



# Check Point

## Exam Questions 156-915.80

Check Point Certified Security Expert Update - R80

#### NEW QUESTION 1

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 2

Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

- A. UDP port 265
- B. TCP port 265
- C. UDP port 256
- D. TCP port 256

**Answer:** D

**Explanation:** Synchronization works in two modes: References:

#### NEW QUESTION 3

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 4

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 5

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 6

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 each kernel instance. The state and processing core number of each instance is displayed, along with:

#### NEW QUESTION 7

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 SmartDashboard client
- D. Execute command cpconfig

**Answer:** D

#### NEW QUESTION 8

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 9

The Firewall kernel is replicated multiple times, therefore:

- A. The Firewall kernel only touches the packet if the connection is accelerated
- B. The Firewall can run different policies per core
- C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
- D. The Firewall can run the same policy on all cores

**Answer:** D

**Explanation:** On a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated copy, or instance, runs on one processing core. These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel. When CoreXL is enabled, all the kernel instances in the Security Gateway process traffic through the same interfaces and apply the same security policy.

#### NEW QUESTION 10

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 10

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 11

The CDT utility supports which of the following?

- A. Major version upgrades to R77.30
- B. Only Jumbo HFA's and hotfixes
- C. Only major version upgrades to R80.10
- D. All upgrades

**Answer:** D

**Explanation:** The Central Deployment Tool (CDT) is a utility that runs on an R77 / R77.X / R80 / R80.10 Security Management Server / Multi-Domain Security Management Server (running Gaia OS).  
It allows the administrator to automatically install CPUSE Offline packages (Hotfixes, Jumbo Hotfix Accumulators (Bundles), Upgrade to a Minor Version, Upgrade to a Major Version) on multiple managed Security Gateways and Cluster Members at the same time.  
References:

#### NEW QUESTION 13

In R80 spoofing is defined as a method of:

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

**Answer:** D

**Explanation:** IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

#### NEW QUESTION 15

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 18

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 19

VPN Tunnel Sharing can be configured with any of the options below, EXCEPT One:

- A. Gateway-based
- B. Subnet-based
- C. IP range based
- D. Host-based

**Answer:** C

**Explanation:** VPN Tunnel Sharing provides interoperability and scalability by controlling the number of VPN tunnels created between peer Security Gateways. There are three available settings:

#### NEW QUESTION 21

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 25

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 26

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 29

What Shell is required in Gaia to use WinSCP?

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

**Answer:** D

#### NEW QUESTION 34

What is the responsibility of SOLR process on R80.10 management server?

- A. Validating all data before it's written into the database
- B. It generates indexes of data written to the database
- C. Communication between SmartConsole applications and the Security Management Server
- D. Writing all information into the database

**Answer:** B

#### NEW QUESTION 35

What is the SandBlast Agent designed to do?

- A. Performs OS-level sandboxing for SandBlast Cloud architecture
- B. Ensure the Check Point SandBlast services is running on the end user's system
- C. If malware enters an end user's system, the SandBlast Agent prevents the malware from spreading with the network
- D. Clean up email sent with malicious attachments.

**Answer:** C

#### NEW QUESTION 40

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 41

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 42

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 47

In Gaia, if one is unsure about a possible command, what command lists all possible commands.

- A. show all |grep commands
- B. show configuration
- C. show commands
- D. get all commands

**Answer:** C

#### NEW QUESTION 52

When Dynamic Dispatcher is enabled, connections are assigned dynamically with the exception of

- A. Threat Emulation
- B. HTTPS
- C. QOS
- D. VoIP

**Answer:** D

**Explanation:** The following types of traffic are not load-balanced by the CoreXL Dynamic Dispatcher (this traffic will always be handled by the same CoreXL FW instance):

#### NEW QUESTION 53

What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?

- A. Stateful Mode
- B. VPN Routing Mode
- C. Wire Mode
- D. Stateless Mode

**Answer:** C

**Explanation:** Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of "Wire Mode".

#### NEW QUESTION 58

Which file gives you a list of all security servers in use, including port number?

- A. \$FWDIR/conf/conf.conf
- B. \$FWDIR/conf/servers.conf
- C. \$FWDIR/conf/fwauthd.conf
- D. \$FWDIR/conf/serversd.conf

**Answer:** C

#### NEW QUESTION 63

Aaron is a Cyber Security Engineer working for Global Law Firm with large scale deployment of Check Point Enterprise Appliances using GAI/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 66

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 71

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 73

Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

- A. Export R80 configuration, clean install R80.10 and import the configuration
- B. CPUSE online upgrade
- C. CPUSE offline upgrade
- D. SmartUpdate upgrade

**Answer:** C

#### NEW QUESTION 76

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 79

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 81

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 throughout 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 85

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 88

Which is a suitable command to check whether Drop Templates are activated or not?

- A. fw ctl get int activate \_drop\_ templates
- B. fwaccel stat
- C. fwaccel stats
- D. fw ctl templates -d

**Answer:** B

#### NEW QUESTION 93

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 97

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 98

SmartEvent does NOT use which of the following procedures to identify events?

- A. Matching a log against each event definition
- B. Create an event candidate
- C. Matching a log against local exclusions
- D. Matching a log against global exclusions

**Answer:** C

**Explanation:** Events are detected by the SmartEvent Correlation Unit. The Correlation Unit task is to scan logs for criteria that match an Event Definition. SmartEvent uses these procedures to identify events:

#### NEW QUESTION 102

GAiA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the:

- A. Check Point Upgrade Service Engine.
- B. Check Point Software Update Agent
- C. Check Point Remote Installation Daemon (CPRID)
- D. Check Point Software Update Daemon

**Answer:** A

#### NEW QUESTION 103

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 108

What command would show the API server status?

- A. cpm status
- B. api restart
- C. api status
- D. show api status

**Answer:** C



#### NEW QUESTION 113

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 117

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 122

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 begin 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 124

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

- A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
- B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
- C. Mail, Block Source, Block Destination, External Script, SNMP Trap
- D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

**Answer:** A

**Explanation:** These are the types of Automatic Reactions:

#### NEW QUESTION 125

What utility would you use to configure route-based VPNs?

- A. `vpn shell`
- B. `vpn tu`
- C. `vpn sw_topology`
- D. `vpn set_slim_server`

**Answer:** A

#### NEW QUESTION 129

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/fwkernel.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 130

Which one of these is NOT a firewall chain?

- A. RTM packet in (rtm)
- B. VPN node add (vpnad)
- C. IP Options restore (in) (ipopt\_res)
- D. Fw SCV inbound (scv)

**Answer:** B

#### NEW QUESTION 133

You want to store the GAIa configuration in a file for later reference. What command should you use?

- A. write mem <filename>
- B. show config -f <filename>
- C. save config -o <filename>
- D. save configuration <filename>

**Answer:** D

#### NEW QUESTION 134

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 138

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 139

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 140

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 142



You are running a R80 Security Gateway on GAIa. In case of a hardware failure, you have a server with the exact same hardware and firewall version installed. What back up method could be used to quickly put the secondary firewall into production?

- A. manual backup
- B. upgrade\_export
- C. backup
- D. snapshot

**Answer:** D

**NEW QUESTION 143**

You have created a Rule Base for firewall, websydney. Now you are going to create a new policy package with security and address translation rules for a second Gateway.

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

What is TRUE about the new package's NAT rules?

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

**Answer: A**

**NEW QUESTION 147**

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 151**

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 155**

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 interval.
- 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 interval.
- 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 interval.
- G. Select that time object's Global Properties > Logs and Masters window, to schedule a logswitch.

**Answer: B**

**NEW QUESTION 157**

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 162**

A Web server behind the Security Gateway is set to Automatic Static NAT. Client side NAT is not checked in the Global Properties. A client on the Internet initiates a session to the Web Server. Assuming there is a rule allowing this traffic, what other configuration must be done to allow the traffic to reach the Web server?

- A. Automatic ARP must be unchecked in the Global Properties.
- B. Nothing else must be configured.
- C. A static route must be added on the Security Gateway to the internal host.

D. A static route for the NAT IP must be added to the Gateway's upstream router.

**Answer: C**

#### NEW QUESTION 163

Access Role objects define users, machines, and network locations as:

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

**Answer: C**

#### NEW QUESTION 168

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 171

Review the rules.

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

Assume domain UDP is enabled in the implied 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 173

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 178

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 180

When restoring R80 using the command upgrade\_import, which of the following items are NOT restored?

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

**Answer: C**

#### NEW QUESTION 181

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

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

**Answer: B**

#### NEW QUESTION 182

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 185

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 190

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 194

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 197

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 199

Before upgrading SecurePlatform to GAiA, you should create a backup. To save time, many administrators use the command backup. This creates a backup of the Check Point configuration as well as the system configuration.

An administrator has installed the latest HFA on the system for fixing traffic problem after creating a backup file. There is a mistake in the very complex static routing configuration. The Check Point configuration has not been changed. Can the administrator use a restore to fix the errors in static routing?

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

**Answer:**



C

#### NEW QUESTION 201

Select the correct statement about Secure Internal Communications (SIC) Certificates. SIC Certificates:

- A. Are used for securing internal network communications between the SmartDashboard and the Security Management Server.
- B. For R75 Security Gateways are created during the Security Management Server installation.
- C. Decrease network security by securing administrative communication among the Security Management Servers and the Security Gateway.
- D. Uniquely identify Check Point enabled machines; they have the same function as VPN Certificates.

**Answer: D**

#### NEW QUESTION 202

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

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

**Answer: D**

#### NEW QUESTION 205

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 209

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 211

Which of the following is a CLI command for Security Gateway R80?

- A. fw tab -u
- B. fw shutdown
- C. fw merge
- D. fwm policy\_print <policyname>

**Answer: A**

#### NEW QUESTION 212

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 213

The Identity Agent is a lightweight endpoint agent that authenticates securely with Single Sign-On (SSO). What is not a recommended usage of this method?

- A. When accuracy in detecting identity is crucial
- B. Leveraging identity for Data Center protection
- C. Protecting highly sensitive servers
- D. Identity based enforcement for non-AD users (non-Windows and guest users)

**Answer: D**



#### NEW QUESTION 215

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 220

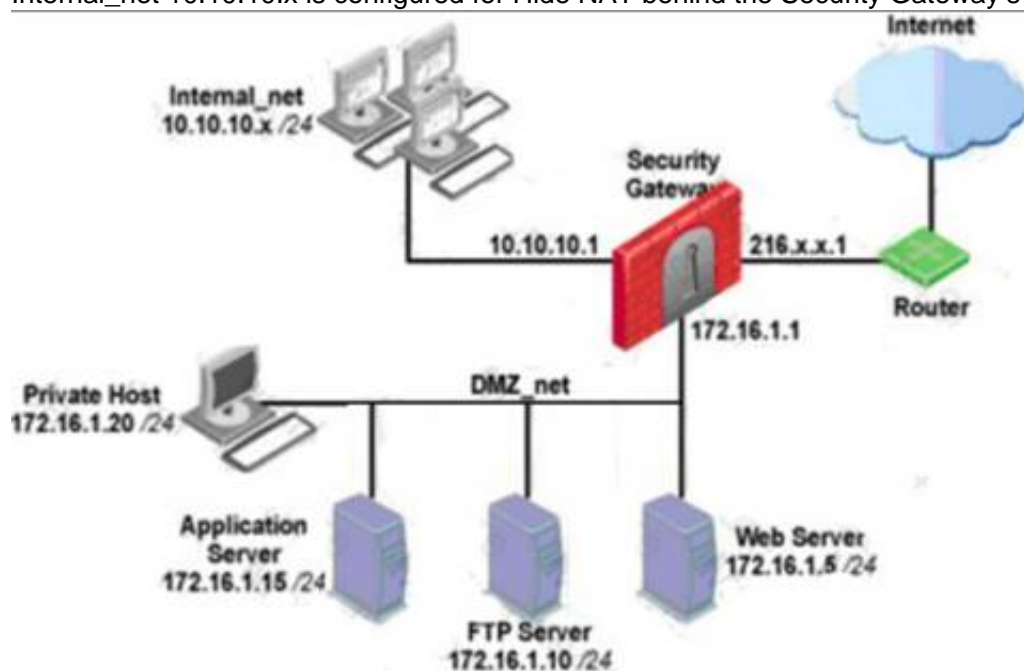
You are about to integrate RSA SecurID users into the Check Point infrastructure. What kind of users are to be defined via SmartDashboard?

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

**Answer: A**

#### NEW QUESTION 221

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 222

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 227

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/sysconfig/netconf.C and put the new MAC address in the field

```
(conf
: (conn
: (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 229

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 234

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 237

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 242

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 245

After implementing Static Address Translation to allow Internet traffic to an internal Web Server on your

DMZ, you notice that any NATed connections to that machine are being dropped by anti-spoofing protections. Which of the following is the MOST LIKELY cause?

- A. The Global Properties setting Translate destination on client side is unchecked
- B. But the topology on the DMZ interface is set to Internal - Network defined by IP and Mas
- C. Check the Global Properties setting Translate destination on client side.
- D. The Global Properties setting Translate destination on client side is unchecked
- E. But the topology on the external interface is set to Others +. Change topology to External.
- F. The Global Properties setting Translate destination on client side is checked
- G. But the topology on the external interface is set to External
- H. Change topology to Others +.
- I. The Global Properties setting Translate destination on client side is checked
- J. But the topology on the DMZ interface is set to Internal - Network defined by IP and Mas
- K. Uncheck the Global Properties setting Translate destination on client side.

**Answer:** A

#### NEW QUESTION 246

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 248

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 250

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned an IP address 10.0.0.19 via DHCP. John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop. He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator:

- 1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy.
- 2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.

John plugged in his laptop to the network on a different network segment and he is not able to connect. How does he solve this problem?

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

**Answer:** B

#### NEW QUESTION 251

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 255

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 field
- 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 Firewall
- 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 257

What is the primary benefit of using the command upgrade\_export over either backup or snapshot?

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

Answer: A

NEW QUESTION 260

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

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

Answer: A

NEW QUESTION 262

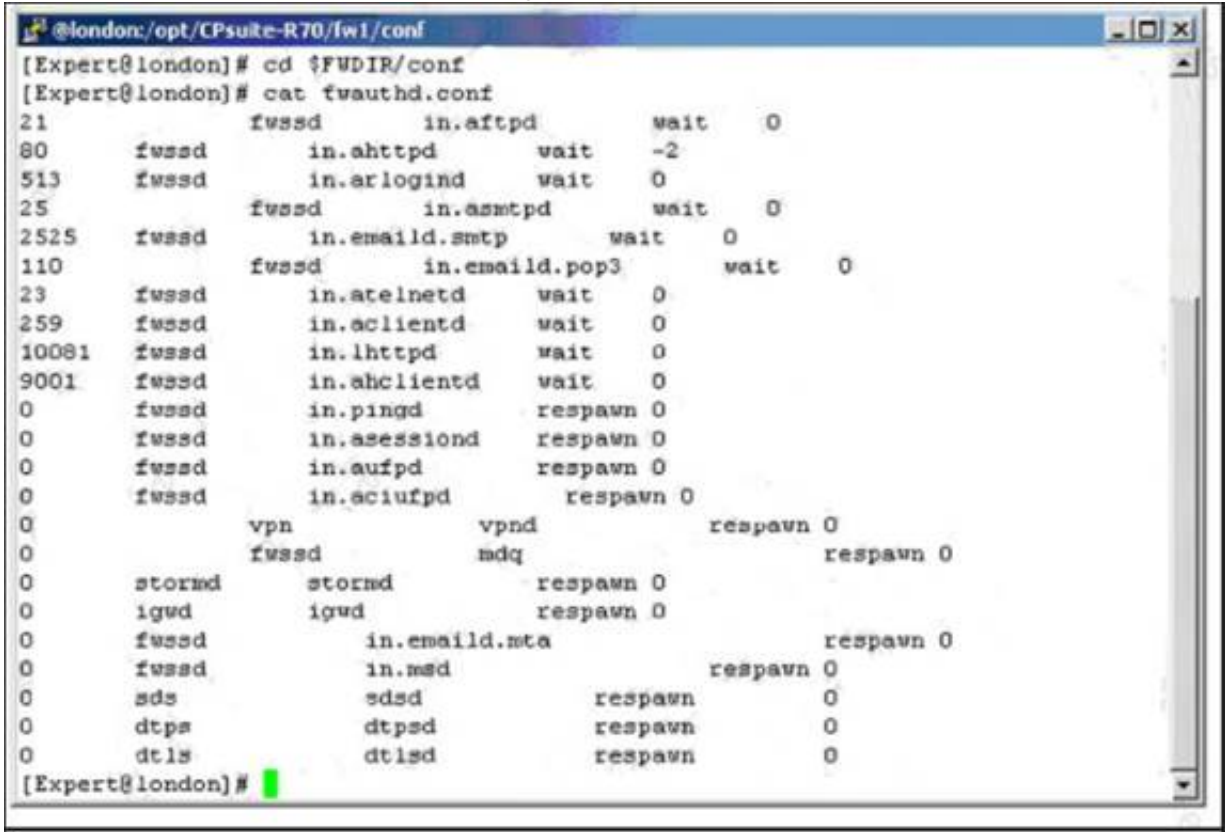
You want to generate a cpinfo file via CLI on a system running GAIa. This will take about 40 minutes since the log files are also needed. What action do you need to take regarding timeout?

- 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 267

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?



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 270

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 275

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	NET	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 278

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 282

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

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

**Answer: D**

#### NEW QUESTION 284

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 286

Which command displays the installed Security Gateway version?

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

**Answer: B**

#### NEW QUESTION 288

As a Security Administrator, you must refresh the Client Authentication authorization time-out every time a new user connection is authorized. How do you do this?

Enable the Refreshable Timeout setting:

- A. in the user object's Authentication screen.
- B. in the Gateway object's Authentication screen.
- C. in the Limit tab of the Client Authentication Action Properties screen.
- D. in the Global Properties Authentication screen.

**Answer: C**

#### NEW QUESTION 292

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 293

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

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

**Answer: A**

**Explanation:** Topic 3, Exam Pool B

#### NEW QUESTION 294

Fill in the blank. To enter the router shell, use command \_\_\_\_\_.

**Answer:**

**Explanation:** cligated

#### NEW QUESTION 298

A ClusterXL configuration is limited to members.

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

**Answer: C**

#### NEW QUESTION 299

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 users 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 301

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 304

To run GAIa in 64bit mode, which of the following is true?

- 1) Run set edition default 64-bit.
- 2) Install more than 4 GB RAM.
- 3) Install more than 4 TB of Hard Disk.

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

**Answer:** B

#### NEW QUESTION 306

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

**Answer:**

**Explanation:** fwaccel stats

#### NEW QUESTION 310

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 311

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

**Answer:**

**Explanation:** cphaprob -i list

#### NEW QUESTION 313

What command syntax would you use to see accounts the gateway suspects are service accounts?

- A. pdp check\_log
- B. pdp show service
- C. adlog check\_accounts
- D. adlog a service\_accounts

**Answer:** D

#### NEW QUESTION 318

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 320

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

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

**Answer:** B

#### NEW QUESTION 324

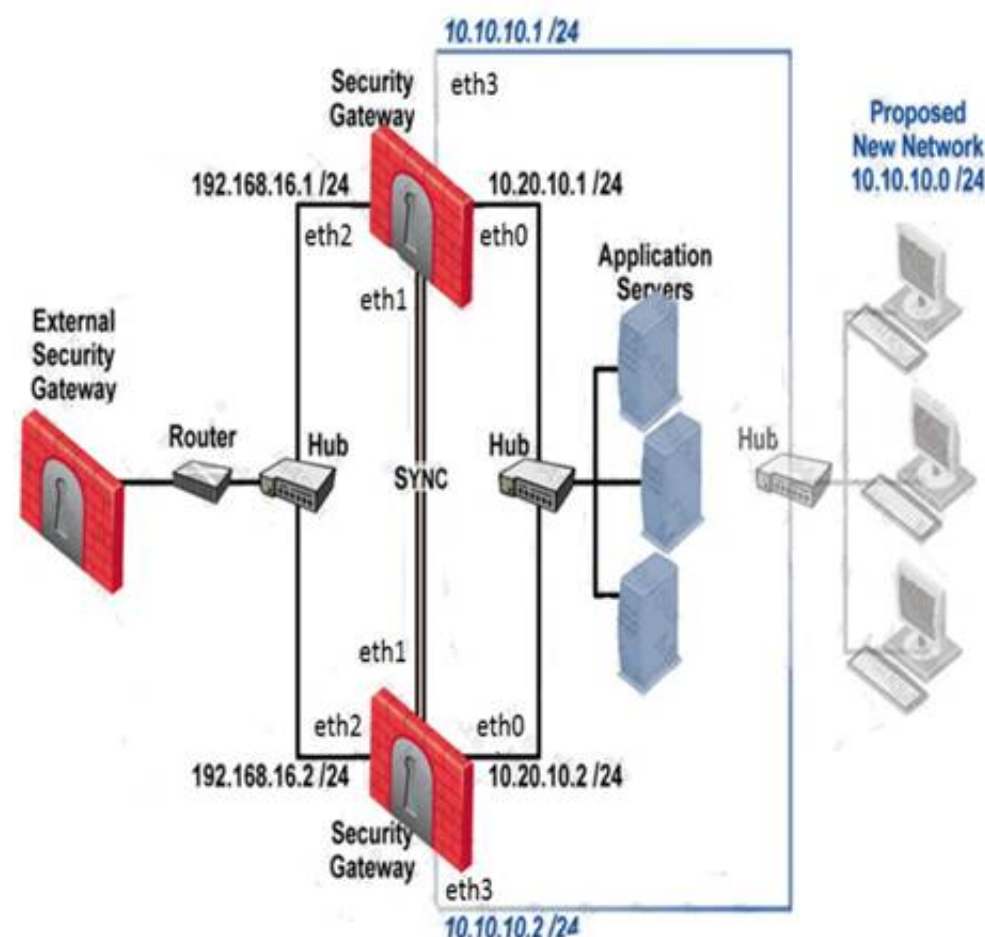
Fill in the blank. To remove site-to-site IKE and IPSEC keys you would enter command and select the option to delete all IKE and IPsec SA's.

**Answer:**

**Explanation:** vpn tu

#### NEW QUESTION 328

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 332

Fill in the blank. To save your OSPF configuration in GAiA, enter the command .

**Answer:**

**Explanation:** save config

#### NEW QUESTION 337

To stop acceleration on a GAiA Security Gateway, enter command:

**Answer:**

**Explanation:** fwaccel off

#### NEW QUESTION 338

Which statements about Management HA are correct?

- 1) Primary SmartCenter describes first installed SmartCenter
- 2) Active SmartCenter is always used to administrate with SmartConsole
- 3) Active SmartCenter describes first installed SmartCenter
- 4) Primary SmartCenter is always used to administrate with SmartConsole

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

**Answer:** C

#### NEW QUESTION 342

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

- A. test\_ldap  
B. test\_ad\_connectivity  
C. test\_ldap\_connectivity  
D. test\_ad

**Answer:** B

#### NEW QUESTION 343

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 344

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 347

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

**Answer:**

**Explanation:** fwaccel stat

#### NEW QUESTION 350

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 353

Which command will only show the number of entries in the connection table?

- A. fw tab -t connections -s  
B. fw tab -t connections -u  
C. fw tab -t connections  
D. fw tab

**Answer:** A

#### NEW QUESTION 355

Which command will erase all CRL's?

- A. vpn crladmin
- B. cpstop/cpstart
- C. vpn crl\_zap
- D. vpn flush

**Answer:** C

#### NEW QUESTION 358

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 360

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 362

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 364

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 368

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 372

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 376

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 379

To provide full connectivity upgrade status, use command

**Answer:**

**Explanation:** cphaprob fcustat

#### NEW QUESTION 384

In a zero downtime scenario, which command do you run manually after all cluster members are upgraded? Answer:  
cphaconf set\_ccp multicast

**Answer:**

#### NEW QUESTION 386

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 389

Fill in the blanks. To view the number of concurrent connections going through core 0 on the firewall, you would use the command and syntax \_\_\_\_\_

**Answer:**

**Explanation:** fw -i 0 tab -t connections -s

#### NEW QUESTION 390

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 391

Type the command and syntax that you would use to view the virtual cluster interfaces of a ClusterXL environment.

**Answer:**

**Explanation:** cphaprob -a if

#### NEW QUESTION 393

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



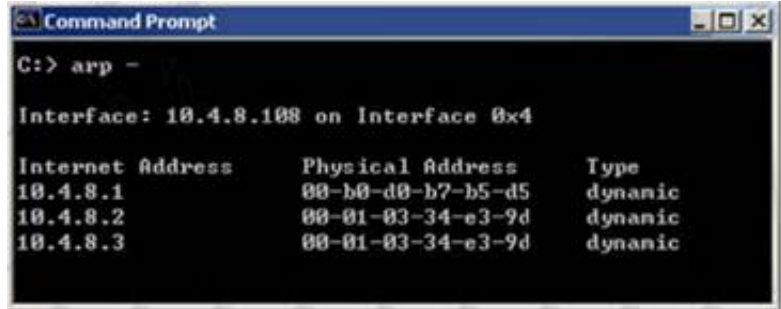
is the most likely reason?

- 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 packets are captured.
- D. Acceleration was turned on and therefore fw monitor sees only SYN.

**Answer:** D

#### NEW QUESTION 395

Fill in the blank.



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 396

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 400

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 403

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 405

MegaCorp is using SmartCenter Server with several gateways. Their requirements result in a heavy log load. Would it be feasible to add the SmartEvent Correlation Unit and SmartEvent Server to their SmartCenter Server?

- A. N
- B. SmartCenter SIC will interfere with the function of SmartEvent.
- C. N
- D. If SmartCenter is already under stress, the use of a separate server for SmartEvent is recommended.
- E. No, SmartEvent and Smartcenter cannot be installed on the same machine at the same time.
- F. Ye
- G. SmartEvent must be installed on your SmartCenter Server.

**Answer:** B

#### NEW QUESTION 409

The command useful for debugging by capturing packet information, including verifying LDAP authentication on all Check Point platforms is



**Answer:**

**Explanation:** fw monitor

#### NEW QUESTION 411

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 414

SmartReporter reports can be used to analyze data from a penetration-testing regimen in all of the following examples, EXCEPT:

- A. Analyzing traffic patterns against public resources.
- B. Possible worm/malware activity.
- C. Analyzing access attempts via social-engineering.
- D. Tracking attempted port scans.

**Answer:** C

#### NEW QUESTION 417

Fill in the blank. The user wants to replace a failed Windows-based firewall with a new server running GAIa. For the most complete restore of an GAIa configuration, he or she will use the command

**Answer:**

**Explanation:** migrate\_import

#### NEW QUESTION 422

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 425

When migrating the SmartEvent data base from one server to another, the last step is to save the files on the new server. Which of the following commands should you run to save the SmartEvent data base files on the new server?

- A. cp
- B. restore
- C. migrate import
- D. eva\_db\_restore

**Answer:** D

#### NEW QUESTION 429

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 431

You have three Gateways in a mesh community. Each gateway's VPN Domain is their internal network as defined on the Topology tab setting All IP Addresses behind Gateway based on Topology information.

You want to test the route-based VPN, so you created VTIs among the Gateways and created static route entries for the VTIs. However, when you test the VPN,

you find out the VPN still go through the regular domain IPsec tunnels instead of the routed VTI tunnels.  
What is the problem and how do you make the VPN use the VTI tunnels?

- A. Domain VPN takes precedence over the route-based VT
- B. To make the VPN go through VTI, remove the Gateways out of the mesh community and replace with a star community
- C. Domain VPN takes precedence over the route-based VT
- D. To make the VPN go through VTI, use an empty group object as each Gateway's VPN Domain
- E. Route-based VTI takes precedence over the Domain VP
- F. To make the VPN go through VTI, use dynamic-routing protocol like OSPF or BGP to route the VTI address to the peer instead of static routes
- G. Route-based VTI takes precedence over the Domain VP
- H. Troubleshoot the static route entries to insure that they are correctly pointing to the VTI gateway IP.

**Answer:** B

#### NEW QUESTION 434

Write the full fw command and syntax that you would use to troubleshoot ClusterXL sync issues.

**Answer:**

**Explanation:** fw tab -s -t connections

#### NEW QUESTION 438

Type the command and syntax you would use to verify that your Check Point cluster is functioning correctly. Answer:  
cphaprob state

**Answer:**

#### NEW QUESTION 443

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 448

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

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

**Answer:** B

#### NEW QUESTION 452

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 453

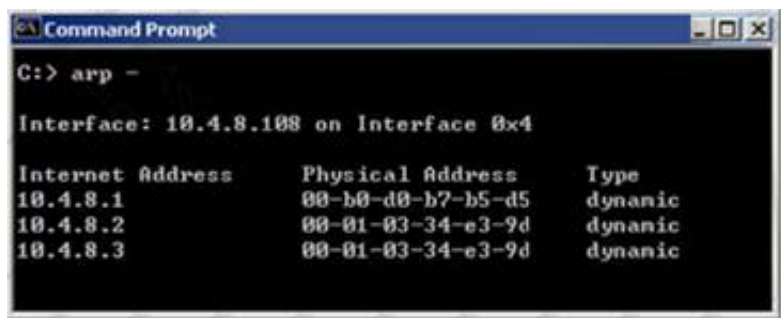
Which CLI tool helps on verifying proper ClusterXL sync?

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

**Answer:** C

#### NEW QUESTION 457

Fill in the blank.



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 460

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 463

Fill in the blank. To verify that a VPN Tunnel is properly established, use the command \_\_\_\_\_

**Answer:**

**Explanation:** vpn tunnelutil

#### NEW QUESTION 465

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 470

Which of the following is the preferred method for adding static routes in GAIa?

- A. In the CLI with the command "route add"
- B. In Web Portal, under Network Management > IPv4 Static Routes
- C. In the CLI via sysconfig
- D. In SmartDashboard under Gateway Properties > Topology

**Answer:** B

#### NEW QUESTION 471

Which is the lowest Gateway version manageable by SmartCenter R80?

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

**Answer:** A

#### NEW QUESTION 473

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 474

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

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

**Answer:** C

#### NEW QUESTION 477

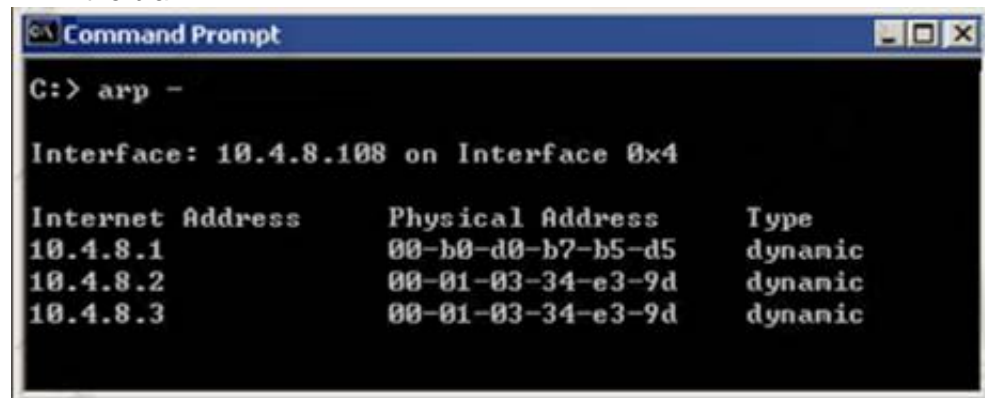
Can you implement a complete IPv6 deployment without IPv4 addresses?

- A. N
- B. SmartCenter cannot be accessed from everywhere on the Internet.
- C. Ye
- D. Only one TCP stack (IPv6 or IPv4) can be used at the same time.
- E. Yes, There is no requirement for managing IPv4 addresses.
- F. N
- G. IPv4 addresses are required for management.

**Answer:** C

#### NEW QUESTION 480

Fill in the blank.



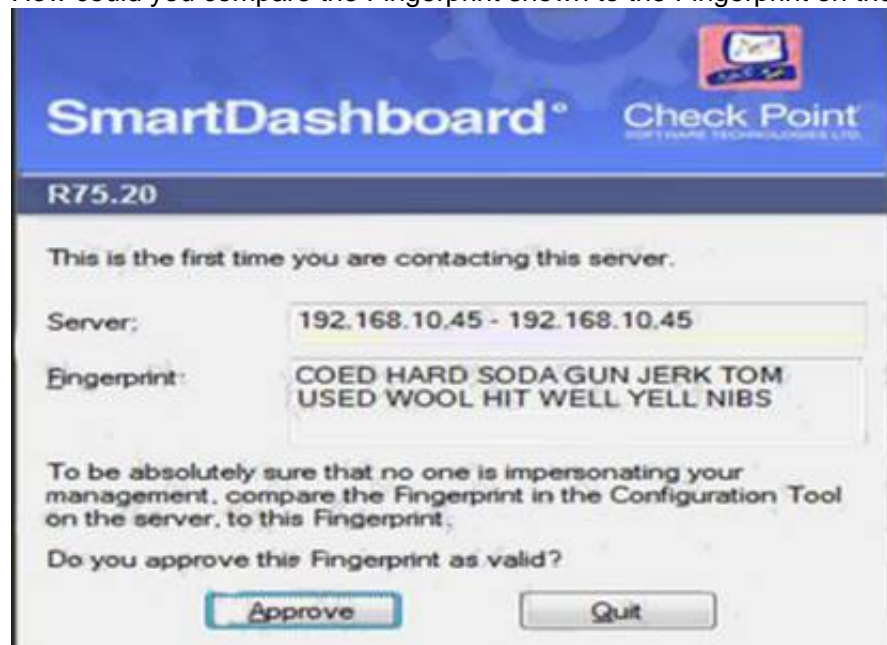
In Load Sharing Unicast mode, the internal cluster IP address is 10.4.8.3. The internal interfaces on two members are 10.4.8.1 and 10.4.8.2. Internal host 10.4.8.108 Pings 10.4.8.3, and receives replies. The following is the ARP table from the internal Windows host 10.4.8.108. Review the exhibit and type the IP address of the member serving as the pivot machine in the space below.

**Answer:**

**Explanation:** 10.4.8.2

#### NEW QUESTION 483

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



- 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 486

MultiCorp is running Smartcenter R71 on an IPSO platform and wants to upgrade to a new Appliance with R80. Which migration tool is recommended?

- A. Download Migration Tool R80 for IPSO and Splat/Linux from Check Point website.
- B. Use already installed Migration Tool.
- C. Use Migration Tool from CD/ISO
- D. Fetch Migration Tool R71 for IPSO and Migration Tool R80 for Splat/Linux from CheckPoint website

**Answer:** A

**NEW QUESTION 489**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

### 156-915.80 Practice Exam Features:

- \* 156-915.80 Questions and Answers Updated Frequently
- \* 156-915.80 Practice Questions Verified by Expert Senior Certified Staff
- \* 156-915.80 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 156-915.80 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 156-915.80 Practice Test Here](#)**