Checkpoint

Exam 156-215.75

Check Point Certified Security Administrator R75

Version: 6.9

[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)

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 : 2 - (Topic 1)

Which of the following commands can provide the most complete restoration of an R75 configuration?

A. Cpconfig
B. Upgrade_import
C. fwm dbimport –p <export file>
D. cpinfo –recover

Answer: B

Question No : 3 - (Topic 1)

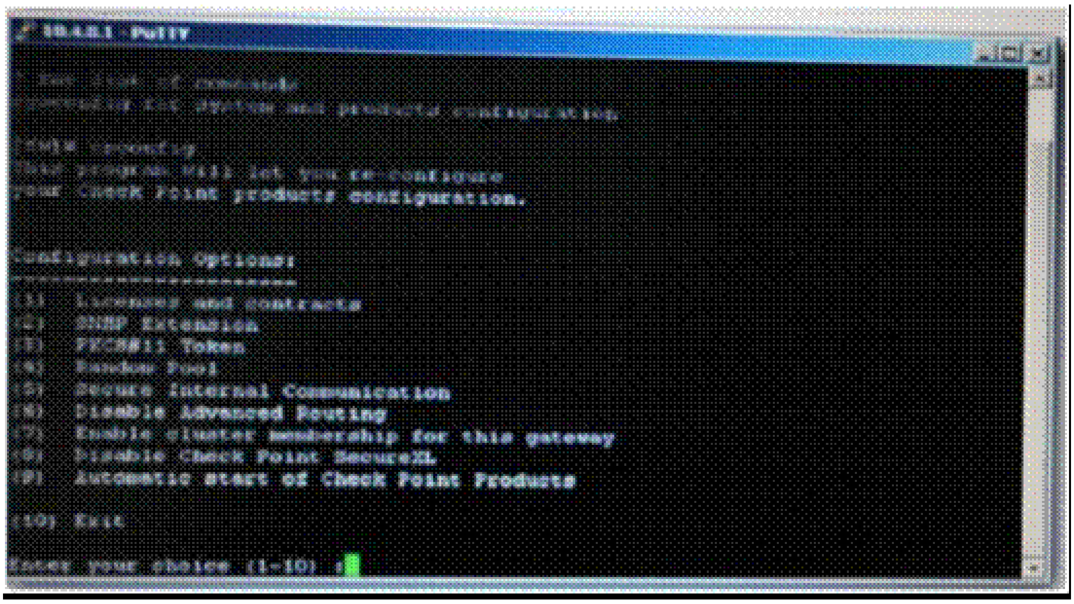
The Security Gateway is installed on SecurePlatform R75. The default port for the Web User Interface is _______.

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

Answer: D

Question No : 4 - (Topic 1)

What information is provided from the options in this screenshot?



```
[illegible]
[illegible] the system and products configuration

cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1)  Licenses and contracts
(2)  SNMP Extension
(3)  PKCS#11 Token
(4)  Random Pool
(5)  Secure Internal Communication
(6)  Disable Advanced Routing
(7)  Enable cluster membership for this gateway
(8)  Disable Check Point SecureXL
(9)  Automatic start of Check Point Products

(10) Exit

Enter your choice (1-10) :
```

(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 : 5 - (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 : 6 - (Topic 1)

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 the R75 Security Gateway appliance in order to remove the restrictive default policy.

Answer: A

Question No : 7 - (Topic 1)

During which step in the installation process is it necessary to note the fingerprint for first-time verification?

A. When establishing SIC between the Security Management Server and the Gateway
B. When configuring the Security Management Server using cpconfig
C. When configuring the Security Gateway object in SmartDashboard
D. When configuring the Gateway in the WebUI

Answer: B

Question No : 8 - (Topic 1)

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 No : 9 - (Topic 1)

You are creating an output file with the following command:

fw monitor -e "accept (src=10.20.30.40 or dst=10.20.30.40);" -o ~/output

Which tool do you use to analyze this file?

A. You can analyze it with Wireshark or Ethereal.
B. You can analyze the output file with any ASCI editor.
C. The output file format is CSV, so you can use MS Excel to analyze it.
D. You cannot analyze it with any tool as the syntax should be:fw monitor -e accept ([12,b]=10.20.30.40 or [16,b]=10.20.30.40); -o ~/output.

Answer: A

Question No : 10 - (Topic 1)

What are you required to do before running upgrade__ export?

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

Answer: D

Question No : 11 - (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 : 12 - (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 : 13 - (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 : 14 - (Topic 1)

Select the correct statement about Secure Internal Communications (SIC) Certificates. SIC Certificates are created:

A. And used for securing internal network communications between SmartView Tracker and an OPSEC device.
B. For the Security Management Server during the Security Management Server installation.
C. For Security Gateways during the Security Gateway installation.
D. To decrease network security by securing administrative communication among the Security Management Servers and the Security Gateway.

Answer: B

Question No : 15 - (Topic 1)

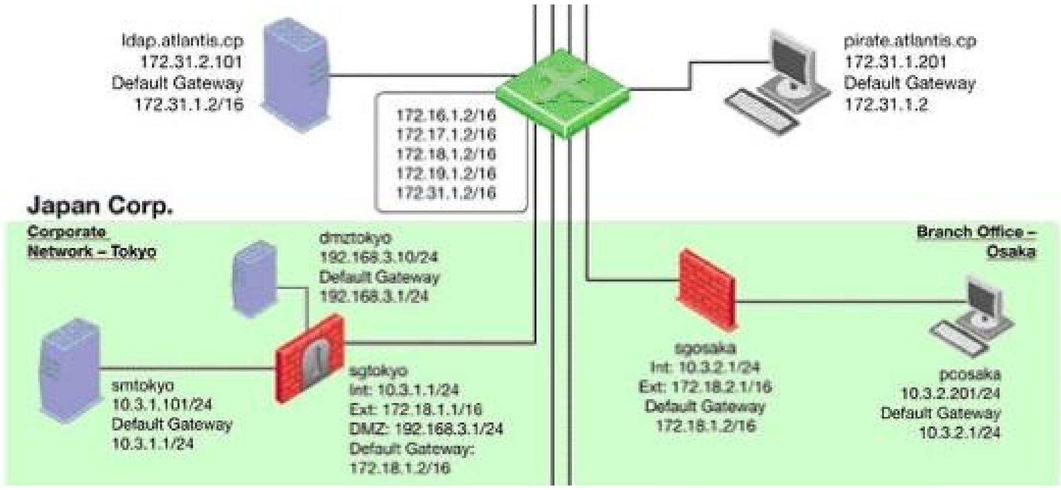
Which utility allows you to configure the DHCP service on SecurePlatform from the command line?

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

Answer: A

Question No : 16 - (Topic 1)

The Administrator of the Tokyo Security Management Server cannot connect from his workstation in Osaka. Which of the following lists the BEST sequence of steps to troubleshoot this issue?



A. Check for matching OS and product versions of the Security Management Server and the client. Then, ping the Gateways to verify connectivity. If successful, scan the log files for any denied management packets.
B. Call Tokyo to check if they can ping the Security Management Server locally. If so, login to sgtokyo, verify management connectivity and Rule Base. If this looks okay, ask your provider if they have some firewall rules that filters out your management traffic.
C. Verify basic network connectivity to the local Gateway, service provider, remote Gateway, remote network and target machine. Then, test for firewall rules that deny management access to the target. If successful, verify that pcosaka is a valid client IP address.
D. Check the allowed clients and users on the Security Management Server. If pcosaka and your user account are valid, check for network problems. If there are no network related issues, this is likely to be a problem with the server itself. Check for any patches and upgrades. If still unsuccessful, open a case with Technical Support.

Answer: C

Question No : 17 - (Topic 1)

Which utility is necessary for reestablishing SIC?

A. fwm sic_reset
B. cpconfig
C. cplic
D. sysconfig

Answer: B

Question No : 18 - (Topic 1)

How can you reset the password of the Security Administrator that was created during initial installation of the Security Management Server on SecurePlatform?

A. Type cpm -a, and provide the existing administrator's account name. Reset the Security Administrator's password.
B. Export the user database into an ASCII file with fwm dbexport. Open this file with an editor, and delete the "Password" portion of the file. Then log in to the account without a password. You will be prompted to assign a new password.
C. Launch SmartDashboard in the User Management screen, and edit the cpconfig administrator.
D. Type fwm -a, and provide the existing administrator's account name. Reset the Security Administrator's password

Answer: D

Question No : 19 - (Topic 1)

UDP packets are delivered if they are _________.

A. A legal response to an allowed request on the inverse UDP ports and IP
B. A Stateful ACK to a valid SYN-SYN-/ACK on the inverse UDP ports and IP
C. Reference in the SAM related Dynamic tables
D. Bypassing the Kernel by the “forwarding layer” of clusterXL

Answer: A

Question No : 20 - (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