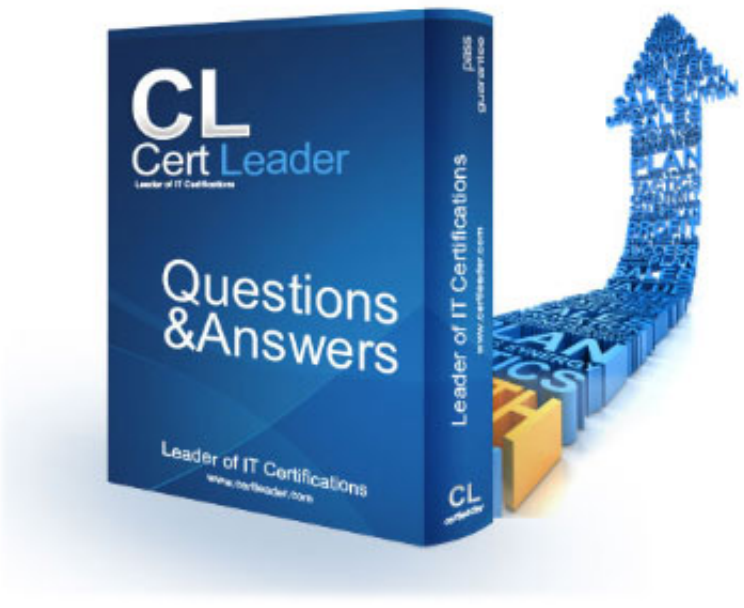
156-215.77 Dumps

Check Point Certified Security Administrator – GAiA

https://www.certleader.com/156-215.77-dumps.html



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

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

Answer: C

NEW QUESTION 2
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 3
An internal host initiates a session to the Google.com website and is set for Hide NAT behind the Security Gateway. The initiating traffic is an example of .

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

Answer: B

NEW QUESTION 4
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 5
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 6
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 7
After filtering a fw monitor trace by port and IP, a packet is displayed three times; in the i, I, and o inspection points, but not in the O inspection point.
Which is the likely source of the issue?

A. The packet has been sent out through a VPN tunnel unencrypted.
B. An IPSO ACL has blocked the packet’s outbound passage.
C. A SmartDefense module has blocked the packet.
D. It is due to NAT.

Answer: D

NEW QUESTION 8

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 9
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 10
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 10
You have detected a possible intruder listed in SmartView Tracker's active pane. What is the fastest method to block this intruder from accessing your network indefinitely?

A. Modify the Rule Base to drop these connections from the network.
B. In SmartView Tracker, select Tools > Block Intruder.
C. In SmartView Monitor, select Tools > Suspicious Activity Rules.
D. In SmartDashboard, select IPS > Network Security > Denial of Service.

Answer: B

NEW QUESTION 15
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 18
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 19
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 24
You receive a notification that long-lasting Telnet connections to a mainframe are dropped after an hour of inactivity. Reviewing SmartView Tracker shows the packet is dropped with the error:
Unknown established connection
How do you resolve this problem without causing other security issues? Choose the BEST answer.

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

Answer: D

NEW QUESTION 29
Which rule is responsible for the client authentication failure? Exhibit:

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

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

Answer: C

NEW QUESTION 31
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 32
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 37
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 42
When using GAiA, it might be necessary to temporarily change the MAC address of the interface eth 0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?

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

As expert user, issue these commands:

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

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

Answer: C

NEW QUESTION 45
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 50
A host on the Internet initiates traffic to the Static NAT IP of your Web server behind the Security Gateway. With the default settings in place for NAT, the initiating packet will translate the .

A. destination on server side
B. source on server side
C. source on client side
D. destination on client side

Answer: D

NEW QUESTION 55
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 59
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 64
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 67
Which of the following is a hash algorithm?

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

Answer: D

NEW QUESTION 72
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 77
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 82
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 83
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 86
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 87
What is the officially accepted diagnostic tool for IP Appliance Support?

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

Answer: D

NEW QUESTION 88
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 89
Select the TRUE statements about the Rule Base shown? Exhibit:

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

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

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

Answer: D

NEW QUESTION 91
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 96
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 100
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 104
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 106
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 111
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 113
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 116
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 121
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 123
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 128
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 132
You have created a Rule Base for firewall, websydney. Now you are going to create a new policy package with security and address translation rules for a second Gateway. What is TRUE about the new package's NAT rules?
Exhibit:

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

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

Answer: A

NEW QUESTION 133
You are MegaCorp's Security Administrator. There are various network objects which must be NATed. Some of them use the Automatic Hide NAT method, while others use the Automatic Static NAT method. What is the rule order if both methods are used together? Give the BEST answer.

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

Answer: B

NEW QUESTION 134
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 139
You are about to test some rule and object changes suggested in an R77 news group.
Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

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

Answer: C

NEW QUESTION 140
Where can an administrator configure the notification action in the event of a policy install time change?

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

Answer: A

NEW QUESTION 142
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 144
How many packets does the IKE exchange use for Phase 1 Aggressive Mode?

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

Answer: C

NEW QUESTION 148
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 149
For which service is it NOT possible to configure user authentication?

A. Telnet
B. SSH
C. FTP
D. HTTPS

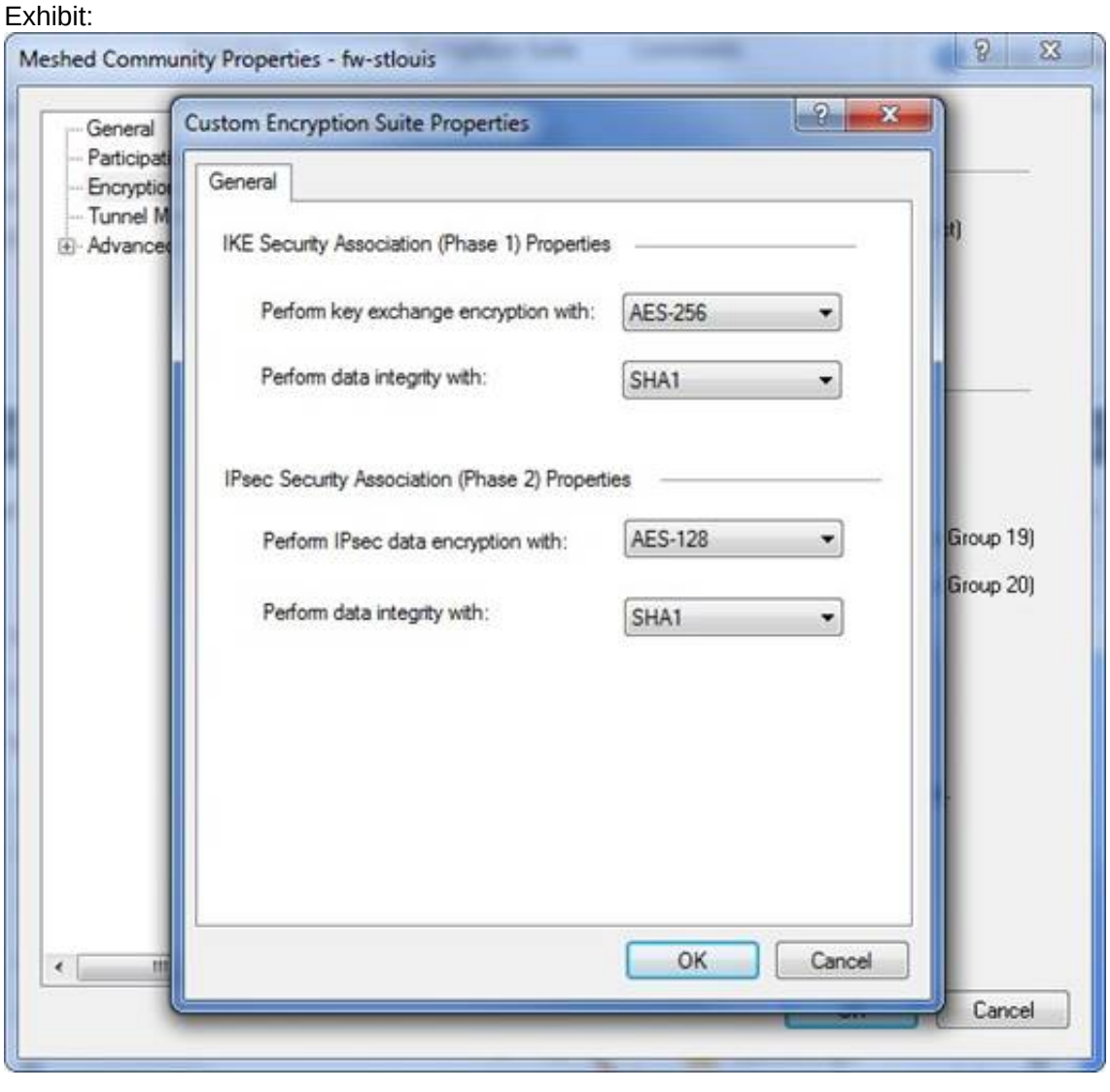
Answer: B

NEW QUESTION 150
You cannot use SmartDashboard's User Directory features to connect to the LDAP server. What should you investigate?
1) Verify you have read-only permissions as administrator for the operating system.
2) Verify there are no restrictions blocking SmartDashboard's User Manager from connecting to the LDAP server.
3) Check that the login Distinguished Name configured has root permission (or at least write permission Administrative access) in the LDAP Server's access control configuration.

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

Answer: B

NEW QUESTION 154
You have a mesh VPN Community configured to create a site-to-site VPN. Given the displayed VPN properties, what can you conclude about this community?
Exhibit:



A. The VPN Community will perform IKE Phase 1 key-exchange encryption using the longest key Security Gateway R77 supports.
B. Changing the setting Perform key exchange encryption with from AES-256 to 3DES will enhance the VPN Community's security , and reduce encryption overhead.
C. Change the data-integrity setting for this VPN Community because MD5 is incompatible with AES.
D. Changing the setting Perform IPsec data encryption with from AES-128 to 3Des will increase the encryption overhead.

Answer: D

NEW QUESTION 159
Captive Portal is a that allows the gateway to request login information from the user.

A. Pre-configured and customizable web-based tool
B. Transparent network inspection tool
C. LDAP server add-on
D. Separately licensed feature

Answer: A

NEW QUESTION 162
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 163

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 165
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 169
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 173
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 174
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 178
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 179
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 183
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 188
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 192
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 194
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 195
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 197
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 199
Which of the following methods is NOT used by Identity Awareness to catalog identities?

A. AD Query
B. Captive Portal
C. Identity Agent
D. GPO

Answer: D

NEW QUESTION 202
Which of the following commands can be used to remove site-to-site IPsec Security Association (SA)?

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

Answer: D

NEW QUESTION 205
The User Directory Software Blade is used to integrate which of the following with Security Gateway R77?

A. RADIUS server
B. Account Management Client server
C. UserAuthority server
D. LDAP server

Answer: D

NEW QUESTION 210
Which type of R77 Security Server does not provide User Authentication?

A. SMTP Security Server
B. HTTP Security Server
C. FTP Security Server
D. HTTPS Security Server

Answer: A

NEW QUESTION 214
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 215
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 218
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 221
You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities should you do first?

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

Answer: B

NEW QUESTION 223
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 226
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 229
Complete this statement from the options provided. Using Captive Portal, unidentified users may be either; blocked, allowed to enter required credentials, or required to download the
.

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

Answer: A

NEW QUESTION 232
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 237
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

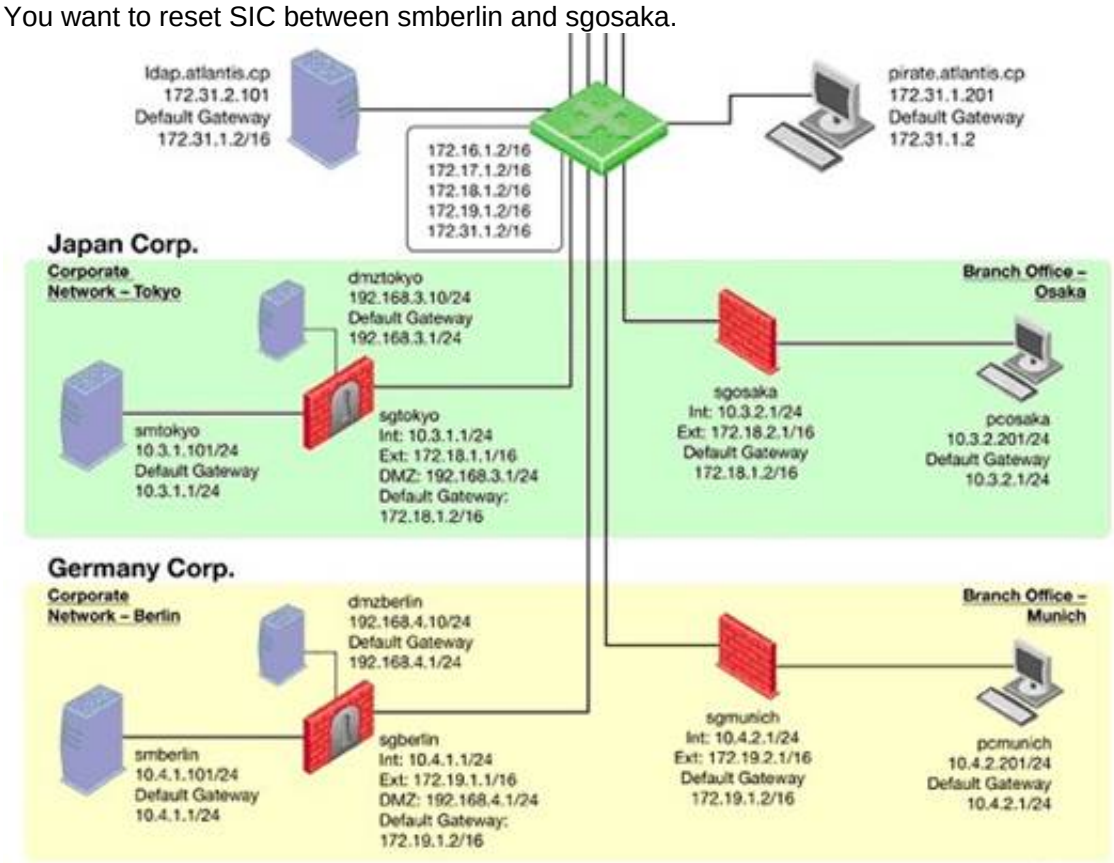
NEW QUESTION 240
Match the terms with their definitions: Exhibit:

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 244
You want to reset SIC between smberlin and sgosaka.



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

What is the reason for this behavior?

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

Answer: C

NEW QUESTION 248
Your shipping company uses a custom application to update the shipping distribution database. The custom application includes a service used only to notify remote sites that the distribution database is malfunctioning. The perimeter Security Gateway's Rule Base includes a rule to accept this traffic. Since you are responsible for multiple sites, you want notification by a text message to your cellular phone, whenever traffic is accepted on this rule. Which of the following would work BEST for your purpose?

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

Answer: B

NEW QUESTION 253

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 254
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 259
Match the following commands to their correct function. Each command has one function only listed.
Exhibit:

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

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

Answer: A

NEW QUESTION 263
An Administrator without access to SmartDashboard installed a new IPSO-based R77 Security Gateway over the weekend. He e-mailed you the SIC activation key. You want to confirm communication between the Security Gateway and the Management Server by installing the Policy. What might prevent you from installing the Policy?

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

Answer: C

NEW QUESTION 265
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 269
What command with appropriate switches would you use to test Identity Awareness connectivity?

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

Answer: B

NEW QUESTION 271
Which of the following options is available with the GAiA cpconfig utility on a Management Server?

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

Answer: C

NEW QUESTION 275
Which command displays the installed Security Gateway version?

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

Answer: A

NEW QUESTION 280
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 285
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 288
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 291
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 293
Where are SmartEvent licenses installed?

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

Answer: A

NEW QUESTION 295
When you hide a rule in a Rule Base, how can you then disable the rule?

A. Hidden rules are already effectively disabled from Security Gateway enforcement.
B. Right-click on the hidden rule place-holder bar and select Disable Rule(s).
C. Right-click on the hidden rule place-holder bar and uncheck Hide, then right-click and select Disable Rule(s); re-hide the rule.
D. Use the search utility in SmartDashboard to view all hidden rule
E. Select the relevant rule and click Disable Rule(s).

Answer: C

NEW QUESTION 298
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 301
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 302
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 307
Which statement is TRUE about implicit rules?

A. You create them in SmartDashboard.
B. The Gateway enforces implicit rules that enable outgoing packets only.
C. Changes to the Security Gateway's default settings do not affect implicit rules.
D. They are derived from Global Properties and explicit object properties.

Answer: D

NEW QUESTION 309
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 310
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 313
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.

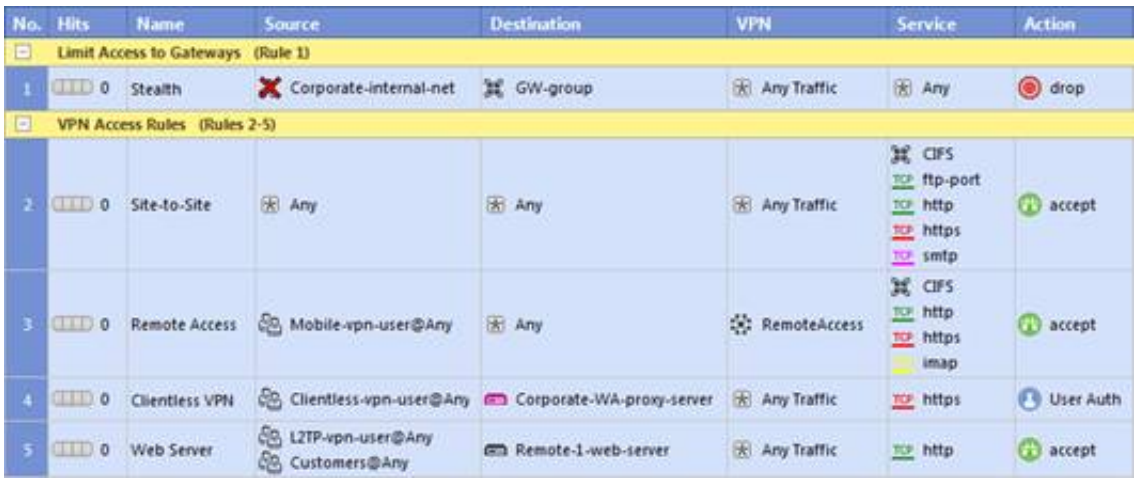
Answer: B

NEW QUESTION 317
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 318
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 321
To check the Rule Base, some rules can be hidden so they do not distract the administrator from the unhidden rules. Assume that only rules accepting HTTP or SSH will be shown. How do you accomplish this?

A. Ask your reseller to get a ticket for Check Point SmartUse and deliver him the Security Management Server cpinfo file.
B. In SmartDashboard, right-click in the column field Service > Query Colum
C. Then, put the services HTTP and SSH in the lis
D. Do the same in the field Action and select Accept here.
E. In SmartDashboard menu, select Search > Rule Base Querie
F. In the window that opens, create a new Query, give it a name (e.
G. “HTTP_SSH”?) and define a clause regarding the two services HTTP and SS
H. When having applied this, define a second clause for the action Accept and combine them with the Boolean operator AND.
I. This cannot be configured since two selections (Service, Action) are not possible.

Answer: C

NEW QUESTION 325
Which command gives an overview of your installed licenses?

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

Answer: D

NEW QUESTION 330
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 333
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 336
To qualify as an Identity Awareness enabled rule, which column MAY include an Access Role?

A. Action

B. Source
C. User
D. Track

Answer: B

NEW QUESTION 341
The Security Gateway is installed on GAiA R77 The default port for the Web User Interface is .

A. TCP 18211
B. TCP 443
C. TCP 4433
D. TCP 257

Answer: B

NEW QUESTION 345
You have included the Cleanup Rule in your Rule Base. Where in the Rule Base should the Accept ICMP Requests implied rule have no effect?

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

Answer: A

NEW QUESTION 348
Which of the following is a CLI command for Security Gateway R77?

A. fw tab -u
B. fw shutdown
C. fw merge
D. fwm policy_print <policyname>

Answer: A

NEW QUESTION 351
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 356
Before upgrading SecurePlatform to GAiA, you should create a backup. To save time, many administrators use the command backup. This creates a backup of the Check Point configuration as well as the system configuration.
An administrator has installed the latest HFA on the system for fixing traffic problem after creating a backup file. There is a mistake in the very complex static routing configuration. The Check Point configuration has not been changed.
Can the administrator use a restore to fix the errors in static routing?

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

Answer: C

NEW QUESTION 361
In a distributed management environment, the administrator has removed the default check from Accept Control Connections under the Policy > Global Properties > FireWall tab. In order for the Security Management Server to install a policy to the Firewall, an explicit rule must be created to allow the server to communicate to the Security Gateway on port _____

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

Answer: C

NEW QUESTION 366
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 370
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 372
You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the authentication credentials. What must happen after authentication that allows the client to connect to the Security Gateway's VPN domain?

A. SNX modifies the routing table to forward VPN traffic to the Security Gateway.
B. An office mode address must be obtained by the client.
C. The SNX client application must be installed on the client.
D. Active-X must be allowed on the client.

Answer: A

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

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

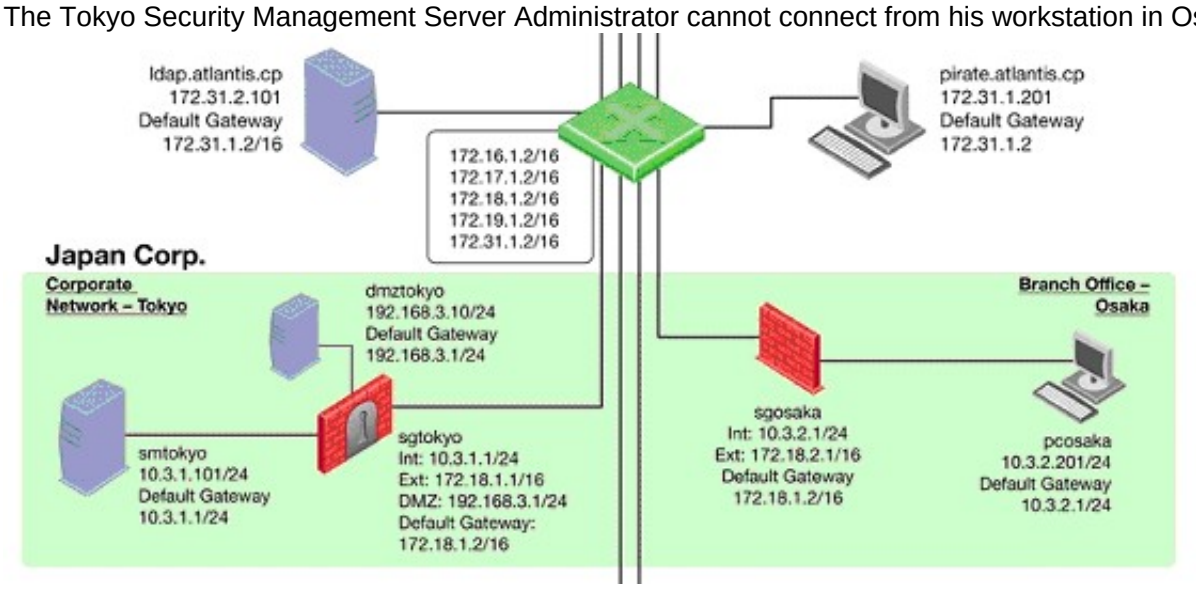
Answer: B

NEW QUESTION 377
Which rule position in the Rule Base should hold the Cleanup Rule? Why?

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

Answer: C

NEW QUESTION 379
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 381
Can you use Captive Portal with HTTPS?

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

Answer: C

NEW QUESTION 386
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 391
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 392
Where do you verify that UserDirectory is enabled?

A. Verify that Security Gateway > General Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked
B. Verify that Global Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked
C. Verify that Security Gateway > General Properties > UserDirectory (LDAP) > UseUserDirectory (LDAP) for Security Gateways is checked
D. Verify that Global Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked

Answer: D

NEW QUESTION 395
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 396
In a distributed management environment, the administrator has removed all default check boxes from the Policy > Global Properties > Firewall tab. In order for the Security Gateway to send logs to the Security Management Server, an explicit rule must be created to allow the Security Gateway to communicate to the Security Management Server on port .

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

Answer: D

NEW QUESTION 401

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 402
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 405
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 409
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 411
Which of the following items should be configured for the Security Management Server to authenticate via LDAP?

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

Answer: B

NEW QUESTION 412
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 415
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 420
Your primary Security Gateway runs on GAiA. What is the easiest way to back up your Security Gateway R77 configuration, including routing and network configuration files?

A. Copying the directories $FWDIR/conf and $FWDIR/lib to another location.
B. Using the native GAiA backup utility from command line or in the Web based user interface.
C. Using the command upgrade_export.
D. Run the pre_upgrade_verifier and save the .tgz file to the directory /temp.

Answer: B

NEW QUESTION 421
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 425
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 430
In which Rule Base can you implement an Access Role?

A. DLP
B. Mobile Access
C. IPS
D. Firewall

Answer: D

NEW QUESTION 431
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 436
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 440
Packages and licenses are loaded into the SmartUpdate repositories from which sources?

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

C. User Center, manually, SCP server
D. command cplic, manually, from a file

Answer: A

NEW QUESTION 444
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 448
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 453
What is also referred to as Dynamic NAT?

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

Answer: D

NEW QUESTION 458
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 460
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 464
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 469
Sally has a Hot Fix Accumulator (HFA) she wants to install on her Security Gateway which operates with GAiA, but she cannot SCP the HFA to the system. She can SSH into the Security Gateway, but she has never been able to SCP files to it. What would be the most likely reason she cannot do so?

A. She needs to edit /etc/SSHd/SSHd_config and add the Standard Mode account.
B. She needs to run sysconfig and restart the SSH process.
C. She needs to edit /etc/scpusers and add the Standard Mode account.
D. She needs to run cpconfig to enable the ability to SCP files.

Answer: C

NEW QUESTION 471
Complete this statement. The block Intruder option in the Active log is available _____.

A. in the SmartView Monitor client
B. in the SmartView Tracker client
C. since R75.40 release
D. only if you have the IPS blade enabled at least in one gateway

Answer: B

NEW QUESTION 472
Which tool CANNOT be launched from SmartUpdate R77?

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

Answer: B

NEW QUESTION 473
You are trying to save a custom log query in R77 SmartView Tracker, but getting the following error:
Could not save <query-name> (Error: Database is Read Only) Which of the following is a likely explanation for this?

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

Answer: C

NEW QUESTION 478
In SmartDashboard, you configure 45 MB as the required free hard-disk space to accommodate logs. What can you do to keep old log files, when free space falls below 45 MB?

A. Do nothin
B. Old logs are deleted, until free space is restored.
C. Use the command fwm logexport to export the old log files to another location.
D. Configure a script to run fw logswitch and SCP the output file to a separate file server.
E. Do nothin
F. The Security Management Server automatically copies old logs to a backup server before purging.

Answer: C

NEW QUESTION 482
Assume you are a Security Administrator for ABCTech. You have allowed authenticated access to users from Mkting_net to Finance_net. But in the user's properties, connections are only permitted within Mkting_net. What is the BEST way to resolve this conflict?

A. Select Ignore Database in the Action Properties window.
B. Permit access to Finance_net.
C. Select Intersect with user database in the Action Properties window.
D. Select Intersect with user database or Ignore Database in the Action Properties window.

Answer: D

NEW QUESTION 486
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.

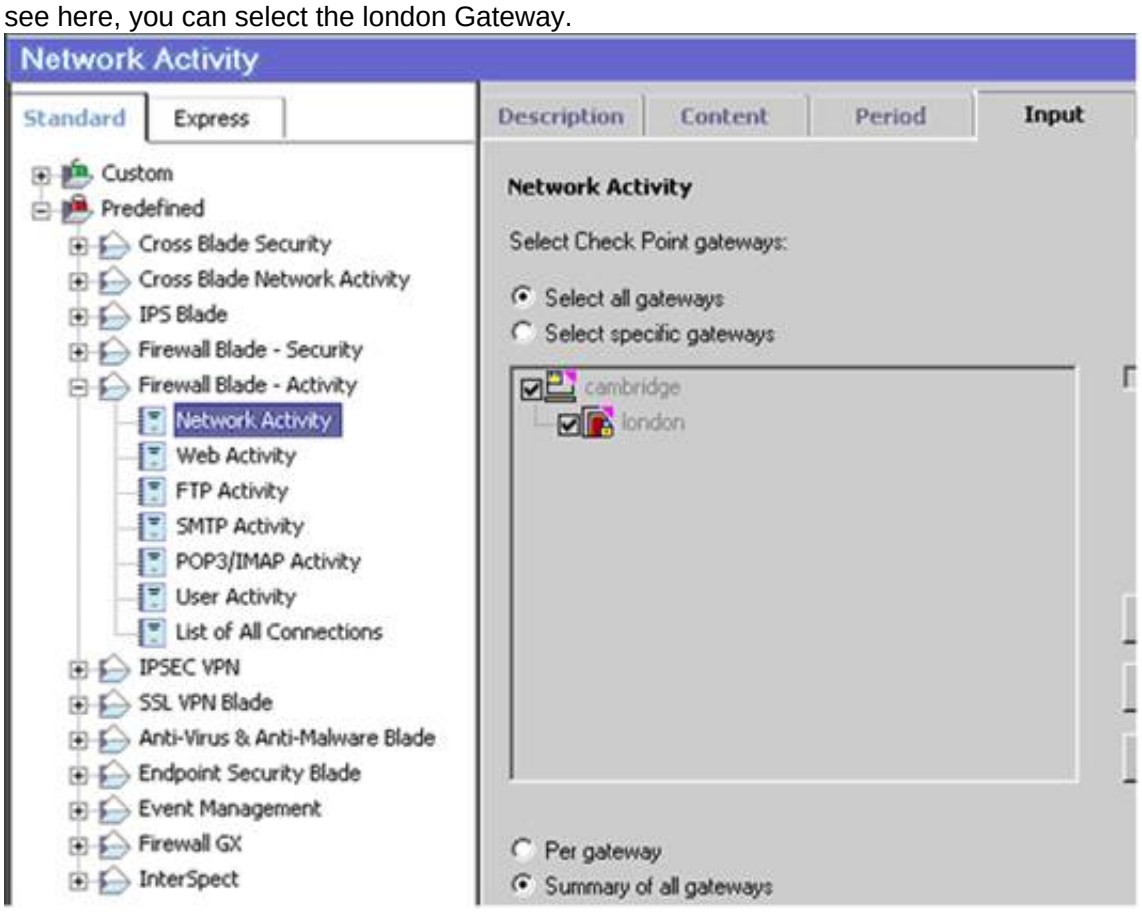
Answer: C

NEW QUESTION 488
What information is found in the SmartView Tracker Management log?

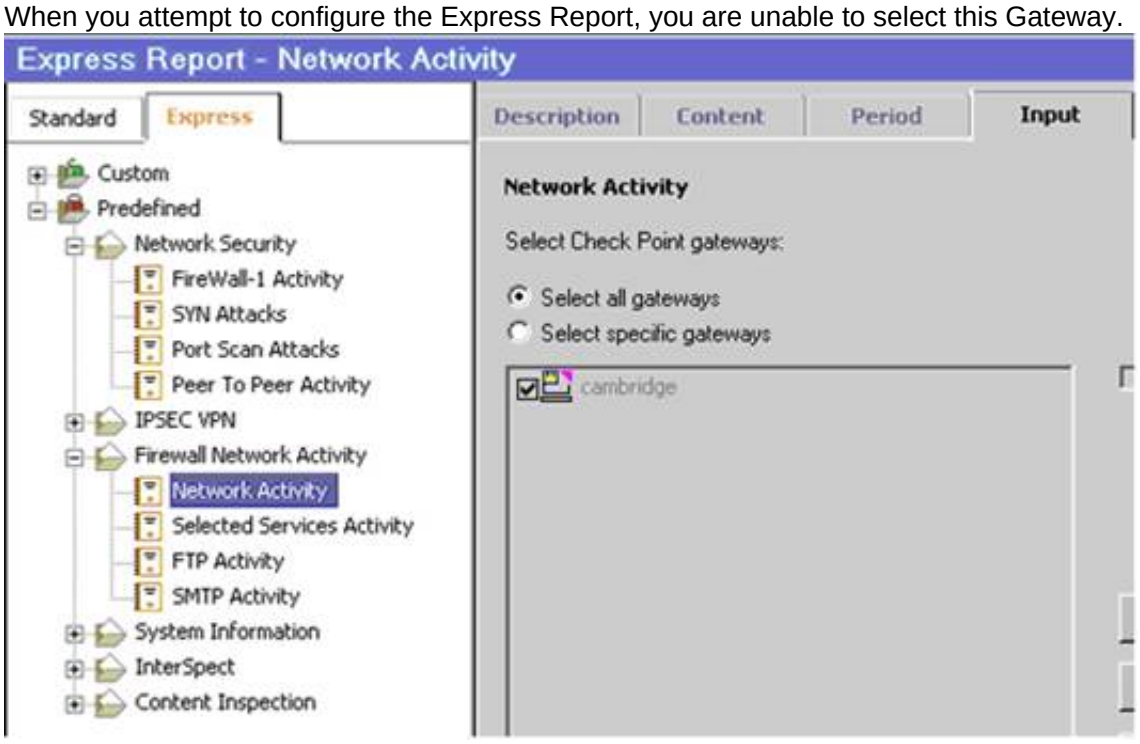
A. SIC revoke certificate event
B. Destination IP address
C. Most accessed Rule Base rule
D. Number of concurrent IKE negotiations

Answer: A

NEW QUESTION 490
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 491
Which R77 SmartConsole tool would you use to verify the installed Security Policy name on a Security Gateway?

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

Answer: A

NEW QUESTION 493
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 495
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 498
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 501
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 506
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 508
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 512
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 517
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 522
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 524
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 529
For remote user authentication, which authentication scheme is NOT supported?

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

Answer: C

NEW QUESTION 532
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 156-215.77 Exam with Our Prep Materials Via below:

https://www.certleader.com/156-215.77-dumps.html