Vendor: CheckPoint

Exam Code:156-215.81

Exam Name: Check Point Certified Security Administrator R81

Version: Demo

QUESTION 1

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.

Correct Answer: C

QUESTION 2

What two ordered layers make up the Access Control Policy Layer?

A. URL Filtering and Network

B. Network and Threat Prevention

C. Application Control and URL Filtering

D. Network and Application Control

Correct Answer: D

QUESTION 3

Your boss wants you to closely monitor an employee suspected of transferring company secrets to the competition. The IT department discovered the suspect installed a WinSCP client in order to use encrypted communication. Which of the following methods is BEST to accomplish this task?

A. Use SmartView Tracker to follow his actions by filtering log entries that feature the WinSCP destination port. Then, export the corresponding entries to a separate log file for documentation.

B. Use SmartDashboard to add a rule in the firewall Rule Base that matches his IP address, and those of potential targets and suspicious protocols. Apply the alert action or customized messaging.

C. Watch his IP in SmartView Monitor by setting an alert action to any packet that matches your Rule Base and his IP address for inbound and outbound traffic.

D. Send the suspect an email with a keylogging Trojan attached, to get direct information about his wrongdoings.

Correct Answer: A

QUESTION 4

Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

A. UserCheck

B. Active Directory Query

C. Account Unit Query

D. User Directory Query

Correct Answer: B

:

AD Query extracts user and computer identity information from the Active Directory Security Event Logs.

The system generates a Security Event log entry when a user or computer accesses a network resource.

For example, this occurs when a user logs in, unlocks a screen, or accesses a network drive.

Reference : https://sc1.checkpoint.com/documents/R76/

CP_R76_IdentityAwareness_AdminGuide/62402.htm

QUESTION 5

Review the rules. Assume domain UDP is enabled in the implied rules.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	http ftp	User Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	accept	None	Policy Targets

What happens when a user from the internal network tries to browse to the internet using HTTP? The user:

A. can connect to the Internet successfully after being authenticated.

B. is prompted three times before connecting to the Internet successfully.

C. can go to the Internet after Telnetting to the client authentication daemon port 259.

D. can go to the Internet, without being prompted for authentication.

Correct Answer: D

QUESTION 6

Which rule is responsible for the user authentication failure?

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	None
3	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log
4	0	User Auth	Any	webSingapore	Any Traffic	http	User Auth	Log
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	http	accept	Log
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	http dns icmp-proto ftp https	accept	Log
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log

A. Rule 4

B. Rule 6

C. Rule 3

D. Rule 5

Correct Answer: C

QUESTION 7

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret is shared and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

A. IPsec VPN blade should be enabled on both Security Gateway.

B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.

C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.

D. The Security Gateways are pre-R75.40.

Correct Answer: C

QUESTION 8

Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs

B. Capsule Cloud

C. Capsule Enterprise

D. Capsule Workspace

Correct Answer: C

Reference: https://www.checkpoint.com/download/products/sg-capsule-solution.pdf

---

QUESTION 9

Which of the following are types of VPN communities?

A. Pentagon, star, and combination

B. Star, octagon, and combination

C. Combined and star

D. Meshed, star, and combination

Correct Answer: D

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_VPN_AdminGuide/13894

QUESTION 10

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

A. remove database lock

B. The database feature has one command lock database override.

C. override database lock

D. The database feature has two commands: lock database override and unlock database. Both will work.

Correct Answer: D

Use the database feature to obtain the configuration lock. The database feature has two commands:

1.

lock database [override].

2.

unlock database

The commands do the same thing: obtain the configuration lock from another administrator.

Description	Use the `lock database override` and `unlock database` commands to get exclusive read-write access to the database by taking write privileges to the database away from other administrators logged into the system.
Syntax	o `lock database override` o `unlock database`

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm#o73091

QUESTION 11

What is the order of NAT priorities?

A. Static NAT, IP pool NAT, hide NAT

B. IP pool NAT, static NAT, hide NAT

C. Static NAT, automatic NAT, hide NAT

D. Static NAT, hide NAT, IP pool NAT

Correct Answer: A

The order of NAT priorities is:

1.

Static NAT

2.

IP Pool NAT

3.

Hide NAT Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods. Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/6724.htm#o6919

QUESTION 12

After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

A. Security Gateway IP-address cannot be changed without re-establishing the trust

B. The Security Gateway name cannot be changed in command line without re-establishing trust

C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust

D. The Security Management Server IP-address cannot be changed without re-establishing the trust

Correct Answer: A