

## Exam Questions 156-215.81

Check Point Certified Security Administrator R81

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



#### NEW QUESTION 1

Which of the following are types of VPN communities?

- A. Pentagon, star, and combination
- B. Star, octagon, and combination
- C. Combined and star
- D. Meshed, star, and combination

**Answer:** D

#### NEW QUESTION 2

With URL Filtering, what portion of the traffic is sent to the Check Point Online Web Service for analysis?

- A. The complete communication is sent for inspection.
- B. The IP address of the source machine.
- C. The end user credentials.
- D. The host portion of the URL.

**Answer:** D

#### Explanation:

"A local cache that gives answers to 99% of URL categorization requests. When the cache does not have an answer, only the host name is sent to the Check Point Online Web Service for categorization. " [https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/24853/FILE/CP\\_R77\\_ApplicationControlURL](https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/24853/FILE/CP_R77_ApplicationControlURL)

#### NEW QUESTION 3

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 4

The default shell of the Gaia CLI is cli.sh. How do you change from the cli.sh shell to the advanced shell to run Linux commands?

- A. Execute the command 'enable' in the cli.sh shell
- B. Execute the 'conf t' command in the cli.sh shell
- C. Execute the command 'expert' in the cli.sh shell
- D. Execute the 'exit' command in the cli.sh shell

**Answer:** C

#### NEW QUESTION 5

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 6

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 7

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	NBT	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	https http	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 8

Name one limitation of using Security Zones in the network?

- A. Security zones will not work in Automatic NAT rules
- B. Security zone will not work in Manual NAT rules
- C. Security zones will not work in firewall policy layer
- D. Security zones cannot be used in network topology

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 9

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

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

**Answer:** B

#### Explanation:

Ref: [https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP\\_R80.40\\_LoggingAndMonitoring\\_Ad](https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_Ad)

#### NEW QUESTION 10

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 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 15

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 19**

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 23**

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 28**

Which command shows the installed licenses?

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

**Answer:** A

**NEW QUESTION 30**

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 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 34**

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 35**

Gaia has two default user accounts that cannot be deleted. What are those user accounts?

- A. Admin and Default
- B. Expert and Clish
- C. Control and Monitor

D. Admin and Monitor

**Answer:** D

#### NEW QUESTION 37

Tom has connected to the Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made?

- A. Tom will have to reboot his SmartConsole computer, clear the cache, and restore changes.
- B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
- C. Tom's changes will be lost since he lost connectivity and he will have to start again.
- D. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.

**Answer:** D

#### NEW QUESTION 41

Please choose correct command syntax to add an “emailserver1” host with IP address 10.50.23.90 using GAIa management CLI?

- A. host name myHost12 ip-address 10.50.23.90
- B. mgmt add host name ip-address 10.50.23.90
- C. add host name emailserver1 ip-address 10.50.23.90
- D. mgmt add host name emailserver1 ip-address 10.50.23.90

**Answer:** D

#### NEW QUESTION 45

What is the default shell for the command line interface?

- A. Clish
- B. Admin
- C. Normal
- D. Expert

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 48

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 53

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 57

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

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

**Answer:** C

#### NEW QUESTION 59

Which SmartConsole application shows correlated logs and aggregated data to provide an overview of potential threats and attack patterns?

- A. SmartEvent
- B. SmartView Tracker
- C. SmartLog
- D. SmartView Monitor

**Answer:** A

**Explanation:**

<https://www.checkpoint.com/downloads/products/smartevent-datasheet.pdf>

**NEW QUESTION 62**

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 67**

What is the purpose of a Clean-up Rule?

- A. Clean-up Rules do not server any purpose.
- B. Provide a metric for determining unnecessary rules.
- C. To drop any traffic that is not explicitly allowed.
- D. Used to better optimize a policy.

**Answer:** C

**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 72**

R80 is supported by which of the following operating systems:

- A. Windows only
- B. Gaia only
- C. Gaia, SecurePlatform, and Windows
- D. SecurePlatform only

**Answer:** B

**NEW QUESTION 76**

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

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

**Answer:** A

**NEW QUESTION 80**

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 84**

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 85

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 87

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 88

How would you determine the software version from the CLI?

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

**Answer:** A

#### NEW QUESTION 91

Fill in the blank: Each cluster, at a minimum, should have at least \_\_\_\_\_ interfaces.

- A. Five
- B. Two
- C. Three
- D. Four

**Answer:** C

#### NEW QUESTION 95

Which one of the following is a way that the objects can be manipulated using the new API integration in R80 Management?

- A. Microsoft Publisher
- B. JSON
- C. Microsoft Word
- D. RC4 Encryption

**Answer:** B

#### NEW QUESTION 98

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 100

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 103

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 108**

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 111**

Which tool is used to enable ClusterXL?

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

**Answer:** B

**NEW QUESTION 114**

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

- A. SmartDashboard
- B. SmartEvent
- C. SmartView Monitor
- D. SmartUpdate

**Answer:** B

**Explanation:**

SmartEvent correlates logs from all Check Point enforcement points, including end-points, to identify suspicious activity from the clutter. Rapid data analysis and custom event logs immediately alert administrators to anomalous behavior such as someone attempting to use the same credential in multiple geographies simultaneously. Ref: <https://www.checkpoint.com/products/smartevent/>

**NEW QUESTION 117**

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

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

**Answer:** A

**NEW QUESTION 122**

After the initial installation on Check Point appliance, you notice that the Management interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

- A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
- B. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
- C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
- D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

**Answer:** A

**NEW QUESTION 124**

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 127

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

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

**Answer:** A

#### NEW QUESTION 129

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 134

When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, what does that indicate?

- A. The gateway is not powered on.
- B. Incorrect routing to reach the gateway.
- C. The Admin would need to login to Read-Only mode
- D. Another Admin has made an edit to that object and has yet to publish the change.

**Answer:** D

#### NEW QUESTION 136

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 141

Which of the following is NOT a method used by Identity Awareness for acquiring identity?

- A. Remote Access
- B. Cloud IdP (Identity Provider)
- C. Active Directory Query
- D. RADIUS

**Answer:** B

#### Explanation:

[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 143

Gaia includes Check Point Upgrade Service Engine (CPUSE), which can directly receive updates for what components?

- A. The Security Gateway (SG) and Security Management Server (SMS) software and the CPUSE engine.
- B. Licensed Check Point products for the Gala operating system and the Gaia operating system itself.
- C. The CPUSE engine and the Gaia operating system.
- D. The Gaia operating system only.

**Answer:** B

#### 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 146

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.

**NEW QUESTION 147**

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 151**

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 156**

What are the three deployment options available for a security gateway?

- A. Standalone, Distributed, and Bridge Mode
- B. Bridge Mode, Remote, and Standalone
- C. Remote, Standalone, and Distributed
- D. Distributed, Bridge Mode, and Remote

**Answer:** A

**Explanation:**

[https://sc1.checkpoint.com/documents/R76/CP\\_R76\\_Installation\\_and\\_Upgrade\\_Guide-webAdmin/86429.htm](https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/86429.htm)

**NEW QUESTION 157**

Which default Gaia user has full read/write access?

- A. admin
- B. superuser
- C. monitor
- D. altuser

**Answer:** A

**Explanation:**

Has full read/write capabilities for all Gaia features, from the Gaia Portal and the Gaia Clish. This user has a User ID of 0, and therefore has all of the privileges of a root user. monitor Has read-only capabilities for all features in the Gaia Portal and the Gaia Clish, and can change its own password. You must give a password for this user before the account can be used.

**NEW QUESTION 161**

How do you manage Gaia?

- A. Through CLI and WebUI
- B. Through CLI only
- C. Through SmartDashboard only
- D. Through CLI, WebUI, and SmartDashboard

**Answer:** D

**NEW QUESTION 162**

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

- A. Explicit Drop
- B. Implied Drop
- C. Explicit CleanUp

D. Implicit Drop

**Answer:** C

**NEW QUESTION 165**

Which of the following is the most secure means of authentication?

- A. Password
- B. Certificate
- C. Token
- D. Pre-shared secret

**Answer:** B

**NEW QUESTION 168**

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 171**

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 172**

Fill in the blank: Once a certificate is revoked from the Security GateWay by the Security Management Server, the certificate information is \_\_\_\_\_.

- A. Sent to the Internal Certificate Authority.
- B. Sent to the Security Administrator.
- C. Stored on the Security Management Server.
- D. Stored on the Certificate Revocation List.

**Answer:** D

**NEW QUESTION 174**

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 179**

Which of the following is NOT an identity source used for Identity Awareness?

- A. Remote Access
- B. UserCheck
- C. AD Query
- D. RADIUS

**Answer:** B

**NEW QUESTION 184**

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 189

Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

- A. Firewall
- B. Application Control
- C. Anti-spam and Email Security
- D. Anti-Virus

**Answer:** D

#### 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)

#### NEW QUESTION 193

Secure Internal Communication (SIC) is handled by what process?

- A. CPM
- B. HTTPS
- C. FWD
- D. CPD

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 195

Name the utility that is used to block activities that appear to be suspicious.

- A. Penalty Box
- B. Drop Rule in the rulebase
- C. Suspicious Activity Monitoring (SAM)
- D. Stealth rule

**Answer:** C

#### Explanation:

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_CLI\\_ReferenceGuide/Topics-CLIG](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_CLI_ReferenceGuide/Topics-CLIG)

#### NEW QUESTION 196

Which is a main component of the Check Point security management architecture?

- A. Identity Collector
- B. Endpoint VPN client
- C. SmartConsole
- D. Proxy Server

**Answer:** C

#### Explanation:

<https://community.checkpoint.com/t5/Check-Point-for-Beginners-2-0/Part-1-The-Architecture/ba-p/88043> Security Gateway (SG) is usually deployed on the perimeter to control and secure traffic with Firewall and Threat Prevention capabilities.

Security Management Server (SMS) defines and controls security policies on the Gateways. It can also be used to as a log server with built-in system of log indexing (SmartLog) and event correlation (SmartEvent – a SIEM-like solution for Check Point products). Usually, SMS is the main element of central management with multiple Security Gateways in operation. Nevertheless, you need an SMS even if your security system has a single gateway only.

SmartConsole is a GUI administration tool to connect to SMS. Through this tool, a security administrator is able to prepare and apply security policies to the Security Gateways.

#### NEW QUESTION 199

How Capsule Connect and Capsule Workspace differ?

- A. Capsule Connect provides a Layer3 VP
- B. Capsule Workspace provides a Desktop with usable applications
- C. Capsule Workspace can provide access to any application
- D. Capsule Connect provides Business data isolation
- E. Capsule Connect does not require an installed application at client

**Answer:** A

#### NEW QUESTION 202

What is the main difference between Threat Extraction and Threat Emulation?

- A. Threat Emulation never delivers a file and takes more than 3 minutes to complete
- B. Threat Extraction always delivers a file and takes less than a second to complete
- C. Threat Emulation never delivers a file that takes less than a second to complete
- D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

**Answer:** B

#### NEW QUESTION 205

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. T 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 208

You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

- A. Right click Accept in the rule, select “More”, and then check “Enable Identity Captive Portal”
- B. On the firewall object, Legacy Authentication screen, check “Enable Identity Captive Portal”
- C. In the Captive Portal screen of Global Properties, check “Enable Identity Captive Portal”
- D. On the Security Management Server object, check the box “Identity Logging”

**Answer:** A

#### NEW QUESTION 210

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

#### NEW QUESTION 211

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 215

.....

## 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