

# CheckPoint

## Exam Questions 156-215.81

Check Point Certified Security Administrator R81



#### 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

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 3

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

- A. Go to clash-Run cpstop | Run cpstart
- B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
- C. Administrator does not need to perform any tas
- D. Check Point will make use of the newly installed CPU and Cores
- E. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

**Answer: B**

#### NEW QUESTION 4

Which one of the following is TRUE?

- A. Ordered policy is a sub-policy within another policy
- B. One policy can be either inline or ordered, but not both
- C. Inline layer can be defined as a rule action
- D. Pre-R80 Gateways do not support ordered layers

**Answer: C**

#### NEW QUESTION 5

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**

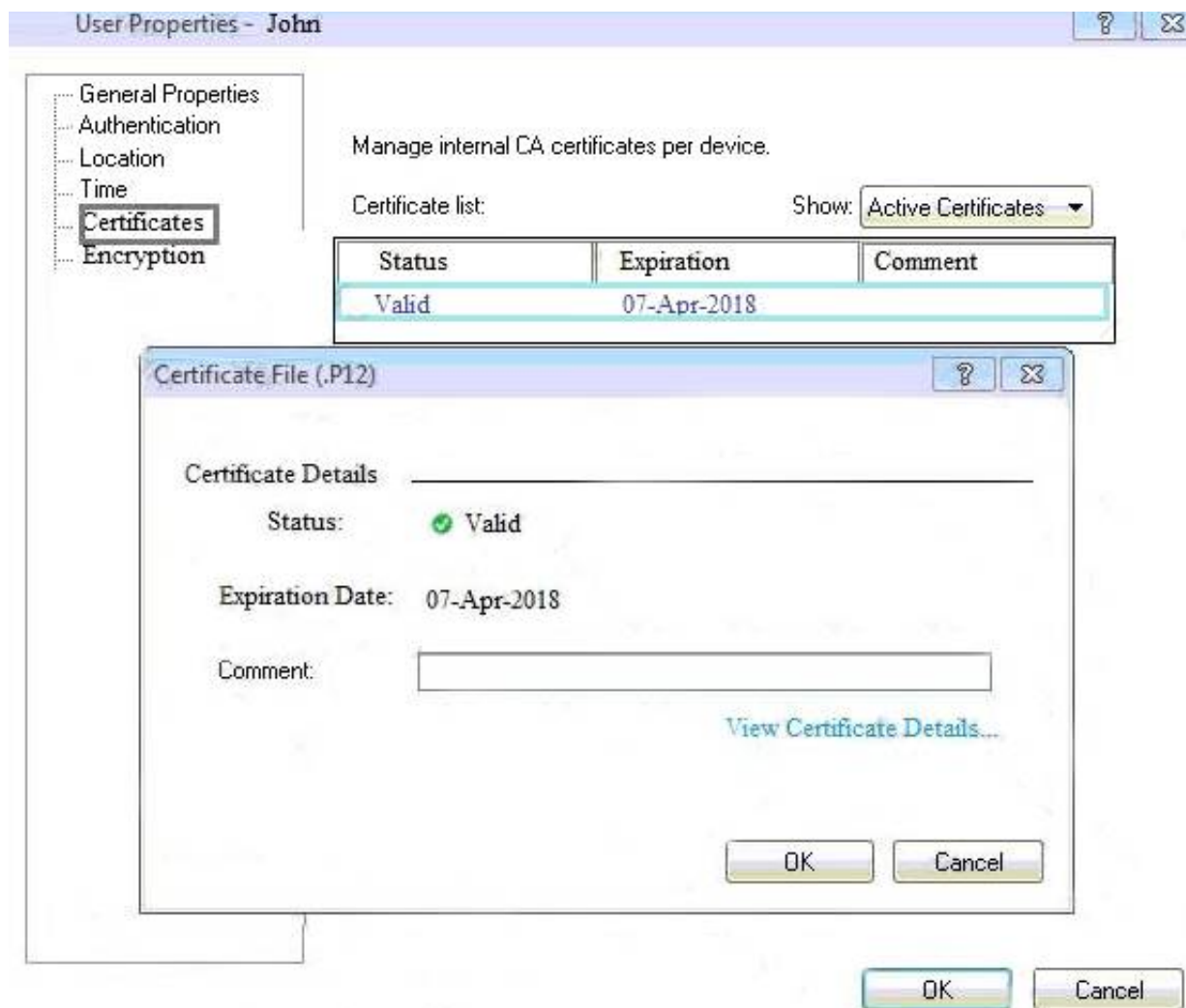
#### Explanation:

"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 6

You can see the following graphic:



What is presented on it?

- A. Properties of personal .p12 certificate file issued for user John.
- B. Shared secret properties of John's password.
- C. VPN certificate properties of the John's gateway.
- D. Expired .p12 certificate properties for user John.

**Answer: A**

#### NEW QUESTION 7

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 8

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 9

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 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 10

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 14

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 18

To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway does what with the data?

- A. Cache the data to speed up its own function.
- B. Share the data to the ThreatCloud for use by other Threat Prevention blades.
- C. Log the traffic for Administrator viewing.
- D. Delete the data to ensure an analysis of the data is done each time.

**Answer: B**

#### Explanation:

Data from malicious attacks are shared between the Threat Prevention Software Blades and help to keep your network safe. For example, the signatures from threats that Threat Emulation identifies are added to the ThreatCloud for use by the other Threat Prevention blades. src <https://infosec.co.il/wp-content/uploads/2020/06/12-GAiA-R80.40-Threat-Prevention.pdf> page 28.

#### NEW QUESTION 23

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 28

Which single Security Blade can be turned on to block both malicious files from being downloaded as well as block websites known to host malware?

- A. Anti-Bot
- B. None - both Anti-Virus and Anti-Bot are required for this
- C. Anti-Virus
- D. None - both URL Filtering and Anti-Virus are required for this.

**Answer: C**

#### Explanation:

Prevent Access to Malicious Websites

The Antivirus Software Blade scans outbound URL requests and ensures users do not visit websites that are known to distribute malware.

Stop Incoming Malicious Files

Check Point Antivirus Software Blade prevents and stops threats such as malware, viruses, and Trojans from entering and infecting a network.

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

### NEW QUESTION 33

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 36

What licensing feature is used to verify licenses and activate new licenses added to the License and Contracts repository?

- A. Verification tool
- B. Verification licensing
- C. Automatic licensing
- D. Automatic licensing and Verification tool

**Answer:** D

### NEW QUESTION 39

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 42

The Gateway Status view in SmartConsole shows the overall status of Security Gateways and Software Blades. What does the Status Attention mean?

- A. Cannot reach the Security Gateway.
- B. The gateway and all its Software Blades are working properly.
- C. At least one Software Blade has a minor issue, but the gateway works.
- D. Cannot make SIC between the Security Management Server and the Security Gateway

**Answer:** C

#### 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 45

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 Restore These options let you: To back up a configuration:  
The Backup window opens.

### NEW QUESTION 50

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 54

What Identity Agent allows packet tagging and computer authentication?

- A. Endpoint Security Client
- B. Full Agent
- C. Light Agent
- D. System Agent

**Answer:** B

**Explanation:**

Identity Agent Description Full

Default Identity AgentClosed that includes packet tagging and computer authentication. It applies to all users on the computer on which it is installed.

Administrator permissions are required to use the Full Identity Agent type. For the Full Identity Agent, you can enforce IP spoofing protection. In addition, you can leverage computer authentication if you specify computers in Access Roles.

Light

Default Identity Agent that does not include packet tagging and computer authentication. You can install this Identity Agent individually for each user on the target computer. Light Identity Agent type does not require Administrator permissions.

[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 55**

What is the purpose of Captive Portal?

- A. It manages user permission in SmartConsole
- B. It provides remote access to SmartConsole
- C. It authenticates users, allowing them access to the Internet and corporate resources
- D. It authenticates users, allowing them access to the Gaia OS

**Answer:** C

**Explanation:**

Captive Portal is a simple method that authenticates users with a web interface. When users try to access a protected web resource, they enter authentication information in a form that shows in their web browser.

[https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP\\_R80.30\\_IdentityAwareness\\_AdminG](https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_IdentityAwareness_AdminG)

**NEW QUESTION 58**

What is true about the IPS-Blade?

- A. in R80, IPS is managed by the Threat Prevention Policy
- B. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
- C. in R80, IPS Exceptions cannot be attached to “all rules”
- D. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

**Answer:** A

**NEW QUESTION 59**

What SmartEvent component creates events?

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

**Answer:** B

**NEW QUESTION 61**

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

- A. All-in-one (stand-alone)
- B. CloudGuard
- C. Distributed
- D. Bridge Mode

**Answer:** B

**NEW QUESTION 64**

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 66**



Which option will match a connection regardless of its association with a VPN community?

- 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 69

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 74

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 78

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 80

Which Check Point software blade monitors Check Point devices and provides a picture of network and security performance?

- A. Application Control
- B. Threat Emulation
- C. Logging and Status
- D. Monitoring

**Answer:** D

#### Explanation:

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_NextGenSecurityGateway\\_Guide/T](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T)

#### NEW QUESTION 84

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 86

What is the purpose of a Stealth Rule?

- A. A rule used to hide a server's IP address from the outside world.
- B. A rule that allows administrators to access SmartDashboard from any device.
- C. To drop any traffic destined for the firewall that is not otherwise explicitly allowed.
- D. A rule at the end of your policy to drop any traffic that is not explicitly allowed.

**Answer:** C

**NEW QUESTION 88**

How can the changes made by an administrator before publishing the session be seen by a superuser administrator?

- A. By impersonating the administrator with the 'Login as...' option
- B. They cannot be seen
- C. From the SmartView Tracker audit log
- D. From Manage and Settings > Sessions, right click on the session and click 'View Changes...'

**Answer:** D

**Explanation:**

From the Smartconsole, you can possibly view the changes via Manage & setting, Sessions

**NEW QUESTION 92**

Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?

- A. The firewall topologies
- B. NAT Rules
- C. The Rule Base
- D. The VPN Domains

**Answer:** C

**NEW QUESTION 95**

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 96**

When dealing with rule base layers, what two layer types can be utilized?

- A. Ordered Layers and Inline Layers
- B. Inbound Layers and Outbound Layers
- C. R81.10 does not support Layers
- D. Structured Layers and Overlap Layers

**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 98**

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

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

**Answer:** D

**Explanation:**

You can change the User Directory templates. Users associated with this template get the changes immediately. If you change user definitions manually in SmartConsole, the changes are immediate on the server.

[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 103**

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 104**

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 106**

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 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
- C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 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 107**

Fill in the blanks: The Application Layer Firewalls inspect traffic through \_\_\_\_\_ the layer(s) of the TCP/IP model and up to and including the \_\_\_\_\_ layer.

- A. Upper; Application
- B. First two; Internet
- C. Lower; Application
- D. First two; Transport

**Answer: C**

**Explanation:**

application firewalls, or application layer firewalls, use a series of configured policies to determine whether to block or allow communications to or from an app.

**NEW QUESTION 110**

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 111**

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 115**

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 120

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 123

True or False: The destination server for Security Gateway logs depends on a Security Management Server configuration.

- A. False, log servers are configured on the Log Server General Properties
- B. True, all Security Gateways will only forward logs with a SmartCenter Server configuration
- C. True, all Security Gateways forward logs automatically to the Security Management Server
- D. False, log servers are enabled on the Security Gateway General Properties

**Answer: B**

#### NEW QUESTION 127

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 129

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 132

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

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

**Answer: A**

#### NEW QUESTION 135

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 139

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 141**

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

- A. INSPECT Engine
- B. Next-Generation Firewall
- C. Packet Filtering
- D. Application Layer Firewall

**Answer:** A

**Explanation:**

Check Point FireWall-1's Stateful Inspection overcomes the limitations of the previous two approaches by providing full application-layer awareness without breaking the client/server model. With 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. This provides a solution which is highly secure and offers maximum performance, scalability, and extensibility.

**NEW QUESTION 142**

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 Gaia 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 147**

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 150**

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 153**

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

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

**Answer:** B

**NEW QUESTION 155**

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 160**

What key is used to save the current CPView page in a filename format cpview\_“cpview process ID”. cap”number of captures”?

- A. S
- B. W
- C. C
- D. Space bar

**Answer:** C

**NEW QUESTION 162**

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 165**

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 167**

Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using \_\_\_\_\_ .

- A. Captive Portal and Transparent Kerberos Authentication
- B. UserCheck
- C. User Directory
- D. Captive Portal

**Answer:** A

**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 171**

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 173**

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 175

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 176

What is the most recommended installation method for Check Point appliances?

- A. SmartUpdate installation
- B. DVD media created with Check Point ISOMorphic
- C. USB media created with Check Point ISOMorphic
- D. Cloud based installation

**Answer:** C

#### NEW QUESTION 177

What protocol is specifically used for clustered environments?

- A. Clustered Protocol
- B. Synchronized Cluster Protocol
- C. Control Cluster Protocol
- D. Cluster Control Protocol

**Answer:** D

#### NEW QUESTION 178

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 182

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 185

Fill in the blanks: A \_\_\_\_\_ license requires an administrator to designate a gateway for attachment whereas a \_\_\_\_\_ license is automatically attached to a Security Gateway.

- A. Formal; corporate
- B. Local; formal
- C. Local; central
- D. Central; local

**Answer:** D

#### NEW QUESTION 188

What are the three deployment considerations for a secure network?

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

**Answer:** A

**NEW QUESTION 191**

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 192**

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 194**

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 197**

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 202**

In SmartEvent, a correlation unit (CU) is used to do what?

- A. Collect security gateway logs, Index the logs and then compress the logs.
- B. Receive firewall and other software blade logs in a region and forward them to the primary log server.
- C. Analyze log entries and identify events.
- D. Send SAM block rules to the firewalls during a DOS attack.

**Answer:** C

**Explanation:**

[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 204**

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 206

Which statement describes what Identity Sharing is in Identity Awareness?

- A. Management servers can acquire and share identities with Security Gateways
- B. Users can share identities with other users
- C. Security Gateways can acquire and share identities with other Security Gateways
- D. Administrators can share identifies with other administrators

**Answer: C**

#### Explanation:

Identity Sharing

Best Practice - In environments that use many Security Gateways and AD Query, we recommend that you set only one Security Gateway to acquire identities from a given Active Directory domain controller for each physical site. If more than one Security Gateway gets identities from the same AD server, the AD server can become overloaded with WMI queries.

Set these options on the Identity Awareness > Identity Sharing page of the Security Gateway object:

#### NEW QUESTION 211

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 213

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 217

CPU-level of your Security gateway is peaking to 100% causing problems with traffic. You suspect that the problem might be the Threat Prevention settings. The following Threat Prevention Profile has been created.

### Company TP Profile

Provide very wide coverage for all products and protocols, with noticeable performance impact.

**General Policy**

IPS

Anti-Bot

Anti-Virus

Threat Emulation

Malware DNS Trap

**Blades Activation**

☒ IPS
 ☒ Anti-Bot
 ☒ Anti-Virus
 ☒ Threat Emulation

**Activate Protections**

Performance Impact:

Severity:

**Activation Mode**

High Confidence:

Medium Confidence:

Low Confidence:

How could you tune the profile in order to lower the CPU load still maintaining security at good level? Select the BEST answer.

- A. Set High Confidence to Low and Low Confidence to Inactive.
- B. Set the Performance Impact to Medium or lower.
- C. The problem is not with the Threat Prevention Profil
- D. Consider adding more memory to the appliance.

E. Set the Performance Impact to Very Low Confidence to Prevent.

**Answer:** B

**NEW QUESTION 218**

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 223**

Which repositories are installed on the Security Management Server by SmartUpdate?

- A. License and Update
- B. Package Repository and Licenses
- C. Update and License & Contract
- D. License & Contract and Package Repository

**Answer:** D

**Explanation:**

References:

**NEW QUESTION 228**

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 229**

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 232**

You want to store the GAIa configuration in a file for later reference. What command should you use?

- A. write mem <filename>
- B. show config -f <filename>
- C. save config -o <filename>
- D. save configuration <filename>

**Answer:** D

**NEW QUESTION 237**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 156-215.81 Practice Test Here](#)**