Check Point CCSA Next Generation

1. Static Source NAT translates public internal source IP addresses to private external source IP addresses.

> A. True

> B. False.

Answer(s): B

---

2. In the Client Authentication Action Properties window (below), for the required Sign On Method section, Manual is selected.

> A. If a connection matches the Rule Base the service is an authenticated service, the client is signed on after a successful authentication.

> B. The user must initiate the Client Authentication Session to the gateway.

> C. If a connection using any service matches Rule Base, the client is authenticated.

> D. If authentication is successful, access is granted from the network that initiated the connection.

> E. The user must TELNET to the target server on port 259.

Answer(s): B

---

3. Client Authentication rules should be placed above the Stealth rule, so users can authenticate to the firewall.

> A. True

> B. False

Answer(s): A

---

4. Your customer has created a rule so that every time a user wants to go to Internet, that user must be authenticated. The customer requires an authentication scheme that provides transparency for the user and granular control for the administrator.

A. Session

B. User

C. Client

D. Dual

E. Reverse

Answer(s): B

---

5. Which of the following characteristics BEST describes the behaviour of Check Point NG with Application Intelligence?

A. All traffic is expressly permitted by explicit rules.

B. Traffic is filtered using controlled ports.

C. TELNET, HTTP; and SMTP are allowed by default.

D. Traffic not expressly permitted is prohibited.

E. Secure connections are authorized by default. Unsecured connectdions are not.

Answer(s): D

---

6. With Blocking Scope default settings, a selected connection is terminated:

A. And all further attempts to establish a connection from the same source IP address to the same destination IP address and port will be blocked.

B. But all further attempts to establish connections from this specific source IP address will be authenticated before being denied.

C. And all further attempts to establish connections to this specific destination IP address will be denied.

D. And all further attempts to establish a connection from the same source IP address to the firewall's IP address will be blocked.

E. Both A and D.

Answer(s): A

---

7. Assume an NT system. What is the default expiration for a Dynamic NAT connection NOT showing any TCP activity?

A. 30 Seconds.

B. 60 Seconds.

C. 330 Seconds.

D. 660 Seconds.

E. 3600 Seconds.

Answer(s): E

---

8. Select what is true of hidden rules.

A. Whether they are displayed, or not, hidden rules are made redundant when the security Policy is installed

B. Whether they are displayed, or not hidden rules numbering would change when the security Policy is installed

C. Whether they are displayed, or not, hidden rules are enforced when the security Policy is installed

D. Whether they are displayed, or not, hidden rules are displayed when the security Policy is installed

E. None of the above

Answer(s): C

---

9. Anna is a security administrator setting up User Authentication for the first time. She has correctly configured her Authentication rule, but authentication still does not work. What is the Check Point recommended way to troubleshoot this issue?

A. Verify the properties of the user attempting authentication and the authentication method selected in the Authentication Properties of your firewall object.

B. Verify the firewall settings of your firewall object, and the properties for the user attempting encryption and authentication.

C. Verify the properties for the user attempting authentication and make sure that the file Stealth Authentication method is selected in the Authentication properties of both the peer gateway object and your firewall object.

D. Verify both Client and User Authentication, and the authentication method selected in the Authentication properties of your Firewall object.

E. Re-import Schema from the VPN-1/FireWall-1 NG installation CD.

Answer(s): A

---

10. User authentication cannot provide access privilege for which services?

A. FTP

B. HTTP

C. TELNET

D. RLOGIN

E. RPC

Answer(s): E

---

11. Omanan Enterprises has the premier reclamation system for scrap aluminum in the western hemisphere. Then phenomenal growth over the last 10 years has led to the decision to establish a presence in the Internet in order to their customers. To that end, Omanan Enterprise network administrator, Jason has acquired a Web Server, and email server and 14 IP addresses from their ISP. Jason also purchased a Checkpoint VPN-1/FireWall-1 stand alone gateway module, with these interfaces, to protect Omanan enterprises' corporate data their ISP will be providing DNS services.

A. The proposed solution meets the required objectives and none of the desired objectives.

B. The proposed solution meets the required objectives and only one of the desired objectives.

C. The proposed solution meets the required objectives and all desired objectives.

D. The proposed solution does not meet the required objective.

Answer(s): C

---

12. You are administering one SmartCenter Server that manages three Enforcement Modules. One of the Enforcement Modules does not appear as a target in the Install Policy screen, when you attempt to install the Security Policy. What is causing this to happen?

A. The licence for the Enforcement Module has expired.

B. No Enforcement Module Master filer was created, designating the SmartCenter Server

C. The Enforcement Module was not listed in the Install On column of its rule.

D. The object representing the Enforcement Module was created as a Node->Gateway.

E. The Enforcement Module requires a reboot.

Answer(s): D

---

13. AlphaBravo Corp has 72 privately addressed internal addresses. Each network is a piece of the 10-net subnetted to a class C address. AlphaBravo uses Dynamic NAT and hides all of the internal networks behind the external IP addresses of the Firewall. The Firewall administrator for AlphaBravo has noticed that policy installation takes significantly longer since adding all 72 internal networks to the address translation rule. What should the Firewall administrator do to reduce the time it takes to install a policy?

A. Create an object for the entire 10-net and use the object for the translation rule instead of the individual network objects.

B. Use automatic NAT rule creation on each network object. Hide the network behind the firewall's external IP addresses.

C. Match packets to the state table, so packets are not dropped. Increase the size of the NAT tables.

D. Reinstall the Firewall and Security Policy Editor. The policy is corrupting Firewall's binaries.

E. Increase the size of state table. Use automatic NAT rule creation to hide the networks behind an IP address other than firewall's external IP.

Answer(s): A

---

14. As a firewall administrator if you want to log packets dropped by "implicit drop anything not covered" rules, you must explicitly define a Clean-up rule. This must be the last rule in the rule base.

A. True

B. False

Answer(s): A

---

15. When you perform a cp fetch, what can you expect from this command?

A. Firewall retrieves the user database from the tables on the Management Module.

B. Firewall retrieves the inspection code from the remote Management Module and installs it to the kernel.

C. Management module retrieves the IP address of the target specified in the command.

D. Management module retrieves the interface information for the target specified in the command.

E. None of the above.

Answer(s): B

---

16. When can Hide Mode not be used?

A. Where the port number cannot be changed

B. Where the port number can be changed

C. Where the external server must distinguish between clients based on their IP address

D. something else

Answer(s): A,C

---

17. You are the Security Administrator with one SmartCenter Server managing one Enforcement Moduel. SmartView Status displayes a computer icon with an "I" in the Status column. What does this mean?

A. The SmartCenter Server cannot contact a gateway.

B. You have entered the wrong password at SmartView Status login.

C. The Enforcement Module is installed and responding to status checks, but the status is problematic.

D. Secure Internal Communications (SIC) has not been established between the SmartCenter Server and the Enforcement Module.

E. The VPN-1/Firewall-1 Enforcement Module has been compromised and is no longer controlled by this SmartCenter Sever.

Answer(s): C

---

18. In the Install On column of a rule, when you select a specific firewall object as the only configuration object, that rule is enforced on all firewalls with in the network, with related configurations.

A. True

B. False.

Answer(s): B

---

19. Which of the following does a Check Point security gateway access, analyze, and use? Choose three.

A. Communications information

B. Information mapping

C. Communication-derivec state

D. Packet sniffing

E. Application-derived state

Answer(s): A,C,E

---

20. Howa re Storm Center Block Lists activated? Choose the correction order.

A. 2, 3, 1

B. 1, 2, 3

C. 3, 2, 1

D. 3, 1, 2

E. 2, 1, 3

Answer(s): B