Exam Questions 156-215.77

Check Point Certified Security Administrator – GAiA

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

NEW QUESTION 1
Several Security Policies can be used for different installation targets. The Firewall protecting Human Resources' servers should have its own Policy Package. These rules must be installed on this machine and not on the Internet Firewall.
How can this be accomplished?

A. A Rule Base is always installed on all possible target
B. The rules to be installed on a Firewall are defined by the selection in the Rule Base row Install On.
C. When selecting the correct Firewall in each line of the Rule Base row Install On, only this Firewall is shown in the list of possible installation targets after selecting Policy > Install on Target.
D. In the menu of SmartDashboard, go to Policy > Policy Installation Targets and select the correct firewall via Specific Targets.
E. A Rule Base can always be installed on any Check Point Firewall objec
F. It is necessary to select the appropriate target directly after selecting Policy > Install on Target.

Answer: C

NEW QUESTION 2
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 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
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 6
Which command allows Security Policy name and install date verification on a Security Gateway?

A. fw show policy
B. fw stat -l
C. fw ctl pstat -policy
D. fw ver -p

Answer: B

NEW QUESTION 7
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 8
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 9
You are working with three other Security Administrators.
Which SmartConsole component can be used to monitor changes to rules or object properties made by the other administrators?

A. Eventia Tracker
B. SmartView Monitor
C. Eventia Monitor
D. SmartView Tracker

Answer: D

NEW QUESTION 10
Where are custom queries stored in R77 SmartView Tracker?

A. On the SmartView Tracker PC local file system under the user's profile.
B. On the Security Management Server tied to the GUI client IP.
C. On the Security Management Server tied to the Administrator User Database login name.
D. On the SmartView Tracker PC local file system shared by all users of that local PC.

Answer: C

NEW QUESTION 10
Your Security Management Server fails and does not reboot. One of your remote Security Gateways managed by the Security Management Server reboots.
What occurs with the remote Gateway after reboot?

A. Since the Security Management Server is not available, the remote Gateway cannotfetch the Security Polic
B. Therefore, all traffic is allowed through the Gateway.
C. Since the Security Management Server is not available, the remote Gateway cannot fetch the Security Polic
D. Therefore, no traffic is allowed through the Gateway.
E. The remote Gateway fetches the last installed Security Policy locally and passes traffic normall
F. The Gateway will log locally, since the Security Management Server is not available.
G. Since the Security Management Server is not available, the remote Gateway uses the local Security Policy, but does not log traffic.

Answer: C

NEW QUESTION 15
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 17
Which of the following R77 SmartView Tracker views will display a popup warning about performance implications on the Security Gateway?

A. All Records Query
B. Account Query
C. Active Tab
D. Audit Tab

Answer: C

NEW QUESTION 18
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 21
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 26
The third-shift Administrator was updating Security Management Server access settings in Global Properties and testing. He managed to lock himself out of his account.
How can you unlock this account?

A. Type fwm unlock_admin from the Security Management Server command line.
B. Type fwm unlock_admin -u from the Security Gateway command line.
C. Type fwm lock_admin -u <account name> from the Security Management Server command line.
D. Delete the file admin.lock in the Security Management Server directory $FWDIR/tmp/.

Answer: C

NEW QUESTION 28
You are a Security Administrator who has installed Security Gateway R77 on your network. You need to allow a specific IP address range for a partner site to access your intranet Web server. To limit the partner's access for HTTP and FTP only, you did the following:
1) Created manual Static NAT rules for the Web server.
2) Cleared the following settings in the Global Properties > Network Address Translation screen:
- Allow bi-directional NAT
- Translate destination on client side
Do the above settings limit the partner's access?

A. Ye
B. This will ensure that traffic only matches the specific rule configured for this traffic, and that the Gateway translates the traffic after accepting the packet.
C. N
D. The first setting is not applicabl
E. The second setting will reduce performance.
F. Ye
G. Both of these settings are only applicable to automatic NAT rules.
H. N
I. The first setting is only applicable to automatic NAT rule
J. The second setting will force translation by the kernel on the interface nearest to the client.

Answer: D

NEW QUESTION 33
You are reviewing the Security Administrator activity for a bank and comparing it to the change log. How do you view Security Administrator activity?

A. SmartView Tracker cannot display Security Administrator activity; instead, view the system logs on the Security Management Server's Operating System.
B. SmartView Tracker in Network and Endpoint Mode
C. SmartView Tracker in Active Mode
D. SmartView Tracker in Management Mode

Answer: D

NEW QUESTION 36
Your internal network is configured to be 10.1.1.0/24. This network is behind your perimeter R77 Gateway, which connects to your ISP provider. How do you configure the Gateway to allow this network to go out to the Internet?

A. Use Hide NAT for network 10.1.1.0/24 behind the external IP address of your perimeter Gateway.
B. Use Hide NAT for network 10.1.1.0/24 behind the internal interface of your perimeter Gateway.
C. Use automatic Static NAT for network 10.1.1.0/24.
D. Do nothing, as long as 10.1.1.0 network has the correct default Gateway.

Answer: A

NEW QUESTION 39
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 44
Which of the following methods will provide the most complete backup of an R77 configuration?

A. Policy Package Management
B. Copying the directories $FWDIR\conf and $CPDIR\conf to another server
C. Execute command upgrade_export
D. Database Revision Control

Answer: C

NEW QUESTION 49
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 52
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 57
A digital signature:

A. Guarantees the authenticity and integrity of a message.
B. Automatically exchanges shared keys.
C. Decrypts data to its original form.
D. Provides a secure key exchange mechanism over the Internet.

Answer: A

NEW QUESTION 61
Which of the following is NOT useful to verify whether or not a Security Policy is active on a Gateway?

A. fw ctl get string active_secpol
B. fw stat
C. cpstat fw -f policy
D. Check the Security Policy name of the appropriate Gateway in SmartView Monitor.

Answer: A

NEW QUESTION 62
What must a Security Administrator do to comply with a management requirement to log all traffic accepted through the perimeter Security Gateway?

A. In Global Properties > Reporting Tools check the box Enable tracking all rules (including rules marked as None in the Track column). Send these logs to a secondary log server for a complete logging histor
B. Use your normal log server for standard logging for troubleshooting.
C. Install the View Implicit Rules package using SmartUpdate.
D. Define two log servers on the R77 Gateway objec
E. Enable Log Implied Rules on the first log serve
F. Enable Log Rule Base on the second log serve
G. Use SmartReporter to merge the two log server records into the same database for HIPPA log audits.
H. Check the Log Implied Rules Globally box on the R77 Gateway object.

Answer: A

NEW QUESTION 64
Message digests use which of the following?

A. DES and RC4
B. IDEA and RC4
C. SSL and MD4
D. SHA-1 and MD5

Answer: D

NEW QUESTION 65
Many companies have defined more than one administrator. To increase security, only one administrator should be able to install a Rule Base on a specific Firewall.
How do you configure this?

A. Define a permission profile in SmartDashboard with read/write privileges, but restrict it to all other firewalls by placing them in the Policy Targets fiel
B. Then, an administrator with this permission profile cannot install a policy on any Firewall not listed here.
C. Put the one administrator in an Administrator group and configure this group in the specific Firewall object in Advanced > Permission to Install.
D. In the object General Properties representing the specific Firewall, go to the Software Blades product list and select Firewal
E. Right-click in the menu, select Administrator to Install to define only this administrator.
F. Right-click on the object representing the specific administrator, and select that Firewall in Policy Targets.

Answer: B

NEW QUESTION 69
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 73
You just installed a new Web server in the DMZ that must be reachable from the Internet. You create a manual Static NAT rule as follows:
Source: Any || Destination: web_public_IP || Service: Any || Translated Source: original || Translated Destination: web_private_IP || Service: Original
“web_public_IP” is the node object that represents the new Web server’s public IP address. “web_private_IP” is the node object that represents the new Web site’s private IP address. You enable all settings from Global Properties > NAT.
When you try to browse the Web server from the Internet you see the error “page cannot be displayed”.
Which of the following is NOT a possible reason?

A. There is no Security Policy defined that allows HTTP traffic to the protected Web server.
B. There is no ARP table entry for the protected Web server’s public IP address.
C. There is no route defined on the Security Gateway for the public IP address to the Web server’s private IP address.
D. There is no NAT rule translating the source IP address of packets coming from the protected Web server.

Answer: A

NEW QUESTION 76
Which answers are TRUE? Automatic Static NAT CANNOT be used when:
1) NAT decision is based on the destination port.
2) Both Source and Destination IP's have to be translated.
3) The NAT rule should only be installed on a dedicated Gateway.
4) NAT should be performed on the server side.

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

Answer: A

NEW QUESTION 80
Which SmartView Tracker selection would most effectively show who installed a Security Policy blocking all traffic from the corporate network?

A. Management tab
B. Custom filter
C. Network and Endpoint tab
D. Active tab

Answer: A

NEW QUESTION 84
Which component functions as the Internal Certificate Authority for R77?

A. Security Gateway
B. Management Server
C. Policy Server
D. SmartLSM

Answer: B

NEW QUESTION 87
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 89
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 93
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 98
Which of the following is a hash algorithm?

A. 3DES
B. IDEA
C. DES
D. MD5

Answer: D

NEW QUESTION 100
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 101
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 105
Your organization’s disaster recovery plan needs an update to the backup and restore section to reap the new distributed R77 installation benefits. Your plan must meet the following required and desired objectives:
Required ObjectivE. The Security Policy repository must be backed up no less frequently than every 24 hours.
Desired ObjectivE. The R77 components that enforce the Security Policies should be backed up at least once a week.
Desired ObjectivE. Back up R77 logs at least once a week.
Your disaster recovery plan is as follows:
- Use the cron utility to run the command upgrade_export each night on the Security Management Servers.
- Configure the organization's routine back up software to back up the files created by the command upgrade_export.

- Configure the GAiA back up utility to back up the Security Gateways every Saturday night.
- Use the cron utility to run the command upgrade_export each Saturday night on the log servers.
- Configure an automatic, nightly logswitch.
- Configure the organization's routine back up software to back up the switched logs every night.

Upon evaluation, your plan:

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

Answer: D

NEW QUESTION 108
In SmartDashboard, Translate destination on client side is checked in Global Properties. When Network Address Translation is used:

A. It is not necessary to add a static route to the Gateway's routing table.
B. It is necessary to add a static route to the Gateway's routing table.
C. The Security Gateway's ARP file must be modified.
D. VLAN tagging cannot be defined for any hosts protected by the Gateway.

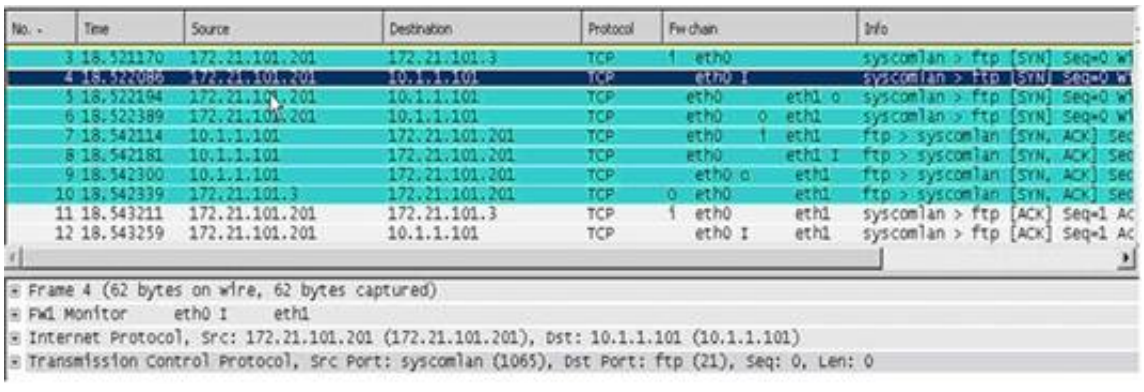
Answer: A

NEW QUESTION 111
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 113
Looking at the SYN packets in the Wireshark output, select the statement that is true about NAT.
Exhibit:



A. This is an example of Hide NAT.
B. There is not enough information provided in the Wireshark capture to determine the NAT settings.
C. This is an example of Static NAT and Translate destination on client side unchecked in Global Properties.
D. This is an example of Static NAT and Translate destination on client side checked in Global Properties.

Answer: D

NEW QUESTION 116
Which SmartConsole tool would you use to see the last policy pushed in the audit log?

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

Answer: A

NEW QUESTION 119
You have a diskless appliance platform. How do you keep swap file wear to a minimum?

A. Issue FW-1 bases its package structure on the Security Management Server, dynamically loading when the firewall is booted.
B. The external PCMCIA-based flash extension has the swap file mapped to it, allowing easy replacement.
C. Use PRAM flash devices, eliminating the longevity.
D. A RAM drive reduces the swap file thrashing which causes fast wear on the device.

Answer: D

NEW QUESTION 123
When restoring R77 using the command upgrade_import, which of the following items are NOT restored?

A. SIC Certificates
B. Licenses
C. Route tables
D. Global properties

Answer: C

NEW QUESTION 127
What is the officially accepted diagnostic tool for IP Appliance Support?

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

Answer: D

NEW QUESTION 130
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 134
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 137
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 140
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 142
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 143
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 146
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 150
Which R77 feature or command allows Security Administrators to revert to earlier Security Policy versions without changing object configurations?

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

Answer: C

NEW QUESTION 151
You believe Phase 2 negotiations are failing while you are attempting to configure a site-to- site VPN with one of your firm's business partners.
Which SmartConsole application should you use to confirm your suspicions?

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

Answer: D

NEW QUESTION 154
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 157
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

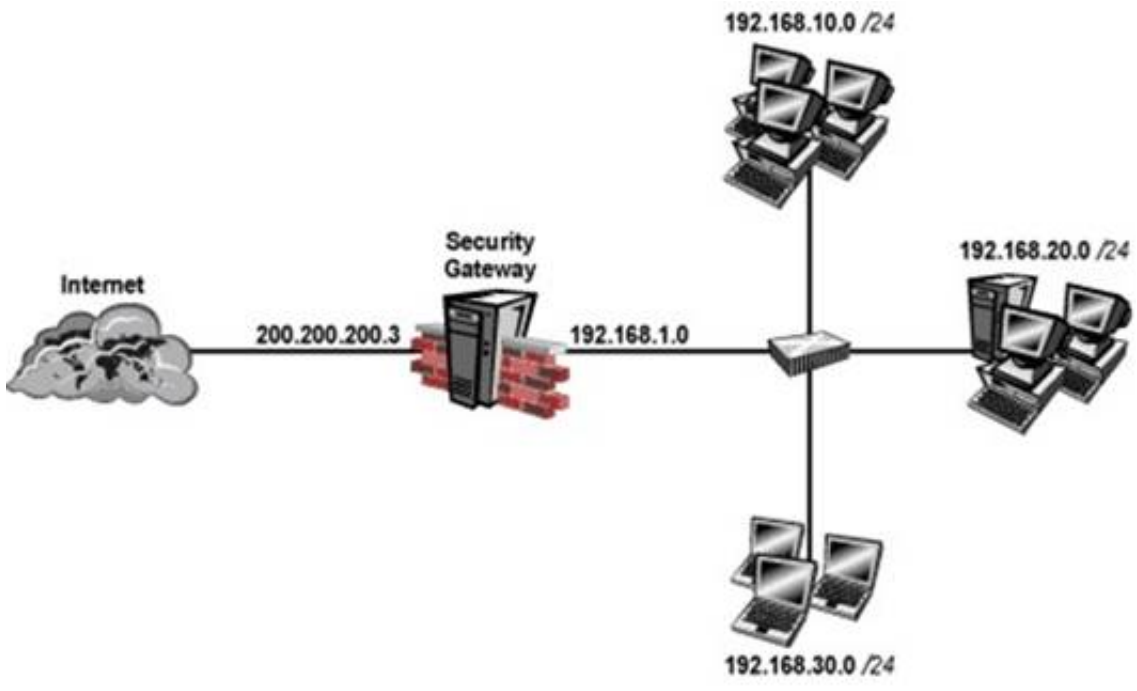
Answer: A

NEW QUESTION 161
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 163
Your perimeter Security Gateway's external IP is 200.200.200.3. Your network diagram shows:



Required. Allow only network 192.168.10.0 and 192.168.20.0 to go out to the Internet, using 200.200.200.5.
The local network 192.168.1.0/24 needs to use 200.200.200.3 to go out to the Internet. Assuming you enable all the settings in the NAT page of Global Properties, how could you
achieve these requirements?

A. Create network objects for 192.168.10.0/24 and 192.168.20.0/24. Enable Hide NAT on both network objects, using 200.200.200.5 as hiding IP addres
B. Add an ARP entry for 200.200.200.3 for the MAC address of 200.200.200.5.
C. Create an Address Range object, starting from 192.168.10.1 to 192.168.20.254. Enable Hide NAT on the NAT page of the address range objec
D. Enter Hiding IP address 200.200.200.5. Add an ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.
E. Create a network object 192.168.0.0/16. Enable Hide NAT on the NAT pag
F. Enter 200.200.200.5 as the hiding IP addres
G. Add an ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.
H. Create two network objects: 192.168.10.0/24 and 192.168.20.0/24. Add the two network objects to a group objec
I. Create a manual NAT rule like the following: Original source - group object; Destination - any; Service - any; Translated source - 200.200.200.5; Destination - original; Service - original.

Answer: B

NEW QUESTION 165
Static NAT connections, by default, translate on which firewall kernel inspection point?

A. Inbound
B. Outbound
C. Post-inbound
D. Eitherbound

Answer: A

NEW QUESTION 168
What happens when you select File > Export from the SmartView Tracker menu?

A. Current logs are exported to a new *.log file.
B. Exported log entries are not viewable in SmartView Tracker.
C. Logs in fw.log are exported to a file that can be opened by Microsoft Excel.
D. Exported log entries are deleted from fw.log.

Answer: C

NEW QUESTION 173
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 176
You are the Security Administrator for ABC-Corp. A Check Point Firewall is installed and in use on GAiA. You are concerned that the system might not be retaining your entries for the
interfaces and routing configuration. You would like to verify your entries in the corresponding file(s) on GAiA. Where can you view them? Give the BEST answer.

A. /etc/sysconfig/netconf.C
B. /etc/conf/route.C
C. /etc/sysconfig/network-scripts/ifcfg-ethx
D. /etc/sysconfig/network

Answer: A

NEW QUESTION 180
SmartView Tracker logs the following Security Administrator activities, EXCEPT:

A. Object creation, deletion, and editing
B. Tracking SLA compliance
C. Administrator login and logout
D. Rule Base changes

Answer: B

NEW QUESTION 184
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	websingapore	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 187
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 189
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 191
When launching SmartDashboard, what information is required to log into R77?

A. User Name, Management Server IP, certificate fingerprint file
B. User Name, Password, Management Server IP
C. Password, Management Server IP
D. Password, Management Server IP, LDAP Server IP

Answer: B

NEW QUESTION 195
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 199
When translation occurs using automatic Hide NAT, what also happens?

A. Nothing happens.
B. The destination is modified.
C. The destination port is modified.
D. The source port is modified.

Answer: D

NEW QUESTION 203
You plan to create a backup of the rules, objects, policies, and global properties from an R77 Security Management Server. Which of the following backup and restore solutions can you use?

1. `upgrade_export` and `upgrade_import` utilities
2. Database revision control
3. SecurePlatform backup utilities
4. Policy package management
5. Manual copies of the `$CPDIR/conf` directory

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

Answer: C

NEW QUESTION 207
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 212
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 an IP address 10.0.0.19 via DHCP.
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. 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.
John plugged in his laptop to the network on a different network segment and he is not able to connect. How does he solve this problem?

A. John should install the Identity Awareness Agent
B. The firewall admin should install the Security Policy
C. John should lock and unlock the computer
D. Investigate this as a network connectivity issue

Answer: B

NEW QUESTION 213
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 214
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 215
When using an encryption algorithm, which is generally considered the best encryption method?

A. Triple DES
B. AES-256
C. CAST cipher
D. DES

Answer: B

NEW QUESTION 219
All R77 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

A. FTP
B. SMTP
C. HTTP
D. RLOGIN

Answer: B

NEW QUESTION 224
Exhibit:

1. Run `cpconfig` on the Gateway, select **Secure Internal Communication**, enter the activation key, and reconfirm.
2. Initialize Internal Certificate Authority (ICA) on the Security Management Server.
3. Configure the Gateway object with the host name and IP addresses for the remote site.
4. Click the **Communication** button in the Gateway object's **General** screen, enter the activation key, and click **Initialize** and **OK**.
5. Install the Security Policy.

You installed Security Management Server on a computer using GAiA in the MegaCorp home office. You use IP address 10.1.1.1. You also installed the Security Gateway on a second GAiA computer, which you plan to ship to another Administrator at a MegaCorp hub office.
What is the correct order for pushing SIC certificates to the Gateway before shipping it?

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

Answer: B

NEW QUESTION 228
Which of the following is a viable consideration when determining Rule Base order?

A. Grouping IPS rules with dynamic drop rules
B. Placing more restrictive rules before more permissive rules
C. Grouping authentication rules with QOS rules
D. Grouping reject and drop rules after the Cleanup Rule

Answer: B

NEW QUESTION 231
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 234
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 239
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 240
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 241
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 246
If you were NOT using IKE aggressive mode for your IPsec tunnel, how many packets would you see for normal Phase 1 exchange?

A. 9
B. 2
C. 3
D. 6

Answer: D

NEW QUESTION 250
When configuring anti-spoofing on the Security Gateway object interfaces, which of the following is NOT a valid R77 topology configuration?

A. External
B. Any
C. Specific
D. Not Defined

Answer: B

NEW QUESTION 254
You are troubleshooting NAT entries in SmartView Tracker. Which column do you check to view the new source IP?

Exhibit:

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. XlateDPort
B. XlateDst
C. XlateSPort
D. XlateSrc

Answer: D

NEW QUESTION 258
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 260
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 263
Why are certificates preferred over pre-shared keys in an IPsec VPN?

A. Weak performanc
B. PSK takes more time to encrypt than Diffie-Hellman.

C. Weak Security: PSK are static and can be brute-forced.
D. Weak security: PSKs can only have 112 bit length.
E. Weak scalability: PSKs need to be set on each and every Gateway.

Answer: B

NEW QUESTION 265
Although SIC was already established and running, Joe reset SIC between the Security Management Server and a remote Gateway. He set a new activation key on the Gateway's side with the command cpconfig and put in the same activation key in the Gateway's object on the Security Management Server. Unfortunately, SIC can not be established. What is a possible reason for the problem?

A. The installed policy blocks the communication.
B. The old Gateway object should have been deleted and recreated.
C. Joe forgot to exit from cpconfig.
D. Joe forgot to reboot the Gateway.

Answer: C

NEW QUESTION 270
If you are experiencing LDAP issues, which of the following should you check?

A. Connectivity between the R77 Gateway and LDAP server
B. Secure Internal Communications (SIC)
C. Overlapping VPN Domains
D. Domain name resolution

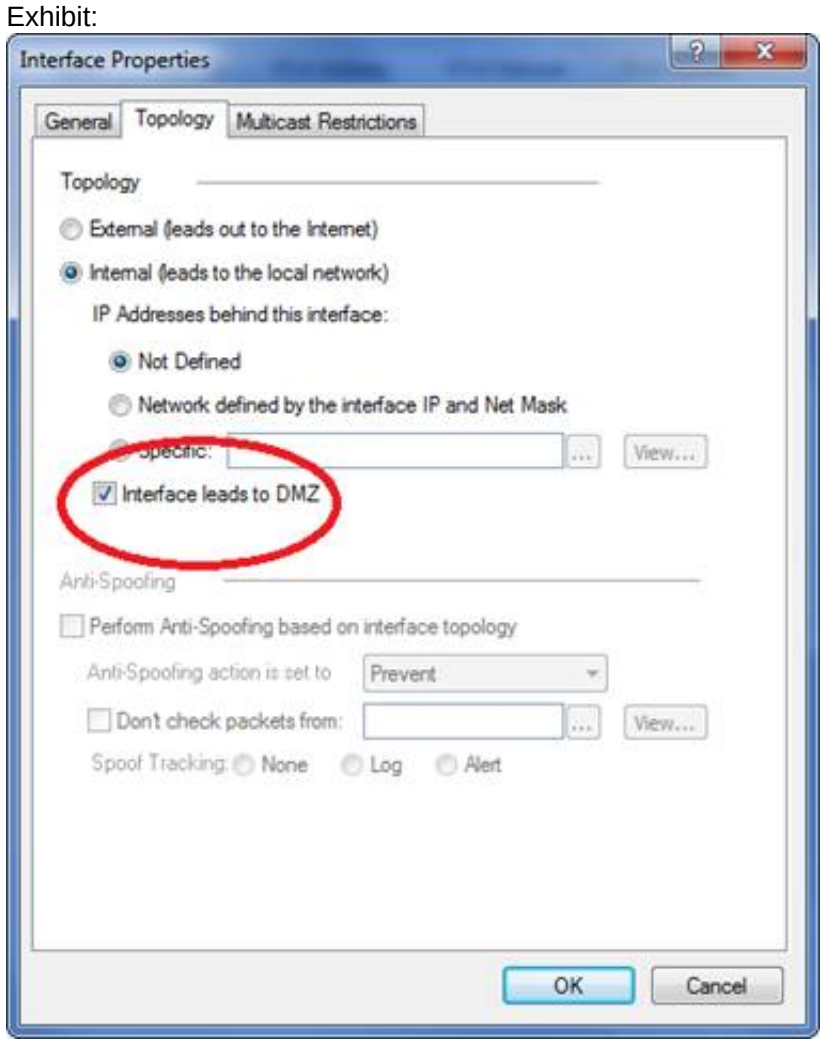
Answer: A

NEW QUESTION 272
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 276
When configuring the Check Point Gateway network interfaces, you can define the direction as Internal or External. What does the option Interface leads to DMZ mean?
Exhibit:



A. Using restricted Gateways, this option automatically turns off the counting of IP Addresses originating from this interface.
B. Activating this option automatically turns this interface to External.
C. It defines the DMZ Interface since this information is necessary for Content Control
D. Select this option to automatically configure Anti-Spoofing to this net.

Answer: C

NEW QUESTION 280
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 282
Choose the BEST sequence for configuring user management in SmartDashboard, using an LDAP server.

A. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object.
B. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties.
C. Enable User Directory in Global Properties, configure a host-node object for the LDAP server, and configure a server object for the LDAP Account Unit.
D. Configure a server object for the LDAP Account Unit, and create an LDAP resource object.

Answer: C

NEW QUESTION 283
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 286
How many packets does the IKE exchange use for Phase 1 Main Mode?

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

Answer: D

NEW QUESTION 287
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 289
Which authentication type permits five different sign-on methods in the authentication properties window?

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

Answer: A

NEW QUESTION 293
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 296
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 297
Exhibit:

1) Create a new activation key on the Security Gateway, then exit `cpconfig`.
2) Click the **Communication** tab on the Security Gateway object, then click **Reset**.
3) Run the `sysconfig` tool, then select **Secure Internal Communication** to reset.
4) Input the new activation key in the Security Gateway object, then click **Initialize**.
5) Run the `cpconfig` tool, then select **Secure Internal Communication** to reset.

Chris has lost SIC communication with his Security Gateway and he needs to re-establish SIC. What would be the correct order of steps needed to perform this task?

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

Answer: A

NEW QUESTION 298
Which of the following allows administrators to allow or deny traffic to or from a specific network based on the user's credentials?

A. Access Policy
B. Access Role
C. Access Rule
D. Access Certificate

Answer: B

NEW QUESTION 300
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 305
When you use the Global Properties' default settings on R77, which type of traffic will be dropped if NO explicit rule allows the traffic?

A. SmartUpdate connections
B. Outgoing traffic originating from the Security Gateway
C. Firewall logging and ICA key-exchange information
D. RIP traffic

Answer: D

NEW QUESTION 307
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 308
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 310
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 314
What is the purpose of an Identity Agent?

A. Provide user and machine identity to a gateway
B. Manual entry of user credentials for LDAP authentication
C. Audit a user's access, and send that data to a log server
D. Disable Single Sign On

Answer: A

NEW QUESTION 316
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 319
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 324
A Security Policy installed by another Security Administrator has blocked all SmartDashboard connections to the stand-alone installation of R77. After running the command fw unloadlocal, you are able to reconnect with SmartDashboard and view all changes. Which of the following change is the most likely cause of the block?

A. The Allow Control Connections setting in Policy > Global Properties has been unchecked.
B. A Stealth Rule has been configured for the R77 Gateway.
C. The Security Policy installed to the Gateway had no rules in it.
D. The Gateway Object representing your Gateway was configured as an Externally Managed VPN Gateway.

Answer: A

NEW QUESTION 325
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 329
Spoofing is a method of:

A. Making packets appear as if they come from an authorized IP address.
B. Detecting people using false or wrong authentication logins.
C. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
D. Hiding your firewall from unauthorized users.

Answer: A

NEW QUESTION 333
You would use the Hide Rule feature to:

A. View only a few rules without the distraction of others.
B. Hide rules from read-only administrators.
C. Hide rules from a SYN/ACK attack.
D. Make rules invisible to incoming packets.

Answer: A

NEW QUESTION 337
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 342
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 344
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 346
Certificates for Security Gateways are created during a simple initialization from ____.

A. sysconfig
B. The ICA management tool
C. SmartUpdate
D. SmartDashboard

Answer: D

NEW QUESTION 349
How can you activate the SNMP daemon on a Check Point Security Management Server?

A. Using the command line, enter snmp_install.
B. From cpconfig, select SNMP extension.
C. Any of these options will work.
D. In SmartDashboard, right-click a Check Point object and select Activate SNMP.

Answer: B

NEW QUESTION 352
How does the button Get Address, found on the Host Node Object > General Properties page retrieve the address?

A. Route Table
B. SNMP Get
C. Address resolution (ARP, RARP)
D. Name resolution (hosts file, DNS, cache)

Answer: D

NEW QUESTION 354
Reviewing the Rule Base, you see that is responsible for the client authentication 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	Log	Policy Targets
3	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log	Policy Targets
4	0	Client Auth	webSydney	webSingapore	Any Traffic	http	Client Aut	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	accept	Log	Policy Targets
7	0	FTP	Any	webSingapore	Any Traffic	ftp	accept	Log	fwsydney
8	0	FTP	Any	webSingapore	Any Traffic	ftp	accept	Account	fwsingapore
9	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets

A. Rule 4
B. Rule 7
C. Rule 8
D. Rule 5

Answer: A

NEW QUESTION 357
How many packets are required for IKE Phase 2?

A. 12
B. 2
C. 6
D. 3

Answer: D

NEW QUESTION 359
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 364
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 368
Which of the following is NOT true for Clientless VPN?

A. The Gateway can enforce the use of strong encryption.
B. The Gateway accepts any encryption method that is proposed by the client and supported in the VPN.
C. Secure communication is provided between clients and servers that support HTTP.
D. User Authentication is supported.

Answer: C

NEW QUESTION 370
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 375
With the User Directory Software Blade, you can create R77 user definitions on a(n)
Server.

A. LDAP
B. Radius
C. SecureID
D. NT Domain

Answer: A

NEW QUESTION 380
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 383
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 386
Which statement below describes the most correct strategy for implementing a Rule Base?

A. Limit grouping to rules regarding specific access.
B. Place the most frequently used rules at the top of the Policy and the ones that are not frequently used further down.
C. Place a network-traffic rule above the administrator access rule.
D. Add the Stealth Rule before the last rule.

Answer: B

NEW QUESTION 387
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 391
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 395
Identify the ports to which the Client Authentication daemon listens by default.

A. 259, 900
B. 256, 600
C. 80, 256
D. 8080, 529

Answer: A

NEW QUESTION 400
Match the terms with their definitions: Exhibit:

Term	Definition
A. VPN Community	1. Traffic routed to VPN tunnel based on route table entries
B. VPN Domain	2. Hosts behind the Gateway
C. Domain based VPN	3. Collection of VPN tunnels
D. Route based VPN	4. Traffic routed to VPN tunnel based on object definitions

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

Answer: A

NEW QUESTION 404
When using vpn tu, which option must you choose if you only want to clear phase 2 for a specific IP (gateway)?
Exhibit:

A. (5) Delete all IPsec SAs for a given peer (GW)
B. (7) Delete all IPsec+IKE SAs for a given peer (GW)
C. (6) Delete all IPsec SAs for a given User (Client)
D. (8) Delete all IPsec+IKE SAs for a given User (Client)

Answer: A

NEW QUESTION 408
John is the Security Administrator in his company. He installs a new R77 Security Management Server and a new R77 Gateway. He now wants to establish SIC between them. After entering the activation key, he gets the following message in SmartDashboard -
“Trust established?”
SIC still does not seem to work because the policy won’t install and interface fetching does not work. What might be a reason for this?

A. SIC does not function over the network.
B. It always works when the trust is established
C. The Gateway’s time is several days or weeks in the future and the SIC certificate is not yet valid.
D. This must be a human error.

Answer: C

NEW QUESTION 411
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 416
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 419
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 420
If a Security Gateway enforces three protections, LDAP Injection, Malicious Code Protector, and Header Rejection, which Check Point license is required in SmartUpdate?

A. IPS
B. SSL: VPN
C. SmartEvent Intro
D. Data Loss Prevention

Answer: A

NEW QUESTION 425
How can you most quickly reset Secure Internal Communications (SIC) between a Security Management Server and Security Gateway?

A. From cpconfig on the Gateway, choose the Secure Internal Communication option and retype the activation ke
B. Next, retype the same key in the Gateway object in SmartDashboard and reinitialize Secure Internal Communications (SIC).
C. Use SmartUpdate to retype the Security Gateway activation ke
D. This will automatically sync SIC to both the Security Management Server and Gateway.
E. From the Security Management Server's command line, type fw putkey -p <shared key><IP Address of Security Gateway>.
F. Run the command fwm sic_reset to reinitialize the Security Management Server Internal Certificate Authority (ICA). Then retype the activation key on the Security Gateway from SmartDashboard.

Answer: A

NEW QUESTION 428
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 433
Which command enables IP forwarding on IPSO?

A. ipsofwd on admin
B. echo 0 > /proc/sys/net/ipv4/ip_forward
C. clish -c set routing active enable
D. echo 1 > /proc/sys/net/ipv4/ip_forward

Answer: A

NEW QUESTION 437
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 438
Which command displays the installed Security Gateway version?

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

Answer: A

NEW QUESTION 440
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 441
Access Role objects define users, machines, and network locations as:

A. Credentialed objects
B. Linked objects
C. One object
D. Separate objects

Answer: C

NEW QUESTION 442
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 446
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 449
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 454

Where are SmartEvent licenses installed?

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

Answer: A

NEW QUESTION 459
Several Security Policies can be used for different installation targets. The firewall protecting Human Resources' servers should have a unique Policy Package. These rules may only be installed on this machine and not accidentally on the Internet firewall. How can this be configured?

A. When selecting the correct firewall in each line of the row Install On of the Rule Base, only this firewall is shown in the list of possible installation targets after selecting Policy > Install.
B. A Rule Base can always be installed on any Check Point firewall objec
C. It is necessary to select the appropriate target directly after selecting Policy > Install.
D. In the SmartDashboard policy, select the correct firewall to be the Specific Target of the rule.
E. A Rule Base is always installed on all possible target
F. The rules to be installed on a firewall are defined by the selection in the row Install On of the Rule Base.

Answer: C

NEW QUESTION 460
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 464
How do you recover communications between your Security Management Server and Security Gateway if you lock yourself out through a rule or policy mis-configuration?

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

Answer: B

NEW QUESTION 469
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 474
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 479
Which command allows you to view the contents of an R77 table?

A. fw tab -a <tablename>
B. fw tab -t <tablename>
C. fw tab -s <tablename>
D. fw tab -x <tablename>

Answer: B

NEW QUESTION 484

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 486
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 490
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 492
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.

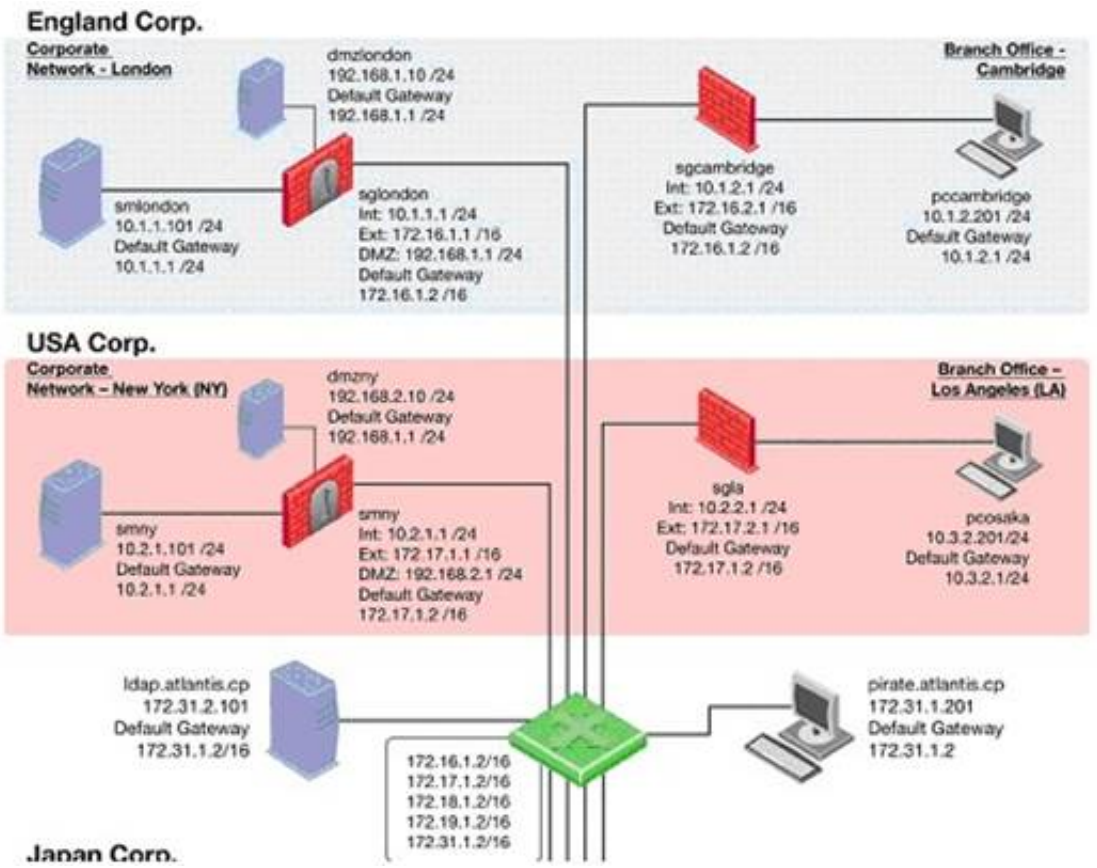
Answer: B

NEW QUESTION 495
Which of the following authentication methods can be configured in the Identity Awareness setup wizard?

A. Check Point Password
B. TACACS
C. LDAP
D. Windows password

Answer: C

NEW QUESTION 498
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 502
Which command gives an overview of your installed licenses?

A. cplicense
B. showlic
C. fw lic print
D. cplic print

Answer: D

NEW QUESTION 503
How can you reset the Security Administrator password that was created during initial Security Management Server installation on GAiA?

A. Launch SmartDashboard in the User Management screen, and edit the cpconfig administrator.
B. As expert user Type fwm -a, and provide the existing administrator's account nam
C. Reset the Security Administrator's password.
D. Type cpm -a, and provide the existing administrator's account nam
E. Reset the Security Administrator's password.
F. Export the user database into an ASCII file with fwm dbexpor
G. Open this file with an editor, and delete the Password portion of the fil
H. Then log in to the account without a passwor
I. You will be prompted to assign a new password.

Answer: B

NEW QUESTION 506
What is the primary benefit of using the command upgrade_export over either backup or snapshot?

A. upgrade_export is operating system independent and can be used when backup or snapshot is not available.
B. upgrade_export will back up routing tables, hosts files, and manual ARP configurations, where backup and snapshot will not.
C. The commands backup and snapshot can take a long time to run whereas upgrade_export will take a much shorter amount of time.
D. upgrade_export has an option to back up the system and SmartView Tracker logs while backup and snapshot will not.

Answer: A

NEW QUESTION 507
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 511
Which item below in a Security Policy would be enforced first?

A. IP spoofing/IP options
B. Security Policy First rule
C. Administrator-defined Rule Base
D. Network Address Translation

Answer: A

NEW QUESTION 514
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 517
Identify the correct step performed by SmartUpdate to upgrade a remote Security Gateway. After selecting Packages > Distribute and Install Selected Package and choosing the target Gateway, the:

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

Answer: A

NEW QUESTION 520
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 524
Which of the following is NOT defined by an Access Role object?

A. Source Network
B. Source Machine
C. Source User
D. Source Server

Answer: D

NEW QUESTION 525
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 527
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 529
A rule is used to prevent all traffic going to the R77 Security Gateway.

A. IPS
B. Cleanup
C. Reject
D. Stealth

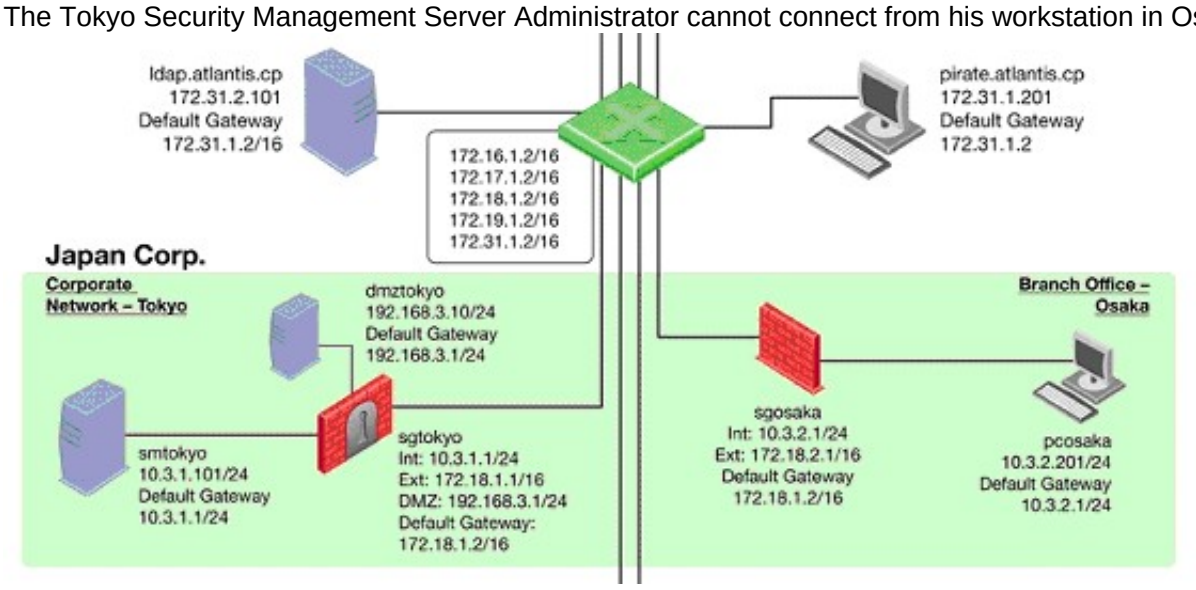
Answer: D

NEW QUESTION 530
You need to completely reboot the Operating System after making which of the following changes on the Security Gateway? (i.e. the command cprestart is not sufficient.)
1. Adding a hot-swappable NIC to the Operating System for the first time.
2. Uninstalling the R77 Power/UTM package.
3. Installing the R77 Power/UTM package.
4. Re-establishing SIC to the Security Management Server.
5. Doubling the maximum number of connections accepted by the Security Gateway.

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

Answer: C

NEW QUESTION 531
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 532
All of the following are Security Gateway control connections defined by default implied rules, EXCEPT:

A. Exclusion of specific services for reporting purposes.
B. Acceptance of IKE and RDP traffic for communication and encryption purposes.
C. Communication with server types, such as RADIUS, CVP, UFP, TACACS, and LDAP.
D. Specific traffic that facilitates functionality, such as logging, management, and key exchange.

Answer: A

NEW QUESTION 537
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 539
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 544
Which of the following firewall modes DOES NOT allow for Identity Awareness to be deployed?

A. Bridge
B. Load Sharing
C. High Availability
D. Fail Open

Answer: A

NEW QUESTION 548
What mechanism does a gateway configured with Identity Awareness and LDAP initially use to communicate with a Windows 2003 or 2008 server?

A. WMI
B. CIFS
C. RCP
D. LDAP

Answer: A

NEW QUESTION 552
Installing a policy usually has no impact on currently existing connections. Which statement is TRUE?

A. Users being authenticated by Client Authentication have to re-authenticate.
B. All connections are reset, so a policy install is recommended during announced downtime only.
C. All FTP downloads are reset; users have to start their downloads again.
D. Site-to-Site VPNs need to re-authenticate, so Phase 1 is passed again after installing the Security Policy.

Answer: A

NEW QUESTION 553
A snapshot delivers a complete GAiA backup. The resulting file can be stored on servers or as a local file in /var/CPsnapshot/snapshots. How do you restore a local snapshot named MySnapshot.tgz?

A. Reboot the system and call the start men
B. Select the option Snapshot Management, provide the Expert password and select [L] for a restore from a local fil
C. Then, provide the correct file name.
D. As expert user, type the command snapshot -r MySnapshot.tgz.
E. As expert user, type the command revert --file MySnapshot.tgz.
F. As expert user, type the command snapshot - R to restore from a local fil
G. Then, provide the correct file name.

Answer: C

NEW QUESTION 555
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 558
You are the Security Administrator for MegaCorp. A Check Point firewall is installed and in use on a platform using GAiA. You have trouble configuring the speed and duplex settings of your Ethernet interfaces. Which of the following commands can be used in CLISH to configure the speed and duplex settings of an Ethernet interface and will survive a reboot? Give the BEST answer.

A. ethtool

B. set interface <options>
C. mii_tool
D. ifconfig -a

Answer: B

NEW QUESTION 563
ALL of the following options are provided by the GAiA sysconfig utility, EXCEPT:

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

Answer: D

NEW QUESTION 564
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 565
A Security Policy has several database versions. What configuration remains the same no matter which version is used?

A. Objects_5_0.C
B. Internal Certificate Authority (ICA) certificate
C. Rule Bases_5_0.fws
D. fwauth.NDB

Answer: B

NEW QUESTION 570
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 571
What is the purpose of a Stealth Rule?

A. To prevent users from connecting directly to the gateway.
B. To permit management traffic.
C. To drop all traffic to the management server that is not explicitly permitted.
D. To permit implied rules.

Answer: A

NEW QUESTION 576
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 580
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 583
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 586
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 589
What are you required to do before running the command upgrade_export?

A. Run a cpstop on the Security Gateway.
B. Run a cpstop on the Security Management Server.
C. Close all GUI clients.
D. Run cpconfig and set yourself up as a GUI client.

Answer: C

NEW QUESTION 592
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 594
What command syntax would you use to see accounts the gateway suspects are service accounts?

A. pdp check_log
B. pdp show service
C. adlog check_accounts
D. adlog a service_accounts

Answer: D

NEW QUESTION 597
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 598
What happens if the identity of a user is known?

A. If the user credentials do not match an Access Role, the system displays the Captive Portal.
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 traffic is automatically dropped.
D. If the user credentials match an Access Role, the rule is applied and traffic is accepted or dropped based on the defined action.

Answer: D

NEW QUESTION 602
Which of the following authentication methods can be configured in the Identity Awareness setup wizard?

A. TACACS
B. Captive Portal
C. Check Point Password
D. Windows password

Answer: B

NEW QUESTION 607
You intend to upgrade a Check Point Gateway from R71 to R77. Prior to upgrading, you want to back up the Gateway should there be any problems with the upgrade. Which of the following allows for the Gateway configuration to be completely backed up into a manageable size in the least amount of time?

A. database revision
B. snapshot
C. upgrade_export
D. backup

Answer: D

NEW QUESTION 611
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 612
What does SmartUpdate allow you to do?

A. SmartUpdate only allows you to update Check Point and OPSEC certified products.
B. SmartUpdate only allows you to manage product licenses.
C. SmartUpdate allows you to update Check Point and OPSEC certified products and to manage product licenses.
D. SmartUpdate is not a Check Point product.

Answer: C

NEW QUESTION 617
How do you configure an alert in SmartView Monitor?

A. An alert cannot be configured in SmartView Monitor.
B. By choosing the Gateway, and Configure Thresholds.
C. By right-clicking on the Gateway, and selecting Properties.
D. By right-clicking on the Gateway, and selecting System Information.

Answer: B

NEW QUESTION 619
SmartUpdate is mainly for which kind of work –
1. Monitoring Performance and traffic
2. Provision Package
3. Managing licenses
4. Creating a Rule Base

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

Answer: A

NEW QUESTION 620
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 625
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 627
What port is used for communication to the User Center with SmartUpdate?

A. CPMI 200
B. TCP 8080
C. HTTP 80
D. HTTPS 443

Answer: D

NEW QUESTION 631
Which of the following is NOT an option for internal network definition of Anti-spoofing?

A. Specific – derived from a selected object
B. Route-based – derived from gateway routing table
C. Network defined by the interface IP and Net Mask
D. Not-defined

Answer: B

NEW QUESTION 634
How can you activate the SNMP daemon on a Check Point Security Management Server?

A. Using the command line, enter snmp_install.
B. From cpconfig, select SNMP extension.
C. Any of these options will work.
D. In SmartDashboard, right-click a Check Point object and select Activate SNMP.

Answer: B

NEW QUESTION 638
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 642
A company has disabled logging for some of the most commonly used Policy rules. This was to decrease load on the Security Management Server and to make tracking dropped connections easier. What action would you recommend to get reliable statistics about the network traffic using SmartReporter?

A. SmartReporter analyzes all network traffic, logged or not.
B. Network traffic cannot be analyzed when the Security Management Server has a high load.
C. Turn the field Track of each rule to LOG.
D. Configure Additional Logging on an additional log server.

Answer: D

NEW QUESTION 643
Which answer below best describes the Administrator Auditing options available in SmartView Tracker?

A. Compliance information compiled from network activity is recorded in logs
B. Administrator network activity observed and logged by gateways
C. Accounting information gathered on network activity as recorded in logs
D. Administrator login and logout, object manipulation, and rule base changes

Answer: D

NEW QUESTION 644
Which of the following is true of a Stealth Rule?

A. The Stealth rule should not be logged
B. The Stealth rule is required for proper firewall protection
C. The Stealth rule should be located just before the Cleanup rule
D. The Stealth rule must be the first rule in a policy

Answer: B

NEW QUESTION 649
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 652
The R77 fw monitor utility is used to troubleshoot which of the following problems?

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

Answer: A

NEW QUESTION 653
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 654
What is also referred to as Dynamic NAT?

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

Answer: D

NEW QUESTION 657
Choose the correct statement regarding Stealth Rules:

A. The Stealth Rule is a default rule that always exists when using Check Point products.
B. The Stealth Rule is part of the Implicit rules.
C. Check Point recommends you include a Stealth Rule as a best practice.
D. The Stealth Rule is a rule that hides your internal networks.

Answer: C

NEW QUESTION 659
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 660
Jack has locked himself out of the Kirk Security Gateway with an incorrect policy and can no longer connect from the McCoy Management Server.
Jack still has access to an out of band console connection on the Kirk Security Gateway. He is logged into the Gaia CLI, what does he need to enter in order to be able to fix his mistake and push policy?

A. Kirk> fw unload local
B. Kirk> fw unloadlocal
C. Kirk> fw unload policy
D. Kirk> fw fetch policy

Answer: B

NEW QUESTION 663
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 666
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 671
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 675
Which tool CANNOT be launched from SmartUpdate R77?

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

Answer: B

NEW QUESTION 679
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 681
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.

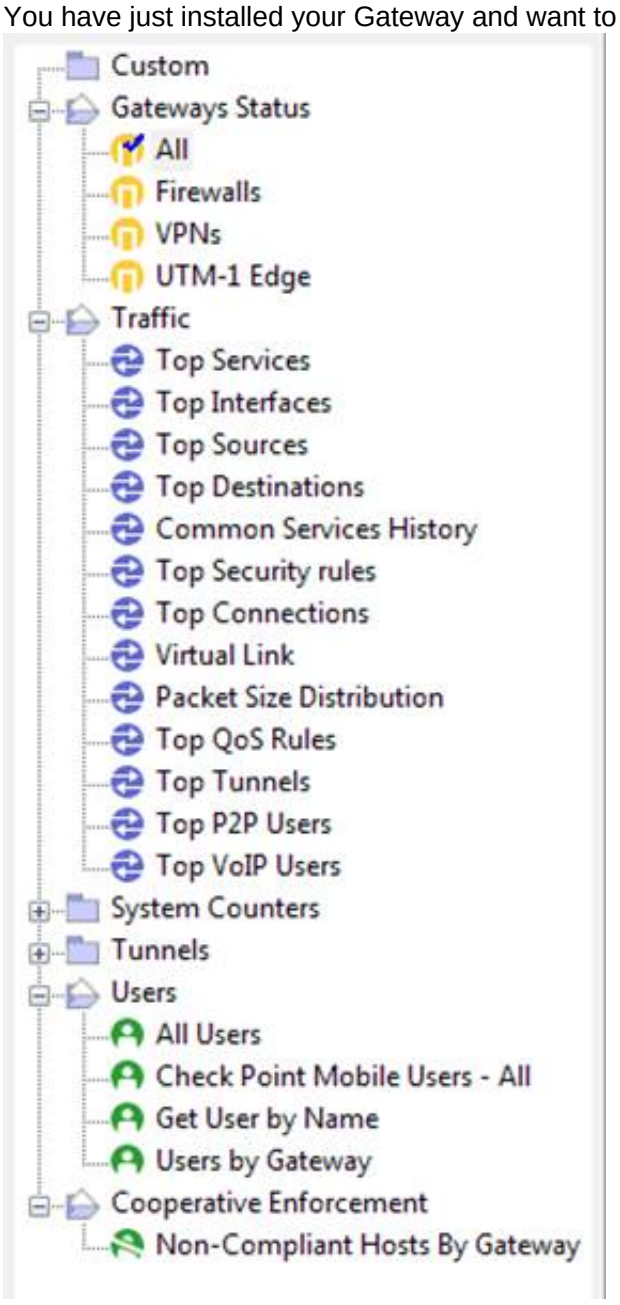
Answer: C

NEW QUESTION 686
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 689
You have just installed your Gateway and want to analyze the packet size distribution of your traffic with SmartView Monitor.



Unfortunately, you get the message.
"There are no machines that contain Firewall Blade and SmartView Monitor."

What should you do to analyze the packet size distribution of your traffic? Give the BEST answer.

A. Purchase the SmartView Monitor license for your Security Management Server.
B. Enable Monitoring on your Security Management Server.
C. Purchase the SmartView Monitor license for your Security Gateway.
D. Enable Monitoring on your Security Gateway.

Answer: D

NEW QUESTION 692
Which port must be allowed to pass through enforcement points in order to allow packet logging to operate correctly?

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

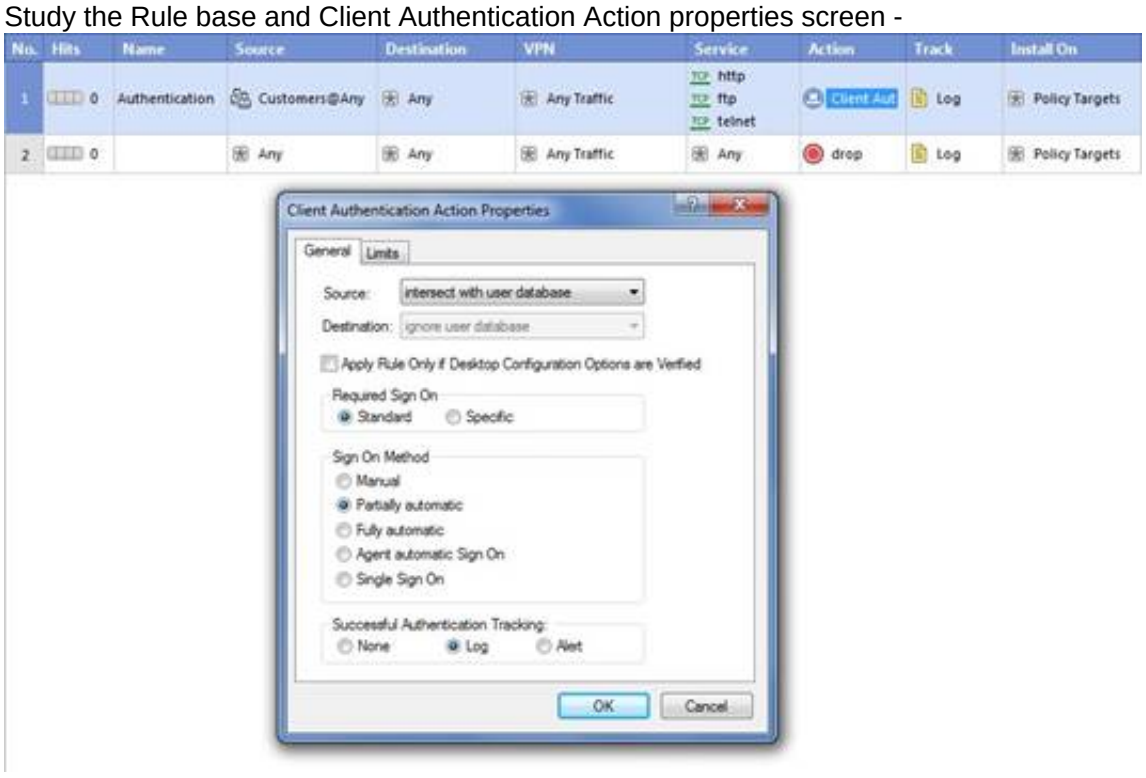
Answer: B

NEW QUESTION 697
In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?

A. Rule 0
B. Blank field under Rule Number
C. Rule 1
D. Cleanup Rule

Answer: A

NEW QUESTION 698
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 701
When configuring LDAP authentication, which of the following items should be configured for the Security Management Server?

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

Answer: A

NEW QUESTION 703
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 708
What information is found in the SmartView Tracker Management log?

A. SIC revoke certificate event
B. Destination IP address
C. Most accessed Rule Base rule
D. Number of concurrent IKE negotiations

Answer: A

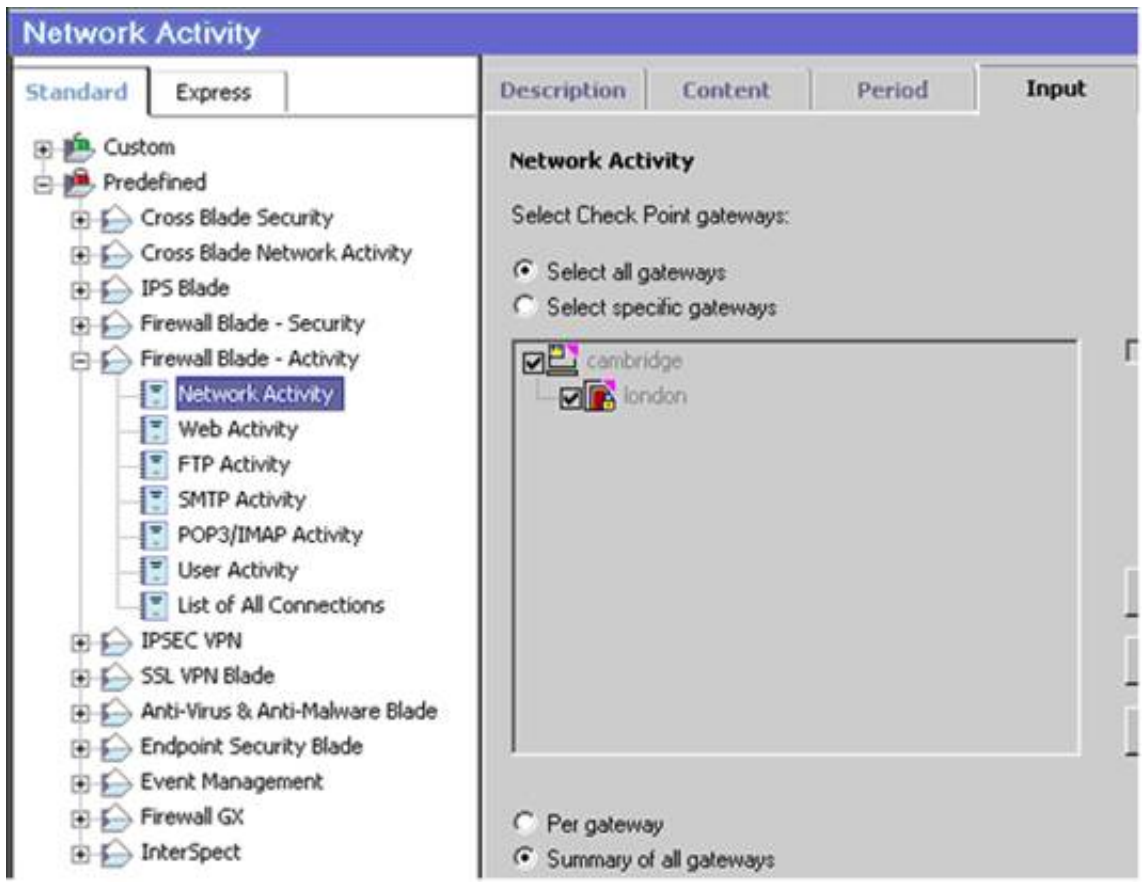
NEW QUESTION 710
In the Rule Base displayed for fwsingapore, user authentication in Rule 4 is configured as fully automatic. Eric is a member of the LDAP group, MSD_Group.
What happens when Eric tries to connect to a server on the Internet?

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

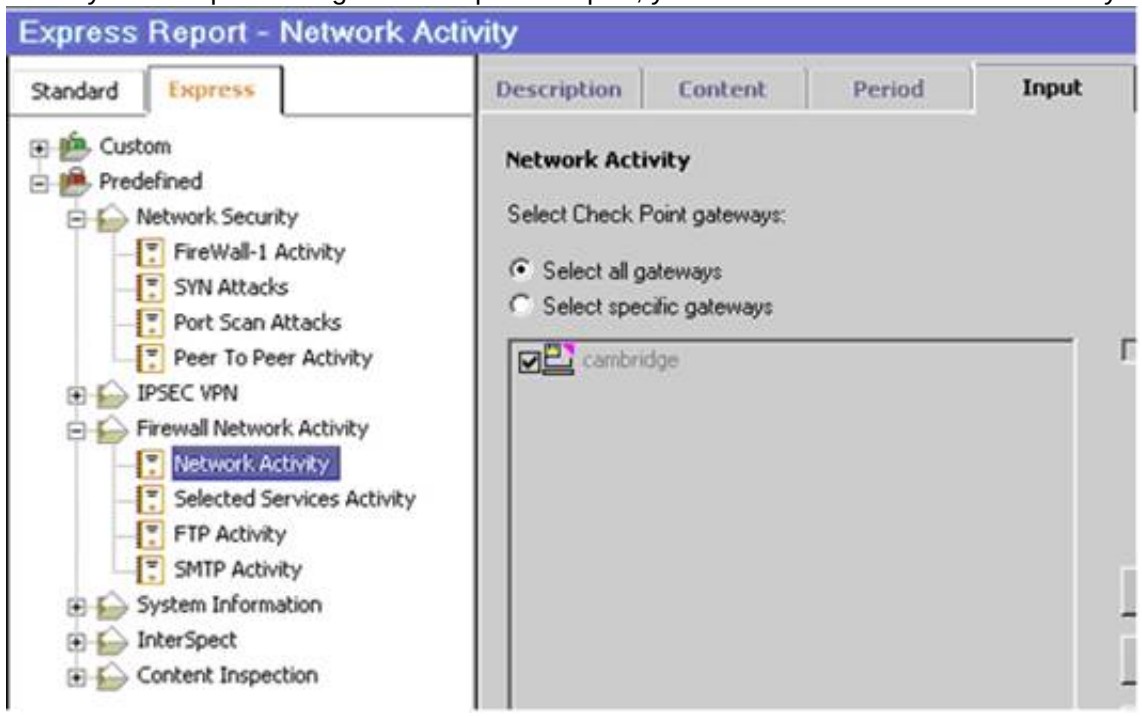
A. None of these things will happen.
B. Eric will be authenticated and get access to the requested server.
C. Eric will be blocked because LDAP is not allowed in the Rule Base.
D. Eric will be dropped by the Stealth Rule.

Answer: D

NEW QUESTION 715
You are the Security Administrator for MegaCorp and would like to view network activity using SmartReporter. You select a standard predefined report. As you can see here, you can select the london Gateway.



When you attempt to configure the Express Report, you are unable to select this Gateway.



What is the reason for this behavior? Give the BEST answer.

A. You must enable the Eventia Express Mode on the london Gateway.
B. You have the license for Eventia Reporter in Standard mode only.
C. You must enable the Express Mode inside Eventia Reporter.
D. You must enable Monitoring in the london Gateway object's General Properties.

Answer: D

NEW QUESTION 718
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 722
What CLI utility allows an administrator to capture traffic along the firewall inspection chain?

A. show interface (interface) - chain
B. tcpdump
C. tcpdump/ snoop
D. fw monitor

Answer: D

NEW QUESTION 727

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 732
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 735
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 738
What information is found in the SmartView Tracker Management log?

A. Historical reports log
B. Policy rule modification date/time stamp
C. Destination IP address
D. Most accessed Rule Base rule

Answer: B

NEW QUESTION 739
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 743
Which authentication type requires specifying a contact agent in the Rule Base?

A. Client Authentication with Partially Automatic Sign On
B. Client Authentication with Manual Sign On
C. User Authentication
D. Session Authentication

Answer: D

NEW QUESTION 744
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 747
One of your remote Security Gateways 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 748
Where do we need to reset the SIC on a gateway object?

A. SmartDashboard > Edit Gateway Object > General Properties > Communication
B. SmartUpdate > Edit Security Management Server Object > SIC
C. SmartUpdate > Edit Gateway Object > Communication
D. SmartDashboard > Edit Security Management Server Object > SIC

Answer: D

NEW QUESTION 752
VPN gateways must authenticate to each other prior to exchanging information. What are the two types of credentials used for authentication?

A. 3DES and MD5
B. Certificates and IPsec
C. Certificates and pre-shared secret
D. IPsec and VPN Domains

Answer: C

NEW QUESTION 757
What information is found in the SmartView Tracker Management log?

A. Creation of an administrator using cpconfig
B. GAiA expert login event
C. FTP username authentication failure
D. Administrator SmartDashboard logout event

Answer: D

NEW QUESTION 759
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 760
Which directory holds the SmartLog index files by default?

A. $ SMARTLOGDIR/ data
B. $ SMARTLOG/ dir
C. $ FWDIR/ smartlog
D. $ FWDIR/ log

Answer: A

Explanation: SmartLog creates and uses index files for fast access to log file contents. The index files are located by default at $SMARTLOGDIR/data.

NEW QUESTION 763
Lilly needs to review VPN History counters for the last week. Where would she do this?

A. SmartView Monitor > Tunnels > VPN History
B. SmartView Monitor > System Counters > VPN History
C. SmartView Monitor > System Counters > Firewall Security History
D. SmartView Monitor > System Counters > VPN

Answer: B

NEW QUESTION 766
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 770
For remote user authentication, which authentication scheme is NOT supported?

A. Check Point Password
B. RADIUS
C. TACACS
D. SecurID

Answer: C

NEW QUESTION 771
.....

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