TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **156-215.75**

Title : Check Point Certified Security Administrator R75

Version : DEMO

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

2.Which of the following statements about Bridge mode is TRUE.?
A. When managing a Security Gateway in Bridge mode, it is possible to use a bridge interface for Network Address Translation.
B. Assuming a new installation, bridge mode requires changing the existing IP routing of the network.
C. All ClusterXL modes are supported.
D. A bridge must be configured with a pair of interfaces.
Answer: D

3.Which SmartConsole component can Administrators use to track remote administrative activities?
A. WebUI
B. Eventia Reporter
C. SmartView Monitor
D. SmartView Tracker
Answer: D

4.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

5.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

6.The Check Point Security Gateway's virtual machine (kernel) exists between which two layers of the OSI model?
A. Session and Network layers
B. Application and Presentation layers
C. Physical and Datalink layers

D. Network and Datalink layers
Answer: D

7.The customer has a small Check Point installation, which includes one Linux Enterprise 3.0 server working as the SmartConsole, and a second server running Windows 2003 as both Security Management Server running Windows 2003 as both Security Management Server and Security Gateway. This is an example of a(n).
A. Stand-Alone Installation
B. Distributed Installation
C. Hybrid Installation
D. Unsupported configuration
Answer: D

8.The customer has a small Check Point installation which includes one Windows 2003 server as the SmartConsole and a second server running SecurePlatform as both Security Management Server and the Security Gateway. This is an example of a(n):
A. Unsupported configuration.
B. Hybrid Installation.
C. Distributed Installation.
D. Stand-Alone Installation.
Answer: D

9.The customer has a small Check Point installation which includes one Windows XP workstation as the SmartConsole, one Solaris server working as Security Management Server, and a third server running SecurePlatform as Security Gateway. This is an example of a(n):
A. Stand-Alone Installation.
B. Unsupported configuration
C. Distributed Installation.
D. Hybrid Installation.
Answer: C

10.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

11.When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?
A. SecureClient
B. Security Gateway

C. SmartConsole
D. None, Security Management Server would be installed by itself
Answer: B

12.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

13.You are installing a Security Management Server. Your security plan calls for three administrators for this particular server. How many can you create during installation?
A. Depends on the license installed on the Security Management Server
B. Only one with full access and one with read-only access
C. One
D. As many as you want
Answer: C

14.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

15.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: D

16.How can you recreate the account of the Security Administrator, which was created during initial installation of the Management Server on SecurePlatform?
A. Launch cpconfig and delete the Administrator's account. Recreate the account with the same name.

B. Export the user database into an ASCII file with fwm dbexport. Open this file with an editor, and delete the Administrator Account portion of the file. You will be prompted to create a new account.
C. Type cpm -a, and provide the existing Administrator's account name. Reset the Security Administrator's password.
D. Launch SmartDashboard in the User Management screen, and delete the cpconfig administrator.
Answer: A

17.You are running the Security Gateway on SecurePlatform and configure SNX with default settings. The client fails to connect to the Security Gateway. What is wrong?
A. The routing table on the client does not get modified.
B. The client has Active-X blocked.
C. The client is configured incorrectly.
D. The SecurePlatform Web User Interface is listening on port 443.
Answer: D

18.When Jon first installed the system, he forgot to configure DNS servers on his Security Gateway. How could Jon configure DNS servers now that his Security Gateway is in production?
A. Login to the firewall using SSH and run cpconfig, then select Domain Name Servers.
B. Login to the firewall using SSH and run fwm, then select System Configuration and Domain Name Servers.
C. Login to the SmartDashboard, edit the firewall Gateway object, select the tab Interfaces, then Domain Name Servers.
D. Login to the firewall using SSH and run sysconfig, then select Domain Name Servers.
Answer: D

19.Once installed, the R75 kernel resides directly below which layer of the OSI model? Note: Application is the top and Physical is the bottom of the IP stack.
A. Network
B. Transport
C. Data Link
D. Session
Answer: A

20.R75's INSPECT Engine inserts itself into the kernel between which two layers of the OSI model?
A. Presentation and Application
B. Physical and Data
C. Session and Transport
D. Data and Network
Answer: D

21.What would be the benefit of upgrading from SmartDefense to IPS R75?
A. The SmartDefense is replaced by the technology of IPS-1.
B. The SmartDefense technology expands IPS-1 to IPS R75.
C. Completely rewritten engine provides improved security performance and reporting.

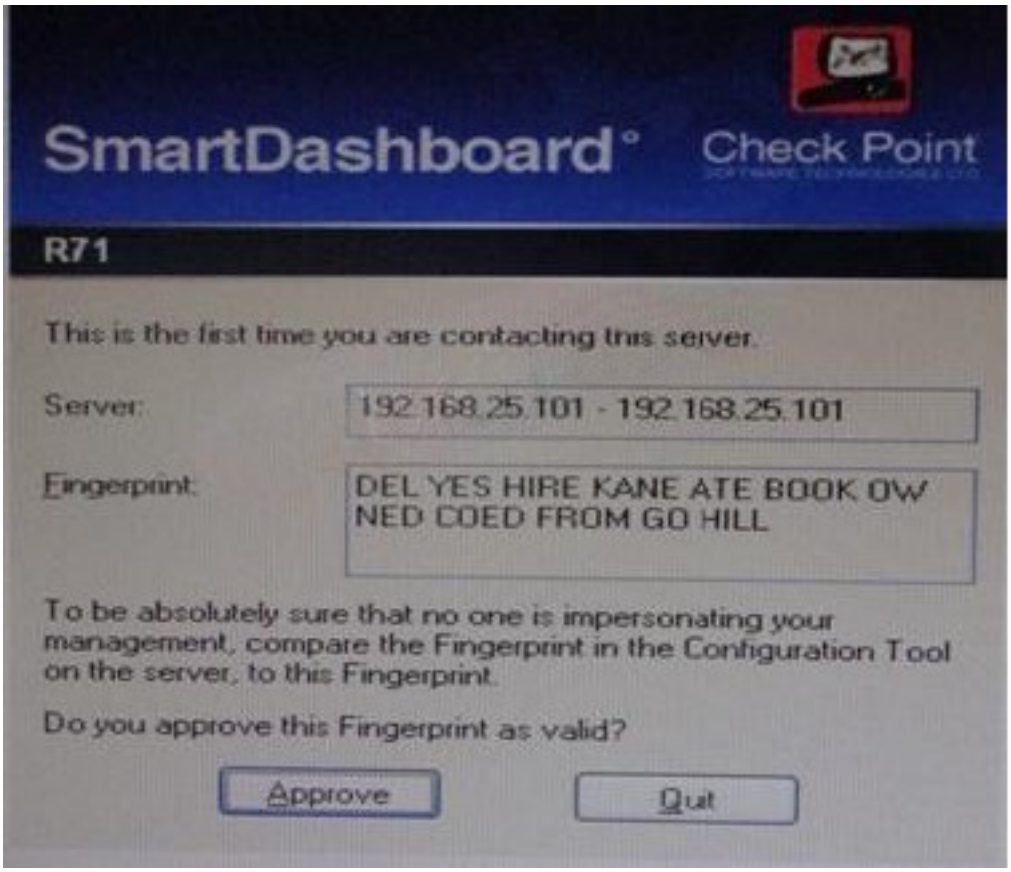
D. There is no difference - IPS R75 is the new name.
Answer: C

22.You need to completely reboot the Operating System after making which of the following changes on the Security Gateway? i.e. the command cprestart is not sufficient.
Adding a hot-swappable NIC to the Operating System for the first time.
Uninstalling the R75 Power/UTM package.
Installing the R75 Power/UTM package.
Re-establishing SIC to the Security Management Server.
Doubling the maximum number of connections accepted by the Security Gateway.
A. 3 only
B. 1, 2, 3, 4, and 5
C. 2, 3 only
D. 3, 4, and 5 only
Answer: C

23.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

24.Your customer wishes to install the SmartConsole on a Windows system. What are the minimum hardware requirements for R75? 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

25.From the output below, where is this fingerprint generated?



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

26.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

27.Over the weekend, an Administrator without access to SmartDashboard installed a new R75 Security Gateway using SecurePlatform. You want to confirm communication between the Gateway and the Management Server by installing the Security Policy. What might prevent you from installing the Policy?
A. You first need to initialize SIC in SmartUpdate.
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. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Server. You must initialize SIC on both the Security Gateway and the Management Server.

D. You first need to run the fw unloadlocal command on the new Security Gateway.
Answer: B

28.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

29.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

30.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