Vendor: Check Point

Exam Code: 156-215.75

Exam Name: Check Point Certified Security Administrator R75

Version: DEMO

QUESTION 1
Once installed, the R75 kernel resides directly below which layer of the OSI model?
Note: Application is the top and Physical is the bottom of the IP stack.

A. Network
B. Transport
C. Data Link
D. Session

Answer: A

QUESTION 2
R75's INSPECT Engine inserts itself into the kernel between which two layers of the OSI model?

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

Answer: D

QUESTION 3
What would be the benefit of upgrading from SmartDefense to IPS R75?

A. The SmartDefense is replaced by the technology of IPS-1.
B. The SmartDefense technology expands IPS-1 to IPS R75.
C. Completely rewritten engine provides improved security performance and reporting.
D. There is no difference - IPS R75is the new name.

Answer: C

QUESTION 4
The Security Gateway is installed on SecurePlatform R75. The default port for the Web User Interface is _____.

A. TCP 18211
B. TCP 257
C. TCP 4433
D. TCP 443

Answer: D

QUESTION 5
Your customer wishes to install the SmartConsole on a Windows system. What are the minimum hardware requirements for R75? Give the BEST answer.

A. 500 MB Free disk space and 512 MB RAM
B. 1 GB Free disk space and 512 MB RAM

C. 1 GB Free disk space and 1 GB RAM
D. 512 MB Free disk space and 1 GB RAM

Answer: A

QUESTION 6
Tom has been tasked to install Check Point R75 in a distributed deployment. Before Tom installs
the systems this way, how many machines will he need if he does not include a SmartConsole
machine in his calculations?

A. One machine
B. One machine, but it needs to be installed using SecurePlatform for compatibility purposes
C. Three machines
D. Two machines

Answer: D

QUESTION 7
Over the weekend, an Administrator without access to SmartDashboard installed a new R75
Security Gateway using SecurePlatform. You want to confirm communication between the
Gateway and the Management Server by installing the Security Policy. What might prevent you
from installing the Policy?

A. You first need to initialize SIC in SmartUpdate.
B. You have not established Secure Internal Communications (SIC) between the Security Gateway and
   Management Server. You must initialize SIC on the Security Management Server.
C. You have not established Secure Internal Communications (SIC) between the Security Gateway and
   Management Server. You must initialize SIC on both the Security Gateway and the Management Server.
D. You first need to run the fw unloadlocal command on the new Security Gateway.

Answer: B

QUESTION 8
An Administrator without access to SmartDashboard installed a new IPSO-based R75 Security
Gateway over the weekend. He e-mailed you the SIC activation key. You want to confirm
communication between the Security Gateway and the Management Server by installing the
Policy. What might prevent you from installing the Policy?

A. You first need to create a new Gateway object in SmartDashboard, establish SIC via the Communication
   button, and define the Gateway's topology.
B. You have not established Secure Internal Communications (SIC) between the Security Gateway and
   Management Server You must initialize SIC on the Security Management Server.
C. An intermediate local Security Gateway does not allow a policy install through it to the remote new
   Security Gateway appliance Resolve by running the tw unloadlocal command on the local Security Gateway.
D. You first need to run the fw unloadlocal command on theR75Security Gateway appliance in order to
   remove the restrictive default policy.

Answer: A

QUESTION 9
Which of the following statements regarding SecureXL and CoreXL is TRUE?

A. SecureXL is an application for accelerating connections.
B. CoreXL enables multi-core processing for program interfaces.
C. SecureXL is only available inR75.
D. CoreXL is included in SecureXL.

Answer: A

QUESTION 10
Beginning with R75, Software Blades were introduced. One of the Software Blades is the IPS
Software Blade as a replacement for SmartDefense. When buying or upgrading to a bundle, some
blades are included, e.g. FW, VPN, IPS in SG103. Which statement is NOT true?

A. The license price includes IPS Updates for the first year.
B. The IPS Software Blade can be used for an unlimited time.
C. There is no need to renew the service contract after one year.
D. After one year, it is mandatory to renew the service contract for the IPS Software Blade because it
   has been bundled with the license when purchased.

Answer: D

QUESTION 11
John is the Security Administrator in his company. He needs to maintain the highest level of
security on the firewalls he manages. He is using Check Point R75. Does he need the IPS
Software Blade for achieving this goal?

A. No, all IPS protections are active, but can't be uploaded without the license like SmartDefense.
B. Yes, otherwise no protections can be enabled.
C. Yes, otherwise the firewall will pass all traffic unfiltered and unchecked.
D. No, the Gateway will always be protected and the IPS checks can't be managed without a license.

Answer: B

QUESTION 12
Which command allows you to view the contents of an R75 table?

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

Answer: D

QUESTION 13
Your R75 enterprise Security Management Server is running abnormally on Windows 2003 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) Run the latest upgrade_export utility to export the configuration
   2) Leave the exported - tgz file in %FWDIR\bin.
   3) Install the primary security Management Server on top of the current installation
   4) Run upgrade_import to Import the configuration.
B. 1) Insert theR75CD-ROM. and select the option to export the configuration into a . tgz file
   2) Skip any upgrade 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 theR75CD_ROM to select the upgrade__import option to import the c
C. 1) Download the latest upgrade_export utility and run it from a \ temp directory to export the Configuration.
   2) Perform any requested upgrade verification suggested steps.
   3) Uninstall allR75packages 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) Download the latest upgrade_export utility and run it from a \ temp directory to export the Configuration.
   2) Transferee .tgz file to another network machine
   3) Uninstall allR75packages via Add/Remove Programs and reboot
   4) Install again using theR75CD ROM as a primary security management server
   5) Reboot and than transfer the .tgz file back to the local\ tem p
   6) Run upgcade_import to import the configuration.

Answer: C

QUESTION 14
Your primary Security Management Server runs on SecurePlatform. What is the easiest way to back up your Security Gateway R75 configuration, including routing and network configuration files?

A. Using the upgrade_export command.
B. Copying the $FWDIR/conf and $FWDIR/lib directory to another location.
C. Run the pre_upgrade_verifier and save the .tgz file to the /temp directory.
D. Using the native SecurePlatform backup utility from command line or in the Web based user interface.

Answer: D

QUESTION 15
Your R75 primary Security Management Server is installed on SecurePlatform. You plan to schedule the Security Management Server to run fw logswitch automatically every 48 hours. How do you create this schedule?

A. Create a time object, and add 48 hours as the interval. Open the primary Security Management Server object's Logs and Masters window, enable Schedule log switch, and select the Time object.
B. Create a time object, and add 48 hours as the interval. Open the Security Gateway object's Logs and Masters window, enable Schedule log switch, and select the Time object.
C. Create a time object, and add 48 hours as the interval. Select that time object's Global Properties > Logs and Masters window, to schedule a logswitch.

D. On a SecurePlatform Security Management Server, this can only be accomplished by configuring the fw logswitch command via the cron utility.

Answer: A

QUESTION 16
Which of the following methods will provide the most complete backup of an R75 configuration?

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

Answer: C

QUESTION 17
Which of the following commands can provide the most complete restore of an R75 configuration?

A. Cpconfig
B. Upgrade_import
C. fwm dbimport -p
D. cpinfo -recover

Answer: B

QUESTION 18
When restoring R75 using the command upgrade > Port. Which of the following items is NOT restored?

A. Licenses
B. Global properties
C. SIC Certificates
D. Route tables

Answer: D

QUESTION 19
Your organization's disaster recovery plan needs an update to the backup and restore section to reap the benefits of the new distributed R75 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 R75 components that enforce the Security Polices
should be blocked up at least once a week.
-Desired Objective: Back up R75 logs at least once a week
```

Your disaster recovery plan is as follows:

```
-Use the cron utility to run the upgrade_ export command each night on the
```

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

Upon evaluation, your plan:

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

Answer: D

QUESTION 20
Your company is running Security Management Server R75 on SecurePlatform, which has been
migrated through each version starting from Check Point 4.1. How do you add a new administrator
account?

A. Using SmartDashboard, under Users, select Add New Administrator
B. Using the Web console on SecurePlatform under Product configuration, select Administrators
C. Using SmartDashboard or cpconf ig
D. Using cpconftg on the Security Management Server, choose Administrators

Answer: A