Checkpoint Certified Security Expert R65

1. Tom has been tasked to install Check Point R80 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. One machine, but it needs to be installed using SecurePlatform for compatibility purposes

B. One machine

C. Two machines

D. Three machines

Answer(s): C

---

2. In order to test ClusterXL failovers which command would you use on one of the ClusterXL nodes to initiate a failover?

A. clusterXL_admin down -p

B. cluster XL_admin up -p

C. cphaprob -d TEST -s ok register

D. cphaprob -d TEST -s problem unregister

Answer(s): A

---

3. Which of the following is NOT a valid “fwaccel” parameter?

A. stat

B. stats

C. templates

D. packets

Answer(s): D

---

4. Which of the following is not one of the relational database domains that stores the management configuration?

A. User Domain

B. System Domain

C. Global Domain

D. Audit Domain

Answer(s): D

---

5. What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

A. .cap

B. .exe

C. .tgz

D. .pcap

Answer(s): A

---

6. Where will the usermode core files located?

A. /var/log/dump/usermode

B. /var/suroot

C. $FWDIR/var/log/dump/usermode

D. $CPDIR/var/log/dump/usermode

Answer(s): A

---

7. How often will a gateway with Performance Pack running by default automatically review and distribute interface affinity between cores?

A. Every 60 seconds

B. Interface affinity is determined at gateway build time and does not change

C. Every 5 minutes

D. Every 10 seconds

Answer(s): A

---

8. Which of the following features is supported in Check Point’s implementation of IPv6?

A. Security Servers

B. QoS

C. ClusterXL High Availability

D. SAM

Answer(s): C

---

9. You verified that Performance Pack is disabled and need to distribute the affinity interfaces. What command would you run to use static affinity to balance the interfaces between the SND cores?

A. cpmq set

B. sim affinity -s

C. fw ctl affinity -a -l -v

D. fw ctl affinity -s

Answer(s): C

---

10. Which command would you use to check CoreXL instances for IPv6 traffic?

A. fwaccel6 stats

B. fwaccel6 stat

C. fw ctl multik stat

D. fw6ctl multik stat

Answer(s): C

---

11. What must be done for the “fw monitor” command to capture packets through the firewall kernel?

A. SecureXL must be disabled

B. ClusterXL must be temporarily disabled

C. Firewall policy must be re-installed

D. The output file must be transferred to a machine with WireShark

Answer(s): A

---

12. Consider a Check Point Security Gateway under high load. What mechanism can be used to confirm that important traffic such as control connections are not dropped?

A. fw debug fgd50 on OPSEC_DEBUG_LEVEL=3

B. fw ctl multik prioq

C. fgate –d load

D. fw ctl debug –m fg all

Answer(s): B

---

13. What is the default and maximum number of entries in the ARP Cache Table in a Check Point appliance?

A. 1,024 and 4,096

B. 4,096 and 16,384

C. 4,096 and 65,536

D. 1,024 and 16,384

Answer(s): D

---

14. Which kernel debug flag should you use to troubleshoot NAT connections?

A. fw ctl debug + xlate xltrc nat table

B. fw ctl debug + xltrc xlate nat conn

C. fw ctl debug + xlate xltrc nat conn drop

D. fw ctl debug + fwx_alloc nat conn drop

Answer(s): C

---

15. You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules

B. Create a separate Security Policy package for each remote Security Gateway

C. Create network objects that restrict all applicable rules to only certain networks

D. Run separate SmartConsole instances to login and configure each Security Gateway directly

Answer(s): B

---

16. Which type of SecureXL templates is enabled by default on Security Gateways?

A. Accept

B. Drop

C. NAT

D. VPN

Answer(s): A

---

17. Which one of following commands should you run to display HTTPS packet content together with kernel debug?

A. fw ctl get int https_inspection_show_decrypted_data_in_debug=1 fw ctl get int ssl_inspection_extra_debug=1

B. fw set int https_inspection_get_encrypted_data_in_debug 1 fw set int https_inspection_show_debug 1

C. fw ctl set int https_inspection_show_decrypted_data_in_debug 1 fw ctl set int ssl_inspection_extra_debug 1

D. fw ctl set int http_inspection_display_encrypted_data_in_debug=1 fw ctl set int http_inspection_extra_debug=1

Answer(s): C

---

18. You issued the command “set ipv6-state on” in order to enable IPv6 protocol on a Security Gateway. The command was executed successfully. After reboot you notice that IPv6 protocol is not enabled. What do you do to permanently enable IPv6 protocol?

A. Issue “set ipv6-state on” again; Save configuration and reboot

B. You need to modify Gateway Properties in SmartConsole and install policy in order to enable IPv6

C. You need to set “ipv6_state” parameter in $FWDIR/boot/modules/fwkern.conf and reboot

D. You need to install a valid license to use IPv6 protocol

Answer(s): A

---

19. Where does the translation occur with Hide NAT?

A. The destination translation occurs at the client side

B. The source translation occurs at the server side

C. The source translation occurs at the client side

D. The destination translation occurs at the server side

Answer(s): B

---

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
