DUMPSARENA

Check Point Certified Security Expert UpdateR80.10

Checkpoint 156-915.80

Version Demo

Total Demo Questions: 15

Total Premium Questions: 303

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Main Questions	99
Topic 2, Exam Pool A	100
Topic 3, Exam Pool B	104
Total	303

QUESTION NO: 1

What API command below creates a new host with the name “New Host” and IP address of “192.168.0.10”?

A. new host name “New Host” ip-address “192.168.0.10”

B. set host name “New Host” ip-address “192.168.0.10”

C. create host name “New Host” ip-address “192.168.0.10”

D. add host name “New Host” ip-address “192.168.0.10”

ANSWER: D

Explanation:

Sample Command with SmartConsole CLI You can use the add host command to create a new host and then publish the changes. > add host name "Sample_Host" ip-address "192.0.2.3" > publish

References:

QUESTION NO: 2

Several Security Policies can be used for different installation targets. The Firewall protecting Human Resources’ servers should have its own Policy Package. These rules must be installed on this machine and not on the Internet Firewall. How can this be accomplished?

A. A Rule Base is always installed on all possible targets. The rules to be installed on a Firewall are defined by the selection in the Rule Base row Install On.

B. When selecting the correct Firewall in each line of the Rule Base row Install On, only this Firewall is shown in the list of possible installation targets after selecting Policy > Install on Target.

C. In the menu of SmartDashboard, go to Policy > Policy Installation Targets and select the correct firewall via Specific Targets.

D. A Rule Base can always be installed on any Check Point Firewall object. It is necessary to select the appropriate target directly after selecting Policy > Install on Target.

ANSWER: C

QUESTION NO: 3

Check Point recommends configuring Disk Space Management parameters to delete old log entities when available disk space is less than or equal to?

A. 50%

B. 75%

C. 80%

D. 15%

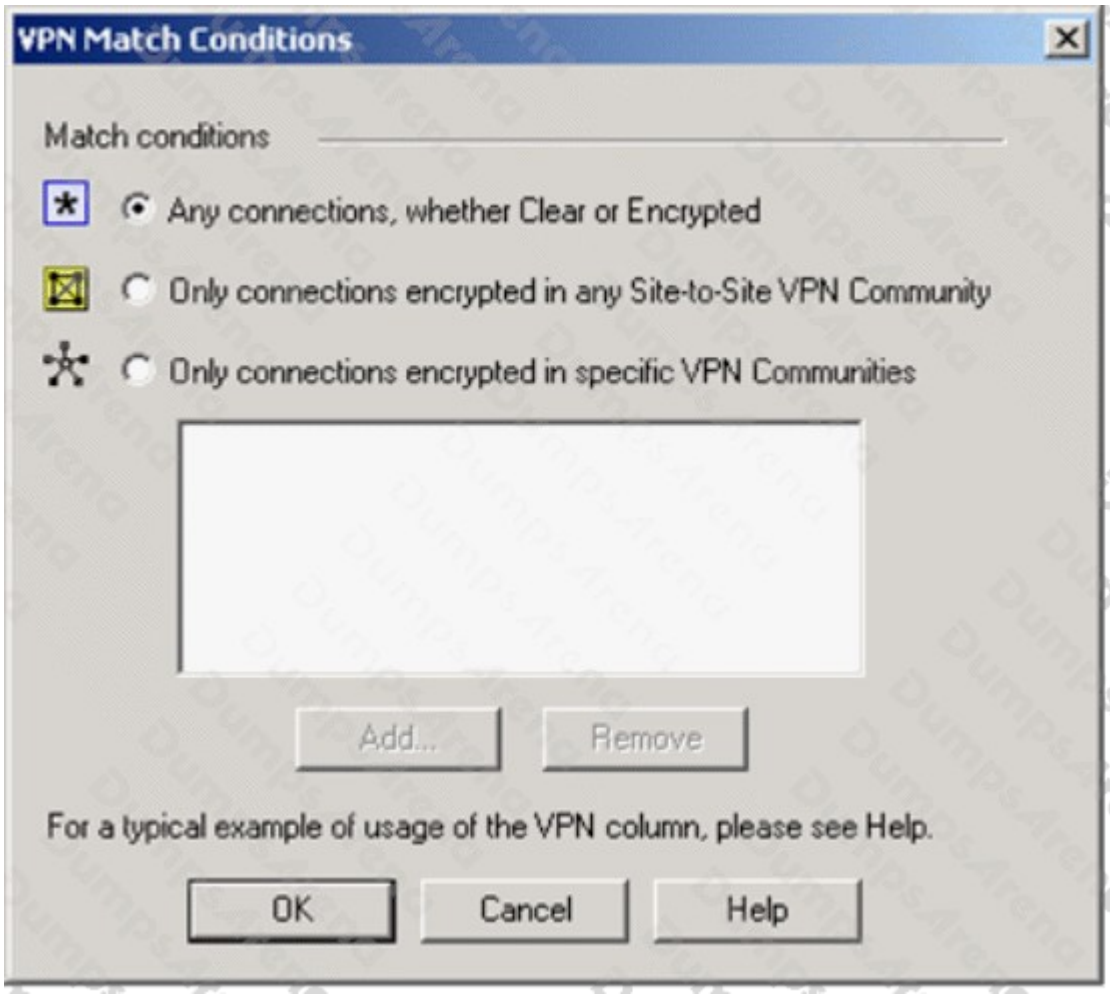
ANSWER: D

Explanation:

References:

QUESTION NO: 4

You are trying to configure Directional VPN Rule Match in the Rule Base. But the Match column does not have the option to see the Directional Match. You see the following window.



What must you enable to see the Directional Match?

A. directional_match(true) in the objects_5_0.C file on Security Management Server

B. VPN Directional Match on the Gateway object's VPN tab

C. VPN Directional Match on the VPN advanced window, in Global Properties

D. Advanced Routing on each Security Gateway

ANSWER: C

QUESTION NO: 5

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to a set of designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.

He has received a new laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop with a static IP (10.0.0.19).

He wants to move around the organization and continue to have access to the HR Web Server. To make this scenario work, the IT administrator:

1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources, and installs the policy.

2) Adds an access role object to the Firewall Rule Base that lets John Adams access the HR Web Server from any machine and from any location and installs policy.

John plugged in his laptop to the network on a different network segment and was not able to connect to the HR Web server. What is the next BEST troubleshooting step?

A. Investigate this as a network connectivity issue

B. Install the Identity Awareness Agent

C. Set static IP to DHCP

D. After enabling Identity Awareness, reboot the gateway

ANSWER: C

QUESTION NO: 6

Which process should you debug if SmartDashboard login fails?

A. sdm

B. cpd

C. fwd

D. fwm

ANSWER: D

QUESTION NO: 7

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap

B. Mail, Block Source, Block Destination, Block Services, SNMP Trap

C. Mail, Block Source, Block Destination, External Script, SNMP Trap

D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

ANSWER: A

Explanation:

These are the types of Automatic Reactions:

References:

QUESTION NO: 8

Which file gives you a list of all security servers in use, including port number?

A. $FWDIR/conf/conf.conf

B. $FWDIR/conf/servers.conf

C. $FWDIR/conf/fwauthd.conf

D. $FWDIR/conf/serversd.conf

ANSWER: C

QUESTION NO: 9

All R80 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

A. FTP

B. SMTP

C. HTTP

D. RLOGIN

ANSWER: B

QUESTION NO: 10

The Identity Agent is a lightweight endpoint agent that authenticates securely with Single Sign-On (SSO). What is not a recommended usage of this method?

A. When accuracy in detecting identity is crucial

B. Leveraging identity for Data Center protection

C. Protecting highly sensitive servers

D. Identity based enforcement for non-AD users (non-Windows and guest users)

ANSWER: D

QUESTION NO: 11

Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

A. Export R80 configuration, clean install R80.10 and import the configuration

B. CPUSE online upgrade

C. CPUSE offline upgrade

D. SmartUpdate upgrade

ANSWER: C

QUESTION NO: 12

You are investigating issues with two gateway cluster members that are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?

A. TCP port 443

B. TCP port 257

C. TCP port 256

D. UDP port 8116

ANSWER: C

Explanation:

Synchronization works in two modes:

Full sync is used for initial transfers of state information, for many thousands of connections. If a cluster member is brought up after being down, it will perform full sync. After all members are synchronized, only updates are transferred via delta sync. Delta sync is quicker than full sync.

References:

QUESTION NO: 13

Users with Identity Awareness Agent installed on their machines login with _____, so that when the user logs into the domain, that information is also used to meet Identity Awareness credential requests.

A. Key-logging

B. ICA Certificates

C. SecureClient

D. Single Sign-On

ANSWER: D

QUESTION NO: 14

Select the command set best used to verify proper failover function of a new ClusterXL configuration.

A. reboot

B. cphaprob -d failDevice -s problem -t 0 register / cphaprob -d failDevice unregister

C. clusterXL_admin down / clusterXL_admin up

D. cpstop/cpstart

ANSWER: C

QUESTION NO: 15

You just installed a new Web server in the DMZ that must be reachable from the Internet. You create a manual Static NAT rule as follows:

Source: Any || Destination: web_public_IP || Service: Any || Translated Source: original || Translated Destination: web_private_IP || Service: Original

“web_public_IP” is the node object that represents the new Web server’s public IP address. “web_private_IP” is the node object that represents the new Web site’s private IP address. You enable all settings from Global Properties > NAT.

When you try to browse the Web server from the Internet you see the error “page cannot be displayed”. Which of the following is NOT a possible reason?

A. There is no Security Policy defined that allows HTTP traffic to the protected Web server.

B. There is no ARP table entry for the protected Web server’s public IP address.

C. There is no route defined on the Security Gateway for the public IP address to the Web server’s private IP address.

D. There is no NAT rule translating the source IP address of packets coming from the protected Web server.

ANSWER: D