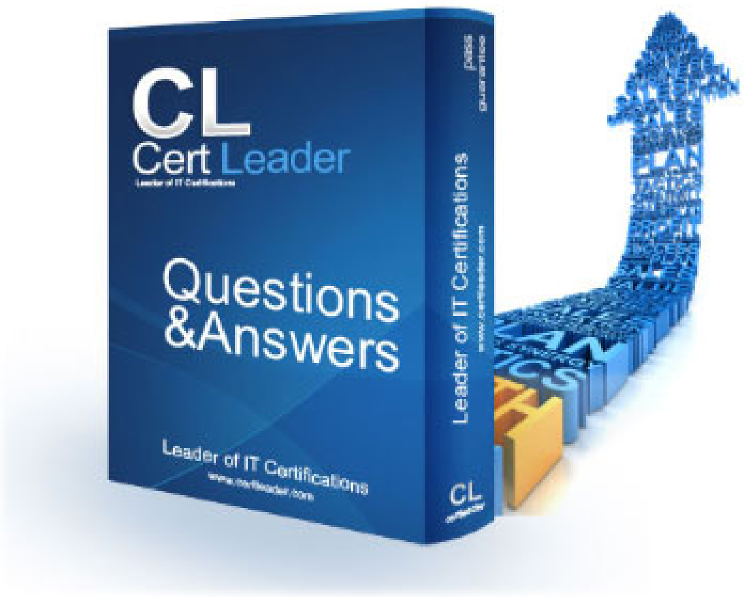
156-915.80 Dumps

Check Point Certified Security Expert Update - R80

https://www.certleader.com/156-915.80-dumps.html



NEW QUESTION 1
When synchronizing clusters, which of the following statements is FALSE?

A. The state of connections using resources is maintained in a Security Server, so their connections cannot be synchronized.
B. Only cluster members running on the same OS platform can be synchronized.
C. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.
D. Client Authentication or Session Authentication connections through a cluster member will be lost if the cluster member fails.

Answer: D

NEW QUESTION 2
Tom has been tasked to install Check Point R80 in a distributed deployment. Before Tom installs the systems this way, how many machines will be need if he does NOT include a SmartConsole machine in his calculations?

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

Answer: C

NEW QUESTION 3
Which components allow you to reset a VPN tunnel?

A. vpn tu command or SmartView monitor
B. delete vpn ike sa or vpn she11 command
C. vpn tunnelutil or delete vpn ike sa command
D. SmartView monitor only

Answer: D

NEW QUESTION 4
Check Point APIs allow system engineers and developers to make changes to their organization’s security policy with CLI tools and Web Services for all of the following except?

A. Create new dashboards to manage 3rd party task
B. Create products that use and enhance 3rd party solutions.
C. Execute automated scripts to perform common tasks.
D. Create products that use and enhance the Check Point Solution.

Answer: A

Explanation: Check Point APIs let system administrators and developers make changes to the security policy with CLI tools and web-services. You can use an API to:
Use an automated script to perform common tasks Integrate Check Point products with 3rd party solutions
Create products that use and enhance the Check Point solution References:

NEW QUESTION 5
As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

A. that is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager
B. Full Layer4 VPN –SSL VPN that gives users network access to all mobile applications
C. Full layer3 VPN –IPSec VPN that gives users network access to all mobile applications
D. You can make sure that documents are sent to the intended recipients only

Answer: C

NEW QUESTION 6
The Correlation Unit performs all but which of the following actions:

A. Marks logs that individually are not events, but may be part of a larger pattern to be identified later
B. Generates an event based on the Event policy
C. Assigns a severity level to the event
D. Takes a new log entry that is part of a group of items that together make up an event, and adds it to an ongoing event

Answer: C

NEW QUESTION 7
You are investigating issues with two gateway cluster members that are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?

A. TCP port 443
B. TCP port 257

C. TCP port 256
D. UDP port 8116

Answer: C

Explanation: Synchronization works in two modes:
Full sync is used for initial transfers of state information, for many thousands of connections. If a cluster member is brought up after being down, it will perform full sync. After all members are synchronized, only updates are transferred via delta sync. Delta sync is quicker than full sync.
References:

NEW QUESTION 8
Which is the correct order of a log flow processed by SmartEvents components:

A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
B. Firewall > SmartEvent Server Database > Correlation unit > Log Server > SmartEvent Client
C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D

NEW QUESTION 9
The “MAC magic” value must be modified under the following condition:

A. There is more than one cluster connected to the same VLAN
B. A firewall cluster is configured to use Multicast for CCP traffic
C. There are more than two members in a firewall cluster
D. A firewall cluster is configured to use Broadcast for CCP traffic

Answer: D

NEW QUESTION 10
Where do you create and modify the Mobile Access policy in R80?

A. SmartConsole
B. SmartMonitor
C. SmartEndpoint
D. SmartDashboard

Answer: A

NEW QUESTION 10
Which command shows the current connections distributed by CoreXL FW instances?

A. fw ctl multik stat
B. fw ctl affinity –l
C. fw ctl instances –v
D. fw ctl iflist

Answer: A

Explanation: The fw ctl multik stat and fw6ctl multik stat (multi-kernel statistics) commands show information for eac kernel instance. The state and processing core number of each instance is displayed, along with:

NEW QUESTION 11
GAiA Software update packages can be imported and installed offline in situation where:

A. Security Gateway with GAiA does NOT have SFTP access to Internet
B. Security Gateway with GAiA does NOT have access to Internet.
C. Security Gateway with GAiA does NOT have SSH access to internet.
D. The desired CPUSE package is ONLY available in the Check Point CLOUD.

Answer: B

NEW QUESTION 16
Which packet info is ignored with Session Rate Acceleration?

A. source port ranges
B. source ip
C. source port
D. same info from Packet Acceleration is used

Answer: C

NEW QUESTION 21
What can you do to see the current number of kernel instances in a system with CoreXL enabled?

A. Browse to Secure Platform Web GUI
B. Only Check Point support personnel can access that information
C. Execute SmarDashboard client
D. Execute command cpconfig

Answer: D

NEW QUESTION 26
Check Point recommends configuring Disk Space Management parameters to delete old log entities when available disk space is less than or equal to?

A. 50%
B. 75%
C. 80%
D. 15%

Answer: D

NEW QUESTION 29
What scenario indicates that SecureXL is enabled?

A. Dynamic objects are available in the Object Explorer
B. SecureXL can be disabled in cpconfig
C. fwaccel commands can be used in clish
D. Only one packet in a stream is seen in a fw monitor packet capture

Answer: C

NEW QUESTION 31
Why would you not see a CoreXL configuration option in cpconfig?

A. The gateway only has one processor
B. CoreXL is not licenses
C. CoreXL is disabled via policy
D. CoreXL is not enabled in the gateway object

Answer: A

NEW QUESTION 34
Which of the following is NOT a valid way to view interface's IP address settings in Gaia?

A. Using the command sthtool in Expert Mode
B. Viewing the file / config/ active
C. Via the Gaia WebUI
D. Via the command show configuration in CLISH

Answer: A

NEW QUESTION 36
The Event List within the Events tab contains:

A. a list of options available for running a query.
B. the top events, destinations, sources, and users of the query results, either as a chart or in a tallied list.
C. events generated by a query.
D. the details of a selected event.

Answer: C

Explanation: These are the components of the Events tab:
Item Description 1
Query Tree - Double-click a query to run the query. The results show in the event List. 2
Event Statistics pane - Shows the top events, destinations, sources and users of the query results, either as a chart or in a tallied list.3
Event List - Shows events generated by a query. 4
Event Preview Pane - Shows the details of the selected event References:

NEW QUESTION 40
When simulating a problem on CLusterXL cluster with cphaprob –d STOP –s problem –t 0 register, to initiate a failover on an active cluster member, what command allows you remove the problematic state?

A. cphaprob –d STOP unregister
B. cphaprob STOP unregister
C. cphaprob unregister STOP
D. cphaprob –d unregister STOP

Answer: A

Explanation: esting a failover in a controlled manner using following command;
# cphaprob -d STOP -s problem -t 0 register
This will register a problem state on the cluster member this was entered on;If you then run;
# cphaprob list
this will show an entry named STOP.
to remove this problematic register run following;
# cphaprob -d STOP unregister References:

NEW QUESTION 45
You have existing dbedit scripts from R77. Can you use them with R80.10?

A. dbedit is not supported in R80.10
B. dbedit is fully supported in R80.10
C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers
D. dbedit scripts are being replaced by mgmt._cli in R80.10

Answer: D

Explanation: dbedit (or GuiDbEdit) uses the cpmi protocol which is gradually being replaced by the new R80.10 automation architecture. cpmi clients are still supported in R80.10, but there are some functionalities that cannot be managed by cpmi anymore. For example, the Access and Threat policies do not have a cpmi representation. They can be managed only by the new mgmt_cli and not by cpmi clients. There are still many tables that have an inner cpmi representation (for example, network objects, services, servers, and global properties) and can still be managed using cpmi.

NEW QUESTION 48
You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

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

Answer: B

NEW QUESTION 49
What is the port used for SmartConsole to connect to the Security Management Server:

A. CPMI port 18191/TCP
B. CPM port / TCP port 19009
C. SIC port 18191/TCP
D. https port 4434/TCP

Answer: A

NEW QUESTION 51
What are the minimum open server hardware requirements for a Security Management Server/Standalone in R80.10?

A. 2 CPU cores, 4GB of RAM and 15GB of disk space
B. 8 CPU cores, 16GB of RAM and 500 GB of disk space
C. 4 CPU cores, 8GB of RAM and 500GB of disk space
D. 8 CPU cores, 32GB of RAM and 1 TB of disk space

Answer: C

NEW QUESTION 56
In R80.10, how do you manage your Mobile Access Policy?

A. Through the Unified Policy
B. Through the Mobile Console
C. From SmartDashboard
D. From the Dedicated Mobility Tab

Answer: C

NEW QUESTION 60
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

A. Smart Cloud Services
B. Load Sharing Mode Services
C. Threat Agent Solution
D. Public Cloud Services

Answer: C

NEW QUESTION 62
What is the most ideal Synchronization Status for Security Management Server High Availability deployment?

A. Lagging
B. Synchronized
C. Never been synchronized
D. Collision

Answer: B

Explanation: The possible synchronization statuses are:
For instance, on account of the fact that the Active SMS has undergone changes since the previous synchronization (objects have been edited, or the Security Policy has been newly installed), the information on the Standby SMS is lagging.
For instance, in the above figure, if a system administrators logs into Security Management server B before it has been synchronized with the Security Management server A, the status of the Security Management server A is Advanced, since it contains more up-to-date information which the former does not have.
In this case, manual synchronization must be initiated by the system administrator by changing the Active
SMS to a Standby SMS. Perform a synch me operation from the more advanced server to the Standby SMS. Change the Standby SMS to the Active SMS.

NEW QUESTION 65
What happen when IPS profile is set in Detect-Only Mode for troubleshooting?

A. It will generate Geo-Protection traffic
B. Automatically uploads debugging logs to Check Point Support Center
C. It will not block malicious traffic
D. Bypass licenses requirement for Geo-Protection control

Answer: C

Explanation: It is recommended to enable Detect-Only for Troubleshooting on the profile during the initial installation of IPS. This option overrides any protections that are set to Prevent so that they will not block any traffic. During this time you can analyze the alerts that IPS generates to see how IPS will handle network traffic, while avoiding any impact on the flow of traffic.

NEW QUESTION 67
Which of these options is an implicit MEP option?

A. Primary-backup
B. Source address based
C. Round robin
D. Load Sharing

Answer: A

Explanation: There are three methods to implement implicit MEP: References:

NEW QUESTION 71
Which one of the following processes below would not start if there was a licensing issue.

A. CPD
B. CPCA
C. FWM
D. CPWD

Answer: A

NEW QUESTION 73
What Shell is required in Gaia to use WinSCP?

A. UNIX
B. CPShell
C. CLISH
D. Bash

Answer: D

NEW QUESTION 74
Which one of the following is true about Threat Emulation?

A. Takes less than a second to complete
B. Works on MS Office and PDF files only
C. Always delivers a file
D. Takes minutes to complete (less than 3 minutes)

Answer: D

NEW QUESTION 79
Fill in the blank: The tool generates a R80 Security Gateway configuration report.

A. infoCP
B. infoview
C. cpinfo
D. fw cpinfo

Answer: C

NEW QUESTION 84
Which command will reset the kernel debug options to default settings?

A. fw ctl dbg –a 0
B. fw ctl dbg resetall
C. fw ctl debug 0
D. fw ctl debug set 0

Answer: C

Explanation: Reset the debugs to the default.
In case someone changed the setting in the past and since then the firewall was not rebooted we should set all back to the defaults.
# fw ctl debug 0Defaulting all kernel debugging options

NEW QUESTION 86
What is the purpose of a SmartEvent Correlation Unit?

A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server
B. The SmartEvent Correlation Unit's task it to assign severity levels to the identified events.
C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.
D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server

Answer: C

NEW QUESTION 87
Aaron is a Cyber Security Engineer working for Global Law Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R80.10. Company's Network Security Developer Team is having issue testing new API with newly deployed R80.10 Security Management Server and blames Check Point Security Management Server as root cause. The ticket has been created and issue is at Aaron's desk for an investigation. What do you recommend as the best suggestion for Aaron to make sure API testing works as expected?

A. Aaron should check API Server status from expert CLI by "fwm api status" and if it's stopped he should start using command "fwm api start" on Security Management Server.
B. Aaron should check API Server5 status from expert CLI by "cpapi status" and if it's stopped he should start using command "cpapi start" on Security Management Server.
C. Aaron should check API Server status from expert CLI by "api status" and if it's stopped he should start using command "api start" on Security Management Server.
D. Aaron should check API Server status from expert CLI by "cpm api status" and if it's stopped he should start using command "cpm api start" on Security Management Server.

Answer: C

NEW QUESTION 91
The SmartEvent R80 Web application for real-time event monitoring is called:

A. SmartView Monitor
B. SmartEventWeb
C. There is no Web application for SmartEvent
D. SmartView

Answer: A

NEW QUESTION 95
Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

A. Symmetric routing
B. Failovers
C. Asymmetric routing
D. Anti-Spoofing

Answer: C

NEW QUESTION 100

What are types of Check Point APIs available currently as part of R80.10 code?

A. Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API
B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
C. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API
D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Answer: B

NEW QUESTION 104
The Security Gateway is installed on GAiA R80. The default port for the Web User Interface is .

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

Answer: D

NEW QUESTION 106
SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

A. This statement is true because SecureXL does improve all traffic
B. This statement is false because SecureXL does not improve this traffic but CoreXL does
C. This statement is true because SecureXL does improve this traffic
D. This statement is false because encrypted traffic cannot be inspected

Answer: C

Explanation: SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.

NEW QUESTION 107
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

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

Answer: D

NEW QUESTION 109
You find one of your cluster gateways showing “Down” when you run the “cphaprob stat” command. You then run the “clusterXL_admin up” on the down member but unfortunately the member continues to show down. What command do you run to determine the case?

A. cphaprob –f register
B. cphaprob –d–s report
C. cpstat–f-all
D. cphaprob –a list

Answer: D

NEW QUESTION 111
John detected high load on sync interface. Which is most recommended solution?

A. For short connections like http service – delay sync for 2 seconds
B. Add a second interface to handle sync traffic
C. For short connections like http service – do not sync
D. For short connections like icmp service – delay sync for 2 seconds

Answer: A

NEW QUESTION 115
Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

A. The rule base can be built of layers, each containing a set of the security rule
B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
D. Time object to a rule to make the rule active only during specified times.
E. Sub Policies are sets of rules that can be created and attached to specific rule
F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule

Answer: A

NEW QUESTION 117
Fill in the blank: The command provides the most complete restoration of a R80 configuration.

A. upgrade_import
B. cpconfig
C. fwn dbimport –p <export file>
D. cpinfo –recover

Answer: A

NEW QUESTION 121
Which statement is true regarding redundancy?

A. System Administrator know when their cluster has failed over and can also see why it failed over by using the cphaprob f it command.
B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
C. Machines in a Cluster XL High Availability configuration must be synchronized.
D. Both Cluster XL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.

Answer: D

NEW QUESTION 126
What is the command to show SecureXL status?

A. fwaccel status
B. fwaccel stats –m
C. fwaccel –s
D. fwaccel stat

Answer: D

Explanation: To check overall SecureXL status: [Expert@HostName]# fwaccel stat

NEW QUESTION 129
What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?

A. Anti-Bot is the only countermeasure against unknown malware
B. Anti-Bot is the only protection mechanism which starts a counter-attack against known Command & Control Centers
C. Anti-Bot is the only signature-based method of malware protection
D. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command & Control Center

Answer: D

NEW QUESTION 130
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via
e-m ail. An e-mail with Security_ report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links. Which component of SandBlast protection is her company using on a Gateway?

A. SandBlast Threat Emulation
B. SandBlast Agent
C. Check Point Protect
D. SandBlast Threat Extraction

Answer: D

NEW QUESTION 135
Which web services protocol is used to communicate to the Check Point R80 identity Awareness Web APi?

A. SOAP
B. REST
C. XLANG
D. XML-RPC

Answer: B

Explanation: The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.

NEW QUESTION 138
For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

A. 20 minutes
B. 15 minutes
C. Admin account cannot be unlocked automatically
D. 30 minutes at least

Answer: D

NEW QUESTION 143
What is the valid range for VRID value in VRRP configuration?

A. 1 – 254
B. 1 – 255
C. 0 – 254
D. 0 – 255

Answer: B

Explanation: Virtual Router ID - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.

NEW QUESTION 145
In SPLAT the command to set the timeout was idle. In order to achieve this and increase the timeout for Gaia, what command do you use?

A. set idle <value>
B. set inactivity–timeout <value>
C. set timeout <value>
D. set inactivity <value>

Answer: B

NEW QUESTION 148
What does the command vpn crl zap do?

A. Nothing, it is not a valid command
B. Erases all CRL's from the gateway cache
C. Erases VPN certificates from cache
D. Erases CRL's from the management server cache

Answer: B

NEW QUESTION 151
When defining QoS global properties, which option below is not valid?

A. Weight
B. Authenticated timeout
C. Schedule
D. Rate

Answer: C

NEW QUESTION 155
What are the three components for Check Point Capsule?

A. Capsule Docs, Capsule Cloud, Capsule Connect
B. Capsule Workspace, Capsule Cloud, Capsule Connect
C. Capsule Workspace, Capsule Docs, Capsule Connect
D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer: D

NEW QUESTION 160
Which is not a blade option when configuring SmartEvent?

A. Correlation Unit
B. SmartEvent Unit
C. SmartEvent Server
D. Log Server

Answer: B

Explanation: On the Management tab, enable these Software Blades:

NEW QUESTION 161
What is the purpose of Priority Delta in VRRP?

A. When a box is up, Effective Priority = Priority + Priority Delta
B. When an Interface is up, Effective Priority = Priority + Priority Delta
C. When an Interface fail, Effective Priority = Priority – Priority Delta
D. When a box fail, Effective Priority = Priority – Priority Delta

Answer: C

Explanation: Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP. If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will beging to send out its own HELLO packet. Once the master sees this packet with a priority greater than its own, then it releases the VIP.

NEW QUESTION 163
Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

A. Detects and blocks malware by correlating multiple detection engines before users are affected.
B. Configure rules to limit the available network bandwidth for specified users or groups.
C. Use UserCheck to help users understand that certain websites are against the company's security policy.
D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Answer: A

Explanation: Use the URL Filtering and Application Control Software Blades to:

NEW QUESTION 164
When deploying multiple clustered firewalls on the same subnet, what does the firewall administrator need to configure to prevent CCP broadcasts being sent to the wrong cluster?

A. Set the fwha_mac_magic_forward parameter in the $CPDIR/boot/modules/ha_boo
B. conf
C. Set the fwha_mac_magic parameter in the $FWDIR/boot/fwkern.conf file
D. Set the cluster global ID using the command "cphaconf cluster_id set <value>"
E. Set the cluster global ID using the command "fw ctt set cluster_id <value>"

Answer: C

NEW QUESTION 168
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

A. fw cti multik dynamic_dispatching on
B. fw cti multik dynamic_dispatching set_mode 9
C. fw cti multik set_mode 9
D. fw cti multik pq enable

Answer: C

Explanation: To fully enable the CoreXL Dynamic Dispatcher on Security Gateway: [Expert@HostName]# fw ctl multik set_mode 9
Example output:

```
[Expert@R77.30:0]# fw ctl multik set_mode 9 Please reboot the system
[Expert@R77.30:0]#
```

NEW QUESTION 170
What CLI command will reset the IPS pattern matcher statistics?

A. ips reset pmstat
B. ips pstats reset
C. ips pmstats refresh
D. ips pmstats reset

Answer: D

Explanation: ips pmstats reset
Description - Resets the data that is collected to calculate the pmstat statistics. Usage - ips pmstats reset

NEW QUESTION 172
Fill in the blank: The R80 feature permits blocking specific IP addresses for a specified time period.

A. Block Port Overflow
B. Local Interface Spoofing
C. Suspicious Activity Monitoring
D. Adaptive Threat Prevention

Answer: C

NEW QUESTION 173
Which of the following is NOT an internal/native Check Point command?

A. fwaccel on
B. fw ct1 debug
C. tcpdump
D. cphaprob

Answer: C

NEW QUESTION 176
Firewall policies must be configured to accept VRRP packets on the GAiA platform if it runs Firewall software. The Multicast destination assigned by the Internet Assigned Numbers Authority (IANA) for VRRP is:

A. 224.0.0.18
B. 224.0.0.5
C. 224.0.0.102
D. 224.0.0.22

Answer: A

Explanation: Topic 2, Exam Pool A

NEW QUESTION 177
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 R80?

A. External-user group
B. LDAP group
C. A group with a generic user
D. All Users

Answer: B

NEW QUESTION 182
Your organization’s disaster recovery plan needs an update to the backup and restore section to reap the new distributed R80 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 R80 components that enforce the Security Policies should be backed up at least once a week.
Desired Objective: Back up R80 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 183
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.
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 184
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 187
How are cached usernames and passwords cleared from the memory of a R80 Security Gateway?

A. By using the Clear User Cache button in SmartDashboard.
B. Usernames and passwords only clear from memory after they time out.
C. By retrieving LDAP user information using the command fw fetchldap.
D. By installing a Security Policy.

Answer: D

NEW QUESTION 191
Which command would provide the most comprehensive diagnostic information to Check Point Technical Support?

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

Answer: B

NEW QUESTION 196
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 201
Your R80 primary Security Management Server is installed on GAiA. You plan to schedule the Security Management Server to run fw logswitch automatically every 48 hours. How do you create this schedule?

A. On a GAiA Security Management Server, this can only be accomplished by configuring the command fw logswitch via the cron utility.
B. Create a time object, and add 48 hours as the interva
C. Open the primary Security Management Server object’s Logs and Masters window, enable Schedule log switch, and select the Time object.
D. Create a time object, and add 48 hours as the interva
E. Open the Security Gateway object's Logs and Masters window, enable Schedule log switch, and select the Time object.
F. Create a time object, and add 48 hours as the interva
G. Select that time object’s Global Properties > Logs and Masters window, to schedule a logswitch.

Answer: B

NEW QUESTION 205
Which command allows you to view the contents of an R80 table?

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

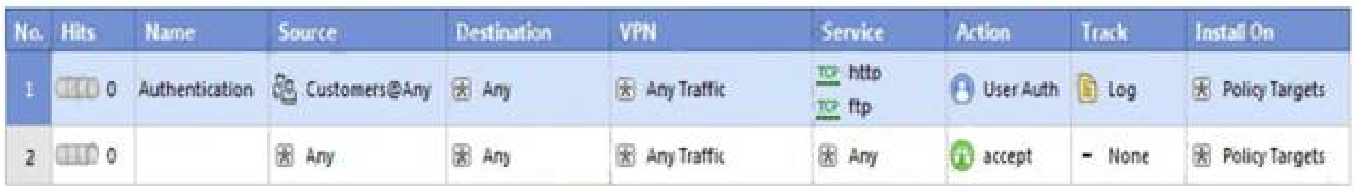
Answer: B

NEW QUESTION 206
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 R80 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 207
Review the rules.



No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	TCP http TCP ftp	User Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	accept	- None	Policy Targets

Assume domain UDP is enabled in the impled rules.
What happens when a user from the internal network tries to browse to the internet using HTTP? The user:

A. can connect to the Internet successfully after being authenticated.
B. is prompted three times before connecting to the Internet successfully.
C. can go to the Internet after Telnetting to the client authentication daemon port 259.
D. can go to the Internet, without being prompted for authentication.

Answer: D

NEW QUESTION 209
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) > Use UserDirectory (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 211
Where can you find the Check Point's SNMP MIB file?

A. $CPDIR/lib/snmp/chkpt.mib
B. $FWDIR/conf/snmp.mib
C. It is obtained only by request from the TAC.
D. There is no specific MIB file for Check Point products.

Answer: A

NEW QUESTION 214
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 219
Your main internal network 10.10.10.0/24 allows all traffic to the Internet using Hide NAT. You also have a small network 10.10.20.0/24 behind the internal router. You want to configure the kernel to translate the source address only when network 10.10.20.0 tries to access the Internet for HTTP, SMTP, and FTP services. Which of the following configurations will allow this network to access the Internet?

A. Configure three Manual Static NAT rules for network 10.10.20.0/24, one for each service.
B. Configure Automatic Static NAT on network 10.10.20.0/24.
C. Configure one Manual Hide NAT rule for HTTP, FTP, and SMTP services for network 10.10.20.0/24.
D. Configure Automatic Hide NAT on network 10.10.20.0/24 and then edit the Service column in the NAT Rule Base on the automatic rule.

Answer: C

NEW QUESTION 223
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 225
What is the officially accepted diagnostic tool for IP Appliance Support?

A. ipsoinfo
B. CST

C. uag-diag
D. cpinfo

Answer: B

NEW QUESTION 230
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 235
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 239
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 244
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 246
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 249
Your primary Security Gateway runs on GAiA. What is the easiest way to back up your Security Gateway R80 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 252
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 256
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 259
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 261
You intend to upgrade a Check Point Gateway from R71 to R80. 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 266
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 268
You enable Hide NAT on the network object, 10.1.1.0 behind the Security Gateway’s external interface. You browse to the Google Website from host, 10.1.1.10 successfully. You enable a log on the rule that allows 10.1.1.1 to exit the network. How many log entries do you see for that connection in SmartView Tracker?

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

Answer: B

NEW QUESTION 270
Which of the following are authentication methods that Security Gateway R80 uses to validate connection attempts? Select the response below that includes the MOST complete list of valid authentication methods.

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

D. User, Proxied, Session

Answer: C

NEW QUESTION 274
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

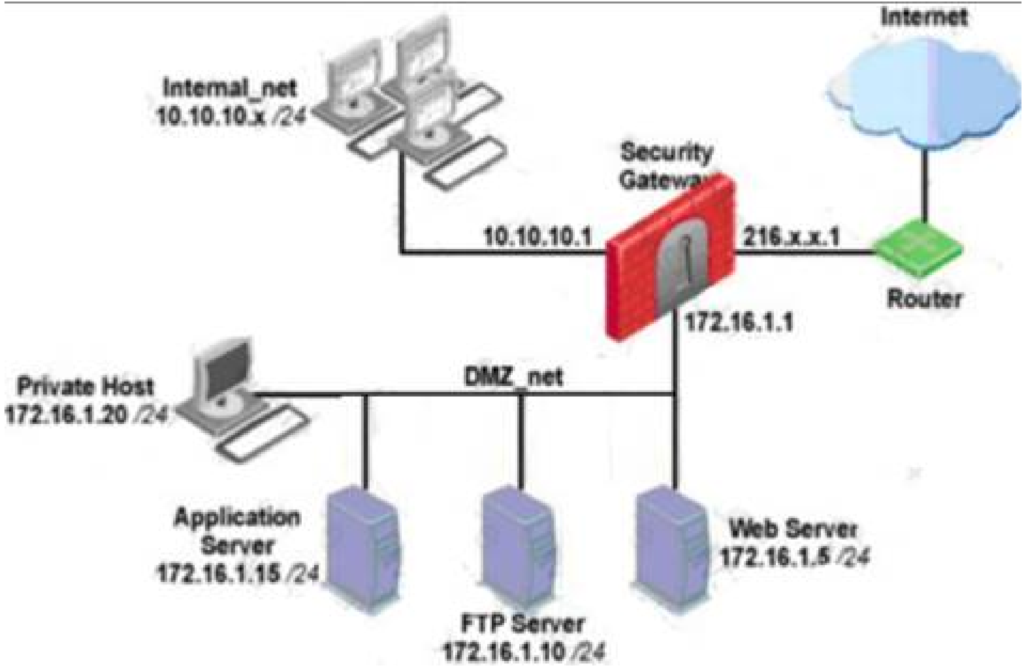
Answer: C

NEW QUESTION 277
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 282
You have three servers located in a DMZ, using private IP addresses. You want internal users from 10.10.10.x to access the DMZ servers by public IP addresses. Internal_net 10.10.10.x is configured for Hide NAT behind the Security Gateway's external interface.



What is the best configuration for 10.10.10.x users to access the DMZ servers, using the DMZ servers' public IP addresses?

A. When connecting to internal network 10.10.10.x, configure Hide NAT for the DMZ network behind the Security Gateway DMZ interface.
B. When the source is the internal network 10.10.10.x, configure manual static NAT rules to translate the DMZ servers.
C. When connecting to the Internet, configure manual Static NAT rules to translate the DMZ servers.
D. When trying to access DMZ servers, configure Hide NAT for 10.10.10.x behind the DMZ's interface.

Answer: B

NEW QUESTION 283
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 basedon the defined action.

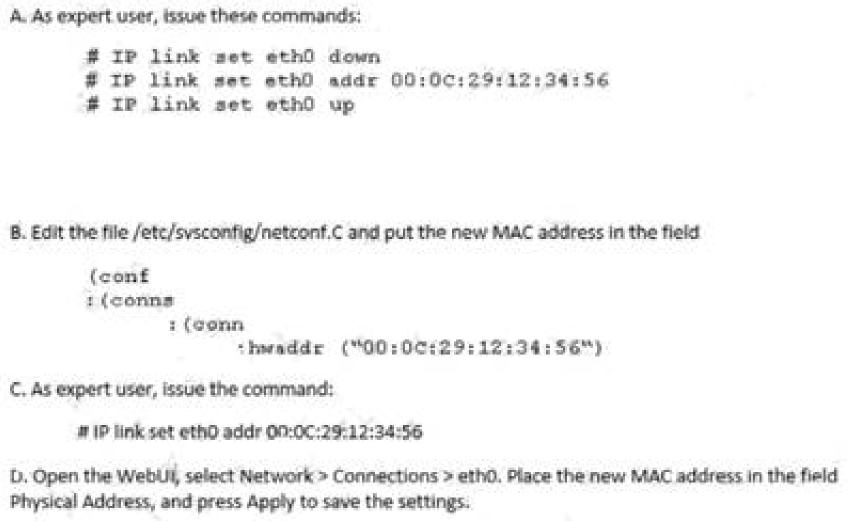
Answer: D

NEW QUESTION 284
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 286
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?



A. As expert user, issue these commands:

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

B. Edit the file /etc/svsconfig/netconf.C and put the new MAC address in the field

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

C. As expert user, issue the command:

```
# 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.

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 287
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 R80 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 290
Because of pre-existing design constraints, you set up manual NAT rules for your HTTP server. However, your FTP server and SMTP server are both using automatic NAT rules. All traffic from your FTP and SMTP servers are passing through the Security Gateway without a problem, but traffic from the Web server is dropped on rule 0 because of anti-spoofing settings. What is causing this?

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

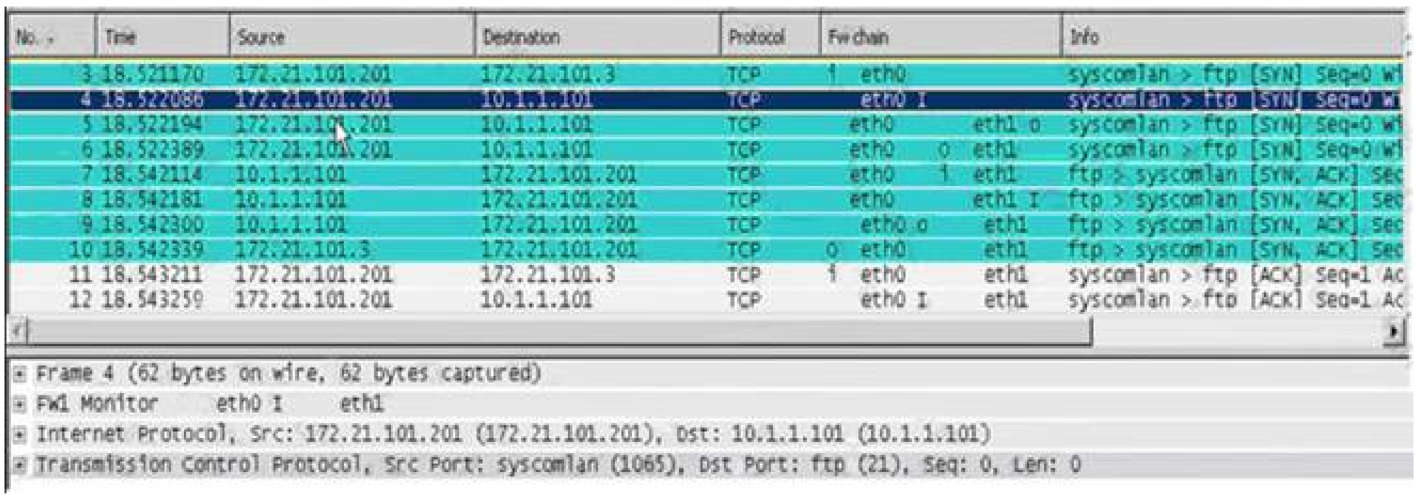
Answer: D

NEW QUESTION 291
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 292
Looking at the SYN packets in the Wireshark output, select the statement that is true about NAT.



No.	Time	Source	Destination	Protocol	Fw chain	Info
3	18.521170	172.21.101.201	172.21.101.3	TCP	i eth0	syscomlan > ftp [SYN] Seq=0 Wi
4	18.522086	172.21.101.201	10.1.1.101	TCP	eth0 I	syscomlan > ftp [SYN] Seq=0 Wi
5	18.522194	172.21.101.201	10.1.1.101	TCP	eth0 eth1 o	syscomlan > ftp [SYN] Seq=0 Wi
6	18.522389	172.21.101.201	10.1.1.101	TCP	eth0 O eth1	syscomlan > ftp [SYN] Seq=0 Wi
7	18.542114	10.1.1.101	172.21.101.201	TCP	eth0 i eth1	ftp > syscomlan [SYN, ACK] Sec
8	18.542181	10.1.1.101	172.21.101.201	TCP	eth0 eth1 I	ftp > syscomlan [SYN, ACK] Sec
9	18.542300	10.1.1.101	172.21.101.201	TCP	eth0 o eth1	ftp > syscomlan [SYN, ACK] Sec
10	18.542339	172.21.101.3	172.21.101.201	TCP	O eth0 eth1	ftp > syscomlan [SYN, ACK] Sec
11	18.543211	172.21.101.201	172.21.101.3	TCP	i eth0 eth1	syscomlan > ftp [ACK] Seq=1 Ac
12	18.543259	172.21.101.201	10.1.1.101	TCP	eth0 I eth1	syscomlan > ftp [ACK] Seq=1 Ac

```
⊞ Frame 4 (62 bytes on wire, 62 bytes captured)
⊞ FW1 Monitor      eth0 I      eth1
⊞ Internet Protocol, Src: 172.21.101.201 (172.21.101.201), Dst: 10.1.1.101 (10.1.1.101)
⊞ Transmission Control Protocol, Src Port: syscomlan (1065), Dst Port: ftp (21), Seq: 0, Len: 0
```

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 296
Your internal network is configured to be 10.1.1.0/24. This network is behind your perimeter R80 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.

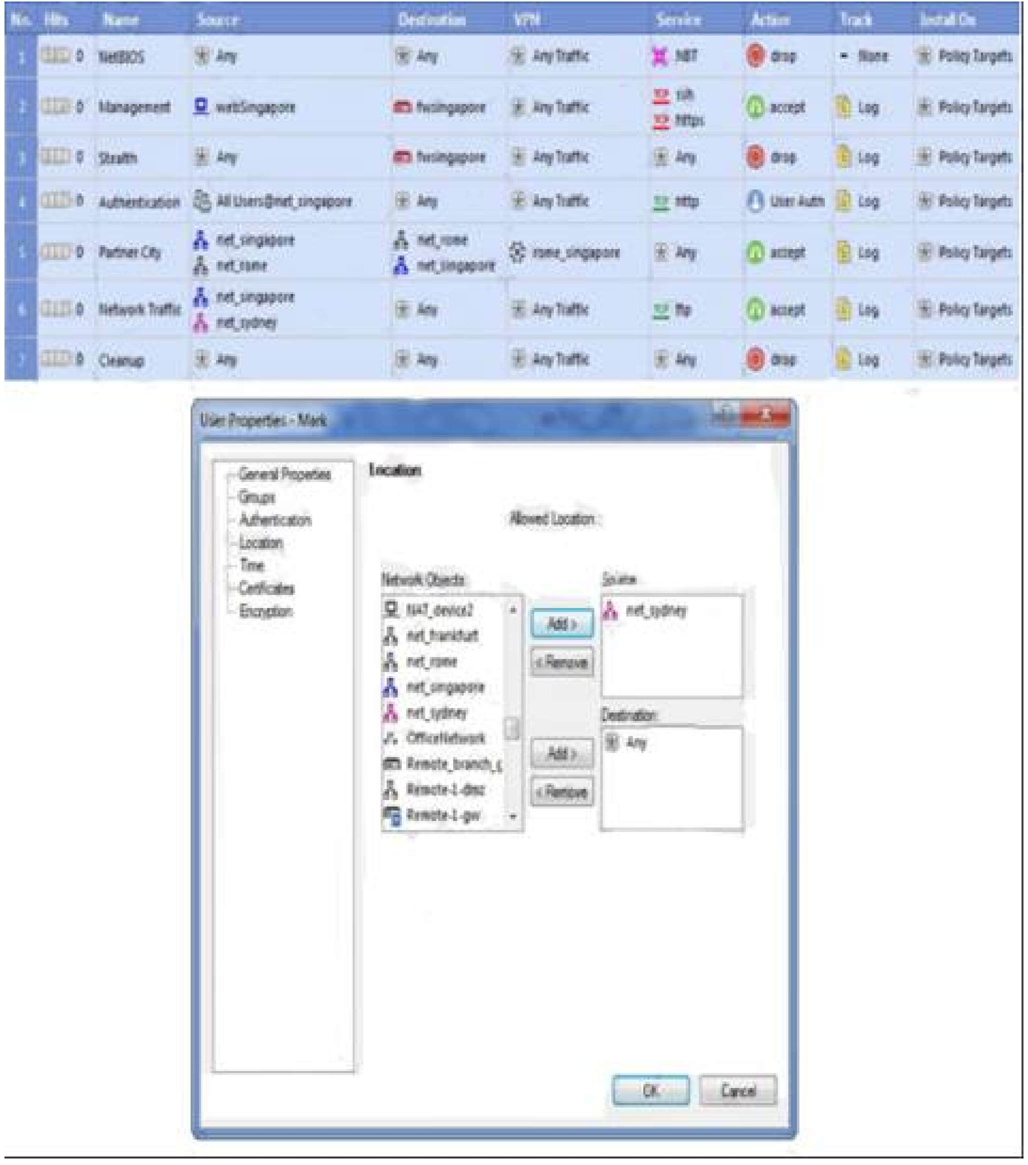
Answer: A

NEW QUESTION 300
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 302
Charles requests a Website while using a computer not in the net_singapore network.



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	Authentication	All Users@net_singapore	Any	Any Traffic	http	User Auth	Log	Policy Targets
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	Any	accept	Log	Policy Targets
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	ftp	accept	Log	Policy Targets
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets

User Properties - Mark

Location

Allowed Location:

Network Objects:
NAT_device2
net_frankfurt
net_rome
net_singapore
net_sydney
OfficeNetwork
Remote_branch_(
Remote-1-dmz
Remote-1-gw

Source:
net_sydney

Destination:
Any

What is TRUE about his location restriction?

A. Source setting in Source column always takes precedence.
B. Source setting in User Properties always takes precedence.
C. As location restrictions add up, he would be allowed from net_singapore and net_sydney.
D. It depends on how the User Auth object is configured; whether User Properties or Source Restriction takes precedence.

Answer: D

NEW QUESTION 303
What is the syntax for uninstalling a package using newpkg?

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

Answer: D

NEW QUESTION 306
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 311
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 312
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 316
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 318
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 320

Your company's Security Policy forces users to authenticate to the Gateway explicitly, before they can use any services. The Gateway does not allow the Telnet service to itself from any location. How would you configure authentication on the Gateway? With a:

A. Client Authentication rule using the manual sign-on method, using HTTP on port 900
B. Client Authentication rule, using partially automatic sign on
C. Client Authentication for fully automatic sign on
D. Session Authentication rule

Answer: A

NEW QUESTION 322
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 327
You want to implement Static Destination NAT in order to provide external, Internet users access to an internal Web Server that has a reserved (RFC 1918) IP address. You have an unused valid IP address on the network between your Security Gateway and ISP router. You control the router that sits between the firewall external interface and the Internet.
What is an alternative configuration if proxy ARP cannot be used on your Security Gateway?

A. Publish a proxy ARP entry on the ISP router instead of the firewall for the valid IP address.
B. Place a static ARP entry on the ISP router for the valid IP address to the firewall's external address.
C. Publish a proxy ARP entry on the internal Web server instead of the firewall for the valid IP address.
D. Place a static host route on the firewall for the valid IP address to the internal Web server.

Answer: B

NEW QUESTION 330
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 andsnapshot will not.

Answer: A

NEW QUESTION 331
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 333
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 334
What type of traffic can be re-directed to the Captive Portal?

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

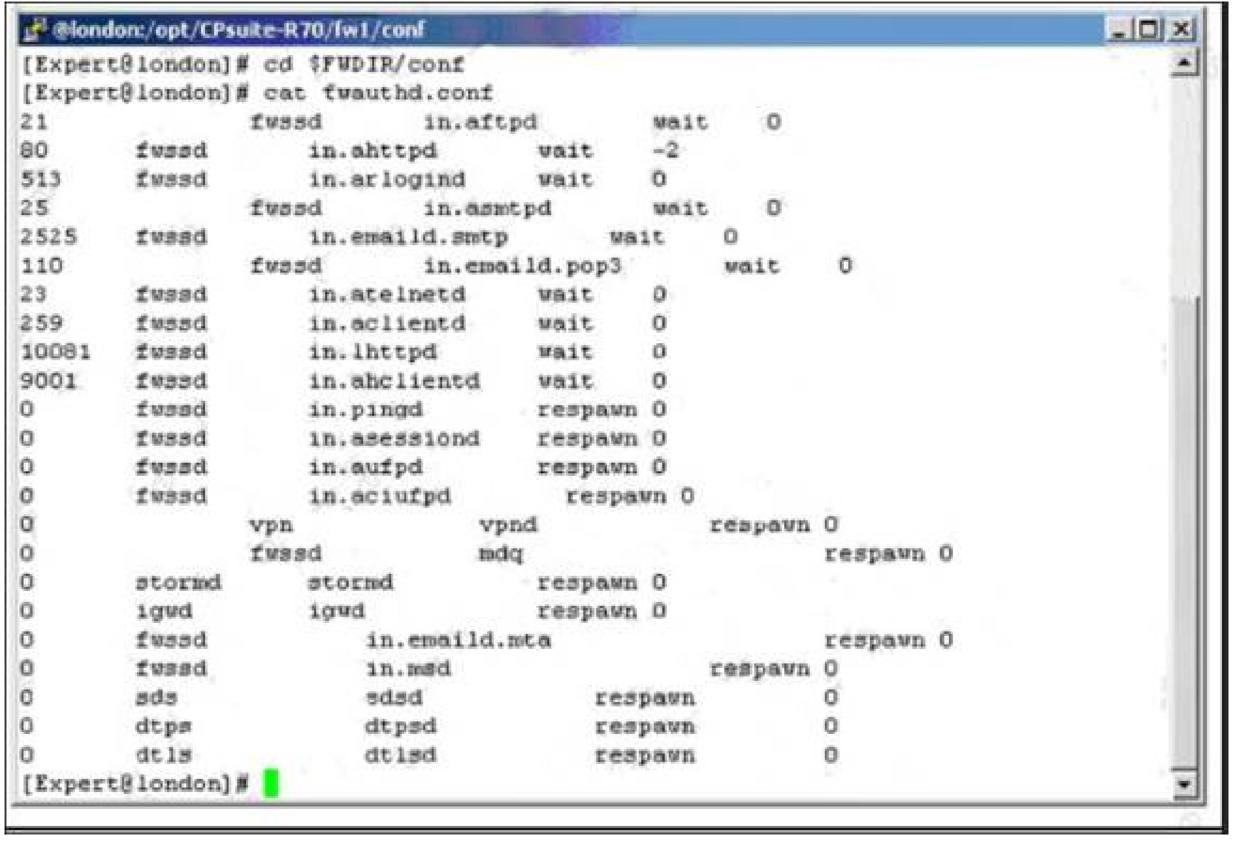
Answer: B

NEW QUESTION 338
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.

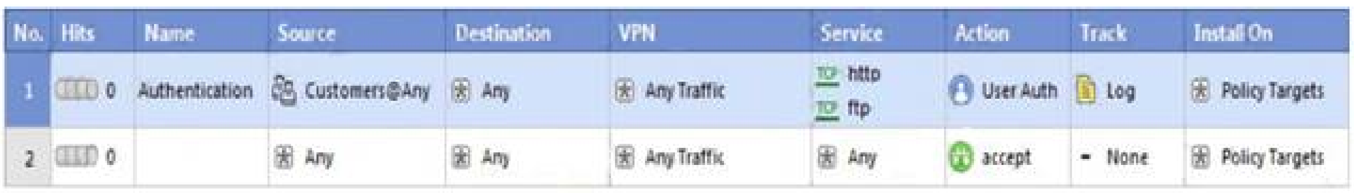
Answer: D

NEW QUESTION 343
Your customer, Mr. Smith needs access to other networks and should be able to use all services. Session authentication is not suitable. You select Client Authentication with HTTP. The standard authentication port for client HTTP authentication (Port 900) is already in use. You want to use Port 9001 but are having connectivity problems. Why are you having problems?



@london:/opt/CPsuite-R70/fw1/conf

```
[Expert@london]# cd $FWDIR/conf
[Expert@london]# cat fwauthd.conf
21              fwssd       in.aftpd        wait    0
80      fwssd       in.ahttpd       wait    -2
513     fwssd       in.arlogind     wait    0
25              fwssd       in.asmtpd       wait    0
2525    fwssd       in.emaild.smtp       wait    0
110             fwssd       in.emaild.pop3       wait    0
23      fwssd       in.atelnetd     wait    0
259     fwssd       in.aclientd     wait    0
10081   fwssd       in.lhttpd       wait    0
9001    fwssd       in.ahclientd    wait    0
0       fwssd       in.pingd        respawn 0
0       fwssd       in.asessiond    respawn 0
0       fwssd       in.aufpd        respawn 0
0       fwssd       in.aciufpd        respawn 0
0               vpn             vpnd            respawn 0
0               fwssd           mdq                     respawn 0
0       stormd      stormd          respawn 0
0       igwd        igwd            respawn 0
0       fwssd           in.emaild.mta                   respawn 0
0       fwssd           in.msd                  respawn 0
0       sds             sdsd            respawn         0
0       dtps            dtpsd           respawn         0
0       dtls            dtlsd           respawn         0
[Expert@london]#
```



No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	http ftp	User Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	accept	- None	Policy Targets

A. The configuration file $FWDIR/conf/fwauthd.conf is incorrect.
B. The Security Policy is not correct.
C. You can't use any port other than the standard port 900 for Client Authentication via HTTP.
D. The service FW_clntauth_http configuration is incorrect.

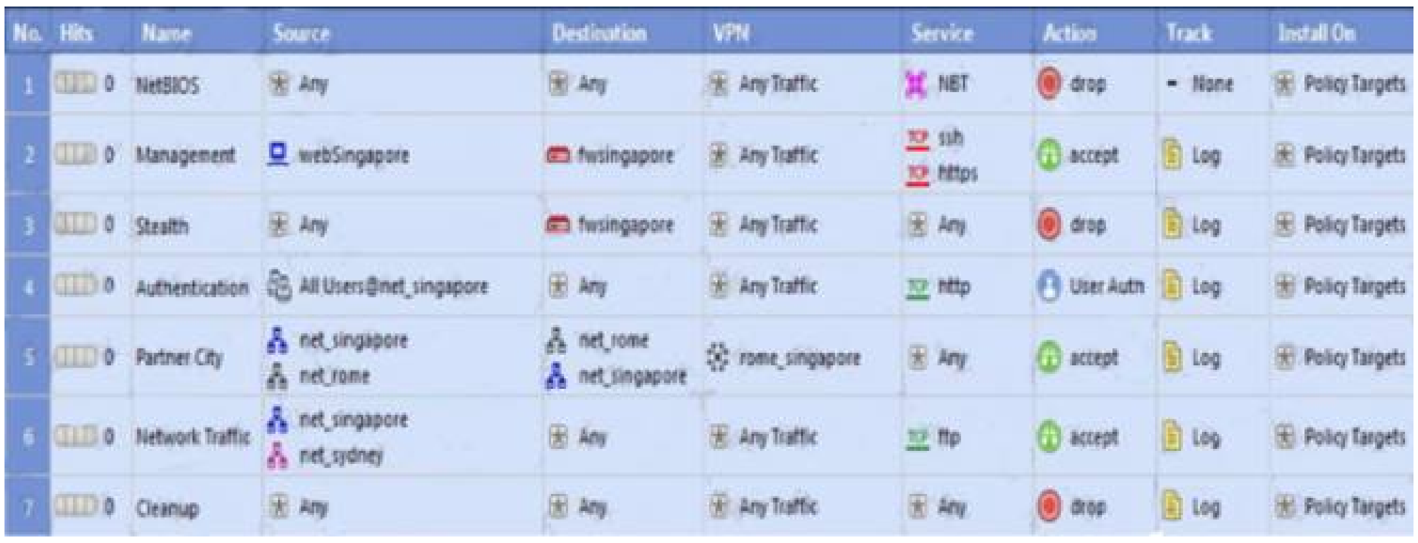
Answer: A

NEW QUESTION 344
You need to back up the routing, interface, and DNS configuration information from your R80 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 348
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	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	Authentication	All Users@net_singapore	Any	Any Traffic	http	User Auth	Log	Policy Targets
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	Any	accept	Log	Policy Targets
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	ftp	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: D

NEW QUESTION 353
Security Gateway R80 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 354
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 356
You are a Security Administrator who has installed Security Gateway R80 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 359
All R80 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 363
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 368
Which command displays the installed Security Gateway version?

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

Answer: B

NEW QUESTION 370
You are responsible for the configuration of MegaCorp's Check Point Firewall. You need to allow two NAT rules to match a connection. Is it possible? Give the BEST answer.

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

Answer: D

NEW QUESTION 375
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 377
Which Security Gateway R80 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 381
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 386
Fill in the blank. To enter the router shell, use command ____.

Answer:

Explanation: cligated

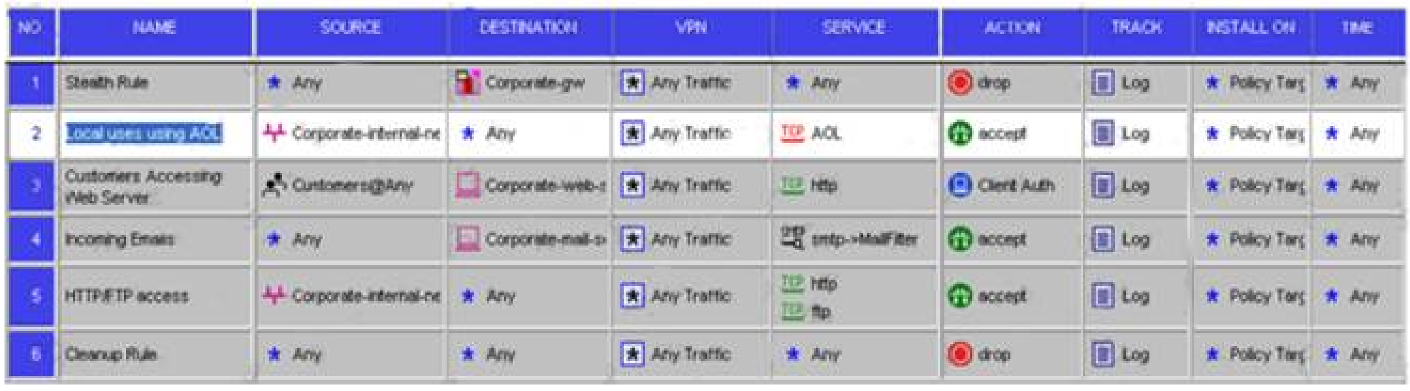
NEW QUESTION 390

A ClusterXL configuration is limited to members.

A. There is no limit.
B. 16
C. 6
D. 2

Answer: C

NEW QUESTION 393
Review the Rule Base displayed.



NO	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	Stealth Rule	Any	Corporate-gw	Any Traffic	Any	drop	Log	Policy Targ	Any
2	Local uses using AOL	Corporate-internal-ne	Any	Any Traffic	AOL	accept	Log	Policy Targ	Any
3	Customers Accessing Web Server	Customers@Any	Corporate-web-s	Any Traffic	http	Client Auth	Log	Policy Targ	Any
4	Incoming Emails	Any	Corporate-mail-s	Any Traffic	smtp->MailFilter	accept	Log	Policy Targ	Any
5	HTTP/FTP access	Corporate-internal-ne	Any	Any Traffic	http ftp	accept	Log	Policy Targ	Any
6	Cleanup Rule	Any	Any	Any Traffic	Any	drop	Log	Policy Targ	Any

For which rules will the connection templates be generated in SecureXL?

A. Rules 2 and 5
B. Rules 2 through 5
C. Rule 2 only
D. All rules except Rule 3

Answer: D

NEW QUESTION 397
Which process should you debug if SmartDashboard login fails?

A. sdm
B. cpd
C. fwd
D. fwm

Answer: D

NEW QUESTION 399
When migrating the SmartEvent data base from one server to another, the first step is to back up the files on the original server. Which of the following commands should you run to back up the SmartEvent data base?

A. migrate export
B. eva_db_backup
C. snapshot
D. backup

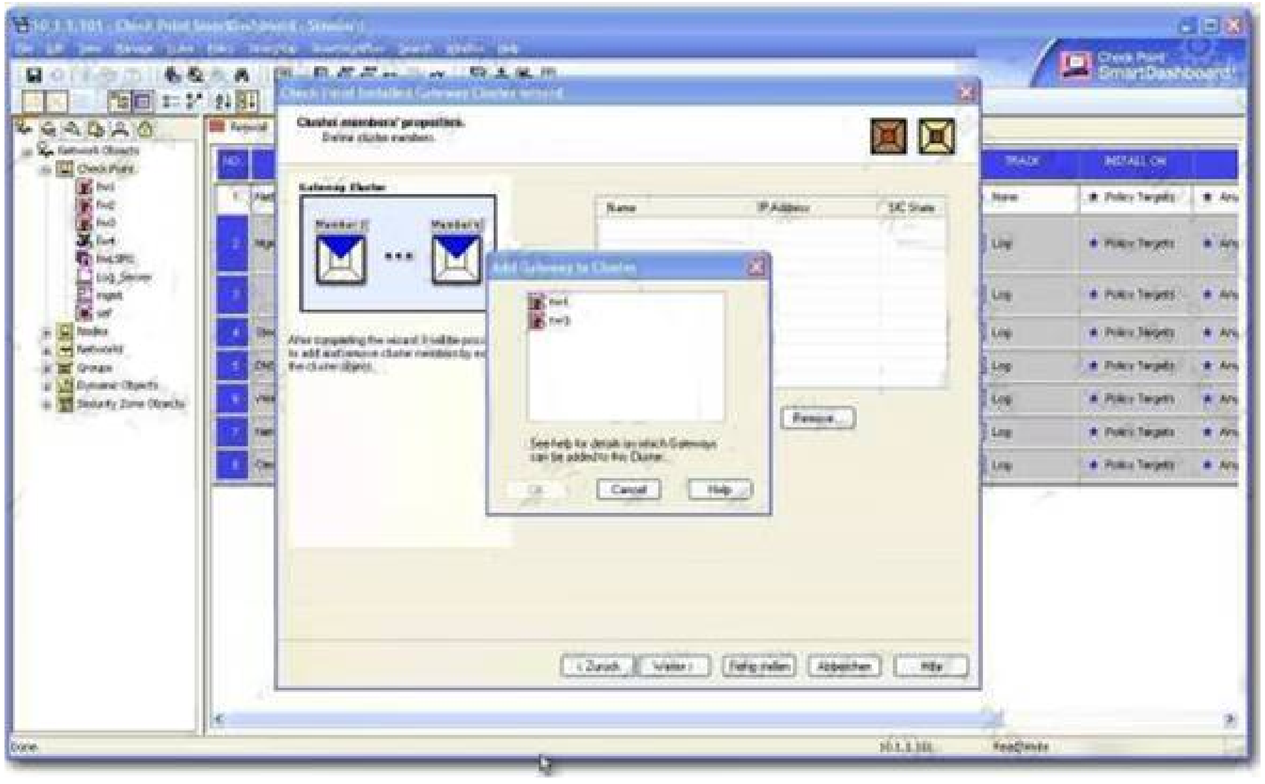
Answer: B

NEW QUESTION 403
Type the full fw command and syntax that will show full synchronization status.

Answer:

Explanation: fw ctl pstat

NEW QUESTION 405
You find that Gateway fw2 can NOT be added to the cluster object. What are possible reasons for that? Exhibit:



1) fw2 is a member in a VPN community.
2) ClusterXL software blade is not enabled on fw2.
3) fw2 is a DAIP Gateway.

A. 2 or 3
B. 1 or 2
C. 1 or 3
D. All

Answer: C

NEW QUESTION 406
Fill in the blank. To verify SecureXL statistics, you would use the command .

Answer:

Explanation: fwaccel stats

NEW QUESTION 409
Your organization maintains several IKE VPN’s. Executives in your organization want to know which mechanism Security Gateway R80 uses to guarantee the authenticity and integrity of messages. Which technology should you explain to the executives?

A. Certificate Revocation Lists
B. Application Intelligence
C. Key-exchange protocols
D. Digital signatures

Answer: D

NEW QUESTION 411
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 anexternal interface.

Answer: A

NEW QUESTION 413
Type the full cphaprob command and syntax that will show full synchronization status.

Answer:

Explanation: cphaprob -i list

NEW QUESTION 416
Which of the following CLISH commands would you use to set the admin user's shell to bash?

A. set user admin shell bash

B. set user admin shell /bin/bash
C. set user admin shell = /bin/bash
D. set user admin /bin/bash

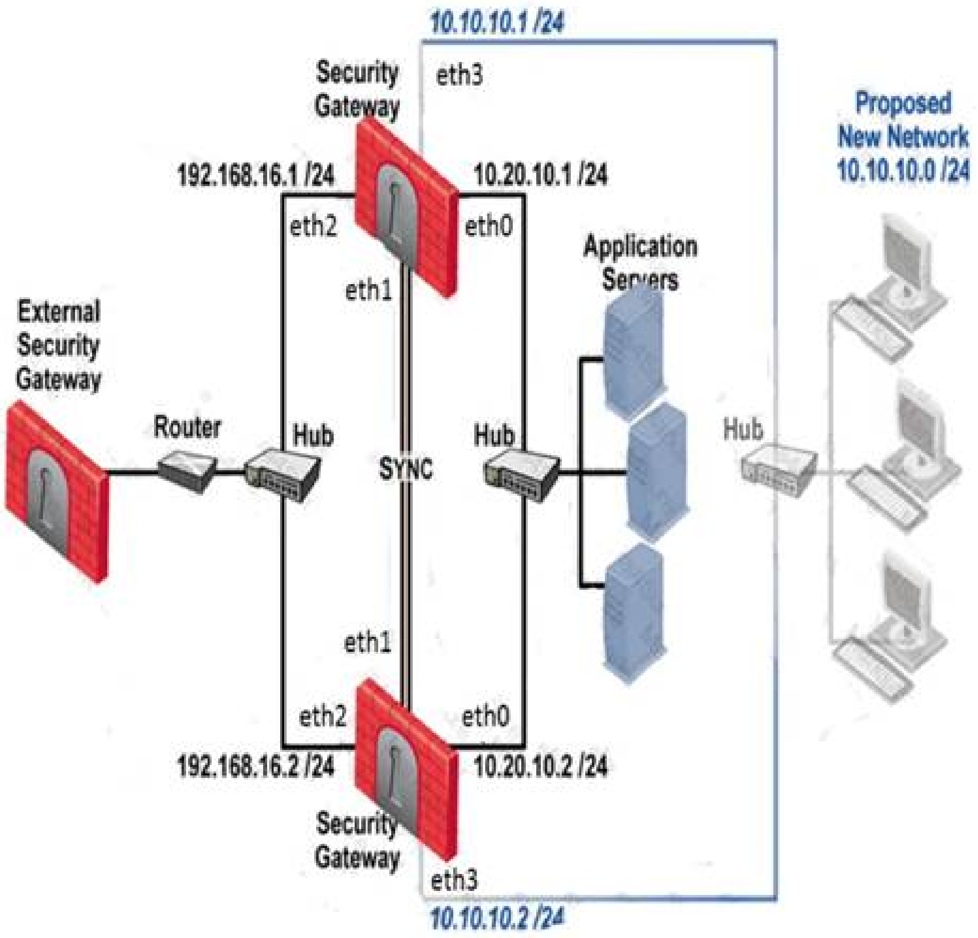
Answer: B

NEW QUESTION 421
Fill in the blank. To remove site-to-site IKE and IPSEC keys you would enter command and select the option to delete all IKE and IPSec SA's.

Answer:

Explanation: vpn tu

NEW QUESTION 422
Your expanding network currently includes ClusterXL running Multicast mode on two members, as shown in this topology:
Exhibit:



You need to add interfaces: 10.10.10.1/24 on Member A, and 10.10.10.2/24 on Member B. The virtual IP address for these interfaces is 10.10.10.3/24. Both cluster gateways have a Quad card with an available eth3 interface. What is the correct procedure to add these interfaces?

A. 1. Disable "Cluster membership" from one Gateway via cpconfig.2. Configure the new interface via sysconfig from the "non-member" Gateway.3. Re-enable "Cluster membership" on the Gateway.4. Perform the same steps on the other Gateway.5. Update the topology in the cluster object.6. Install the Security Policy.
B. 1. Configure the new interface on both members using WebUI.2. Update the new topology in the clusterobject from SmartDashboard.3. Define virtual IP in the Dashboard4. Install the Security Policy.
C. 1. Use WebUI to configure the new interfaces on both member.2. Update the topology in the cluster object.3. Reboot both gateways.4. Install the Security Policy.
D. 1. Use the command ifconfig to configure and enable the new interface on both members.2. Update the topology in the cluster object for the cluster and both members.3. Install the Security Policy.4. Reboot the gateway.

Answer: B

NEW QUESTION 423
You run cphaprob -a if. When you review the output, you find the word DOWN. What does DOWN mean?

A. The cluster link is down.
B. The physical interface is administratively set to DOWN.
C. The physical interface is down.
D. CCP pakets couldn't be sent to or didn't arrive from neighbor member.

Answer: D

NEW QUESTION 424
In the following cluster configuration; if you reboot sglondon_1 which device will be active when sglondon_1 is back up and running? Why?

A. sglondon_1 because it the first configured object with the lowest IP.
B. sglondon_2 because sglondon_1 has highest IP.
C. sglondon_1, because it is up again, sglondon_2 took over during reboot.
D. sglondon_2 because it has highest priority.

Answer: D

NEW QUESTION 426
MicroCorp experienced a security appliance failure. (LEDs of all NICs are off.) The age of the unit required that the RMA-unit be a different model. Will a revert to an existing snapshot bring the new unit up and
running?

A. There is no dynamic update at reboot.
B. N
C. The revert will most probably not match to hard disk.
D. Ye
E. Everything is dynamically updated at reboot.
F. N
G. At installation the necessary hardware support is selecte
H. The snapshot saves this state.

Answer: D

NEW QUESTION 431
Fill in the blank. To verify the SecureXL status, you would enter command .

Answer:

Explanation: fwaccel stat

NEW QUESTION 434
When configuring numbered VPN Tunnel Interfaces (VTIs) in a clustered environment, what issues need to be considered?
1) Each member must have a unique source IP address.
2) Every interface on each member requires a unique IP address.
3) All VTI's going to the same remote peer must have the same name.
4) Cluster IP addresses are required.

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

Answer: C

NEW QUESTION 435
Which command will erase all CRL's?

A. vpn crladmin
B. cpstop/cpstart
C. vpn crl_zap
D. vpn flush

Answer: C

NEW QUESTION 436
MultiCorp is located in Atlanta. It has a branch office in Europe, Asia, and Africa. Each location has its own AD controller for local user login. How many ADqueries have to be configured?

Answer:

Explanation: 4

NEW QUESTION 438
Which Check Point tool allows you to open a debug file and see the VPN packet exchange details.

A. PacketDebug.exe
B. VPNDebugger.exe
C. IkeView.exe
D. IPSECDebug.exe

Answer: C

NEW QUESTION 442
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 447
Complete this statement. To save interface information before upgrading a Windows Gateway, use command

Answer:

Explanation: ipconfig -a > [filename].txt

NEW QUESTION 448
Which file defines the fields for each object used in the file objects.C (color, num/string, default value…)?

A. $FWDIR/conf/classes.C
B. $FWDIR/conf/scheam.C
C. $FWDIR/conf/fields.C
D. $FWDIR/conf/table.C

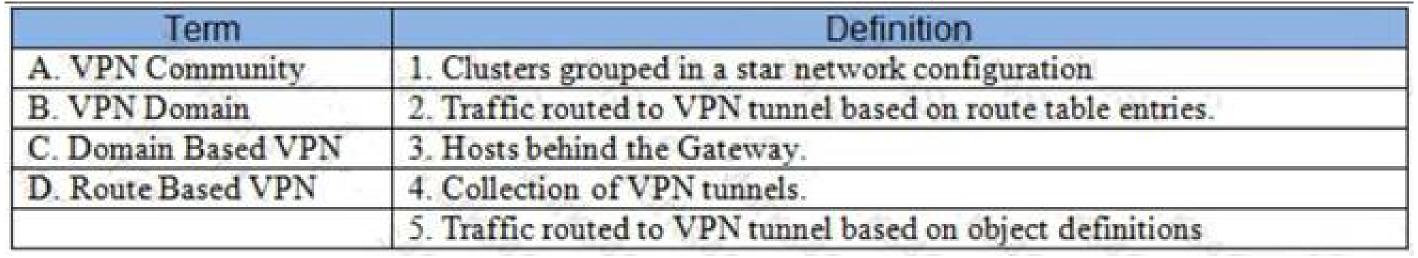
Answer: A

NEW QUESTION 452
What is the purpose of the pre-defined exclusions included with SmartEvent R80?

A. To allow SmartEvent R80 to function properly with all other R71 devices.
B. To avoid incorrect event generation by the default IPS event definition; a scenario that may occur in deployments that include Security Gateways of versions prior to R71.
C. As a base for starting and building exclusions.
D. To give samples of how to write your own exclusion.

Answer: B

NEW QUESTION 453
Match the VPN-related terms with their definitions. Each correct term is only used once. Exhibit:



Term	Definition
A. VPN Community	1. Clusters grouped in a star network configuration
B. VPN Domain	2. Traffic routed to VPN tunnel based on route table entries.
C. Domain Based VPN	3. Hosts behind the Gateway.
D. Route Based VPN	4. Collection of VPN tunnels.
	5. Traffic routed to VPN tunnel based on object definitions

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

Answer: B

NEW QUESTION 454
Fill in the blanks. To view the number of concurrent connections going through your firewall, you would use the command and syntax ____ .

Answer:

Explanation: fw tab –t connections –s

NEW QUESTION 458
If Jack was concerned about the number of log entries he would receive in the SmartReporter system, which policy would he need to modify?

A. Log Sequence Policy
B. Report Policy
C. Log Consolidator Policy
D. Consolidation Policy

Answer: D

NEW QUESTION 459
Which two processes are responsible on handling Identity Awareness?

A. pdp and lad
B. pdp and pdp-11
C. pep and lad

D. pdp and pep

Answer: D

NEW QUESTION 464
Your company has the requirement that SmartEvent reports should show a detailed and accurate view of network activity but also performance should be guaranteed. Which actions should be taken to achieve that?
1) Use same hard drive for database directory, log files, and temporary directory.
2) Use Consolidation Rules.
3) Limit logging to blocked traffic only.
4) Use Multiple Database Tables.

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

Answer: A

NEW QUESTION 468
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 472
To provide full connectivity upgrade status, use command

Answer:

Explanation: cphaprob fcustat

NEW QUESTION 477
MultiCorp has bought company OmniCorp and now has two active AD domains. How would you deploy Identity Awareness in this environment?

A. You must run an ADquery for every domain.
B. Identity Awareness can only manage one AD domain.
C. Only one ADquery is necessary to ask for all domains.
D. Only Captive Portal can be used.

Answer: A

NEW QUESTION 478
To bind a NIC to a single processor when using CoreXL on GAiA, you would use the command

Answer:

Explanation: sim affinity

NEW QUESTION 482
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. Exchange exported CA keys and use them to create a new server object to represent your partner’s Certificate Authority (CA).
B. Create a new logical-server object to represent your partner’s CA.
C. Manually import your partner’s Access Control List.
D. Manually import your partner’s Certificate Revocation List.

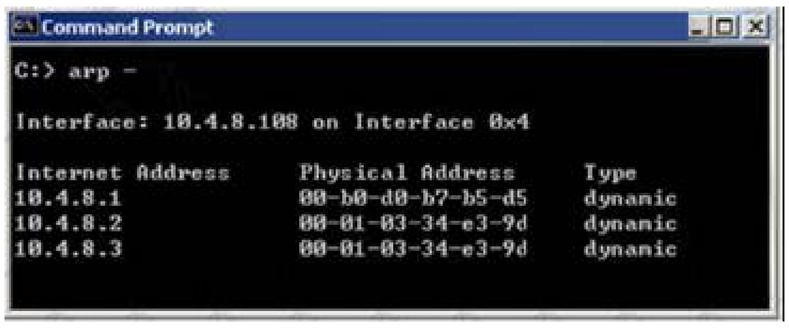
Answer: A

NEW QUESTION 484
You are troubleshooting a HTTP connection problem. You've started fw monitor -o http.pcap. When you open http.pcap with Wireshark there is only one line. What is the most likely reason?

A. fw monitor was restricted to the wrong interface.
B. Like SmartView Tracker only the first packet of a connection will be captured by fw monitor.
C. By default only SYN pakets are captured.
D. Acceleration was turned on and therefore fw monitor sees only SYN.

Answer: D

NEW QUESTION 487
Fill in the blank.



```
C:> arp -

Interface: 10.4.8.108 on Interface 0x4

Internet Address      Physical Address      Type
10.4.8.1              00-b0-d0-b7-b5-d5     dynamic
10.4.8.2              00-01-03-34-e3-9d     dynamic
10.4.8.3              00-01-03-34-e3-9d     dynamic
```

In New Mode HA, the internal cluster IP VIP address is 10.4.8.3. An internal host 10.4.8.108 successfully pings its Cluster and receives replies. Review the ARP table from the internal Windows host 10.4.8.108. Based on this information, what is the active cluster member's IP address?

Answer:

Explanation: 10.4.8.2

NEW QUESTION 492
What is Check Point's CoreXL?

A. A way to synchronize connections across cluster members
B. TCP-18190
C. Multiple core interfaces on the device to accelerate traffic
D. Multi Core support for Firewall Inspection

Answer: D

NEW QUESTION 493
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
Where is it necessary to configure historical records in SmartView Monitor to generate Express reports in SmartReporter?

A. In SmartDashboard, the SmartView Monitor page in the R80 Security Gateway object
B. In SmartReporter, under Express > Network Activity
C. In SmartReporter, under Standard > Custom
D. In SmartView Monitor, under Global Properties > Log and Masters

Answer: A

NEW QUESTION 502
Fill in the blank. You can set Acceleration to ON or OFF using command syntax .

Answer:

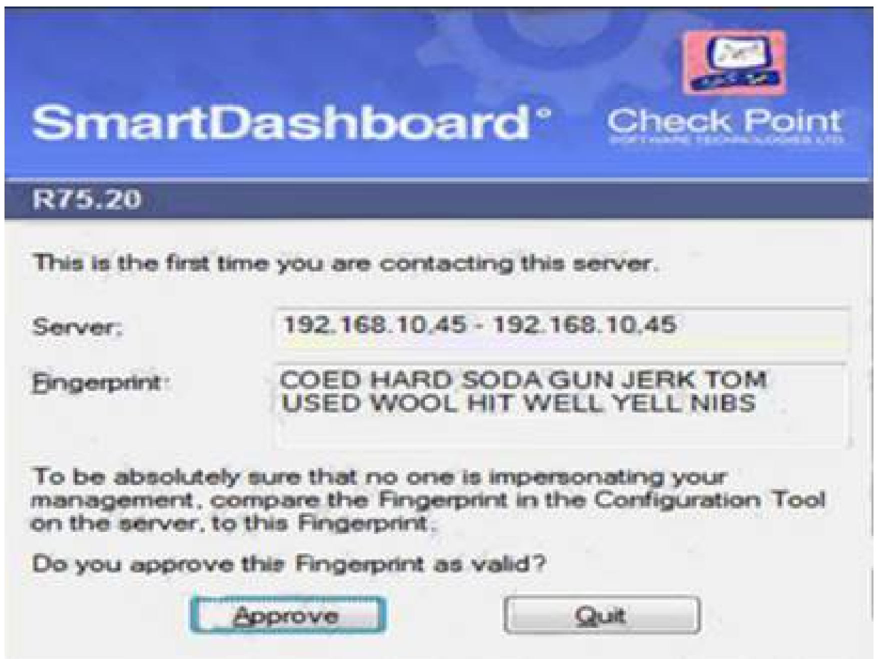
Explanation: fwaccel off/on

NEW QUESTION 503
To qualify as an Identity Awareness enabled rule, which column MAY include an Access Role?

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

Answer: A

NEW QUESTION 508
How could you compare the Fingerprint shown to the Fingerprint on the server? Exhibit:



This is the first time you are contacting this server.

Server: 192.168.10.45 - 192.168.10.45

Fingerprint: COED HARD SODA GUN JERK TOM USED WOOL HIT WELL YELL NIBS

To be absolutely sure that no one is impersonating your management, compare the Fingerprint in the Configuration Tool on the server, to this Fingerprint.

Do you approve this Fingerprint as valid?

A. Run cpconfig, select the Certificate's Fingerprint option and view the fingerprint
B. Run cpconfig, select the GUI Clients option and view the fingerprint
C. Run cpconfig, select the Certificate Authority option and view the fingerprint
D. Run sysconfig, select the Server Fingerprint option and view the fingerprint

Answer: A

NEW QUESTION 513
Which three of the following are ClusterXL member requirements?
1) same operating systems
2) same Check Point version
3) same appliance model
4) same policy

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

Answer: B

NEW QUESTION 516
MegaCorp is running Smartcenter R70, some Gateways at R65 and some other Gateways with R60. Management wants to upgrade to the most comprehensive IPv6 support. What should the administrator do first?

A. Upgrade Smartcenter to R80 first.
B. Upgrade R60-Gateways to R65.
C. Upgrade every unit directly to R80.
D. Check the ReleaseNotes to verify that every step is supported.

Answer: D

NEW QUESTION 519
You have selected the event Port Scan from Internal Network in SmartEvent, to detect an event when 30 port scans have occurred within 60 seconds. You also want to detect two port scans from a host within 10 seconds of each other. How would you accomplish this?

A. Define the two port-scan detections as an exception.
B. You cannot set SmartEvent to detect two port scans from a host within 10 seconds of each other.
C. Select the two port-scan detections as a sub-event.
D. Select the two port-scan detections as a new event.

Answer: A

NEW QUESTION 524
Which of the following items should be configured for the Security Management Server to authenticate using LDAP?

A. Check Point Password
B. WMI object
C. Domain Admin username
D. Windows logon password

Answer: A

NEW QUESTION 528
In a zero downtime firewall cluster environment, what command syntax do you run to avoid switching problems around the cluster for command cphaconf?

Answer:

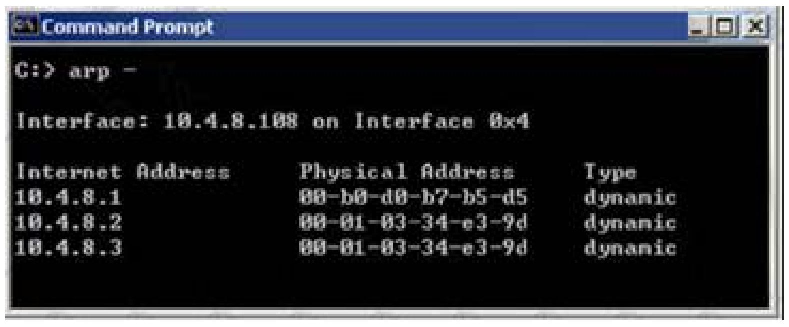
Explanation: set_ccp broadcast

NEW QUESTION 532
Which CLI tool helps on verifying proper ClusterXL sync?

A. fw stat
B. fw ctl sync
C. fw ctl pstat
D. cphaprob stat

Answer: C

NEW QUESTION 534
Fill in the blank.



```
C:> arp -

Interface: 10.4.8.108 on Interface 0x4

Internet Address      Physical Address      Type
10.4.8.1              00-b0-d0-b7-b5-d5     dynamic
10.4.8.2              00-01-03-34-e3-9d     dynamic
10.4.8.3              00-01-03-34-e3-9d     dynamic
```

In New Mode HA, the internal cluster IP VIP address is 10.4.8.3. The internal interfaces on two members are 10.4.8.1 and 10.4.8.2 Internal host 10.4.8.108 pings 10.4.8.3, and receives replies. Review the ARP table from the internal Windows host 10.4.8.108. According to the output, which member is the standby machine?

Answer:

Explanation: 10.4.8.1

NEW QUESTION 536
Fill in the blank. What is the correct command and syntax used to view a connection table summary on a Check Point Firewall?

Answer:

Explanation: fw tab -t connections -s

NEW QUESTION 538
Fill in the blank. To verify that a VPN Tunnel is properly established, use the command _____

Answer:

Explanation: vpn tunnelutil

NEW QUESTION 541
How many pre-defined exclusions are included by default in SmartEvent R80 as part of the product installation?

A. 5
B. 10
C. 3

Answer:

NEW QUESTION 545
Which is the lowest Gateway version manageable by SmartCenter R80?

A. R65
B. S71
C. R55
D. R60A

Answer: A

NEW QUESTION 547
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 551
If you need strong protection for the encryption of user data, what option would be the BEST choice?

A. Use Diffie-Hellman for key construction and pre-shared keys for Quick Mod
B. Choose SHA in Quick Mode and encrypt with AE
C. Use AH protoco
D. Switch to Aggressive Mode.
E. When you need strong encryption, IPsec is not the best choic
F. SSL VPN's are a better choice.
G. Use certificates for Phase 1, SHA for all hashes, AES for all encryption and PFS, and use ESP protocol.
H. Disable Diffie-Hellman by using stronger certificate based key-derivatio
I. Use AES-256 bit on all encrypted channels and add PFS to QuickMod
J. Use double encryption by implementing AH and ESP as protocols.

Answer: C

NEW QUESTION 555
You want VPN traffic to match packets from internal interfaces. You also want the traffic to exit the Security Gateway bound for all site-to-site VPN Communities, including Remote Access Communities. How should you configure the VPN match rule?

A. internal_clear > All_communities
B. Internal_clear > External_Clear
C. Communities > Communities
D. internal_clear > All_GwToGw

Answer: A

NEW QUESTION 558
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 562
Select the command set best used to verify proper failover function of a new ClusterXL configuration.

A. reboot
B. cphaprob -d failDevice -s problem -t 0 register / cphaprob -d failDevice unregister
C. clusterXL_admin down / clusterXL_admin up
D. cpstop/cpstart

Answer: C

NEW QUESTION 564
Type the full fw command and syntax that allows you to disable only sync on a cluster firewall member.

Answer:

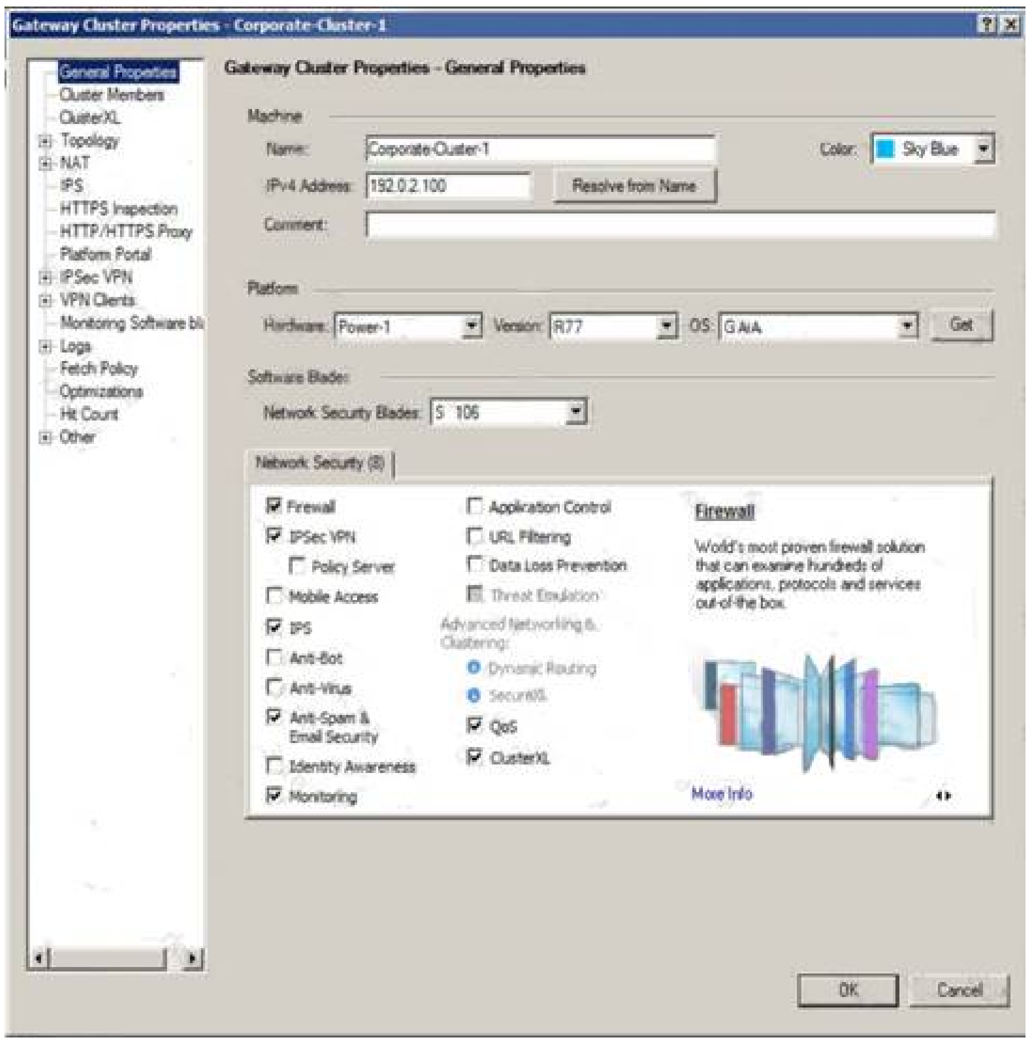
Explanation: fw ctl setsync off

NEW QUESTION 565
Fill in the blank with a numeric value. The default port number for Secure Sockets Layer (SSL) connections with the LDAP Server is

Answer:

Explanation: 636

NEW QUESTION 567
John is configuring a new R80 Gateway cluster but he can not configure the cluster as Third Party IP Clustering because this option is not available in Gateway Cluster Properties.



Gateway Cluster Properties - Corporate-Cluster-1

Gateway Cluster Properties - General Properties

Machine

Name: Corporate-Cluster-1

Color: Sky Blue

IPv4 Address: 192.0.2.100 Resolve from Name

Comment:

Platform

Hardware: Power-1 Version: R77 OS: GAiA Get

Software Blade:

Network Security Blades: S 106

Network Security (8)

☑ Firewall
☑ IPSec VPN
□ Policy Server
□ Mobile Access
☑ IPS
□ Anti-Bot
□ Anti-Virus
☑ Anti-Spam & Email Security
□ Identity Awareness
☑ Monitoring

□ Application Control
□ URL Filtering
□ Data Loss Prevention
▨ Threat Emulation

Advanced Networking & Clustering:
● Dynamic Routing
● SecureXL
☑ QoS
☑ ClusterXL

Firewall

World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

What's happening?

A. ClusterXL needs to be unselected to permit third party clustering configuration.
B. Third Party Clustering is not available for R80 Security Gateways.
C. John has an invalid ClusterXL license.
D. John is not using third party hardware as IP Clustering is part of Check Point's IP Appliance.

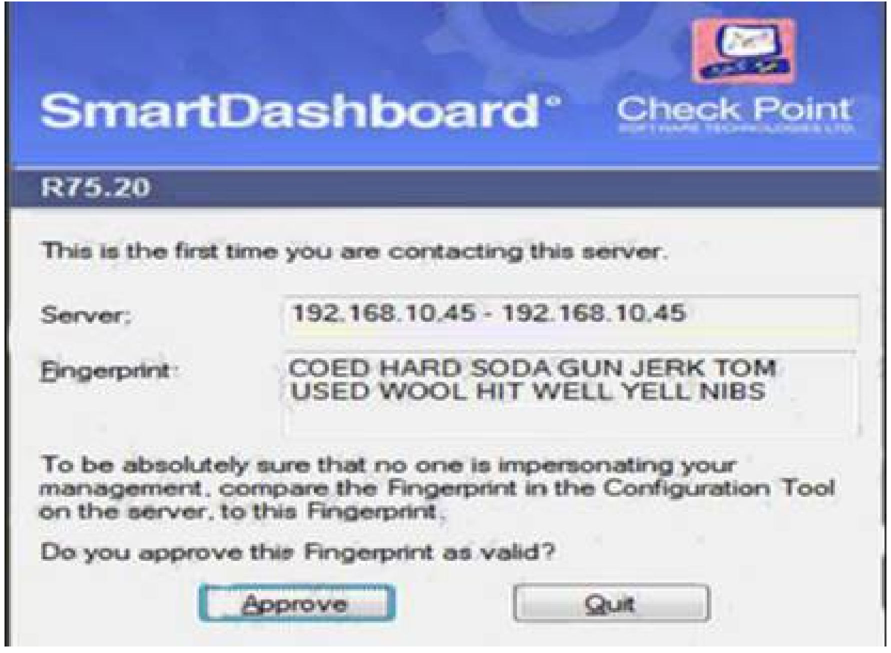
Answer: A

NEW QUESTION 569
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 573
How could you compare the Fingerprint shown to the Fingerprint on the server? Run cpconfig and select: Exhibit:



This is the first time you are contacting this server.

Server: 192.168.10.45 - 192.168.10.45

Fingerprint: COED HARD SODA GUN JERK TOM USED WOOL HIT WELL YELL NIBS

To be absolutely sure that no one is impersonating your management, compare the Fingerprint in the Configuration Tool on the server, to this Fingerprint.

Do you approve this Fingerprint as valid?

A. the Certificate Authority option and view the fingerprint.
B. the GUI Clients option and view the fingerprint.
C. the Certificate's Fingerprint option and view the fingerprint.
D. the Server Fingerprint option and view the fingerprint.

Answer: C

NEW QUESTION 576
When do modifications to the Event Policy take effect?

A. As soon as the Policy Tab window is closed.
B. When saved on the SmartEvent Server and installed to the Correlation Units.
C. When saved on the Correlation Units, and pushed as a policy.
D. When saved on the SmartEvent Client, and installed on the SmartEvent Server.

Answer: B

NEW QUESTION 577
......