Checkpoint

Exam 156-215.71

Check Point Certified Security Administrator R71

Version: 14.1

[Total Questions: 465]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	100
Topic 4: Volume D	100
Topic 5: Volume E	65

Topic 1, Volume A

Question No : 1 - (Topic 1)

Which of the following commands identifies whether or not a Security Policy is installed or the Security Gateway is operating with the initial policy?

A. fw monitor
B. fw ctl pstat
C. cp stat
D. fw stat

Answer: D

Question No : 2 - (Topic 1)

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

Answer: C

Question No : 3 - (Topic 1)

You need to plan the company's new security system. The company needs a very high level of security and also high performance and high throughput for their applications. You need to turn on most of the integrated IPS checks while maintaining high throughput. What would be the BEST solution for this scenario?

A. You need to buy a strong multi-core machine and run R70 or later on SecurePlatform

with CoreXL technology enabled.
B. Bad luck, both together can not be achieved.
C. The IPS does not run when CoreXL is enabled.
D. The IPS system does not affect the firewall performance and CoreXL is not needed in this scenario.

Answer: A

Question No : 4 - (Topic 1)

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

A. fw delete all.all@localhost
B. cpstop
C. fw unloadlocal
D. fw unload policy

Answer: C

Question No : 5 - (Topic 1)

Of the three mechanisms Check Point uses for controlling traffic, which enables firewalls to incorporate layer 4 awareness in packet inspection?

A. IPS
B. Packet filtering
C. Stateful Inspection
D. Application Intelligence

Answer: C

Question No : 6 - (Topic 1)

John currently administers a network using single CPU single core servers for the Security Gateways and is running R71. His company is now going to implement VOIP and needs more performance on the Gateways. He is now adding more memory to the systems and also upgrades the CPU to a modern quad core CPU in the server. He wants to use CoreXL

technology to benefit from the new performance benchmarks of this technology. How can he achieve this?

A. Nothing needs to be done. SecurePlatform recognized the change during reboot and adjusted all the settings automatically.
B. He just needs to go to cpconfig on the CLI and enable CoreXL. Only a restart of the firewall is required to benefit from CoreXL technology.
C. He needs to reinstall the Gateways because during the initial installation, it was a single-core CPU but the wrong Linux kernel was installed. There is no other upgrade path available.
D. He just needs to go to cpconfig on the CLI and enable CoreXL. After the required reboot he will benefit from the new technology.

Answer: D

Question No : 7 - (Topic 1)

You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the authentication credentials. What must happen after authentication that allows the client to connect to the Security Gateway's VPN domain?

A. Active-X must be allowed on the client.
B. An office mode address must be obtained by the client.
C. SNX modifies the routing table to forward VPN traffic to the Security Gateway.
D. The SNX client application must be installed on the client.

Answer: C

Question No : 8 - (Topic 1)

Your R71 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 No : 9 - (Topic 1)

Your organization's disaster recovery plan needs an update to the backup and restore section to reap the benefits of the new distributed R71 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 R71 components that enforce the Security Polices should be blocked up at least once a week.

Desired Objective: Back up R71 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

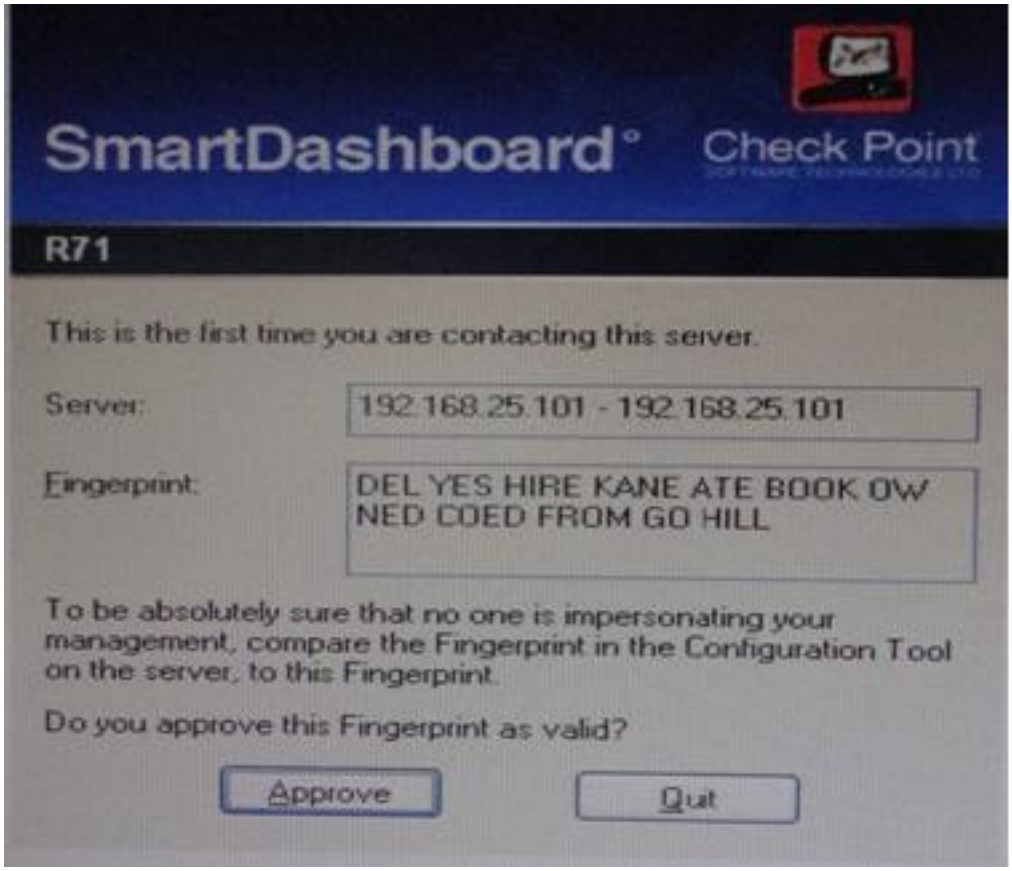
Upon evaluation, your plan:

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 No : 10 - (Topic 1)

From the output below, where is this fingerprint generated?



A. SmartUpdate
B. Security Management Server
C. SmartDashboard
D. SmartConsole

Answer: B

Question No : 11 - (Topic 1)

Which of the following statements is TRUE about management plug-ins?

A. The plug-in is a package installed on the Security Gateway.
B. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
C. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.
D. Installing a management plug-in is just like an upgrade process. (It overwrites existing components.)

Answer: B

Question No : 12 - (Topic 1)

The Internal Certificate Authority (ICA) CANNOT be used for:

A. Virtual Private Network (VPN) Certificates for gateways
B. NAT rules
C. Remote-access users
D. SIC connections

Answer: B

Question No : 13 - (Topic 1)

Your customer wishes to install the SmartConsole on a Windows system. What are the minimum hardware requirements for R71? 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 No : 14 - (Topic 1)

Several Security Policies can be used for different installation targets. The Firewall protecting Human Resources' servers should have its own Policy Package. These rules must be installed on this machine and not on the Internet Firewall. How can this be accomplished?

A. A Rule Base can always be installed on any Check Point Firewall object. It is necessary to select the appropriate target directly after selecting Policy / Install on Target.
B. A Rule Base is always installed on all possible targets. The rules to be installed on a Firewall are defined by the selection in the row Install On of the Rule Base.
C. In the menu of SmartDashboard, go to Policy / Policy Installation Targets and select the correct firewall via Specific Targets.
D. When selecting the correct Firewall in each line of the row Install On of the Rule Base, only this Firewall is shown in the list of possible installation targets after selecting Policy / Install on Target.

Answer: C

Question No : 15 - (Topic 1)

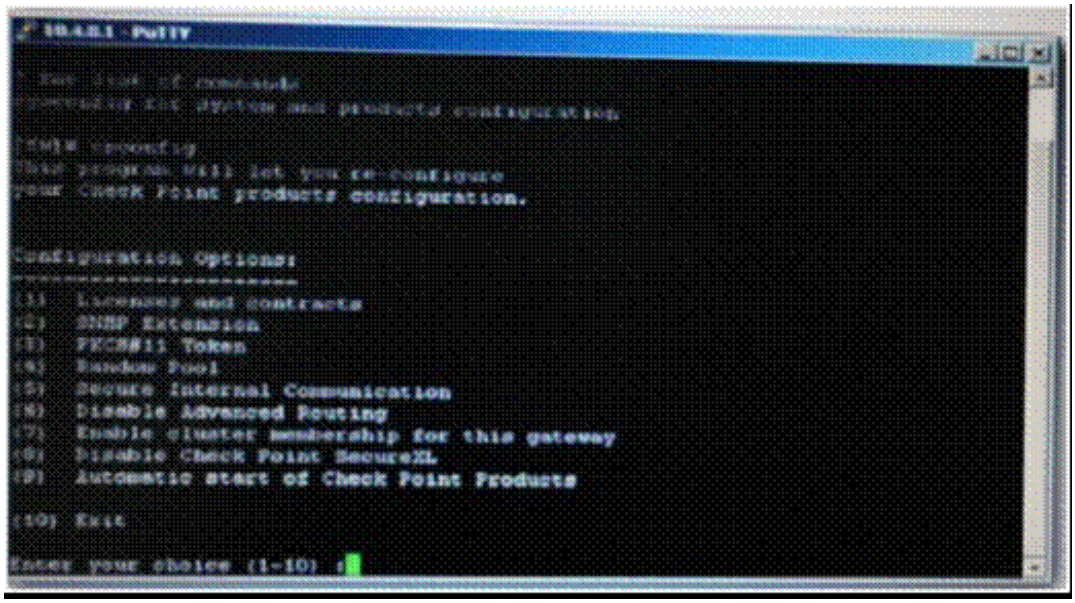
Which command line interface utility allows the administrator to verify the name and timestamp of the Security Policy currently installed on a firewall module?

A. fw ctl pstat
B. fw stat
C. cpstat fwd
D. fw ver

Answer: B

Question No : 16 - (Topic 1)

What information is provided from the options in this screenshot?



(i)Whether a SIC certificate was generated for the Gateway

(ii)Whether the operating system is SecurePlatform or SecurePlatform Pro

(iii)Whether this is a standalone or distributed installation

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

Answer: D

Question No : 17 - (Topic 1)

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 problem 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 can be done easily by the command restore and selecting the appropriate backup file.
B. A backup cannot be restored, because the binary files are missing.