

## Exam Questions 156-215.81

Check Point Certified Security Administrator R81

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



### NEW QUESTION 1







An administrator wishes to enable Identity Awareness on the Check Point firewalls. However they allow users to use company issued or personal laptops. Since the administrator cannot manage the personal laptops, which of the following methods would BEST suit this company?

- A. AD Query
- B. Browser-Based Authentication
- C. Identity Agents
- D. Terminal Servers Agent

Answer: B

### NEW QUESTION 2

What does it mean if Deyra sees the gateway status:

Status	Name	IP	Versi...	Active Bla...
	A-GW	10.1.1.1	R80	
	SMS	10.1.1.101	R80	  

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: B

Explanation:



**fw-mini-ced**  
IP Address: **10.90.0.253**  
Version: **R77.30**  
OS: **Gaia Kernel Version: 2.6**  
Up Time: **3 days and 4 hours**  
[System Information](#), [Network Activity](#), [Licenses](#)

	<b>Firewall</b>	Security Policy: <b>Standard_1</b> Installed On: <b>Fri Dec 16 15:21:03 2016</b>	 <a href="#">More...</a>
	<b>ClusterXL</b>	Working mode: <b>High Availability (Active Up)</b> Member state: <b>active</b>	 <a href="#">More...</a>
	<b>IPSec VPN</b>	Gateway to Gateway Tunnels: <b>0</b> Remote User Tunnels: <b>0</b>	 <a href="#">More...</a>
	<b>Identity Awareness</b>	Error: At least one DC is currently disconnected	 <a href="#">More...</a>
	<b>Mobile Access</b>	Number of active sessions: <b>2</b>	
	<b>Anti-Bot &amp; Anti-Virus</b>	Anti-Bot subscription Status: <b>Valid</b> Anti-Bot subscription Expiration: <b>Thu Jun 22 01:00:00 2017</b> Anti-Virus subscription Status: <b>Valid</b> Anti-Virus subscription Expiration: <b>Thu Jun 22 01:00:00 2017</b>	 <a href="#">More...</a>
	<b>URL Filtering</b>	Subscription Status: <b>Valid</b> Subscription Expiration: <b>Thu Jun 22 01:00:00 2017</b>	 <a href="#">More...</a>
	<b>Application Control</b>	Subscription Status: <b>Valid</b> Subscription Expiration: <b>Thu Jun 22 01:00:00 2017</b>	 <a href="#">More...</a>
	<b>Anti-Spam</b>		 <a href="#">More...</a>

### NEW QUESTION 3

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 4

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 5**

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 6**

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

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

**Answer:** C

**Explanation:**

User Directory lets you configure:

High Availability, to duplicate user data across multiple servers for backup. See Account Units and High Availability.

Multiple Account Units, for distributed databases.

Define LDAP Account Units, for encrypted User Directory connections. See Modifying the LDAP Server. Profiles, to support multiple LDAP vendors. See User Directory Profiles. [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**

From the Gaia web interface, which of the following operations CANNOT be performed on a Security Management Server?

- A. Verify a Security Policy
- B. Open a terminal shell
- C. Add a static route
- D. View Security Management GUI Clients

**Answer:** B

**NEW QUESTION 8**

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 9**

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 10**

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. These rules are applied immediately (policy installation is not required).

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_LoggingAndMonitoring\\_AdminGuide](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide)

**NEW QUESTION 10**

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 12**

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 15**

Which of the following is NOT a tracking option? (Select three)

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

**Answer:** ACD

**NEW QUESTION 16**

What are the advantages of a "shared policy" in R80?

- A. Allows the administrator to share a policy between all the users identified by the Security Gateway
- B. Allows the administrator to share a policy between all the administrators managing the Security Management Server
- C. Allows the administrator to share a policy so that it is available to use in another Policy Package
- D. Allows the administrator to install a policy on one Security Gateway and it gets installed on another managed Security Gateway

**Answer:** C

**Explanation:**

Ref: [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 21**

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

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

**Answer:** A

**NEW QUESTION 26**

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 31**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 33**

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

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

**Answer:** B

**NEW QUESTION 38**

Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

- A. Centos Linux
- B. Gaia embedded
- C. Gaia
- D. Red Hat Enterprise Linux version 5

**Answer:** B

**Explanation:**

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

**NEW QUESTION 43**

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 44**

In HTTPS Inspection policy, what actions are available in the "Actions" column of a rule?

- A. "Inspect", "Bypass"
- B. "Inspect", "Bypass", "Categorize"
- C. "Inspect", "Bypass", "Block"
- D. "Detect", "Bypass"

**Answer:** A

**Explanation:**

[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 49**

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 53

A network administrator has informed you that they have identified a malicious host on the network, and instructed you to block it. Corporate policy dictates that firewall policy changes cannot be made at this time. What tool can you use to block this traffic?

- A. Anti-Bot protection
- B. Anti-Malware protection
- C. Policy-based routing
- D. Suspicious Activity Monitoring (SAM) rules

**Answer:** D

**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 55

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

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

**Answer:** C

#### NEW QUESTION 56

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

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

**Answer:** B

#### NEW QUESTION 61

What data MUST be supplied to the SmartConsole System Restore window to restore a backup?

- A. Server, Username, Password, Path, Version
- B. Username, Password, Path, Version
- C. Server, Protocol, Username, Password, Destination Path
- D. Server, Protocol, Username, Password, Path

**Answer:** D

**Explanation:**

References:

#### NEW QUESTION 62

You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

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

**Answer:** C

#### NEW QUESTION 67

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

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

**Answer:** B

#### NEW QUESTION 68

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 72

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 75

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 76

Fill in the blank: The position of an implied rule is manipulated in the \_\_\_\_\_ window.

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

**Answer:** C

#### Explanation:

"Note - In addition, users can access the Implied Rules configurations through Global Properties and use the implied policy view below Configuration."

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

#### NEW QUESTION 80

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

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

**Answer:** A

#### NEW QUESTION 82

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 86

Which back up method uses the command line to create an image of the OS?

- A. System backup
- B. Save Configuration
- C. Migrate
- D. snapshot

**Answer:** D

#### NEW QUESTION 89

Which message indicates IKE Phase 2 has completed successfully?

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

**Answer:** A

#### NEW QUESTION 93

Which part of SmartConsole allows administrators to add, edit delete, and clone objects?

- A. Object Browser
- B. Object Editor
- C. Object Navigator
- D. Object Explorer

**Answer:** D

#### NEW QUESTION 94

Fill in the blank: When a policy package is installed, \_\_\_\_\_ are also distributed to the target installation Security Gateways.

- A. User and objects databases
- B. Network databases
- C. SmartConsole databases
- D. User databases

**Answer:** A

#### Explanation:

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

The installation process:

If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.

#### NEW QUESTION 99

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 100

A stateful inspection firewall works by registering connection data and compiling this information. Where is the information stored?

- A. In the system SMEM memory pool.
- B. In State tables.
- C. In the Sessions table.
- D. In a CSV file on the firewall hard drive located in \$FWDIR/conf/.

**Answer:** B

#### Explanation:

The information stored in the state tables provides cumulative data that can be used to evaluate future connections.....

<https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-stateful-firewall/>

#### NEW QUESTION 105

What are the Threat Prevention software components available on the Check Point Security Gateway?



- A. IPS, Threat Emulation and Threat Extraction
- B. IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction
- C. IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction
- D. IDS, Forensics, Anti-Virus, Sandboxing

**Answer:** C

#### NEW QUESTION 109

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

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

**Answer:** D

#### NEW QUESTION 113

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 118

Which of the following commands is used to monitor cluster members?

- A. cphaprob state
- B. cphaprob status
- C. cphaprob
- D. cluster state

**Answer:** A

#### NEW QUESTION 121

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 123

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

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

**Answer:** B

#### NEW QUESTION 124

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 127

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 128

Which Threat Prevention profile uses sanitization technology?

- A. Cloud/data Center
- B. perimeter
- C. Sandbox
- D. Guest Network

**Answer:** B

#### Explanation:

Strict Security for Perimeter Profile & Perimeter Profile use sanitization as a technology in Threat prevention profile

#### NEW QUESTION 133

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 137

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 138

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 143

What Check Point technologies deny or permit network traffic?

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

**Answer:** B

#### NEW QUESTION 147

Which statement is TRUE of anti-spoofing?

- A. Anti-spoofing is not needed when IPS software blade is enabled
- B. It is more secure to create anti-spoofing groups manually
- C. It is BEST Practice to have anti-spoofing groups in sync with the routing table
- D. With dynamic routing enabled, anti-spoofing groups are updated automatically whenever there is a routing change

**Answer:** C

#### NEW QUESTION 152

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 155

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

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

**Answer:** A

#### NEW QUESTION 159

URL Filtering cannot be used to:

- A. Control Bandwidth issues
- B. Control Data Security
- C. Improve organizational security
- D. Decrease legal liability

**Answer:** D

#### Explanation:

[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 163

Which application is used for the central management and deployment of licenses and packages?

- A. SmartProvisioning
- B. SmartLicense
- C. SmartUpdate
- D. Deployment Agent

**Answer:** C

#### NEW QUESTION 166

What command from the CLI would be used to view current licensing?

- A. license view
- B. fw ctl tab -t license -s
- C. show license -s
- D. cplic print

**Answer:** D

#### NEW QUESTION 168

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 171

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 174

Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

- A. Symmetric routing
- B. Failovers
- C. Asymmetric routing
- D. Anti-Spoofing

**Answer:** B

#### NEW QUESTION 179

Which firewall daemon is responsible for the FW CLI commands?

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

**Answer:** A

#### NEW QUESTION 184

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

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

**Answer:** C

#### Explanation:

Endpoint Identity Agents and Browser-Based Authentication - When a high level of security is necessary.

Captive Portal is used for distributing the Endpoint Identity Agent. IP Spoofing protection can be set to prevent packets from being IP spoofed.

#### NEW QUESTION 189

The SIC Status “Unknown” means

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

**Answer:** C

#### Explanation:

SIC Status

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

#### NEW QUESTION 193

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 196

Which of the following log queries would show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1?

- A. src:192.168.1.1 OR dst:172.26.1.1 AND action:Drop
- B. src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop
- C. 192.168.1.1 AND 172.26.1.1 AND drop
- D. 192.168.1.1 OR 172.26.1.1 AND action:Drop

**Answer:** B

**NEW QUESTION 197**

Security Zones do not work with what type of defined rule?

- A. Application Control rule
- B. Manual NAT rule
- C. IPS bypass rule
- D. Firewall rule

**Answer:** B

**Explanation:**

<https://community.checkpoint.com/t5/Management/Workaround-for-manual-NAT-when-security-zones-are-use>

**NEW QUESTION 201**

When configuring Anti-Spoofing, which tracking options can an Administrator select?

- A. Log, Alert, None
- B. Log, Allow Packets, Email
- C. Drop Packet, Alert, None
- D. Log, Send SNMP Trap, Email

**Answer:** A

**Explanation:**

Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected: Log - Create a log entry (default)

Alert - Show an alert None - Do not log or alert

[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 203**

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

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

**Answer:** B

**Explanation:**

Shared Policies

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

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

Description Mobile Access

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

DLP

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

Geo Policy

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

**NEW QUESTION 206**

Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

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

**Answer:** B

**Explanation:**

The first rule is the automatic rule for the Accept All Encrypted Traffic feature. The Firewalls for the Security Gateways in the BranchOffices and LondonOffices VPN communities allow all VPN traffic from hosts in clients in these communities. Traffic to the Security Gateways is dropped. This rule is installed on all Security Gateways in these communities.

\* 2. Site to site VPN - Connections between hosts in the VPN domains of all Site to Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.

\* 3. Remote access - Connections between hosts in the VPN domains of RemoteAccess VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

**NEW QUESTION 210**

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

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



D. QoS

**Answer:** D

**Explanation:**

[https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP\\_R80.30\\_QoS\\_AdminGuide/html\\_fram](https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_QoS_AdminGuide/html_fram)

#### NEW QUESTION 211

The purpose of the Communication Initialization process is to establish a trust between the Security Management Server and the Check Point gateways. Which statement best describes this Secure Internal Communication (SIC)?

- A. After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA.
- B. Secure Internal Communications authenticates the security gateway to the SMS before http communications are allowed.
- C. A SIC certificate is automatically generated on the gateway because the gateway hosts a subordinate CA to the SMS ICA.
- D. New firewalls can easily establish the trust by using the expert password defined on the SMS and the SMS IP address.

**Answer:** A

**Explanation:**

[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 215

Which of the following is NOT a valid configuration screen of an Access Role Object?

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

**Answer:** C

#### NEW QUESTION 216

What is the default shell of Gaia CLI?

- A. clish
- B. Monitor
- C. Read-only
- D. Bash

**Answer:** A

**Explanation:**

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_Gaia\\_AdminGuide/Topics-GAG/C](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/C)

#### NEW QUESTION 220

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

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

**Answer:** A

#### NEW QUESTION 223

What is NOT an advantage of Stateful Inspection?

- A. High Performance
- B. Good Security
- C. No Screening above Network layer
- D. Transparency

**Answer:** A

#### NEW QUESTION 224

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 227

Can you use the same layer in multiple policies or rulebases?

- A. Yes - a layer can be shared with multiple policies and rules.
- B. No - each layer must be unique.
- C. No - layers cannot be shared or reused, but an identical one can be created.
- D. Yes - but it must be copied and pasted with a different name.

**Answer:** A

**Explanation:**

<https://community.checkpoint.com/t5/Management/Sharing-a-layer-across-different-policies/td-p/1660>

#### NEW QUESTION 231

Name the authentication method that requires token authenticator.

- A. SecureID
- B. Radius
- C. DynamicID
- D. TACACS

**Answer:** A

**Explanation:**

[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 233

.....

## 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