member 192.168.1.2 fails over and is rebooted?

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

Answer: C

Explanation:

QUESTION NO: 159

Review the cphaprob state command output from a New Mode High Availability cluster member.

```
Cluster Mode: New High Availability <Active Up>
Number      Unique IP Address    Assigned Load    State
1 <local>   192.168.1.1         0%              down
2           192.168.1.2         100%           active
```

Which machine has the highest priority?

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

Answer: B

Explanation:

QUESTION NO: 160

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

- A. 5 seconds.
- B. 0.5 second.
- C. 0.1 second.
- D. 1 second.

Answer: C

Explanation:

QUESTION NO: 161

You have just upgraded your Load Sharing gateway cluster (both members) from NGX R65 to R76. cphaprob stat shows:

Cluster Mode: New High Availability (Active Up)

Member	Unique Address	Assigned Load	State
1	172.16.185.21	100%	Active
2	172.16.185.22	0%	Ready

Which of the following is not a possible cause of this?

- A. You have a different number of cores defined for CoreXL between the two members
- B. Member 1 has CoreXL disabled and member 2 does not
- C. Member 1 is at a lower version than member 2
- D. You have not run cpconfig on member 2 yet.

Answer: D

Explanation:

QUESTION NO: 162

In Management High Availability, what is an Active SMS?

- A. Active Security Master Server
- B. Active Smart Management Server
- C. Active Security Management Server
- D. Active Smart Master Server

Answer: C

Explanation:

QUESTION NO: 163

For Management High Availability, if an Active SMS goes down, does the Standby SMS automatically take over?

- A. Yes, if you set up ClusterXL
- B. Yes, if you set up SecureXL
- C. No, the transition should be initiated manually
- D. Yes, if you set up VRRP

Answer: C

Explanation:

QUESTION NO: 164

For Management High Availability synchronization, what does the Advance status mean?

- A. The peer SMS has not been synchronized properly.
- B. The peer SMS is properly synchronized.
- C. The active SMS and its peer have different installed policies and databases.
- D. The peer SMS is more up-to-date.

Answer: D

Explanation:

QUESTION NO: 165

Which of the following would be a result of having more than one active Security Management

Server in a Management High Availability (HA) configuration?

- A. The need to manually synchronize the secondary Security Management Server with the Primary Security Management Server is eliminated.
- B. Allows for faster seamless failover: from active-to-active instead of standby-to-active.
- C. An error notification will popup during SmartDashboard login if the two machines can communicate indicating Collision status.
- D. Creates a High Availability implementation between the Gateways installed on the Security Management Servers.

Answer: C

Explanation:

QUESTION NO: 166

You want to verify that your Check Point cluster is working correctly. Which command line tool can you use?

- A. cphastart -status
- B. cphainfo -s
- C. cphaprob state
- D. cphaconf state

Answer: C

Explanation:

QUESTION NO: 167

How can you view the virtual cluster interfaces of a Cluster XL environment?

- A. cphaprob -ia if
- B. cphaprob -a if
- C. cphaprob -a list
- D. cphaprob -ia list

Answer: B

Explanation:

QUESTION NO: 168

How can you view the critical devices on a cluster member in a Cluster XL environment?

- A. cphaprob -ia list
- B. cphaprob -a if
- C. cphaprob -a list
- D. cphaprob -ia if

Answer: A

Explanation:

QUESTION NO: 169

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

- A. All members receive all packets. The Security Management Server decides which member will process the packets. Other members delete the packets from memory.
- B. All cluster members process all packets and members synchronize with each other.
- C. All members receive all packets. All members run an algorithm which determines which member processes packets further and which members delete the packet from memory.
- D. Only one member at a time is active. The active cluster member processes all packets.

Answer: C

Explanation:

QUESTION NO: 170

Which of the following does NOT happen when using Pivot Mode in ClusterXL?

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

Answer: A

Explanation:

QUESTION NO: 171

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

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

Answer: D

Explanation:

QUESTION NO: 172

By default, the Cluster Control Protocol (CCP) uses this to send delta sync messages to other cluster members.

- A. Broadcast
- B. Unicast
- C. Multicast
- D. Shoutcast

Answer: C

Explanation:

QUESTION NO: 173

To configure the Cluster Control Protocol (CCP) to use Broadcast, the following command is run:

- A. `set_ccp cpcluster broadcast`
- B. `ccp broadcast`
- C. `clusterconfig set_ccp broadcast`
- D. `cphaconf set_ccp broadcast`

Answer: D

Explanation:

QUESTION NO: 174

What cluster mode is represented in this case?

- 1). (local) 172.168.1.1 100\$ active
- 2). 172.14*.1.2 0\$ standby

- A. Load Sharing (multicast mode)
- B. HA (New mode).
- C. 3rd party cluster
- D. Load Sharing Unicast (Pivot) mode

Answer: B

Explanation:

QUESTION NO: 175

What cluster mode is represented in this case?

```

1 (local) 172.168.1.1    50%    active
2          172.168.1.2    50%    active
    
```

- A. 3rd party cluster
- B. Load Sharing (multicast mode)
- C. Load Sharing Unicast (Pivot) mode
- D. HA (New mode)

Answer: B

Explanation:

QUESTION NO: 176

Which of the listed load-balancing methods is NOT valid?

- A. Random
- B. Domain
- C. They are all valid
- D. Round Trip

Answer: C

Explanation:

QUESTION NO: 177

Which method of load balancing describes "Round Robin"?

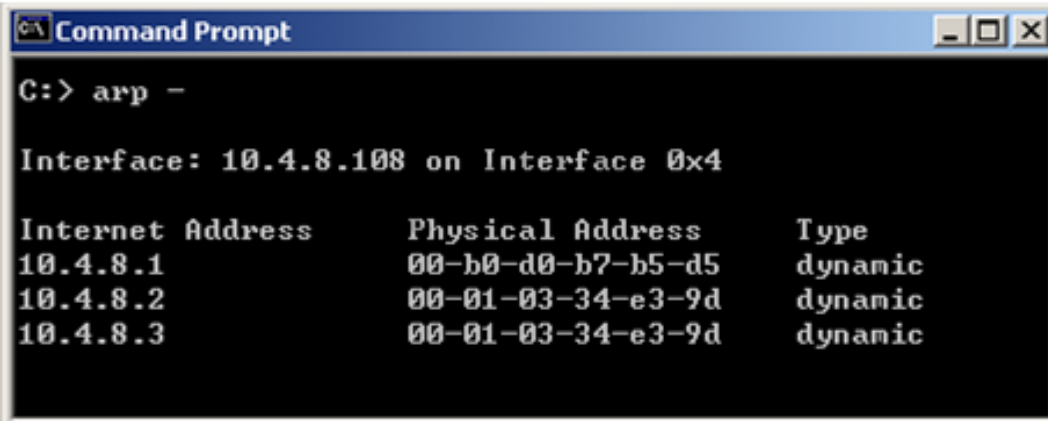
- A. Assigns service requests to the next server in a series.
- B. Assigns service requests to servers at random.
- C. Measures the load on each server to determine which server has the most available resources.
- D. Ensures that incoming requests are handled by the server with the fastest response time.

Answer: A

Explanation:

QUESTION NO: 178

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.



```
Command Prompt
C:\> arp -

Interface: 10.4.8.108 on Interface 0x4

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

Review the ARP table from the internal Windows host 10.4.8.108. According to the output, which

member is the standby machine?

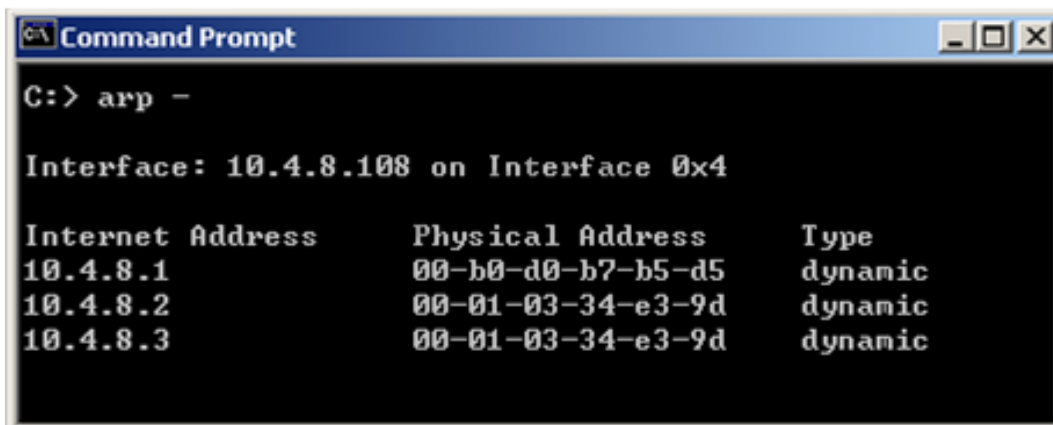
- A. 10.4.8.3
- B. The standby machine cannot be determined by this test.
- C. 10.4.8.1
- D. 10.4.8.2

Answer: C

Explanation:

QUESTION NO: 179

In New Mode HA, the internal cluster IP VIP address is 10.4.8.3. An internal host 10.4.8.108 successfully pings its Cluster and receives replies. Review 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?



```
Command Prompt
C:> arp -

Interface: 10.4.8.108 on Interface 0x4

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

- A. The active cluster member's IP address cannot be determined by this ARP cache.
- B. 10.4.8.3
- C. 10.4.8.1
- D. 10.4.8.2

Answer: D

Explanation:

QUESTION NO: 180

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

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

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

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

Is State Synchronization working properly between the two members?

- A. Members A and B are not synchronized, because #VALS in the connections table are not close.
- B. Members A and B are not synchronized, because #PEAK for both members is not close in the connections table.
- C. Members A and B are synchronized, because #SLINKS are identical in the connections table.
- D. Members A and B are synchronized, because ID for both members is identical in the connections table.

Answer: A

Explanation:

QUESTION NO: 181

You have two IP Appliances: one IP565 and one IP395. Both appliances have IPSO 6.2 and R76 installed in a distributed deployment. Can they be members of a Gateway Cluster?

- A. No, because the Security Gateways must be installed in a stand-alone installation.
- B. No, because IP does not have a cluster option.
- C. Yes, as long as they have the same IPSO and Check Point versions.
- D. No, because the appliances must be of the same model (both should be IP565 or IP395).

Answer: C

Explanation:

QUESTION NO: 182

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

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

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

Answer: D

Explanation:

QUESTION NO: 183

Included in the client's network are some switches, which rely on IGMP snooping. You must find a solution to work with these switches. Which of the following answers does NOT lead to a successful solution?

- A. Set the value of fwaha_enable_igmp_snooping module configuration parameter to 1.
- B. Configure static CAMs to allow multicast traffic on specific ports.
- C. ClusterXL supports IGMP snooping by default. There is no need to configure anything.
- D. Disable IGMP registration in switches that rely on IGMP packets

Answer: C

Explanation:

QUESTION NO: 184

The customer wishes to install a cluster. In his network, there is a switch which is incapable of forwarding multicast. Is it possible to install a cluster in this situation?

- A. Yes, you can toggle on ClusterXL between broadcast and multicast by setting the multicast mode using the command `cphaconf set_ccp multicast on/off`. The default setting is broadcast.
- B. Yes, you can toggle on ClusterXL between broadcast and multicast using the command `cphaconf set_ccp broadcast/multicast`.
- C. No, the customer needs to replace the switch with a new switch, which supports multicast forwarding.
- D. Yes, the ClusterXL changes automatically to the broadcast mode if the multicast is not forwarded.

Answer: B

Explanation:

QUESTION NO: 185

What could be a reason why synchronization between primary and secondary Security Management Servers does not occur?

- A. You did not activate synchronization within Global Properties.
- B. You are using different time zones.
- C. You have installed both Security Management Servers on different server systems (e. g. one machine on HP hardware and the other one on DELL).
- D. If the set of installed products differ from each other, the Security Management Servers do not synchronize the database to each other.

Answer: D

Explanation:

QUESTION NO: 186

What is the proper command for importing users into the R76 User Database?

- A. `fwm dbimport`
- B. `fwm importusrs`
- C. `fwm import`
- D. `fwm importdb`

Answer: A

Explanation:

QUESTION NO: 187

In a R76 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 trigger.

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

Answer: A

Explanation:

QUESTION NO: 188

What is a requirement for setting up R76 Management High Availability?

- A. All Security Management Servers must have the same number of NICs.
- B. All Security Management Servers must have the same operating system.
- C. State synchronization must be enabled on the secondary Security Management Server.
- D. All Security Management Servers must reside in the same LAN.

Answer: B

Explanation:

QUESTION NO: 189

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



Are these machines correctly configured for a ClusterXL deployment?

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

Answer: A

Explanation:

QUESTION NO: 190

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: 1 GB, Security Gateway only, version: R76

Cluster Member 2: OS: SecurePlatform, NICs: 4 Intel 3Com, memory: 1 GB, Security Gateway

only, version: R76

Cluster Member 3: OS: SecurePlatform, NICs: 4 other manufacturers, memory: 512 MB, Security Gateway only, version: R76

Security Management Server: MS Windows 2003, NIC. Intel NIC (1), Security Gateway and primary Security Management Server installed, version: R76

Are these machines correctly configured for a ClusterXL deployment?

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

Answer: C

Explanation:

QUESTION NO: 191

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

Cluster Member 1: 4 NICs, 3 enable: hme0: 192.168.10/24, hme1: 10.10.10/24, qfe2: 172.16.10.1/24

Cluster Member 2: 5 NICs, 3 enable: hme0: 192.168.10/24, hme1: 10.10.10/24, qfe2: 172.16.10.1/24

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 Security Management Server is located on the internal network with IP 172.16.10.3. What is the problem with this configuration?

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

Answer: C

Explanation:

QUESTION NO: 192

What is the reason for the following error?

```
[fw1]#  
[fw1]#  
[fw1]#  
[fw1]#  
[fw1]#  
[fw1]#  
[fw1]#  
[fw1]#  
[fw1]#  
[fw1]#  
[fw1]# cphaprob -i list  
Built-in Devices:  
Device Name: Interface Active Check  
Device Name: HA Initialization  
Registered Devices:  
Device Name: #iw##6#  
Registration number: 0  
Timeout: none  
Failed to query kernel for device no. 1  
[fw1]# _
```

- A. A third-party cluster solution is implemented.
- B. Cluster membership is not enabled on the gateway.
- C. Objects.C does not contain a cluster object.
- D. Device Name contains non-ASCII characters.

Answer: B

Explanation:

QUESTION NO: 193

You find that Gateway fw2 can NOT be added to the cluster object. What are possible reasons for that?

- (i) Center in Star Topology
- (ii) Satellite in Star Topology
- (iii) Center in Remote Access Community
- (iv) Meshed Community

- A. (i) or (ii)
- B. (ii) or (iii)
- C. (i) or (iii)
- D. All

Answer: C

Explanation:

QUESTION NO: 194

In which ClusterXL Load Sharing mode, does the pivot machine get chosen automatically by ClusterXL?

- A. Hot Standby Load Sharing
- B. Unicast Load Sharing
- C. Multicast Load Sharing
- D. CCP Load Sharing

Answer: B

Explanation:

QUESTION NO: 195

What configuration change must you make to change an existing ClusterXL cluster object from Multicast to Unicast mode?

- A. Reset Secure Internal Communications (SIC) on the cluster-member objects. Reinstall the Security Policy.
- B. Run cpstop and cpstart, to re-enable High Availability on both objects. Select Pivot mode in cpconfig.
- C. Change the cluster mode to Unicast on the cluster object. Reinstall the Security Policy.
- D. Change the cluster mode to Unicast on each of the cluster-member objects.

Answer: C

Explanation:

QUESTION NO: 196

In a R76 ClusterXL Load Sharing configuration, which type of ARP related problem can force the

use of Unicast Mode (Pivot) configuration due to incompatibility on some adjacent routers and switches?

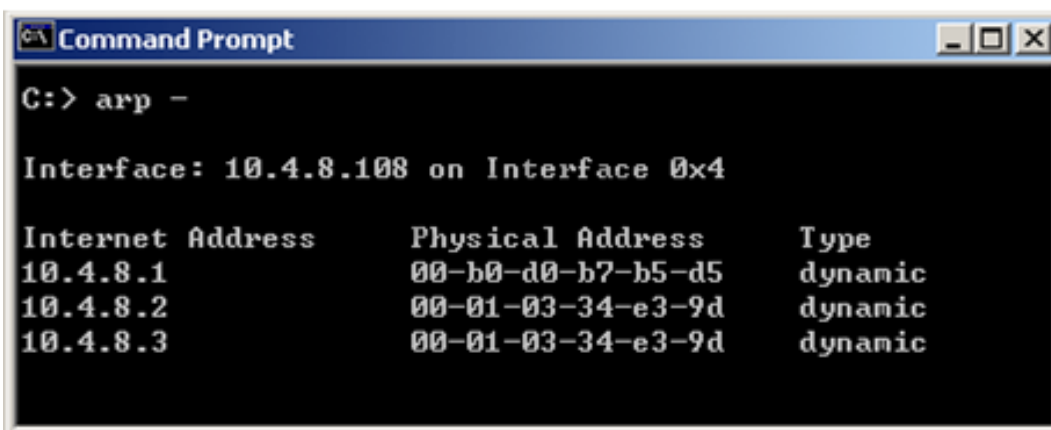
- A. Multicast MAC address response to a Unicast IP request
- B. Unicast MAC address response to a Multicast IP request
- C. Multicast MAC address response to a RARP request
- D. MGCP MAC address response to a Multicast IP request

Answer: A

Explanation:

QUESTION NO: 197

In Load Sharing Unicast mode, the internal cluster IP address is 10.4.8.3. The internal interfaces on two members are 10.4.8.1 and 10.4.8.2. Internal host 10.4.8.108 Pings 10.4.8.3, and receives replies. The following is the ARP table from the internal Windows host 10.4.8.108.



```
C:\> arp -

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
```

Review the exhibit and identify the member serving as the pivot machine.

- A. 10.4.8.3
- B. 10.4.8.2
- C. The pivot machine cannot be determined by this test.
- D. 10.4.8.1

Answer: B

Explanation:

QUESTION NO: 198

Which of the following commands will stop acceleration on a Security Gateway running on SecurePlatform?

- A. splat_accel off
- B. perf_pack off
- C. fw accel off
- D. fwaccel off

Answer: D

Explanation:

QUESTION NO: 199

How do new connections get established through a Security Gateway with SecureXL enabled?

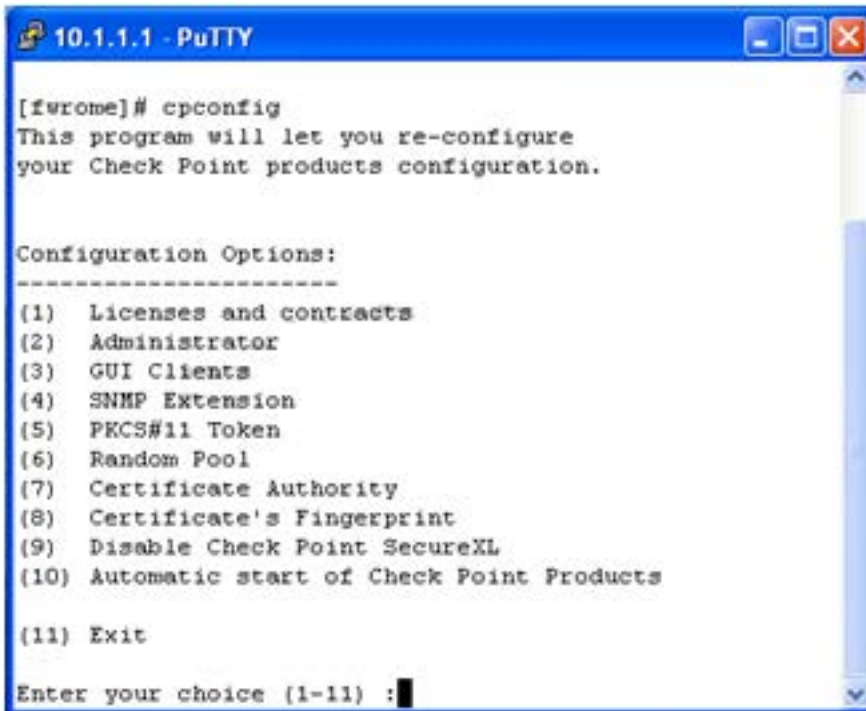
- A. New connections are always inspected by the firewall and if they are accepted, the subsequent packets of the same connection will be passed through SecureXL
- B. The new connection will be first inspected by SecureXL and if it does not match the drop table of SecureXL, then it will be passed to the firewall module for a rule match.
- C. New connection packets never reach the SecureXL module.
- D. If the connection matches a connection or drop template in SecureXL, it will either be established or dropped without performing a rule match, else it will be passed to the firewall module for a rule match.

Answer: D

Explanation:

QUESTION NO: 200

Which of the following commands can be used to bind a NIC to a single processor when using a Performance Pack on SecurePlatform?



- A. sim affinity
- B. splat proc
- C. set proc
- D. fw fat path nic

Answer: A

Explanation:

Topic 3, Volume C

QUESTION NO: 201

Review the Rule Base displayed.

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	Stealth Rule	* Any	Corporate-gw	* Any Traffic	* Any	drop	Log	* Policy Tar	* Any
2	Local uses using ACL	+ Corporate-internal-ne	* Any	* Any Traffic	TOP AOL	accept	Log	* Policy Tar	* Any
3	Customers Accessing Web Server	Customers@Any	Corporate-web-s	* Any Traffic	TOP http	Client Auth	Log	* Policy Tar	* Any
4	Incoming Emails	* Any	Corporate-mail-s	* Any Traffic	SMTP smtp->MailFilter	accept	Log	* Policy Tar	* Any
5	HTTPFTP access	+ Corporate-internal-ne	* Any	* Any Traffic	TOP http TOP ftp	accept	Log	* Policy Tar	* Any
6	Cleanup Rule	* Any	* Any	* Any Traffic	* Any	drop	Log	* Policy Tar	* Any

For which rules will the connection templates be generated in SecureXL?

- A. Rule nos. 2 and 5

- B. Rule no. 2 only
- C. All rules except rule no. 3
- D. Rule nos. 2 to 5

Answer: B

Explanation:

QUESTION NO: 202

Your customer asks you about the Performance Pack. You explain to him that a Performance Pack is a software acceleration product which improves the performance of the Security Gateway. You may enable or disable this acceleration by either:

- 1) The command `cpconfig`

- 2) The command `fwaccel on|off`

What is the difference between these two commands?

- A. Both commands function identically.
- B. The `fwaccel` command determines the default setting. The command `cpconfig` can dynamically change the setting, but after the reboot it reverts to the default setting.
- C. The command `cpconfig` works on the Security Platform only. The command `fwaccel` can be used on all platforms.
- D. The `cpconfig` command enables acceleration. The command `fwaccel` can dynamically change the setting, but after the reboot it reverts to the default setting.

Answer: D

Explanation:

QUESTION NO: 203

Your customer complains of the weak performance of his systems. He has heard that Connection Templates accelerate traffic. How do you explain to the customer about template restrictions and how to verify that they are enabled?

- A. To enhance connection-establishment acceleration, a mechanism attempts to "group together" all connections that match a particular service and whose sole discriminating element is the

source port. To test if connection templates are enabled, use the command `fwaccel stat`.

B. To enhance connection-establishment acceleration, a mechanism attempts to "group together" all connections that match a particular service and whose sole discriminating element is the destination port. To test if connection templates are enabled, use the command `fwaccel templates`.

C. To enhance connection-establishment acceleration, a mechanism attempts to "group together" all connections that match a particular service and whose sole discriminating element is the destination port. To test if connection templates are enabled, use the command `fw ctl templates`.

D. To enhance connection-establishment acceleration, a mechanism attempts to "group together" all connections that match a particular service and whose sole discriminating element is the source port. To test if connection templates are enabled, use the command `fw ctl templates`.

Answer: A

Explanation:

QUESTION NO: 204

Frank is concerned with performance and wants to configure the affinities settings. His gateway does not have the Performance Pack running. What would Frank need to perform in order to configure those settings?

- A.** Edit `$FWDIR/conf/fwaffinity.conf` and change the settings.
- B.** Edit `affinity.conf` and change the settings.
- C.** Run `fw affinity` and change the settings.
- D.** Run `sim affinity` and change the settings.

Answer: A

Explanation:

QUESTION NO: 205

You are concerned that the processor for your firewall running NGX R71 SecurePlatform may be overloaded. What file would you view to determine the speed of your processor(s)?

- A.** `cat /etc/cpuinfo`
- B.** `cat /proc/cpuinfo`
- C.** `cat /var/opt/CPsuite-R71/fw1/conf/cpuinfo`
- D.** `cat /etc/sysconfig/cpuinfo`

Answer: B

Explanation:

QUESTION NO: 206

Which of the following is NOT a restriction for connection template generation?

- A. SYN Defender
- B. ISN Spoofing
- C. UDP services with no protocol type or source port mentioned in advanced properties
- D. VPN Connections

Answer: C

Explanation:

QUESTION NO: 207

In CoreXL, what process is responsible for processing incoming traffic from the network interfaces, securely accelerating authorized packets, and distributing non-accelerated packets among kernel instances?

- A. NAD (Network Accelerator Daemon)
- B. SND (Secure Network Distributor)
- C. SSD (Secure System Distributor)
- D. SNP (System Networking Process)

Answer: B

Explanation:

QUESTION NO: 208

Due to some recent performance issues, you are asked to add additional processors to your firewall. If you already have CoreXL enabled, how are you able to increase Kernel instances?

- A. Once CoreXL is installed you cannot enable additional Kernel instances without reinstalling R76.
- B. In SmartUpdate, right-click on Firewall Object and choose Add Kernel Instances.
- C. Use cpconfig to reconfigure CoreXL.
- D. Kernel instances are automatically added after process installed and no additional configuration is needed.

Answer: C

Explanation:

QUESTION NO: 209

Which of the following platforms does NOT support SecureXL?

- A. Power-1 Appliance
- B. IP Appliance
- C. UTM-1 Appliance
- D. UNIX

Answer: D

Explanation:

QUESTION NO: 210

Which of the following is NOT supported by CoreXL?

- A. SmartView Tracker
- B. Route-based VPN
- C. IPS
- D. IPV4

Answer: B

Explanation:

QUESTION NO: 211

If the number of kernel instances for CoreXL shown is 6, how many cores are in the physical machine?

- A. 6
- B. 8
- C. 4
- D. 12

Answer: B

Explanation:

QUESTION NO: 212

Which of the following is NOT accelerated by SecureXL?

- A. Telnet
- B. FTP
- C. SSH
- D. HTTPS

Answer: B

Explanation:

QUESTION NO: 213

To verify SecureXL statistics you would use the command _____?

- A. fwaccel stats
- B. fw ctl pstat
- C. fwaccel top
- D. cphaprob stat

Answer: A

Explanation:

QUESTION NO: 214

How can you disable SecureXL via the command line (it does not need to survive a reboot)?

- A. cphaprob off
- B. fw ctl accel off
- C. securexl off
- D. fwaccel off

Answer: D

Explanation:

QUESTION NO: 215

Which of these is a type of acceleration in SecureXL?

- A. FTP
- B. connection rate
- C. GRE
- D. QoS

Answer: B

Explanation:

QUESTION NO: 216

The CoreXL SND (Secure Network Distributor) is responsible for:

- A. distributing non-accelerated packets among kernel instances
- B. accelerating VPN traffic
- C. shutting down cores when they are not needed
- D. changing routes to distribute the load across multiple firewalls

Answer: A

Explanation:

QUESTION NO: 217

How can you verify that SecureXL is running?

- A. cpstat os
- B. fw ver
- C. fwaccel stat
- D. securexl stat

Answer: C

Explanation:

QUESTION NO: 218

Which of the following services will cause SecureXL templates to be disabled?

- A. TELNET
- B. FTP
- C. HTTPS
- D. LDAP

Answer: B

Explanation:

QUESTION NO: 219

How do you enable SecureXL (command line) on GAiA?

- A. fw securexl on
- B. fw accel on
- C. fwaccel on
- D. fwsecurexl on

Answer: C

Explanation:

QUESTION NO: 220

The following graphic illustrates which command being issued on SecurePlatform?

Name	Value	Name	Value
conns created	21	conns deleted	2
temporary conns	0	templates	1
nat conns	0	accel packets	698
accel bytes	118462	F2F packets	26183
ESP enc pkts	0	ESP enc err	0
ESP dec pkts	0	ESP dec err	0
ESP other err	0	espudp enc pkts	0
espudp enc err	0	espudp dec pkts	0
espudp dec err	0	espudp other err	0
AH enc pkts	0	AH enc err	0
AH dec pkts	0	AH dec err	0
AH other err	0	memory used	0
free memory	0	acct update interval	3688
current total conns	14	TCP violations	1
conns from templates	11	TCP conns	12
delayed TCP conns	0	non TCP conns	2
delayed nonTCP conns	0	F2F conns	5
F2F bytes	1754802	crypt conns	0
enc bytes	0	dec bytes	0
partial conns	0	anticipated conns	0
dropped packets	56	dropped bytes	7472
--More--			

- A. fwaccel stats
- B. fw accel stats
- C. fw securexl stats
- D. fwsecurexl stats

Answer: A

Explanation:

QUESTION NO: 221

After Travis added new processing cores on his server, CoreXL did not use them. What would be the most plausible reason why? Travis did not:

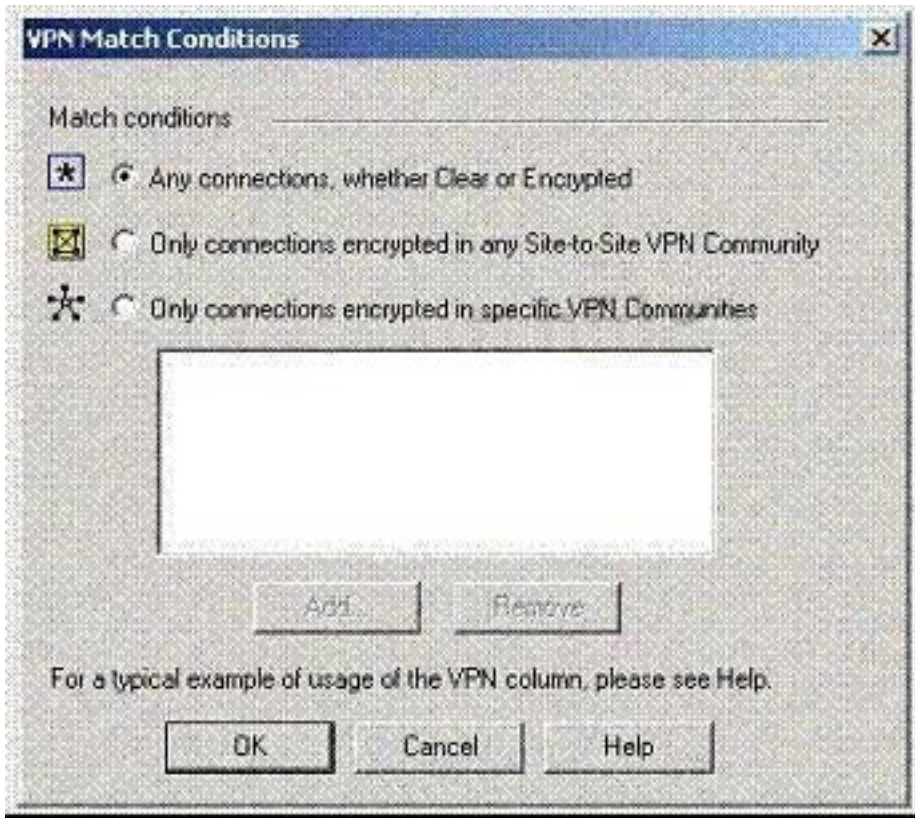
- A. Edit the Gateway Properties and increase the kernel instances.
- B. Run cpconfig to increase the number of CPU cores.
- C. Edit the Gateway Properties and increase the number of CPU cores.
- D. Run cpconfig to increase the kernel instances.

Answer: D

Explanation:

QUESTION NO: 222

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



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

Answer: C

Explanation:

QUESTION NO: 223

A SmartProvisioning Gateway could be a member of which VPN communities?

- (i) Center In Star Topology
- (ii) Satellite in Star Topology
- (iii) Carter in Remote Access Community
- (iv) Meshed Community

A. (ii) and (iii)

- B. All
- C. (i), (ii) and (iii)
- D. (ii) only

Answer: A

Explanation:

QUESTION NO: 224

What process manages the dynamic routing protocols (OSPF, RIP, etc.) on SecurePlatform Pro?

- A. Gated
- B. There's no separate process, but the Linux default router can take care of that.
- C. Routerd
- D. Arouted

Answer: A

Explanation:

QUESTION NO: 225

What is the command to enter the router shell?

- A. gated
- B. routerd
- C. clirouter
- D. router

Answer: D

Explanation:

QUESTION NO: 226

Which statement is TRUE for route-based VPN's?

- A. Route-based VPN's replace domain-based VPN's.
- B. Route-based VPN's are a form of partial overlap VPN Domain.
- C. Dynamic-routing protocols are not required.

D. IP Pool NAT must be configured on each Gateway.

Answer: C

Explanation:

QUESTION NO: 227

VPN routing can also be configured by editing which file?

- A. \$FWDIR\conf\vpn_route.c
- B. \$FWDIR\bin\vpn_route.conf
- C. \$FWDIR\conf\vpn_route.conf
- D. \$FWDIR\VPN\route_conf.c

Answer: C

Explanation:

QUESTION NO: 228

If both domain-based and route-based VPN's are configured, which will take precedence?

- A. Must be chosen/configured manually by the Administrator in the Policy > Global Properties
- B. Must be chosen/configured manually by the Administrator in the VPN community object
- C. Domain-based
- D. Route-based

Answer: C

Explanation:

QUESTION NO: 229

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

- A. They are only supported on the IPSO Operating System.
- B. VTIs cannot be assigned a proxy interface.
- C. VTIs can only be physical, not loopback.
- D. Local IP addresses are not configured, remote IP addresses are configured.

Answer: A

Explanation:

QUESTION NO: 230

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

- A. VTIs must be assigned a proxy interface.
- B. VTIs can only be physical, not loopback.
- C. VTIs are only supported on SecurePlatform.
- D. Local IP addresses are not configured, remote IP addresses are configured.

Answer: A

Explanation:

QUESTION NO: 231

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

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

Answer: B

Explanation:

QUESTION NO: 232

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

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

Answer: D

Explanation:

QUESTION NO: 233

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

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

Answer: C

Explanation:

QUESTION NO: 234

When configuring numbered VPN Tunnel Interfaces (VTIs) in a clustered environment, what issues need to be considered?

- (1) Each member must have a unique source IP address
- (2) Every interface on each member required a unique IP address
- (3) All VTIs going to the same remote peer must have the same name.
- (4) Cluster IP addresses are required.

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

Answer: D

Explanation:

QUESTION NO: 235

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

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

Answer: C

Explanation:

QUESTION NO: 236

What is used to validate a digital certificate?

- A. S/MIME
- B. CRL
- C. IPsec
- D. PKCS

Answer: B

Explanation:

QUESTION NO: 237

Which statement defines Public Key Infrastructure? Security is provided:

- A. by Certificate Authorities, digital certificates, and two-way symmetric-key encryption.
- B. by Certificate Authorities, digital certificates, and public key encryption.
- C. via both private and public keys, without the use of digital Certificates.
- D. by authentication.

Answer: B

Explanation:

QUESTION NO: 238

Match the VPN-related terms with their definitions:

Term	Definition
A. VPN Community	1. Traffic routed to VPN tunnel based on route table entries
B. VPN Domain	2. Hosts behind the Gateway
C. Domain based VPN	3. Collection of VPN tunnels
D. Route based VPN	4. Traffic routed to VPN tunnel based on object definitions

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

Answer: C

Explanation:

QUESTION NO: 239

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

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

Answer: C

Explanation:

QUESTION NO: 240

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

- A. Communities > Communities
- B. internal_clear > All_GwToGw
- C. internal_clear > All_communities
- D. Internal_clear > External_Clear

Answer: C

Explanation:

QUESTION NO: 241

Which of the following statements is FALSE regarding OSPF configuration on SecurePlatform Pro?

- A.** router ospf 1 creates the Router ID for the Security Gateway and should be the same ID for all Gateways.
- B.** router ospf 1 creates the Router ID for the Security Gateway and should be different for all Gateways.
- C.** router ospf 1 creates an OSPF routing instance and this process ID should be different for each Security Gateway.
- D.** router ospf 1 creates an OSPF routing instance and this process ID should be the same on all Gateways.

Answer: D

Explanation:

QUESTION NO: 242

If you need strong protection for the encryption of user data, what option would be the BEST choice?

- A.** When you need strong encryption, IPsec is not the best choice. SSL VPN's are a better choice.
- B.** Use Diffie-Hellman for key construction and pre-shared keys for Quick Mode. Choose SHA in Quick Mode and encrypt with AES. Use AH protocol. Switch to Aggressive Mode.
- C.** Disable Diffie-Hellman by using stronger certificate based key-derivation. Use AES-256 bit on all encrypted channels and add PFS to QuickMode. Use double encryption by implementing AH and ESP as protocols.
- D.** Use certificates for Phase 1, SHA for all hashes, AES for all encryption and PFS, and use ESP protocol.

Answer: D

Explanation:

QUESTION NO: 243

Review the following list of actions that Security Gateway R76 can take when it controls packets. The Policy Package has been configured for Simplified Mode VPN. Select the response below that includes the available actions:

- A. Accept, Drop, Encrypt, Session Auth
- B. Accept, Drop, Reject, Client Auth
- C. Accept, Hold, Reject, Proxy
- D. Accept, Reject, Encrypt, Drop

Answer: B

Explanation:

QUESTION NO: 244

Your organization maintains several IKE VPN's. Executives in your organization want to know which mechanism Security Gateway R76 uses to guarantee the authenticity and integrity of messages. Which technology should you explain to the executives?

- A. Digital signatures
- B. Certificate Revocation Lists
- C. Key-exchange protocols
- D. Application Intelligence

Answer: A

Explanation:

QUESTION NO: 245

There are times when you want to use Link Selection to manage high-traffic VPN connections. With Link Selection you can:

- A. Probe links for availability.
- B. Use links based on Day/Time.
- C. Assign links to specific VPN communities.
- D. Use links based on authentication method.

Answer: A

Explanation:

QUESTION NO: 246

There are times when you want to use Link Selection to manage high-traffic VPN connections. With Link Selection you can:

- A. Assign links to use Dynamic DNS.
- B. Use links based on authentication method.
- C. Use links based on Day/Time.
- D. Use Load Sharing to distribute VPN traffic.

Answer: D

Explanation:

QUESTION NO: 247

There are times when you want to use Link Selection to manage high-traffic VPN connections. With Link Selection you can:

- A. Assign links to specific VPN communities.
- B. Assign links to use Dynamic DNS.
- C. Use links based on services.
- D. Prohibit Dynamic DNS.

Answer: C

Explanation:

QUESTION NO: 248

There are times when you want to use Link Selection to manage high-traffic VPN connections. With Link Selection you can:

- A. Use links based on Day/Time.
- B. Set up links for Remote Access.
- C. Assign links to specific VPN communities.
- D. Assign links to use Dynamic DNS.

Answer: B

Explanation:

QUESTION NO: 249

What type of object may be explicitly defined as a MEP VPN?

- A. Mesh VPN Community
- B. Any VPN Community
- C. Remote Access VPN Community
- D. Star VPN Community

Answer: D

Explanation:

QUESTION NO: 250

MEP VPN's use the Proprietary Probing Protocol to send special UDP RDP packets to port _____ to discover if an IP is accessible.

- A. 259
- B. 256
- C. 264
- D. 201

Answer: A

Explanation:

QUESTION NO: 251

Which of the following statements is TRUE concerning MEP VPN's?

- A. State synchronization between Security Gateways is required.
- B. MEP VPN's are not restricted to the location of the gateways.
- C. The VPN Client is assigned a Security Gateway to connect to based on a priority list, should the first connection fail.
- D. MEP Security Gateways cannot be managed by separate Management Servers.

Answer: B

Explanation:

QUESTION NO: 252

Which of the following statements is TRUE concerning MEP VPN's?

- A. The VPN Client is assigned a Security Gateway to connect to based on a priority list, should the first connection fail.
- B. MEP Security Gateways can be managed by separate Management Servers.
- C. MEP VPN's are restricted to the location of the gateways.
- D. State synchronization between Security Gateways is required.

Answer: B

Explanation:

QUESTION NO: 253

Which of the following statements is TRUE concerning MEP VPN's?

- A. State synchronization between Security Gateways is NOT required.
- B. MEP Security Gateways cannot be managed by separate Management Servers.
- C. The VPN Client is assigned a Security Gateway to connect to based on a priority list, should the first connection fail.
- D. MEP VPN's are restricted to the location of the gateways.

Answer: A

Explanation:

QUESTION NO: 254

Which of the following statements is TRUE concerning MEP VPN's?

- A. MEP Security Gateways cannot be managed by separate Management Servers.
- B. MEP VPN's are restricted to the location of the gateways.
- C. The VPN Client selects which Security Gateway takes over, should the first connection fail.
- D. State synchronization between Security Gateways is required.

Answer: C

Explanation:

QUESTION NO: 255

You need to publish GAIa routes using the OSPF routing protocol. What is the correct command structure, once entering the route command, to implement OSPF successfully?

- A. Run cpconfig utility to enable ospf routing
- B. ip route ospf
ospf network1
ospf network2
- C. Enable
Configure terminal
Router ospf [id]
Network [network] [wildmask] area [id]
- D. Use DBedit utility to either the objects_5_0.c file

Answer: C

Explanation:

QUESTION NO: 256

At what router prompt would you save your OSPF configuration?

- A. localhost.localdomain(config)#
- B. localhost.localdomain(config-if)#
- C. localhost.localdomain#
- D. localhost.localdomain(config-router-ospf)#

Answer: C

Explanation:

QUESTION NO: 257

What is the router command to save your OSPF configuration?

- A. save memory
- B. write config
- C. save
- D. write mem

Answer: D

Explanation:

QUESTION NO: 258

What is the command to show OSPF adjacencies?

- A. show ospf interface
- B. show ospf summary-address
- C. show running-config
- D. show ip ospf neighbor

Answer: D

Explanation:

QUESTION NO: 259

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

Answer: B

Explanation:

QUESTION NO: 260

Which of the following operating systems support numbered VTI's?

- A. SecurePlatform Pro
- B. Solaris

- C. IPSO 4.0 +
- D. Windows Server 2008

Answer: A

Explanation:

QUESTION NO: 261

Which type of routing relies on a VPN Tunnel Interface (VTI) to route traffic?

- A. Domain-based VPN
- B. Route-based VPN
- C. Subnet-based VPN
- D. Host-based VPN

Answer: B

Explanation:

QUESTION NO: 262

You have installed SecurePlatform R76 as Security Gateway operating system. As company requirements changed, you need the VTI features of R76. What should you do?

- A. Only IPSO 3.9 supports VTI feature, so you have to replace your Security Gateway with Nokia appliances.
- B. In SmartDashboard click on the OS drop down menu and choose SecurePlatform Pro. You have to reboot the Security Gateway in order for the change to take effect.
- C. Type pro enable on your Security Gateway and reboot it.
- D. You have to re-install your Security Gateway with SecurePlatform ProR76, as SecurePlatformR76 does not support VTIs.

Answer: C

Explanation:

QUESTION NO: 263

Which operating system(s) support(s) unnumbered VPN Tunnel Interfaces (VTIs) for route-based VPN's?

- A. Solaris 9 and higher
- B. IPSO 3.9 and higher
- C. Red Hat Linux
- D. SecurePlatform for NGX and higher

Answer: B

Explanation:

QUESTION NO: 264

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 use the VTI tunnels?

- A. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, remove the Gateways out of the mesh community and replace with a star community
- B. Route-based VTI takes precedence over the Domain VPN. Troubleshoot the static route entries to insure that they are correctly pointing to the VTI gateway IP.
- 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

Explanation:

QUESTION NO: 265

When configuring a Permanent Tunnel between two gateways in a Meshed VPN community, in what object is the tunnel managed?

- A. VPN Community object
- B. Each participating Security Gateway object

- C. Security Management Server
- D. Only the local Security Gateway object

Answer: A

Explanation:

QUESTION NO: 266

Which of the following commands would you run to remove site-to-site IKE and IPSec Keys?

- A. vpn tu
- B. ikeoff
- C. vpn export_p12
- D. vpn accel off

Answer: A

Explanation:

QUESTION NO: 267

Which of the following log files contains information about the negotiation process for encryption?

- A. ike.elg
- B. iked.elg
- C. vpnd.elg
- D. vpn.elg

Answer: A

Explanation:

QUESTION NO: 268

Which of the following log files contains verbose information regarding the negotiation process and other encryption failures?

- A. iked.elg
- B. ike.elg
- C. vpn.elg

D. vpnd.elg

Answer: D

Explanation:

QUESTION NO: 269

What is the most common cause for a Quick mode packet 1 failing with the error "No Proposal Chosen" error?

- A. The OS and patch level of one gateway does not match the other.
- B. The previously established Permanent Tunnel has failed.
- C. There is a network connectivity issue.
- D. The encryption strength and hash settings of one peer does not match the other.

Answer: D

Explanation:

QUESTION NO: 270

Which component receives events and assigns severity levels to the events; invokes any defined automatic reactions, and adds the events to the Events Data Base?

- A. SmartEvent Analysis DataServer
- B. SmartEvent Client
- C. SmartEvent Correlation Unit
- D. SmartEvent Server

Answer: D

Explanation:

QUESTION NO: 271

The _____ contains the Events Data Base.

- A. SmartEvent Client
- B. SmartEvent Correlation Unit
- C. SmartEvent DataServer

D. SmartEvent Server

Answer: D

Explanation:

QUESTION NO: 272

The SmartEvent Correlation Unit:

- A. adds events to the events database.
- B. assigns a severity level to an event.
- C. analyzes each IPS log entry as it enters the Log server.
- D. displays the received events.

Answer: C

Explanation:

QUESTION NO: 273

The SmartEvent Server:

- A. analyzes each IPS log entry as it enters the Log server.
- B. displays the received events.
- C. forwards what is known as an event to the SmartEvent Server.
- D. assigns a severity level to an event.

Answer: D

Explanation:

QUESTION NO: 274

The SmartEvent Client:

- A. analyzes each IPS log entry as it enters the Log server.
- B. displays the received events.
- C. adds events to the events database.
- D. assigns a severity level to an event.

Answer: B

Explanation:

QUESTION NO: 275

The SmartEvent Correlation Unit:

- A. adds events to the events database.
- B. displaya the received events.
- C. looks for patterns according to the installed Event Policy.
- D. assigns a severity level to an event.

Answer: C

Explanation:

QUESTION NO: 276

The SmartEvent Correlation Unit:

- A. adds events to the events database.
- B. assigns a severity level to an event.
- C. forwards what is identified as an event to the SmartEvent server.
- D. displays the received events.

Answer: C

Explanation:

QUESTION NO: 277

The SmartEvent Server:

- A. displays the received events
- B. adds events to the events database
- C. invokes defined automatic reactions
- D. analyzes each IPS log entry as it enters the Log server

Answer: C

Explanation:

QUESTION NO: 278

What are the 3 main components of the SmartEvent Software Blade?

- i) Correlation Unit
- ii) Correlation Client
- iii) Correlation Server
- iv) Analyzer Server
- v) Analyzer Client
- vi) Analyzer Unit

- A. i, ii, iii
- B. iv, v, vi
- C. i, iv, v
- D. i, iii, iv

Answer: C

Explanation:

QUESTION NO: 279

How many Events can be shown at one time in the Event preview pane?

- A. 5,000
- B. 30,000
- C. 15,000
- D. 1,000

Answer: B

Explanation:

QUESTION NO: 280

You are reviewing computer information collected in ClientInfo. You can NOT:

- A. Enter new credential for accessing the computer information.

- B. Save the information in the active tab to an .exe file.
- C. Copy the contents of the selected cells.
- D. Run Google.com search using the contents of the selected cell.

Answer: B

Explanation:

QUESTION NO: 281

Which of the following is NOT a SmartEvent Permission Profile type?

- A. Events Database
- B. View
- C. No Access
- D. Read/Write

Answer: B

Explanation:

QUESTION NO: 282

What is the SmartEvent Correlation Unit's function?

- A. Assign severity levels to events.
- B. Display received threats and tune the Events Policy.
- C. Analyze log entries, looking for Event Policy patterns.
- D. Invoke and define automatic reactions and add events to the database.

Answer: C

Explanation:

QUESTION NO: 283

What is the SmartEvent Analyzer's function?

- A. Assign severity levels to events.
- B. Analyze log entries, looking for Event Policy patterns.
- C. Display received threats and tune the Events Policy.

D. Generate a threat analysis report from the Analyzer database.

Answer: A

Explanation:

QUESTION NO: 284

What is the SmartEvent Client's function?

- A. Display received threats and tune the Events Policy.
- B. Generate a threat analysis report from the Reporter database.
- C. Invoke and define automatic reactions and add events to the database.
- D. Assign severity levels to events.

Answer: A

Explanation:

QUESTION NO: 285

A tracked SmartEvent Candidate in a Candidate Pool becomes an Event. What does NOT happen in the Analyzer Server?

- A. SmartEvent provides the beginning and end time of the Event.
- B. The Correlation Unit keeps adding matching logs to the Event.
- C. The Event is kept open, but condenses many instances into one Event.
- D. SmartEvent stops tracking logs related to the Candidate.

Answer: D

Explanation:

QUESTION NO: 286

How many pre-defined exclusions are included by default in SmartEvent R76 as part of the product installation?

- A. 3
- B. 0
- C. 5

D. 10

Answer: A

Explanation:

QUESTION NO: 287

What is the purpose of the pre-defined exclusions included with SmartEvent R76?

- A. To avoid incorrect event generation by the default IPS event definition; a scenario that may occur in deployments that include Security Gateways of versions prior to R71.
- B. To allow SmartEventR76to function properly with all other R71 devices.
- C. To give samples of how to write your own exclusion.
- D. As a base for starting and building exclusions.

Answer: A

Explanation:

QUESTION NO: 288

What is the benefit to running SmartEvent in Learning Mode?

- A. There is no SmartEvent Learning Mode
- B. To run SmartEvent with preloaded sample data in a test environment
- C. To run SmartEvent, with a step-by-step online configuration guide for training/setup purposes
- D. To generate a report with system Event Policy modification suggestions

Answer: D

Explanation:

QUESTION NO: 289

_____ is NOT an SmartEvent event-triggered Automatic Reaction.

- A. SNMP Trap
- B. Mail
- C. Block Access
- D. External Script

Answer: C

Explanation:

QUESTION NO: 290

For best performance in Event Correlation, you should use:

- A. IP address ranges
- B. Large groups
- C. Nothing slows down Event Correlation
- D. Many objects

Answer: A

Explanation:

QUESTION NO: 291

What access level cannot be assigned to an Administrator in SmartEvent?

- A. No Access
- B. Write only
- C. Read only
- D. Events Database

Answer: B

Explanation:

QUESTION NO: 292

_____ manages Standard Reports and allows the administrator to specify automatic uploads of reports to a central FTP server.

- A. SmartDashboard Log Consolidator
- B. SmartReporter
- C. Security Management Server
- D. SmartReporter Database

Answer: B

Explanation:

QUESTION NO: 293

_____ generates a SmartEvent Report from its SQL database.

- A. SmartEvent Client
- B. Security Management Server
- C. SmartReporter
- D. SmartDashboard Log Consolidator

Answer: C

Explanation:

QUESTION NO: 294

Which SmartReporter report type is generated from the SmartView Monitor history file?

- A. Custom
- B. Express
- C. Traditional
- D. Standard

Answer: B

Explanation:

QUESTION NO: 295

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

- A. SmartReporter Client
- B. Security Management Server
- C. SmartDashboard Log Consolidator
- D. SmartEvent Server

Answer: C

Explanation:

QUESTION NO: 296

Which Check Point product implements a Consolidation Policy?

- A. SmartReporter
- B. SmartView Monitor
- C. SmartLSM
- D. SmartView Tracker

Answer: A

Explanation:

QUESTION NO: 297

You have selected the event Port Scan from Internal Network in SmartEvent, to detect an event when 30 port scans have occurred within 60 seconds. You also want to detect two port scans from a host within 10 seconds of each other. How would you accomplish this?

- A. Define the two port-scan detections as an exception.
- B. Select the two port-scan detections as a new event.
- C. Select the two port-scan detections as a sub-event.
- D. You cannot set SmartEvent to detect two port scans from a host within 10 seconds of each other.

Answer: A

Explanation:

QUESTION NO: 298

When do modifications to the Event Policy take effect?

- A. When saved on the Correlation Units, and pushed as a policy.
- B. As soon as the Policy Tab window is closed.
- C. When saved on the SmartEvent Client, and installed on the SmartEvent Server.
- D. When saved on the SmartEvent Server and installed to the Correlation Units.

Answer: D

Explanation:

QUESTION NO: 299

To back up all events stored in the SmartEvent Server, you should back up the contents of which folder(s)?

- A. \$RTDIR/distrib
- B. \$RTDIR/distrib_db and \$FWDIR/events
- C. \$RTDIR/distrib and \$RTDIR/events_db
- D. \$RTDIR/events_db

Answer: C

Explanation:

QUESTION NO: 300

To clean the system of all events, you should delete the files in which folder(s)?

- A. \$RTDIR/distrib and \$RTDIR/events_db
- B. \$RTDIR/events_db
- C. \$FWDIR/distrib_db and \$FWDIR/events
- D. \$FWDIR/distrib

Answer: A

Explanation:

Topic 4, Volume D

QUESTION NO: 301

What SmartConsole application allows you to change the Log Consolidation Policy?

- A. SmartDashboard
- B. SmartReporter
- C. SmartUpdate
- D. SmartEvent Server

Answer: B

Explanation:

QUESTION NO: 302

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

- A. In SmartView Monitor, under Global Properties > Log and Masters
- B. In SmartReporter, under Express > Network Activity
- C. In SmartDashboard, the SmartView Monitor page in the R76 Security Gateway object
- D. In SmartReporter, under Standard > Custom

Answer: C

Explanation:

QUESTION NO: 303

In a UNIX environment, SmartReporter Data Base settings could be modified in:

- A. \$FWDIR/Eventia/conf/ini.C
- B. \$RTDIR/Database/conf/my.cnf
- C. \$CPDIR/Database/conf/conf.C
- D. \$ERDIR/conf/my.cnf

Answer: B

Explanation:

QUESTION NO: 304

In a Windows environment, SmartReporter Data Base settings could be modified in:

- A. %RTDIR%\Database\conf\my.ini
- B. \$ERDIR/conf/my.cnf
- C. \$CPDIR/Database/conf/conf.C
- D. \$FWDIR/Eventia/conf/ini.C

Answer: A

Explanation:

QUESTION NO: 305

Which specific R76 GUI would you use to view the length of time a TCP connection was open?

- A. SmartView Tracker
- B. SmartView Status
- C. SmartReporter
- D. SmartView Monitor

Answer: A

Explanation:

QUESTION NO: 306

SmartReporter reports can be used to analyze data from a penetration-testing regimen in all of the following examples, EXCEPT:

- A. Possible worm/malware activity.
- B. Analyzing traffic patterns against public resources.
- C. Analyzing access attempts via social-engineering.
- D. Tracking attempted port scans.

Answer: C

Explanation:

QUESTION NO: 307

What is the best tool to produce a report which represents historical system information?

- A. SmartView Tracker
- B. Smartview Monitor
- C. SmartReporter-Standard Reports
- D. SmartReporter-Express Reports

Answer: D

Explanation:

QUESTION NO: 308

If Jack was concerned about the number of log entries he would receive in the SmartReporter system, which policy would he need to modify?

- A. Consolidation Policy
- B. Log Consolidator Policy
- C. Log Sequence Policy
- D. Report Policy

Answer: A

Explanation:

QUESTION NO: 309

Your company has the requirement that SmartEvent reports should show a detailed and accurate view of network activity but also performance should be guaranteed.

Which actions should be taken to achieve that?

- (i) Use same hard driver for database directory, log files and temporary directory
- (ii) Use Consolidation Rules
- (iii) Limit logging to blocked traffic only
- (iv) Using Multiple Database Tables

- A. (i) and (ii)
- B. (ii) and (iv)
- C. (i), (ii) and (iv)
- D. (i), (iii) and (iv)

Answer: B

Explanation:

QUESTION NO: 310

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying our product !

- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

[Guarantee & Policy](#) | [Privacy & Policy](#) | [Terms & Conditions](#)

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © 2004-2015, All Rights Reserved.