



# Check-Point

## Exam Questions 156-215.80

Check Point Certified Security Administrator

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

- (Exam Topic 1)

Which of the following are types of VPN communicates?

- A. Pentagon, star, and combination
- B. Star, octagon, and combination
- C. Combined and star
- D. Meshed, star, and combination

**Answer:** D

#### NEW QUESTION 2

- (Exam Topic 1)

Which utility allows you to configure the DHCP service on GAIA from the command line?

- A. ifconfig
- B. dhcp\_cfg
- C. sysconfig
- D. cpconfig

**Answer:** C

#### Explanation:

Sysconfig Configuration Options

#### NEW QUESTION 3

- (Exam Topic 1)

Which product correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

- A. SmartView Monitor
- B. SmartEvent
- C. SmartUpdate
- D. SmartDashboard

**Answer:** B

#### Explanation:

SmartEvent correlates logs from all Check Point enforcement points, including end-points, to identify suspicious activity from the clutter. Rapid data analysis and custom event logs immediately alert administrators to anomalous behavior such as someone attempting to use the same credential in multiple geographies simultaneously.

#### NEW QUESTION 4

- (Exam Topic 1)

Which of the following statements is TRUE about R80 management plug-ins?

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

**Answer:** C

#### NEW QUESTION 5

- (Exam Topic 1)

Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

- A. Auditor
- B. Read Only All
- C. Super User
- D. Full Access

**Answer:** B

**Explanation:**

To create a new permission profile:

In SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.

Click New Profile.

The New Profile window opens.

Enter a unique name for the profile.

Select a profile type:

Read/Write All - Administrators can make changes

Auditor (Read Only All) - Administrators can see information but cannot make changes

Customized - Configure custom settings

Click OK.

**NEW QUESTION 6**

- (Exam Topic 1)

Which of the following is NOT a SecureXL traffic flow?

- A. Medium Path
- B. Accelerated Path
- C. Fast Path
- D. Slow Path

**Answer: C**

**Explanation:**

SecureXL is an acceleration solution that maximizes performance of the Firewall and does not compromise security. When SecureXL is enabled on a Security Gateway, some CPU intensive operations are processed by virtualized software instead of the Firewall kernel. The Firewall can inspect and process connections more efficiently and accelerate throughput and connection rates. These are the SecureXL traffic flows:

Slow path - Packets and connections that are inspected by the Firewall and are not processed by SecureXL. Accelerated path - Packets and connections that are offloaded to SecureXL and are not processed by the Firewall.

Medium path - Packets that require deeper inspection cannot use the accelerated path. It is not necessary for the Firewall to inspect these packets, they can be offloaded and do not use the slow path. For example, packets that are inspected by IPS cannot use the accelerated path and can be offloaded to the IPS PSL (Passive Streaming Library). SecureXL processes these packets more quickly than packets on the slow path.

**NEW QUESTION 7**

- (Exam Topic 1)

By default, which port does the WebUI listen on?

- A. 80
- B. 4434
- C. 443
- D. 8080

**Answer: C**

**Explanation:**

To configure Security Management Server on Gaia:

Open a browser to the WebUI: <https://Gaia management IP address>

**NEW QUESTION 8**

- (Exam Topic 1)

Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

- A. UserCheck
- B. Active Directory Query
- C. Account Unit Query
- D. User Directory Query

**Answer: B**

**Explanation:**

AD Query extracts user and computer identity information from the Active Directory Security Event Logs. The system generates a Security Event log entry when a user or computer accesses a network resource. For example, this occurs when a user logs in, unlocks a screen, or accesses a network drive.

Reference : [https://sc1.checkpoint.com/documents/R76/CP\\_R76\\_IdentityAwareness\\_AdminGuide/62402.htm](https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm)

**NEW QUESTION 9**

- (Exam Topic 1)

The Gaia operating system supports which routing protocols?

- A. BGP, OSPF, RIP
- B. BGP, OSPF, EIGRP, PIM, IGMP
- C. BGP, OSPF, RIP, PIM, IGMP
- D. BGP, OSPF, RIP, EIGRP

**Answer: A**

**Explanation:**

The Advanced Routing Suite

The Advanced Routing Suite CLI is available as part of the Advanced Networking Software Blade.

For organizations looking to implement scalable, fault-tolerant, secure networks, the Advanced Networking blade enables them to run industry-standard dynamic routing protocols including BGP, OSPF, RIPv1, and RIPv2 on security gateways. OSPF, RIPv1, and RIPv2 enable dynamic routing over a single autonomous system—like a single department, company, or service provider—to avoid network failures. BGP provides dynamic routing support across more complex networks involving multiple autonomous systems—such as when a company uses two service providers or divides a network into multiple areas with different administrators responsible for the performance of each.

#### NEW QUESTION 10

- (Exam Topic 1)

Which default user has full read/write access?

- A. Monitor
- B. Altuser
- C. Administrator
- D. Superuser

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 1)

Which command is used to add users to or from existing roles?

- A. Add rba user <User Name> roles <List>
- B. Add rba user <User Name>
- C. Add user <User Name> roles <List>
- D. Add user <User Name>

**Answer:** A

#### Explanation:

Configuring Roles - CLI (rba)

#### NEW QUESTION 12

- (Exam Topic 1)

Kofi, the administrator of the ABC Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?

- A. set web ssl-port <new port number>
- B. set Gaia-portal <new port number>
- C. set Gaia-portal https-port <new port number>
- D. set web https-port <new port number>

**Answer:** A

**Explanation:**

In Clish

Connect to command line on Security Gateway / each

Log in to Clish.

Set the desired port (e.g., port 4434):

Cluster member.

HostName> set web ssl-port <Port\_Number>

Save the changes:

HostName> save config

Verify that the configuration was saved:

[Expert@HostName]# grep 'httpd:ssl\_port' /config/db/initial References:

**NEW QUESTION 13**

- (Exam Topic 1)

When you upload a package or license to the appropriate repository in SmartUpdate, where is the package or license stored

- A. Security Gateway
- B. Check Point user center
- C. Security Management Server
- D. SmartConsole installed device

**Answer:** C

**Explanation:**

SmartUpdate installs two repositories on the Security Management server:

License & Contract Repository, which is stored on all platforms in the directory \$FWDIR\conf\.

Package Repository, which is stored:

on Windows machines in C:\SUroot.

on UNIX machines in /var/suroot.

The Package Repository requires a separate license, in addition to the license for the Security Management server. This license should stipulate the number of nodes that can be managed in the Package Repository.

**NEW QUESTION 15**

- (Exam Topic 1)

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 object 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 17**

- (Exam Topic 1)

What is the default shell for the command line interface?

- A. Expert
- B. Clish
- C. Admin
- D. Normal

**Answer:** B

**Explanation:**

The default shell of the CLI is called clish References:

**NEW QUESTION 21**

- (Exam Topic 1)

Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using \_\_\_\_ .

- A. User Directory
- B. Captive Portal and Transparent Kerberos Authentication
- C. Captive Portal
- D. UserCheck

**Answer:** B

**Explanation:**

To enable Identity Awareness:

Log in to SmartDashboard.

From the Network Objects tree, expand the Check Point branch.

Double-click the Security Gateway on which to enable Identity Awareness.

In the Software Blades section, select Identity Awareness on the Network Security tab.

The Identity Awareness

Configuration wizard opens.

Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.

AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers

Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.

#### NEW QUESTION 24

- (Exam Topic 1)

What will be the effect of running the following command on the Security Management Server?

- A. Remove the installed Security Policy.
- B. Remove the local ACL lists.
- C. No effect.
- D. Reset SIC on all gateways.

**Answer:** A

#### Explanation:

This command uninstall actual security policy (already installed) References:

#### NEW QUESTION 25

- (Exam Topic 1)

Review the following screenshot and select the BEST answer.

- A. Data Center Layer is an inline layer in the Access Control Policy.
- B. By default all layers are shared with all policies.
- C. If a connection is dropped in Network Layer, it will not be matched against the rules in Data Center Layer.
- D. If a connection is accepted in Network-layer, it will not be matched against the rules in Data Center Layer.

**Answer:** C

#### NEW QUESTION 27

- (Exam Topic 1)

Joey wants to configure NTP on R80 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

- A. `https://<Device_IP_Address>`
- B. `https://<Device_IP_Address>:443`
- C. `https://<Device_IP_Address>:10000`
- D. `https://<Device_IP_Address>:4434`

**Answer:** A

#### Explanation:

Access to Web UI Gaia administration interface, initiate a connection from a browser to the default administration IP address: Logging in to the WebUI

Logging in

To log in to the WebUI:

Enter this URL in your browser: `https://<Gaia IP address>`

Enter your user name and password. References:

#### NEW QUESTION 31

- (Exam Topic 1)

Choose the Best place to find a Security Management Server backup file named backup\_fw, on a Check Point Appliance.

- A. `/var/log/Cpbackup/backups/backup/backup_fw.tgs`
- B. `/var/log/Cpbackup/backups/backup/backup_fw.tar`

- C. /var/log/Cpbackup/backups/backups/backup\_fw.tar
- D. /var/log/Cpbackup/backups/backups/backup\_fw.tgz

**Answer:** D

**Explanation:**

Gaia's Backup feature allows backing up the configuration of the Gaia OS and of the Security Management server database, or restoring a previously saved configuration. The configuration is saved to a .tgz file in the following directory:

Gaia OS Version Hardware  
Local Directory R75.40 - R77.20  
Check Point appliances  
/var/log/CPbackup/backups/ Open Server  
/var/CPbackup/backups/ R77.30  
Check Point appliances  
/var/log/CPbackup/backups/ Open Server

**NEW QUESTION 36**

- (Exam Topic 1)

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

- A. To satellites through center only
- B. To center only
- C. To center and to other satellites through center
- D. To center, or through the center to other satellites, to internet and other VPN targets

**Answer:** D

**Explanation:**

On the VPN Routing page, enable the VPN routing for satellites section, by selecting one of these options:

To center and to other Satellites through center; this allows connectivity between Gateways; for example, if the spoke Gateways are DAIP Gateways, and the hub is a Gateway with a static IP address

To center, or through the center to other satellites, to Internet and other VPN targets; this allows connectivity between the Gateways, as well as the ability to inspect all communication passing through the hub to the Internet.

**NEW QUESTION 39**

- (Exam Topic 1)

Fill in the blank: The \_\_\_\_\_ is used to obtain identification and security information about network users.

- A. User Directory
- B. User server
- C. UserCheck
- D. User index

**Answer:** A

**NEW QUESTION 43**

- (Exam Topic 1)

Fill in the blank: Gaia can be configured using the \_\_\_\_\_ or \_\_\_\_\_.

- A. Gaia; command line interface
- B. WebUI; Gaia Interface
- C. Command line interface; WebUI
- D. Gaia Interface; GaiaUI

**Answer:** C

**Explanation:**

Configuring Gaia for the First Time In This Section:

Running the First Time Configuration Wizard in WebUI Running the First Time Configuration Wizard in CLI

After you install Gaia for the first time, use the First Time Configuration Wizard to configure the system and the Check Point products on it.

**NEW QUESTION 45**

- (Exam Topic 1)

Fill in the blank: The command \_\_\_\_\_ provides the most complete restoration of a R80 configuration.

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

**Answer:** A

**Explanation:**

(Should be "migrate import")

"migrate import" Restores backed up configuration for R80 version, in previous versions the command was " upgrade\_import ".

**NEW QUESTION 49**



- (Exam Topic 1)

In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server (Security Management Server)?

- A. Display policies and logs on the administrator's workstation.
- B. Verify and compile Security Policies.
- C. Processing and sending alerts such as SNMP traps and email notifications.
- D. Store firewall logs to hard drive storage.

**Answer:** A

#### NEW QUESTION 50

- (Exam Topic 1)

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 52

- (Exam Topic 1)

Fill in the blank: A \_\_\_\_ VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.

- A. Clientless remote access
- B. Clientless direct access
- C. Client-based remote access
- D. Direct access

**Answer:** A

#### Explanation:

Clientless - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.

#### NEW QUESTION 53

- (Exam Topic 1)

Packages and licenses are loaded from all of these sources EXCEPT

- A. Download Center Web site
- B. UserUpdate
- C. User Center
- D. Check Point DVD

**Answer:** B

#### Explanation:

the Download Center web site (packages)

the Check Point DVD (packages)

the User Center (licenses)

by importing a file (packages and licenses)

by running the cplic command line

Packages and licenses are loaded into these repositories from several sources: References:

#### NEW QUESTION 57

- (Exam Topic 1)

WeBControl Layer has been set up using the settings in the following dialogue:

Consider the following policy and select the BEST answer.

- A. Traffic that does not match any rule in the subpolicy is dropped.
- B. All employees can access only Youtube and Vimeo.
- C. Access to Youtube and Vimeo is allowed only once a day.
- D. Anyone from internal network can access the internet, except the traffic defined in drop rules 5.2, 5.5 and 5.6.

**Answer:** D

**Explanation:**

Policy Layers and Sub-Policies

R80 introduces the concept of layers and sub-policies, allowing you to segment your policy according to your network segments or business units/functions. In addition, you can also assign granular privileges by layer or sub-policy to distribute workload and tasks to the most qualified administrators

With layers, the rule base is organized into a set of security rules. These set of rules or layers, are inspected in the order in which they are defined, allowing control over the rule base flow and the security functionalities that take precedence. If an “accept” action is performed across a layer, the inspection will continue to the next layer. For example, a compliance layer can be created to overlay across a cross-section of rules.

Sub-policies are sets of rules that are created for a specific network segment, branch office or business unit, so if a rule is matched, inspection will continue through this subset of rules before it moves on to the next rule.

Sub-policies and layers can be managed by specific administrators, according to their permissions profiles. This facilitates task delegation and workload distribution.

**NEW QUESTION 59**

- (Exam Topic 1)

Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

- A. Central
- B. Corporate
- C. Formal
- D. Local

**Answer:** D

**NEW QUESTION 60**

- (Exam Topic 1)

When attempting to start a VPN tunnel, in the logs the error 'no proposal chosen' is seen numerous times. No other VPN-related log entries are present. Which phase of the VPN negotiations has failed?

- A. IKE Phase 1
- B. IPSEC Phase 2
- C. IPSEC Phase 1
- D. IKE Phase 2

**Answer:** D

**NEW QUESTION 61**

- (Exam Topic 1)

Fill in the blank: The \_\_\_\_ collects logs and sends them to the \_\_\_\_.

- A. Log server; security management server
- B. Log server; Security Gateway
- C. Security management server; Security Gateway
- D. Security Gateways; log server

**Answer:** D

**NEW QUESTION 62**

- (Exam Topic 1)

Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when \_\_\_\_.

- A. The license is attached to the wrong Security Gateway
- B. The existing license expires
- C. The license is upgraded
- D. The IP address of the Security Management or Security Gateway has changed

**Answer:** A

**Explanation:**

There is no need to generate new license in this situation, just need to detach license from wrong Security Gateway and attach it to the right one.

**NEW QUESTION 66**

- (Exam Topic 1)

With which command can you view the running configuration of Gaia-based system.

- A. show conf-active
- B. show configuration active
- C. show configuration
- D. show running-configuration

**Answer:** C

#### NEW QUESTION 68

- (Exam Topic 1)

Fill in the blank: Each cluster has \_\_\_\_\_ interfaces.

- A. Five
- B. Two
- C. Three
- D. Four

**Answer:** C

#### Explanation:

Each cluster member has three interfaces: one external interface, one internal interface, and one for synchronization. Cluster member interfaces facing in each direction are connected via a switch, router, or VLAN switch.

#### NEW QUESTION 70

- (Exam Topic 1)

Harriet wants to protect sensitive information from intentional loss when users browse to a specific URL: <https://personal.mymail.com>, which blade will she enable to achieve her goal?

- A. DLP
- B. SSL Inspection
- C. Application Control
- D. URL Filtering

**Answer:** A

#### Explanation:

Check Point revolutionizes DLP by combining technology and processes to move businesses from passive detection to active Data Loss Prevention. Innovative MultiSpect™ data classification combines user, content and process information to make accurate decisions, while UserCheck™ technology empowers users to remediate incidents in real time. Check Point's self-educating network-based DLP solution frees IT/security personnel from incident handling and educates users on proper data handling policies—protecting sensitive corporate information from both intentional and unintentional loss.

#### NEW QUESTION 73

- (Exam Topic 1)

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

#### Explanation:

Suspicious Activity Rules Solution

Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).

The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation

#### NEW QUESTION 75

- (Exam Topic 1)

What is the default time length that Hit Count Data is kept?

- A. 3 month
- B. 4 weeks
- C. 12 months
- D. 6 months

**Answer:** A

#### Explanation:

Keep Hit Count data up to - Select one of the time range options. The default is 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.

#### NEW QUESTION 78

- (Exam Topic 1)

Examine the following Rule Base.

What can we infer about the recent changes made to the Rule Base?

- A. Rule 7 was created by the 'admin' administrator in the current session
- B. 8 changes have been made by administrators since the last policy installation
- C. The rules 1, 5 and 6 cannot be edited by the 'admin' administrator
- D. Rule 1 and object webserver are locked by another administrator

**Answer:**

D

**Explanation:**

On top of the print screen there is a number "8" which consists for the number of changes made and not saved. Session Management Toolbar (top of SmartConsole)

**NEW QUESTION 82**

- (Exam Topic 1)

Which Threat Prevention Software Blade provides comprehensive against malicious and unwanted network traffic, focusing on application and server vulnerabilities?

- A. Anti-Virus
- B. IPS
- C. Anti-Spam
- D. Anti-bot

**Answer:** B

**Explanation:**

The IPS Software Blade provides a complete Intrusion Prevention System security solution, providing comprehensive network protection against malicious and unwanted network traffic, including:

Malware attacks

Dos and DDoS attacks

Application and server vulnerabilities

Insider threats

Unwanted application traffic, including IM and P2P

**NEW QUESTION 83**

- (Exam Topic 1)

Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below.

Where can the administrator check for more information on these errors?

- A. The Log and Monitor section in SmartConsole
- B. The Validations section in SmartConsole
- C. The Objects section in SmartConsole
- D. The Policies section in SmartConsole

**Answer:** B

**Explanation:**

Validation Errors

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.

To publish, you must fix the errors.

**NEW QUESTION 84**

- (Exam Topic 2)

Mesh and Star are two types of VPN topologies. Which statement below is TRUE about these types of communities?

- A. A star community requires Check Point gateways, as it is a Check Point proprietary technology.
- B. In a star community, satellite gateways cannot communicate with each other.
- C. In a mesh community, member gateways cannot communicate directly with each other.
- D. In a mesh community, all members can create a tunnel with any other member.

**Answer:** D

**NEW QUESTION 85**

- (Exam Topic 2)

Provide very wide coverage for all products and protocols, with noticeable performance impact.

How could you tune the profile in order to lower the CPU load still maintaining security at good level? Select the BEST answer.

- A. Set High Confidence to Low and Low Confidence to Inactive.
- B. Set the Performance Impact to Medium or lower.
- C. The problem is not with the Threat Prevention Profil
- D. Consider adding more memory to the appliance.
- E. Set the Performance Impact to Very Low Confidence to Prevent.

**Answer:** B

**NEW QUESTION 87**

- (Exam Topic 2)

You want to reset SIC between smberlin and sgosaka.

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

What is the reason for this behavior?

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

**Answer:** C

**NEW QUESTION 91**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 96**

- (Exam Topic 2)

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 100**

- (Exam Topic 2)

Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is \_\_\_\_ all traffic. However, in the Application Control policy layer, the default action is \_\_\_\_\_ all traffic.

- A. Accept; redirect

- B. Accept; drop
- C. Redirect; drop
- D. Drop; accept

**Answer:** D

#### NEW QUESTION 105

- (Exam Topic 2)

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

- A. RADIUS
- B. Remote Access and RADIUS
- C. AD Query
- D. AD Query and Browser-based Authentication

**Answer:** D

#### Explanation:

Identity Awareness gets identities from these acquisition sources:

AD Query  
Browser-Based Authentication  
Endpoint Identity Agent  
Terminal Servers Identity Agent  
Remote Access

#### NEW QUESTION 106

- (Exam Topic 2)

Fill in the blanks: The Application Layer Firewalls inspect traffic through the \_\_\_\_ layer(s) of the TCP/IP model and up to and including the \_\_\_\_ layer.

- A. Lower; Application
- B. First two; Internet
- C. First two; Transport
- D. Upper; Application

**Answer:** A

#### NEW QUESTION 108

- (Exam Topic 2)

Why would an administrator see the message below?

- A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
- D. A new Policy Package created on the Gateway and transferred to the management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

**Answer:** B

#### NEW QUESTION 113

- (Exam Topic 2)

Which of the following is NOT an advantage to using multiple LDAP servers?

- A. You achieve a faster access time by placing LDAP servers containing the database at remote sites
- B. Information on a user is hidden, yet distributed across several servers
- C. You achieve compartmentalization by allowing a large number of users to be distributed across several servers
- D. You gain High Availability by replicating the same information on several servers

**Answer:** B

#### NEW QUESTION 115

- (Exam Topic 2)

You want to define a selected administrator's permission to edit a layer. However, when you click the + sign in the "Select additional profile that will be able edit this layer" you do not see anything. What is the most likely cause of this problem? Select the BEST answer.

- A. "Edit layers by Software Blades" is unselected in the Permission Profile
- B. There are no permission profiles available and you need to create one first.
- C. All permission profiles are in use.
- D. "Edit layers by selected profiles in a layer editor" is unselected in the Permission profile.

**Answer:** B

#### NEW QUESTION 116

- (Exam Topic 2)

In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

- A. Pentagon
- B. Combined
- C. Meshed
- D. Star

**Answer:** D

#### Explanation:

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN connections between each Security Gateway. In a Star community, satellites have a VPN connection with the center Security Gateway, but not to each other.

#### NEW QUESTION 120

- (Exam Topic 2)

What action can be performed from SmartUpdate R77?

- A. upgrade\_export
- B. fw stat -1
- C. cpinfo
- D. remote\_uninstall\_verifier

**Answer:** C

#### NEW QUESTION 121

- (Exam Topic 2)

Fill in the blanks: A Check Point software license consists of a \_\_\_\_\_ and \_\_\_\_\_.

- A. Software container; software package
- B. Software blade; software container
- C. Software package; signature
- D. Signature; software blade

**Answer:** B

#### Explanation:

Check Point's licensing is designed to be scalable and modular. To this end, Check Point offers both predefined packages as well as the ability to custom build a solution tailored to the needs of the Network Administrator. This is accomplished by the use of the following license components:

Software Blades  
Container

#### NEW QUESTION 126

- (Exam Topic 2)

MyCorp has the following NAT rules. You need to disable the NAT function when Alpha-internal networks try to reach the Google DNS (8.8.8.8) server. What can you do in this case?

- A. Use manual NAT rule to make an exception
- B. Use the NAT settings in the Global Properties
- C. Disable NAT inside the VPN community
- D. Use network exception in the Alpha-internal network object

**Answer:** D



#### NEW QUESTION 129

- (Exam Topic 2)

At what point is the Internal Certificate Authority (ICA) created?

- A. Upon creation of a certificate
- B. During the primary Security Management Server installation process.
- C. When an administrator decides to create one.
- D. When an administrator initially logs into SmartConsole.

**Answer:** B

#### Explanation:

Introduction to the ICA

The ICA is a Certificate Authority which is an integral part of the Check Point product suite. It is fully compliant with X.509 standards for both certificates and CRLs. See the relevant X.509 and PKI documentation, as well as RFC 2459 standards for more information. You can read more about Check Point and PKI in the R76 VPN Administration Guide.

The ICA is located on the Security Management server. It is created during the installation process, when the Security Management server is configured.

#### NEW QUESTION 133

- (Exam Topic 2)

Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

- A. Firewall
- B. Application Control
- C. Anti-spam and Email Security
- D. Antivirus

**Answer:** D

#### Explanation:

The enhanced Check Point Antivirus Software Blade uses real-time virus signatures and anomaly-based protections from ThreatCloud™, the first collaborative network to fight cybercrime, to detect and block malware at the gateway before users are affected.

#### NEW QUESTION 134

- (Exam Topic 2)

Office mode means that:

- A. SecureID client assigns a routable MAC address
- B. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
- C. Users authenticate with an Internet browser and use secure HTTPS connection.
- D. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
- E. Allows a security gateway to assign a remote client an IP address
- F. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

**Answer:** D

#### Explanation:

Office Mode enables a Security Gateway to assign internal IP addresses to SecureClient users. This IP address will not be exposed to the public network, but is encapsulated inside the VPN tunnel between the client and the Gateway. The IP to be used externally should be assigned to the client in the usual way by the Internet Service provider used for the Internet connection. This mode allows a Security Administrator to control which addresses are used by remote clients inside the local network and makes them part of the local network. The mechanism is based on an IKE protocol extension through which the Security Gateway can send an internal IP address to the client.

#### NEW QUESTION 139

- (Exam Topic 2)

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

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

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

**Answer:** B

#### NEW QUESTION 144

- (Exam Topic 2)

Choose the SmartLog property that is TRUE.

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



**Answer:** D

#### NEW QUESTION 147

- (Exam Topic 2)

Choose what BEST describes users on Gaia Platform.

- A. There is one default user that cannot be deleted.
- B. There are two default users and one cannot be deleted.
- C. There is one default user that can be deleted.
- D. There are two default users that cannot be deleted and one SmartConsole Administrator.

**Answer:** B

#### Explanation:

These users are created by default and cannot be deleted:

admin — Has full read/write capabilities for all Gaia features, from the WebUI and the CLI. This user has a User ID of 0, and therefore has all of the privileges of a root user.

monitor — Has read-only capabilities for all features in the WebUI and the CLI, and can change its own password. You must give a password for this user before the account can be used.

#### NEW QUESTION 151

- (Exam Topic 2)

There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW\_A and FW\_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW\_A is configured to have higher priority than FW\_B. FW\_A was active and processing the traffic in the morning. FW\_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW\_B became active. After an hour, FW\_A's interface issues were resolved and it became operational. When it re-joins the cluster, will it become active automatically?

- A. No, since "maintain current active cluster member" option on the cluster object properties is enabled by default
- B. No, since "maintain current active cluster member" option is enabled by default on the Global Properties
- C. Yes, since "Switch to higher priority cluster member" option on the cluster object properties is enabled by default
- D. Yes, since "Switch to higher priority cluster member" option is enabled by default on the Global Properties

**Answer:** A

#### Explanation:

What Happens When a Security Gateway Recovers?

In a Load Sharing configuration, when the failed Security Gateway in a cluster recovers, all connections are redistributed among all active members. High Availability and Load Sharing in ClusterXL ClusterXL Administration Guide R77 Versions | 31 In a High Availability configuration, when the failed Security Gateway in a cluster recovers, the recovery method depends on the configured cluster setting. The options are:

- Maintain Current Active Security Gateway means that if one member passes on control to a lower priority member, control will be returned to the higher priority member only if the lower priority member fails. This mode is recommended if all members are equally capable of processing traffic, in order to minimize the number of failover events.
- Switch to Higher Priority Security Gateway means that if the lower priority member has control and the higher priority member is restored, then control will be returned to the higher priority member. This mode is recommended if one member is better equipped for handling connections, so it will be the default Security Gateway.

#### NEW QUESTION 154

- (Exam Topic 2)

Which policy type is used to enforce bandwidth and traffic control rules?

- A. Threat Emulation
- B. Access Control
- C. QoS
- D. Threat Prevention

**Answer:** C

#### Explanation:

Check Point's QoS Solution

QoS is a policy-based QoS management solution from Check Point Software Technologies Ltd., satisfies your needs for a bandwidth management solution. QoS is a unique, software-only based application that manages traffic end-to-end across networks, by distributing enforcement throughout network hardware and software.

#### NEW QUESTION 159

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 160

- (Exam Topic 2)

Fill in the blank: The IPS policy for pre-R80 gateways is installed during the \_\_\_\_\_.

- A. Firewall policy install
- B. Threat Prevention policy install
- C. Anti-bot policy install
- D. Access Control policy install

**Answer:** B

**Explanation:**

[https://sc1.checkpoint.com/documents/R80/CP\\_R80BC\\_ThreatPrevention/html\\_frameset.htm?topic=documents](https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents)

**NEW QUESTION 164**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 167**

- (Exam Topic 2)

Fill in the blank: RADIUS Accounting gets \_\_\_\_\_ data from requests generated by the accounting client

- A. Destination
- B. Identity
- C. Payload
- D. Location

**Answer:** B

**Explanation:**

How RADIUS Accounting Works with Identity Awareness

RADIUS Accounting gets identity data from RADIUS Accounting Requests generated by the RADIUS accounting client.

**NEW QUESTION 171**

- (Exam Topic 2)

The Captive Portal tool:

- A. Acquires identities from unidentified users.
- B. Is only used for guest user authentication.
- C. Allows access to users already identified.
- D. Is deployed from the Identity Awareness page in the Global Properties settings.

**Answer:** A

**NEW QUESTION 175**

- (Exam Topic 2)

Where can administrator edit a list of trusted SmartConsole clients in R80?

- A. cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server.
- B. Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
- C. In cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server, in SmartConsole: Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients.
- D. WebUI client logged to Security Management Server, SmartDashboard: Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients, via cpconfig on a Security Gateway.

**Answer:** C

**NEW QUESTION 179**

- (Exam Topic 2)

Which command is used to obtain the configuration lock in Gaia?

- A. Lock database override
- B. Unlock database override
- C. Unlock database lock
- D. Lock database user

**Answer:** A

**Explanation:**

Obtaining a Configuration Lock  
lock database override

unlock database

**NEW QUESTION 181**

- (Exam Topic 2)

Message digests use which of the following?

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

**Answer:** D

**NEW QUESTION 184**

- (Exam Topic 2)

The most important part of a site-to-site VPN deployment is the \_\_\_\_.

- A. Internet
- B. Remote users
- C. Encrypted VPN tunnel
- D. VPN gateways

**Answer:** C

**Explanation:**

Site to Site VPN

The basis of Site to Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.

**NEW QUESTION 188**

- (Exam Topic 2)

Look at the following screenshot and select the BEST answer.

- A. Clients external to the Security Gateway can download archive files from FTP\_Ext server using FTP.
- B. Internal clients can upload and download any-files to FTP\_Ext-server using FTP.
- C. Internal clients can upload and download archive-files to FTP\_Ext server using FTP.
- D. Clients external to the Security Gateway can upload any files to the FTP\_Ext-server using FTP.

**Answer:** A

**NEW QUESTION 193**

- (Exam Topic 2)

Which information is included in the “Full Log” tracking option, but is not included in the “Log” tracking option?

- A. file attributes
- B. application information
- C. destination port
- D. data type information

**Answer:** D

**Explanation:**

Network Log - Generates a log with only basic Firewall information: Source, Destination, Source Port, Destination Port, and Protocol.

Log - Equivalent to the Network Log option, but also includes the application name (for example, Dropbox), and application information (for example, the URL of the Website). This is the default Tracking option.

Full Log - Equivalent to the log option, but also records data for each URL request made.

If suppression is not selected, it generates a complete log (as defined in pre-R80 management).  
If suppression is selected, it generates an extended log(as defined in pre-R80 management).  
None - Do not generate a log.

#### NEW QUESTION 197

- (Exam Topic 2)

Which authentication scheme requires a user to possess a token?

- A. TACACS
- B. SecurID
- C. Check Point password
- D. RADIUS

**Answer:** B

#### Explanation:

SecurID

SecurID requires users to both possess a token authenticator and to supply a PIN or password References:

#### NEW QUESTION 200

- (Exam Topic 2)

Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as \_\_\_\_\_

- A. UserCheck
- B. User Directory
- C. User Administration
- D. User Center

**Answer:** B

#### Explanation:

Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution. If you have a large user count, we recommend that you use an external user management database such as LDAP for enhanced Security Management Server performance.

#### NEW QUESTION 202

- (Exam Topic 2)

Which of the following licenses are considered temporary?

- A. Perpetual and Trial
- B. Plug-and-play and Evaluation
- C. Subscription and Perpetual
- D. Evaluation and Subscription

**Answer:** B

#### Explanation:

Should be Trial or Evaluation, even Plug-and-play (all are synonyms ). Answer B is the best choice.

#### NEW QUESTION 207

- (Exam Topic 2)

AdminA and AdminB are both logged in on SmartConsole. What does it mean if AdminB sees a locked icon on a rule? Choose the BEST answer.

- A. Rule is locked by AdminA, because the save bottom has not been press.
- B. Rule is locked by AdminA, because an object on that rule is been edited.
- C. Rule is locked by AdminA, and will make it available if session is published.
- D. Rule is locked by AdminA, and if the session is saved, rule will be available

**Answer:** C

#### NEW QUESTION 208

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 211

- (Exam Topic 2)

On the following picture an administrator configures Identity Awareness:

After clicking “Next” the above configuration is supported by:

- A. Kerberos SSO which will be working for Active Directory integration
- B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user
- C. Obligatory usage of Captive Portal
- D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication

**Answer: B**

**Explanation:**

To enable Identity Awareness:

Log in to R80 SmartConsole.

From the Awareness.

Gateway&s

Servers

view, double-click the Security Gateway on which to enable Identity

On the Network Security tab, select Identity Awareness.

The Identity Awareness

Configuration wizard opens.

Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.

AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers

Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.

Terminal Servers - Identify users in a Terminal Server environment (originating from one IP address).

**NEW QUESTION 212**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 215**

- (Exam Topic 2)

You are going to upgrade from R77 to R80. Before the upgrade, you want to back up the system so that, if there are any problems, you can easily restore to the old version with all configuration and management files intact. What is the BEST backup method in this scenario?

- A. backup
- B. Database Revision
- C. snapshot
- D. migrate export

**Answer: C**

**Explanation:**

2. Snapshot Management

The snapshot creates a binary image of the entire root (lv\_current) disk partition. This includes Check Point products, configuration, and operating system.

Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported.

The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be save

**NEW QUESTION 220**

- (Exam Topic 2)

Jack works for a managed service provider and he has been tasked to create 17 new policies for several new customers. He does not have much time. What is the BEST way to do this with R80 security management?

- A. Create a text-file with mgmt\_cli script that creates all objects and policie
- B. Open the file in SmartConsole Command Line to run it.
- C. Create a text-file with Gaia CLI -commands in order to create all objects and policie
- D. Run the file in CLISH with command load configuration.
- E. Create a text-file with DBEDIT script that creates all objects and policie
- F. Run the file in the command line of the management server using command dbedit -f.
- G. Use Object Explorer in SmartConsole to create the objects and Manage Policies from the menu to create the policies.

**Answer: A**

**Explanation:**

Did you know: mgmt\_cli can accept csv files as inputs using the --batch option.

The first row should contain the argument names and the rows below it should hold the values for these parameters.

So an equivalent solution to the powershell script could look like this:

data.csv:

mgmt\_cli add host --batch data.csv -u <username> -p <password> -m <management server>

This can work with any type of command not just "add host" : simply replace the column names with the ones relevant to the command you need.

**NEW QUESTION 225**



- (Exam Topic 3)

SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

- A. Threat Emulation
- B. Mobile Access
- C. Mail Transfer Agent
- D. Threat Cloud

**Answer:** C

#### NEW QUESTION 229

- (Exam Topic 3)

As you review this Security Policy, what changes could you make to accommodate Rule 4?

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

**Answer:** B

#### NEW QUESTION 233

- (Exam Topic 3)

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

#### NEW QUESTION 234

- (Exam Topic 3)

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 235

- (Exam Topic 3)

According to Check Point Best Practice, when adding a 3rd party gateway to a Check Point security solution what object SHOULD be added? A(n):

- A. Interoperable Device
- B. Network Node
- C. Externally managed gateway
- D. Gateway

**Answer:** A

#### NEW QUESTION 238

- (Exam Topic 3)

Jennifer McHanry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.

To make this scenario work, the IT administrator must:

- 1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
- 2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
- 3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action.
- 4) Install policy.

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 239

- (Exam Topic 3)

The WebUI offers three methods for downloading Hotfixes via CPUSE. One of them is Automatic method. How many times per day will CPUSE agent check for hotfixes and automatically download them?

- A. Six times per day
- B. Seven times per day
- C. Every two hours
- D. Every three hours

**Answer:** D

#### NEW QUESTION 243

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 246

- (Exam Topic 3)

A Cleanup rule:

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

**Answer:** A

#### NEW QUESTION 248

- (Exam Topic 3)

Choose the correct statement regarding Implicit Rules.

- A. To edit the Implicit rules you go to: Launch Button > Policy > Global Properties > Firewall.
- B. Implied rules are fixed rules that you cannot change.
- C. You can directly edit the Implicit rules by double-clicking on a specific Implicit rule.
- D. You can edit the Implicit rules but only if requested by Check Point support personnel.

**Answer:** A

#### NEW QUESTION 253

- (Exam Topic 3)

An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).

Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval.

If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute.

Which of the following is the BEST Explanation: for this behavior?

- A. The setting Log does not capture this level of detail for GR
- B. Set the rule tracking action to Audit since certain types of traffic can only be tracked this way.
- C. The log unification process is using a LUUID (Log Unification Unique Identification) that has become corrup
- D. Because it is encrypted, the R77 Security Gateway cannot distinguish between GRE session
- E. This is a known issue with GR
- F. Use IPSEC instead of the non-standard GRE protocol for encapsulation.
- G. The Log Server log unification process unifies all log entries from the Security Gateway on a specific connection into only one log entry in the SmartView Tracke
- H. GRE traffic has a 10 minute session timeout, thus each keep-alive packet is considered part of the original logged connection at the beginning of the day.
- I. The Log Server is failing to log GRE traffic properly because it is VPN traffi
- J. Disable all VPN configuration to the partner site to enable proper logging.

**Answer:** C

#### NEW QUESTION 254

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 258

- (Exam Topic 3)

Which rule is responsible for the user authentication failure?

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

**Answer:** C

#### NEW QUESTION 259

- (Exam Topic 3)

Which of the following are available SmartConsole clients which can be installed from the R77 Windows CD? Read all answers and select the most complete and valid list.

- A. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
- B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
- C. SmartView Tracker, CPINFO, SmartUpdate
- D. Security Policy Editor, Log Viewer, Real Time Monitor GUI

**Answer:** C

#### NEW QUESTION 261

- (Exam Topic 3)

The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

- A. There is a virus found
- B. Traffic is still allowed but not accelerated
- C. The connection required a Security server
- D. Acceleration is not enabled
- E. The traffic is originating from the gateway itself

**Answer:** D

#### NEW QUESTION 264

- (Exam Topic 3)

Which of these statements describes the Check Point ThreatCloud?

- A. Blocks or limits usage of web applications
- B. Prevents or controls access to web sites based on category
- C. Prevents Cloud vulnerability exploits
- D. A worldwide collaborative security network

**Answer:** D

#### NEW QUESTION 265

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 266

- (Exam Topic 3)

What is the difference between an event and a log?

- A. Events are generated at gateway according to Event Policy
- B. A log entry becomes an event when it matches any rule defined in Event Policy
- C. Events are collected with SmartWorkflow from Trouble Ticket systems



D. Logs and Events are synonyms

**Answer:** B

#### NEW QUESTION 267

- (Exam Topic 3)

Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

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

**Answer:** B

#### NEW QUESTION 269

- (Exam Topic 3)

Which command can you use to verify the number of active concurrent connections?

- A. fw conn all
- B. fw ctl pst pstat
- C. show all connections
- D. show connections

**Answer:** B

#### NEW QUESTION 271

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 272

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 273

- (Exam Topic 3)

Which remote Access Solution is clientless?

- A. Checkpoint Mobile
- B. Endpoint Security Suite
- C. SecuRemote
- D. Mobile Access Portal

**Answer:** D

#### NEW QUESTION 274

- (Exam Topic 3)

A digital signature:

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

**Answer:** A

#### NEW QUESTION 278

- (Exam Topic 3)

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

- A. Use dbedit to script the addition of a rule directly into the Rule Bases\_5\_0.fws configuration file.
- B. Select Block intruder from the Tools menu in SmartView Tracker.
- C. Create a Suspicious Activity Rule in Smart Monitor.
- D. Add a temporary rule using SmartDashboard and select hide rule.

**Answer: C**

#### NEW QUESTION 280

- (Exam Topic 3)

During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

- A. Dropped without sending a negative acknowledgment
- B. Dropped without logs and without sending a negative acknowledgment
- C. Dropped with negative acknowledgment
- D. Dropped with logs and without sending a negative acknowledgment

**Answer: D**

#### NEW QUESTION 285

- (Exam Topic 3)

What is Consolidation Policy?

- A. The collective name of the Security Policy, Address Translation, and IPS Policies.
- B. The specific Policy written in SmartDashboard to configure which log data is stored in the SmartReporter database.
- C. The collective name of the logs generated by SmartReporter.
- D. A global Policy used to share a common enforcement policy for multiple Security Gateways.

**Answer: B**

#### NEW QUESTION 289

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 293

- (Exam Topic 3)

Which of the following firewall modes DOES NOT allow for Identity Awareness to be deployed?

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

**Answer: A**

#### NEW QUESTION 297

- (Exam Topic 3)

While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?

- 1) Select Active Mode tab in SmartView Tracker.
- 2) Select Tools > Block Intruder.
- 3) Select Log Viewing tab in SmartView Tracker.
- 4) Set Blocking Timeout value to 60 minutes.
- 5) Highlight connection that should be blocked.

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

**Answer: C**

#### NEW QUESTION 302

- (Exam Topic 3)

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

- A. Run fwm dbexport -1 filename
- B. Restore the databas
- C. Then, run fwm dbimport -1 filename to import the users.
- D. Run fwm\_dbexport to export the user databas
- E. Select restore the entire database in the Database Revision scree
- F. Then, run fwm\_dbimport.
- G. Restore the entire database, except the user database, and then create the new user and user group.
- H. Restore the entire database, except the user database.

**Answer: D**

#### NEW QUESTION 306

- (Exam Topic 3)

Which of the following is NOT an attribute of packer acceleration?

- A. Source address
- B. Protocol
- C. Destination port
- D. Application Awareness

**Answer: D**

#### NEW QUESTION 311

- (Exam Topic 3)

MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. How do you apply the license?

- A. Using the remote Gateway's IP address, and attaching the license to the remote Gateway via SmartUpdate.
- B. Using your Security Management Server's IP address, and attaching the license to the remote Gateway via SmartUpdate.
- C. Using the remote Gateway's IP address, and applying the license locally with command cplic put.
- D. Using each of the Gateway's IP addresses, and applying the licenses on the Security Management Server with the command cprlic put.

**Answer: B**

#### NEW QUESTION 313

- (Exam Topic 3)

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 316

- (Exam Topic 3)

How do you configure an alert in SmartView Monitor?

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

**Answer: B**

#### NEW QUESTION 321

- (Exam Topic 3)

According to Check Point Best Practice, when adding a non-managed Check Point Gateway to a Check Point security solution what object SHOULD be added?  
A(n):

- A. Gateway
- B. Interoperable Device
- C. Externally managed gateway
- D. Network Node

**Answer: C**

#### NEW QUESTION 324

- (Exam Topic 3)

What port is used for communication to the User Center with SmartUpdate?

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

**Answer: D**

#### NEW QUESTION 329

- (Exam Topic 3)

Which of the following is a hash algorithm?

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

**Answer: D**

#### NEW QUESTION 332

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 337

- (Exam Topic 3)

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:(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.

**Answer: C**

#### NEW QUESTION 340

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 343

- (Exam Topic 3)

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 Prevention API and Policy Editor API
- D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

**Answer:** B

#### NEW QUESTION 344

- (Exam Topic 3)

Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?

- A. Source Address
- B. Destination Address
- C. TCP Acknowledgment Number
- D. Source Port

**Answer:** C

#### NEW QUESTION 346

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 349

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 354

- (Exam Topic 4)

Which of the following commands is used to verify license installation?

- A. Cplic verify license
- B. Cplic print
- C. Cplic show
- D. Cplic license

**Answer:** B

#### NEW QUESTION 358

- (Exam Topic 4)

Tom has connected to the R80 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made:

- A. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of this work.
- B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
- C. Tom's changes will be lost since he lost connectivity and he will have to start again.
- D. Tom will have to reboot his SmartConsole computer, clear the cache and restore changes.

**Answer:** A

#### NEW QUESTION 362

- (Exam Topic 4)

What is the BEST method to deploy identity Awareness for roaming users?

- A. Use Office Mode
- B. Use identity agents
- C. Share user identities between gateways
- D. Use captive portal

**Answer:** A

#### NEW QUESTION 366

- (Exam Topic 4)

Which one of the following is TRUE?

- A. Ordered policy is a sub-policy within another policy
- B. One policy can be either inline or ordered, but not both
- C. Inline layer can be defined as a rule action
- D. Pre-R80 Gateways do not support ordered layers

**Answer: C**

#### NEW QUESTION 367

- (Exam Topic 4)

Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic?

- A. Slow Path
- B. Medium Path
- C. Fast Path
- D. Accelerated Path

**Answer: A**

#### NEW QUESTION 369

- (Exam Topic 4)

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: A**

#### NEW QUESTION 373

- (Exam Topic 4)

Which identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

- A. ADQuery
- B. Terminal Servers Endpoint Identity Agent
- C. Endpoint Identity Agent and Browser-Based Authentication
- D. RADIUS and Account Logon

**Answer: D**

#### NEW QUESTION 375

- (Exam Topic 4)

From SecureXL perspective, what are the tree paths of traffic flow:

- A. Initial Path; Medium Path; Accelerated Path
- B. Layer Path; Blade Path; Rule Path
- C. Firewall Path; Accept Path; Drop Path
- D. Firewall Path; Accelerated Path; Medium Path

**Answer: D**

#### NEW QUESTION 377

- (Exam Topic 4)

The \_\_\_\_\_ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

- A. Next Generation Threat Prevention
- B. Next Generation Threat Emulation
- C. Next Generation Threat Extraction
- D. Next Generation Firewall

**Answer: B**

#### NEW QUESTION 382

- (Exam Topic 4)

When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

- A. Security Management Server's /home/.fgpt file and is available for future SmartConsole authentications.
- B. Windows registry is available for future Security Management Server authentications.
- C. there is no memory used for saving a fingerprint anyway.
- D. SmartConsole cache is available for future Security Management Server authentications.

**Answer: D**



**NEW QUESTION 385**

- (Exam Topic 4)

Fill in the blank: Authentication rules are defined for \_\_\_\_ .

- A. User groups
- B. Users using UserCheck
- C. Individual users
- D. All users in the database

**Answer:** A

**NEW QUESTION 386**

- (Exam Topic 4)

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:** B

**NEW QUESTION 387**

- (Exam Topic 4)

Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

What is the possible Explanation: for this?

- A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.
- B. Another administrator is logged into the Management and currently editing the DNS Rule.
- C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.
- D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

**Answer:** B

**NEW QUESTION 392**

- (Exam Topic 4)

Which message indicates IKE Phase 2 has completed successfully?

- A. Quick Mode Complete
- B. Aggressive Mode Complete
- C. Main Mode Complete
- D. IKE Mode Complete

**Answer:** A

**NEW QUESTION 397**

- (Exam Topic 4)

If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

- A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
- B. Change the Standby Security Management Server to Active.
- C. Change the Active Security Management Server to Standby.
- D. Manually synchronize the Active and Standby Security Management Servers.

**Answer:** A

**NEW QUESTION 400**

- (Exam Topic 4)

In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

- A. SND is a feature to accelerate multiple SSL VPN connections
- B. SND is an alternative to IPSec Main Mode, using only 3 packets
- C. SND is used to distribute packets among Firewall instances
- D. SND is a feature of fw monitor to capture accelerated packets

**Answer:** C

**NEW QUESTION 401**

- (Exam Topic 4)

Fill in the blank: In Security Gateways R75 and above, SIC uses \_\_\_\_ for encryption.

- A. AES-128
- B. AES-256

- C. DES
- D. 3DES

**Answer:** A

#### NEW QUESTION 403

- (Exam Topic 4)

What Identity Agent allows packet tagging and computer authentication?

- A. Endpoint Security Client
- B. Full Agent
- C. Light Agent
- D. System Agent

**Answer:** B

#### NEW QUESTION 408

- (Exam Topic 4)

Can multiple administrators connect to a Security Management Server at the same time?

- A. No, only one can be connected
- B. Yes, all administrators can modify a network object at the same time
- C. Yes, every administrator has their own username, and works in a session that is independent of other administrators
- D. Yes, but only one has the right to write

**Answer:** C

#### NEW QUESTION 411

- (Exam Topic 4)

What is the Transport layer of the TCP/IP model responsible for?

- A. It transports packets as datagrams along different routes to reach their destination.
- B. It manages the flow of data between two hosts to ensure that the packets are correctly assembled and delivered to the target application.
- C. It defines the protocols that are used to exchange data between networks and how host programs interact with the Application layer.
- D. It deals with all aspects of the physical components of network connectivity and connects with different network types.

**Answer:** B

#### NEW QUESTION 414

- (Exam Topic 4)

Using ClusterXL, what statement is true about the Sticky Decision Function?

- A. Can only be changed for Load Sharing implementations
- B. All connections are processed and synchronized by the pivot
- C. Is configured using cpconfig
- D. Is only relevant when using SecureXL

**Answer:** A

#### NEW QUESTION 415

- (Exam Topic 4)

What is the purpose of the Clean-up Rule?

- A. To log all traffic that is not explicitly allowed or denied in the Rule Base.
- B. To clean up policies found inconsistent with the compliance blade reports.
- C. To remove all rules that could have a conflict with other rules in the database.
- D. To eliminate duplicate log entries in the Security Gateway

**Answer:** A

#### NEW QUESTION 419

- (Exam Topic 4)

Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the \_\_\_\_\_ algorithm.

- A. SHA-256
- B. SHA-200
- C. MD5
- D. SHA-128

**Answer:** A

#### NEW QUESTION 420

- (Exam Topic 4)

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

#### NEW QUESTION 422

- (Exam Topic 4)

What two ordered layers make up the Access Control Policy Layer?

- A. URL Filtering and Network
- B. Network and Threat Prevention
- C. Application Control and URL Filtering
- D. Network and Application Control

**Answer:** C

#### NEW QUESTION 426

- (Exam Topic 4)

Which method below is NOT one of the ways to communicate using the Management API's?

- A. Typing API commands using the "mgmt\_cli" command
- B. Typing API commands from a dialog box inside the SmartConsole GUI application
- C. Typing API commands using Gaia's secure shell (clash)19+
- D. Sending API commands over an http connection using web-services

**Answer:** D

#### NEW QUESTION 427

- (Exam Topic 4)

Please choose correct command syntax to add an "emailserver1" host with IP address 10.50.23.90 using GAIa management CLI?

- A. host name myHost12 ip-address 10.50.23.90
- B. mgmt add host name ip-address 10.50.23.90
- C. add host name emailserver1 ip-address 10.50.23.90
- D. mgmt add host name emailserver1 ip-address 10.50.23.90

**Answer:** D

#### NEW QUESTION 432

- (Exam Topic 4)

Which of the following is an authentication method used for Identity Awareness?

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

**Answer:** B

#### NEW QUESTION 435

- (Exam Topic 4)

When configuring LDAP User Directory integration, Changes applied to a User Directory template are:

- A. Reflected immediately for all users who are using template.
- B. Not reflected for any users unless the local user template is changed.
- C. Reflected for all users who are using that template and if the local user template is changed as well.
- D. Not reflected for any users who are using that template.

**Answer:** A

#### Explanation:

The users and user groups are arranged on the Account Unit in the tree structure of the LDAP server. User management in User Directory is external, not local. You can change the User Directory templates. Users associated with this template get the changes immediately. You can change user definitions manually in SmartDashboard, and the changes are immediate on the server.

#### NEW QUESTION 438

- (Exam Topic 4)

What are the steps to configure the HTTPS Inspection Policy?

- A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
- B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
- C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
- D. Go to Application&url filtering blade > Https Inspection > Policy

**Answer:** C

**NEW QUESTION 440**

- (Exam Topic 4)

Which firewall daemon is responsible for the FW CLI commands?

- A. fwd
- B. fwm
- C. cpm
- D. cpd

**Answer:** A

**NEW QUESTION 445**

- (Exam Topic 4)

Which deployment adds a Security Gateway to an existing environment without changing IP routing?

- A. Distributed
- B. Bridge Mode
- C. Remote
- D. Standalone

**Answer:** B

**NEW QUESTION 447**

- (Exam Topic 4)

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 ctl multik dynamic\_dispatching on
- B. fw ctl multik dynamic\_dispatching set\_mode 9
- C. fw ctl multik set\_mode 9
- D. fw ctl miltik pq enable

**Answer:** C

**NEW QUESTION 452**

- (Exam Topic 4)

What protocol is specifically used for clustered environments?

- A. Clustered Protocol
- B. Synchronized Cluster Protocol
- C. Control Cluster Protocol
- D. Cluster Control Protocol

**Answer:** D

**NEW QUESTION 454**

- (Exam Topic 4)

How many sessions can be opened on the Management Server at the same time?

- A. Unlimited, One per each licensed Gateway
- B. One
- C. Unlimited, Multiple per administrator
- D. Unlimited, One per administrator

**Answer:** D

**NEW QUESTION 457**

- (Exam Topic 4)

What is the SOLR database for?

- A. Used for full text search and enables powerful matching capabilities
- B. Writes data to the database and full text search
- C. Serves GUI responsible to transfer request to the DLE server
- D. Enables powerful matching capabilities and writes data to the database

**Answer:** A

**NEW QUESTION 458**

- (Exam Topic 4)

When an encrypted packet is decrypted, where does this happen?

- A. Security policy
- B. Inbound chain

- C. Outbound chain
- D. Decryption is not supported

**Answer:** A

#### NEW QUESTION 459

- (Exam Topic 4)

Under which file is the proxy arp configuration stored?

- A. \$FWDIR/state/proxy\_arp.conf on the management server
- B. \$FWDIR/conf/local.arp on the management server
- C. \$FWDIR/state/\_tmp/proxy.arp on the security gateway
- D. \$FWDIR/conf/local.arp on the gateway

**Answer:** D

#### NEW QUESTION 464

- (Exam Topic 4)

When using Monitored circuit VRRP, what is a priority delta?

- A. When an interface fails the priority changes to the priority delta
- B. When an interface fails the delta claims the priority
- C. When an interface fails the priority delta is subtracted from the priority
- D. When an interface fails the priority delta decides if the other interfaces takes over

**Answer:** C

#### NEW QUESTION 468

- (Exam Topic 4)

What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

- A. ifconfig -a
- B. show interfaces
- C. show interfaces detail
- D. show configuration interface

**Answer:** D

#### NEW QUESTION 470

- (Exam Topic 4)

Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

- A. Save Policy
- B. install Database
- C. Save Session
- D. install Policy

**Answer:** D

#### NEW QUESTION 472

- (Exam Topic 4)

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 474

- (Exam Topic 4)

Which of the following is NOT a tracking option?

- A. Partial log
- B. Log
- C. Network log
- D. Full log

**Answer:** A

#### NEW QUESTION 475

- (Exam Topic 4)

Fill in the blanks. In \_\_\_\_\_ NAT, the \_\_\_\_\_ is translated.

- A. Hide; source
- B. Static; source
- C. Simple; source
- D. Hide; destination

**Answer:** B

#### NEW QUESTION 477

- (Exam Topic 4)

Which of the following is NOT a method used by Identity Awareness for acquiring identity?

- A. RADIUS
- B. Active Directory Query
- C. Remote Access
- D. Certificates

**Answer:** D

#### NEW QUESTION 479

- (Exam Topic 4)

Fill in the blank: Service blades must be attached to a \_\_\_\_\_. .

- A. Security Gateway
- B. Management container
- C. Management server
- D. Security Gateway container

**Answer:** A

#### NEW QUESTION 484

- (Exam Topic 4)

What Check Point technologies deny or permit network traffic?

- A. Application Control DLP
- B. Packet Filtering, Stateful Inspection, Application Layer Firewall
- C. ACL SandBlast, MPT
- D. IPS, Mobile Threat Protection

**Answer:** B

#### NEW QUESTION 489

- (Exam Topic 4)

Fill in the blank: An LDAP server holds one or more \_\_\_\_\_.

- A. Server Units
- B. Administrator Units
- C. Account Units
- D. Account Server

**Answer:** C

#### NEW QUESTION 491

- (Exam Topic 4)

After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

- A. Security Gateway IP-address cannot be changed without re-establishing the trust
- B. The Security Gateway name cannot be changed in command line without re-establishing trust
- C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust
- D. The Security Management Server IP-address cannot be changed without re-establishing the trust

**Answer:** A

#### NEW QUESTION 495

- (Exam Topic 4)

Which SmartConsole tab is used to monitor network and security performance?

- A. Manage Seeting
- B. Security Policies
- C. Gateway and Servers
- D. Logs and Monitor

**Answer:** C

#### NEW QUESTION 499

- (Exam Topic 4)

Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?

- A. The firewall topologies
- B. NAT Rules
- C. The Rule Base
- D. The VPN Domains

**Answer:** C

#### NEW QUESTION 504

- (Exam Topic 4)

Which GUI tool can be used to view and apply Check Point licenses?

- A. cpconfig
- B. Management Command Line
- C. SmartConsole
- D. SmartUpdate

**Answer:** D

#### Explanation:

SmartUpdate GUI is the recommended way of managing licenses. References:

#### NEW QUESTION 507

- (Exam Topic 4)

What is the main difference between Threat Extraction and Threat Emulation?

- A. Threat Emulation never delivers a file and takes more than 3 minutes to complete
- B. Threat Extraction always delivers a file and takes less than a second to complete
- C. Threat Emulation never delivers a file that takes less than a second to complete
- D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

**Answer:** B

#### NEW QUESTION 512

- (Exam Topic 4)

In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:

- A. 3rd Party integration of CLI and API for Gateways prior to R80.
- B. A complete CLI and API interface using SSH and custom CPCode integration.
- C. 3rd Party integration of CLI and API for Management prior to R80.
- D. A complete CLI and API interface for Management with 3rd Party integration.

**Answer:** B

#### NEW QUESTION 514

- (Exam Topic 4)

What command would show the API server status?

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

**Answer:** D

#### NEW QUESTION 515

- (Exam Topic 4)

Which two Identity Awareness commands are used to support identity sharing?

- A. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
- B. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
- C. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
- D. Policy Activation Point (PAP) and Policy Decision Point (PDP)

**Answer:** A

#### NEW QUESTION 518

- (Exam Topic 4)

Using R80 Smart Console, what does a “pencil icon” in a rule mean?

- A. I have changed this rule
- B. Someone else has changed this rule
- C. This rule is managed by check point's SOC
- D. This rule can't be changed as it's an implied rule

**Answer:**

A

#### NEW QUESTION 522

- (Exam Topic 4)

Fill in the blanks: A \_\_\_\_\_ license requires an administrator to designate a gateway for attachment whereas a \_\_\_\_\_ license is automatically attached to a Security Gateway.

- A. Format; corporate
- B. Local; formal
- C. Local; central
- D. Central; local

**Answer: D**

#### NEW QUESTION 525

- (Exam Topic 4)

To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members? Choose the best answer.

- A. fw ctl set int fwha vmac global param enabled
- B. fw ctl get int fwha vmac global param enabled; result of command should return value 1
- C. cphaprob -a if
- D. fw ctl get int fwha\_vmac\_global\_param\_enabled; result of command should return value 1

**Answer: B**

#### NEW QUESTION 528

- (Exam Topic 4)

Session unique identifiers are passed to the web api using which http header option?

- A. X-chkp-sid
- B. Accept-Charset
- C. Proxy-Authorization
- D. Application

**Answer: C**

#### NEW QUESTION 530

- (Exam Topic 4)

How Capsule Connect and Capsule Workspace differ?

- A. Capsule Connect provides a Layer3 VP
- B. Capsule Workspace provides a Desktop with usable applications
- C. Capsule Workspace can provide access to any application
- D. Capsule Connect provides Business data isolation
- E. Capsule Connect does not require an installed application at client

**Answer: A**

#### NEW QUESTION 534

.....

## Relate Links

**100% Pass Your 156-215.80 Exam with Exambible Prep Materials**

<https://www.exambible.com/156-215.80-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>