156-215.80^{Q&As}

Check Point Certified Security Administrator

Pass CheckPoint 156-215.80 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/156-215-80.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

When configuring Spoof Tracking, which tracking actions can an administrator select to be done when spoofed packets are detected?

A. Log, send snmp trap, email

B. Drop packet, alert, none

C. Log, alert, none

D. Log, allow packets, email

Correct Answer: C

Explanation: Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected:

1.

Log - Create a log entry (default)

2.

Alert - Show an alert

3.

None - Do not log or alert

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

QUESTION 2

Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

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

What is the possible explanation for this?

A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.

B. Another administrator is logged into the Management and currently editing the DNS Rule.

C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.

D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

Correct Answer: B

QUESTION 3

Fill in the blank: Service blades must be attached to a _____.

A. Security Gateway

B. Management container

C. Management server

D. Security Gateway container

Correct Answer: A

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?
eventSubmit_doGoviewsolutiondetails=andsolutionid=sk80840

QUESTION 4

You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

A. Right click Accept in the rule, select "More", and then check "Enable Identity Captive Portal"

B. On the firewall object, Legacy Authentication screen, check "Enable Identity Captive Portal"

C. In the Captive Portal screen of Global Properties, check "Enable Identity Captive Portal"

D. On the Security Management Server object, check the box "Identity Logging"

Correct Answer: A

QUESTION 5

Which of the following commands is used to verify license installation?

A. Cplic verify license

B. Cplic print

C. Cplic show

D. Cplic license

Correct Answer: B

QUESTION 6

In order to modify Security Policies the administrator can use which of the following tools? Select the BEST answer.

A. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.

B. SmartConsole and WebUI on the Security Management Server.

C. mgmt_cli or WebUI on Security Gateway and SmartConsole on the Security Management Server.

D. SmartConsole or mgmt_cli on any computer where SmartConsole is installed.

Correct Answer: D

QUESTION 7

Which NAT rules are prioritized first?

A. Post-Automatic/Manual NAT rules

B. Manual/Pre-Automatic NAT

C. Automatic Hide NAT

D. Automatic Static NAT

Correct Answer: B

QUESTION 8

Which of the following Windows Security Events will NOT map a username to an IP address in Identity Awareness?

A. Kerberos Ticket Renewed

B. Kerberos Ticket Requested

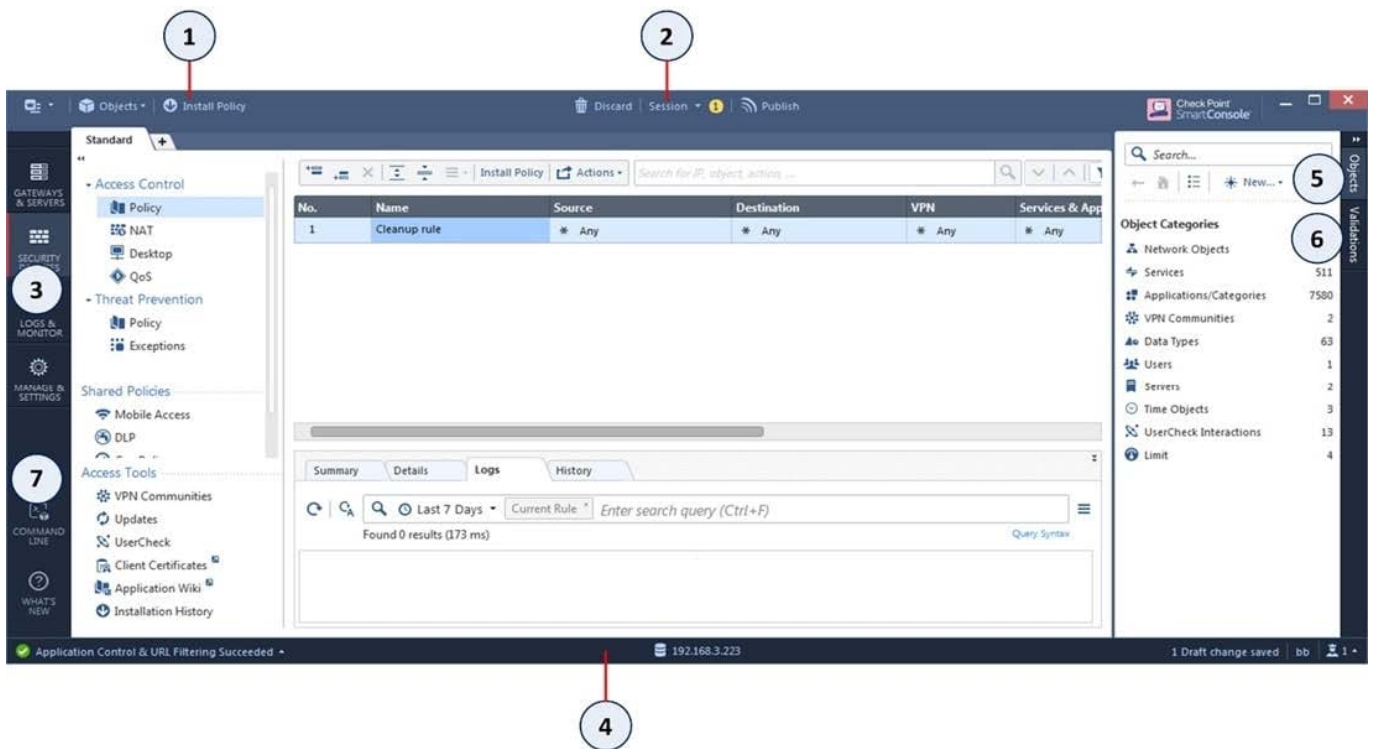C. Account Logon

D. Kerberos Ticket Timed Out

Correct Answer: D

QUESTION 9

Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

A. Manage and Command Line

B. Logs and Monitor

C. Security Policies

D. Gateway and Servers

Correct Answer: A

Item	Description	Item	Description
1	Global Toolbar	5	Objects Bar (F11)
2	Session Management Toolbar	6	Validations pane
3	Navigation Toolbar	7	Command line interface button
4	System Information Area		

Reference: https://sc1.checkpoint.com/documents/R80.10/SmartConsole_OLH/EN/html_frameset.htm?

topic=documents/R80.10/SmartConsole_OLH/EN/4x3HIUbSkxYhtcFgIKlg0w2

QUESTION 10

Fill in the blank: _____ is the Gaia command that turns the server off.

A. sysdown

B. exit

C. halt

D. shut-down

Correct Answer: C

QUESTION 11

How is communication between different Check Point components secured in R80? As with all questions, select the best answer.

A. By using IPSEC

B. By using SIC

C. By using ICA

D. By using 3DES

Correct Answer: B

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?
topic=documents/R80/CP_R80_SecMGMT/125443

QUESTION 12

Fill in the blanks: A security Policy is created in _____ , stored in the _____ , and Distributed to the various _____ .

A. Rule base, Security Management Server, Security Gateways

B. SmartConsole, Security Gateway, Security Management Servers

C. SmartConsole, Security Management Server, Security Gateways

D. The Check Point database, SmartConsole, Security Gateways

Correct Answer: C

QUESTION 13

There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW_A and FW_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW_A is configured to have higher priority than FW_B. FW_A was active and processing the traffic in the morning. FW_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW_B became active. After an hour, FW_A\\'s interface issues were resolved and it became operational. When it re-joins the cluster, will it become active automatically?

A. No, since "maintain current active cluster member" option on the cluster object properties is enabled by default

B. No, since "maintain current active cluster member" option is enabled by default on the Global Properties

C. Yes, since "Switch to higher priority cluster member" option on the cluster object properties is enabled by default

D. Yes, since "Switch to higher priority cluster member" option is enabled by default on the Global Properties

Correct Answer: A

What Happens When a Security Gateway Recovers?

In a Load Sharing configuration, when the failed Security Gateway in a cluster recovers, all connections are redistributed among all active members. High Availability and Load Sharing in ClusterXL ClusterXL Administration Guide R77 Versions | 31 In a High Availability configuration, when the failed Security Gateway in a cluster recovers, the recovery method depends on the configured cluster setting. The options are: Maintain Current Active Security Gateway means that if one member passes on control to a lower priority member, control will be returned to the higher priority member only if the lower priority member fails. This mode is recommended if all members are equally capable of processing traffic, in order to minimize the number of failover events. Switch to Higher Priority Security Gateway means that if the lower priority member has control and the higher priority member is restored, then control will be returned to the higher priority member. This mode is recommended if one member is better equipped for handling connections, so it will be the default Security Gateway.

Reference: http://dl3.checkpoint.com/paid/7e/7ef174cf00762ceaf228384ea20ea64a/
CP_R77_ClusterXL_AdminGuide.pdf? HashKey=1479822138_31410b1f8360074be87fd8f1ab682464andxtn=.pdf

QUESTION 14

Fill in the blank: To build an effective Security Policy, use a _____ and _____ rule.

A. Cleanup; stealth

B. Stealth; implicit

C. Cleanup; default

D. Implicit; explicit

Correct Answer: A

QUESTION 15

Fill in the blank: RADIUS protocol uses _____ to communicate with the gateway.

A. UDP

B. TDP

C. CCP

D. HTTP

Correct Answer: A

Parameters:

Parameter	Description
port	UDP port on the RADIUS server. This value must match the port as configured on the RADIUS server. Typically this 1812 (default) or 1645 (non-standard but a commonly used alternative).

Reference: https://sc1.checkpoint.com/documents/R76SP/
CP_R76SP_Security_System_WebAdminGuide/105209.htm

[Latest 156-215.80 Dumps](#)   [156-215.80 PDF Dumps](#)   [156-215.80 VCE Dumps](#)