DUMPSARENA

Check Point Certified Security Expert Update

Checkpoint 156-915.77

Version Demo

Total Demo Questions: 15

Total Premium Questions: 203

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Deployment Platforms Obj 1	14
Topic 2, Deployment Platforms Obj 2	16
Topic 3, Deployment Platforms Obj 3	11
Topic 4, Network Address Translation	23
Topic 5, User Managment and Authentication Obj 1	12
Topic 6, User Managment and Authentication Obj 2	6
Topic 7, Identity Awareness Obj 1	7
Topic 8, Identity Awareness Obj 2	6
Topic 9, Identity Awareness Obj 3	4
Topic 10, Identity Awareness Obj 4	14
Topic 11, Advanced Firewall	9
Topic 12, Advanced upgrading	13
Topic 13, Advanced User Management	15
Topic 14, Advanced Clustering and Acceleration	27
Topic 15, IPSEC VPN and Remote Access	14
Topic 16, SmartReporting and SmartEvent	12
Total	203

QUESTION NO: 1

If Jack was concerned about the number of log entries he would receive in the

SmartReporter system, which policy would he need to modify?

A. Log Sequence Policy

B. Report Policy

C. Log Consolidator Policy

D. Consolidation Policy

ANSWER: D

QUESTION NO: 2

You have three servers located in a DMZ, using private IP addresses. You want internal users from 10.10.10.x to access the DMZ servers by public IP addresses. Internal_net

10.10.10.x is configured for Hide NAT behind the Security Gateway's external interface.

What is the best configuration for 10.10.10.x users to access the DMZ servers, using the

DMZ servers' public IP addresses?

A. When connecting to internal network 10.10.10.x, configure Hide NAT for the DMZ network behind the Security Gateway DMZ interface.

B. When the source is the internal network 10.10.10.x, configure manual static NAT rules to translate the DMZ servers.

C. When connecting to the Internet, configure manual Static NAT rules to translate the DMZ servers.

D. When trying to access DMZ servers, configure Hide NAT for 10.10.10.x behind the DMZ's interface.

ANSWER: B

QUESTION NO: 3

As a Security Administrator, you must refresh the Client Authentication authorization timeout every time a new user connection is authorized. How do you do this? Enable the

Refreshable Timeout setting:

A. in the user object's Authentication screen.

B. in the Gateway object's Authentication screen.

C. in the Limit tab of the Client Authentication Action Properties screen.

D. in the Global Properties Authentication screen.

ANSWER: C

QUESTION NO: 4

When migrating the SmartEvent data base from one server to another, the last step is to save the files on the new server. Which of the following commands should you run to save the SmartEvent data base files on the new server?

A. cp

B. restore

C. migrate import

D. eva_db_restore

ANSWER: D

QUESTION NO: 5

A Web server behind the Security Gateway is set to Automatic Static NAT. Client side NAT is not checked in the Global Properties. A client on the Internet initiates a session to the Web Server. Assuming there is a rule allowing this traffic, what other configuration must be done to allow the traffic to reach the Web server?

A. Automatic ARP must be unchecked in the Global Properties.

B. Nothing else must be configured.

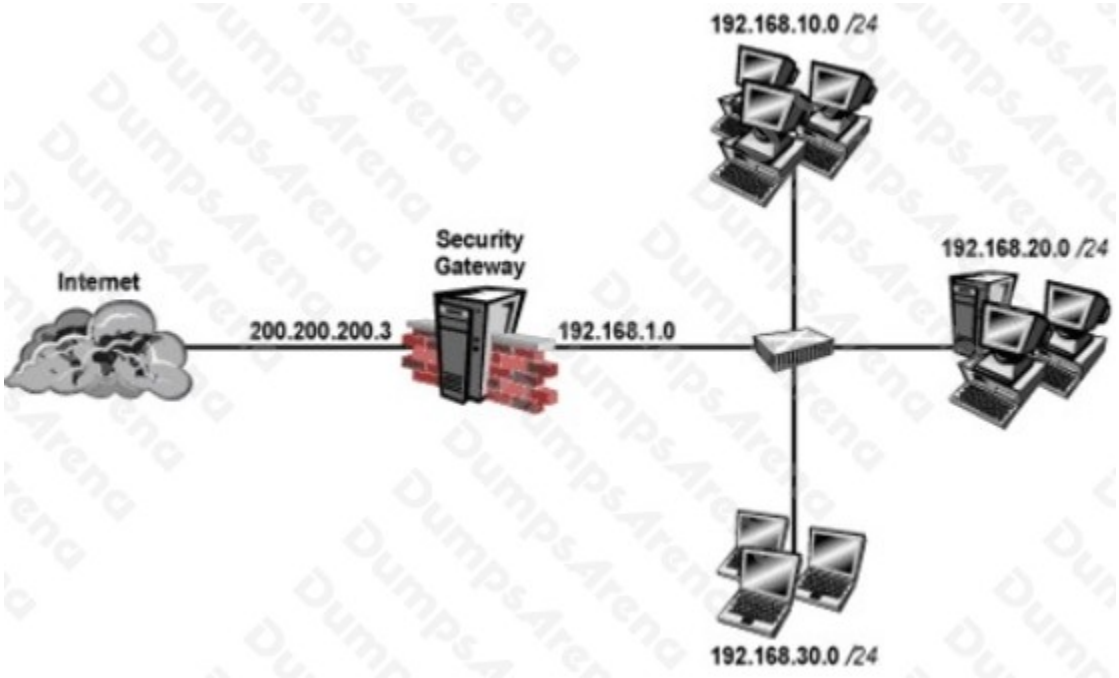
C. A static route must be added on the Security Gateway to the internal host.

D. A static route for the NAT IP must be added to the Gateway's upstream router.

ANSWER: C

QUESTION NO: 6

Your perimeter Security Gateway's external IP is 200.200.200.3. Your network diagram shows:



Required: Allow only network 192.168.10.0 and 192.168.20.0 to go out to the Internet, using 200.200.200.5.

The local network 192.168.1.0/24 needs to use 200.200.200.3 to go out to the Internet.

Assuming you enable all the settings in the NAT page of Global Properties, how could you achieve these requirements?

A. Create network objects for 192.168.10.0/24 and 192.168.20.0/24. Enable Hide NAT on both network objects, using 200.200.200.5 as hiding IP address. Add an ARP entry for 200.200.200.3 for the MAC address of 200.200.200.5.

B. Create an Address Range object, starting from 192.168.10.1 to 192.168.20.254. Enable
Hide NAT on the NAT page of the address range object. Enter Hiding IP address 200.200.200.5. Add an ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.

C. Create a network object 192.168.0.0/16. Enable Hide NAT on the NAT page. Enter 200.200.200.5 as the hiding IP address. Add an ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.

D. Create two network objects: 192.168.10.0/24 and 192.168.20.0/24. Add the two network objects to a group object. Create a manual NAT rule like the following: Original source group object; Destination - any; Service - any; Translated source - 200.200.200.5;
Destination - original; Service - original.

ANSWER: B

QUESTION NO: 7

Captive Portal is a _____ that allows the gateway to request login information from the user.

A. Pre-configured and customizable web-based tool

B. Transparent network inspection tool

C. LDAP server add-on

D. Separately licensed feature

ANSWER: A

QUESTION NO: 8

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: 9

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

QUESTION NO: 10

Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client

Authentication rule in R77?

A. External-user group

B. LDAP group

C. A group with a generic user

D. All Users

ANSWER: B

QUESTION NO: 11

Which three of the following are ClusterXL member requirements?

1) same operating systems

2) same Check Point version

3) same appliance model

4) same policy

A. 1, 3, and

B. 1, 2, and

C. 2, 3, and

D. 1, 2, and 3

ANSWER: B

QUESTION NO: 12

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: 13

SmartReporter reports can be used to analyze data from a penetration-testing regimen in all of the following examples, EXCEPT:

A. Analyzing traffic patterns against public resources.

B. Possible worm/malware activity.

C. Analyzing access attempts via social-engineering.

D. Tracking attempted port scans.

ANSWER: C

QUESTION NO: 14

Your R77 primary Security Management Server is installed on GAiA. You plan to schedule the Security Management Server to run fw logswitch automatically every 48 hours. How do you create this schedule?

A. On a GAiA Security Management Server, this can only be accomplished by configuring the command fw logswitch via the cron utility.

B. Create a time object, and add 48 hours as the interval. Open the primary Security Management Server object's Logs and Masters window, enable Schedule log switch, and select the Time object.

C. Create a time object, and add 48 hours as the interval. Open the Security Gateway object's Logs and Masters window, enable Schedule log switch, and select the Time object.

D. Create a time object, and add 48 hours as the interval. Select that time object's Global Properties > Logs and Masters window, to schedule a logswitch.

ANSWER: B

QUESTION NO: 15

You have selected the event Port Scan from Internal Network in SmartEvent, to detect an event when 30 port scans have occurred within 60 seconds. You also want to detect two port scans from a host within 10 seconds of each other. How would you accomplish this?

A. Define the two port-scan detections as an exception.

B. You cannot set SmartEvent to detect two port scans from a host within 10 seconds of each other.

C. Select the two port-scan detections as a sub-event.

D. Select the two port-scan detections as a new event.

ANSWER: A