Exam Questions 156-215.77

Check Point Certified Security Administrator – GAiA

https://www.2passeasy.com/dumps/156-215.77/

NEW QUESTION 1
How do you view a Security Administrator's activities with SmartConsole?

A. Eventia Suite
B. SmartView Monitor using the Administrator Activity filter
C. SmartView Tracker in the Management tab
D. SmartView Tracker in the Network and Endpoint tabs

Answer: C

NEW QUESTION 2
You are responsible for the configuration of MegaCorp's Check Point Firewall. You need to allow two NAT rules to match a connection. Is it possible? Give the BEST answer.

A. No, it is not possible to have more than one NAT rule matching a connectio
B. When the firewall receives a packet belonging to a connection, it compares it against the first rule in the Rule Base, then the second rule, and so o
C. When it finds a rule that matches, it stops checking and applies that rule.
D. Yes, it is possible to have two NAT rules which match a connection, but only in using Manual NAT (bidirectional NAT).
E. Yes, there are always as many active NAT rules as there are connections.
F. Yes, it is possible to have two NAT rules which match a connection, but only when using Automatic NAT (bidirectional NAT).

Answer: D

NEW QUESTION 3
How can you configure an application to automatically launch on the Security Management Server when traffic is dropped or accepted by a rule in the Security Policy?

A. SNMP trap alert script
B. Custom scripts cannot be executed through alert scripts.
C. User-defined alert script
D. Pop-up alert script

Answer: C

NEW QUESTION 4
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

Answer: B

NEW QUESTION 5
The customer has a small Check Point installation which includes one Windows 7 workstation as the SmartConsole, one GAiA device working as Security Management Server, and a third server running SecurePlatform as Security Gateway. This is an example of a(n):

A. Hybrid Installation
B. Unsupported configuration
C. Stand-Alone Installation
D. Distributed Installation

Answer: D

NEW QUESTION 6
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.

Answer: D

NEW QUESTION 7
You want to implement Static Destination NAT in order to provide external, Internet users access to an internal Web Server that has a reserved (RFC 1918) IP address. You have an unused valid IP address on the network between your Security Gateway and ISP router. You control the router that sits between the firewall external interface and the Internet.
What is an alternative configuration if proxy ARP cannot be used on your Security Gateway?

A. Publish a proxy ARP entry on the ISP router instead of the firewall for the valid IP address.
B. Place a static ARP entry on the ISP router for the valid IP address to the firewall's external address.

C. Publish a proxy ARP entry on the internal Web server instead of the firewall for the valid IP address.
D. Place a static host route on the firewall for the valid IP address to the internal Web server.

Answer: B

NEW QUESTION 8
Which utility allows you to configure the DHCP service on GAiA from the command line?

A. ifconfig
B. sysconfig
C. cpconfig
D. dhcp_cfg

Answer: B

NEW QUESTION 9
Which of the following can be found in cpinfo from an enforcement point?

A. Everything NOT contained in the file r2info
B. VPN keys for all established connections to all enforcement points
C. The complete file objects_5_0.c
D. Policy file information specific to this enforcement point

Answer: D

NEW QUESTION 10
Which feature or command provides the easiest path for Security Administrators to revert to earlier versions of the same Security Policy and objects configuration?

A. Database Revision Control
B. Policy Package management
C. dbexport/dbimport
D. upgrade_export/upgrade_import

Answer: A

NEW QUESTION 10
Your bank's distributed R77 installation has Security Gateways up for renewal.
Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

A. SmartView Tracker
B. SmartPortal
C. SmartUpdate
D. SmartDashboard

Answer: C

NEW QUESTION 11
The customer has a small Check Point installation which includes one Windows 2008 server as SmartConsole and Security Management Server with a second server running GAiA as Security Gateway. This is an example of a(n):

A. Stand-Alone Installation.
B. Distributed Installation.
C. Unsupported configuration.
D. Hybrid Installation.

Answer: B

NEW QUESTION 16
Which of the following commands can provide the most complete restoration of a R77 configuration?

A. upgrade_import
B. cpinfo -recover
C. cpconfig
D. fwm dbimport -p <export file>

Answer: A

NEW QUESTION 20
The customer has a small Check Point installation which includes one Windows 2008 server as the SmartConsole and a second server running GAiA as both Security Management Server and the Security Gateway. This is an example of a(n):

A. Distributed Installation
B. Unsupported configuration
C. Hybrid Installation
D. Stand-Alone Installation

Answer: D

NEW QUESTION 24
NAT can NOT be configured on which of the following objects?

A. HTTP Logical Server
B. Gateway
C. Address Range
D. Host

Answer: A

NEW QUESTION 28
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

A. None, Security Management Server would be installed by itself.
B. SmartConsole
C. SecureClient
D. Security Gateway

Answer: D

NEW QUESTION 32
Because of pre-existing design constraints, you set up manual NAT rules for your HTTP server. However, your FTP server and SMTP server are both using automatic NAT rules. All traffic from your FTP and SMTP servers are passing through the Security Gateway without a problem, but traffic from the Web server is dropped on rule 0 because of anti- spoofing settings.
What is causing this?

A. Manual NAT rules are not configured correctly.
B. Allow bi-directional NAT is not checked in Global Properties.
C. Routing is not configured correctly.
D. Translate destination on client side is not checked in Global Properties under Manual NAT Rules.

Answer: D

NEW QUESTION 33
When using GAiA, it might be necessary to temporarily change the MAC address of the interface eth 0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?

```
# IP link set eth0 down
# IP link set eth0 addr 00:0C:29:12:34:56
# IP link set eth0 up
```

As expert user, issue these commands:

```
(conf
:(conns
      :(conn
            :hwaddr ("00:0C:29:12:34:56")
```

A. Edit the file /etc/sysconfig/netconf.C and put the new MAC address in the field
B. As expert user, issue the command:
C. # IP link set eth0 addr 00:0C:29:12:34:56
D. Open the WebUI, select Network > Connections > eth0. Place the new MAC address in the field Physical Address, and press Apply to save the settings.

Answer: C

NEW QUESTION 34
What is the default setting when you use NAT?

A. Destination Translated on Server side
B. Destination Translated on Client side
C. Source Translated on both sides
D. Source Translated on Client side

Answer: B

NEW QUESTION 36
After implementing Static Address Translation to allow Internet traffic to an internal Web Server on your DMZ, you notice that any NATed connections to that machine are being dropped by anti-spoofing protections. Which of the following is the MOST LIKELY cause?

A. The Global Properties setting Translate destination on client side is unchecke
B. But the topology on the DMZ interface is set to Internal - Network defined by IP and Mas
C. Check the Global Properties setting Translate destination on client side.
D. The Global Properties setting Translate destination on client side is unchecke
E. But the topology on the external interface is set to Others +. Change topology to External.
F. The Global Properties setting Translate destination on client side is checke
G. But the topology on the external interface is set to Externa

H. Change topology to Others +.
I. The Global Properties setting Translate destination on client side is checke
J. But the topology on the DMZ interface is set to Internal - Network defined by IP and Mas
K. Uncheck the Global Properties setting Translate destination on client side.

Answer: A

NEW QUESTION 41
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.

Answer: C

NEW QUESTION 43
Which NAT option applicable for Automatic NAT applies to Manual NAT as well?

A. Allow bi-directional NAT
B. Automatic ARP configuration
C. Translate destination on client-side
D. Enable IP Pool NAT

Answer: C

NEW QUESTION 48
Tom has been tasked to install Check Point R77 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

A. Three machines
B. One machine
C. Two machines
D. One machine, but it needs to be installed using SecurePlatform for compatibility purposes

Answer: C

NEW QUESTION 53
You enable Automatic Static NAT on an internal host node object with a private IP address of 10.10.10.5, which is NATed into 216.216.216.5. (You use the default settings in Global Properties / NAT.)
When you run fw monitor on the R77 Security Gateway and then start a new HTTP connection from host 10.10.10.5 to browse the Internet, at what point in the monitor output will you observe the HTTP SYN-ACK packet translated from 216.216.216.5 back into 10.10.10.5?

A. o=outbound kernel, before the virtual machine
B. I=inbound kernel, after the virtual machine
C. O=outbound kernel, after the virtual machine
D. i=inbound kernel, before the virtual machine

Answer: B

NEW QUESTION 54
Where is the easiest and BEST place to find information about connections between two machines?

A. All options are valid.
B. On a Security Gateway using the command fw log.
C. On a Security Management Server, using SmartView Tracker.
D. On a Security Gateway Console interface; it gives you detailed access to log files and state table information.

Answer: C

NEW QUESTION 59
You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways.
Which two SmartConsole applications will you use to create this report and outline?

A. SmartView Tracker and SmartView Monitor
B. SmartLSM and SmartUpdate
C. SmartDashboard and SmartView Tracker
D. SmartView Monitor and SmartUpdate

Answer: D

NEW QUESTION 61

What is the officially accepted diagnostic tool for IP Appliance Support?

A. ipsoinfo
B. CST
C. uag-diag
D. cpinfo

Answer: D

NEW QUESTION 65
By default, when you click File > Switch Active File in SmartView Tracker, the Security Management Server:

A. Saves the current log file, names the log file by date and time, and starts a new log file.
B. Purges the current log file, and starts a new log file.
C. Prompts you to enter a filename, and then saves the log file.
D. Purges the current log file, and prompts you for the new log's mode.

Answer: A

NEW QUESTION 67
The third-shift Administrator was updating Security Management Server access settings in Global Properties. He managed to lock all administrators out of their accounts.
How should you unlock these accounts?

A. Delete the file admin.lock in the Security Management Server directory $FWDIR/tmp/.
B. Reinstall the Security Management Server and restore using upgrade_import.
C. Type fwm lock_admin -ua from the Security Management Server command line.
D. Login to SmartDashboard as the special cpconfig_admin user account; right-click on each administrator object and select unlock.

Answer: C

NEW QUESTION 71
Select the TRUE statements about the Rule Base shown? Exhibit:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None	Policy Targets
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	None	Policy Targets
3	0	Web Server	Any	webSingapore	Any Traffic	http	Client Aut	Log	Policy Targets
4	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log	Policy Targets
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	http	accept	Log	Policy Targets
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	http dns icmp-proto ftp https	accept	Log	Policy Targets
7	0	Network Traffic	webSydney	Any	Any Traffic	ftp	reject	Log	Policy Targets
8	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets

1) HTTP traffic from webrome to websingapore will be encrypted.
2) HTTP traffic from websingapore to webrome will be encrypted.
3) HTTP traffic from webrome to websingapore will be authenticated.
4) HTTP traffic from websingapore to webrome will be blocked.

A. 1, 2, and 3
B. 3 only
C. 2 and 3
D. 3 and 4

Answer: D

NEW QUESTION 76
You want to generate a cpinfo file via CLI on a system running GAiA. This will take about 40 minutes since the log files are also needed.
What action do you need to take regarding timeout?

A. No action is needed because cpshell has a timeout of one hour by default.
B. Log in as the default user expert and start cpinfo.
C. Log in as admin, switch to expert mode, set the timeout to one hour with the command, idle 60, then start cpinfo.
D. Log in as Administrator, set the timeout to one hour with the command idle 60 and start cpinfo.

Answer: D

NEW QUESTION 79
Which of the following statements BEST describes Check Point's Hide Network Address Translation method?

A. Translates many destination IP addresses into one destination IP address
B. One-to-one NAT which implements PAT (Port Address Translation) for accomplishing both Source and Destination IP address translation
C. Translates many source IP addresses into one source IP address
D. Many-to-one NAT which implements PAT (Port Address Translation) for accomplishing both Source and Destination IP address translation

Answer: C

NEW QUESTION 81
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

Answer: A

NEW QUESTION 86
Exhibit:

1. Simplified mode Rule Bases
2. Traditional mode Rule Bases
3. SecurePlatform WebUI Users
4. SIC certificates
5. SmartView Tracker audit logs
6. SmartView Tracker traffic logs
7. Implied Rules
8. IPS Profiles
9. Blocked connections
10. Manual NAT rules
11. VPN communities
12. Gateway route table
13. Gateway licenses

Of the following, what parameters will not be preserved when using Database Revision Control?

A. 2, 4, 7, 10, 11
B. 3, 4, 5, 6, 9, 12, 13
C. 5, 6, 9, 12, 13
D. 1, 2, 8, 10, 11

Answer: B

NEW QUESTION 91
While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?
1) Select Active Mode tab in SmartView Tracker.
2) Select Tools > Block Intruder.
3) Select Log Viewing tab in SmartView Tracker.
4) Set Blocking Timeout value to 60 minutes.
5) Highlight connection that should be blocked.

A. 1, 2, 5, 4
B. 3, 2, 5, 4
C. 1, 5, 2, 4
D. 3, 5, 2, 4

Answer: C

NEW QUESTION 96
Which R77 SmartConsole tool would you use to verify the installed Security Policy name on a Security Gateway?

A. SmartView Tracker
B. None, SmartConsole applications only communicate with the Security Management Server.
C. SmartView Server
D. SmartUpdate

Answer: A

NEW QUESTION 100
SmartView Tracker R77 consists of three different modes. They are:

A. Log, Active, and Audit
B. Log, Active, and Management
C. Network and Endpoint, Active, and Management
D. Log, Track, and Management

Answer: C

NEW QUESTION 103
Your company is running Security Management Server R77 on GAiA, which has been migrated through each version starting from Check Point 4.1.

How do you add a new administrator account?

A. Using SmartDashboard, under Users, select Add New Administrator
B. Using SmartDashboard or cpconfig
C. Using the Web console on GAiA under Product configuration, select Administrators
D. Using cpconfig on the Security Management Server, choose Administrators

Answer: A

NEW QUESTION 106
You can include External commands in SmartView Tracker by the menu Tools > Custom Commands.
The Security Management Server is running under GAiA, and the GUI is on a system running Microsoft Windows. How do you run the command traceroute on an IP address?

A. There is no possibility to expand the three pre-defined options Ping, Whois, and Nslookup.
B. Go to the menu Tools > Custom Commands and configure the Windows command tracert.exe to the list.
C. Use the program GUIdbedit to add the command traceroute to the Security Management Server properties.
D. Go to the menu, Tools > Custom Commands and configure the Linux command traceroute to the list.

Answer: B

NEW QUESTION 108
Peter is your new Security Administrator. On his first working day, he is very nervous and enters the wrong password three times. His account is locked.
What can be done to unlock Peter's account? Give the BEST answer.

A. You can unlock Peter's account by using the command fwm lock_admin -u Peter on the Security Management Server.
B. You can unlock Peter's account by using the command fwm unlock_admin -u Peter on the Security Management Server
C. It is not possible to unlock Peter's accoun
D. You have to install the firewall once again or abstain from Peter's help.
E. You can unlock Peter's account by using the command fwm unlock_admin -u Peter on the Security Gateway.

Answer: A

NEW QUESTION 110
Which SmartView Tracker mode allows you to read the SMTP e-mail body sent from the Chief Executive Officer (CEO) of a company?

A. This is not a SmartView Tracker feature.
B. Display Capture Action
C. Network and Endpoint Tab
D. Display Payload View

Answer: A

NEW QUESTION 114
You enable Hide NAT on the network object, 10.1.1.0 behind the Security Gateway's external interface. You browse to the Google Website from host, 10.1.1.10 successfully. You enable a log on the rule that allows 10.1.1.0 to exit the network.
How many log entries do you see for that connection in SmartView Tracker?

A. Two, one for outbound, one for inbound
B. Only one, outbound
C. Two, both outbound, one for the real IP connection and one for the NAT IP connection
D. Only one, inbound

Answer: B

NEW QUESTION 119
You have created a Rule Base for firewall, websydney. Now you are going to create a new policy package with security and address translation rules for a second Gateway. What is TRUE about the new package's NAT rules?
Exhibit:

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
1	websydney	Any	Any	websydney (Hid	Original	Original	fwsydney
2	net_singapore	net_singapore	Any	Original	Original	Original	All
3	net_singapore	Any	Any	net_singapore (H	Original	Original	All
4	Any	websydney	Any	Original	websydney	Original	Policy Targets
5	Any	websignapore	HTTP_and_HTTPS	Original	Original	http	Policy Targets

A. Rules 1, 2, 3 will appear in the new package.
B. Only rule 1 will appear in the new package.
C. NAT rules will be empty in the new package.
D. Rules 4 and 5 will appear in the new package.

Answer: A

NEW QUESTION 121
You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After awhile, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database.
How can you do this?

A. Run fwm dbexport -l filenam
B. Restore the databas
C. Then, run fwm dbimport -l filename to import the users.
D. Run fwm_dbexport to export the user databas
E. Select restore the entire database in the Database Revision scree
F. Then, run fwm_dbimport.
G. Restore the entire database, except the user database, and then create the new user and user group.
H. Restore the entire database, except the user database.

Answer: D

NEW QUESTION 124
You are MegaCorp's Security Administrator. There are various network objects which must be NATed. Some of them use the Automatic Hide NAT method, while others use the Automatic Static NAT method. What is the rule order if both methods are used together? Give the BEST answer.

A. The Administrator decides the rule order by shifting the corresponding rules up and down.
B. The Static NAT rules have priority over the Hide NAT rules and the NAT on a node has priority over the NAT on a network or an address range.
C. The Hide NAT rules have priority over the Static NAT rules and the NAT on a node has priority over the NAT on a network or an address range.
D. The rule position depends on the time of their creatio
E. The rules created first are placed at the top; rules created later are placed successively below the others.

Answer: B

NEW QUESTION 127
Which of these Security Policy changes optimize Security Gateway performance?

A. Using groups within groups in the manual NAT Rule Base.
B. Use Automatic NAT rules instead of Manual NAT rules whenever possible.
C. Using domain objects in rules when possible.
D. Putting the least-used rule at the top of the Rule Base.

Answer: B

NEW QUESTION 130
The fw monitor utility is used to troubleshoot which of the following problems?

A. Phase two key negotiation
B. Address translation
C. Log Consolidation Engine
D. User data base corruption

Answer: B

NEW QUESTION 132
You are about to test some rule and object changes suggested in an R77 news group.
Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

A. Manual copies of the directory $FWDIR/conf
B. upgrade_export command
C. Database Revision Control
D. GAiA backup utilities

Answer: C

NEW QUESTION 135
Where can an administrator configure the notification action in the event of a policy install time change?

A. SmartView Monitor > Gateways > Thresholds Settings
B. SmartView Monitor > Gateway Status > System Information > Thresholds
C. SmartDashboard > Policy Package Manager
D. SmartDashboard > Security Gateway Object > Advanced Properties Tab

Answer: A

NEW QUESTION 136
Which Check Point address translation method is necessary if you want to connect from a host on the Internet via HTTP to a server with a reserved (RFC 1918) IP address on your DMZ?

A. Dynamic Source Address Translation
B. Hide Address Translation
C. Port Address Translation

D. Static Destination Address Translation

Answer: D

NEW QUESTION 137
Identity Awareness is implemented to manage access to protected resources based on a user's .

A. Application requirement
B. Computer MAC address
C. Identity
D. Time of connection

Answer: C

NEW QUESTION 139
What type of traffic can be re-directed to the Captive Portal?

A. SMTP
B. HTTP
C. All of the above
D. FTP

Answer: B

NEW QUESTION 143
Which of the following is a viable consideration when determining Rule Base order?

A. Grouping rules by date of creation
B. Grouping reject and drop rules after the Cleanup Rule
C. Grouping authentication rules with address-translation rules
D. Grouping functionally related rules together

Answer: D

NEW QUESTION 144
When you change an implicit rule's order from Last to First in Global Properties, how do you make the change take effect?

A. Run fw fetch from the Security Gateway.
B. Select Install Database from the Policy menu.
C. Select Save from the File menu.
D. Reinstall the Security Policy.

Answer: D

NEW QUESTION 149
Security Gateway R77 supports User Authentication for which of the following services? Select the response below that contains the MOST correct list of supported services.

A. SMTP, FTP, TELNET
B. SMTP, FTP, HTTP, TELNET
C. FTP, HTTP, TELNET
D. FTP, TELNET

Answer: C

NEW QUESTION 154
Which of the following is a viable consideration when determining Rule Base order?

A. Placing frequently accessed rules before less frequently accessed rules
B. Grouping IPS rules with dynamic drop rules
C. Adding SAM rules at the top of the Rule Base
D. Grouping rules by date of creation

Answer: A

NEW QUESTION 156
Which of the below is the MOST correct process to reset SIC from SmartDashboard?

A. Run cpconfig, and click Reset.
B. Click the Communication button for the firewall object, then click Rese
C. Run cpconfig and type a new activation key.
D. Run cpconfig, and select Secure Internal Communication > Change One Time Password.
E. Click Communication > Reset on the Gateway object, and type a new activation key.

Answer: B

NEW QUESTION 158
Which SmartConsole component can Administrators use to track changes to the Rule Base?

A. WebUI
B. SmartView Tracker
C. SmartView Monitor
D. SmartReporter

Answer: B

NEW QUESTION 160
Which of the following are authentication methods that Security Gateway R77 uses to validate connection attempts? Select the response below that includes the MOST complete list of valid authentication methods.

A. Proxied, User, Dynamic, Session
B. Connection, User, Client
C. User, Client, Session
D. User, Proxied, Session

Answer: C

NEW QUESTION 163
Which rule is responsible for the installation failure? Exhibit:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None	Policy Targets
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	None	Policy Targets
3	0	Web Server	Any	webSingapore	Any Traffic	http	Client Aut	Log	Policy Targets
4	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log	Policy Targets
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	http	accept	Log	Policy Targets
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	http dns icmp-proto ftp https	accept	Log	Policy Targets
7	0	Network Traffic	webSydney	Any	Any Traffic	ftp	reject	Log	Policy Targets
8	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets

A. Rule 5
B. Rule 4
C. Rule 3
D. Rule 6

Answer: B

NEW QUESTION 164
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

NEW QUESTION 168
The SIC certificate is stored in the directory .

A. $CPDIR/registry
B. $CPDIR/conf
C. $FWDIR/database
D. $FWDIR/conf

Answer: B

NEW QUESTION 171
Which Security Gateway R77 configuration setting forces the Client Authentication authorization time-out to refresh, each time a new user is authenticated? The:

A. Time properties, adjusted on the user objects for each user, in the Client Authentication rule Source.
B. IPS > Application Intelligence > Client Authentication > Refresh User Timeout option enabled.
C. Refreshable Timeout setting, in Client Authentication Action Properties > Limits.
D. Global Properties > Authentication parameters, adjusted to allow for Regular Client Refreshment.

Answer: C

NEW QUESTION 173
A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway

object, the object does not appear in the Install On check box. What should you look for?

A. Secure Internal Communications (SIC) not configured for the object.
B. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.
C. Anti-spoofing not configured on the interfaces on the Gateway object.
D. A Gateway object created using the Check Point > Security Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

Answer: D

NEW QUESTION 176
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.

Answer: C

NEW QUESTION 181
Which of the following describes the default behavior of an R77 Security Gateway?

A. Traffic not explicitly permitted is dropped.
B. Traffic is filtered using controlled port scanning.
C. All traffic is expressly permitted via explicit rules.
D. IP protocol types listed as secure are allowed by default, i.
E. ICMP, TCP, UDP sessions are inspected.

Answer: A

NEW QUESTION 186
Which of the following is an authentication method used by Identity Awareness?

A. SSL
B. Captive Portal
C. RSA
D. PKI

Answer: B

NEW QUESTION 187
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.

Answer: B

NEW QUESTION 192
Which of the following is NOT a valid option when configuring access for Captive Portal?

A. From the Internet
B. Through internal interfaces
C. Through all interfaces
D. According to the Firewall Policy

Answer: A

NEW QUESTION 197
What is a possible reason for the IKE failure shown in this screenshot?

A. Mismatch in VPN Domains.
B. Mismatch in preshared secrets.
C. Mismatch in Diffie-Hellman group.
D. Mismatch in encryption schemes.

Answer: B

NEW QUESTION 198
A marketing firm's networking team is trying to troubleshoot user complaints regarding access to audio-streaming material from the Internet. The networking team asks you to check the object and rule configuration settings for the perimeter Security Gateway.
Which SmartConsole application should you use to check these objects and rules?

A. SmartView Tracker
B. SmartView Monitor
C. SmartView Status
D. SmartDashboard

Answer: D

NEW QUESTION 201
Which do you configure to give remote access VPN users a local IP address?

A. Encryption domain pool
B. NAT pool
C. Office mode IP pool
D. Authentication pool

Answer: C

NEW QUESTION 203
The technical-support department has a requirement to access an intranet server. When configuring a User Authentication rule to achieve this, which of the following should you remember?

A. You can only use the rule for Telnet, FTP, SMTP, and rlogin services.
B. The Security Gateway first checks if there is any rule that does not require authentication for this type of connection before invoking the Authentication Security Server.
C. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.
D. You can limit the authentication attempts in the User Properties' Authentication tab.

Answer: B

NEW QUESTION 204
Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE phase 2. Why is this a problematic setup?

A. The two algorithms do not have the same key length and so don't work togethe
B. You will get the error …. No proposal chosen….
C. All is fine as the longest key length has been chosen for encrypting the data and a shorter key length for higher performance for setting up the tunnel.
D. Only 128 bit keys are used for phase 1 keys which are protecting phase 2, so the longer key length in phase 2 only costs performance and does not add security due to a shorter key in phase 1.
E. All is fine and can be used as is.

Answer: C

NEW QUESTION 205
The INSPECT engine inserts itself into the kernel between which two OSI model layers?

A. Session and Transport
B. Physical and Data
C. Presentation and Application
D. Datalink and Network

Answer: D

NEW QUESTION 209
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

NEW QUESTION 210
What is the Manual Client Authentication TELNET port?

A. 23
B. 264
C. 900
D. 259

Answer: D

NEW QUESTION 213
UDP packets are delivered if they are .

A. a stateful ACK to a valid SYN-SYN/ACK on the inverse UDP ports and IP
B. a valid response to an allowed request on the inverse UDP ports and IP
C. bypassing the kernel by the forwarding layer of ClusterXL
D. referenced in the SAM related dynamic tables

Answer: B

NEW QUESTION 216
Your company is still using traditional mode VPN configuration on all Gateways and policies. Your manager now requires you to migrate to a simplified VPN policy to benefit from the new features. This needs to be done with no downtime due to critical applications which must run constantly. How would you start such a migration?

A. This cannot be done without downtime as a VPN between a traditional mode Gateway and a simplified mode Gateway does not work.
B. This can not be done as it requires a SIC- reset on the Gateways first forcing an outage.
C. You first need to completely rewrite all policies in simplified mode and then push this new policy to all Gateways at the same time.
D. Convert the required Gateway policies using the simplified VPN wizard, check their logic and then migrate Gateway per Gateway.

Answer: D

NEW QUESTION 221
Which of the following actions do NOT take place in IKE Phase 1?

A. Peers agree on encryption method.
B. Diffie-Hellman key is combined with the key material to produce the symmetrical IPsec key.
C. Peers agree on integrity method.
D. Each side generates a session key from its private key and the peer’s public key.

Answer: B

NEW QUESTION 224
Jennifer McHanry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.
To make this scenario work, the IT administrator must:
1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action.
Ms. McHanry tries to access the resource but is unable. What should she do?

A. Have the security administrator select the Action field of the Firewall Rule “Redirect HTTP connections to an authentication (captive) portal?
B. Have the security administrator reboot the firewall
C. Have the security administrator select Any for the Machines tab in the appropriate Access Role
D. Install the Identity Awareness agent on her iPad

Answer: A

NEW QUESTION 228
You have installed a R77 Security Gateway on GAiA. To manage the Gateway from the enterprise Security Management Server, you create a new Gateway object and Security Policy. When you install the new Policy from the Policy menu, the Gateway object does not appear in the Install Policy window as a target. What is the problem?

A. The object was created with Node > Gateway.
B. No Masters file is created for the new Gateway.
C. The Gateway object is not specified in the first policy rule column Install On.
D. The new Gateway's temporary license has expired.

Answer: A

NEW QUESTION 230
Your company has two headquarters, one in London, one in New York. Each of the headquarters includes several branch offices. The branch offices only need to communicate with the headquarters in their country, not with each other, and the headquarters need to communicate directly. What is the BEST configuration for establishing VPN Communities among the branch offices and their headquarters, and between the two headquarters? VPN Communities comprised of:

A. Three mesh Communities: one for London headquarters and its branches; one for New York headquarters and its branches; and one for London and New York headquarters.
B. Two mesh and one star Community: Each mesh Community is set up for each site between headquarters their branche
C. The star Community has New York as the center and London as its satellite.
D. Two star communities and one mesh: A star community for each city with headquarters as center, and branches as satellite
E. Then one mesh community for the two headquarters.
F. One star Community with the option to mesh the center of the star: New York and London Gateways added to the center of the star with the “mesh center Gateways? option checked; all London branch offices defined in one satellite window; but, all New York branch offices defined in another satellite window.

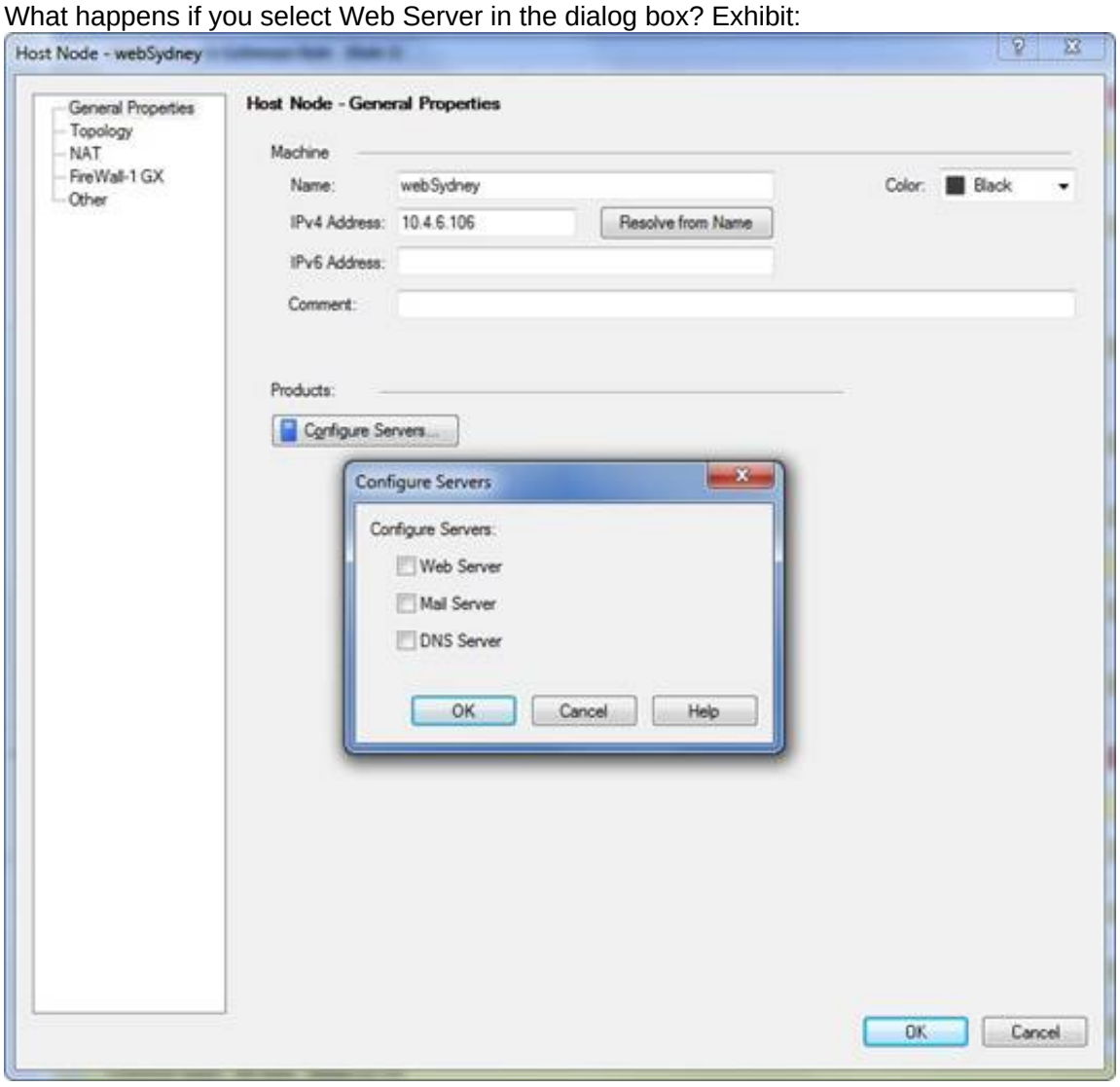
Answer: C

NEW QUESTION 233
You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause?

A. The POP3 rule is disabled.
B. POP3 is accepted in Global Properties.
C. The POP3 rule is hidden.
D. POP3 is one of 3 services (POP3, IMAP, and SMTP) accepted by the default mail object in R77.

Answer: C

NEW QUESTION 236
What happens if you select Web Server in the dialog box? Exhibit:



A. An implied rule will be added allowing HTTP requests to the host.
B. Anti-virus settings will be applied to the host.
C. Web Intelligence will be applied to the host.
D. An implied rule will be added allowing HTTP request from and to the host.

Answer: C

NEW QUESTION 240
Which of the following commands can be used to remove site-to-site IPsec Security Association (SA)?

A. vpn debug ipsec
B. vpn ipsec
C. fw ipsec tu
D. vpn tu

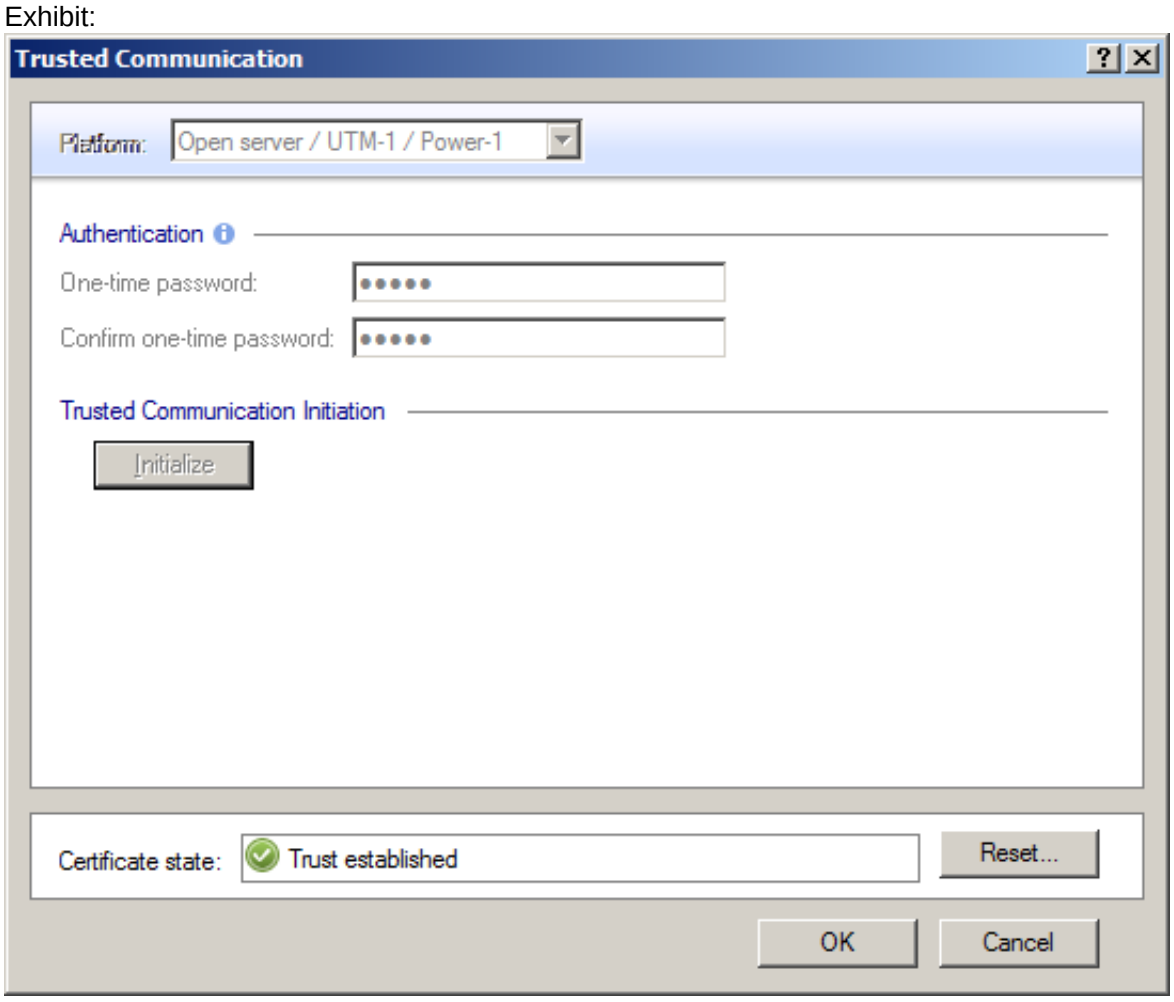
Answer: D

NEW QUESTION 244
When using vpn tu, which option must you choose if you want to rebuild your VPN for a specific IP (gateway)?
Exhibit:

A. (6) Delete all IPsec SAs for a given User (Client)
B. (5) Delete all IPsec SAs for a given peer (GW)
C. (8) Delete all IPsec+IKE SAs for a given User (Client)
D. Delete all IPsec+IKE SAs for a given peer (GW)

Answer: D

NEW QUESTION 248
What happens when you open the Gateway object window Trusted Communication and press and confirm Reset?
Exhibit:



A. Sic will be reset on the Gateway only.
B. The Gateway certificate will be revoked on the Gateway only.
C. The Gateway certificate will be revoked on the Security Management Server only.
D. The Gateway certificate will be revoked on the Security Management Server and SIC will be reset on the Gateway.

Answer: C

NEW QUESTION 253
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

NEW QUESTION 255
You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

URL List Version	☐	100
Unreachable directories	☐	100
Update Service	☐	100
Update Source	☐	100
Update Status	☐	100
User Action Comment	☐	100
User Additional Information	☐	100
User Check	☐	1
User DN	☐	100
User Directory	☐	100
User Display Name	☐	100
User Group	☐	100
User Reported Wrong Category	☐	100
User Response	☐	50
User SID	☐	100
User UID	☐	100
User's IP	☐	100
UserCheck ID	☐	100
UserCheck Interaction Name	☐	100
UserCheck Message to User	☐	100
UserCheck Scope	☐	100
UserCheck User Input	☐	100
VLAN ID	☐	100
VPN Feature	☐	100
VPN Peer Gateway	☐	100
Version	☐	100
Virtual Link	☐	100
Virus Name	☐	100
VoIP Duration	☐	100
VoIP Log Type	☐	100
VoIP Reject Reason	☐	100
VoIP Reject Reason Information	☐	100
Web Filtering Categories	☐	100
Wire Byte/Sec Out	☐	100
Wire Byte/Sec in	☐	100
Wire Packet/Sec Out	☐	100
Wire Packet/Sec in	☐	100
Write Access	☐	100
XlateDPort	☐	100
XlateDst	☐	100
XlateSPort	☐	100
XlateSrc	☐	100
special properties	☐	100

A. XlateDst
B. XlateSPort
C. XlateDPort
D. XlateSrc

Answer: B

NEW QUESTION 257
Which of the following actions take place in IKE Phase 2 with Perfect Forward Secrecy disabled?

A. Symmetric IPsec keys are generated.
B. Each Security Gateway generates a private Diffie-Hellman (DH) key from random pools.
C. The DH public keys are exchanged.
D. Peers authenticate using certificates or preshared secrets.

Answer: B

NEW QUESTION 260
You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities should you do first?

A. Create a new logical-server object to represent your partner's CA.
B. Exchange exported CA keys and use them to create a new server object to represent your partner's Certificate Authority (CA).
C. Manually import your partner's Certificate Revocation List.
D. Manually import your partner's Access Control List.

Answer: B

NEW QUESTION 262
When using AD Query to authenticate users for Identity Awareness, identity data is received seamlessly from the Microsoft Active Directory (AD). What is NOT a recommended usage of this method?

A. Leveraging identity in the application control blade
B. Basic identity enforcement in the internal network
C. Identity-based auditing and logging
D. Identity-based enforcement for non-AD users (non-Windows and guest users)

Answer: D

NEW QUESTION 266
You are about to integrate RSA SecurID users into the Check Point infrastructure. What kind of users are to be defined via SmartDashboard?

A. A group with generic user
B. All users
C. LDAP Account Unit Group
D. Internal user Group

Answer: A

NEW QUESTION 271
Which Client Authentication sign-on method requires the user to first authenticate via the User Authentication mechanism, when logging in to a remote server with Telnet?

A. Manual Sign On
B. Agent Automatic Sign On
C. Partially Automatic Sign On
D. Standard Sign On

Answer: C

NEW QUESTION 274
Complete this statement from the options provided. Using Captive Portal, unidentified users may be either; blocked, allowed to enter required credentials, or required to download the
.

A. Identity Awareness Agent
B. Full Endpoint Client
C. ICA Certificate
D. SecureClient

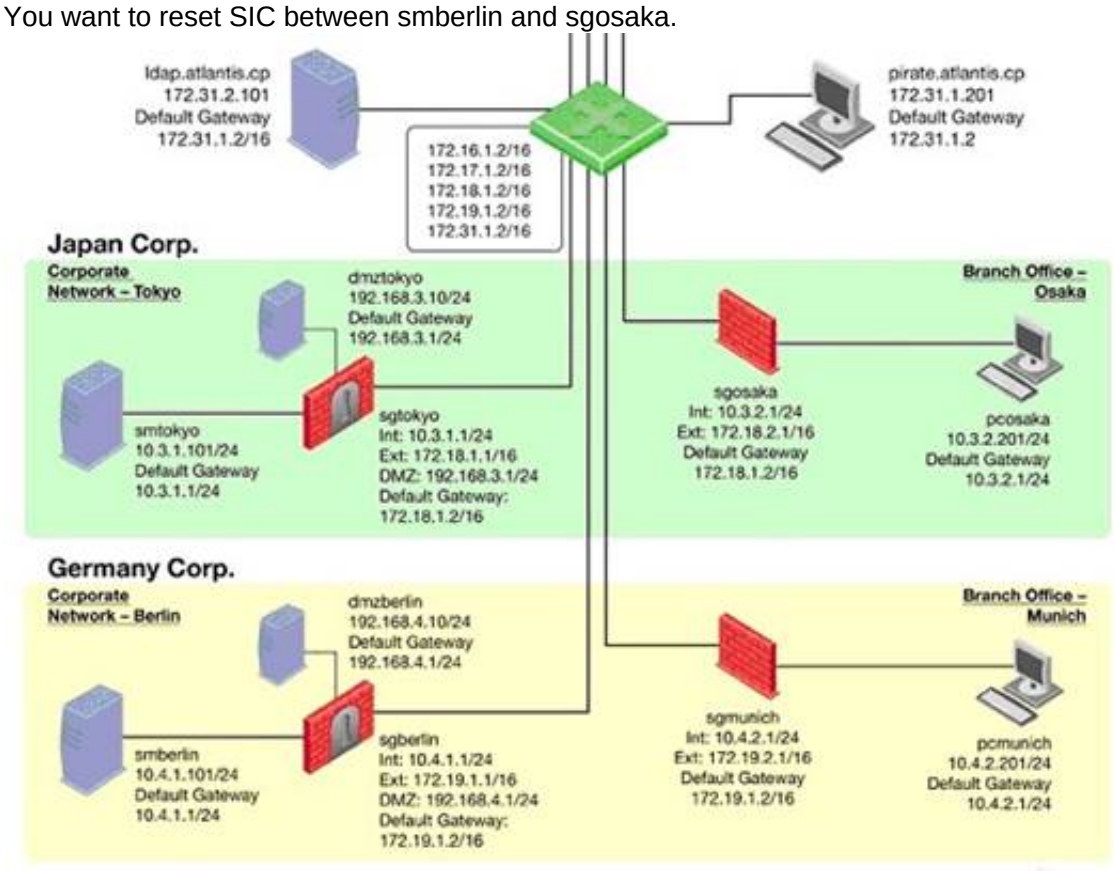
Answer: A

NEW QUESTION 276
Anti-Spoofing is typically set up on which object type?

A. Security Gateway
B. Host
C. Security Management object
D. Network

Answer: A

NEW QUESTION 280
You want to reset SIC between smberlin and sgosaka.



In SmartDashboard, you choose sgosaka, Communication, Reset. On sgosaka, you start cpconfig, choose Secure Internal Communication and enter the new SIC Activation Key. The screen reads The SIC was successfully initialized and jumps back to the cpconfig menu. When trying to establish a connection, instead of a working connection, you receive this error message:

What is the reason for this behavior?

A. The Gateway was not rebooted, which is necessary to change the SIC key.
B. You must first initialize the Gateway object in SmartDashboard (i.e., right-click on the object, choose Basic Setup > Initialize).
C. The Check Point services on the Gateway were not restarted because you are still in the cpconfig utility.
D. The activation key contains letters that are on different keys on localized keyboard
E. Therefore, the activation can not be typed in a matching fashion.

Answer: C

NEW QUESTION 281
John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to 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.
John received a 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 installs the policy.
2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.
3) Changes from static IP address to DHCP for the client PC.
What should John do when he cannot access the web server from a different personal computer?

A. John should lock and unlock his computer
B. Investigate this as a network connectivity issue
C. The access should be changed to authenticate the user instead of the PC
D. John should install the Identity Awareness Agent

Answer: C

NEW QUESTION 283
Match the following commands to their correct function. Each command has one function only listed.
Exhibit:

Command	Function
C1 `cp_admin_convert`	F1: export and import different revisions of the database.
C2 `cpca_client`	F2: export and import policy packages.
C3 `cp_merge`	F3: transfer Log data to an external database.
C4 `cpwd_admin`	F4: execute operations on the ICA.
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in `cpconfig` to SmartDashboard.

A. C1>F6; C2>F4; C3>F2; C4>F5
B. C1>F2; C2>F1; C3>F6; C4>F4
C. C1>F2; C2>F4; C3>F1; C4>F5
D. C1>F4; C2>F6; C3>F3; C4>F2

Answer: A

NEW QUESTION 286
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

Answer: C

NEW QUESTION 290
An Administrator without access to SmartDashboard installed a new IPSO-based R77 Security Gateway over the weekend. He e-mailed you the SIC activation key. You want to confirm communication between the Security Gateway and the Management Server by installing the Policy. What might prevent you from installing the Policy?

A. An intermediate local Security Gateway does not allow a policy install through it to the remote new Security Gateway applianc
B. Resolve by running the command fw unloadlocal on the local Security Gateway.
C. You first need to run the command fw unloadlocal on the R77 Security Gateway appliance in order to remove the restrictive default policy.
D. You first need to create a new Gateway object in SmartDashboard, establish SIC via the Communication button, and define the Gateway's topology.
E. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Serve
F. You must initialize SIC on the Security Management Server.

Answer: C

NEW QUESTION 292
When using LDAP as an authentication method for Identity Awareness, the query:

A. Requires client and server side software.
B. Prompts the user to enter credentials.
C. Requires administrators to specifically allow LDAP traffic to and from the LDAP Server and the Security Gateway.
D. Is transparent, requiring no client or server side software, or client intervention.

Answer: D

NEW QUESTION 294
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.

Answer: B

NEW QUESTION 298
What command with appropriate switches would you use to test Identity Awareness connectivity?

A. test_ldap
B. test_ad_connectivity
C. test_ldap_connectivity
D. test_ad

Answer: B

NEW QUESTION 300
How granular may an administrator filter an Access Role with identity awareness? Per:

A. Specific ICA Certificate
B. AD User
C. Radius Group
D. Windows Domain

Answer: B

NEW QUESTION 301
You are installing a Security Management Server. Your security plan calls for three administrators for this particular server. How many can you create during installation?

A. One
B. Only one with full access and one with read-only access
C. As many as you want
D. Depends on the license installed on the Security Management Server

Answer: A

NEW QUESTION 302
Which command displays the installed Security Gateway version?

A. fw ver
B. fw stat
C. fw printver
D. cpstat –gw

Answer: A

NEW QUESTION 307
If a SmartUpdate upgrade or distribution operation fails on GAiA, how is the system recovered?

A. The Administrator can only revert to a previously created snapshot (if there is one) with the command cprinstall snapshot <object name> <filename>.
B. The Administrator must reinstall the last version via the command cprinstall revert <object name> <file name>.
C. The Administrator must remove the rpm packages manually, and re-attempt the upgrade.
D. GAiA will reboot and automatically revert to the last snapshot version prior to upgrade.

Answer: D

NEW QUESTION 311
Identify the correct step performed by SmartUpdate to upgrade a remote Security Gateway. After selecting Packages > Distribute Only and choosing the target Gateway, the:

A. selected package is copied from the CD-ROM of the SmartUpdate PC directly to the Security Gateway and the installation IS performed.
B. selected package is copied from the Package Repository on the Security Management Server to the Security Gateway and the installation IS performed.
C. SmartUpdate wizard walks the Administrator through a distributed installation.
D. selected package is copied from the Package Repository on the Security Management Server to the Security Gateway but the installation IS NOT performed.

Answer: D

NEW QUESTION 315
You find that Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Choose the BEST reason why.

A. You checked the cache password on desktop option in Global Properties.
B. Another rule that accepts HTTP without authentication exists in the Rule Base.
C. You have forgotten to place the User Authentication Rule before the Stealth Rule.
D. Users must use the SecuRemote Client, to use the User Authentication Rule.

Answer: B

NEW QUESTION 319
How can you check whether IP forwarding is enabled on an IP Security Appliance?

A. clish -c show routing active enable
B. cat /proc/sys/net/ipv4/ip_forward
C. echo 1 > /proc/sys/net/ipv4/ip_forward
D. ipsofwd list

Answer: D

NEW QUESTION 322
Where is the fingerprint generated, based on the output display? Exhibit:

A. SmartConsole
B. SmartUpdate
C. Security Management Server
D. SmartDashboard

Answer: C

NEW QUESTION 324
Where are SmartEvent licenses installed?

A. SmartEvent server
B. Log Server
C. Security Management Server
D. Security Gateway

Answer: A

NEW QUESTION 329
What happens if the identity of a user is known?

A. If the user credentials do not match an Access Role, the traffic is automatically dropped.
B. If the user credentials do not match an Access Role, the system displays a sandbox.
C. If the user credentials do not match an Access Role, the gateway moves onto the next rule.
D. If the user credentials do not match an Access Role, the system displays the Captive Portal.

Answer: C

NEW QUESTION 332
You are running the license_upgrade tool on your GAiA Gateway. Which of the following can you NOT do with the upgrade tool?

A. Perform the actual license-upgrade process
B. Simulate the license-upgrade process
C. View the licenses in the SmartUpdate License Repository
D. View the status of currently installed licenses

Answer: C

NEW QUESTION 334
Which of the following items should be configured for the Security Management Server to authenticate using LDAP?

A. Login Distinguished Name and password
B. Windows logon password
C. Check Point Password
D. WMI object

Answer: A

NEW QUESTION 336

Which rules are not applied on a first-match basis?

A. User Authentication
B. Client Authentication
C. Session Authentication
D. Cleanup

Answer: A

NEW QUESTION 340
An advantage of using central instead of local licensing is:

A. A license can be taken from one Security Management Server and given to another Security Management Server.
B. Only one IP address is used for all licenses.
C. The license must be renewed when changing the IP address of a Security Gatewa
D. Each module's license has a unique IP address.
E. Licenses are automatically attached to their respective Security Gateways.

Answer: B

NEW QUESTION 343
You are running a R77 Security Gateway on GAiA. In case of a hardware failure, you have a server with the exact same hardware and firewall version installed. What back up method could be used to quickly put the secondary firewall into production?

A. manual backup
B. upgrade_export
C. backup
D. snapshot

Answer: D

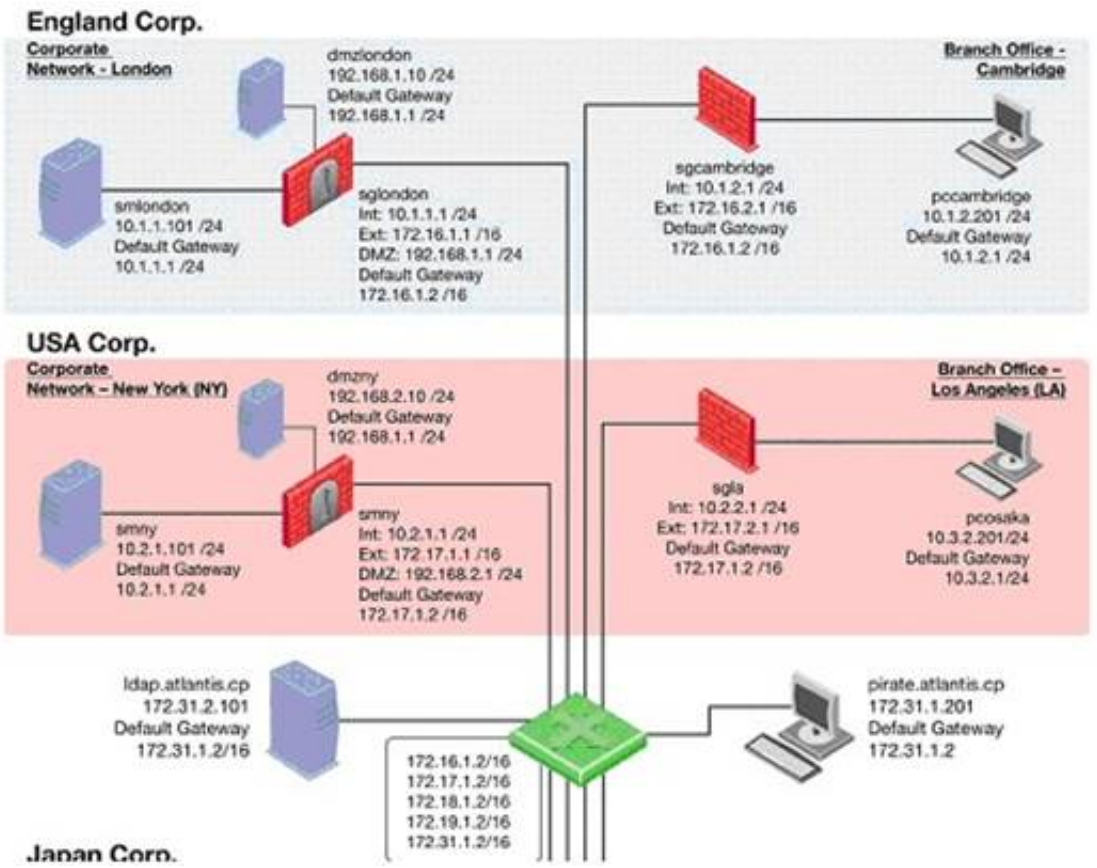
NEW QUESTION 346
As you review this Security Policy, what changes could you make to accommodate Rule 4? Exhibit:

No.	Hits	Name	Source	Destination	VPN	Service	Action
		Limit Access to Gateways (Rule 1)					
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
		VPN Access Rules (Rules 2-5)					
2	0	Site-to-Site	Any	Any	Any Traffic	CIFS ftp-port http https smtp	accept
3	0	Remote Access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS http https imap	accept
4	0	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA-proxy-server	Any Traffic	https	User Auth
5	0	Web Server	L2TP-vpn-user@Any Customers@Any	Remote-1-web-server	Any Traffic	http	accept

A. Remove the service HTTP from the column Service in Rule 4.
B. Modify the column VPN in Rule 2 to limit access to specific traffic.
C. Nothing at all
D. Modify the columns Source or Destination in Rule 4.

Answer: B

NEW QUESTION 351
The London Security Gateway Administrator has just installed the Security Gateway and Management Server. He has not changed any default settings. As he tries to configure the Gateway, he is unable to connect.



Which troubleshooting suggestion will NOT help him?

A. Check if some intermediate network device has a wrong routing table entry, VLAN assignment, duplex-mismatch, or trunk issue.
B. Test the IP address assignment and routing settings of the Security Management Server, Gateway, and console client.
C. Verify the SIC initialization.
D. Verify that the Rule Base explicitly allows management connections.

Answer: D

NEW QUESTION 353
Which of the following statements accurately describes the command snapshot?

A. snapshot creates a full OS-level backup, including network-interface data, Check Point product information, and configuration settings during an upgrade of a GAiA Security Gateway.
B. snapshot creates a Security Management Server full system-level backup on any OS.
C. snapshot stores only the system-configuration settings on the Gateway.
D. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server.

Answer: A

NEW QUESTION 354
To qualify as an Identity Awareness enabled rule, which column MAY include an Access Role?

A. Action
B. Source
C. User
D. Track

Answer: B

NEW QUESTION 359
Over the weekend, an Administrator without access to SmartDashboard installed a new R77 Security Gateway using GAiA. You want to confirm communication between the Gateway and the Management Server by installing the Security Policy. What might prevent you from installing the Policy?

A. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Serve
B. You must initialize SIC on both the Security Gateway and the Management Server.
C. You first need to run the command fw unloadlocal on the new Security Gateway.
D. You first need to initialize SIC in SmartUpdate.
E. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Serve
F. You must initialize SIC on the Security Management Server.

Answer: D

NEW QUESTION 362
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

Answer: A

NEW QUESTION 365
Which of these components does NOT require a Security Gateway R77 license?

A. Security Management Server
B. Check Point Gateway
C. SmartConsole
D. SmartUpdate upgrading/patching

Answer: C

NEW QUESTION 366
Before upgrading SecurePlatform to GAiA, you should create a backup. To save time, many administrators use the command backup. This creates a backup of the Check Point configuration as well as the system configuration.
An administrator has installed the latest HFA on the system for fixing traffic problem after creating a backup file. There is a mistake in the very complex static routing configuration. The Check Point configuration has not been changed.
Can the administrator use a restore to fix the errors in static routing?

A. The restore is not possible because the backup file does not have the same buildnumber (version).
B. The restore is done by selecting Snapshot Management from the boot menu of GAiA.
C. The restore can be done easily by the command restore and copying netconf.C from the production environment.
D. A backup cannot be restored, because the binary files are missing.

Answer: C

NEW QUESTION 368
In a distributed management environment, the administrator has removed the default check from Accept Control Connections under the Policy > Global Properties > FireWall tab. In order for the Security Management Server to install a policy to the Firewall, an explicit rule must be created to allow the server to communicate to the Security Gateway on port _____

A. 259
B. 900
C. 256
D. 80

Answer: C

NEW QUESTION 369
What physical machine must have access to the User Center public IP address when checking for new packages with SmartUpdate?

A. A Security Gateway retrieving the new upgrade package
B. SmartUpdate installed Security Management Server PC
C. SmartUpdate GUI PC
D. SmartUpdate Repository SQL database Server

Answer: C

NEW QUESTION 374
Why should the upgrade_export configuration file (.tgz) be deleted after you complete the import process?

A. SmartUpdate will start a new installation process if the machine is rebooted.
B. It will prevent a future successful upgrade_export since the .tgz file cannot be overwritten.
C. It contains your security configuration, which could be exploited.
D. It will conflict with any future upgrades when using SmartUpdate.

Answer: C

NEW QUESTION 376
Which of the following statements accurately describes the command upgrade_export?

A. upgrade_export stores network-configuration data, objects, global properties, and the database revisions prior to upgrading the Security Management Server.
B. Used primarily when upgrading the Security Management Server, upgrade_export stores all object databases and the /conf directories for importing to a newer Security Gateway version.
C. upgrade_export is used when upgrading the Security Gateway, and allows certain files to be included or excluded before exporting.
D. This command is no longer supported in GAiA.

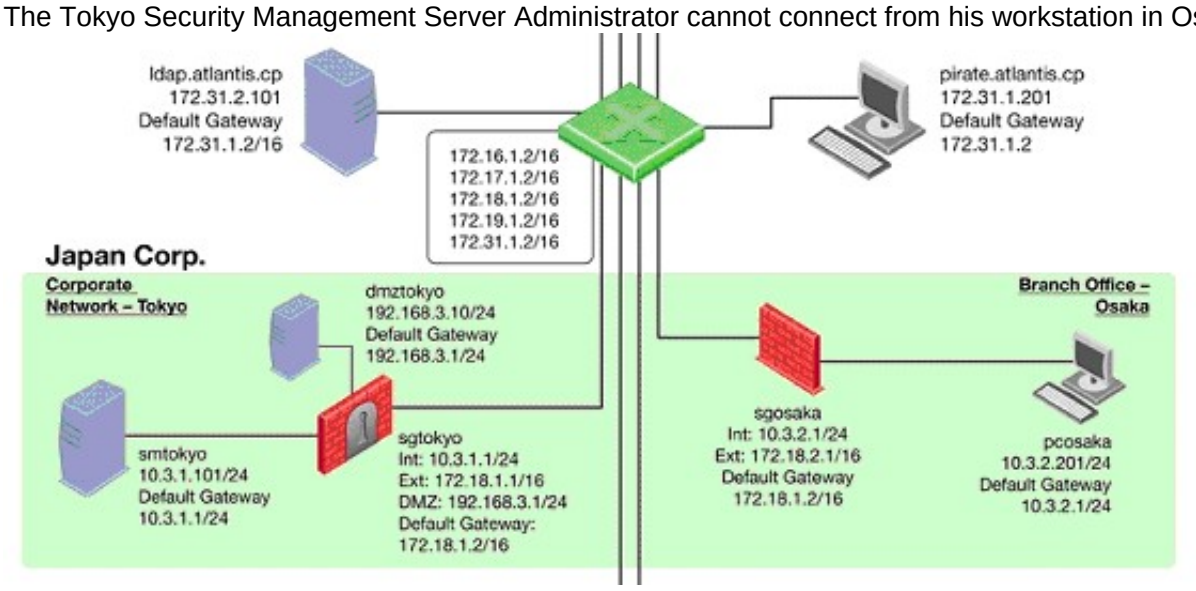
Answer: B

NEW QUESTION 378
Which rule position in the Rule Base should hold the Cleanup Rule? Why?

A. Firs
B. It explicitly accepts otherwise dropped traffic.
C. Las
D. It explicitly drops otherwise accepted traffic.
E. Las
F. It serves a logging function before the implicit drop.
G. Before last followed by the Stealth Rule.

Answer: C

NEW QUESTION 380
The Tokyo Security Management Server Administrator cannot connect from his workstation in Osaka.



Which of the following lists the BEST sequence of steps to troubleshoot this issue?

A. Check for matching OS and product versions of the Security Management Server and the clien
B. Then, ping the Gateways to verify connectivit
C. If successful, scan the log filesfor any denied management packets.
D. Verify basic network connectivity to the local Gateway, service provider, remote Gateway, remote network and target machin
E. Then, test for firewall rules that deny management access to the targe
F. If successful, verify that pcosaka is a valid client IP address.
G. Check the allowed clients and users on the Security Management Serve
H. If pcosaka and your user account are valid, check for network problem
I. If there are no network related issues, this is likely to be a problem with the server itsel
J. Check for any patches and upgrade
K. If still unsuccessful, open a case with Technical Support.
L. Call Tokyo to check if they can ping the Security Management Server locall
M. If so, login to sgtokyo, verify management connectivity and Rule Bas
N. If this looks okay, ask your provider if they have some firewall rules that filters out your management traffic.

Answer: B

NEW QUESTION 384
Can you use Captive Portal with HTTPS?

A. No, it only works with FTP
B. No, it only works with FTP and HTTP
C. Yes
D. No, it only works with HTTP

Answer: C

NEW QUESTION 387
You review this Security Policy because Rule 4 is inhibited. Which Rule is responsible? Exhibit:

No.	Hits	Name	Source	Destination	VPN	Service	Action
	Limit Access to Gateways (Rule 1)						
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
	VPN Access Rules (Rules 2-5)						
2	0	Site-to-Site	Any	Any	Any Traffic	CIFS ftp-port http https smtp	accept
3	0	Remote Access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS http https imap	accept
4	0	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA-proxy-server	Any Traffic	https	User Auth
5	0	Web Server	L2TP-vpn-user@Any Customers@Any	Remote-1-web-server	Any Traffic	http	accept

A. No rule inhibits Rule 4.
B. Rule 1
C. Rule 2
D. Rule 3

Answer: C

NEW QUESTION 389
You need to back up the routing, interface, and DNS configuration information from your R77 GAiA Security Gateway. Which backup-and-restore solution do you use?

A. Manual copies of the directory $FWDIR/conf

B. GAiA back up utilities
C. upgrade_export and upgrade_import commands
D. Database Revision Control

Answer: B

NEW QUESTION 393
What command syntax would you use to turn on PDP logging in a distributed environment?

A. pdp track=1
B. pdp tracker on
C. pdp logging on
D. pdp log=1

Answer: B

NEW QUESTION 395
Which command would provide the most comprehensive diagnostic information to Check Point Technical Support?

A. fw cpinfo
B. cpinfo -o date.cpinfo.txt
C. diag
D. cpstat - date.cpstat.txt

Answer: B

NEW QUESTION 400
In a distributed management environment, the administrator has removed all default check boxes from the Policy > Global Properties > Firewall tab. In order for the Security Gateway to send logs to the Security Management Server, an explicit rule must be created to allow the Security Gateway to communicate to the Security Management Server on port .

A. 259
B. 900
C. 256
D. 257

Answer: D

NEW QUESTION 403
Which of the following statements is TRUE about management plug-ins?

A. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
B. Installing a management plug-in is just like an upgrade process.
C. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.
D. The plug-in is a package installed on the Security Gateway.

Answer: A

NEW QUESTION 406
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 necessar
C. This access is available by default.
D. Change the Identity Awareness settings under Global Properties to allow Captive Portal access on all interfaces.
E. Change the Identity Awareness settings under Global Properties to allow Captive Portal access for an external interface.

Answer: A

NEW QUESTION 407
Which of the following items should be configured for the Security Management Server to authenticate via LDAP?

A. Check Point Password
B. Active Directory Server object
C. Windows logon password
D. WMI object

Answer: B

NEW QUESTION 408
Where does the security administrator activate Identity Awareness within SmartDashboard?

A. Gateway Object > General Properties
B. Security Management Server > Identity Awareness
C. Policy > Global Properties > Identity Awareness

D. LDAP Server Object > General Properties

Answer: A

NEW QUESTION 413
What action CANNOT be run from SmartUpdate R77?

A. Fetch sync status
B. Reboot Gateway
C. Preinstall verifier
D. Get all Gateway Data

Answer: A

NEW QUESTION 417
Which command line interface utility allows the administrator to verify the Security Policy name and timestamp currently installed on a firewall module?

A. cpstat fwd
B. fw ver
C. fw stat
D. fw ctl pstat

Answer: C

NEW QUESTION 419
Which operating systems are supported by a Check Point Security Gateway on an open server? Select MOST complete list.

A. Sun Solaris, Red Hat Enterprise Linux, Check Point SecurePlatform, IPSO, Microsoft Windows
B. Check Point GAiA and SecurePlatform, and Microsoft Windows
C. Check Point GAiA, Microsoft Windows, Red Hat Enterprise Linux, Sun Solaris, IPSO
D. Check Point GAiA and SecurePlatform, IPSO, Sun Solaris, Microsoft Windows

Answer: B

NEW QUESTION 423
A Cleanup rule:

A. logs connections that would otherwise be dropped without logging by default.
B. drops packets without logging connections that would otherwise be dropped and logged by default.
C. logs connections that would otherwise be accepted without logging by default.
D. drops packets without logging connections that would otherwise be accepted and logged by default.

Answer: A

NEW QUESTION 424
You are working with multiple Security Gateways that enforce an extensive number of rules. To simplify security administration, which one of the following would you choose to do?

A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
B. Run separate SmartConsole instances to login and configure each Security Gateway directly.
C. Create network objects that restrict all applicable rules to only certain networks.
D. Create a separate Security Policy package for each remote Security Gateway.

Answer: D

NEW QUESTION 428
Central license management allows a Security Administrator to perform which of the following functions?
1. Check for expired licenses.
2. Sort licenses and view license properties.
3. Attach both R77 Central and Local licesnes to a remote module.
4. Delete both R77 Local Licenses and Central licenses from a remote module.
5. Add or remove a license to or from the license repository.
6. Attach and/or delete only R77 Central licenses to a remote module (not Local licenses).

A. 1, 2, 5, & 6
B. 2, 3, 4, & 5
C. 2, 5, & 6
D. 1, 2, 3, 4, & 5

Answer: D

NEW QUESTION 432
What CANNOT be configured for existing connections during a policy install?

A. Keep all connections

B. Keep data connections
C. Re-match connections
D. Reset all connections

Answer: D

NEW QUESTION 433
What is the syntax for uninstalling a package using newpkg?

A. -u <pathname of package>
B. -i <full pathname of package>
C. -S <pathname of package>
D. newpkg CANNOT be used to uninstall a package

Answer: D

NEW QUESTION 436
Suppose the Security Gateway hard drive fails and you are forced to rebuild it. You have a snapshot file stored to a TFTP server and backups of your Security Management Server.
What is the correct procedure for rebuilding the Gateway quickly?

A. Reinstall the base operating system (i.e., GAiA). Configure the Gateway interface so that the Gateway can communicate with the TFTP serve
B. Revert to the stored snapshot image, and install the Security Policy.
C. Run the command revert to restore the snapshot, establish SIC, and install the Policy.
D. Run the command revert to restore the snapsho
E. Reinstall any necessary Check Point product
F. Establish SIC and install the Policy.
G. Reinstall the base operating system (i.e., GAia). Configure the Gateway interface so that the Gateway can communicate with the TFTP serve
H. Reinstall any necessary Check Point products and previously applied hotfixe
I. Revert to the stored snapshot image, and install the Policy.

Answer: A

NEW QUESTION 441
How can you recreate the Security Administrator account, which was created during initial Management Server installation on GAiA?

A. Export the user database into an ASCII file with fwm dbexpor
B. Open this file with an editor, and delete the Administrator Account portion of the fil
C. You will be prompted to create a new account.
D. Type cpm -a, and provide the existing Administrator's account nam
E. Reset the Security Administrator's password.
F. Launch cpconfig and delete the Administrator's accoun
G. Recreate the account with the same name.
H. Launch SmartDashboard in the User Management screen, and delete the cpconfig administrator.

Answer: C

NEW QUESTION 446
What statement is true regarding Visitor Mode?

A. VPN authentication and encrypted traffic are tunneled through port TCP 443.
B. Only ESP traffic is tunneled through port TCP 443.
C. Only Main mode and Quick mode traffic are tunneled on TCP port 443.
D. All VPN traffic is tunneled through UDP port 4500.

Answer: A

NEW QUESTION 448
One of your remote Security Gateway's suddenly stops sending logs, and you cannot install the Security Policy on the Gateway. All other remote Security Gateways are logging normally to the Security Management Server, and Policy installation is not affected. When you click the Test SIC status button in the problematic Gateway object, you receive an error message. What is the problem?

A. The remote Gateway's IP address has changed, which invalidates the SIC Certificate.
B. The time on the Security Management Server's clock has changed, which invalidates the remote Gateway's Certificate.
C. The Internal Certificate Authority for the Security Management Server object has been removed from objects_5_0.C.
D. There is no connection between the Security Management Server and the remote Gatewa
E. Rules or routing may block the connection.

Answer: D

NEW QUESTION 453
You install and deploy GAiA with default settings. You allow Visitor Mode in the Gateway object's Remote Access properties and install policy. What additional steps are required for this to function correctly?

A. You need to start SSL Network Extender first, then use Visitor Mode.
B. Set Visitor Mode in Policy > Global Properties > Remote-Access > VPN - Advanced.
C. Office mode is not configured.

D. The WebUI on GAiA runs on port 443 (HTTPS). When you configure Visitor Mode it cannot bind to default port 443, because it's used by another program (WebUI). With multi- port no additional changes are necessary.

Answer: D

NEW QUESTION 456
Packages and licenses are loaded into the SmartUpdate repositories from which sources?

A. Download Center, Check Point DVD, User Center, and from command cplic
B. FTP server, User Center from a file
C. User Center, manually, SCP server
D. command cplic, manually, from a file

Answer: A

NEW QUESTION 457
What action can be performed from SmartUpdate R77?

A. upgrade_export
B. fw stat -l
C. cpinfo
D. remote_uninstall_verifier

Answer: C

NEW QUESTION 458
What happens when you run the command. fw sam -J src [Source IP Address]?

A. Connections from the specified source are blocked without the need to change the Security Policy.
B. Connections to the specified target are blocked without the need to change the Security Policy.
C. Connections to and from the specified target are blocked without the need to change the Security Policy.
D. Connections to and from the specified target are blocked with the need to change the Security Policy.

Answer: A

NEW QUESTION 459
A third-shift Security Administrator configured and installed a new Security Policy early this morning. When you arrive, he tells you that he has been receiving complaints that Internet access is very slow. You suspect the Security Gateway virtual memory might be the problem. Which SmartConsole component would you use to verify this?

A. Eventia Analyzer
B. SmartView Tracker
C. SmartView Monitor
D. This information can only be viewed with the command fw ctl pstat from the CLI.

Answer: C

NEW QUESTION 461
SmartView Monitor is mainly for which kind of work –
1. Monitoring Performance and traffic
2. Provision Package
3. Managing licenses
4. Managing VPN Tunnels

A. 2, 3
B. 2, 4
C. 1, 4
D. 1, 3

Answer: C

NEW QUESTION 466
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

Answer: C

NEW QUESTION 467
Your Security Gateways are running near performance capacity and will get upgraded
hardware next week. Which of the following would be MOST effective for quickly dropping all connections from a specific attacker’s IP at a peak time of day?

A. Intrusion Detection System (IDS) Policy install
B. Change the Rule Base and install the Policy to all Security Gateways
C. SAM - Block Intruder feature of SmartView Tracker
D. SAM - Suspicious Activity Rules feature of SmartView Monitor

Answer: D

NEW QUESTION 471
What is also referred to as Dynamic NAT?

A. Automatic NAT
B. Static NAT
C. Manual NAT
D. Hide NAT

Answer: D

NEW QUESTION 474
Choose the SmartLog property that is TRUE.

A. SmartLog has been an option since release R71.10.
B. SmartLog is not a Check Point product.
C. SmartLog and SmartView Tracker are mutually exclusive.
D. SmartLog is a client of SmartConsole that enables enterprises to centrally track log records and security activity with Google-like search.

Answer: D

NEW QUESTION 479
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.

Answer: B

NEW QUESTION 481
Which set of objects have an Authentication tab?

A. Templates, Users
B. Users, Networks
C. Users, User Groups
D. Networks, Hosts

Answer: A

NEW QUESTION 482
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.

Answer: A

NEW QUESTION 485
Which command displays the installed Security Gateway kernel version?

A. fw printver
B. fw ver
C. fw ver -k
D. cpstat -gw

Answer: C

NEW QUESTION 486
Your company enforces a strict change control policy. Which of the following would be MOST effective for quickly dropping an attacker’s specific active connection?

A. Change the Rule Base and install the Policy to all Security Gateways
B. Block Intruder feature of SmartView Tracker
C. Intrusion Detection System (IDS) Policy install
D. SAM - Suspicious Activity Rules feature of SmartView Monitor

Answer: B

NEW QUESTION 489
Which tool CANNOT be launched from SmartUpdate R77?

A. IP Appliance Voyager
B. snapshot
C. GAiA WebUI
D. cpinfo

Answer: B

NEW QUESTION 491
Katie has been asked to setup a rule to allow the new webserver in the DMZ to be accessible from the internet on port 443. The IP address of the Web Server, Apothos, is 192.168.126.3 and the external address should be 10.4.2.3. This needs to be the only server associated with this External IP address.
Which answer below will accomplish the steps needed to complete this task?

A. Katie will create a host node object with an IP address of 10.4.2.3 and will configure a static NAT of 192.168.126.3. She will add a new rule in the DMZ section of the policy for the Apothos serve
B. The rule will have an “Any Source, Destination of Apothos Host Object andservice of HTTPS”.
C. Katie will create a host node object with an IP address of 192.168.126.3 and will configure a static NAT of 10.4.2.3. She will add a new rule in the DMZ section of the policy for the Apothos serve
D. The rule will have an “Any Source, Destination of Apothos Host Object and service of HTTPS”.
E. Katie will create a Network object with an IP address of 192.168.126.3 and will configure a Hide NAT of 10.4.2.3. She will add a new rule in the DMZ section of the policy for the Apothos serve
F. The rule will have an “Any Source, Destination of Apothos Host Object and service of HTTPS”.
G. Katie will create a host node object with an IP address of 192.168.126.3 and willconfigure a static NAT of 10.4.2.3. She will add a new rule in the DMZ section of the policy for the Apothos serve
H. The rule will have an “Apothos Host Object Source, Destination of Any andservice of HTTPS”.

Answer: A

NEW QUESTION 495
Which feature in R77 permits blocking specific IP addresses for a specified time period?

A. Suspicious Activity Monitoring
B. HTTP Methods
C. Local Interface Spoofing
D. Block Port Overflow

Answer: A

NEW QUESTION 496
What is the difference between Standard and Specific Sign On methods?

A. Standard Sign On allows the user to be automatically authorized for all services that the rule allow
B. Specific Sign On requires that the user re-authenticate for each service specifically defined in the window Specific Action Properties.
C. Standard Sign On allows the user to be automatically authorized for all services that the rule allows, but re-authenticate for each host to which he is trying to connec
D. Specific Sign On requires that the user re-authenticate for each service.
E. Standard Sign On allows the user to be automatically authorized for all services that the rule allow
F. Specific Sign On requires that the user re-authenticate for each service and each host to which he is trying to connect.
G. Standard Sign On requires the user to re-authenticate for each service and each host to which he is trying to connec
H. Specific Sign On allows the user to sign on only to a specific IP address.

Answer: C

NEW QUESTION 501
You are a Security Administrator preparing to deploy a new HFA (Hotfix Accumulator) to ten Security Gateways at five geographically separate locations. What is the BEST method to implement this HFA?

A. Use a SSH connection to SCP the HFA to each Security Gatewa
B. Once copied locally, initiate a remote installation command and monitor the installation progress with SmartView Monitor.
C. Send a CD-ROM with the HFA to each location and have local personnel install it.
D. Send a Certified Security Engineer to each site to perform the update.
E. Use SmartUpdate to install the packages to each of the Security Gateways remotely.

Answer: D

NEW QUESTION 504
You are trying to save a custom log query in R77 SmartView Tracker, but getting the following error:
Could not save <query-name> (Error: Database is Read Only) Which of the following is a likely explanation for this?

A. Another administrator is currently connected to the Security Management Server with read/write permissions which impacts your ability to save custom log queries to the Security Management Server.
B. You do not have OS write permissions on the local SmartView Tracker PC in order to save the custom query locally.
C. You have read-only rights to the Security Management Server database.

D. You do not have the explicit right to save a custom query in your administrator permission profile under SmartConsole customization.

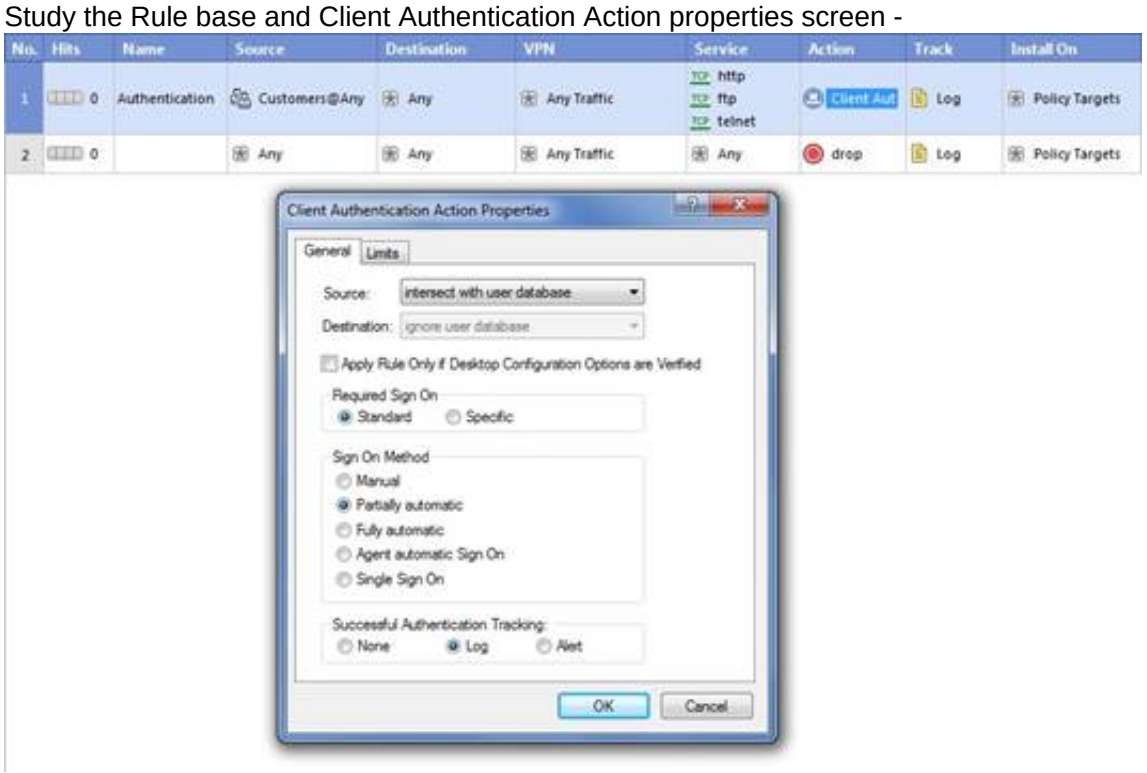
Answer: C

NEW QUESTION 505
Lily has completed the initial setup of her Management Server with an IP address of 192.168.12.12. She must now run the First Time Configuration Wizard via the Gaia Portal to finish the setup. Lily knows she must use a browser to access the device, but it unsure of the correct URL to enter; which one below will she need to use?

A. http://192.168.12.12
B. https://192.168.12.12:4433
C. https://192.168.12.12
D. http://192.168.12.12:8080

Answer: C

NEW QUESTION 509
Study the Rule base and Client Authentication Action properties screen -



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.

Answer: C

Explanation: Manual Users must use either telnet to port 259 on the firewall, or use a Web browser to connect to port 900 on the firewall to authenticate before being granted access.
Partially Automatic If user authentication is configured for the service the user is attempting to access and they pass this authentication, then no further client authentication is required. For example, if HTTP is permitted on a client authentication rule, the user will be able to transparently authenticate since FireWall-1 has a security server for HTTP.Then, if this setting is chosen, users will not have to manually authenticate for this connection. Note that this applies to all services for which FireWall-1 has built-in security servers (HTTP, FTP, telnet, and rlogin).
Fully Automatic If the client has the session authentication agent installed, then no further client authentication is required (see session authentication below). For HTTP, FTP, telnet, or rlogin, the firewall will authenticate via user authentication, and then session authentication will be used to authenticate all other services.
http://www.syngress.com
Figure 6.19 Client Authentication Action Properties 278 Chapter 6 • Authenticating Users
Agent Automatic Sign On Uses session authentication agent to provide transparent authentication (see session authentication below).
Single Sign-On System Used in conjunction with UserAuthority servers to provide enhanced application level security. Discussion of UserAuthority is beyond the scope of this book.

NEW QUESTION 511
How do you use SmartView Monitor to compile traffic statistics for your company's Internet Web activity during production hours?

A. Select Tunnels view, and generate a report on the statistics.
B. Configure a Suspicious Activity Rule which triggers an alert when HTTP traffic passes through the Gateway.
C. Use Traffic settings and SmartView Monitor to generate a graph showing the total HTTP traffic for the day.
D. View total packets passed through the Security Gateway.

Answer: C

NEW QUESTION 514
Which R77 SmartConsole tool would you use to verify the installed Security Policy name on a Security Gateway?

A. SmartView Monitor
B. SmartUpdate
C. SmartView Status
D. None, SmartConsole applications only communicate with the Security Management Server.

Answer: A

NEW QUESTION 515
You are the Security Administrator for MegaCorp. In order to see how efficient your firewall Rule Base is, you would like to see how often the particular rules match. Where can you see it? Give the BEST answer.

A. In the SmartView Tracker, if you activate the column Matching Rate.
B. In SmartReporter, in the section Firewall Blade - Activity > Network Activity with information concerning Top Matched Logged Rules.
C. SmartReporter provides this information in the section Firewall Blade - Security > Rule Base Analysis with information concerning Top Matched Logged Rules.
D. It is not possible to see it directl
E. You can open SmartDashboard and select UserDefined in the Track colum
F. Afterwards, you need to create your own program with an external counter.

Answer: C

NEW QUESTION 516
Is it possible to track the number of connections each rule matches in a Rule Base?

A. Yes, but you need SPLAT operating system to enable the feature Hits Count in the SmartDashboard client.
B. Yes, since R75 40 you can use the feature Hits Count in the SmartDashboard client.
C. Yes, but you need Gala operating system to enable the feature Hits Count in the SmartDashboard client.
D. No, due to an architecture limitation it is not possible to track the number of connections each rule matches.

Answer: B

NEW QUESTION 520
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

NEW QUESTION 525
Jack has been asked do enable Identify Awareness.
What are the three methods for Acquiring Identify available in the Identify Awareness Configuration Wizard?

A. LDAP Query, Terminal Servers, Light-weight Identity Agent
B. AD Query, Browser-Based Authentication, Light-Weight Identity Agent
C. AD Query, Browser-Based Authentication, Terminal Servers
D. LDAP Query, Browser-Based Authentication, Terminal Servers

Answer: C

NEW QUESTION 528
Which NAT option is available for Manual NAT as well as Automatic NAT?

A. Allow bi-directional NAT
B. Automatic ARP configuration
C. Translate destination on client-side
D. Enable IP Pool NAT

Answer: C

NEW QUESTION 531
You find a suspicious FTP site trying to connect to one of your internal hosts. How do you block it in real time and verify it is successfully blocked? Highlight the suspicious connection in SmartView Tracker:

A. Log mod
B. Block it using Tools > Block Intruder men
C. Observe in the Log mode that the suspicious connection does not appear again in this SmartView Tracker view.
D. Log mod
E. Block it using Tools > Block Intruder men
F. Observe in the Log mode that thesuspicious connection is listed in this SmartView Tracker view as “dropped.”
G. Active mod
H. Block it using Tools > Block Intruder men
I. Observe in the Active mode that the suspicious connection does not appear again in this SmartView Tracker view.
J. Active mod
K. Block it using Tools > Block Intruder men

L. Observe in the Active mode that the suspicious connection is listed in this SmartView Tracker view as “dropped.”

Answer: C

NEW QUESTION 534
An Administrator without access to SmartDashboard installed a new IPSO-based R77 Security Gateway over the weekend. He e-mailed you the SIC activation key and the IP
address of the Security Gateway. You want to confirm communication between the Security Gateway and the Management Server by installing the Policy. What might prevent you from installing the Policy?

A. An intermediate local Security Gateway does not allow a policy install through it to the remote new Security Gateway applianc
B. Resolve by running the command fw unloadlocal on the local Security Gateway.
C. You first need to run the command fw unloadlocal on the R77 Security Gateway appliance in order to remove the restrictive default policy.
D. You first need to create a new Gateway object in SmartDashboard, establish SIC via the Communication button, and define the Gateway’s topology.
E. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Serve
F. You must initialize SIC on the Security Management Server.

Answer: C

NEW QUESTION 539
Which R77 GUI would you use to see the number of packets accepted since the last policy install?

A. SmartView Monitor
B. SmartView Tracker
C. SmartDashboard
D. SmartView Status

Answer: A

NEW QUESTION 542
You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the Rule Base.
How do you achieve this?

A. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0.fws configuration file.
B. Select Block intruder from the Tools menu in SmartView Tracker.
C. Create a Suspicious Activity Rule in SmartView Monitor.
D. Add a temporary rule using SmartDashboard and select hide rule.

Answer: C

NEW QUESTION 543
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.77 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.77 Product From:

https://www.2passeasy.com/dumps/156-215.77/

Money Back Guarantee

156-215.77 Practice Exam Features:

* 156-215.77 Questions and Answers Updated Frequently

* 156-215.77 Practice Questions Verified by Expert Senior Certified Staff

* 156-215.77 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-215.77 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year