Check Point Certified Security Administrator R81

1. Which is a suitable command to check whether Drop Templates are activated or not?

A. fw ctl get int activate_drop_templates

B. fwaccel stat

C. fwaccel stats

D. fw ctl templates d

Answer(s): B

---

2. Please choose correct command syntax to add an "emailserver1" host with IP address 10.50.23.90 using GAiA management CLI?

A. hostname myHost12 ip-address 10.50.23.90

B. mgmt add host name ip-address 10.50.23.90

C. add host name emailserver1 ip-address 10.50.23.90

D. mgmt add host name emailserver1 ip-address 10.50.23.90

Answer(s): D

---

3. The CDT utility supports which of the following?

A. Major version upgrades to R77.30

B. Only Jumbo HFA's and hotfixes

C. Only major version upgrades to R80.10

D. All upgrades

Answer(s): D

---

4. Using ClusterXL, what statement is true about the Sticky Decision Function?

A. Can only be changed for Load Sharing implementations

B. All connections are processed and synchronized by the pivot

C. Is configured using cpconfig

D. Is only relevant when using SecureXL

Answer(s): A

---

5. What command would show the API server status?

A. cpm status

B. api restart

C. api status

D. show api status

Answer(s): D

---

6. How Capsule Connect and Capsule Workspace differ?

A. Capsule Connect provides a Layer3 VPN. Capsule Workspace provides a Desktop with usable applications

B. Capsule Workspace can provide access to any application

C. Capsule Connect provides Business data isolation

D. Capsule Connect does not require an installed application at client

Answer(s): A

---

7. Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

A. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.

B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.

C. Time object to a rule to make the rule active only during specified times.

D. Sub Policies are sets of rules that can be created and attached to specific rules. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Answer(s): D

---

8. What are the three components for Check Point Capsule?

A. Capsule Docs, Capsule Cloud, Capsule Connect

B. Capsule Workspace, Capsule Cloud, Capsule Connect

C. Capsule Workspace, Capsule Docs, Capsule Connect

D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer(s): D

---

9. Full synchronization between cluster members is handled by Firewall Kernel.
Which port is used for this?

A. UDP port 265

B. TCP port 265

C. UDP port 256

D. TCP port 256

Answer(s): B

---

10. What is true about the IPS-Blade?

A. in R80, IPS is managed by the Threat Prevention Policy

B. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict

C. in R80, IPS Exceptions cannot be attached to "all rules"

D. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer(s): A

---

11. Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

A. Go to clash-Run cpstop | Run cpstart

B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway

C. Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores

D. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Answer(s): B

---

12. When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

A. Any size

B. Less than 20GB

C. More than 10GB and less than 20 GB

D. At least 20GB

Answer(s): D

---

13. Which firewall daemon is responsible for the FW CLI commands?

A. fwd

B. fwm

C. cpm

D. cpd

Answer(s): A

---

14. If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.

B. Change the Standby Security Management Server to Active.

C. Change the Active Security Management Server to Standby.

D. Manually synchronize the Active and Standby Security Management Servers.

Answer(s): A

---

15. Using R80 Smart Console, what does a "pencil icon" in a rule mean?

A. I have changed this rule

B. Someone else has changed this rule

C. This rule is managed by check point's SOC

D. This rule can't be changed as it's an implied rule

Answer(s): A

---

16. Which method below is NOT one of the ways to communicate using the Management API's?

A. Typing API commands using the "mgmt_cli" command

B. Typing API commands from a dialog box inside the SmartConsole GUI application

C. Typing API commands using Gaia's secure shell (clash)19+

D. Sending API commands over an http connection using web-services

Answer(s): D

---

17. Session unique identifiers are passed to the web api using which http header option?

A. X-chkp-sid

B. Accept-Charset

C. Proxy-Authorization

D. Application

Answer(s): A

---

18. What is the main difference between Threat Extraction and Threat Emulation?

A. Threat Emulation never delivers a file and takes more than 3 minutes to complete

B. Threat Extraction always delivers a file and takes less than a second to complete

C. Threat Emulation never delivers a file that takes less than a second to complete

D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

Answer(s): B

---

19. Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

A. Detects and blocks malware by correlating multiple detection engines before users are affected.

B. Configure rules to limit the available network bandwidth for specified users or groups.

C. Use UserCheck to help users understand that certain websites are against the company's security policy.

D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Answer(s): A

---

20. You want to store the GAiA configuration in a file for later reference. What command should you use?

A. write mem

B. show config -f

C. save config -o

D. save configuration

Answer(s): D