

Checkpoint

Exam 156-915.77

Check Point Certified Security Expert Update

Version: 7.0

[Total Questions: 203]

Topic break down

Topic	No. of Questions
Topic 1: Deployment Platforms Obj 1	15
Topic 2: Deployment Platforms Obj 2	16
Topic 3: Deployment Platforms Obj 3	11
Topic 4: Network Address Translation	23
Topic 5: User Managment and Authentication Obj 1	12
Topic 6: User Managment and Authentication Obj 2	6
Topic 7: Identity Awareness Obj 1	7
Topic 8: Identity Awareness Obj 2	6
Topic 9: Identity Awareness Obj 3	4
Topic 10: Identity Awareness Obj 4	14
Topic 11: Advanced Firewall	9
Topic 12: Advanced upgrading	13
Topic 13: Advanced User Management	15
Topic 14: Advanced Clustering and Acceleration	27
Topic 15: IPSEC VPN and Remote Access	14
Topic 16: SmartReporting and SmartEvent	11

Topic 1, Deployment Platforms Obj 1**Question No : 1 - (Topic 1)**

You are running a R77 Security Gateway on GAIa. In case of a hardware failure, you have a server with the exact same hardware and firewall version installed. What back up method could be used to quickly put the secondary firewall into production?

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

Answer: D

Question No : 2 - (Topic 1)

Which operating systems are supported by a Check Point Security Gateway on an open server? Select MOST complete list.

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

Answer: B

Question No : 3 - (Topic 1)

What is the syntax for uninstalling a package using newpkg?

- A. -u <pathname of package>
- B. -i <full pathname of package>
- C. -S <pathname of package>
- D. newpkg CANNOT be used to uninstall a package

Answer: D

Question No : 4 - (Topic 1)

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

- A. `upgrade_export` stores network-configuration data, objects, global properties, and the database revisions prior to upgrading the Security Management Server.
- B. Used primarily when upgrading the Security Management Server, `upgrade_export` stores all object databases and the `/conf` directories for importing to a newer Security Gateway version.
- C. `upgrade_export` is used when upgrading the Security Gateway, and allows certain files to be included or excluded before exporting.
- D. This command is no longer supported in GAIa.

Answer: B

Question No : 5 - (Topic 1)

Before upgrading SecurePlatform to GAIa, 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 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 boot menu of GAIa.
- C. The restore can be done easily by the command `restore` and copying `netconf.C` from the production environment.
- D. A backup cannot be restored, because the binary files are missing.

Answer: C

Question No : 6 - (Topic 1)

Suppose the Security Gateway hard drive fails and you are forced to rebuild it. You have a snapshot file stored to a TFTP server and backups of your Security Management Server. What is the correct procedure for rebuilding the Gateway quickly?

- A. Reinstall the base operating system (i.e., GAIa). Configure the Gateway interface so

that the Gateway can communicate with the TFTP server. Revert to the stored snapshot image, and install the Security Policy.

B. Run the command revert to restore the snapshot, establish SIC, and install the Policy.

C. Run the command revert to restore the snapshot. Reinstall any necessary Check Point products. Establish SIC and install the Policy.

D. Reinstall the base operating system (i.e., GAIa). Configure the Gateway interface so that the Gateway can communicate with the TFTP server. Reinstall any necessary Check Point products and previously applied hotfixes. Revert to the stored snapshot image, and install the Policy.

Answer: A

Question No : 7 - (Topic 1)

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

A. `upgrade_export` is operating system independent and can be used when `backup` or `snapshot` is not available.

B. `upgrade_export` will back up routing tables, hosts files, and manual ARP configurations, where `backup` and `snapshot` will not.

C. The commands `backup` and `snapshot` can take a long time to run whereas `upgrade_export` will take a much shorter amount of time.

D. `upgrade_export` has an option to back up the system and SmartView Tracker logs while `backup` and `snapshot` will not.

Answer: A

Question No : 8 - (Topic 1)

You need to back up the routing, interface, and DNS configuration information from your R77 GAIa Security Gateway. Which backup-and-restore solution do you use?

A. Manual copies of the directory `$FWDIR/conf`

B. GAIa back up utilities

C. `upgrade_export` and `upgrade_import` commands

D. Database Revision Control

Answer: B

Question No : 9 - (Topic 1)

Match the following commands to their correct function.

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

Each command has one function only listed.

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

Answer: A

Question No : 10 - (Topic 1)

Which command displays the installed Security Gateway version?

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

Answer: B

Question No : 11 - (Topic 1)

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

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

Answer: C

Question No : 12 - (Topic 1)

You intend to upgrade a Check Point Gateway from R71 to R77. Prior to upgrading, you want to back up the Gateway should there be any problems with the upgrade. Which of the following allows for the Gateway configuration to be completely backed up into a manageable size in the least amount of time?

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

Answer: D

Question No : 13 - (Topic 1)

A snapshot delivers a complete GAIa backup. 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. 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.
- B. As expert user, type the command snapshot -r MySnapshot.tgz.
- C. As expert user, type the command revert --file MySnapshot.tgz.
- D. As expert user, type the command snapshot - R to restore from a local file. Then, provide the correct file name.

Answer: C

Question No : 14 - (Topic 1)

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

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

Answer: C

Question No : 15 - (Topic 1)

Your primary Security Gateway runs on GAIa. What is the easiest way to back up your Security Gateway R77 configuration, including routing and network configuration files?

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

Answer: B

Topic 2, Deployment Platforms Obj 2

Question No : 16 - (Topic 2)

Your organization's disaster recovery plan needs an update to the backup and restore section to reap the new distributed R77 installation benefits. 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 R77 components that enforce the Security Policies should be backed up at least once a week.

Desired Objective: Back up R77 logs at least once a week.

Your disaster recovery plan is as follows:

- Use the cron utility 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 GAIa back up utility to back up the Security Gateways every Saturday night.
- Use the cron utility 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 but does not meet either desired objective.
- C.** Does not meet the required objective.
- D.** Meets the required objective and both desired objectives.

Answer: D

Question No : 17 - (Topic 2)

Peter is your new Security Administrator. On his first working day, he is very nervous and enters the wrong password three times. His account is locked. What can be done to unlock Peter's account? Give the BEST answer.

- A.** You can unlock Peter's account by using the command `fwm lock_admin -u Peter` on the Security Management Server.
- B.** You can unlock Peter's account by using the command `fwm unlock_admin -u Peter` on the Security Management Server
- C.** It is not possible to unlock Peter's account. You have to install the firewall once again or abstain from Peter's help.
- D.** You can unlock Peter's account by using the command `fwm unlock_admin -u Peter` on the Security Gateway.

Answer: A

Question No : 18 - (Topic 2)

Which of the following commands can provide the most complete restoration of a R77 configuration?

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

Answer: A

Question No : 19 - (Topic 2)

The third-shift Administrator was updating Security Management Server access settings in Global Properties and testing. He managed to lock himself out of his account. How can you unlock this account?

- A. Type fwm unlock_admin from the Security Management Server command line.
- B. Type fwm unlock_admin -u from the Security Gateway command line.
- C. Type fwm lock_admin -u <account name> from the Security Management Server command line.
- D. Delete the file admin.lock in the Security Management Server directory \$FWDIR/tmp/.

Answer: C

Question No : 20 - (Topic 2)

What is the officially accepted diagnostic tool for IP Appliance Support?

- A. ipsoinfo
- B. CST
- C. uag-diag
- D. cpinfo

Answer: B

Question No : 21 - (Topic 2)