

Checkpoint

Exam 156-215-75

Check Point Certified Security Administrator R75

Version: 6.7

[Total Questions: 543]

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	143

Topic 1, Volume A**Question No : 1 - (Topic 1)**

Which CLI command verifies the number of cores on your firewall machine?

- A. fw ctl pstat
- B. fw ctl core stat
- C. fw ctl multik stat
- D. cpstat fw -f core

Answer: C

Question No : 2 - (Topic 1)

What is the command used to view which policy is installed?

- A. fw ctl install
- B. fwm stat
- C. fw ctl pstat
- D. fw stat

Answer: D

Question No : 3 - (Topic 1)

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 No : 4 - (Topic 1)

In previous versions, the full TCP three-way handshake was sent to the firewall kernel for inspection. How is this improved in the current version of IPSO Flows/SecureXL?

- A. Only the initial SYN packet is inspected. The rest are handled by IPSO.
- B. Packets are offloaded to a third-party hardware card for near-line inspection.
- C. Packets are virtualized to a RAM drive-based FW VM.
- D. Resources are proactively assigned using predictive algorithmic techniques.

Answer: A

Question No : 5 - (Topic 1)

A Web server behind the Security Gateway is set to Automatic Static NAT. Client side NAT is enabled in the Global Properties. A client on the Internet initiates a session to the Web Server. On the initiating packet, NAT occurs on which inspection point?

- A. I
- B. O
- C. o
- D. i

Answer: A

Question No : 6 - (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 : 7 - (Topic 1)

Where is the IPSO Boot Manager physically located on an IP Appliance?

- A. In the / nvram directory
- B. On an external jump drive
- C. On the platform's BIOS
- D. On built-in compact Flash memory

Answer: D

Question No : 8 - (Topic 1)

You need to back up the routing, interface, and DNS configuration information from your R75 SecurePlatform Security Gateway. Which backup-and-restore solution do you use?

- A. SecurePlatform backup utilities
- B. upgrade_export and upgrade_import commands
- C. Database Revision Control
- D. Manual copies of the \$FWDIR/conf directory

Answer: A

Question No : 9 - (Topic 1)

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 No : 10 - (Topic 1)

You issue the fw monitor command with no arguments. Which of the following inspection points will be displayed?

- A. Before the virtual machine, in the inbound direction
- B. After the virtual machine, in the outbound direction
- C. All inspection points
- D. Before the virtual machine, in the outbound direction

Answer: C

Question No : 11 - (Topic 1)

You are a security architect and need to design a secure firewall, VPN and IPS solution. Where would be the best place to install IPS in the topology if the internal network is already protected?

- A. On the firewall itself to protect all connected networks centrally.
- B. On each network segment separately.
- C. On the LAN is enough, the DMZ does not need to be protected.
- D. In front of the firewall is enough.

Answer: A

Question No : 12 - (Topic 1)

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

- A. Run the command `fwm sic-reset` to initialize the Internal Certificate Authority (ICA) of the Security Management Server. Then retype the activation key on the Security Gateway from SmartDashboard.
- B. Use SmartDashboard to retype the activation key on the Security Gateway. This will automatically Sync SIC to both the Security Management Server and Gateway.
- C. From `cpconfig` on the Gateway, choose the Secure Internal Communication option and retype the activation key. Next, retype the same key in the Gateway object in SmartDashboard and reinitialize Secure Internal Communications (SIC).
- D. From the Security Management Server's command line, Type `fw putkey -p <shared key> < IP Address of security Gateway>`.

Answer: C

Question No : 13 - (Topic 1)

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

- A. sysconfig
- B. dhcp_cfg
- C. cpconfig
- D. ifconfig

Answer: A

Question No : 14 - (Topic 1)

Which operating systems are supported by a Check Point Security Gateway on an open server?

- A. Check Point SecurePlatform and Microsoft Windows
- B. Sun Solaris, Red Hat Enterprise Linux, Check Point SecurePlatform, IPSO, Microsoft Windows
- C. Check Point SecurePlatform, IPSO, Sun Solaris, Microsoft Windows
- D. Microsoft Windows, Red Hat Enterprise Linux, Sun Solaris, IPSO

Answer: A

Question No : 15 - (Topic 1)

Which of the following statements accurately describes the snapshot command?

- A. snapshot creates a full OS-level backup, including network-interface data, Check Point product information, and configuration settings during an upgrade of a SecurePlatform Security Gateway.
- B. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server.
- C. snapshot creates a full system-level backup of the Security Management Server on any OS
- D. snapshot stores only the system-configuration settings on the Gateway.

Answer: A

Question No : 16 - (Topic 1)

Which command displays the installed Security Gateway version?

- A. fw stat
- B. cpstat -gw
- C. fw ver
- D. tw printver

Answer: C

Question No : 17 - (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 : 18 - (Topic 1)

The customer has a small Check Point installation which includes one Windows 2003 server as SmartConsole and Security Management Server with a second server running SecurePlatform as Security Gateway. This is an example of a(n):

- A. Hybrid Installation.
- B. Unsupported configuration.
- C. Distributed Installation.

D. Stand-Alone Installation.

Answer: C

Question No : 19 - (Topic 1)

You are consulting with an Administrator who has locked himself out of SmartDashboard installed on a standalone SecurePlatform Security Gateway. Now, he cannot access the Security Management Server via SmartDashboard or any other SmartConsole tools. How can you get him reconnected to SmartDashboard?

- A. Run fw uninstall localhost on the Security Gateway.
- B. Run fw unloadlocal on the Security Gateway.
- C. Run fw unlocklocal on the Security Management Server.
- D. Delete the \$fwdir/database/manage.lock file and run cprestart.

Answer: B

Question No : 20 - (Topic 1)

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

- A. WebUI
- B. Eventia Reporter
- C. SmartView Monitor
- D. SmartView Tracker

Answer: D

Question No : 21 - (Topic 1)

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 No : 22 - (Topic 1)

Which of the following tools is used to generate a Security Gateway R75 configuration report?

- A. ethereal
- B. cpinfo
- C. licview
- D. infoview

Answer: B

Question No : 23 - (Topic 1)

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 the R75 CD-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 the R75 CD_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.