KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **156-215.13**

Title : Check Point Certified Security Administrator - GAiA

Version : DEMO

1.CHECK POINT SOFTWARE TECHNOLOGIES, INC.NONDISCLOSURE AGREEMENT
This Nondisclosure Agreement (the "Agreement") is entered into and effective as of the date appearing next to the signature line (the "Effective Date"), or on the date of electronic acceptance, by and between Check Point Software Technologies, Inc. ("Check Point") and, Examinee hereinafter "Recipient".
1 CONFIDENTIAL INFORMATION. Recipient understands that Check Point will be disclosing information to Recipient regarding Check Point Examination Materials (the "Subject"). Recipient acknowledges that the discussions and the dissemination of examination materials between Recipient and Check Point regarding the Subject, the terms and conditions and the existence of this Agreement, and other information Check Point may be disclosing to Recipient, including but not limited to information learned by Recipient from Check Point employees, will be considered "Confidential Information." Confidential Information does not include information that: (a) is now or subsequently becomes generally available to the public through no fault or breach of Recipient; (b) Recipient can demonstrate was rightfully in its possession prior to disclosure to Recipient by Check Point;
2 USE OF CONFIDENTIAL INFORMATION. Recipient agrees to accept Confidential Information solely for use in connection with Recipient's examination purposes and will not disclose, publish, or disseminate Confidential Information to anyone. Recipient agrees to use reasonable care, but in no event less than the same degree of care that it uses to protect its own confidential and proprietary information of similar importance, to prevent any unauthorized use, disclosure, publication, or dissemination of Confidential Information and further agrees not to use Confidential Information otherwise for its own or any third party's benefit without the prior written approval of an authorized representative of Check Point. Recipient may disclose Confidential Information if required by any judicial or governmental order, provided that Recipient takes reasonable steps to first give Check Point sufficient prior notice to contest such order.
3. OWNERSHIP OF CONFIDENTIAL INFORMATION. All Confidential Information remains the property of Check Point and/or its licensors and no license or other rights to Confidential Information are granted or implied hereby.
4. RETURN OF DOCUMENTS. Recipient will return all tangible Confidential Information, including but not limited to all computer programs, documentation, notes, plans, drawings, and copies thereof, to Check Point. With respect to Confidential Information stored in electronic form, Recipient shall, delete all such Confidential Information from its systems and shall confirm in a writing signed by an authorized representative of Recipient, that all such Confidential Information has been deleted.
5. ENTIRE AGREEMENT AND GOVERNING LAW. This Agreement constitutes the entire agreement between the parties regarding the Confidential Information and supersedes all prior or contemporaneous oral or written agreements concerning such Confidential Information. This Agreement may not be amended except by a written agreement signed by authorized representatives of both parties. This Agreement will be governed by and construed in accordance with the laws of the State of California, excluding that body of California law concerning conflicts of law.
YOU AGREE THAT YOU HAVE READ, UNDERSTOOD AND THAT YOU FREELY ACCEPT THESE TERMS.
A. I ACCEPT
B.I DO NOT ACCEPT
Answer:A

2.CHECK POINT SOFTWARE TECHNOLOGIES, INC.NONDISCLOSURE AGREEMENT
This Nondisclosure Agreement (the "Agreement") is entered into and effective as of the date appearing

next to the signature line (the "Effective Date"), or on the date of electronic acceptance, by and between Check Point Software Technologies, Inc. ("Check Point") and, Examinee hereinafter "Recipient".
1. CONFIDENTIAL INFORMATION. Recipient understands that Check Point will be disclosing information to Recipient regarding Check Point Examination Materials (the "Subject"). Recipient acknowledges that the discussions and the dissemination of examination materials between Recipient and Check Point regarding the Subject, the terms and conditions and the existence of this Agreement, and other information Check Point may be disclosing to Recipient, including but not limited to information learned by Recipient from Check Point employees, will be considered "Confidential Information." Confidential Information does not include information that: (a) is now or subsequently becomes generally available to the public through no fault or breach of Recipient; (b) Recipient can demonstrate was rightfully in its possession prior to disclosure to Recipient by Check Point;
2. USE OF CONFIDENTIAL INFORMATION. Recipient agrees to accept Confidential Information solely for use in connection with Recipient's examination purposes and will not disclose, publish, or disseminate Confidential Information to anyone. Recipient agrees to use reasonable care, but in no event less than the same degree of care that it uses to protect its own confidential and proprietary information of similar importance, to prevent any unauthorized use, disclosure, publication, or dissemination of Confidential Information and further agrees not to use Confidential Information otherwise for its own or any third party's benefit without the prior written approval of an authorized representative of Check Point. Recipient may disclose Confidential Information if required by any judicial or governmental order, provided that Recipient takes reasonable steps to first give Check Point sufficient prior notice to contest such order.
3 OWNERSHIP OF CONFIDENTIAL INFORMATION. All Confidential Information remains the property of Check Point and/or its licensors and no license or other rights to Confidential Information are granted or implied hereby.
4. RETURN OF DOCUMENTS. Recipient will return all tangible Confidential Information, including but not limited to all computer programs, documentation, notes, plans, drawings, and copies thereof, to Check Point. With respect to Confidential Information stored in electronic form, Recipient shall, delete all such Confidential Information from its systems and shall confirm in a writing signed by an authorized representative of Recipient, that all such Confidential Information has been deleted.
5. ENTIRE AGREEMENT AND GOVERNING LAW. This Agreement constitutes the entire agreement between the parties regarding the Confidential Information and supersedes all prior or contemporaneous oral or written agreements concerning such Confidential Information. This Agreement may not be amended except by a written agreement signed by authorized representatives of both parties. This Agreement will be governed by and construed in accordance with the laws of the State of California, excluding that body of California law concerning conflicts of law.
YOU AGREE THAT YOU HAVE READ, UNDERSTOOD AND THAT YOU FREELY ACCEPT THESE TERMS.
A.I ACCEPT
B.I DO NOT ACCEPT
Answer:A

3.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

4.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

5.The INSPECT engine inserts itself into the kernel between which two OSI model layers?
A.Physical and Data
B.Session and Transport
C.Data and Network
D.Presentation and Application
Answer:C

6.The customer has a small Check Point installation, which includes one SecurePlatform server working as the SmartConsole, and a second server running Windows 2008 as both Security Management Server and Security Gateway. This is an example of a(n):
A.Distributed Installation
B.Stand-Alone Installation
C.Hybrid Installation
D.Unsupported configuration
Answer:D

7.The customer has a small Check Point installation which includes one Windows 2008 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.Stand-Alone Installation
B.Distributed Installation
C.Unsupported configuration
D.Hybrid Installation
Answer:A

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

9.The customer has a small Check Point installation which includes one Windows 2008 server as SmartConsole and Security Management Server with a second server running SecurePlatform as Security Gateway. This is an example of a(n):
A.Stand-Alone Installation.
B.Distributed Installation.
C.Hybrid Installation.
D.Unsupported configuration.
Answer:B

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

11.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

12.Which of the following statements is TRUE about management plug-ins?
A.A management plug-in interacts with a Security Management Server to provide new features and support for new products.
B.The plug-in is a package installed on the Security Gateway.
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.
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.One
C.As many as you want
D.Only one with full access and one with read-only access
Answer:B

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

verification?
A.When configuring the Security Gateway object in SmartDashboard
B.When configuring the Security Management Server using cpconfig
C.When establishing SIC between the Security Management Server and the Gateway
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.From the Security Management Server's command line, type fw putkey -p <shared key> <IP Address of Security Gateway>.
B.Run the command fwm sic_reset to reinitialize the Security Management Server Internal Certificate Authority (ICA). Then retype the activation key on the Security Gateway from SmartDashboard.
C.Use SmartUpdate to retype the Security Gateway activation key. This will automatically sync SIC to both the Security Management Server and Gateway.
D.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).
Answer:D

16.How can you recreate the Security Administrator account, which was created during initial Management Server installation on SecurePlatform?
A.Launch cpconfig and delete the Administrator's account. Recreate the account with the same name.
B.Launch SmartDashboard in the User Management screen, and delete the cpconfig administrator.
C.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.
D.Type cpm -a, and provide the existing Administrator's account name. Reset the Security Administrator's password.
Answer:A

17.When Jon first installed his new security 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 SmartDashboard, edit the firewall Gateway object, select the tab Interfaces > Domain Name Servers.
B.Login to the firewall using SSH and run cpconfig, then select Domain Name Servers.
C.Login to the firewall using SSH and run fwm, then select System Configuration > Domain Name Servers.
D.Login to the firewall using SSH and run sysconfig, then select Domain Name Servers.
Answer:D

18.The London Security Gateway Administrator has just installed the Security Gateway and Management Server. He has not changed any default settings. As he tries to configure the Gateway, he is unable to connect. Which troubleshooting suggestion will NOT help him?
A.Check if some intermediate network device has a wrong routing table entry, VLAN assignment,

duplex-mismatch, or trunk issue.
B.Verify that the Rule Base explicitly allows management connections.
C.Test the IP address assignment and routing settings of the Security Management Server, Gateway, and console client.
D.Verify the SIC initialization.
Answer:B

19.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.)
1. Adding a hot-swappable NIC to the Operating System for the first time.
2. Uninstalling the R75 Power/UTM package.
3. Installing the R75 Power/UTM package.
4. Re-establishing SIC to the Security Management Server.
5. Doubling the maximum number of connections accepted by the Security Gateway.

A.2, 3 only
B.3 only
C.3, 4, and 5 only
D.1, 2, 3, 4, and 5
Answer:A

20.The Security Gateway is installed on SecurePlatform R76 The default port for the Web User Interface is _____.
A.TCP 443
B.TCP 4433
C.TCP 18211
D.TCP 257
Answer:A