Check Point Certified Security Administrator

1. You receive a notification that long-lasting Telnet connections to a mainframe are dropped after an hour of inactivity. Reviewing SmartView Tracker shows the packet is dropped with the error:

A. Create a new TCP service object on port 23 called Telnet-mainframe. Define a service- based session timeout of 24-hours. Use this new object only in the rule that allows the Telnet connections to the mainframe.

B. Ask the mainframe users to reconnect every time this error occurs.

C. Increase the TCP session timeout under Global Properties > Stateful Inspection.

D. Increase the service-based session timeout of the default Telnet service to 24-hours.

Answer(s): A

---

2. Which of the following is true of a Stealth Rule?

A. The Stealth rule should be located just before the Cleanup rule

B. The Stealth rule must be the first rule in a policy

C. The Stealth rule is required for proper firewall protection

D. The Stealth rule should not be logged

Answer(s): C

---

3. What command syntax would you use to see accounts the gateway suspects are service accounts?

A. pdp show service

B. adlog a service_accounts

C. adlog check_accounts

D. pdp check_log

Answer(s): B

---

4. You are a Security Administrator using one Security Management Server managing three different firewalls. One firewall does NOT show up in the dialog box when attempting to install a Security Policy. Which of the following is a possible cause?

A. The firewall object has been created but SIC has not yet been established.

B. The firewall has failed to sync with the Security Management Server for 60 minutes.

C. The license for this specific firewall has expired.

D. The firewall is not listed in the Policy Installation Targets screen for this policy package.

Answer(s): D

---

5. What command syntax would you use to turn on PDP logging in a distributed environment?

A. pdp log=1

B. pdp logging on

C. pdp track=1

D. pdp tracker on

Answer(s): D

---

6. You are MegaCorp's Security Administrator. There are various network objects which must be NATed. Some of them use the Automatic Hide NAT method, while others use the Automatic Static NAT method. What is the rule order if both methods are used together?

A. The Static NAT rules have priority over the Hide NAT rules and the NAT on a node has priority over the NAT on a network or an address range.

B. The Administrator decides the rule order by shifting the corresponding rules up and down.

C. The rule position depends on the time of their creation. The rules created first are placed at the top; rules created later are placed successively below the others.

D. The Hide NAT rules have priority over the Static NAT rules and the NAT on a node has priority over the NAT on a network or an address range.

Answer(s): A

---

7. 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. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

C. The plug-in is a package installed on the Security Gateway.

D. Installing a management plug-in is just like an upgrade process.

Answer(s): A

---

8. Where is the fingerprint generated, based on the output display?

A. Security Management Server

B. SmartDashboard

C. SmartUpdate

D. SmartConsole

Answer(s): A

---

9. You are running a R77 Security Gateway on GAiA. In case of a hardware failure, you have a server with the exact same hardware and firewall version installed. What back up method could be used to quickly put the secondary firewall into production?

A. upgrade_export

B. snapshot

C. backup

D. manual backup

Answer(s): B

---

10. Your bank's distributed R77 installation has Security Gateways up for renewal.

A. SmartDashboard

B. SmartPortal

C. SmartView Tracker

D. SmartUpdate

Answer(s): D

---

11. Which command allows Security Policy name and install date verification on a Security Gateway?

A. fw ver -p

B. fw show policy

C. fw stat -l

D. fw ctl pstat -policy

Answer(s): C

---

12. Before upgrading SecurePlatform to GAiA, 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.

A. A backup cannot be restored, because the binary files are missing.

B. The restore is not possible because the backup file does not have the same build number (version).

C. The restore can be done easily by the command restore and copying netconf.C from the production environment.

D. The restore is done by selecting Snapshot Management from the boot menu of GAiA.

Answer(s): C

---

13. You are trying to save a custom log query in R77 SmartView Tracker, but getting the following error:

A. You do not have OS write permissions on the local SmartView Tracker PC in order to save the custom query locally.

B. You have read-only rights to the Security Management Server database.

C. Another administrator is currently connected to the Security Management Server with read/write permissions which impacts your ability to save custom log queries to the Security Management Server.

D. You do not have the explicit right to save a custom query in your administrator permission profile under SmartConsole customization.

Answer(s): B

---

14. Which Client Authentication sign-on method requires the user to first authenticate via the User Authentication mechanism, when logging in to a remote server with Telnet?

A. Manual Sign On

B. Partially Automatic Sign On

C. Agent Automatic Sign On

D. Standard Sign On

Answer(s): B

---

15. Which of the following is NOT useful to verify whether or not a Security Policy is active on a Gateway?

A. cpstat fw -f policy

B. fw ctl get string active_secpol

C. Check the Security Policy name of the appropriate Gateway in SmartView Monitor.

D. fw stat

Answer(s): B

---

16. _____ is an R77 component that displays the number of packets accepted, rejected, and dropped on a specific Security Gateway, in real time.

A. SmartView Status

B. SmartEvent

C. SmartUpdate

D. SmartView Monitor

Answer(s): D

---

17. How do you recover communications between your Security Management Server and Security Gateway if you lock yourself out through a rule or policy mis-configuration?

A. fw unloadlocal

B. fwm unloadlocal

C. fw unload policy

D. fw delete all.all@localhost

Answer(s): A

---

18. Jack has locked himself out of the Kirk Security Gateway with an incorrect policy and can no longer connect from the McCoy Management Server.

A. Kirk> fw unload policy

B. Kirk> fw unload local

C. Kirk> fw fetch policy

D. Kirk> fw unloadlocal

Answer(s): D

---

19. When configuring LDAP authentication, which of the following items should be configured for the Security Management Server?

A. Windows logon password

B. Login Distinguished Name and password

C. Check Point Password

D. WMI object

Answer(s): B

---

20. Your organization's disaster recovery plan needs an update to the backup and restore section to reap the new distributed R77 installation benefits. Your plan must meet the following required and desired objectives:

A. Meets the required objective but does not meet either desired objective.

B. Meets the required objective and both desired objectives.

C. Meets the required objective and only one desired objective.

D. Does not meet the required objective.

Answer(s): B
