

## Exam Questions 156-215.81

Check Point Certified Security Administrator R81

<https://www.2passeasy.com/dumps/156-215.81/>



#### NEW QUESTION 1

What is the purpose of the Stealth Rule?

- A. To prevent users from directly connecting to a Security Gateway.
- B. To reduce the number of rules in the database.
- C. To reduce the amount of logs for performance issues.
- D. To hide the gateway from the Internet.

**Answer:** A

#### NEW QUESTION 2

When URL Filtering is set, what identifying data gets sent to the Check Point Online Web Service?

- A. The URL and server certificate are sent to the Check Point Online Web Service
- B. The full URL, including page data, is sent to the Check Point Online Web Service
- C. The host part of the URL is sent to the Check Point Online Web Service
- D. The URL and IP address are sent to the Check Point Online Web Service

**Answer:** C

#### NEW QUESTION 3

Which of the following is NOT a component of a Distinguished Name?

- A. Common Name
- B. Country
- C. User container
- D. Organizational Unit

**Answer:** C

#### NEW QUESTION 4

The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?

- A. Add tcpdump to CLISH using add command. Create a new access role. Add tcpdump to the role. Create new user with any UID and assign role to the user.
- B. Add tcpdump to CLISH using add command. Create a new access role. Add tcpdump to the role. Create new user with UID 0 and assign role to the user.
- C. Create a new access role. Add expert-mode access to the role. Create new user with UID 0 and assign role to the user.
- D. Create a new access role. Add expert-mode access to the role. Create new user with any UID and assign role to the user.

**Answer:** A

#### NEW QUESTION 5

Which of the following is NOT a component of Check Point Capsule?

- A. Capsule Docs
- B. Capsule Cloud
- C. Capsule Enterprise
- D. Capsule Workspace

**Answer:** C

#### NEW QUESTION 6

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

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

**Answer:** D

#### Explanation:

"The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. They are shared between all Policy packages."  
[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_SecurityManagement\\_AdminGuide](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide)

#### NEW QUESTION 7

When enabling tracking on a rule, what is the default option?

- A. Accounting Log
- B. Extended Log
- C. Log
- D. Detailed Log

**Answer:** C

#### NEW QUESTION 8

Fill in the bank: In Office mode, a Security Gateway assigns a remote client to an IP address once \_\_\_\_\_ .

- A. the user connects and authenticates
- B. office mode is initiated
- C. the user requests a connection
- D. the user connects

**Answer:** A

#### Explanation:

Office Mode enables a Security Gateway to assign a remote client an IP address. The assignment takes place once the user connects and authenticates. The assignment lease is renewed as long as the user is connected.

#### NEW QUESTION 9

What is the purpose of the CPCA process?

- A. Monitoring the status of processes
- B. Sending and receiving logs
- C. Communication between GUI clients and the SmartCenter server
- D. Generating and modifying certificates

**Answer:** D

#### NEW QUESTION 10

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 10

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

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

**Answer:** B

#### NEW QUESTION 14

What is the purpose of the Clean-up Rule?

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

**Answer:** A

#### Explanation:

These are basic access control rules we recommend for all Rule Bases:

There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

#### NEW QUESTION 19

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

- A. AES-128
- B. AES-256
- C. DES
- D. 3DES

**Answer:** A

#### NEW QUESTION 21

Fill in the blanks: Default port numbers for an LDAP server is \_\_\_\_\_ for standard connections and \_\_\_\_\_ SSL connections.

- A. 675, 389
- B. 389, 636
- C. 636, 290
- D. 290, 675

**Answer:** B

**Explanation:**

A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS.

**NEW QUESTION 26**

Which of the following is NOT a tracking log option in R80.x?

- A. Log
- B. Full Log
- C. Detailed Log
- D. Extended Log

**Answer:** C

**NEW QUESTION 31**

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

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

**Answer:** D

**NEW QUESTION 36**

When a SAM rule is required on Security Gateway to quickly block suspicious connections which are not restricted by the Security Policy, what actions does the administrator need to take?

- A. SmartView Monitor should be opened and then the SAM rule/s can be applied immediately
- B. Installing policy is not required.
- C. The policy type SAM must be added to the Policy Package and a new SAM rule must be applied. Simply Publishing the changes applies the SAM rule on the firewall.
- D. The administrator must work on the firewall CLI (for example with SSH and PuTTY) and the command 'sam block' must be used with the right parameters.
- E. The administrator should open the LOGS & MONITOR view and find the relevant log
- F. Right clicking on the log entry will show the Create New SAM rule option.

**Answer:** A

**Explanation:**

A Security Gateway Closed with SAM enabled has Firewall rules to block suspicious connections that are not restricted by the security policy Closed. These rules are applied immediately (policy installation is not required).

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_LoggingAndMonitoring\\_AdminGu](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu)

**NEW QUESTION 40**

Core Protections are installed as part of what Policy?

- A. Access Control Policy.
- B. Desktop Firewall Policy
- C. Mobile Access Policy.
- D. Threat Prevention Policy.

**Answer:** A

**Explanation:**

Core protections - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy. ThreatCloud protections - Updated from the Check Point cloud, (see Updating IPS Protections). These protections are part of the Threat Prevention policy.

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_ThreatPrevention\\_AdminGuide/To](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To)

**NEW QUESTION 43**

Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers? (Choose the best answer.)

- A. IPS
- B. Anti-Virus
- C. Anti-Malware
- D. Content Awareness

**Answer:** B

**Explanation:**

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_ThreatPrevention\\_AdminGuide/To](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To) "Check Point Antivirus Software Blade prevents and stops

threats such as malware, viruses, and Trojans from entering and infecting a network"

Also here - <https://www.checkpoint.com/downloads/products/antivirus-datasheet.pdf>

#### NEW QUESTION 46

Which is NOT an encryption algorithm that can be used in an IPSEC Security Association (Phase 2)?

- A. AES-GCM-256
- B. AES-CBC-256
- C. AES-GCM-128

**Answer:** B

#### NEW QUESTION 50

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

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

**Answer:** B

#### NEW QUESTION 55

Identify the ports to which the Client Authentication daemon listens on by default?

- A. 259, 900
- B. 256, 257
- C. 8080, 529
- D. 80, 256

**Answer:** A

#### NEW QUESTION 57

Fill in the blank: \_\_\_\_\_ is the Gaia command that turns the server off.

- A. sysdown
- B. exit
- C. halt
- D. shut-down

**Answer:** C

#### NEW QUESTION 58

Which command shows the installed licenses?

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

**Answer:** A

#### NEW QUESTION 61

How do logs change when the "Accounting" tracking option is enabled on a traffic rule?

- A. Involved traffic logs will be forwarded to a log server.
- B. Provides log details view email to the Administrator.
- C. Involved traffic logs are updated every 10 minutes to show how much data has passed on the connection.
- D. Provides additional information to the connected user.

**Answer:** C

#### Explanation:

Accounting - Select this to update the log at 10 minutes intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time. [https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_LoggingAndMonitoring\\_AdminGu](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu)

#### NEW QUESTION 65

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

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

**Answer:** D

#### Explanation:

Gateways send their logs to the log server.

#### NEW QUESTION 66

Both major kinds of NAT support Hide and Static NAT. However, one offers more flexibility. Which statement is true?

- A. Manual NAT can offer more flexibility than Automatic NAT.
- B. Dynamic Network Address Translation (NAT) Overloading can offer more flexibility than Port Address Translation.
- C. Dynamic NAT with Port Address Translation can offer more flexibility than Network Address Translation (NAT) Overloading.
- D. Automatic NAT can offer more flexibility than Manual NAT.

**Answer:** A

#### Explanation:

"An Auto-NAT rule only uses the source address and port when matching and translating. Manual NAT can match and translate source and destination addresses and ports." <https://networkdirection.net/articles/firewalls/firepowermanagementcentre/fmcnatpolicies/>

#### NEW QUESTION 69

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 73

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 76

Fill in the blank: Back up and restores can be accomplished through \_\_\_\_\_.

- A. SmartConsole, WebUI, or CLI
- B. WebUI, CLI, or SmartUpdate
- C. CLI, SmartUpdate, or SmartBackup
- D. SmartUpdate, SmartBackup, or SmartConsole

**Answer:** A

#### Explanation:

Backup and RestoreThese options let you: To back up a configuration:  
The Backup window opens.

#### NEW QUESTION 77

What is the default tracking option of a rule?

- A. Tracking
- B. Log
- C. None
- D. Alert

**Answer:** B

#### Explanation:

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_LoggingAndMonitoring\\_AdminGu](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu)

#### NEW QUESTION 79

SmartEvent does NOT use which of the following procedures to identity events:

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

**Answer:** C

#### NEW QUESTION 80

Which backup 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 85

What type of NAT is a one-to-one relationship where each host is translated to a unique address?

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

**Answer:** B

#### NEW QUESTION 86

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

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

**Answer:** B

#### NEW QUESTION 88

Where is the “Hit Count” feature enabled or disabled in SmartConsole?

- A. On the Policy Package
- B. On each Security Gateway
- C. On the Policy layer
- D. In Global Properties for the Security Management Server

**Answer:** B

#### Explanation:

References:

#### NEW QUESTION 93

Your internal networks 10.1.1.0/24, 10.2.2.0/24 and 192.168.0.0/16 are behind the Internet Security Gateway. Considering that Layer 2 and Layer 3 setup is correct, what are the steps you will need to do in SmartConsole in order to get the connection working?

- A. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway’s external IP.3. Publish and install the policy.
- B. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish the policy.
- C. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish and install the policy.
- D. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway’s external IP.3. Publish the policy.

**Answer:** C

#### NEW QUESTION 95

In order to modify Security Policies the administrator can use which of the following tools? (Choose the best answer.)

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

**Answer:** B

#### NEW QUESTION 97

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 101

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 105

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 109

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

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

**Answer:** A

#### Explanation:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=)

#### NEW QUESTION 111

How many layers make up the TCP/IP model?

- A. 2
- B. 7
- C. 6
- D. 4

**Answer:** D

#### NEW QUESTION 115

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:** D

#### NEW QUESTION 118

In \_\_\_\_\_ NAT, the \_\_\_\_\_ is translated.

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

**Answer:** A

#### NEW QUESTION 121

To increase security, the administrator has modified the Core protection 'Host Port Scan' from 'Medium' to 'High' Predefined Sensitivity. Which Policy should the administrator install after Publishing the changes?

- A. The Access Control and Threat Prevention Policies.
- B. The Access Control Policy.
- C. The Access Control & HTTPS Inspection Policy.
- D. The Threat Prevention Policy.

**Answer:** D

#### Explanation:



<https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubm>

#### NEW QUESTION 122

You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be?

- A. Open SmartLog and connect remotely to the IP of the wireless controller
- B. Open SmartView Tracker and filter the logs for the IP address of the tablet
- C. Open SmartView Tracker and check all the IP logs for the tablet
- D. Open SmartLog and query for the IP address of the Manager's tablet

**Answer:** B

#### NEW QUESTION 126

The "Hit count" feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits even if the Track option is set to "None"?

- A. No, it will not work independentl
- B. Hit Count will be shown only for rules with Track options set as Log or alert
- C. Yes, it will work independently as long as "analyze all rules" tick box is enabled on the Security Gateway
- D. No, it will not work independently because hit count requires all rules to be logged
- E. Yes, it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways

**Answer:** D

#### NEW QUESTION 130

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 133

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

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

**Answer:** B

#### NEW QUESTION 137

Which of the following is considered a "Subscription Blade", requiring renewal every 1-3 years?

- A. IPS blade
- B. IPSEC VPN Blade
- C. Identity Awareness Blade
- D. Firewall Blade

**Answer:** A

#### NEW QUESTION 141

Which of these is NOT a feature or benefit of Application Control?

- A. Eliminate unknown and unwanted applications in your network to reduce IT complexity and application risk.
- B. Identify and control which applications are in your IT environment and which to add to the IT environment.
- C. Scans the content of files being downloaded by users in order to make policy decisions.
- D. Automatically identify trusted software that has authorization to run

**Answer:** C

#### Explanation:

File scanning is a job for ThreatCloud and it sandboxes/scrubs files.

#### NEW QUESTION 143

Which of the following is considered to be the more secure and preferred VPN authentication method?

- A. Password
- B. Certificate
- C. MD5

D. Pre-shared secret

**Answer:** B

**Explanation:**

References:

#### NEW QUESTION 148

Which of the following is used to extract state related information from packets and store that information in state tables?

- A. STATE Engine
- B. TRACK Engine
- C. RECORD Engine
- D. INSPECT Engine

**Answer:** D

**Explanation:**

Stateful Inspection, the packet is intercepted at the network layer, but then the INSPECT Engine takes over.

It extracts state-related information required for the security decision from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts.

#### NEW QUESTION 149

In SmartConsole, on which tab are Permissions and Administrators defined?

- A. Manage and Settings
- B. Logs and Monitor
- C. Security Policies
- D. Gateways and Servers

**Answer:** A

#### NEW QUESTION 150

When configuring Spoof Tracking, which tracking actions can an administrator select to be done when spoofed packets are detected?

- A. Log, send snmp trap, email
- B. Drop packet, alert, none
- C. Log, alert, none
- D. Log, allow packets, email

**Answer:** C

**Explanation:**

Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected:

#### NEW QUESTION 152

Which tool is used to enable ClusterXL?

- A. SmartUpdate
- B. cpconfig
- C. SmartConsole
- D. sysconfig

**Answer:** B

#### NEW QUESTION 154

The Online Activation method is available for Check Point manufactured appliances. How does the administrator use the Online Activation method?

- A. The SmartLicensing GUI tool must be launched from the SmartConsole for the Online Activation tool to start automatically.
- B. No action is required if the firewall has internet access and a DNS server to resolve domain names.
- C. Using the Gaia First Time Configuration Wizard, the appliance connects to the Check Point User Center and downloads all necessary licenses and contracts.
- D. The cpinfo command must be run on the firewall with the switch -online-license-activation.

**Answer:** C

**Explanation:**

"Online activation: this method of activation is available for Check Point manufactured appliances. These appliances should be configured to have internet connectivity during the completion of the First Time Configuration Wizard for software version R77 and below. Customers using R80 and higher will be able to use this feature during or after the completion of the First Time Configuration Wizard."

[https://supportcenter.checkpoint.com/supportcenter/portal?eventsubmit\\_dogoviewsolutiondetails=&solutionid=s](https://supportcenter.checkpoint.com/supportcenter/portal?eventsubmit_dogoviewsolutiondetails=&solutionid=s)

#### NEW QUESTION 159

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

- A. Slow Path

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

**Answer:** A

#### NEW QUESTION 163

Which of the following is NOT a valid deployment option for R80?

- A. All-in-one (stand-alone)
- B. Log server
- C. SmartEvent
- D. Multi-domain management server

**Answer:** D

#### NEW QUESTION 167

Which of the following is used to initially create trust between a Gateway and Security Management Server?

- A. Internal Certificate Authority
- B. Token
- C. One-time Password
- D. Certificate

**Answer:** C

#### Explanation:

To establish the initial trust, a gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_SecurityManagement\\_AdminGuide](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide)

#### NEW QUESTION 171

An administrator can use section titles to more easily navigate between large rule bases. Which of these statements is FALSE?

- A. Section titles are not sent to the gateway side.
- B. These sections are simple visual divisions of the Rule Base and do not hinder the order of rule enforcement.
- C. A Sectional Title can be used to disable multiple rules by disabling only the sectional title.
- D. Sectional Titles do not need to be created in the SmartConsole.

**Answer:** C

#### Explanation:

Section titles are only for visual categorization of rules.

#### NEW QUESTION 173

After a new Log Server is added to the environment and the SIC trust has been established with the SMS what will the gateways do?

- A. The gateways can only send logs to an SMS and cannot send logs to a Log Serve
- B. Log Servers are proprietary log archive servers.
- C. Gateways will send new firewall logs to the new Log Server as soon as the SIC trust is set up between the SMS and the new Log Server.
- D. The firewalls will detect the new Log Server after the next policy install and redirect the new logs to the new Log Server.
- E. Logs are not automatically forwarded to a new Log Serve
- F. SmartConsole must be used to manually configure each gateway to send its logs to the server.

**Answer:** D

#### Explanation:

[https://sc1.checkpoint.com/documents/SMB\\_R80.20/AdminGuides/Locally\\_Managed/EN/Content/Topics/Conf](https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Conf)

[https://sc1.checkpoint.com/documents/SMB\\_R80.20/AdminGuides/Locally\\_Managed/EN/Content/Topics/Conf](https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Conf)

#### NEW QUESTION 177

To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?

- A. Protections
- B. IPS Protections
- C. Profiles
- D. ThreatWiki

**Answer:** B

#### NEW QUESTION 178

True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

- A. False, this feature has to be enabled in the Global Properties.
- B. True, every administrator works in a session that is independent of the other administrators.
- C. True, every administrator works on a different database that is independent of the other administrators.

D. False, only one administrator can login with write permission.

**Answer:** B

**Explanation:**

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.

**NEW QUESTION 180**

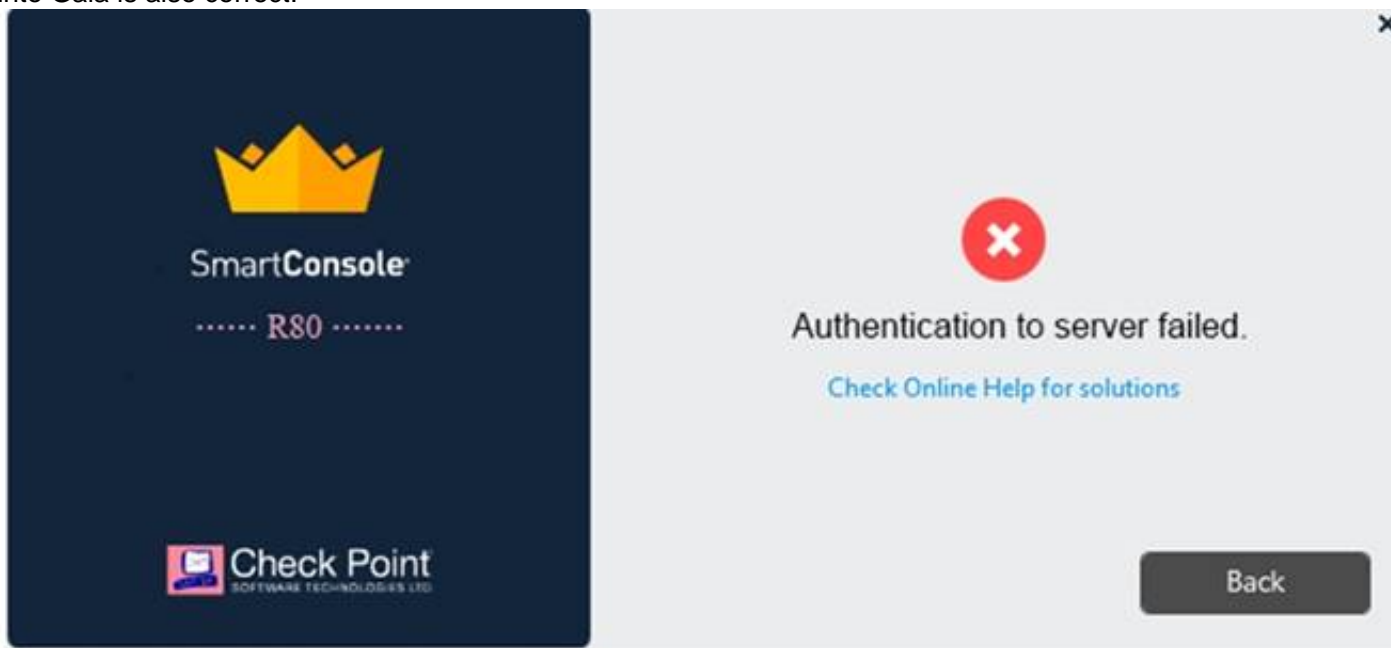
In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

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

**Answer:** C

**NEW QUESTION 183**

Vanessa is attempting to log into the Gaia Web Portal. She is able to login successfully. Then she tries the same username and password for SmartConsole but gets the message in the screenshot image below. She has checked that the IP address of the Server is correct and the username and password she used to login into Gaia is also correct.



What is the most likely reason?

- A. Check Point R80 SmartConsole authentication is more secure than in previous versions and Vanessa requires a special authentication key for R80 SmartConsole
- B. Check that the correct key details are used.
- C. Check Point Management software authentication details are not automatically the same as the Operating System authentication detail
- D. Check that she is using the correct details.
- E. SmartConsole Authentication is not allowed for Vanessa until a Super administrator has logged in first and cleared any other administrator sessions.
- F. Authentication failed because Vanessa's username is not allowed in the new Threat Prevention console update checks even though these checks passed with Gaia.

**Answer:** B

**NEW QUESTION 185**

A security zone is a group of one or more network interfaces from different centrally managed gateways. What is considered part of the zone?

- A. The zone is based on the network topology and determined according to where the interface leads to.
- B. Security Zones are not supported by Check Point firewalls.
- C. The firewall rule can be configured to include one or more subnets in a zone.
- D. The local directly connected subnet defined by the subnet IP and subnet mask.

**Answer:** A

**Explanation:**

The Interface window opens. The Topology area of the General pane shows the Security Zone to which the interface is already bound. By default, the Security Zone is calculated according to where the interface Leads To.

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_SecurityManagement\\_AdminGuide](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide)

**NEW QUESTION 188**

A Check Point Software license consists of two components, the Software Blade and the Software Container. There are \_\_\_\_\_ types of Software Containers: \_\_\_\_\_.

- A. Two; Security Management and Endpoint Security
- B. Two; Endpoint Security and Security Gateway
- C. Three; Security Management, Security Gateway, and Endpoint Security
- D. Three; Security Gateway, Endpoint Security, and Gateway Management

**Answer:** C

**Explanation:**

There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security. Ref:  
<https://downloads.checkpoint.com/dc/download.htm?ID=11608>

**NEW QUESTION 193**

When using Automatic Hide NAT, what is enabled by default?

- A. Source Port Address Translation (PAT)
- B. Static NAT
- C. Static Route
- D. HTTPS Inspection

**Answer:** A

**Explanation:**

Hiding multiple IP addresses behind one, gateway, IP address requires PAT to differentiate between traffic.

**NEW QUESTION 196**

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

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

**Answer:** A

**NEW QUESTION 200**

Name the pre-defined Roles included in Gaia OS.

- A. AdminRole, and MonitorRole
- B. ReadWriteRole, and ReadyOnly Role
- C. AdminRole, cloningAdminRole, and Monitor Role
- D. AdminRole

**Answer:** A

**NEW QUESTION 205**

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

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

**Answer:** A

**NEW QUESTION 206**

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 208**

How is communication between different Check Point components secured in R80? As with all questions, select the best answer.

- A. By using IPSEC
- B. By using SIC
- C. By using ICA
- D. By using 3DES

**Answer:** B

**NEW QUESTION 209**

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 (SMS). While configuring the VPN community to specify the pre-shared secret, the administrator did not find a box to input the pre-shared secret. Why does it not allow him to specify the pre-shared secret?

- A. The Gateway is an SMB device
- B. The checkbox "Use only Shared Secret for all external members" is not checked
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS



D. Pre-shared secret is already configured in Global Properties

**Answer:** C

#### NEW QUESTION 210

Fill in the blank: SmartConsole, SmartEvent GUI client, and \_\_\_\_\_ allow viewing of billions of consolidated logs and shows them as prioritized security events.

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

**Answer:** A

#### Explanation:

"The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents"

[https://sc1.checkpoint.com/documents/R80/CP\\_R80\\_LoggingAndMonitoring/html\\_frameset.htm?topic=docume](https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=docume)

#### NEW QUESTION 213

Which option, when applied to a rule, allows all encrypted and non-VPN traffic that matches the rule?

- A. All Site-to-Site VPN Communities
- B. Accept all encrypted traffic
- C. All Connections (Clear or Encrypted)
- D. Specific VPN Communities

**Answer:** B

#### NEW QUESTION 218

When defining group-based access in an LDAP environment with Identity Awareness, what is the BEST object type to represent an LDAP group in a Security Policy?

- A. Access Role
- B. User Group
- C. SmartDirectory Group
- D. Group Template

**Answer:** A

#### NEW QUESTION 220

Which of the following cannot be configured in an Access Role Object?

- A. Networks
- B. Users
- C. Time
- D. Machines

**Answer:** C

#### Explanation:

Access Role objects includes one or more of these objects: Networks.

Users and user groups. Computers and computer groups. Remote Access Clients.

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_IdentityAwareness\\_AdminGuide/T](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T)

#### NEW QUESTION 222

In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

- A. Publish changes
- B. Save changes
- C. Install policy
- D. Install database

**Answer:** C

#### NEW QUESTION 225

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

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

**Answer:** B



#### NEW QUESTION 227

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

- A. Save Policy
- B. Install Database
- C. Save session
- D. Install Policy

**Answer:** D

#### NEW QUESTION 229

In which scenario will an administrator need to manually define Proxy ARP?

- A. When they configure an "Automatic Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
- B. When they configure an "Automatic Hide NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
- C. When they configure a "Manual Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
- D. When they configure a "Manual Hide NAT" which translates to an IP address that belongs to one of the firewall's interfaces.

**Answer:** C

#### NEW QUESTION 233

Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine?

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

**Answer:** A

#### NEW QUESTION 236

Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

- A. Detects and blocks malware by correlating multiple detection engines before users are affected.
- B. Configure rules to limit the available network bandwidth for specified users or groups.
- C. Use UserCheck to help users understand that certain websites are against the company's security policy.
- D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

**Answer:** A

#### NEW QUESTION 237

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

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

**Answer:** D

#### Explanation:

Local licensing is associated with the IP address of the Security Gateway, to which the license will be applied. Each time the IP address of the Security Gateway changes, a new license must be generated and installed.  
[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=)

#### NEW QUESTION 242

To view statistics on detected threats, which Threat Tool would an administrator use?

- A. Protections
- B. IPS Protections
- C. Profiles
- D. ThreatWiki

**Answer:** D

#### NEW QUESTION 246

What are the three main components of Check Point security management architecture?

- A. SmartConsole, Security Management, and Security Gateway
- B. Smart Console, Standalone, and Security Management
- C. SmartConsole, Security policy, and Logs & Monitoring
- D. GUI-Client, Security Management, and Security Gateway

**Answer:** A

#### NEW QUESTION 251

Which of the following is NOT supported by Bridge Mode Check Point Security Gateway

- A. Antivirus
- B. Data Loss Prevention
- C. NAT
- D. Application Control

**Answer:** C

#### NEW QUESTION 253

Log query results can be exported to what file format?

- A. Word Document (docx)
- B. Comma Separated Value (csv)
- C. Portable Document Format (pdf)
- D. Text (txt)

**Answer:** B

#### NEW QUESTION 258

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 261

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

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

**Answer:** D

#### NEW QUESTION 266

What command would show the API server status?

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

**Answer:** D

#### NEW QUESTION 268

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

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

**Answer:** C

#### NEW QUESTION 270

Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or \_\_\_\_\_.

- A. On all satellite gateway to satellite gateway tunnels
- B. On specific tunnels for specific gateways
- C. On specific tunnels in the community
- D. On specific satellite gateway to central gateway tunnels

**Answer:** C

#### Explanation:

Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:

#### NEW QUESTION 271

True or False: More than one administrator can log into the Security Management Server with SmartConsole with write permission at the same time.

- A. True, every administrator works on a different database that is independent of the other administrators
- B. False, this feature has to be enabled in the Global Properties.
- C. True, every administrator works in a session that is independent of the other administrators
- D. False, only one administrator can login with write permission

**Answer:** C

#### Explanation:

Multiple R/W admins can log into SmartConsole and edit rules but they can't edit a rule that is being worked on by another admin.

#### NEW QUESTION 276

The CDT utility supports which of the following?

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

**Answer:** D

#### NEW QUESTION 277

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

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

**Answer:** A

#### Explanation:

Phase I modes

Between Security Gateways, there are two modes for IKE phase I. These modes only apply to IKEv1:

#### NEW QUESTION 281

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.81 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.81 Product From:

<https://www.2passeasy.com/dumps/156-215.81/>

## Money Back Guarantee

### 156-215.81 Practice Exam Features:

- \* 156-215.81 Questions and Answers Updated Frequently
- \* 156-215.81 Practice Questions Verified by Expert Senior Certified Staff
- \* 156-215.81 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 156-215.81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year