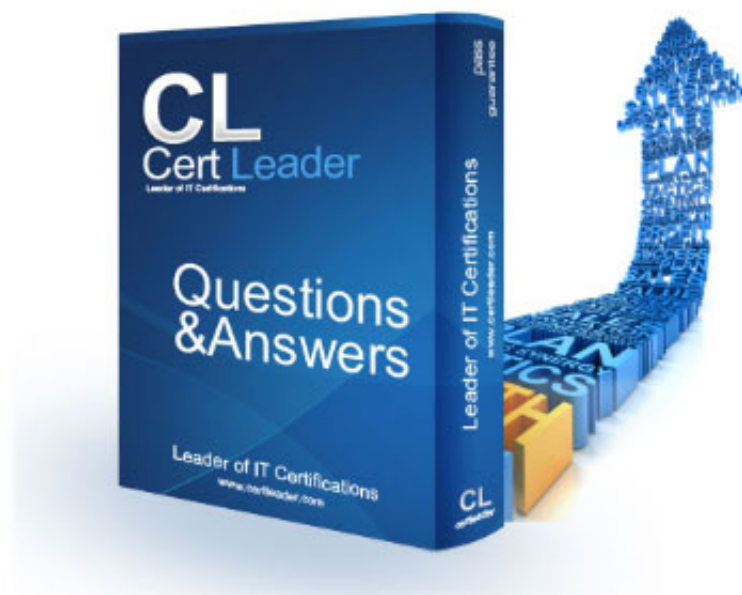


## 156-215.80 Dumps

### Check Point Certified Security Administrator

<https://www.certleader.com/156-215.80-dumps.html>



### NEW QUESTION 1

- (Exam Topic 1)

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

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

**Answer: C**

#### Explanation:

Sysconfig Configuration Options

	Menu Item	Purpose
7	DHCP Server Configuration	Configure SecurePlatform DHCP Server.
8	DHCP Relay Configuration	Setup DHCP Relay.

### NEW QUESTION 2

- (Exam Topic 1)

The Gaia operating system supports which routing protocols?

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

**Answer: A**

#### Explanation:

The Advanced Routing Suite

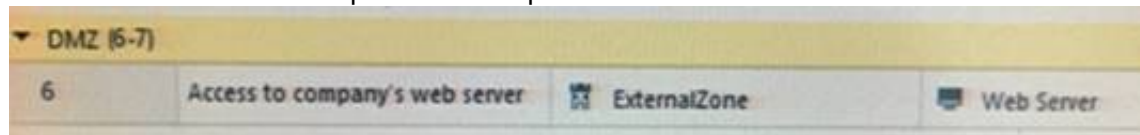
The Advanced Routing Suite CLI is available as part of the Advanced Networking Software Blade.

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

### NEW QUESTION 3

- (Exam Topic 1)

What does ExternalZone represent in the presented rule?



- A. The Internet.
- B. Interfaces that administrator has defined to be part of External Security Zone.
- C. External interfaces on all security gateways.
- D. External interfaces of specific gateways.

**Answer: B**

#### Explanation:

Configuring Interfaces

Configure the Security Gateway 80 interfaces in the Interfaces tab in the Security Gateway window. To configure the interfaces:

From the Devices window, double-click the Security Gateway 80.

The Security Gateway window opens.

Select the Interfaces tab.

Select Use the following settings. The interface settings open.

Select the interface and click Edit.

The Edit window opens.

From the IP Assignment section, configure the IP address of the interface:

Select Static IP.

Enter the IP address and subnet mask for the interface.

In Security Zone, select Wireless, DMS, External, or Internal. Security zone is a type of zone, created by a bridge to easily create segments, while maintaining IP addresses and router configurations. Security zones let you choose if to enable or not the firewall between segments.

References:

**NEW QUESTION 4**

- (Exam Topic 1)

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 5**

- (Exam Topic 1)

Vanessa is firewall administrator in her company; her company is using Check Point firewalls on central and remote locations, which are managed centrally by R80 Security Management Server. One central location has an installed R77.30 Gateway on Open server. Remote location is using Check Point UTM-1 570 series appliance with R71. Which encryption is used in Secure Internal Communication (SIC) between central management and firewall on each location?

- A. On central firewall AES128 encryption is used for SIC, on Remote firewall 3DES encryption is used for SIC.
- B. On both firewalls, the same encryption is used for SI
- C. This is AES-GCM-256.
- D. The Firewall Administrator can choose which encryption suite will be used by SIC.
- E. On central firewall AES256 encryption is used for SIC, on Remote firewall AES128 encryption is used for SIC.

**Answer:** A

**Explanation:**

Gateways above R71 use AES128 for SIC. If one of the gateways is R71 or below, the gateways use 3DES.

**NEW QUESTION 6**

- (Exam Topic 1)

Fill in the blank: To build an effective Security Policy, use a \_\_\_\_\_ and \_\_\_\_\_ rule.

- A. Cleanup; stealth
- B. Stealth; implicit
- C. Cleanup; default
- D. Implicit; explicit

**Answer:** A

**NEW QUESTION 7**

- (Exam Topic 1)

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:**

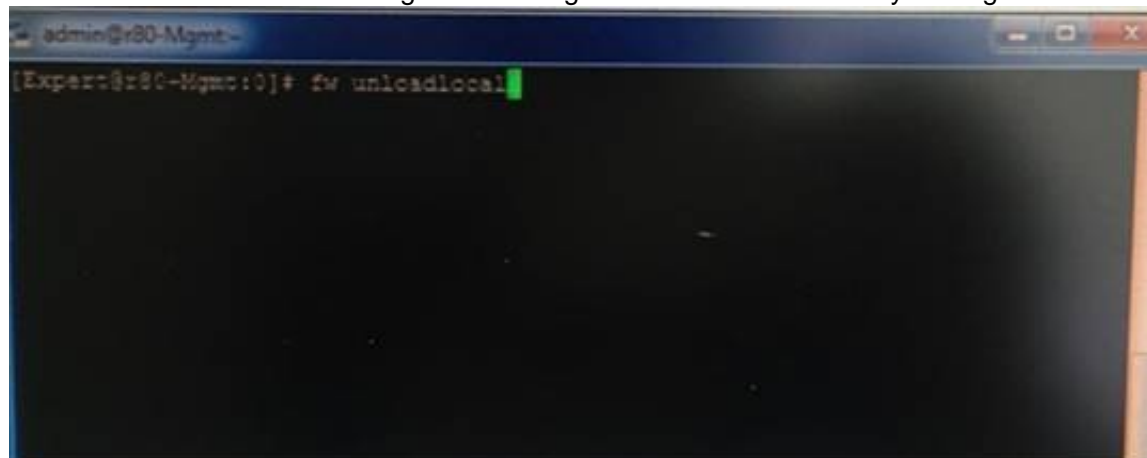
Captive Portal – a simple method that authenticates users through a web interface before granting them access to Intranet resources. When users try to access a protected resource, they get a web page that must be filled out to continue.

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

**NEW QUESTION 8**

- (Exam Topic 1)

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



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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 9**

- (Exam Topic 1)

Which type of the Check Point license ties the package license to the IP address of the Security Management Server?

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

**Answer:** B

**NEW QUESTION 10**

- (Exam Topic 1)

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

- A. remove database lock
- B. The database feature has one command lock database override.
- C. override database lock
- D. The database feature has two commands: lock database override and unlock databas
- E. Both will work.

**Answer:** D

**Explanation:**

Use the database feature to obtain the configuration lock. The database feature has two commands:

lock database [override].

unlock database

The commands do the same thing: obtain the configuration lock from another administrator.

<b>Description</b>	Use the lock database override and unlock database commands to get exclusive read-write access to the database by taking write privileges to the database away from other administrators logged into the system.
<b>Syntax</b>	<ul style="list-style-type: none"> <li>o lock database override</li> <li>o unlock database</li> </ul>

**NEW QUESTION 10**

- (Exam Topic 1)

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 13**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

(Should be "migrate import")

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

**NEW QUESTION 16**

- (Exam Topic 1)

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 20**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 22**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 26**

- (Exam Topic 1)

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 29**

- (Exam Topic 1)

Fill in the blank: The R80 feature \_\_\_\_\_ permits blocking specific IP addresses for a specified time period.

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

**Answer:** C

**Explanation:**

Suspicious Activity Rules Solution

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

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



### NEW QUESTION 33

- (Exam Topic 1)

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 36

- (Exam Topic 1)

You are the administrator for ABC Corp. You have logged into your R80 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Name	* Any	* Any	* Any	NetBIOS	Drop	None	Policy Targets
2	Management	Net_10.25.0.0	10.10.0.77/8	* Any	HTTPS, ssh	Accept	Log	Policy Targets
3	Traffic	* Any	10.10.0.77/8	* Any	* Any	Drop	Log	Policy Targets
4	DMZ	Net_10.25.0.0	* Any	* Any	80, 443	Accept	Log	Policy Targets
5	Web	Net_10.25.0.0	* Any	* Any	80, 443	Accept	Log	Policy Targets
6	DMZ Access	Net_10.25.0.0	DMZ_Net_10.10.0.0	* Any	Any	Accept	Log	Policy Targets
7	Outgoing	* Any	* Any	* Any	* Any	Drop	Log	Policy Targets

What does this mean?

- A. The rule No.6 has been marked for deletion in your Management session.
- B. The rule No.6 has been marked for deletion in another Management session.
- C. The rule No.6 has been marked for editing in your Management session.
- D. The rule No.6 has been marked for editing in another Management session.

**Answer:** C

### NEW QUESTION 40

- (Exam Topic 1)

What are the two types of address translation rules?

- A. Translated packet and untranslated packet
- B. Untranslated packet and manipulated packet
- C. Manipulated packet and original packet
- D. Original packet and translated packet

**Answer:** D

#### Explanation:

NAT Rule Base

The NAT Rule Base has two sections that specify how the IP addresses are translated:

Original Packet

Translated Packet References:

### NEW QUESTION 44

- (Exam Topic 2)

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 46

- (Exam Topic 2)

Which of the following is NOT an element of VPN Simplified Mode and VPN Communities?

- A. "Encrypt" action in the Rule Base
- B. Permanent Tunnels
- C. "VPN" column in the Rule Base
- D. Configuration checkbox "Accept all encrypted traffic"

**Answer:** A

#### Explanation:

Migrating from Traditional Mode to Simplified Mode

To migrate from Traditional Mode VPN to Simplified Mode:

1. On the Global Properties > VPN page, select one of these options:
  - Simplified mode to all new Firewall Policies
  - Traditional or Simplified per new Firewall Policy
2. Click OK.
3. From the R80 SmartConsole Menu, select Manage policies. The Manage Policies window opens.
4. Click New.

The New Policy window opens.

5. Give a name to the new policy and select Access Control.

In the Security Policy Rule Base, a new column marked VPN shows and the Encrypt option is no longer available in the Action column. You are now working in Simplified Mode.

#### NEW QUESTION 51

- (Exam Topic 2)

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

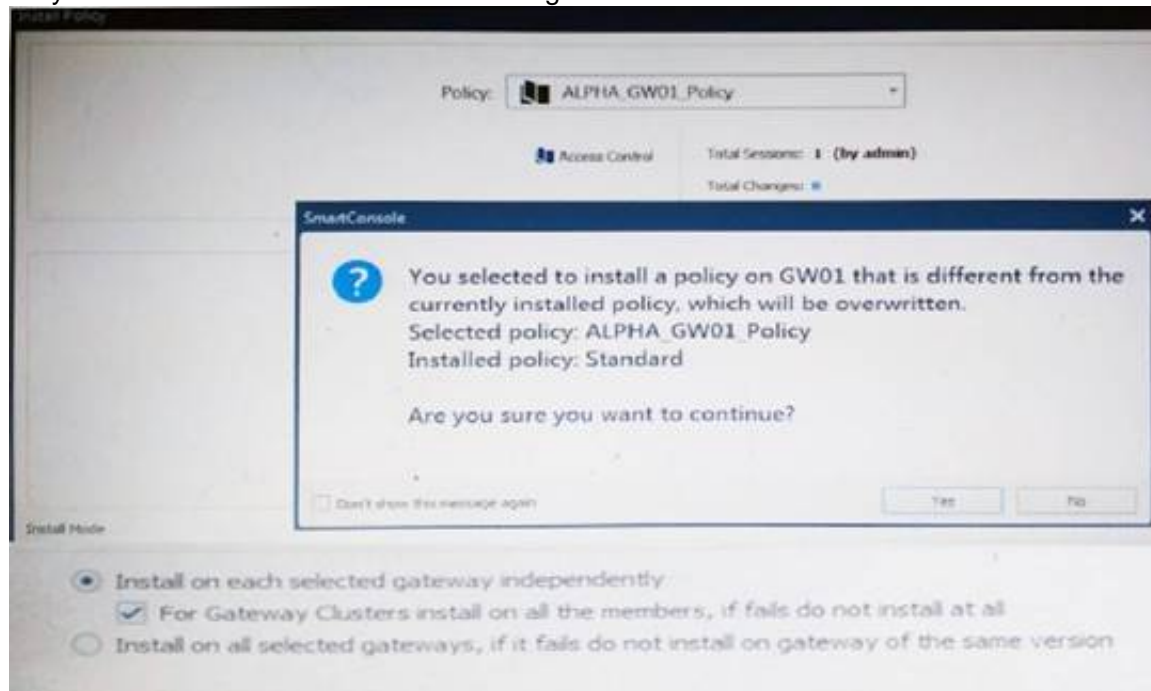
- A. SmartDashboard > Edit Gateway Object > General Properties > Communication
- B. SmartUpdate > Edit Security Management Server Object > SIC
- C. SmartUpdate > Edit Gateway Object > Communication
- D. SmartDashboard > Edit Security Management Server Object > SIC

**Answer: A**

#### NEW QUESTION 53

- (Exam Topic 2)

Why would an administrator see the message below?



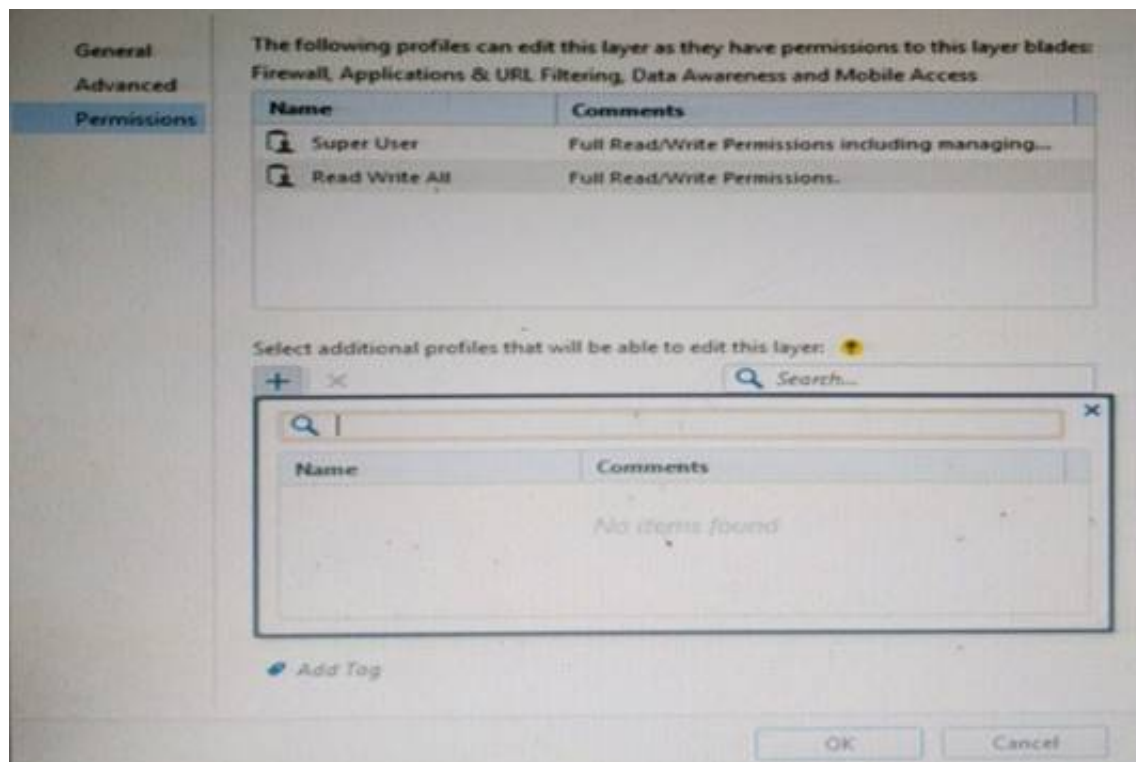
- A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed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

**Answer: B**

#### NEW QUESTION 55

- (Exam Topic 2)

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



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

**Answer:** B

#### NEW QUESTION 56

- (Exam Topic 2)

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 59

- (Exam Topic 2)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 62

- (Exam Topic 2)

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 66

- (Exam Topic 2)

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



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

**Answer:** B

**Explanation:**

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

Software Blades  
Container

**NEW QUESTION 71**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

Introduction to the ICA

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

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

**NEW QUESTION 72**

- (Exam Topic 2)

Choose the SmartLog property that is TRUE.

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

**Answer:** D

**NEW QUESTION 73**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

How RADIUS Accounting Works with Identity Awareness

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

**NEW QUESTION 78**

- (Exam Topic 2)

The Captive Portal tool:

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

**Answer:** A

**NEW QUESTION 79**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 83**

- (Exam Topic 2)

The IT Management team is interested in the new features of the Check Point R80 Management and wants to upgrade but they are concerned that the existing R77.30 Gaia Gateways cannot be managed by R80 because it is so different. As the administrator responsible for the Firewalls, how can you answer or confirm these concerns?

- A. R80 Management contains compatibility packages for managing earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.
- B. R80 Management requires the separate installation of compatibility hotfix packages for managing the earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.
- C. R80 Management was designed as a completely different Management system and so can only monitor Check Point Gateways prior to R80.
- D. R80 Management cannot manage earlier versions of Check Point Gateways prior to R80. Only R80 and above Gateways can be manage
- E. Consult the R80 Release Notes for more information.

**Answer:** A

**NEW QUESTION 86**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

Site to Site VPN

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

**NEW QUESTION 87**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

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

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

If suppression is not selected, it generates a complete log (as defined in pre-R80 management).

If suppression is selected, it generates an extended log(as defined in pre-R80 management).

None - Do not generate a log.

**NEW QUESTION 89**

- (Exam Topic 2)

Which type of Endpoint Identity Agent includes packet tagging and computer authentication?

- A. Full
- B. Light
- C. Custom
- D. Complete

**Answer:** A

**Explanation:**

Endpoint Identity Agents – dedicated client agents installed on users’ computers that acquire and report identities to the Security Gateway.

**NEW QUESTION 94**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 98**

- (Exam Topic 3)

A Cleanup rule:

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

**Answer:** A

**NEW QUESTION 102**

- (Exam Topic 3)

Choose the correct statement regarding Implicit Rules.

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

**Answer:** A

**NEW QUESTION 105**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 107**

- (Exam Topic 3)

How do you configure the Security Policy to provide users 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 necessary
- 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 110**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 113**

- (Exam Topic 3)

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 116**

- (Exam Topic 3)

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

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his desktop with a static IP (10.0.0.19). He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator:

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

What should John request when he cannot access the web server from his laptop?

- A. John should lock and unlock his computer
- B. Investigate this as a network connectivity issue
- C. The access should be changed to authenticate the user instead of the PC
- D. John should install the Identity Awareness Agent

**Answer: C**

**NEW QUESTION 120**

- (Exam Topic 3)

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 124**

- (Exam Topic 3)

A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

- A. Secure Internal Communications (SIC) not configured for the object.
- B. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.
- C. Anti-spoofing not configured on the interfaces on the Gateway object.
- D. A Gateway object created using the Check Point > Secure Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

**Answer: B**

**NEW QUESTION 126**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 131**

- (Exam Topic 3)

The technical-support department has a requirement to access an intranet server. When configuring a User Authentication rule to achieve this, which of the following should you remember?

- A. You can only use the rule for Telnet, FTP, SMTP, and rlogin services.
- B. The Security Gateway first checks if there is any rule that does not require authentication for this type of connection before invoking the Authentication Security Server.
- C. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.
- D. You can limit the authentication attempts in the User Properties' Authentication tab.

**Answer: B**

**NEW QUESTION 135**

- (Exam Topic 3)

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

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



**Answer:** D

**NEW QUESTION 136**

- (Exam Topic 3)

What is the Manual Client Authentication TELNET port?

- A. 23
- B. 264
- C. 900
- D. 259

**Answer:** D

**NEW QUESTION 140**

- (Exam Topic 3)

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 142**

- (Exam Topic 3)

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

URL List Version	<input type="checkbox"/>	100
Unreachable directories	<input type="checkbox"/>	100
Update Service	<input type="checkbox"/>	100
Update Source	<input type="checkbox"/>	100
Update Status	<input type="checkbox"/>	100
User Action Comment	<input type="checkbox"/>	100
User Additional Information	<input type="checkbox"/>	100
User Check	<input type="checkbox"/>	100
User DN	<input type="checkbox"/>	100
User Directory	<input type="checkbox"/>	100
User Display Name	<input type="checkbox"/>	100
User Group	<input type="checkbox"/>	100
User Reported Wrong Category	<input type="checkbox"/>	100
User Response	<input type="checkbox"/>	100
User SID	<input type="checkbox"/>	100
User UID	<input type="checkbox"/>	100
User's IP	<input type="checkbox"/>	100
UserCheck ID	<input type="checkbox"/>	100
UserCheck Interaction Name	<input type="checkbox"/>	100
UserCheck Message to User	<input type="checkbox"/>	100
UserCheck Scope	<input type="checkbox"/>	100
UserCheck User Input	<input type="checkbox"/>	100
VLAN ID	<input type="checkbox"/>	100
VPN Feature	<input type="checkbox"/>	100
VPN Peer Gateway	<input type="checkbox"/>	100
Version	<input type="checkbox"/>	100
Virtual Link	<input type="checkbox"/>	100
Virus Name	<input type="checkbox"/>	100
VoIP Duration	<input type="checkbox"/>	100
VoIP Log Type	<input type="checkbox"/>	100
VoIP Reject Reason	<input type="checkbox"/>	100
VoIP Reject Reason Information	<input type="checkbox"/>	100
Web Filtering Categories	<input type="checkbox"/>	100
Wire Byte/Sec Out	<input type="checkbox"/>	100
Wire Byte/Sec in	<input type="checkbox"/>	100
Wire Packet/Sec Out	<input type="checkbox"/>	100
Wire Packet/Sec in	<input type="checkbox"/>	100
Write Access	<input type="checkbox"/>	100
XlateDPort	<input type="checkbox"/>	100
XlateDst	<input type="checkbox"/>	100
XlateSPort	<input type="checkbox"/>	100
XlateSrc	<input type="checkbox"/>	100
Special properties	<input type="checkbox"/>	100

A. XlateDst



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

**Answer:** B

#### NEW QUESTION 143

- (Exam Topic 3)

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

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

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

**Answer:** C

#### NEW QUESTION 145

- (Exam Topic 3)

VPN gateways must authenticate to each other prior to exchanging information. What are the two types of credentials used for authentication?

- A. 3DES and MD5
- B. Certificates and IPsec
- C. Certificates and pre-shared secret
- D. IPsec and VPN Domains

**Answer:** C

#### NEW QUESTION 146

- (Exam Topic 3)

Which one of the following is true about Threat Extraction?

- A. Always delivers a file to user
- B. Works on all MS Office, Executables, and PDF files
- C. Can take up to 3 minutes to complete
- D. Delivers file only if no threats found

**Answer:** B

#### NEW QUESTION 149

- (Exam Topic 3)

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 150

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 151

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 155**

- (Exam Topic 3)

All R77 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

- A. FTP
- B. SMTP
- C. HTTP
- D. RLOGIN

**Answer:** B

**NEW QUESTION 160**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 164**

- (Exam Topic 4)

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 168**

- (Exam Topic 4)

You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

**Answer:** B

**NEW QUESTION 169**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 172**

- (Exam Topic 4)

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

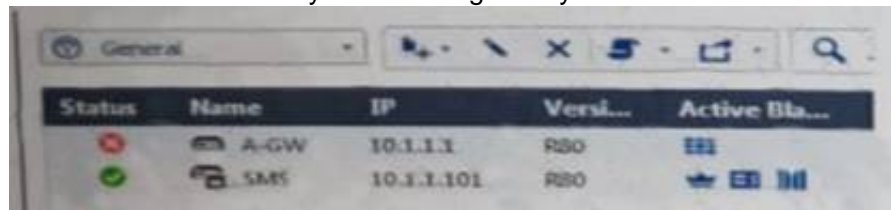
- A. ADQuery
- B. Terminal Servers Endpoint Identity Agent
- C. Endpoint Identity Agent and Browser-Based Authentication
- D. RADIUS and Account Logon

**Answer:** D

**NEW QUESTION 176**

- (Exam Topic 4)

What does it mean if Deyra sees the gateway status



Choose the BEST answer.

- A. SmartCenter Server cannot reach this Security Gateway
- B. There is a blade reporting a problem
- C. VPN software blade is reporting a malfunction
- D. Security Gateway s MGNT NIC card is disconnected

**Answer:** A

#### NEW QUESTION 181

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 186

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 188

- (Exam Topic 4)

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

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	NT	Drop	- None	Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	* Any	https, ssh	Accept	Log	Policy Targets
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop	Log	Policy Targets
4	DNS	Net_10.28.0.0	* Any	* Any	* Any	Accept	Log	Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http, https	Accept	Log	Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp	Accept	Log	Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	Policy Targets

What is the possible Explanation: for this?

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

**Answer:** B

#### NEW QUESTION 189

- (Exam Topic 4)

Which message indicates IKE Phase 2 has completed successfully?

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

**Answer:** A

#### NEW QUESTION 193

- (Exam Topic 4)

Which two of these Check Point Protocols are used by ?

- A. ELA and CPD
- B. FWD and LEA
- C. FWD and CPLOG
- D. ELA and CPLOG

**Answer:** B

**NEW QUESTION 198**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 203**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 205**

- (Exam Topic 4)

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 206**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 208**

- (Exam Topic 4)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 213**

- (Exam Topic 4)

Which firewall daemon is responsible for the FW CLI commands?

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

D. cpd

**Answer:** A

**NEW QUESTION 217**

- (Exam Topic 4)

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 220**

- (Exam Topic 4)

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

- A. Security policy
- B. Inbound chain
- C. Outbound chain
- D. Decryption is not supported

**Answer:** A

**NEW QUESTION 221**

- (Exam Topic 4)

Under which file is the proxy arp configuration stored?

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

**Answer:** D

**NEW QUESTION 226**

- (Exam Topic 4)

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 228**

- (Exam Topic 4)

What is the difference between SSL VPN and IPSec VPN?

- A. IPSec VPN does not require installation of a resident VPN client
- B. SSL VPN requires installation of a resident VPN client
- C. SSL VPN and IPSec VPN are the same
- D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser

**Answer:** D

**NEW QUESTION 229**

- (Exam Topic 4)

Choose what BEST describes the reason why querying logs now is very fast.

- A. New Smart-1 appliances double the physical memory install
- B. Indexing Engine indexes logs for faster search results
- C. SmartConsole now queries results directly from the Security Gateway
- D. The amount of logs been store is less than the usual in older versions

**Answer:** B

**NEW QUESTION 233**

- (Exam Topic 4)

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

- A. Server Units



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

**Answer:** C

**NEW QUESTION 236**

- (Exam Topic 4)

Which of the following describes how Threat Extraction functions?

- A. Detect threats and provides a detailed report of discovered threats
- B. Proactively detects threats
- C. Delivers file with original content
- D. Delivers PDF versions of original files with active content removed

**Answer:** B

**NEW QUESTION 237**

- (Exam Topic 4)

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 242**

- (Exam Topic 4)

Which path below is available only when CoreXL is enabled?

- A. Slow path
- B. Firewall path
- C. Medium path
- D. Accelerated path

**Answer:** C

**NEW QUESTION 245**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 156-215.80 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/156-215.80-dumps.html>