

## Exam Questions 156-215.80

Check Point Certified Security Administrator



### NEW QUESTION 1

Which of the following commands can be used to remove site-to-site IPSEC Security Associations (SA)?

- A. vpn tu
- B. vpn ipsec remove -l
- C. vpn debug ipsec
- D. fw ipsec tu

**Answer:** A

**Explanation:** vpn tu

Description Launch the TunnelUtil tool which is used to control VPN tunnels.

Usage vpn tu vpn tunnelutil Example vpn tu Output

```
*****      Select Option      *****

(1)          List all IKE SAs
(2)          List all IPsec SAs
(3)          List all IKE SAs for a given peer (GW) or user (Client)
(4)          List all IPsec SAs for a given peer (GW) or user (Client)
(5)          Delete all IPsec SAs for a given peer (GW)
(6)          Delete all IPsec SAs for a given User (Client)
(7)          Delete all IPsec+IKE SAs for a given peer (GW)
(8)          Delete all IPsec+IKE SAs for a given User (Client)
(9)          Delete all IPsec SAs for ALL peers and users
(0)          Delete all IPsec+IKE SAs for ALL peers and users

(Q)          Quit
```

### NEW QUESTION 2

What does the “unknown” SIC status shown on SmartConsole mean?

- A. The SMS can contact the Security Gateway but cannot establish Secure Internal Communication.
- B. SIC activation key requires a reset.
- C. The SIC activation key is not known by any administrator.
- D. There is no connection between the Security Gateway and SMS.

**Answer:** D

**Explanation:** The most typical status is Communicating. Any other status indicates that the SIC communication is problematic. For example, if the SIC status is Unknown then there is no connection between the Gateway and the Security Management server. If the SIC status is Not Communicating, the Security Management server is able to contact the gateway, but SIC communication cannot be established.

### NEW QUESTION 3

You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the right protections in place. Check Point has been selected for the security vendor. Which Check Point products protect BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

- A. IPS and Application Control
- B. IPS, anti-virus and anti-bot
- C. IPS, anti-virus and e-mail security
- D. SandBlast

**Answer:** D

**Explanation:** SandBlast Zero-Day Protection

Hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. Zero-day exploit protection from Check Point provides a deeper level of inspection so you can prevent more malware and zero-day attacks, while ensuring quick delivery of safe content to your users.

### NEW QUESTION 4

You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

- A. Logging has disk space issue
- B. Change logging storage options on the logging server or Security Management Server properties and install database.

- C. Data Awareness is not enabled.
- D. Identity Awareness is not enabled.
- E. Logs are arriving from Pre-R80 gateways.

**Answer:** A

**Explanation:** The most likely reason for the logs data to stop is the low disk space on the logging device, which can be the Management Server or the Gateway Server.

#### NEW QUESTION 5

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 6

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

- A. INSPECT Engine
- B. Stateful Inspection
- C. Packet Filtering
- D. Application Layer Firewall

**Answer:** B

#### NEW QUESTION 7

What are the three essential components of the Check Point Security Management Architecture?

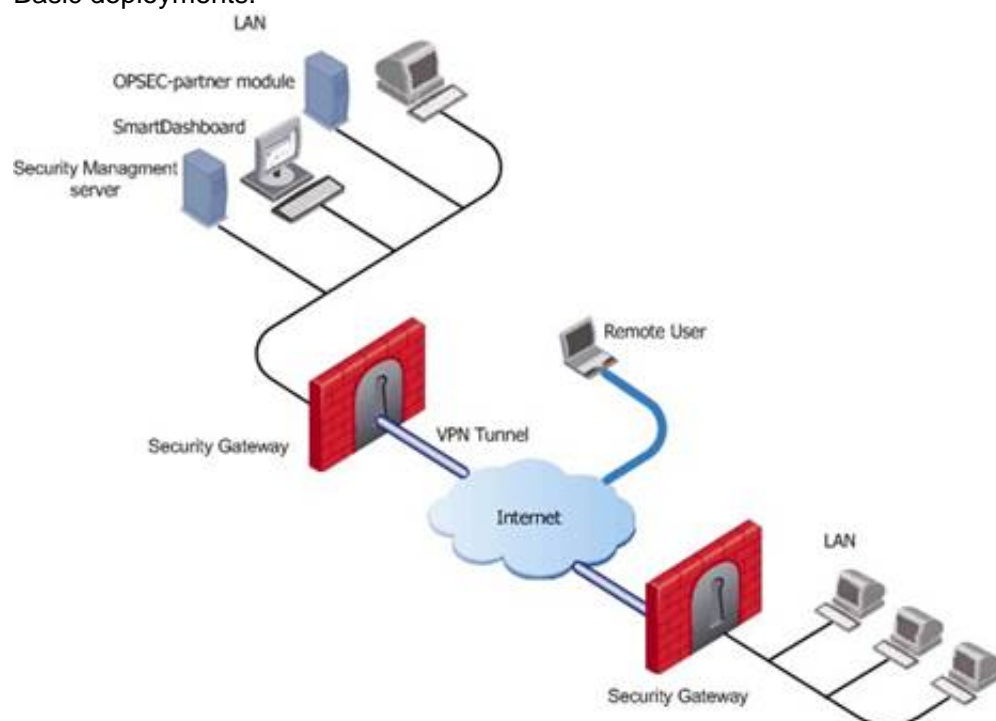
- A. SmartConsole, Security Management Server, Security Gateway
- B. SmartConsole, SmartUpdate, Security Gateway
- C. Security Management Server, Security Gateway, Command Line Interface
- D. WebUI, SmartConsole, Security Gateway

**Answer:** A

**Explanation:** Standalone deployment - Security Gateway and the Security Management server are installed on the same machine.  
 Distributed deployment - Security Gateway and the Security Management server are installed on different machines.

Deployments

Basic deployments:



Assume an environment with gateways on different sites. Each Security Gateway connects to the Internet on one side, and to a LAN on the other. You can create a Virtual Private Network (VPN) between the two Security Gateways, to secure all communication between them.

The Security Management server is installed in the LAN, and is protected by a Security Gateway. The Security Management server manages the Security Gateways and lets remote users connect securely to the corporate network. SmartDashboard can be installed on the Security Management server or another computer.

There can be other OPSEC-partner modules (for example, an Anti-Virus Server) to complete the network security with the Security Management server and its Security Gateways.

#### NEW QUESTION 8

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 9

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 10

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 10

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

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

**Answer:** D

**Explanation:** There are different deployment scenarios for Check Point software products.

Standalone Deployment - The Security Management Server and the Security Gateway are installed on the same computer or appliance.

#### NEW QUESTION 14

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 16

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 18


Which of the following is TRUE regarding Gaia command line?

- A. Configuration changes should be done in mgmt\_cli and use CLISH for monitoring, Expert mode is used only for OS level tasks.
- B. Configuration changes should be done in expert-mode and CLISH is used for monitoring.
- C. Configuration changes should be done in mgmt-cli and use expert-mode for OS-level tasks.
- D. All configuration changes should be made in CLISH and expert-mode should be used for OS-level tasks.

**Answer:** D

#### NEW QUESTION 21

Two administrators Dave and Jon both manage R80 Management as administrators for ABC Corp. Jon logged into the R80 Management and then shortly after Dave logged in to the same server. They are both in the Security Policies view. From the screenshots below, why does Dave not have the rule no.6 in his SmartConsole view even though Jon has it in his SmartConsole view?



No.	Name	Source	Destination	VPN	Services & Applications	Action
1	HerBOSG Policy	Any	Any	Any	Any	Drop
2	Management	Net_10.28.0.0	10W-67736	Any	https, ssh	Accept
3	Stealth	Any	10W-67736	Any	Any	Drop
4	DMZ	Net_10.28.0.0	Any	Any	Any	Accept
5	Web	Net_10.28.0.0	Any	Any	https, http	Accept
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.5.2.0	Any	Any	Accept
7	Cleanup rule	Any	Any	Any	Any	Drop

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	HerBOSG Policy	Any	Any	Any	Any	Drop
2	Management	Net_10.28.0.0	10W-67736	Any	https, ssh	Accept
3	Stealth	Any	10W-67736	Any	Any	Drop
4	DMZ	Net_10.28.0.0	Any	Any	Any	Accept
5	Web	Net_10.28.0.0	Any	Any	https, http	Accept
6	Cleanup rule	Any	Any	Any	Any	Drop

- A. Jon is currently editing rule no.6 but has Published part of his changes.
- B. Dave is currently editing rule no.6 and has marked this rule for deletion.
- C. Dave is currently editing rule no.6 and has deleted it from his Rule Base.
- D. Jon is currently editing rule no.6 but has not yet Published his changes.

**Answer:** D

**Explanation:** When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited. To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

#### NEW QUESTION 26

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

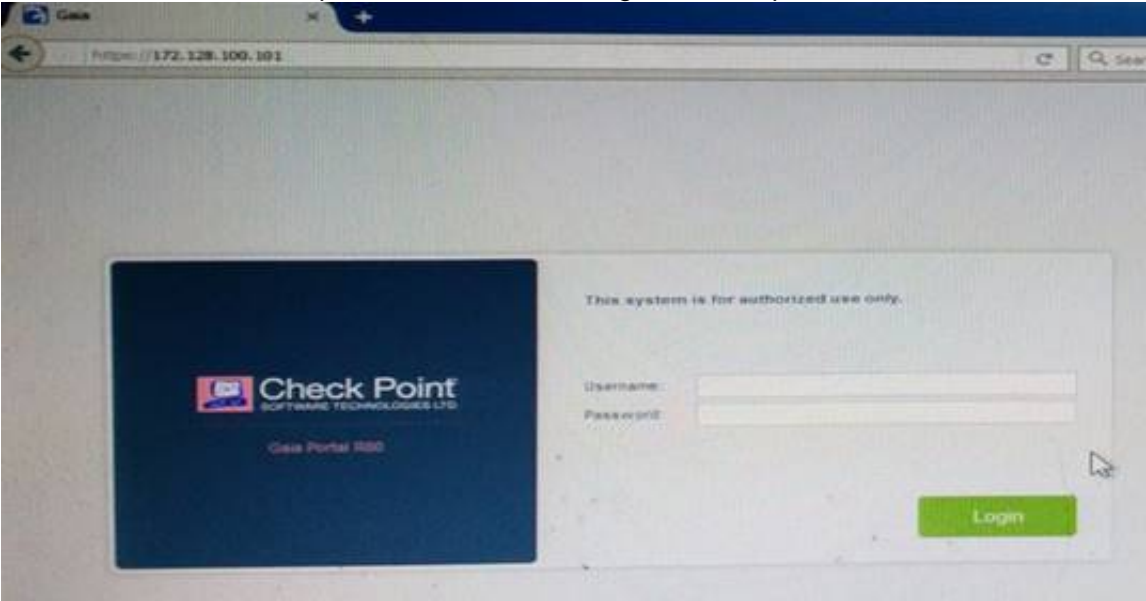
**Explanation:** Configuring Roles - CLI (rba)



Description	<div>1. Add, change or delete role definitions.</div> <div>2. Add or remove users to or from existing roles.</div> <div>3. Add or remove access mechanism (WebUI or CLI) permissions for a specified user.</div>
Syntax	<div>add rba role &lt;Name&gt; domain-type System</div> <div>    readonly-features &lt;List&gt;</div> <div>    readwrite-features &lt;List&gt;</div> <div> </div> <div>add rba user &lt;User name&gt; access-mechanisms [Web-UI   CLI]</div> <div>add rba user &lt;User Name&gt; roles &lt;List&gt;</div> <div> </div> <div>delete rba role &lt;Name&gt;</div> <div> </div> <div>delete rba role &lt;Name&gt;</div> <div>    readonly-features &lt;List&gt;</div> <div>    readwrite-features &lt;List&gt;</div> <div> </div> <div>delete rba user &lt;User Name&gt; access-mechanisms [Web-UI   CLI]</div> <div>delete rba user &lt;User Name&gt; roles &lt;List&gt;</div>

**NEW QUESTION 30**

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 35**

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 38**

Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

- A. Security questions
- B. Check Point password

- C. SecurID
- D. RADIUS

**Answer:** A

**Explanation:** Authentication Schemes :- Check Point Password

- Operating System Password
- RADIUS
- SecurID
- TACAS
- Undefined If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, access is always denied.

#### NEW QUESTION 42

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 45

What is the purpose of Captive Portal?

- A. It provides remote access to SmartConsole
- B. It manages user permission in SmartConsole
- C. It authenticates users, allowing them access to the Internet and corporate resources
- D. It authenticates users, allowing them access to the Gaia OS

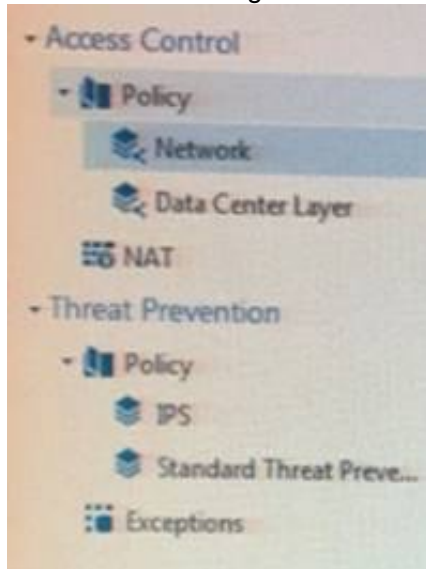
**Answer:** C

**Explanation:** Captive Portal – a simple method that authenticates users through a web interface before granting them access to Intranet resources. When users try to access a protected resource, they get a web page that must be filled out to continue.

Reference : <https://www.checkpoint.com/products/identity-awareness-software-blade/>

#### NEW QUESTION 46

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 50**

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>](https://<Device_IP_Address>)
- B. [https://<Device\\_IP\\_Address>:443](https://<Device_IP_Address>:443)
- C. [https://<Device\\_IP\\_Address>:10000](https://<Device_IP_Address>:10000)
- D. [https://<Device\\_IP\\_Address>:4434](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>](https://<Gaia_IP_address>)

Enter your user name and password. References:

**NEW QUESTION 53**

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

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

**Answer:** C

**Explanation:** One for Security Management Server and the other one for the Security Gateway.

**NEW QUESTION 57**

Which application should you use to install a contract file?

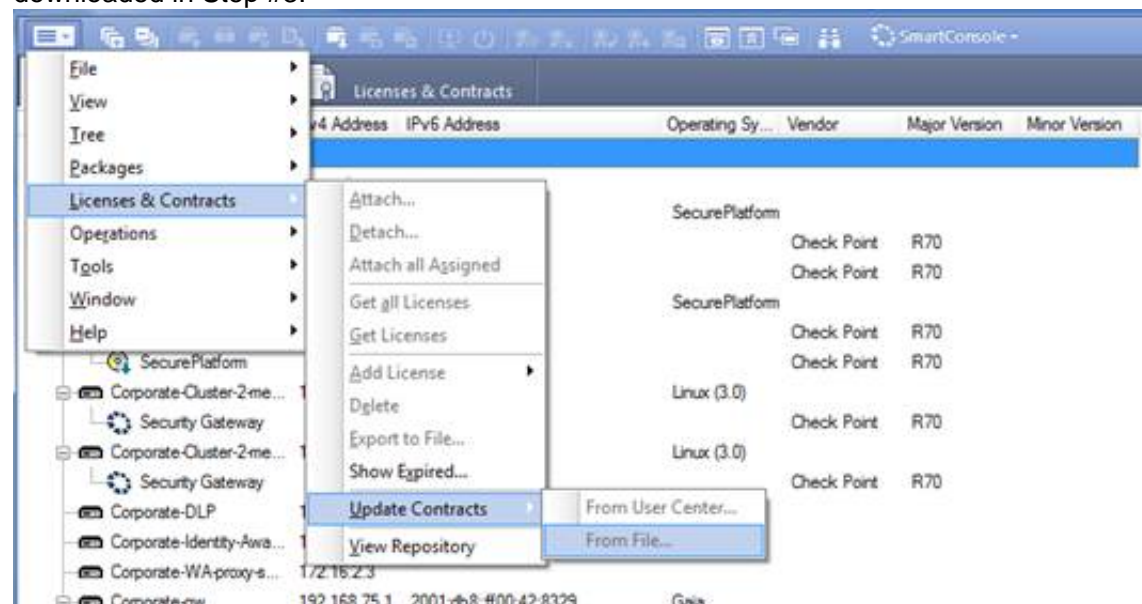
- A. SmartView Monitor
- B. WebUI
- C. SmartUpdate
- D. SmartProvisioning

**Answer:** C

**Explanation:** Using SmartUpdate: If you already use an NGX R65 (or higher) Security Management / Provider-1 /

Multi-Domain Management Server, SmartUpdate allows you to import the service contract file that you have downloaded in Step #3.

Open SmartUpdate and from the Launch Menu select 'Licenses & Contracts' -> 'Update Contracts' -> 'From File...' and provide the path to the file you have downloaded in Step #3:



Note: If SmartUpdate is connected to the Internet, you can download the service contract file directly from the UserCenter without going through the download and import steps.

**NEW QUESTION 62**

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/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 66

Fill in the blank: With the User Directory Software Blade, you can create R80 user definitions on a(an) \_\_\_\_\_ Server.

- A. NT domain
- B. SMTP
- C. LDAP
- D. SecurID

**Answer:** C

#### NEW QUESTION 69

Which utility shows the security gateway general system information statistics like operating system information and resource usage, and individual software blade statistics of VPN, Identity Awareness and DLP?

- A. cpconfig
- B. fw ctl pstat
- C. cpview
- D. fw ctl multik stat

**Answer:** C

**Explanation:** CPView Utility is a text based built-in utility that can be run ('cpview' command) on Security Gateway / Security Management Server / Multi-Domain Security Management Server. CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Gateway). The data is continuously updated in easy to access views.

#### NEW QUESTION 72

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 74

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 77

The following graphic shows:

[illegible]

- A. View from SmartLog for logs initiated from source address 10.1.1.202  
B. View from SmartView Tracker for logs of destination address 10.1.1.202  
C. View from SmartView Tracker for logs initiated from source address 10.1.1.202  
D. View from SmartView Monitor for logs initiated from source address 10.1.1.202

**Answer: C**

**NEW QUESTION 78**

Which of the following is NOT an integral part of VPN communication within a network?

- A. VPN key
- B. VPN community
- C. VPN trust entities
- D. VPN domain

**Answer: A**

**Explanation:** VPN key (to not be confused with pre-shared key that is used for authentication).

VPN trust entities, such as a Check Point Internal Certificate Authority (ICA). The ICA is part of the Check Point suite used for creating SIC trusted connection between Security Gateways, authenticating administrators and third party servers. The ICA provides certificates for internal Security Gateways and remote access clients which negotiate the VPN link.

VPN Domain - A group of computers and networks connected to a VPN tunnel by one VPN gateway that handles encryption and protects the VPN Domain members.

VPN Community - A named collection of VPN domains, each protected by a VPN gateway. References:

[http://sc1.checkpoint.com/documents/R77/CP\\_R77\\_VPN\\_AdminGuide/13868.htm](http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm)

**NEW QUESTION 79**

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 83**

What is the order of NAT priorities?

- A. Static NAT, IP pool NAT, hide NAT  
B. IP pool NAT, static NAT, hide NAT  
C. Static NAT, automatic NAT, hide NAT  
D. Static NAT, hide NAT, IP pool NAT

**Answer: A**

**Explanation:** The order of NAT priorities is:

- Static NAT
- IP Pool NAT
- Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

### NEW QUESTION 87

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CPApp

**Answer:** B

**Explanation:** AppWiki Application Classification Library

AppWiki enables application scanning and detection of more than 5,000 distinct applications and over 300,000 Web 2.0 widgets including instant messaging, social networking, video streaming, VoIP, games and more.

#### NEW QUESTION 90

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret is shared and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

- A. IPsec VPN blade should be enabled on both Security Gateway.
- B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
- D. The Security Gateways are pre-R75.40.

**Answer:** C

#### NEW QUESTION 94

Which of the following is NOT a license activation method?

- A. SmartConsole Wizard
- B. Online Activation
- C. License Activation Wizard
- D. Offline Activation

**Answer:** A

#### NEW QUESTION 98

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 101

In R80, Unified Policy is a combination of

- A. Access control policy, QoS Policy, Desktop Security Policy and endpoint policy.
- B. Access control policy, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
- C. Firewall policy, address Translation and application and URL filtering, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
- D. Access control policy, QoS Policy, Desktop Security Policy and VPN policy.

**Answer:** D

**Explanation:** D is the best answer given the choices. Unified Policy

In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:

Firewall and VPN  
Application Control and URL Filtering  
Identity Awareness  
Data Awareness  
Mobile Access  
Security Zones

#### NEW QUESTION 103

Which one of the following is the preferred licensing model? Select the Best answer.

- A. Local licensing because it ties the package license to the IP-address of the gateway and has no dependency of the Security Management Server.
- B. Central licensing because it ties the package license to the IP-address of the Security Management Server and has no dependency of the gateway.
- C. Local licensing because it ties the package license to the MAC-address of the gateway management interface and has no Security Management Server dependency.
- D. Central licensing because it ties the package license to the MAC-address of the Security Management Server Mgmt-interface and has no dependency of the

gateway.

**Answer:** B

**Explanation:** Central License

A Central License is a license attached to the Security Management server IP address, rather than the gatewa IP address. The benefits of a Central License are:

Only one IP address is needed for all licenses.

A license can be taken from one gateway and given to another.

The new license remains valid when changing the gateway IP address. There is no need to create and install a new license.

#### NEW QUESTION 106

Fill in the blank: RADIUS protocol uses \_\_\_\_\_ to communicate with the gateway.

- A. UDP
- B. TDP
- C. CCP
- D. HTTP

**Answer:** A

**Explanation:** Parameters:

Parameter	Description
port	UDP port on the RADIUS server. This value must match the port as configured on the RADIUS server. Typically this 1812 (default) or 1645 (non-standard but a commonly used alternative).

#### NEW QUESTION 107

Which options are given on features, when editing a Role on Gaia Platform?

- A. Read/Write, Read Only
- B. Read/Write, Read only, None
- C. Read/Write, None
- D. Read Only, None

**Answer:** B

**Explanation:** Roles

Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (readonly) access to other features, and no access to other features.

You can also specify which access mechanisms (WebUI or the CLI) are available to the user.

Note - When users log in to the WebUI, they see only those features that they have read-only or read/write access to. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.

Gaia includes these predefined roles:

You cannot delete or change the predefined roles.

Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.

#### NEW QUESTION 112

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 117

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

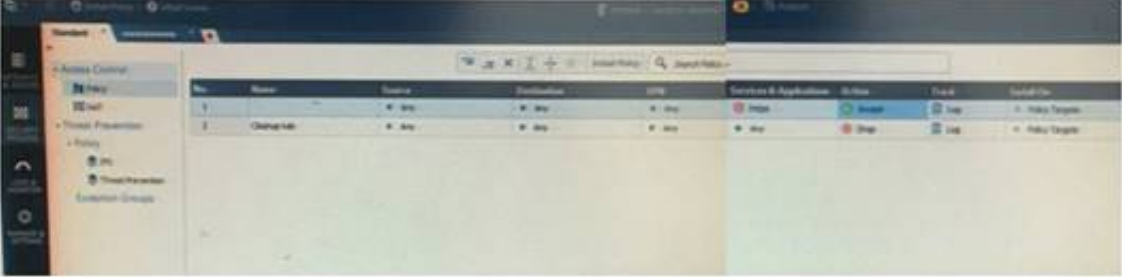
**Explanation:** the Download Center web site (packages)  
the Check Point DVD (packages)



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 121**

On the following graphic, you will find layers of policies.



What is a precedence of traffic inspection for the defined polices?

- A. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if implicit Drop Rule drops the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer.
- B. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer
- C. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to Threat Prevention layer and then after accepting the packet it passes to IPS layer.
- D. A packet arrives at the gateway, it is checked against the rules in IPS policy layer and then it comes next to the Network policy layer and then after accepting the packet it passes to Threat Prevention layer.

**Answer: B**

**Explanation:** To simplify Policy management, R80 organizes the policy into Policy Layers. A layer is a set of rules, or a Rule Base.

For example, when you upgrade to R80 from earlier versions:

Gateways that have the Firewall and the Application Control Software Blades enabled will have their Access Control Policy split into two ordered layers: Network and Applications.

When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.

Gateways that have the IPS and Threat Emulation Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention.

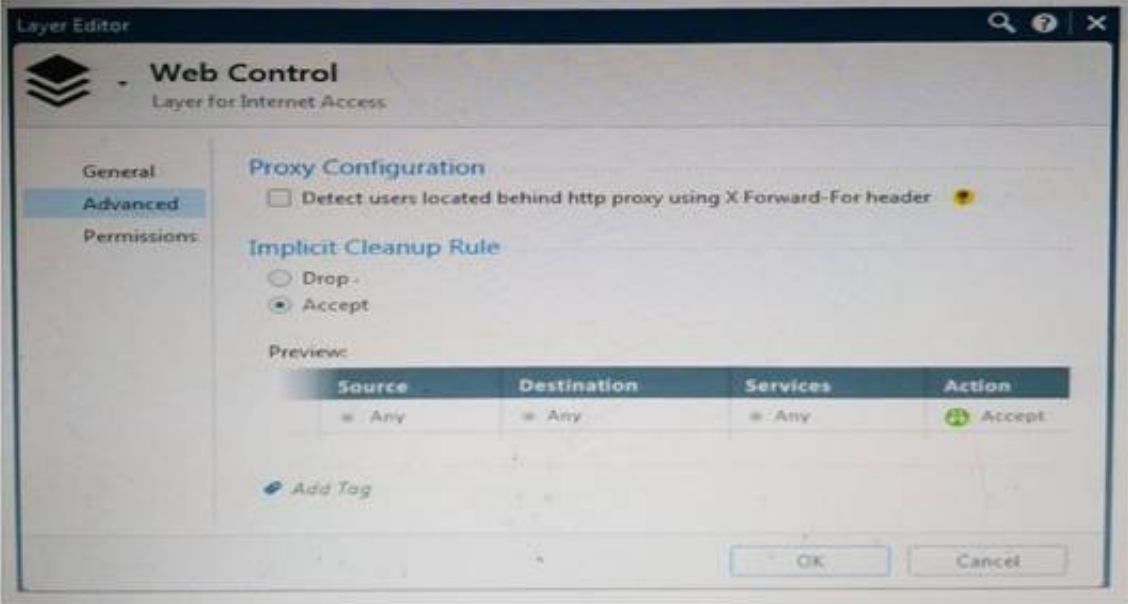
All layers are evaluated in parallel

When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.

All layers are evaluated in parallel

**NEW QUESTION 123**

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, expect 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 125

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 128

Fill in the blank: The tool \_\_\_\_ generates a R80 Security Gateway configuration report.

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

**Answer: C**

**Explanation:** CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp\_uploader utility for uploading files to Check Point servers). The CPinfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPinfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings. When contacting Check Point Support, collect the cpinfo files from the Security Management server and Security Gateways involved in your case.

#### NEW QUESTION 131

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 134

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 137

What are the three conflict resolution rules in the Threat Prevention Policy Layers?

- A. Conflict on action, conflict on exception, and conflict on settings
- B. Conflict on scope, conflict on settings, and conflict on exception
- C. Conflict on settings, conflict on address, and conflict on exception
- D. Conflict on action, conflict on destination, and conflict on settings

**Answer: C**

#### NEW QUESTION 141

Which policy type has its own Exceptions section?

- A. Threat Prevention
- B. Access Control
- C. Threat Emulation
- D. Desktop Security

**Answer:** A

**Explanation:** The Exceptions Groups pane lets you define exception groups. When necessary, you can create exception groups to use in the Rule Base. An exception group contains one or more defined exceptions. This option facilitates ease-of-use so you do not have to manually define exceptions in multiple rules for commonly required exceptions. You can choose to which rules you want to add exception groups. This means they can be added to some rules and not to others, depending on necessity.

**NEW QUESTION 145**

Where can you trigger a failover of the cluster members?  
 Log in to Security Gateway CLI and run command clusterXL\_admin down.  
 In SmartView Monitor right-click the Security Gateway member and select Cluster member stop. Log into Security Gateway CLI and run command cphaprob down.

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

**Answer:** C

**Explanation:** How to Initiate Failover

Method	To Stop ClusterXL	To Start ClusterXL
Run: o cphaprob -d faildevice -t 0 -s ok register o cphaprob -d faildevice -s problem report and: o cphaprob -d faildevice -s ok report o cphaprob -d faildevice unregister	Effect: o Disables ClusterXL o Does not disable synchronization	Effect: o Enables ClusterXL o Does not initiate full synchronization
<b>Recommended method:</b> Run: o clusterXL_admin down o clusterXL_admin up	o Disables ClusterXL o Does not disable synchronization	o Enables ClusterXL o Does not initiate full synchronization
In SmartView Monitor: 1. Click the Cluster object. 2. Select one of the member gateway branches. 3. Right click the cluster member. 4. Select <b>Down</b> .	o Disables ClusterXL o Disables synchronization	o Enables ClusterXL o Does not initiate full synchronization

**NEW QUESTION 147**

What is NOT an advantage of Packet Filtering?

- A. Low Security and No Screening above Network Layer
- B. Application Independence
- C. High Performance
- D. Scalability

**Answer:** A

**Explanation:** Packet Filter Advantages and Disadvantages

Advantages	Disadvantages
Application independence	Low security
High performance	No screening above the network layer
Scalability	

**NEW QUESTION 152**

What are the two high availability modes?

- A. Load Sharing and Legacy
- B. Traditional and New
- C. Active and Standby
- D. New and Legacy

**Answer:** D

**Explanation:** ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.  
 Load Sharing Multicast Mode

Load Sharing Unicast Mode  
 New High Availability Mode  
 High Availability Legacy Mode

#### NEW QUESTION 155

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 159

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 160

You are unable to login to SmartDashboard. You log into the management server and run #cpwd\_admin list with the following output:

APP	PID	STAT	#START	START_TIME	MON	COMMAND
CPFWIND	1078	E	1	[16:28:34] 3/5/2016	N	cpfwind
CPD	0	T	1	[17:13:57] 6/5/2016	N	cpd
FWO	21781	E	1	[17:13:51] 6/5/2016	N	fwd -c
CPM	0	T	1	[18:32:23] 6/5/2016	N	/opt/CPsuite-R80/fw1/scripts/cpm.sh -s
FWM	0	T	1	[17:13:49] 6/5/2016	N	fwm
FTL	7873	E	1	[16:32:52] 3/5/2016	N	LogCore
SMARTVIEW	7884	E	1	[16:32:52] 3/5/2016	N	SmartView
INDEXER	7934	E	1	[16:32:53] 3/5/2016	N	/opt/CPfw-R80/log_indexer/log_indexer
SMARTLOG_SERVER	7977	E	1	[16:32:53] 3/5/2016	N	/opt/CPsmartlog-R80/smartlog_server
SVR	8045	E	1	[16:32:54] 3/5/2016	N	SVRServer
DASERVICE	8084	E	1	[16:32:54] 3/5/2016	N	DAService_script
CPSM	0	T	0	[17:17:02] 6/5/2016	N	cpstat_monitor

What reason could possibly BEST explain why you are unable to connect to SmartDashboard?

- A. CDP is down
- B. SVR is down
- C. FWM is down
- D. CPSM is down

**Answer:** C

**Explanation:** The correct answer would be FWM (is the process making available communication between SmartConsole applications and Security Management Server.). STATE is T (Terminate = Down)

Symptoms

SmartDashboard fails to connect to the Security Management server.

Verify if the FWM process is running. To do this, run the command:

[Expert@HostName:0]# ps -aux | grep fwm

If the FWM process is not running, then try force-starting the process with the following command: [Expert@HostName:0]# cpwd\_admin start -name FWM -path

"\$FWDIR/bin/fwm" -command "fwm" [Expert@HostName:0]# ps -aux | grep fwm

[Expert@HostName:0]# cpwd\_admin start -name FWM -path "\$FWDIR/bin/fwm" -command "fwm"

#### NEW QUESTION 164

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

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

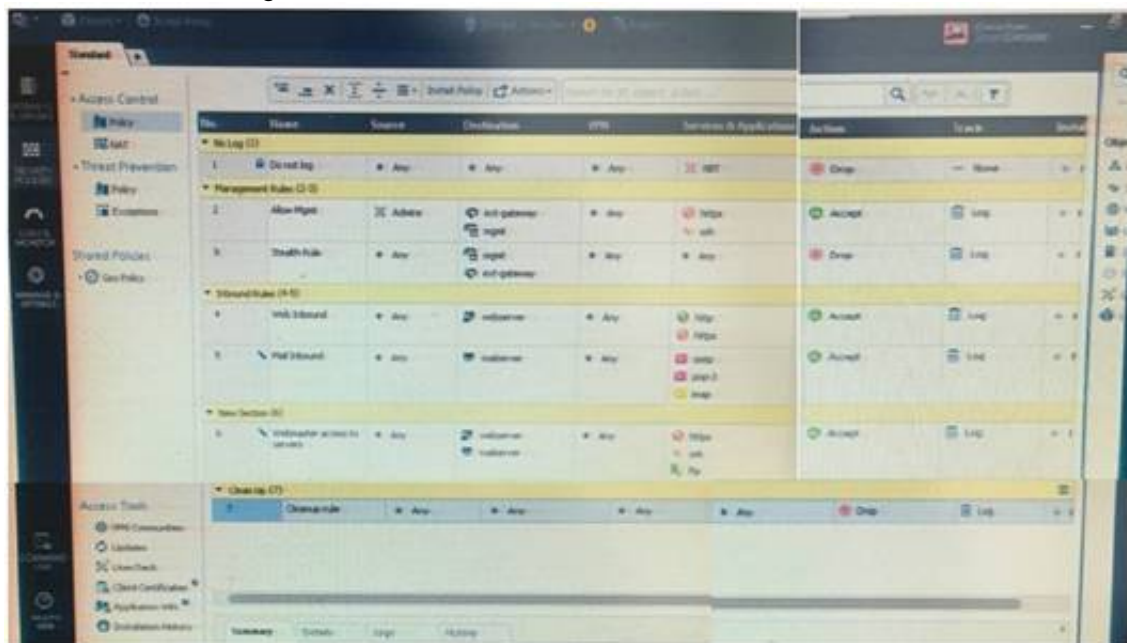
D. 6 months

**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 169

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)

	Description
	Discard changes made during the session
	Enter session details and see the number of changes made in the session
	Commit policy changes to the database and make them visible to other administrators <b>Note</b> - The changes are saved on the gateways and enforced after the next policy install

#### NEW QUESTION 172

Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address?

- A. High Availability
- B. Load Sharing Multicast
- C. Load Sharing Pivot
- D. Master/Backup

**Answer:** B

**Explanation:** ClusterXL uses the Multicast mechanism to associate the virtual cluster IP addresses with all cluster members. By binding these IP addresses to a Multicast MAC address, it ensures that all packets sent to the cluster, acting as a gateway, will reach all members in the cluster.

#### NEW QUESTION 176

What is the potential downside or drawback to choosing the Standalone deployment option instead of the Distributed deployment option?

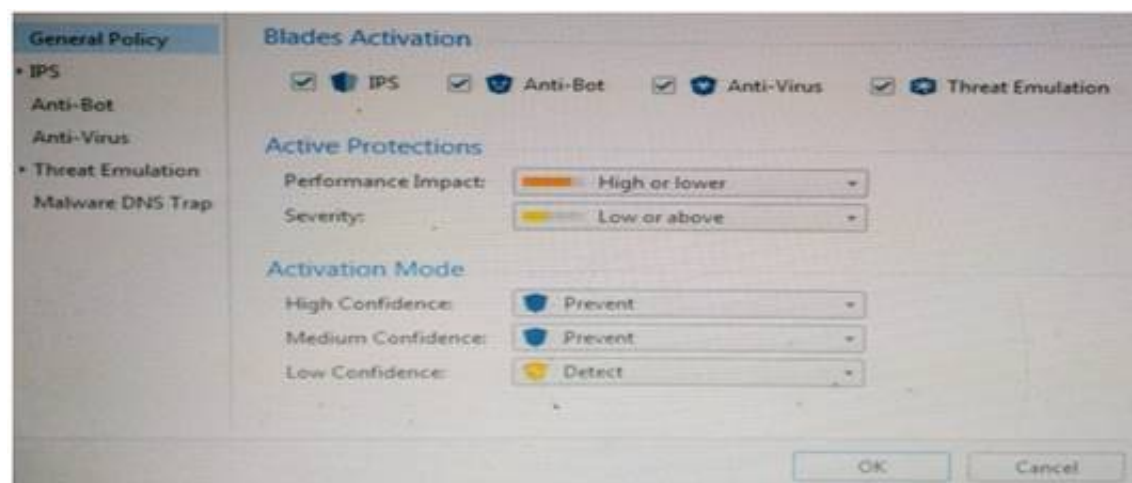
- A. degrades performance as the Security Policy grows in size
- B. requires additional Check Point appliances
- C. requires additional software subscription
- D. increases cost

**Answer:** A

#### NEW QUESTION 181

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 Profile
- D. Consider adding more memory to the appliance.
- E. Set the Performance Impact to Very Low Confidence to Prevent.

**Answer: B**

#### NEW QUESTION 183

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 185

What statement is true regarding Visitor Mode?

- A. VPN authentication and encrypted traffic are tunneled through port TCP 443.
- B. Only ESP traffic is tunneled through port TCP 443.
- C. Only Main mode and Quick mode traffic are tunneled on TCP port 443.
- D. All VPN traffic is tunneled through UDP port 4500.

**Answer: A**

#### NEW QUESTION 187

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 189

What are the three tabs available in SmartView Tracker?

- A. Network & Endpoint, Management, and Active
- B. Network, Endpoint, and Active
- C. Predefined, All Records, Custom Queries
- D. Endpoint, Active, and Custom Queries

**Answer: C**

#### NEW QUESTION 194

You are the Security Administrator for MegaCorp. In order to see how efficient your firewall Rule Base is, you would like to see how many often the particular rules match. Where can you see it? Give the BEST answer.

- A. In the SmartView Tracker, if you activate the column Matching Rate.
- B. In SmartReporter, in the section Firewall Blade – Activity > Network Activity with information concerning Top Matched Logged Rules.
- C. SmartReporter provides this information in the section Firewall Blade – Security > Rule Base Analysis with information concerning Top Matched Logged Rules.
- D. It is not possible to see it directly
- E. You can open SmartDashboard and select UserDefined in the Track column
- F. Afterwards, you need to create your own program with an external counter.

**Answer: C**



#### NEW QUESTION 195

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 196

Can a Check Point gateway translate both source IP address and destination IP address in a given packet?

- A. Yes.
- B. No.
- C. Yes, but only when using Automatic NAT.
- D. Yes, but only when using Manual NAT.

**Answer:** A

#### NEW QUESTION 200

Where do we need to reset the SIC on a gateway object?

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

**Answer:** A

#### NEW QUESTION 203

Which of the following is NOT an alert option?

- A. SNMP
- B. High alert
- C. Mail
- D. User defined alert

**Answer:** B

**Explanation:** In Action, select:

none - No alert.

log - Sends a log entry to the database.

alert - Opens a pop-up window to your desktop.

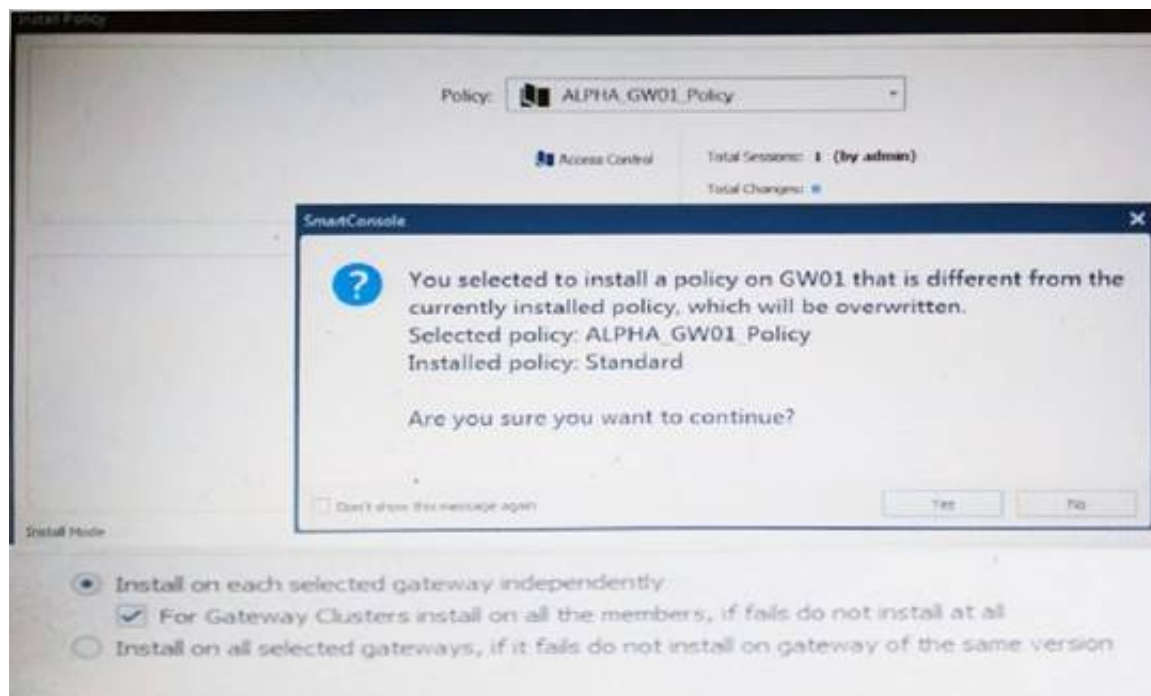
mail - Sends a mail alert to your Inbox.

snmptrap - Sends an SNMP alert.

useralert - Runs a script. Make sure a user-defined action is available. Go to SmartDashboard > Global Properties > Log and Alert > Alert Commands.

#### NEW QUESTION 206

Why would an administrator see the message below?

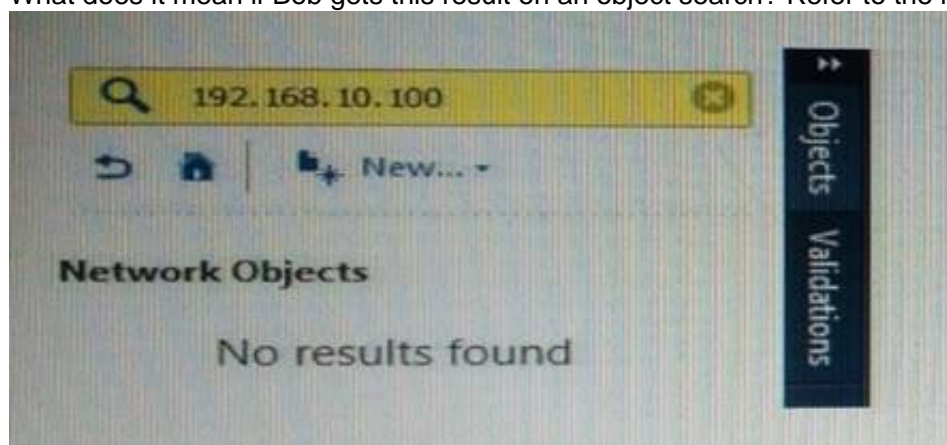


- A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed 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 209

What does it mean if Bob gets this result on an object search? Refer to the image below. Choose the BEST answer.



- A. Search detailed is missing the subnet mask.
- B. There is no object on the database with that name or that IP address.
- C. There is no object on the database with that IP address.
- D. Object does not have a NAT IP address.

**Answer: B**

#### NEW QUESTION 213

Which of the following is NOT a VPN routing option available in a star community?

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

**Answer: A**

#### Explanation: SmartConsole

For simple hubs and spokes (or if there is only one Hub), the easiest way is to configure a VPN star community in R80 SmartConsole:

On the Star Community window, in the:

Center Gateways section, select the Security Gateway that functions as the "Hub".

Satellite Gateways section, select Security Gateways as the "spokes", or satellites.

On the VPN Routing page, Enable VPN routing for satellites section, select one of these options:

To center and to other Satellites through center - This allows connectivity between the Security Gateways, for example if the spoke Security Gateways are DAIP Security Gateways, and the Hub is a Security 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 Security Gateways as well as the ability to inspect all communication passing through the Hub to the Internet.

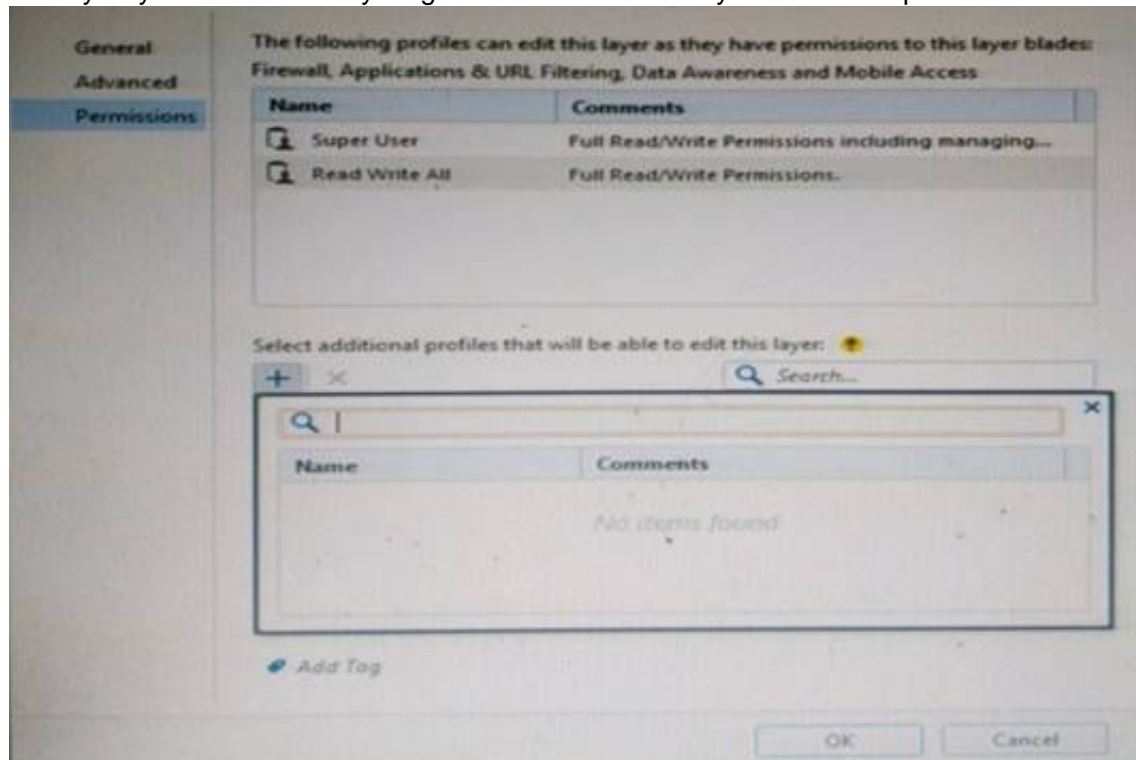
Create an appropriate Access Control Policy rule.

NAT the satellite Security Gateways on the Hub if the Hub is used to route connections from Satellites to the Internet.

The two Dynamic Objects (DAIP Security Gateways) can securely route communication through the Security Gateway with the static IP address.

#### NEW QUESTION 214

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 215

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, gateway policy permits access only from John's desktop which is assigned an IP address 10.0.0.19 via DHCP.

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but the limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop. He wants to move around the organization and continue to have access to the HR Web Server. To make this scenario work, the IT administrator:

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

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

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

**Answer: C**

#### NEW QUESTION 218

Fill in the blank: A \_\_\_\_\_ is used by a VPN gateway to send traffic as if it were a physical interface.

- A. VPN Tunnel Interface
- B. VPN community
- C. VPN router
- D. VPN interface

**Answer: A**

**Explanation:** Route Based VPN

VPN traffic is routed according to the routing settings (static or dynamic) of the Security Gateway operating system. The Security Gateway uses a VTI (VPN Tunnel Interface) to send the VPN traffic as if it were a physical interface. The VTIs of Security Gateways in a VPN community connect and can support dynamic routing protocols.

#### NEW QUESTION 221

Which of these components does NOT require a Security Gateway R77 license?

- A. Security Management Server
- B. Check Point Gateway
- C. SmartConsole
- D. SmartUpdate upgrading/patching

**Answer: C**

#### NEW QUESTION 222

Fill in the blank: The \_\_\_\_\_ software blade enables Application Security policies to allow, block, or limit website access based on user, group, and machine identities.

- A. Application Control
- B. Data Awareness
- C. URL Filtering
- D. Threat Emulation

**Answer:** A

#### NEW QUESTION 223

Choose what BEST describes a Session.

- A. Starts when an Administrator publishes all the changes made on SmartConsole.
- B. Starts when an Administrator logs in to the Security Management Server through SmartConsole and ends when it is published.
- C. Sessions ends when policy is pushed to the Security Gateway.
- D. Sessions locks the policy package for editing.

**Answer:** B

**Explanation:** Administrator Collaboration

More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited.

To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

#### NEW QUESTION 227

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 228

If there is an Accept Implied Policy set to "First", what is the reason Jorge cannot see any logs?

- A. Log Implied Rule was not selected on Global Properties.
- B. Log Implied Rule was not set correctly on the track column on the rules base.
- C. Track log column is set to none.
- D. Track log column is set to Log instead of Full Log.

**Answer:** A

**Explanation:** Implied Rules are configured only on Global Properties.

#### NEW QUESTION 232

Fill in the blanks: A High Availability deployment is referred to as a \_\_\_\_\_ cluster and a Load Sharing deployment is referred to as a \_\_\_\_\_ cluster.

- A. Standby/standby; active/active
- B. Active/active; standby/standby
- C. Active/active; active/standby;
- D. Active/standby; active/active

**Answer:** D

**Explanation:** In a High Availability cluster, only one member is active (Active/Standby operation).

ClusterXL Load Sharing distributes traffic within a cluster so that the total throughput of multiple members is increased. In Load Sharing configurations, all functioning members in the cluster are active, and handle network traffic (Active/Active operation).

#### NEW QUESTION 237

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 240

Fill in the blank: A(n) \_\_\_\_\_ rule is created by an administrator and is located before the first and before last rules in the Rule Base.

- A. Firewall drop
- B. Explicit
- C. Implicit accept
- D. Implicit drop
- E. Implied

Answer: E

**Explanation:** This is the order that rules are enforced:

First Implied Rule: You cannot edit or delete this rule and no explicit rules can be placed before it.

Explicit Rules: These are rules that you create.

Before Last Implied Rules: These implied rules are applied before the last explicit rule.

Last Explicit Rule: We recommend that you use the Cleanup rule as the last explicit rule.

Last Implied Rules: Implied rules that are configured as Last in Global Properties.

Implied Drop Rule: Drops all packets without logging.

NEW QUESTION 241

In order to modify Security Policies the administrator can use which of the following tools? Select the BEST answer.

- A. Command line of the Security Management Server or mgmt\_cli.exe on any Windows computer.
- B. SmartConsole and WebUI on the Security Management Server.
- C. mgmt\_cli or WebUI on Security Gateway and SmartConsole on the Security Management Server.
- D. SmartConsole or mgmt\_cli on any computer where SmartConsole is installed.

Answer: D

NEW QUESTION 245

Which directory holds the SmartLog index files by default?

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

Answer: A

NEW QUESTION 248

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.

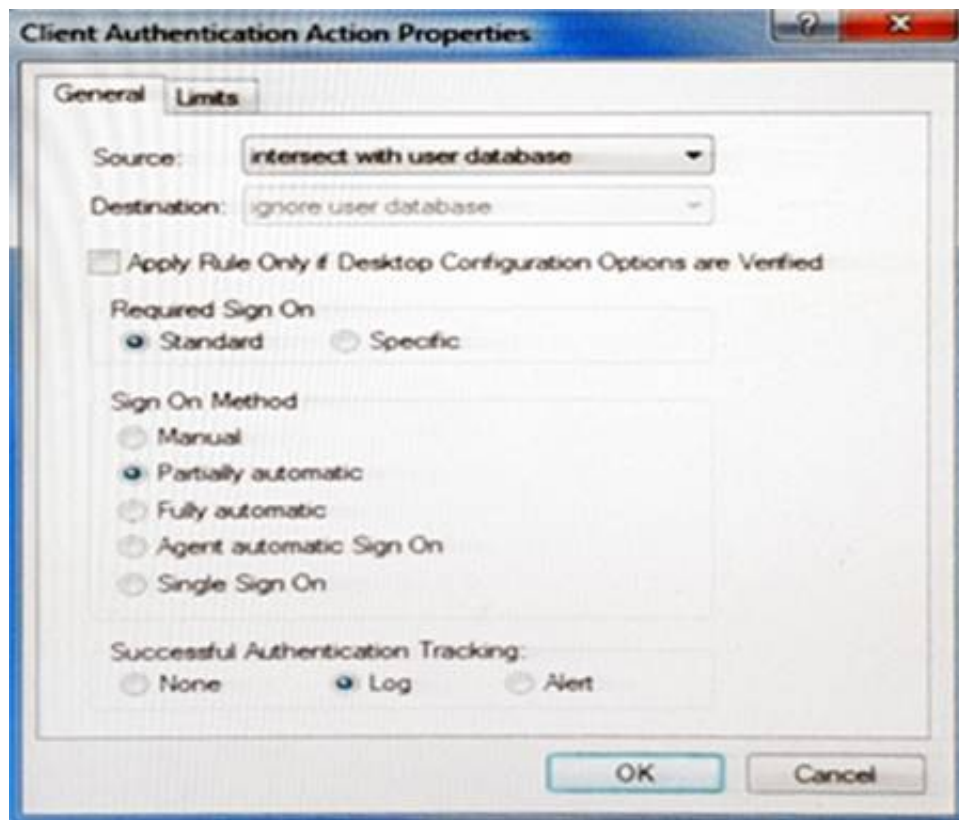
The ICA is located on the Security Management server. It is created during the installation process, when the Security Management server is configured.

NEW QUESTION 250

Study the Rule base and Client Authentication Action properties screen.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	http ftp telnet	Client Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	drop	Log	Policy Targets





After being authenticated by the Security Gateways, a user starts a HTTP connection to a Web site. What happens when the user tries to FTP to another site using the command line? The:

- A. user is prompted for authentication by the Security Gateways again.
- B. FTP data connection is dropped after the user is authenticated successfully.
- C. user is prompted to authenticate from that FTP site only, and does not need to enter his username and password for Client Authentication
- D. FTP connection is dropped by Rule 2.

**Answer: C**

#### NEW QUESTION 251

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 253

Joey is using the computer with IP address 192.168.20.13. He wants to access web page “www.Check Point.com”, which is hosted on Web server with IP address 203.0.113.111. How many rules on Check Point Firewall are required for this connection?

- A. Two rules – first one for the HTTP traffic and second one for DNS traffic.
- B. Only one rule, because Check Point firewall is a Packet Filtering firewall
- C. Two rules – one for outgoing request and second one for incoming replay.
- D. Only one rule, because Check Point firewall is using Stateful Inspection technology.

**Answer: D**

#### NEW QUESTION 256

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 258

Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?

- A. Firewall
- B. Identity Awareness
- C. Application Control
- D. URL Filtering

**Answer:** B

**Explanation:** Check Point Identity Awareness Software Blade provides granular visibility of users, groups and machines, providing unmatched application and access control through the creation of accurate, identity-based policies. Centralized management and monitoring allows for policies to be managed from a single, unified console.

#### NEW QUESTION 259

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 264

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

- A. assign privileges to users.
- B. edit the home directory of the user.
- C. add users to your Gaia system.
- D. assign user rights to their home directory in the Security Management Server

**Answer:** D

**Explanation:** Users

Use the WebUI and CLI to manage user accounts. You can:

Add users to your Gaia system.

Edit the home directory of the user.

Edit the default shell for a user.

Give a password to a user.

Give privileges to users.

#### NEW QUESTION 265

Which feature in R77 permits blocking specific IP addresses for a specified time period?

- A. Suspicious Activity Monitoring
- B. HTTP Methods
- C. Local Interface Spoofing
- D. Block Port Overflow

**Answer:** A

#### NEW QUESTION 268

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 272

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 273

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 275

Anti-Spoofing is typically set up on which object type?

- A. Security Gateway
- B. Host
- C. Security Management object
- D. Network

**Answer:** A

#### NEW QUESTION 279

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 283

What happens if the identity of a user is known?

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

**Answer:** D

#### NEW QUESTION 284

NAT can NOT be configured on which of the following objects?

- A. HTTP Logical Server
- B. Gateway
- C. Address Range
- D. Host

**Answer:** A

#### NEW QUESTION 286

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 291

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 296

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 301

What CLI utility allows an administrator to capture traffic along the firewall inspection chain?

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

**Answer:** D

#### NEW QUESTION 302

Fill in the blank: The R80 SmartConsole, SmartEvent GUI client, and \_\_\_\_\_ consolidate billions of logs and shows them as prioritized security events.

- A. SmartMonitor
- B. SmartView Web Application
- C. SmartReporter
- D. SmartTracker

**Answer:** B

**Explanation:** Event Analysis with SmartEvent

The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents, and do the necessary actions to prevent more attacks. You can customize the views to monitor the events that are most important to you. You can move from a high level view to detailed forensic analysis in a few clicks. With the free-text search and suggestions, you can quickly run data analysis and identify critical security events.

#### NEW QUESTION 306

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 307

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 308

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 310

Which of the following statements accurately describes the command snapshot?

- A. snapshot creates a full OS-level backup, including network-interface data, Check Point production information, and configuration settings of a GAiA Security Gateway.
- B. snapshot creates a Security Management Server full system-level backup on any OS
- C. snapshot stores only the system-configuration settings on the Gateway
- D. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server

**Answer:** A

#### NEW QUESTION 312

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 313

You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause?

- A. The POP3 rule is disabled.
- B. POP3 is accepted in Global Properties.
- C. The POP3 rule is hidden.
- D. POP3 is one of 3 services (POP3, IMAP, and SMTP) accepted by the default mail object in R77.

**Answer:** C

#### NEW QUESTION 315

The fw monitor utility is used to troubleshoot which of the following problems?

- A. Phase two key negotiation
- B. Address translation
- C. Log Consolidation Engine



D. User data base corruption

**Answer:** B

#### NEW QUESTION 318

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 322

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 323

Fill in the blank: Licenses can be added to the License and Contract repository \_\_\_\_\_.

- A. From the User Center, from a file, or manually
- B. From a file, manually, or from SmartView Monitor
- C. Manually, from SmartView Monitor, or from the User Center
- D. From SmartView Monitor, from the User Center, or from a file

**Answer:** A

#### NEW QUESTION 327

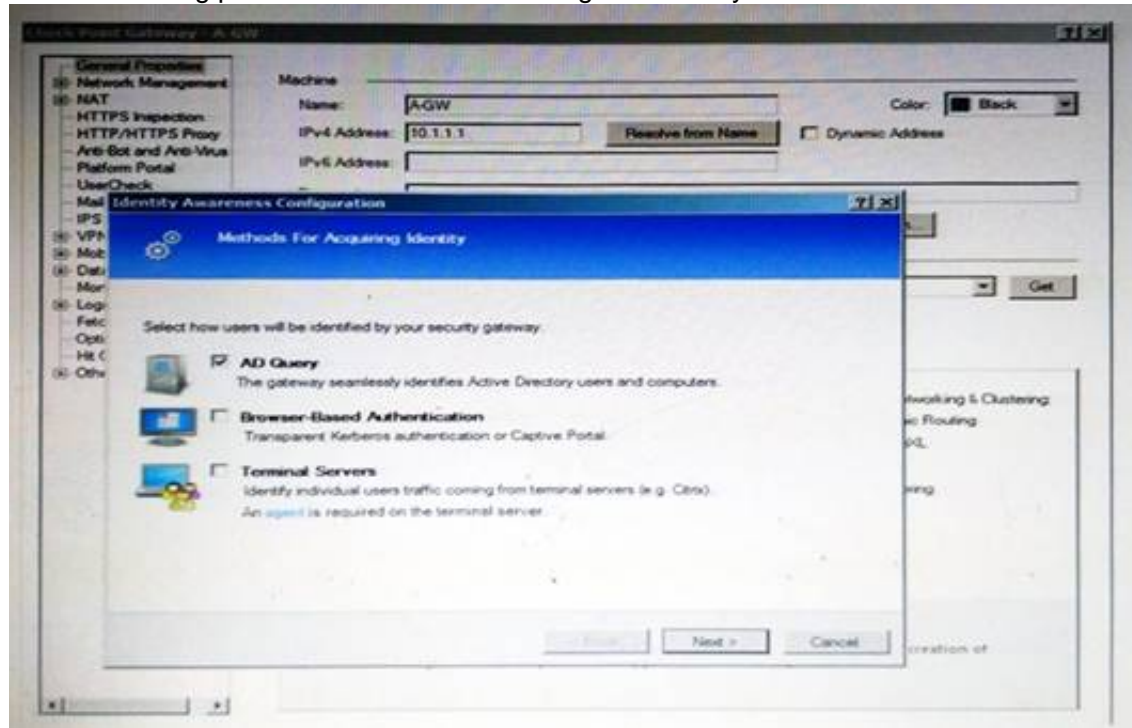
When using LDAP as an authentication method for Identity Awareness, the query:

- 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 332

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 337

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 339

Fill in the blank: The \_\_\_\_\_ feature allows administrators to share a policy with other policy packages.

- A. Shared policy packages
- B. Shared policies
- C. Concurrent policy packages
- D. Concurrent policies

**Answer:** A

#### NEW QUESTION 342

What port is used for delivering logs from the gateway to the management server?

- A. Port 258
- B. Port 18209
- C. Port 257
- D. Port 981

**Answer:** C

#### NEW QUESTION 343

Your bank's distributed R77 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

- A. SmartView Tracker
- B. SmartPortal
- C. SmartUpdate
- D. SmartDashboard

**Answer:** C

#### NEW QUESTION 347

How many users can have read/write access in Gaia at one time?

- A. Infinite
- B. One
- C. Three
- D. Two

**Answer:** B

#### NEW QUESTION 352

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:

name	ip v4-address	color
host1	192.168.35.1	black
host2	192.168.35.2	red
host3	192.168.35.3	blue

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 353

The organization's security manager wishes to back up just the Gaia operating system parameters. Which command can be used to back up only Gaia operating system parameters like interface details, Static routes and Proxy ARP entries?

- A. show configuration
- B. backup
- C. migrate export
- D. upgrade export

**Answer:** B

**Explanation:** 3. System Backup (and System Restore)

System Backup can be used to backup current system configuration. A backup creates a compressed file that contains the Check Point configuration including the networking and operating system parameters, such as routing and interface configuration etc., but unlike a snapshot, it does not include the operating system, product binaries, and hotfixes.

Topic 3, Exam Pool C

### NEW QUESTION 354

Your company enforces a strict change control policy. Which of the following would be MOST effective for quickly dropping an attacker's specific active connection?

- A. Change the Rule Base and install the Policy to all Security Gateways
- B. Block Intruder feature of SmartView Tracker
- C. Intrusion Detection System (IDS) Policy install
- D. SAM – Suspicious Activity Rules feature of SmartView Monitor

**Answer:** B

### NEW QUESTION 356

Which limitation of CoreXL is overcome by using (mitigated by) Multi-Queue?

- A. There is no traffic queue to be handled
- B. Several NICs can use one traffic queue by one CPU
- C. Each NIC has several traffic queues that are handled by multiple CPU cores
- D. Each NIC has one traffic queue that is handled by one CPU

**Answer:** C

### NEW QUESTION 361

What is the mechanism behind Threat Extraction?

- A. This is a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender
- B. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient
- C. This is a new mechanism to identify the IP address of the sender of malicious codes and to put it into the SAM database (Suspicious Activity Monitoring).
- D. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast

**Answer:** D

### NEW QUESTION 362

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

No.	Hits	Name	Source	Destination	VPN	Service	Action
Limit Access to Gateways (Rule 1)							
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
VPN Access Rules (Rules 2-5)							
2	0	Site-to-Site	Any	Any	Any Traffic	CIFS, ftp-port, http, https, smtp	accept
3	0	Remote Access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS, http, https, imap	accept
4	0	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA-proxy-server	Any Traffic	https	User Auth.
5	0	Web Server	L2TP-vpn-user@Any, Customers@Any	Remote-1-web-server	Any Traffic	http	accept

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

**Answer: B**

#### NEW QUESTION 367

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 368

What component of R80 Management is used for indexing?

- A. DBSync
- B. API Server
- C. fwm
- D. SOLR

**Answer: D**

#### NEW QUESTION 371

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 373

The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

- A. Secure Internal Communication (SIC)
- B. Restart Daemons if they fail
- C. Transfer messages between Firewall processes
- D. Pulls application monitoring status

**Answer: D**

#### NEW QUESTION 375

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 379

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 383

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 386

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 389

What is also referred to as Dynamic NAT?

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

**Answer:** D

#### NEW QUESTION 390

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 393

How do you configure the Security Policy to provide uses access to the Captive Portal through an external (Internet) interface?

- A. Change the gateway settings to allow Captive Portal access via an external interface.
- B. No action is necessar
- C. This access is available by default.
- D. Change the Identity Awareness settings under Global Properties to allow Captive Policy access on all interfaces.
- E. Change the Identity Awareness settings under Global Properties to allow Captive Policy access for an external interface.

**Answer:** A

#### NEW QUESTION 394

Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all of the following except:

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

**Answer:** A

#### NEW QUESTION 399

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 401

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 402

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 405

Review the rules. Assume domain UDP is enabled in the implied rules.

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

What happens when a user from the internal network tries to browse to the internet using HTTP? The user:

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

**Answer:** D

#### NEW QUESTION 410

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 414

Which remote Access Solution is clientless?

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

**Answer:** D

#### NEW QUESTION 415

How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

- A. Install appliance TE250X on SpanPort on LAN switch in MTA mode
- B. Install appliance TE250X in standalone mode and setup MTA
- C. You can utilize only Check Point Cloud Services for this scenario
- D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance

**Answer:** C

#### NEW QUESTION 420

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 421

Which of the following uses the same key to decrypt as it does to encrypt?

- A. Asymmetric encryption
- B. Dynamic encryption
- C. Certificate-based encryption
- D. Symmetric encryption

**Answer:** D

#### NEW QUESTION 422

What happens if the identity of a user is known?

- A. If the user credentials do not match an Access Role, the traffic is automatically dropped.
- B. If the user credentials do not match an Access Role, the system displays a sandbox.
- C. If the user credentials do not match an Access Role, the gateway moves onto the next rule.
- D. If the user credentials do not match an Access Role, the system displays the Captive Portal.

**Answer:** C

#### NEW QUESTION 425

Which the following type of authentication on Mobile Access can NOT be used as the first authentication method?

- A. Dynamic ID
- B. RADIUS
- C. Username and Password
- D. Certificate

**Answer:** A

#### NEW QUESTION 429

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 434

On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

- A. 18210
- B. 18184
- C. 257
- D. 18191

**Answer:** B

#### NEW QUESTION 439

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

- A. Manual copies of the directory \$FWDIR/conf
- B. upgrade\_export command
- C. Database Revision Control
- D. GAIa backup utilities

**Answer:** C

**NEW QUESTION 441**

You find that Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Choose the BEST reason why.

- A. You checked the cache password on desktop option in Global Properties.
- B. Another rule that accepts HTTP without authentication exists in the Rule Base.
- C. You have forgotten to place the User Authentication Rule before the Stealth Rule.
- D. Users must use the SecuRemote Client, to use the User Authentication Rule.

**Answer:** B

**NEW QUESTION 443**

There are 4 ways to use the Management API for creating host object with R80 Management API. Which one is NOT correct?

- A. Using Web Services
- B. Using Mgmt\_cli tool
- C. Using CLISH
- D. Using SmartConsole GUI console

**Answer:** C

**NEW QUESTION 445**

You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities sh you do first?

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

**Answer:** B

**NEW QUESTION 448**

Katie has been asked to do a backup on the Blue Security Gateway. Which command would accomplish this in the Gaia CLI?

- A. Blue > add local backup
- B. Expert&Blue#add local backing
- C. Blue > set backup local
- D. Blue > add backup local

**Answer:** D

**NEW QUESTION 450**

What is the command to see cluster status in cli expert mode?

- A. fw ctl stat
- B. clusterXL stat
- C. clusterXL status
- D. cphaprob stat

**Answer:** A

**NEW QUESTION 455**

Using mgmt\_cli, what is the correct syntax to import a host object called Server\_1 from the CLI?

- A. mgmt\_cli add-host "Server\_1" ip\_address "10.15.123.10" --format txt
- B. mgmt\_cli add host name "Server\_1" ip\_address "10.15.123.10" --format json
- C. mgmt\_cli add object-host "Server\_1" ip\_address "10.15.123.10" --format json
- D. mgmt\_cli add object "Server\_1" ip\_address "10.15.123.10" --format json

**Answer:** A

**NEW QUESTION 459**

Where would an administrator enable Implied Rules logging?

- A. In Smart Log Rules View
- B. In SmartDashboard on each rule
- C. In Global Properties under Firewall
- D. In Global Properties under log and alert

**Answer:** B

**NEW QUESTION 462**



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 463

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

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

**Answer: D**

#### NEW QUESTION 467

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 470

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 474

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 476

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 481

Which NAT rules are prioritized first?

- A. Post-Automatic/Manual NAT rules
- B. Manual/Pre-Automatic NAT
- C. Automatic Hide NAT
- D. Automatic Static NAT

**Answer: B**

#### NEW QUESTION 485

Which of the following is a hash algorithm?

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

**Answer:** D

#### NEW QUESTION 489

Which component functions as the Internal Certificate Authority for R77?

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

**Answer:** B

#### NEW QUESTION 491

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 492

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 497

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

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

**Answer:** C

#### NEW QUESTION 498

What is the purpose of Priority Delta in VRRP?

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

**Answer:** C

#### NEW QUESTION 499

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 500

Which of these attributes would be critical for a site-to-site VPN?

- A. Scalability to accommodate user groups
- B. Centralized management
- C. Strong authentication
- D. Strong data encryption

**Answer: D**

#### NEW QUESTION 503

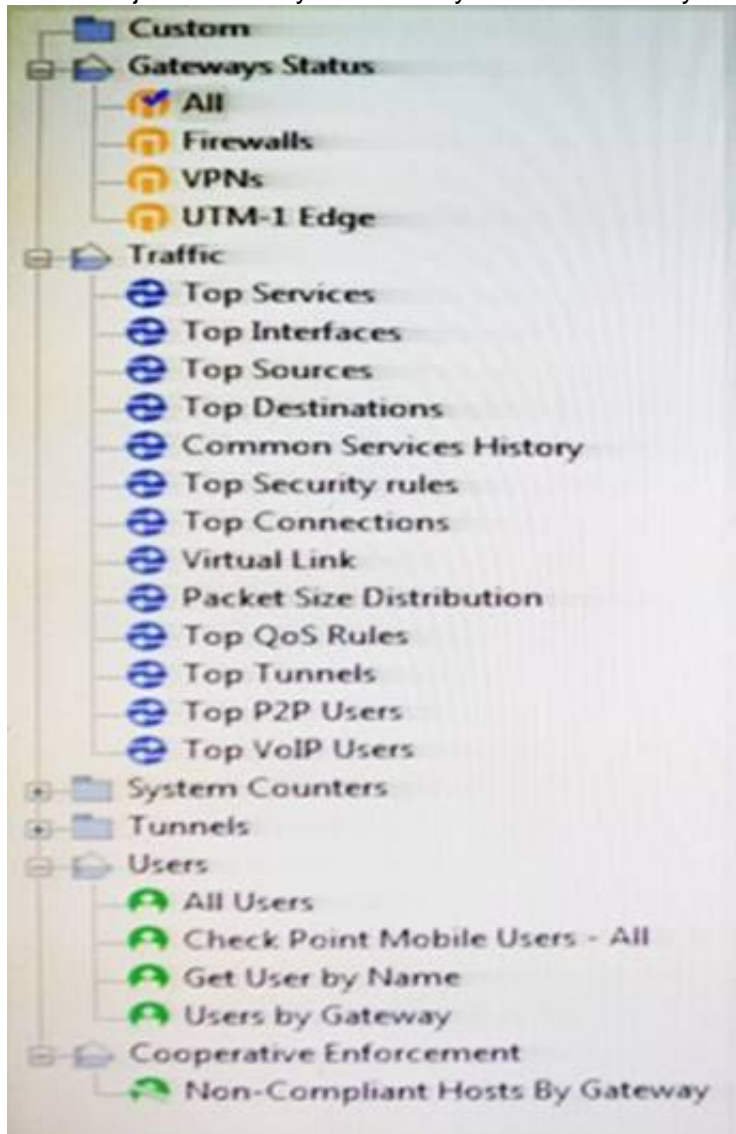
What happens when you run the command: fw sam -J src [Source IP Address]?

- A. Connections from the specified source are blocked without the need to change the Security Policy.
- B. Connections to the specified target are blocked without the need to change the Security Policy.
- C. Connections to and from the specified target are blocked without the need to change the Security Policy.
- D. Connections to and from the specified target are blocked with the need to change the Security Policy.

**Answer: A**

#### NEW QUESTION 504

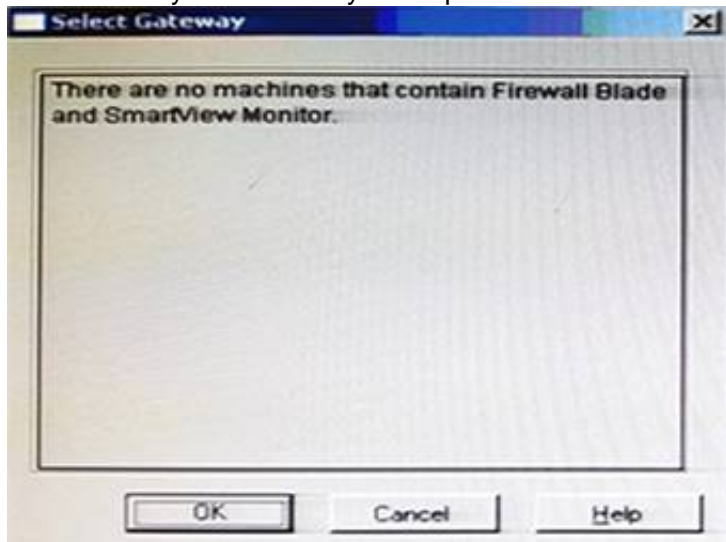
You have just installed your Gateway and want to analyze the packet size distribution of your traffic with SmartView Monitor.



Unfortunately, you get the message:

“There are no machines that contain Firewall Blade and SmartView Monitor”.

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



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

**Answer: D**

#### NEW QUESTION 507

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

**Explanation:** Topic 4, Exam Pool D

#### NEW QUESTION 510

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 513

What key is used to save the current CPView page in a filename format cpview\_"cpview process ID".cap"number of captures"?

- A. S
- B. W
- C. C
- D. Space bar

**Answer:** B

#### NEW QUESTION 515

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 520

How are the backups stored in Chock Point appliances?

- A. Saved as \*.tar under /var/log/Cpbackup/backups
- B. Saved as \*.tgz under /var/cppbackup
- C. Saved as \*.tar under /var/cppbackup
- D. Saved as \*.tgz under /var/log/CPbackup/backups

**Answer:** D

#### NEW QUESTION 522

To enforce the Security Policy correctly, a Security Gateway requires:

- A. a routing table
- B. awareness of the network topology
- C. a Demilitarized Zone
- D. a Security Policy install

**Answer:** B

**Explanation:** The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:

- Correctly enforce the Security Policy.
- Ensure the validity of IP addresses for inbound and outbound traffic.
- Configure a special domain for Virtual Private Networks.

#### NEW QUESTION 525



R80.10 management server can manage gateways with which versions installed?

- A. Versions R77 and higher
- B. Versions R76 and higher
- C. Versions R75.20 and higher
- D. Version R75 and higher

**Answer: B**

#### NEW QUESTION 527

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

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

**Answer: D**

#### NEW QUESTION 531

What is a reason for manual creation of a NAT rule?

- A. In R80 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
- B. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.
- C. Network Address Translation is desired for some services, but not for others.
- D. The public IP-address is different from the gateway's external IP

**Answer: D**

#### NEW QUESTION 536

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 539

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 544

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 547

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 551

What needs to be configured if the NAT property 'Translate destination on client side' is not enabled in Global properties?

- A. A host route to route to the destination IP
- B. Use the file local.arp to add the ARP entries for NAT to work
- C. Nothing, the Gateway takes care of all details necessary
- D. Enabling 'Allow bi-directional NAT' for NAT to work correctly

**Answer:** C

**NEW QUESTION 552**

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 554**

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

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

**Answer:** C

**NEW QUESTION 559**

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 563**

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 564**

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 565**

Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

- A. SmartManager
- B. SmartConsole
- C. Security Gateway
- D. Security Management Server

**Answer:** C

**NEW QUESTION 568**

Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays \_\_\_\_ for the given VPN tunnel.

- A. Down
- B. No Response
- C. Inactive
- D. Failed

**Answer:** A

**NEW QUESTION 573**

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 575**

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 579**

Which back up utility captures the most information and tends to create the largest archives?

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

**Answer:** B

**NEW QUESTION 582**

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 586**

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 590**

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

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

**Answer:** B

**NEW QUESTION 591**

When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:

- A. Only the objects being modified in the Management Database and other administrators can connect to make changes using a special session as long as they all connect from the same LAN network.
- B. The entire Management Database and other administrators can connect to make changes only if the first administrator switches to Read-only.
- C. The entire Management Database and all sessions and other administrators can connect only as Read-only.
- D. Only the objects being modified in his session of the Management Database and other administrators can connect to make changes using different sessions.

**Answer:** D

#### NEW QUESTION 593

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 594

Which of the following is NOT an option to calculate the traffic direction?

- A. Incoming
- B. Internal
- C. External
- D. Outgoing

**Answer:** D

#### NEW QUESTION 599

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 601

The SIC Status “Unknown” means

- A. There is connection between the gateway and Security Management Server but it is not trusted.
- B. The secure communication is established.
- C. There is no connection between the gateway and Security Management Server.
- D. The Security Management Server can contact the gateway, but cannot establish SIC.

**Answer:** AC

**Explanation:** After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:

Communicating - The secure communication is established.

Unknown - There is no connection between the gateway and Security Management Server.

Not Communicating - The Security Management Server can contact the gateway, but cannot establish SIC. A message shows more information.

#### NEW QUESTION 603

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 608

How would you determine the software version from the CLI?

- A. fw ver
- B. fw stat
- C. fw monitor
- D. cpinfo

**Answer:** A

#### NEW QUESTION 610

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

- A. Go to clash-Run cpstop | Run cpstart
- B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
- C. Administrator does not need to perform any tas
- D. Check Point will make use of the newly installed CPU and Cores
- E. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy



**Answer:** B

**NEW QUESTION 613**

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 616**

Which Threat Prevention Profile is not included by default in R80 Management?

- A. Basic – Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance
- B. Optimized – Provides excellent protection for common network products and protocols against recent or popular attacks
- C. Strict – Provides a wide coverage for all products and protocols, with impact on network performance
- D. Recommended – Provides all protection for all common network products and servers, with impact on network performance

**Answer:** D

**NEW QUESTION 620**

What is true about the IPS-Blade?

- A. in R80, IPS is managed by the Threat Prevention Policy
- B. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
- C. in R80, IPS Exceptions cannot be attached to “all rules”
- D. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

**Answer:** A

**NEW QUESTION 621**

What is the best sync method in the ClusterXL deployment?

- A. Use 1 cluster + 1st sync
- B. Use 1 dedicated sync interface
- C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
- D. Use 2 clusters + 1st sync + 2nd sync

**Answer:** B

**NEW QUESTION 626**

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 630**

Fill the blank. IT is Best Practice to have a \_\_\_\_\_ rule at the end of each policy layer.

- A. Explicit Drop
- B. Implied Drop
- C. Explicit Cleanup
- D. Implicit Drop

**Answer:** A

**NEW QUESTION 632**

John is using Management HA. Which Smartcenter should be connected to for making changes?

- A. secondary Smartcenter
- B. active Smartcenter
- C. connect virtual IP of Smartcenter HA
- D. primary Smartcenter

**Answer:** B

**NEW QUESTION 637**

Fill in the blank: To create policy for traffic to or from a particular location, use the\_\_\_\_\_ .

- A. DLP shared policy
- B. Geo policy shared policy
- C. Mobile Access software blade
- D. HTTPS inspection

**Answer:** B

**Explanation:** Shared Policies

The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. They are shared between all Policy packages.

Shared policies are installed with the Access Control Policy. Software Blade

Description Mobile Access

Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.

DLP Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.

Geo Policy

Create a policy for traffic to or from specific geographical or political locations. References:

#### NEW QUESTION 639

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 640

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 645

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 648

Which command shows the installed licenses?

- A. cplic print
- B. print cplic
- C. fwlic print
- D. show licenses

**Answer:** A

#### NEW QUESTION 649

What SmartEvent component creates events?

- A. Consolidation Policy
- B. Correlation Unit
- C. SmartEvent Policy
- D. SmartEvent GUI

**Answer:** B

#### NEW QUESTION 651

Fill in the blanks. There are \_\_\_\_\_ types of software containers \_\_\_\_\_

- A. Three; security management
- B. Security Gateway and endpoint security.
- C. Three; Security Gateway, endpoint Security, and gateway management.
- D. Two; security management and endpoint security
- E. Two; endpoint security and Security Gateway

**Answer:** A

**NEW QUESTION 655**

When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

- A. Distributed
- B. Standalone
- C. Bridge

**Answer:** A

**NEW QUESTION 659**

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 664**

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 665**

You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

- A. restore\_backup
- B. import backup
- C. cp\_merge
- D. migrate import

**Answer:** A

**NEW QUESTION 666**

Fill in the blank; The position of an Implied rule is manipulated in the \_\_\_\_\_ window

- A. NAT
- B. Firewall
- C. Global Properties
- D. Object Explorer

**Answer:** C

**NEW QUESTION 667**

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 671**

Access roles allow the firewall administrator to configure Network access according to:

- A. a combination of computer or computer groups and network
- B. users and user groups
- C. all of above
- D. remote access clients

**Answer:** C

**NEW QUESTION 676**

When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

- A. Any size
- B. Less than 20GB
- C. More than 10GB and less than 20 GB
- D. At least 20GB

**Answer:** D

**NEW QUESTION 679**

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 681**

Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?

- A. All options stop Check Point processes
- B. backup
- C. migrate export
- D. snapshot

**Answer:** D

**NEW QUESTION 683**

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 688**

You have discovered activity in your network. What is the BEST immediate action to take?

- A. Create a policy rule to block the traffic.
- B. Create a suspicious action rule to block that traffic.
- C. Wait until traffic has been identified before making any changes.
- D. Contact ISP to block the traffic.

**Answer:** B

**NEW QUESTION 691**

Which repositories are installed on the Security Management Server by SmartUpdate?

- A. License and Update
- B. Package Repository and Licenses
- C. Update and License and Contract
- D. License and Contract and Package Repository

**Answer:** D

**NEW QUESTION 694**

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 698**

Fill in the blank: In order to install a license, it must first be added to the \_\_\_\_\_. .



- A. User Center
- B. Package repository
- C. Download Center Web site
- D. License and Contract repository

**Answer:** B

**NEW QUESTION 700**

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 705**

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 708**

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 709**

In the Check Point Security Management Architecture, which component(s) can store logs?

- A. SmartConsole
- B. Security Management Server and Security Gateway
- C. Security Management Server
- D. SmartConsole and Security Management Server

**Answer:** B

**NEW QUESTION 711**

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 712**

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 714**

Phase 1 of the two-phase negotiation process conducted by IKE operates in a \_\_\_\_\_ mode.

- A. Main
- B. Authentication
- C. Quick
- D. High Alert

**Answer:** A

**NEW QUESTION 716**

You want to verify if there are unsaved changes in GAIa that will be lost with a reboot. What command can be used?

- A. show unsaved
- B. show save-state
- C. show configuration diff
- D. show config-state

**Answer:** D

**NEW QUESTION 717**

Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

- A. ThreatWiki
- B. Whitelist Files
- C. AppWiki
- D. IPS Protections

**Answer:** A

**NEW QUESTION 719**

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 724**

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 727**

Fill in the blank: An identity server uses a \_\_\_\_\_ for user authentication.

- A. Shared secret
- B. Certificate
- C. One-time password
- D. Token

**Answer:** A

**NEW QUESTION 728**

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 730**

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 734**

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 739**

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 743**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### 156-215.80 Practice Exam Features:

- \* 156-215.80 Questions and Answers Updated Frequently
- \* 156-215.80 Practice Questions Verified by Expert Senior Certified Staff
- \* 156-215.80 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 156-215.80 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 156-215.80 Practice Test Here](#)**