Check Point Certified Security Administrator R71

1. With the User Directory Software Blade, you can create R71 user definitions on a(n) _______Server.

A. NT Domain

B. Radius

C. LDAP

D. SecureID

Answer(s): C

---

2. You want to create an ASCII formatted output file of the fw monitor command. What is the correct syntax to accomplish this task?

A. fw monitor -e "accept;" > /tmp/monitor.txt

B. fw monitor -e "accept;" -w /tmp/monitor.txt

C. fw monitor -m iO -e "accept;" -o /tmp/monitor.txt

D. fw monitor -e "accept;" -f > /tmp/monitor.txt

Answer(s): A

---

3. Which of the following statements about service contracts, i.e., Certificate, software subscription, or support contract, is FALSE?

A. Service Contracts can apply for an entire User Center account.

B. Most software-subscription contracts are permanent, and need not be renewed after a certain time passes.

C. The contract file is stored on the Security Management Server and downloaded to all Security Gateways during the upgrade process.

D. A service contract can apply only for a single set of Security Gateways managed by the same Security Management Server.

Answer(s): B

---

4. If you check the box Use Aggressive Mode in the IKE Properties dialog box, the standard:

A. three-packet IKE Phase 2 exchange is replaced by a two-packet exchange

B. three-packet IKE Phase 2 exchange Is replaced by a six-packet exchange

C. three-packet IKE Phase 1 exchange is replaced by a six-packet exchange

D. six-packet IKE Phase 1 exchange is replaced by a three-packet exchange

Answer(s): D

---

5. The Security Gateway is installed on SecurePlatform R71. The default port for the Web User Interface is _______.

A. TCP 4433

B. TCP 18211

C. TCP 443

D. TCP 257

Answer(s): C

---

6. What is the size of a hash produced by SHA-1?

A. 160

B. 40

C. 56

D. 128

Answer(s): A

---

7. You enable Automatic Static NAT on an internal host node object with a private IP address of 10.10.10.5, which is NATed into 216.216.216.5. (You use the default settings in Global Properties / NAT.)

A. o=outbound kernel, before the virtual machine

B. I=inbound kernel, after the virtual machine

C. i=inbound kernel, before the virtual machine

D. O=outbound kernel, after the virtual machine

Answer(s): B

---

8. The URL Filtering Policy can be configured to monitor URLs in order to:

A. Block sites only once.

B. Alert the Administrator to block a suspicious site.

C. Redirect users to a new URL.

D. Log sites from blocked categories.

Answer(s): D

---

9. Match each of the following command to there correct function. Each command has one function only listed.

A. C1>F2; C4>F4; C3>F1; C4>F5

B. C1>F2; C2>F1; C3>F6; C4>F4

C. C1>F4; C2>F6, C3>F3; C4>F2

D. C1>F6; C2>F4; C3>F2; C4>F5

Answer(s): D

---

10. In a distributed management environment, the administrator has removed all default check boxes from the Policy / Global Properties / Firewall tab. In order for the Security Gateway to send logs to the Security Management Server, an explicit rule must be created to allow the Security Gateway to communicate to the Security Management Server on port ______.

A. 257

B. 900

C. 256

D. 259

Answer(s): A

---

11. How many inspection capture points are shown in fw monitor?

A. Depends on the number of interfaces on the Gateway

B. 1

C. 2

D. 4

Answer(s): D

---

12. The Internal Certificate Authority (ICA) CANNOT be used for:

A. Remote-access users

B. SIC connections

C. NAT rules

D. Virtual Private Network (VPN) Certificates for gateways

Answer(s): C

---

13. Which command allows verification of the Security Policy name and install date on a Security Gateway?

A. fw show policy

B. fwver-p

C. fw stat -l

D. fw ctl pstat -policy

Answer(s): C

---

14. MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. How do you apply the license?

A. Using your Security Management Server's IP address, and attaching the license to the remote Gateway via SmartUpdate.

B. Using the remote Gateway's IP address and applying the license locally with the cplic put command.

C. Using each of the Gateways' IP addresses, and applying the license on the Security Management Server with the cprlic put command.

D. Using the remote Gateway's IP address, and attaching the license to the remote Gateway via SmartUpdate.

Answer(s): A

---

15. You have configured Automatic Static NAT on an internal host-node object. You clear the box Translate destination on client site from Global Properties / NAT. Assuming all other NAT settings in Global Properties are selected, what else must be configured so that a host on the Internet can initiate an inbound connection to this host?

A. No extra configuration is needed

B. The NAT IP address must be added to the anti-spoofing group of the external gateway interface

C. A static route, to ensure packets destined for the public NAT IP address will reach the Gateway's internal interface.

D. A proxy ARP entry, to ensure packets destined for the public IP address will reach the Security Gateway's external interface.

Answer(s): C

---

16. Which of the following actions take place in IKE Phase 2 with Perfect Forward Secrecy disabled?

A. Each Security Gateway generates a private Diffie-Hellman (DH) key from random pools.

B. The DH public keys are exchanged.

C. Peers authenticate using certificates or preshared secrets.

D. Symmetric IPsec keys are generated.

Answer(s): D

---

17. Which command enables IP forwarding on IPSO?

A. echo 0 > /proc/sys/net/ipv4/ip_forward

B. echo 1 > /proc/sys/net/ipv4/ip_forward

C. clish -c set routing active enable

D. ipsofwd on admin

Answer(s): D

---

18. John currently administers a network using NGX R65.4 on the Security Management Server and NGX R65.2.100 (the VOIP release with the VOIP plug-ins enabled). He wants to upgrade to R71 to get the benefits of Check Point's Software Blades. What would be the best way of doing this?

A. This is not supported today as currently the VOIP Software Blade and VOIP plug-in is not available in R71.

B. Just insert the R71 CD-ROM and run the in-place upgrade.

C. Run upgrade_export on R65 management, then install R71 on this machine and run upgrade_import and re-license the systems to use software blades.

D. This can not be done yet as R71 can not manage NGX R65 Gateways due to SmartDefense and IPS mismatch problems.

Answer(s): A

---

19. You installed Security Management Server on a computer using SecurePlatform in the MegaCorp home office. You use IP address 10.1.1.1. You also installed the Security Gateway on a second SecurePlatform computer, which you plan to ship to another Administrator at a MegaCorp hub office. What is the correct order for pushing SIC certificates to the Gateway before shipping it?

A. 2, 1, 3, 4, 5

B. 2, 3, 4, 5, 1

C. 2, 3, 4, 1, 5

D. 1, 3, 2, 4, 5

Answer(s): A

---

20. You have traveling salesmen connecting to your VPN community from all over the world. Which technology would you choose?

A. IPsec: It allows complex setups that match any network situation available to the client, i.e. connection from a private customer network or various hotel networks.

B. IPsec: It offers encryption, authentication, replay protection and all algorithms that are state of the art (AES) or that perform very well. It is native to many client operating systems, so setup can easily be scripted.

C. SSL VPN: It only requires HTTPS connections between client and server. These are most likely open from all networks, unlike IPsec, which uses protocols and ports which are blocked by many sites.

D. SSL VPN: It has more secure and robust encryption schemes than IPsec.

Answer(s): C
