Checkpoint Certified Security Master R80

1. Which of the following is NOT an internal/native Check Point command?

A. fwaccel on

B. fw ct1 debug

C. tcpdump

D. cphaprob

Answer(s): C

---

2. What CLI command will reset the IPS pattern matcher statistics?

A. ips reset pmstat

B. ips pstats reset

C. ips pmstats refresh

D. ips pmstats reset

Answer(s): D

---

3. As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

A. that is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager

B. Full Layer4 VPN SSL VPN that gives users network access to all mobile applications

C. Full layer3 VPN IPSec VPN that gives users network access to all mobile applications

D. You can make sure that documents are sent to the intended recipients only

Answer(s): C

---

4. What is the purpose of Priority Delta in VRRP?

A. When a box is up, Effective Priority = Priority + Priority Delta

B. When an Interface is up, Effective Priority = Priority + Priority Delta

C. When an Interface fail, Effective Priority = Priority Priority Delta

D. When a box fail, Effective Priority = Priority Priority Delta

Answer(s): C

---

5. You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

A. fw cti multik dynamic_dispatching on

B. fw cti multik dynamic_dispatching set_mode 9

C. fw cti multik set_mode 9

D. fw cti multik pq enable

Answer(s): C

---

6. John detected high load on sync interface. Which is most recommended solution?

A. For short connections like http service delay sync for 2 seconds

B. Add a second interface to handle sync traffic

C. For short connections like http service do not sync

D. For short connections like icmp service delay sync for 2 seconds

Answer(s): A

---

7. What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?

A. Anti-Bot is the only countermeasure against unknown malware

B. Anti-Bot is the only protection mechanism which starts a counter-attack against known Command & Control Centers

C. Anti-Bot is the only signature-based method of malware protection

D. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command & Control Center

Answer(s): D

---

8. GAiA Software update packages can be imported and installed offline in situation where:

A. Security Gateway with GAiA does NOT have SFTP access to Internet

B. Security Gateway with GAiA does NOT have access to Internet.

C. Security Gateway with GAiA does NOT have SSH access to internet.

D. The desired CPUSE package is ONLY available in the Check Point CLOU

Answer(s): B

---

9. What scenario indicates that SecureXL is enabled?

A. Dynamic objects are available in the Object Explorer

B. SecureXL can be disabled in cpconfig

C. fwaccel commands can be used in clish

D. Only one packet in a stream is seen in a fw monitor packet capture

Answer(s): C

---

10. What is mandatory for ClusterXL to work properly?

A. The number of cores must be the same on every participating cluster node

B. The Magic MAC number must be unique per cluster node.

C. The Sync Interface must not have an IP address configured

D. If you have "Non-monitored Private" interfaces, the number of those interfaces must be the same on allcluster members

Answer(s): B

---

11. Check Point recommends configuring Disk Space Management parameters to delete old log entities when available disk space is less than or equal to?

A. 50%

B. 75%

C. 80%

D. 15%

Answer(s): D

---

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

A. None, Security Management Server would be installed by itself

B. SmartConsole

C. SecureClient

D. SmartEvent

Answer(s): D

---

13. Which of the following statements is TRUE about R80 management plug-ins?

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

B. Installing a management plug-in requires a Snapshot, just like any upgrade process.

C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.

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

Answer(s): C

---

14. What is the SandBlast Agent designed to do?

A. Performs OS-level sandboxing for SandBlast Cloud architecture

B. Ensure the Check Point SandBlast services is running on the end user's system

C. If malware enters an end user's system, the SandBlast Agent prevents the malware form spreading with the network

D. Clean up email sent with malicious attachments.

Answer(s): C

---

15. In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap

B. Mail, Block Source, Block Destination, Block Services, SNMP Trap

C. Mail, Block Source, Block Destination, External Script, SNMP Trap

D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Answer(s): A

---

16. What are types of Check Point APIs available currently as part of R80.10 code?

A. Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API

B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API

C. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API

D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Answer(s): B

---

17. What does the command vpn crl__zap do?

A. Nothing, it is not a valid command

B. Erases all CRL's from the gateway cache

C. Erases VPN certificates from cache

D. Erases CRL's from the management server cache

Answer(s): B

---

18. 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, andrisk levels.

Answer(s): A

---

19. When deploying multiple clustered firewalls on the same subnet, what does the firewall administrator need to configure to prevent CCP broadcasts being sent to the wrong cluster?

A. Set the fwha_mac_magic_forward parameter in the $CPDIR/boot/modules/ha_boot. conf

B. Set the fwha_mac_magic parameter in the $FWDIR/boot/fwkern.conf file

C. Set the cluster global ID using the command "cphaconf cluster_id set "

D. Set the cluster global ID using the command "fw ctt set cluster_id "

Answer(s): C

20. Fill in the blank: The tool _____ generates a R80 Security Gateway configuration report.

A. infoCP

B. infoview

C. cpinfo

D. fw cpinfo

Answer(s): C