

## Exam Questions 156-215.80

Check Point Certified Security Administrator

<https://www.2passeasy.com/dumps/156-215.80/>



### NEW QUESTION 1

- (Exam Topic 1)

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

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

**Answer:** C

### NEW QUESTION 2

- (Exam Topic 1)

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 3

- (Exam Topic 1)

Which default user has full read/write access?

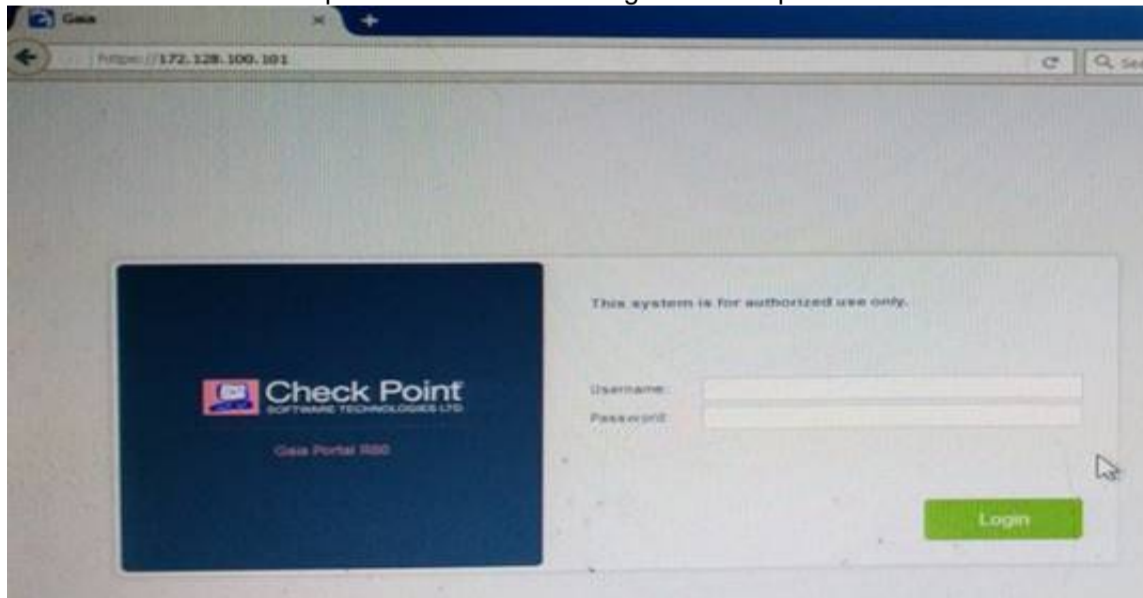
- A. Monitor
- B. Altuser
- C. Administrator
- D. Superuser

**Answer:** C

### NEW QUESTION 4

- (Exam Topic 1)

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



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

**Answer:** A

#### Explanation:

In Clish

Connect to command line on Security Gateway / each

Log in to Clish.

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

Cluster member.

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

Save the changes:

HostName> save config

Verify that the configuration was saved:

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

## NEW QUESTION 5

- (Exam Topic 1)

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

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

**Answer: C**

### Explanation:

SmartUpdate installs two repositories on the Security Management server:

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

Package Repository, which is stored:

on Windows machines in C:\SUroot.

on UNIX machines in /var/suroot.

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

## NEW QUESTION 6

- (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 7

- (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 8

- (Exam Topic 1)

ABC Corp., and have recently returned from a training course on Check Point's new advanced R80 management platform. You are presenting an in-house R80 Management to the other administrators in ABC Corp.



How will you describe the new "Publish" button in R80 Management Console?

- A. The Publish button takes any changes an administrator has made in their management session, publishes a copy to the Check Point of R80, and then saves it to the R80 database.
- B. The Publish button takes any changes an administrator has made in their management session and publishes a copy to the Check Point Cloud of R80 and but does not save it to the R80
- C. The Publish button makes any changes an administrator has made in their management session visible to all other administrator sessions and saves it to the Database.
- D. The Publish button makes any changes an administrator has made in their management session visible to the new Unified Policy session and saves it to the Database.

**Answer: C**

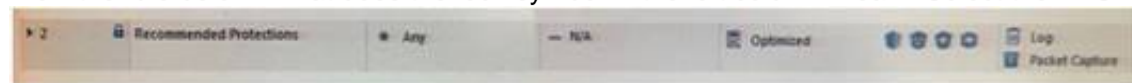
### Explanation:

To make your changes available to other administrators, and to save the database before installing a policy, you must publish the session. When you publish a session, a new database version is created.

### NEW QUESTION 9

- (Exam Topic 1)

View the rule below. What does the lock-symbol in the left column mean? Select the BEST answer.



- A. The current administrator has read-only permissions to Threat Prevention Policy.
- B. Another user has locked the rule for editing.
- C. Configuration lock is present
- D. Click the lock symbol to gain read-write access.
- E. The current administrator is logged in as read-only because someone else is editing the policy.

**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.

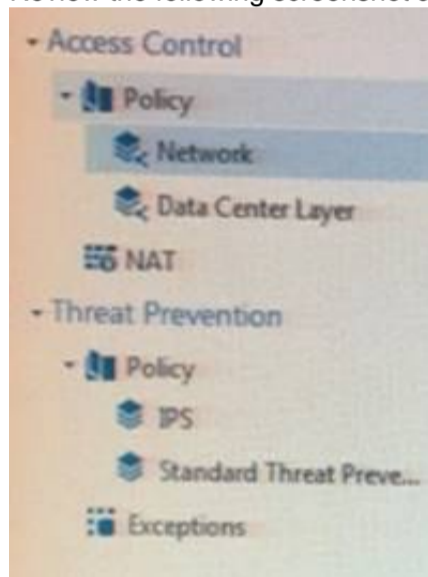
When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited.

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 10

- (Exam Topic 1)

Review the following screenshot and select the BEST answer.



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

**Answer: C**

### NEW QUESTION 10

- (Exam Topic 1)

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

- A. [https://<Device\\_IP\\_Address>](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>>

Enter your user name and password. References:

### NEW QUESTION 11

- (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 14

- (Exam Topic 1)

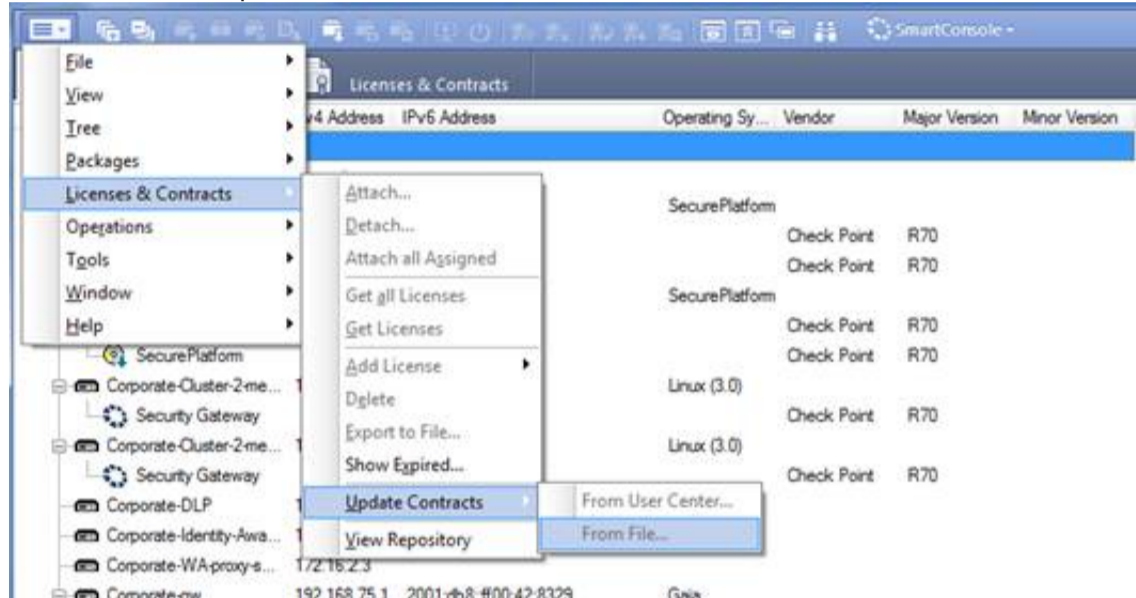
Which application should you use to install a contract file?

- 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 18

- (Exam Topic 1)

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

- A. /var/log/Cpbackup/backups/backup/backup\_fw.tgs
- B. /var/log/Cpbackup/backups/backup/backup\_fw.tar
- C. /var/log/Cpbackup/backups/backups/backup\_fw.tar
- D. /var/log/Cpbackup/backups/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 21

- (Exam Topic 1)

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 23

- (Exam Topic 1)

What are the three authentication methods for SIC?

- A. Passwords, Users, and standards-based SSL for the creation of security channels
- B. Certificates, standards-based SSL for the creation of secure channels, and 3DES or AES128 for encryption
- C. Packet Filtering, certificates, and 3DES or AES128 for encryption

D. Certificates, Passwords, and Tokens

**Answer:** B

**Explanation:**

Secure Internal Communication (SIC)

Secure Internal Communication (SIC) lets Check Point platforms and products authenticate with each other. The SIC procedure creates a trusted status between gateways, management servers and other Check Point components. SIC is required to install policies on gateways and to send logs between gateways and management servers.

These security measures make sure of the safety of SIC:

Certificates for authentication

Standards-based SSL for the creation of the secure channel

3DES for encryption

References:

**NEW QUESTION 28**

- (Exam Topic 1)

Fill in the blanks: VPN gateways authenticate using \_\_\_\_\_ and \_\_\_\_\_.

A. Passwords; tokens

B. Certificates; pre-shared secrets

C. Certificates; passwords

D. Tokens; pre-shared secrets

**Answer:** B

**Explanation:**

VPN gateways authenticate using Digital Certificates and Pre-shared secrets.

**NEW QUESTION 29**

- (Exam Topic 1)

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 32**

- (Exam Topic 1)

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 34**

- (Exam Topic 1)

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:

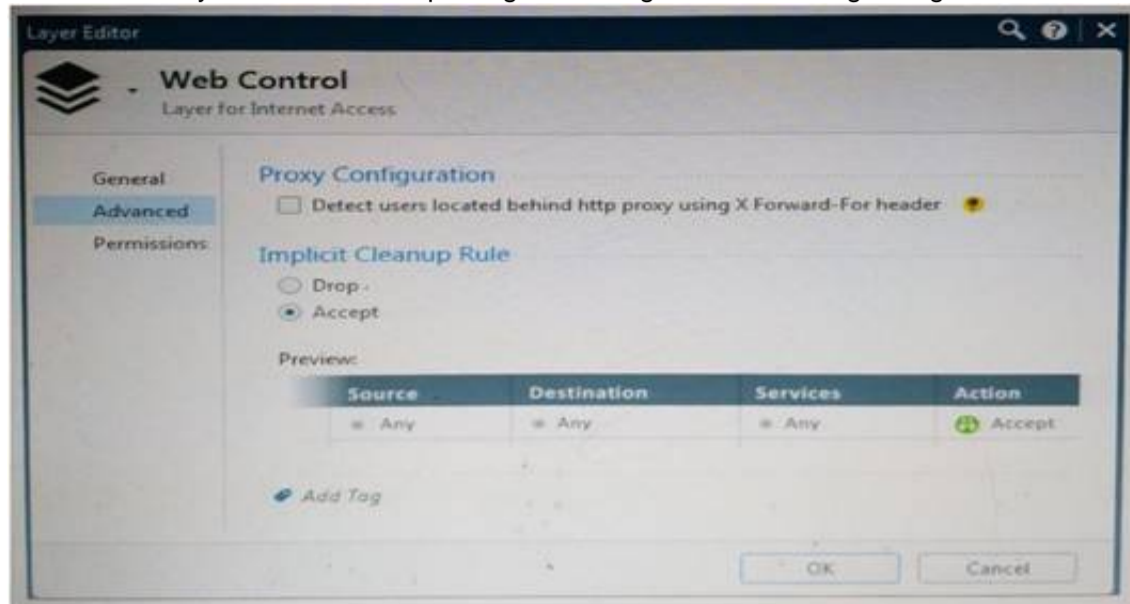
You cannot delete or change the predefined roles.

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 38

- (Exam Topic 1)

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



Consider the following policy and select the BEST answer.

Policy	Source	Destination	Services	Action
1. Allow Internet Access	Any	Internet	Any	Accept
2. Block access to high risk applications	Any	Any	Facebook, Twitter, LinkedIn, YouTube, Vimeo	Drop
3. Block access to social network applications	Any	Any	Facebook, Twitter, LinkedIn, YouTube, Vimeo	Drop
4. All employees can access Internet	Corporate LAN	Internet	Any	Accept
5. Block specific traffic	Any	Any	YouTube, Vimeo	Drop
6. Block specific applications	Any	Any	YouTube, Vimeo	Drop

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

**Answer: D**

### Explanation:

Policy Layers and Sub-Policies

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

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

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

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

### NEW QUESTION 40

- (Exam Topic 1)

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 44

- (Exam Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 48

- (Exam Topic 1)

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: <ul style="list-style-type: none"> <li>o cphaprob -d faildevice -t 0 -s ok register</li> <li>o cphaprob -d faildevice -s problem report</li> </ul> and: <ul style="list-style-type: none"> <li>o cphaprob -d faildevice -s ok report</li> <li>o cphaprob -d faildevice unregister</li> </ul>	Effect: <ul style="list-style-type: none"> <li>o Disables ClusterXL</li> <li>o Does not disable synchronization</li> </ul>	Effect: <ul style="list-style-type: none"> <li>o Enables ClusterXL</li> <li>o Does not initiate full synchronization</li> </ul>
<b>Recommended method:</b> Run: <ul style="list-style-type: none"> <li>o clusterXL_admin down</li> <li>o clusterXL_admin up</li> </ul>	<ul style="list-style-type: none"> <li>o Disables ClusterXL</li> <li>o Does not disable synchronization</li> </ul>	<ul style="list-style-type: none"> <li>o Enables ClusterXL</li> <li>o Does not initiate full synchronization</li> </ul>
In SmartView Monitor: <ol style="list-style-type: none"> <li>1. Click the Cluster object.</li> <li>2. Select one of the member gateway branches.</li> <li>3. Right click the cluster member.</li> <li>4. Select <b>Down</b>.</li> </ol>	<ul style="list-style-type: none"> <li>o Disables ClusterXL</li> <li>o Disables synchronization</li> </ul>	<ul style="list-style-type: none"> <li>o Enables ClusterXL</li> <li>o Does not initiate full synchronization</li> </ul>

#### NEW QUESTION 50

- (Exam Topic 1)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 52

- (Exam Topic 1)

To optimize Rule Base efficiency, the most hit rules should be where?

- A. Removed from the Rule Base.
- B. Towards the middle of the Rule Base.
- C. Towards the top of the Rule Base.
- D. Towards the bottom of the Rule Base.

**Answer: C**

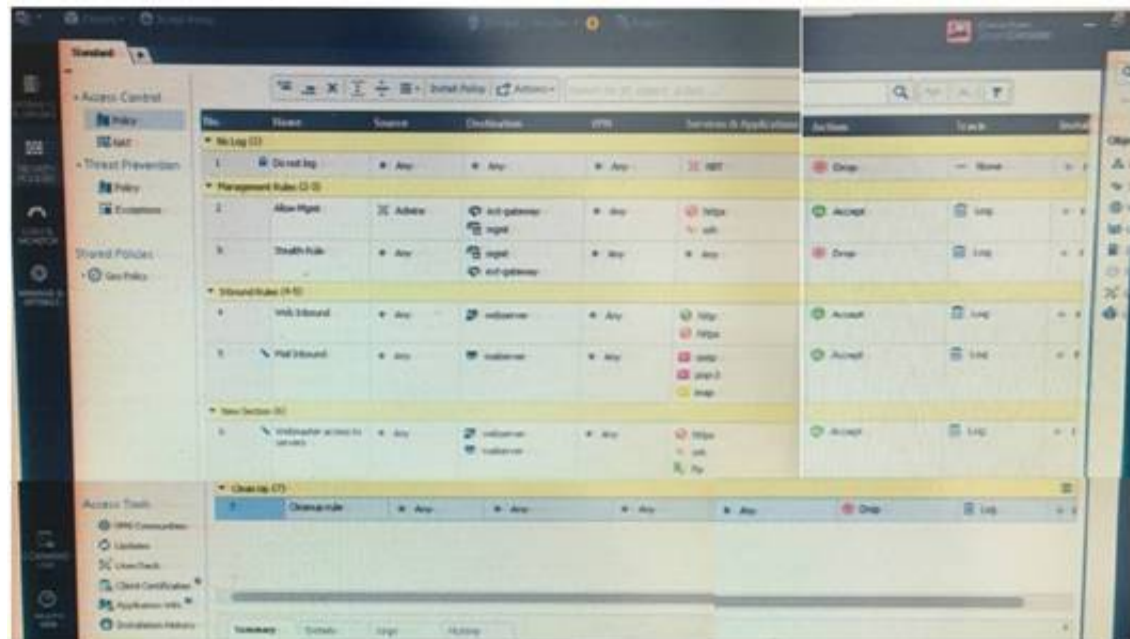
#### Explanation:

It is logical that if lesser rules are checked for the matched rule to be found the lesser CPU cycles the device is using. Checkpoint match a session from the first rule on top till the last on the bottom.

### NEW QUESTION 53

- (Exam Topic 1)

Examine the following Rule Base.



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

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

**Answer: D**

#### Explanation:

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

	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 58

- (Exam Topic 1)

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

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

**Answer: B**

#### Explanation:

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

- Malware attacks
- Dos and DDoS attacks
- Application and server vulnerabilities
- Insider threats
- Unwanted application traffic, including IM and P2P

### NEW QUESTION 59

- (Exam Topic 2)

Which Check Point software blade provides protection from zero-day and undiscovered threats?

- A. Firewall
- B. Threat Emulation
- C. Application Control
- D. Threat Extraction

Answer: D

#### Explanation:

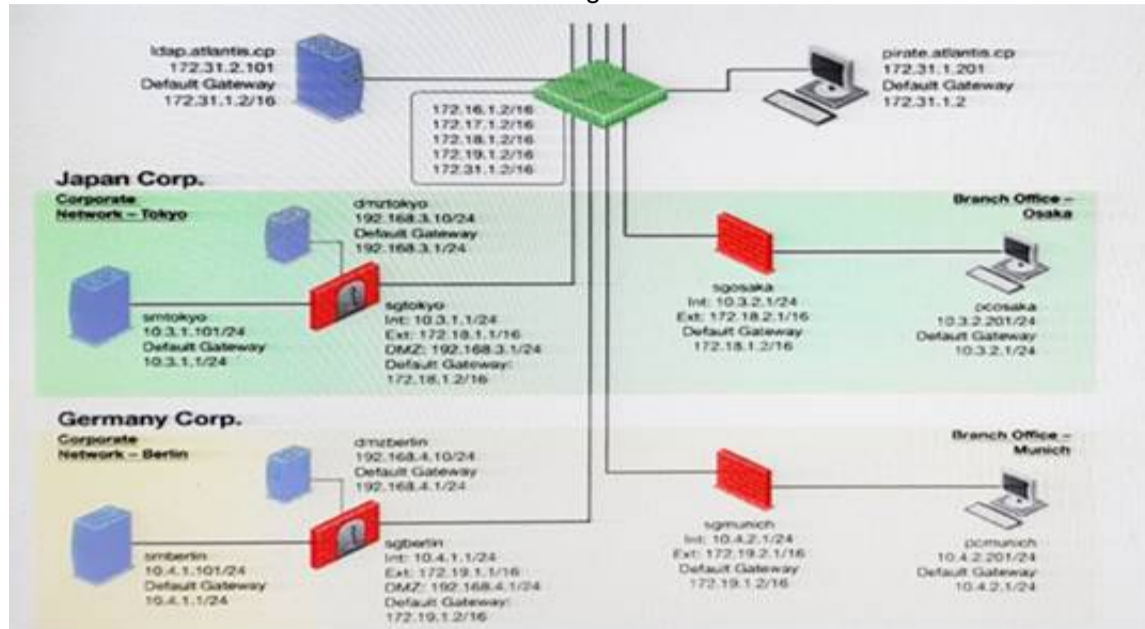
SandBlast Threat Emulation

As part of the Next Generation Threat Extraction software bundle (NGTX), the SandBlast Threat Emulation capability prevents infections from undiscovered exploits zero-day and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network.

#### NEW QUESTION 64

- (Exam Topic 2)

You want to reset SIC between smberlin and sgosaka.



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



What is the reason for this behavior?

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

Answer: C

#### NEW QUESTION 68

- (Exam Topic 2)

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

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

Answer: A

#### NEW QUESTION 71

- (Exam Topic 2)

Which of the following is NOT defined by an Access Role object?

- A. Source Network
- B. Source Machine
- C. Source User
- D. Source Server

Answer: D

#### NEW QUESTION 76

- (Exam Topic 2)

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

- A. Accept; redirect
- B. Accept; drop

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

**Answer:** D

#### NEW QUESTION 79

- (Exam Topic 2)

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 directl
- E. You can open SmartDashboard and select UserDefined in the Track colum
- F. Afterwards, you need to create your own program with an external counter.

**Answer:** C

#### NEW QUESTION 82

- (Exam Topic 2)

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

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

**Answer:** D

#### Explanation:

Identity Awareness gets identities from these acquisition sources:

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

#### NEW QUESTION 86

- (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 88

- (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 89

- (Exam Topic 2)

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 94**

- (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 99**

- (Exam Topic 2)

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 101**

- (Exam Topic 2)

Bob and Joe both have Administrator Roles on their Gaia Platform. Bob logs in on the WebUI and then Joe logs in through CLI. Choose what BEST describes the following scenario, where Bob and Joe are both logged in:

- A. When Joe logs in, Bob will be log out automatically.
- B. Since they both are log in on different interfaces, they both will be able to make changes.
- C. If Joe tries to make changes, he won't, database will be locked.
- D. Bob will be prompt that Joe logged in.

**Answer:** C

**NEW QUESTION 105**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 107**

- (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 112**

- (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 113**

- (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 115**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

Obtaining a Configuration Lock

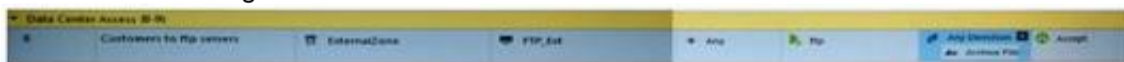
lock database override

unlock database

**NEW QUESTION 119**

- (Exam Topic 2)

Look at the following screenshot and select the BEST answer.



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

**Answer:** A

**NEW QUESTION 121**

- (Exam Topic 2)

Which of the following licenses are considered temporary?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 123**

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 128

- (Exam Topic 2)

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

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

**Answer:** A

#### Explanation:

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

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

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

data.csv:

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 131

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 132

- (Exam Topic 3)

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 136

- (Exam Topic 3)

Which is the correct order of a log flow processed by SmartEvent components:

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

**Answer:** D

#### NEW QUESTION 141

- (Exam Topic 3)

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

- A. Run cpconfig, and click Reset.

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

**Answer:** B

#### NEW QUESTION 142

- (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 147

- (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 149

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 151

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 155

- (Exam Topic 3)

Match the following commands to their correct function. Each command has one function only listed.

Command	Function
C1 cp_admin_convert	F1: export and import different revisions of the database.
C2 cpca_client	F2: export and import policy package
C3 cp_merge	F3: transfer Log data to an external database.
C4 cpwd_admin	F4: execute operations on the ICA.
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in cpconfig to SmartDashboard.

- A. C1>F6; C2>F4; C3>F2; C4>F5
- B. C1>F2; C2>F1; C3>F6; C4>F4
- C. C1>F2; C2>F4; C3>F1; C4>F5
- D. C1>F4; C2>F6; C3>F3; C4>F5

**Answer:** A

#### NEW QUESTION 158

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 160

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 163

- (Exam Topic 3)

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 167

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 172

- (Exam Topic 3)

Which of the following authentication methods can be configured in the Identity Awareness setup wizard?

- A. Check Point Password
- B. TACACS
- C. LDAP
- D. Windows password

**Answer:** C

#### NEW QUESTION 174

- (Exam Topic 3)

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 178

- (Exam Topic 3)

What is the Manual Client Authentication TELNET port?

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

**Answer:** D

#### NEW QUESTION 180

- (Exam Topic 3)

Where does the security administrator activate Identity Awareness within SmartDashboard?

- A. Gateway Object > General Properties
- B. Security Management Server > Identity Awareness
- C. Policy > Global Properties > Identity Awareness
- D. LDAP Server Object > General Properties

**Answer:** A

#### NEW QUESTION 184

- (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 185

- (Exam Topic 3)

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 189

- (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 191

- (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 196

- (Exam Topic 3)

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 199

- (Exam Topic 3)

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 201

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 205

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 207

- (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 208

- (Exam Topic 3)

Which of the following is a hash algorithm?

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

**Answer:** D

#### NEW QUESTION 210

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 215

- (Exam Topic 4)

How are the backups stored in Check 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 220

- (Exam Topic 4)

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 225

- (Exam Topic 4)

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 226

- (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 230

- (Exam Topic 4)

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

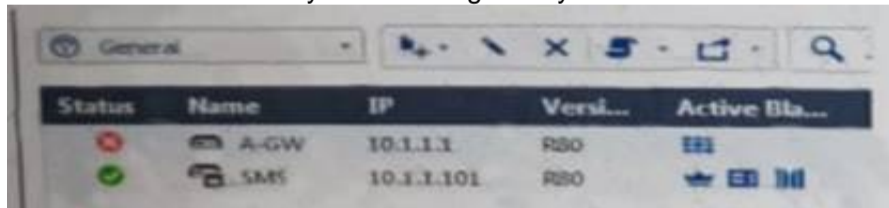
- A. A host route to route to the destination IP
- B. Use the file local.arp to add the ARP entries for NAT to work
- C. Nothing, the Gateway takes care of all details necessary
- D. Enabling 'Allow bi-directional NAT' for NAT to work correctly

Answer: C

#### NEW QUESTION 234

- (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 235

- (Exam Topic 4)

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 239

- (Exam Topic 4)

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

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

Answer: B

#### NEW QUESTION 244

- (Exam Topic 4)

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

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

Answer: D

#### NEW QUESTION 249

- (Exam Topic 4)

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

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

Answer: B

#### NEW QUESTION 254

- (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 257

- (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 260

- (Exam Topic 4)

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 263

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 265

- (Exam Topic 4)

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 269

- (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 270

- (Exam Topic 4)

Which command shows the installed licenses?

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

**Answer:** A

#### NEW QUESTION 274

- (Exam Topic 4)

What SmartEvent component creates events?

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

**Answer:** B

#### NEW QUESTION 276

- (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 281

- (Exam Topic 4)

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 286

- (Exam Topic 4)

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 289

- (Exam Topic 4)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 294

- (Exam Topic 4)

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 295

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 299

- (Exam Topic 4)

Which statement is NOT TRUE about Delta synchronization?

- A. Using UDP Multicast or Broadcast on port 8161
- B. Using UDP Multicast or Broadcast on port 8116
- C. Quicker than Full sync
- D. Transfers changes in the Kernel tables between cluster members

**Answer:** A

#### NEW QUESTION 301

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 302

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 303

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.80 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.80 Product From:

<https://www.2passeasy.com/dumps/156-215.80/>

## Money Back Guarantee

### 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