Checkpoint

Exam 156-215.13

Check Point Certified Security Administrator – GAiA

Version: 6.2

[Total Questions: 358]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	158

Topic 1, Volume A

Question No : 1 - (Topic 1)

UDP packets are delivered if they are _____.

A. referenced in the SAM related dynamic tables
B. a valid response to an allowed request on the inverse UDP ports and IP
C. a stateful ACK to a valid SYN-SYN/ACK on the inverse UDP ports and IP
D. bypassing the kernel by the forwarding layer of ClusterXL

Answer: B

Question No : 2 - (Topic 1)

The _____ and _____ Rules are the two basic rules which should be used by all Security Administrators?

A. Cleanup; Stealth
B. Administrator Access; Stealth
C. Cleanup; Administrator Access
D. Network Traffic; Stealth

Answer: A

Question No : 3 - (Topic 1)

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

A. GAiA back up utilities
B. upgrade_export and upgrade_import commands
C. Database Revision Control
D. Manual copies of the directory $FWDIR/conf

Answer: A

Question No : 4 - (Topic 1)

Anti-Spoofing is typically set up on which object type?

A. Network
B. Security Management object
C. Host
D. Security Gateway

Answer: D

Question No : 5 - (Topic 1)

You run cpconfig to reset SIC on the Security Gateway. After the SIC reset operation is complete, the policy that will be installed is the:

A. Default filter.
B. Last policy that was installed.
C. Standard policy.
D. Initial policy.

Answer: D

Question No : 6 - (Topic 1)

You are the Security Administrator for MegaCorp. A Check Point firewall is installed and in use on a platform using GAiA. You have trouble configuring the speed and duplex settings of your Ethernet interfaces. Which of the following commands can be used in Expert Mode to configure the speed and duplex settings of an Ethernet interface and will survive a reboot? Give the BEST answer.

A. eth_set
B. mii_tool
C. ifconfig -a
D. ethtool

Answer: A

Question No : 7 - (Topic 1)

The third-shift Administrator was updating Security Management Server access settings in Global Properties. He managed to lock all administrators out of their accounts. How should you unlock these accounts?

A. Reinstall the Security Management Server and restore using upgrade_import.
B. Delete the file admin.lock in the Security Management Server directory $FWDIR/tmp/.
C. Type fwm lock_admin -ua from the Security Management Server command line.
D. Login to SmartDashboard as the special cpconfig_admin user account; right-click on each administrator object and select unlock.

Answer: C

Question No : 8 - (Topic 1)

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

Answer: C

Question No : 9 - (Topic 1)

You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

A. SmartLSM and SmartUpdate
B. SmartView Tracker and SmartView Monitor
C. SmartView Monitor and SmartUpdate
D. SmartDashboard and SmartView Tracker

Answer: D

Question No : 10 - (Topic 1)

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

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

Answer: D

Question No : 11 - (Topic 1)

Which command enables IP forwarding on IPSO?

A. echo 1 > /proc/sys/net/ipv4/ip_forward
B. ipsofwd on admin
C. echo 0 > /proc/sys/net/ipv4/ip_forward
D. clish -c set routing active enable

Answer: B

Question No : 12 - (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 is done by selecting Snapshot Management from the boot menu of GAiA.
B. A backup cannot be restored, because the binary files are missing.
C. The restore can be done easily by the command restore and selecting the file netconf.C.
D. The restore is not possible because the backup file does not have the same build number (version).

Answer: C

Question No : 13 - (Topic 1)

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

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

Answer: A

Question No : 14 - (Topic 1)

Which command would provide the most comprehensive diagnostic information to Check Point Technical Support?

A. cpstat - date.cpstat.txt
B. fw cpinfo
C. cpinfo -o date.cpinfo.txt
D. diag

Answer: C

Question No : 15 - (Topic 1)

Which SmartConsole component can Administrators use to track changes to the Rule Base?

A. SmartView Monitor
B. SmartReporter
C. WebUI
D. SmartView Tracker

Answer: D

Question No : 16 - (Topic 1)

Tom has been tasked to install Check Point R76 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. Three machines
B. One machine
C. One machine, but it needs to be installed using SecurePlatform for compatibility purposes
D. Two machines

Answer: D

Question No : 17 - (Topic 1)

Your organization's disaster recovery plan needs an update to the backup and restore section to reap the new distributed R76 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 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 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. Meets the required objective and both desired objectives.
D. Does not meet the required objective.

Answer: C

Question No : 18 - (Topic 1)

Spoofing is a method of:

A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
B. Making packets appear as if they come from an authorized IP address.
C. Detecting people using false or wrong authentication logins.
D. Hiding your firewall from unauthorized users.

Answer: B

Question No : 19 - (Topic 1)

The SIC certificate is stored in the directory _____.

A. $CPDIR/conf
B. $FWDIR/database
C. $CPDIR/registry
D. $FWDIR/conf

Answer: A

Question No : 20 - (Topic 1)

You have installed a R76 Security Gateway on GAiA. To manage the Gateway from the enterprise Security Management Server, you create a new Gateway object and Security Policy. When you install the new Policy from the Policy menu, the Gateway object does not appear in the Install Policy window as a target. What is the problem?

A. The new Gateway's temporary license has expired.
B. The object was created with Node > Gateway.
C. The Gateway object is not specified in the first policy rule column Install On.
D. No Masters file is created for the new Gateway.

Answer: B

Question No : 21 - (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. The SNX client application must be installed on the client.
C. SNX modifies the routing table to forward VPN traffic to the Security Gateway.
D. An office mode address must be obtained by the client.

Answer: C

Question No : 22 - (Topic 1)

You intend to upgrade a Check Point Gateway from R71 to R76. Prior to upgrading, you want to back up the Gateway should there be any problems with the upgrade. Which of the