Check Point Certified Security Administrator (CCSA R80)

1. Which of the following is NOT an integral part of VPN communication within a network?

A. VPN key

B. VPN community

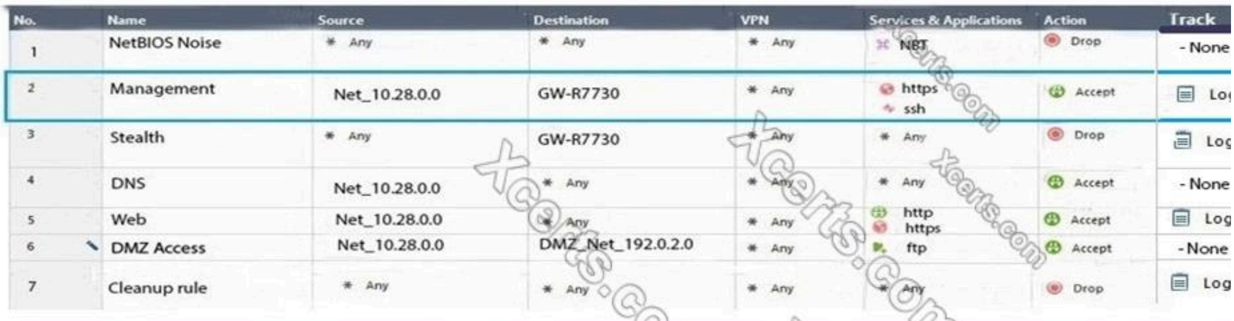
C. VPN trust entities

D. VPN domain

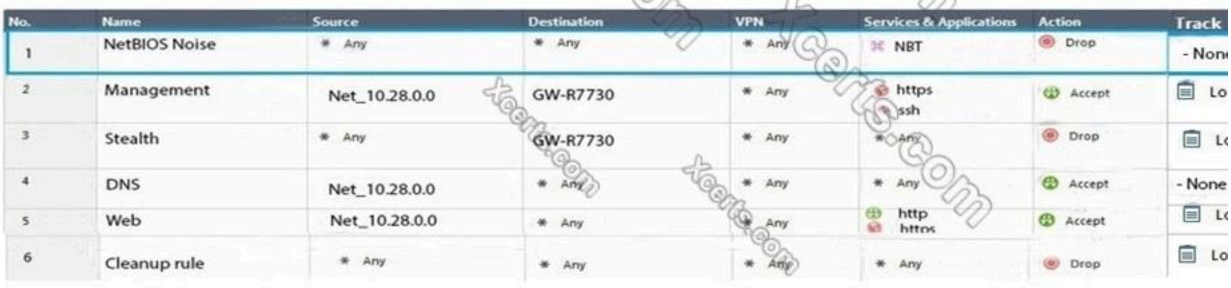
Answer(s): A

---

2. Two administrators Dave and Jon both manage R80 Management as administrators for ABC Corp. Jon logged into the R80 Management and then shortly after Dave logged in to the same server. They are both in the Security Policies view. From the screenshots below, why does Dave not have the rule no.6 in his SmartConsole view even though Jon has it his in his SmartConsole view?



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop	- None
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh	Accept	Lo
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop	Log
4	DNS	Net_10.28.0.0	* Any	* Any	* Any	Accept	- None
5	Web	Net_10.28.0.0	* Any	* Any	http https	Accept	Log
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp	Accept	- None
7	Cleanup rule	* Any	* Any	* Any	Any	Drop	Log



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop	- Non
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh	Accept	Lo
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop	L
4	DNS	Net_10.28.0.0	* Any	* Any	* Any	Accept	- None
5	Web	Net_10.28.0.0	* Any	* Any	http https	Accept	L
6	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Lo

A. Jon is currently editing rule no.6 but has Published part of his changes.

B. Dave is currently editing rule no.6 and has marked this rule for deletion.

C. Dave is currently editing rule no.6 and has deleted it from his Rule Base.

D. Jon is currently editing rule no.6 but has not yet Published his changes.

Answer(s): D

---

3. Vanessa is firewall administrator in her company; her company is using Check Point firewalls on central and remote locations, which are managed centrally by R80 Security Management Server. One central location has an installed R77.30 Gateway on Open server. Remote location is using Check Point UTM-1 570 series appliance with R71. Which encryption is used in Secure Internal Communication (SIC) between central management and firewall on each location?

A. On central firewall AES128 encryption is used for SIC, on Remote firewall 3DES encryption is used for SIC.

B. On both firewalls, the same encryption is used for SIC. This is AES-GCM-256.

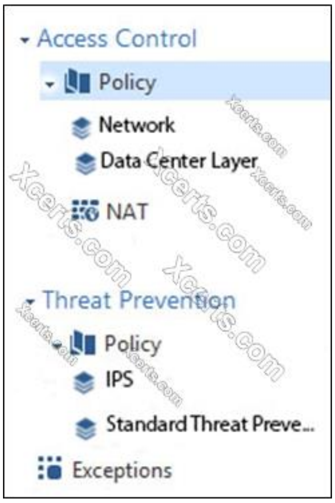
C. The Firewall Administrator can choose which encryption suite will be used by SI

D. On central firewall AES256 encryption is used for SIC, on Remote firewall AES128 encryption is used for SIC.

Answer(s): A

---

4. Review the following screenshot and select the BEST answer.



A. Data Center Layer is an inline layer in the Access Control Policy.

B. By default all layers are shared with all policies.

C. If a connection is dropped in Network Layer, it will not be matched against the rules in Data Center Layer.

D. If a connection is accepted in Network-layer, it will not be matched against the rules in Data Center Layer.

Answer(s): C

---

5. Which of the following is NOT a SecureXL traffic flow?

A. Medium Path

B. Accelerated Path

C. High Priority Path

D. Slow Path

Answer(s): C

---

6. Which of the following Automatically Generated Rules NAT rules have the lowest implementation priority?

☐ A. Machine Hide NAT

☐ B. Address Range Hide NAT

☐ C. Network Hide NAT

□ D. Machine Static NAT

Answer(s): B C

---

7. VPN gateways authenticate using ___________and _____________.

A. Passwords; tokens

B. Certificates; pre-shared secrets

C. Certificates; passwords

D. Tokens; pre-shared secrets

Answer(s): B

---

8. In R80 spoofing is defined as a method of:

A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.

B. Hiding your firewall from unauthorized users.

C. Detecting people using false or wrong authentication logins

D. Making packets appear as if they come from an authorized IP address.

Answer(s): D

---

9. The __________is used to obtain identification and security information about network users.

A. User Directory

B. User server

C. UserCheck

D. User index

Answer(s): A

---

10. Which Check Point feature enables application scanning and the detection?

A. Application Dictionary

B. AppWiki

C. Application Library

D. CPApp

Answer(s): B

---

11. DLP and Geo Policy are examples of what type of Policy?

A. Standard Policies

B. Shared Policies

C. Inspection Policies

D. Unified Policies

Answer(s): B

---

12. In which deployment is the security management server and Security Gateway installed on the same appliance?

A. Bridge Mode

B. Remote

C. Standalone

D. Distributed

Answer(s): C

---

13. A _____________VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.

A. Clientless remote access

B. Clientless direct access

C. Client-based remote access

D. Direct access

Answer(s): A

---

14. 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

---

15. Gaia can be configured using the __________or ______________ ____________.

A. GaiaUI; command line interface

B. WebUI; Gaia Interface

C. Command line interface; WebUI

D. Gaia Interface; GaiaUI

Answer(s): C

---

16. Where can you trigger a failover of the cluster members?
1. Log in to Security Gateway CLI and run command clusterXL_admin down.
2. In SmartView Monitor right-click the Security Gateway member and select Cluster member stop.
3. Log into Security Gateway CLI and run command cphaprob down.

A. 1, 2, and 3

B. 2 and 3

C. 1 and 2

D. 1 and 3

Answer(s): C

---

17. Which utility allows you to configure the DHCP service on GAIA from the command line?

A. ifconfig

B. dhcp_cfg

C. sysconfig

D. cpconfig

Answer(s): C

---

18. Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

A. To satellites through center only

B. To center only

C. To center and to other satellites through center

D. To center, or through the center to other satellites, to internet and other VPN targets

Answer(s): D

---

19. Which product correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

A. SmartView Monitor

B. SmartEvent

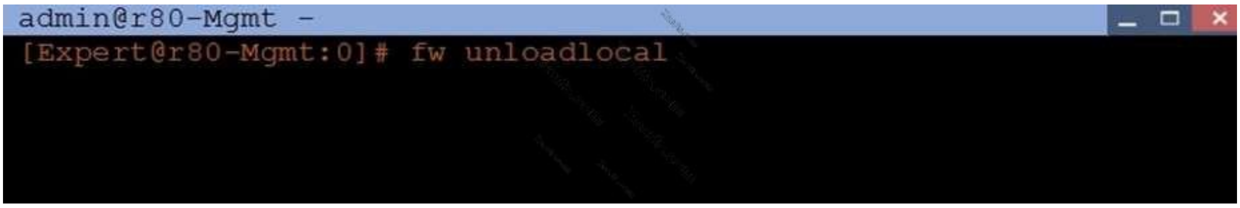
C. SmartUpdate

D. SmartDashboard

Answer(s): B

---

20. Assuming you have a Distributed Deployment, what will be the effect of running the following command on the Security Management Server?



```
admin@r80-Mgmt -
[Expert@r80-Mgmt:0]# fw unloadlocal
```

A. Remove the installed Security Policy.

B. Remove the local ACL lists.

C. No effect.

D. Reset SIC on all gateways.

Answer(s): A
