Vendor: Check Point

Exam Code: 156-215.77

Exam Name: Check Point Certified Security Administrator

Version: Demo

DEMO

QUESTION 1
Your organization's disaster recovery plan needs an update to the backup and restore section to reap the new distributed R77 installation benefits. Your plan must meet the following required and desired objectives:

Required ObjectivE. The Security Policy repository must be backed up no less frequently than every 24

▪

hours.
Desired ObjectivE. The R77 components that enforce the Security Policies should be backed up at

▪

least once a week.
Desired ObjectivE. Back up R77 logs at least once a week.

▪

Your disaster recovery plan is as follows:
- Use the cron utility to run the command upgrade_export each night on the Security Management Servers.
- Configure the organization's routine back up software to back up the files created by the command upgrade_export.
- Configure the GAiA back up utility to back up the Security Gateways every Saturday night.
- Use the cron utility to run the command upgrade_export each Saturday night on the log servers.
- Configure an automatic, nightly logswitch.
- Configure the organization's routine back up software to back up the switched logs every night.

Upon evaluation, your plan:

A. Meets the required objective and only one desired objective.
B. Meets the required objective but does not meet either desired objective.
C. Does not meet the required objective.
D. Meets the required objective and both desired objectives.

Correct Answer: D

QUESTION 2
Which Check Point address translation method allows an administrator to use fewer ISP- assigned IP addresses than the number of internal hosts requiring Internet connectivity?

A. Hide
B. Static Destination
C. Static Source
D. Dynamic Destination

Correct Answer: A

QUESTION 3
An internal host initiates a session to the Google.com website and is set for Hide NAT behind the Security Gateway. The initiating traffic is an example of _____.

A. client side NAT
B. source NAT
C. destination NAT
D. None of these

Correct Answer: B

QUESTION 4

Secure Internal Communications (SIC) is completely NAT-tolerant because it is based on:

A. IP addresses.
B. SIC is not NAT-tolerant.
C. SIC names.
D. MAC addresses.

Correct Answer: C

QUESTION 5
You have configured Automatic Static NAT on an internal host-node object. You clear the box Translate destination on client site from Global Properties > NAT. Assuming all other NAT settings in Global Properties are selected, what else must be configured so that a host on the Internet can initiate an inbound connection to this host?

A. No extra configuration is needed.
B. A proxy ARP entry, to ensure packets destined for the public IP address will reach the Security Gateway's external interface.
C. The NAT IP address must be added to the external Gateway interface anti-spoofing group.
D. A static route, to ensure packets destined for the public NAT IP address will reach the Gateway's internal interface.

Correct Answer: D

QUESTION 6
You receive a notification that long-lasting Telnet connections to a mainframe are dropped after an hour of inactivity. Reviewing SmartView Tracker shows the packet is dropped with the error:
Unknown established connection
How do you resolve this problem without causing other security issues? Choose the BEST answer.

A. Increase the service-based session timeout of the default Telnet service to 24-hours.
B. Ask the mainframe users to reconnect every time this error occurs.
C. Increase the TCP session timeout under Global Properties > Stateful Inspection.
D. Create a new TCP service object on port 23 called Telnet-mainframe. Define a service-based session timeout of 24-hours. Use this new object only in the rule that allows the Telnet connections to the mainframe.

Correct Answer: D

QUESTION 7
Your shipping company uses a custom application to update the shipping distribution database. The custom application includes a service used only to notify remote sites that the distribution database is malfunctioning. The perimeter Security Gateway's Rule Base includes a rule to accept this traffic. Since you are responsible for multiple sites, you want notification by a text message to your cellular phone, whenever traffic is accepted on this rule. Which of the following would work BEST for your purpose?

A. Logging implied rules
B. User-defined alert script
C. SNMP trap
D. SmartView Monitor Threshold

Correct Answer: B

QUESTION 8
As a Security Administrator, you must refresh the Client Authentication authorization time-out 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.

Correct Answer: C

QUESTION 9
All R77 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

Correct Answer: B

QUESTION 10
In the Rule Base displayed, user authentication in Rule 4 is configured as fully automatic. Eric is a member of the LDAP group, MSD_Group.

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

What happens when Eric tries to connect to a server on the Internet?

A. None of these things will happen.
B. Eric will be authenticated and get access to the requested server.
C. Eric will be blocked because LDAP is not allowed in the Rule Base.
D. Eric will be dropped by the Stealth Rule.

Correct Answer: B

QUESTION 11
How many packets does the IKE exchange use for Phase 1 Main Mode?

A. 12
B. 1
C. 3
D. 6

Correct Answer: D

QUESTION 12
You have included the Cleanup Rule in your Rule Base. Where in the Rule Base should the Accept ICMP Requests implied rule have no effect?

A. Last
B. After Stealth Rule
C. First
D. Before Last

Correct Answer: A

QUESTION 13
Several Security Policies can be used for different installation targets. The firewall protecting Human Resources' servers should have a unique Policy Package. These rules may only be installed on this machine and not accidentally on the Internet firewall. How can this be configured?

A. When selecting the correct firewall in each line of the row Install On of the Rule Base, only this firewall is shown in the list of possible installation targets after selecting Policy > Install.
B. 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.
C. In the SmartDashboard policy, select the correct firewall to be the Specific Target of the rule.
D. 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 row Install On of the Rule Base.

Correct Answer: C

QUESTION 14
MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. How do you apply the license?

A. Using the remote Gateway's IP address, and attaching the license to the remote Gateway via SmartUpdate.
B. Using your Security Management Server's IP address, and attaching the license to the remote Gateway via SmartUpdate.
C. Using the remote Gateway's IP address, and applying the license locally with the command cplic put.
D. Using each of the Gateways' IP addresses, and applying the licenses on the Security Management Server with the command cprlic put.

Correct Answer: B

QUESTION 15
How do you configure the Security Policy to provide user access to the Captive Portal through an external (Internet) interface?

A. Change the gateway settings to allow Captive Portal access via an external interface.
B. No action is necessary. This access is available by default.
C. Change the Identity Awareness settings under Global Properties to allow Captive Portal access on all interfaces.
D. Change the Identity Awareness settings under Global Properties to allow Captive Portal access for an external interface.

Correct Answer: A

QUESTION 16
What gives administrators more flexibility when configuring Captive Portal instead of LDAP query for Identity Awareness authentication?

A. Captive Portal is more secure than standard LDAP
B. Nothing, LDAP query is required when configuring Captive Portal
C. Captive Portal works with both configured users and guests
D. Captive Portal is more transparent to the user

Correct Answer: C

QUESTION 17
ALL of the following options are provided by the GAiA sysconfig utility, EXCEPT:

A. Export setup
B. DHCP Server configuration
C. Time & Date
D. GUI Clients

Correct Answer: D

QUESTION 18
How do you recover communications between your Security Management Server and Security Gateway if you lock yourself out through a rule or policy mis-configuration?

A. fw unload policy
B. fw unloadlocal
C. fw delete all.all@localhost
D. fwm unloadlocal

Correct Answer: B

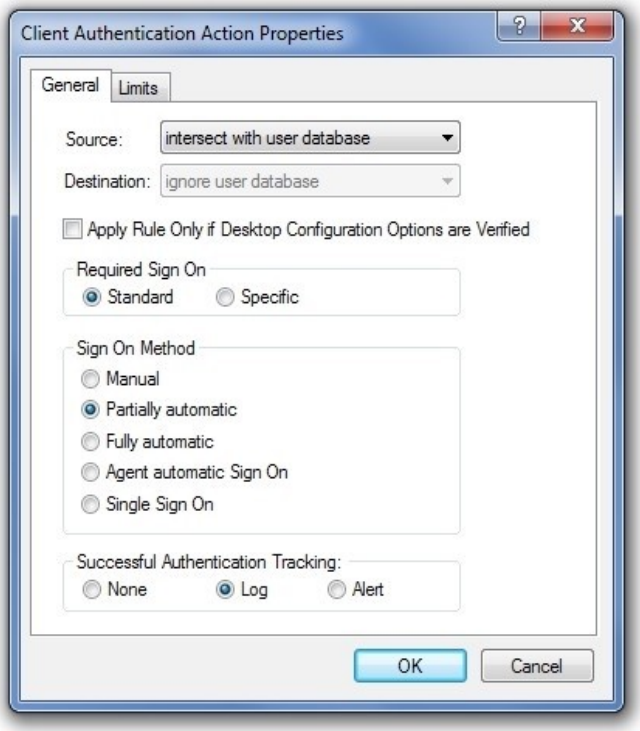
QUESTION 19
Which of the following objects is a valid source in an authentication rule?

A. Host@Any
B. User@Network
C. User_group@Network
D. User@Any

Correct Answer: C

QUESTION 20
Study the Rule base and Client Authentication Action properties screen -

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	TCP http TCP ftp TCP telnet	Client Aut	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	drop	Log	Policy Targets



After being authenticated by the Security Gateway, when a user starts an HTTP connection to a Web site, the user tries to FTP to another site using the command line. What happens to the user?

A. user is prompted for authentication by the Security Gateway again.
B. FTP data connection is dropped after the user is authenticated successfully.
C. user is prompted to authenticate from that FTP site only, and does not need to enter his username and password for Client Authentication.
D. FTP connection is dropped by Rule 2.

Correct Answer: C

QUESTION 21
Which port must be allowed to pass through enforcement points in order to allow packet logging to operate correctly?

A. 514
B. 257
C. 256
D. 258

Correct Answer: B

QUESTION 22
True or FalsE. SmartView Monitor can be used to create alerts on a specified Gateway.

A. True, by right-clicking on the Gateway and selecting Configure Thresholds.
B. True, by choosing the Gateway and selecting System Information.
C. False, an alert cannot be created for a specified Gateway.
D. False, alerts can only be set in SmartDashboard Global Properties.

Correct Answer: A

QUESTION 23
What is a Consolidation Policy?

A. The collective name of the Security Policy, Address Translation, and IPS Policies.
B. The specific Policy written in SmartDashboard to configure which log data is stored in the SmartReporter database.
C. The collective name of the logs generated by SmartReporter.
D. A global Policy used to share a common enforcement policy for multiple Security Gateways.

Correct Answer: B

QUESTION 24
When attempting to connect with SecureClient Mobile you get the following error message:

The certificate provided is invalid. Please provide the username and password.

What is the probable cause of the error?

A. Your user configuration does not have an office mode IP address so the connection failed.
B. Your certificate is invalid.
C. There is no connection to the server, and the client disconnected.
D. Your user credentials are invalid.

Correct Answer: B

QUESTION 25
Which of the following are available SmartConsole clients which can be installed from the R77 Windows CD? Read all answers and select the most complete and valid list.

A. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
C. SmartView Tracker, CPINFO, SmartUpdate
D. Security Policy Editor, Log Viewer, Real Time Monitor GUI

Correct Answer: C

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

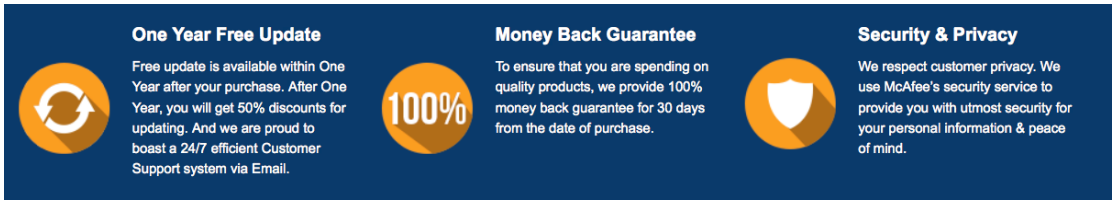
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions