# CheckPoint

## Exam Questions 156-215.81

Check Point Certified Security Administrator R81

**NEW QUESTION 1**
Name the file that is an electronically signed file used by Check Point to translate the features in the license into a code?

A. Both License (.lic) and Contract (.xml) files
B. cp.macro
C. Contract file (.xml)
D. license File (.lie)

**Answer:** B

**Explanation:**
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

**NEW QUESTION 2**
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 3**
Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

A. RADIUS
B. Check Point password
C. Security questions
D. SecurID

**Answer:** C

**NEW QUESTION 4**
What are the two types of NAT supported by the Security Gateway?

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

**Answer:** B

**Explanation:**
A Security Gateway can use these procedures to translate IP addresses in your network:

**NEW QUESTION 5**
In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?

A. Limit
B. Resource
C. Custom Application / Site
D. Network Object

**Answer:** B

**NEW QUESTION 6**
Under which file is the proxy arp configuration stored?

A. $FWDIR/state/proxy_arp.conf on the management server
B. $FWDIR/conf/local.arp on the management server
C. $FWDIR/state/_tmp/proxy.arp on the security gateway
D. $FWDIR/conf/local.arp on the gateway

**Answer:** D

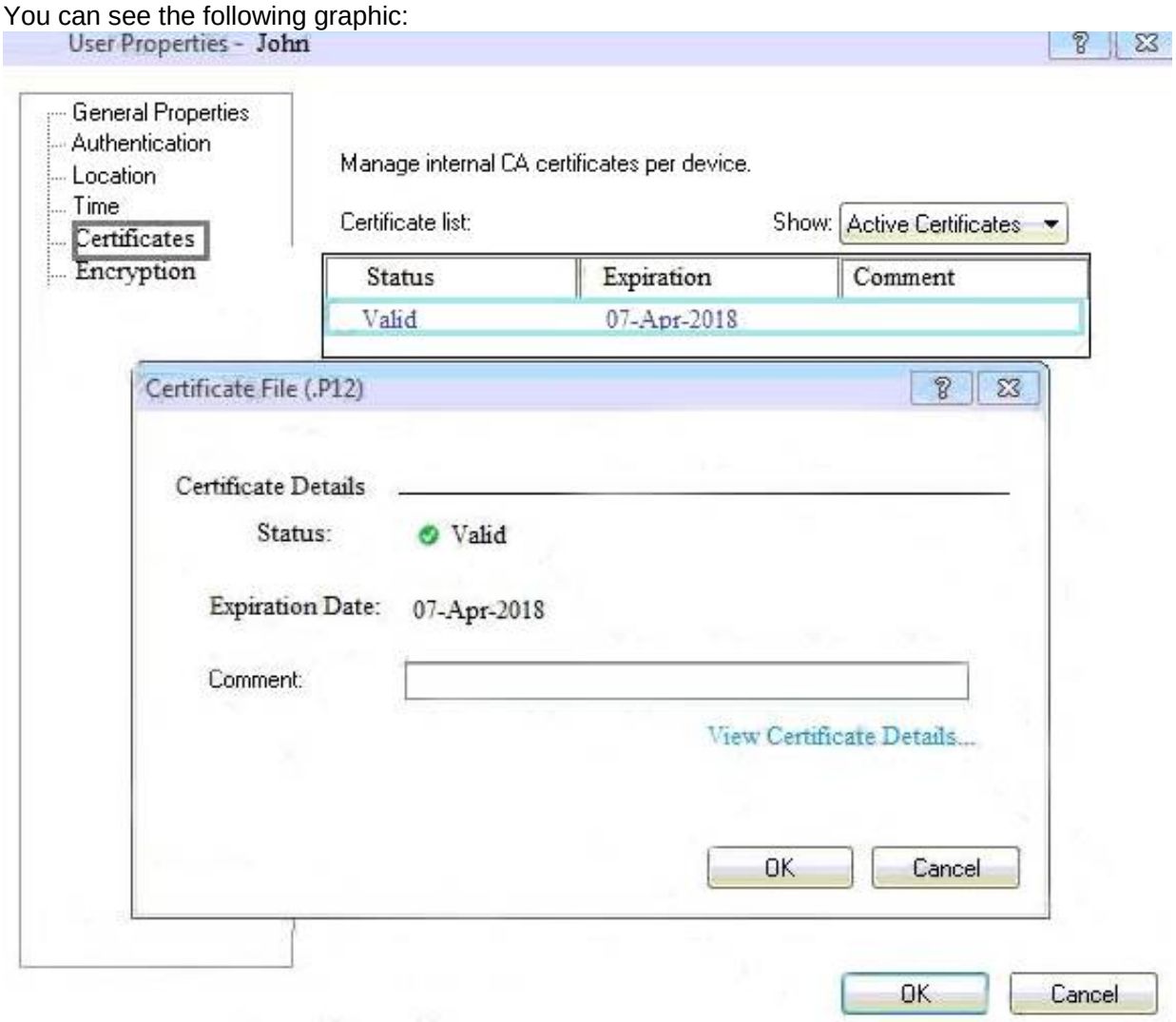
**NEW QUESTION 7**
The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?

A. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with any UID and assign role to the user.
B. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Createnew user with UID 0 and assign role to the user.

C. Create a new access role.Add expert-mode access to the role.Create new user with UID 0 and assign role to the user.
D. Create a new access role.Add expert-mode access to the role.Create new user with any UID and assign role to the user.

**Answer:** A

**NEW QUESTION 8**
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 9**
You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

A. Open SmartLog and connect remotely to the wireless controller
B. Open SmartEvent to see why they are being blocked
C. Open SmartDashboard and review the logs tab
D. From SmartConsole, go to the Log & Monitor and filter for the IP address of the tablet.

**Answer:** D

**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 10**
Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers? (Choose the best answer.)

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

**Answer:** B

**Explanation:**
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To "Check Point Antivirus Software Blade prevents

and stops
threats such as malware, viruses, and Trojans from entering and infecting a network"
Also here -https://www.checkpoint.com/downloads/products/antivirus-datasheet.pdf

**NEW QUESTION 11**
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 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

**NEW QUESTION 19**
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 23**
Session unique identifiers are passed to the web api using which http header option?

A. X-chkp-sid
B. Accept-Charset
C. Proxy-Authorization
D. Application

**Answer:** C

**NEW QUESTION 26**
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

**NEW QUESTION 30**
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 32**
Fill in the blank: Back up and restores can be accomplished through _____.

A. SmartConsole, WebUI, or CLI
B. WebUI, CLI, or SmartUpdate

C. CLI, SmartUpdate, or SmartBackup
D. SmartUpdate, SmartBackup, or SmartConsole

**Answer:** A

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

**NEW QUESTION 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 38**
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

**NEW QUESTION 42**
Check Point licenses come in two forms. What are those forms?

A. Central and Local.
B. Access Control and Threat Prevention.
C. On-premise and Public Cloud.
D. Security Gateway and Security Management.

**Answer:** A

**NEW QUESTION 45**
Which deployment adds a Security Gateway to an existing environment without changing IP routing?

A. Distributed
B. Bridge Mode
C. Remote
D. Standalone

**Answer:** B

**NEW QUESTION 50**
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 52**
SmartEvent does NOT use which of the following procedures to identity events:

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

**Answer:** C

**NEW QUESTION 56**
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 57**
Which Check Point software blade provides Application Security and identity control?

A. Identity Awareness
B. Data Loss Prevention
C. URL Filtering
D. Application Control

**Answer:** D

**Explanation:**
Check Point Application Control provides the industry's strongest application security and identity control to organizations of all sizes.

**NEW QUESTION 60**
Where is the "Hit Count" feature enabled or disabled in SmartConsole?

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

**Answer:** B

**Explanation:**
References:

**NEW QUESTION 61**
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 65**
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

**NEW QUESTION 67**
Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

A. The rule base can be built of layers, each containing a set of the security rule
B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
D. Time object to a rule to make the rule active only during specified times.
E. Sub Policies are sets of rules that can be created and attached to specific rule
F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

**Answer:** D

**NEW QUESTION 69**
What SmartEvent component creates events?

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

**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 73**
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 which scenario is it a valid option to transfer a license from one hardware device to another?

A. From a 4400 Appliance to a 2200 Appliance
B. From a 4400 Appliance to an HP Open Server
C. From an IBM Open Server to an HP Open Server
D. From an IBM Open Server to a 2200 Appliance

**Answer:** A

**Explanation:**
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

**NEW QUESTION 78**
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=

**NEW QUESTION 83**
In _____ NAT, the _____ is translated.

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

**Answer:** A

**NEW QUESTION 86**
If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
B. Change the Standby Security Management Server to Active.
C. Change the Active Security Management Server to Standby.
D. Manually synchronize the Active and Standby Security Management Servers.

**Answer:** A

**NEW QUESTION 90**
Choose what BEST describes users on Gaia Platform.

A. There are two default users and neither can be deleted.
B. There are two default users and one cannot be deleted.
C. There is one default user that can be deleted.
D. There is one default user that cannot be deleted.

**Answer:** A

**Explanation:**
These users are created by default and cannot be deleted: admin
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.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/U

**NEW QUESTION 91**
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 96**
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 100**
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 102**
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 106**
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

**NEW QUESTION 110**
Fill in the blank: Authentication rules are defined for _____.

A. User groups
B. Users using UserCheck
C. Individual users
D. All users in the database

**Answer:** A

**NEW QUESTION 114**
Application Control/URL filtering database library is known as:

A. Application database
B. AppWiki
C. Application-Forensic Database
D. Application Library

**Answer:** B

**Explanation:**
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

**NEW QUESTION 117**
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 122**
Fill in the blank: An LDAP server holds one or more _____.

A. Server Units
B. Administrator Units
C. Account Units
D. Account Servers

**Answer:** C

**NEW QUESTION 125**
Which of the following describes how Threat Extraction functions?

A. Detect threats and provides a detailed report of discovered threats
B. Proactively detects threats
C. Delivers file with original content
D. Delivers PDF versions of original files with active content removed

**Answer:** B

**NEW QUESTION 130**
Which of the following is used to enforce changes made to a Rule Base?

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

**Answer:** A

**NEW QUESTION 135**
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 ail 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

**NEW QUESTION 140**
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 145**
Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic?

A. Slow Path
B. Medium Path
C. Fast Path
D. Accelerated Path

**Answer:** A

**NEW QUESTION 146**
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 149**
You are going to perform a major upgrade. Which back up solution should you use to ensure your database can be restored on that device?

A. backup
B. logswitch
C. Database Revision
D. snapshot

**Answer:** D

**Explanation:**
The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system.
Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported.
The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be save

**NEW QUESTION 150**
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 153**

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 158**
Which type of attack can a firewall NOT prevent?

A. Network Bandwidth Saturation
B. Buffer Overflow
C. SYN Flood
D. SQL Injection

**Answer:** A

**NEW QUESTION 160**
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 161**
Is it possible to have more than one administrator connected to a Security Management Server at once?

A. Yes, but only if all connected administrators connect with read-only permissions.
B. Yes, but objects edited by one administrator will be locked for editing by others until the session is published.
C. No, only one administrator at a time can connect to a Security Management Server
D. Yes, but only one of those administrators will have write-permission
E. All others will have read-only permission.

**Answer:** B

**NEW QUESTION 166**
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 169**
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

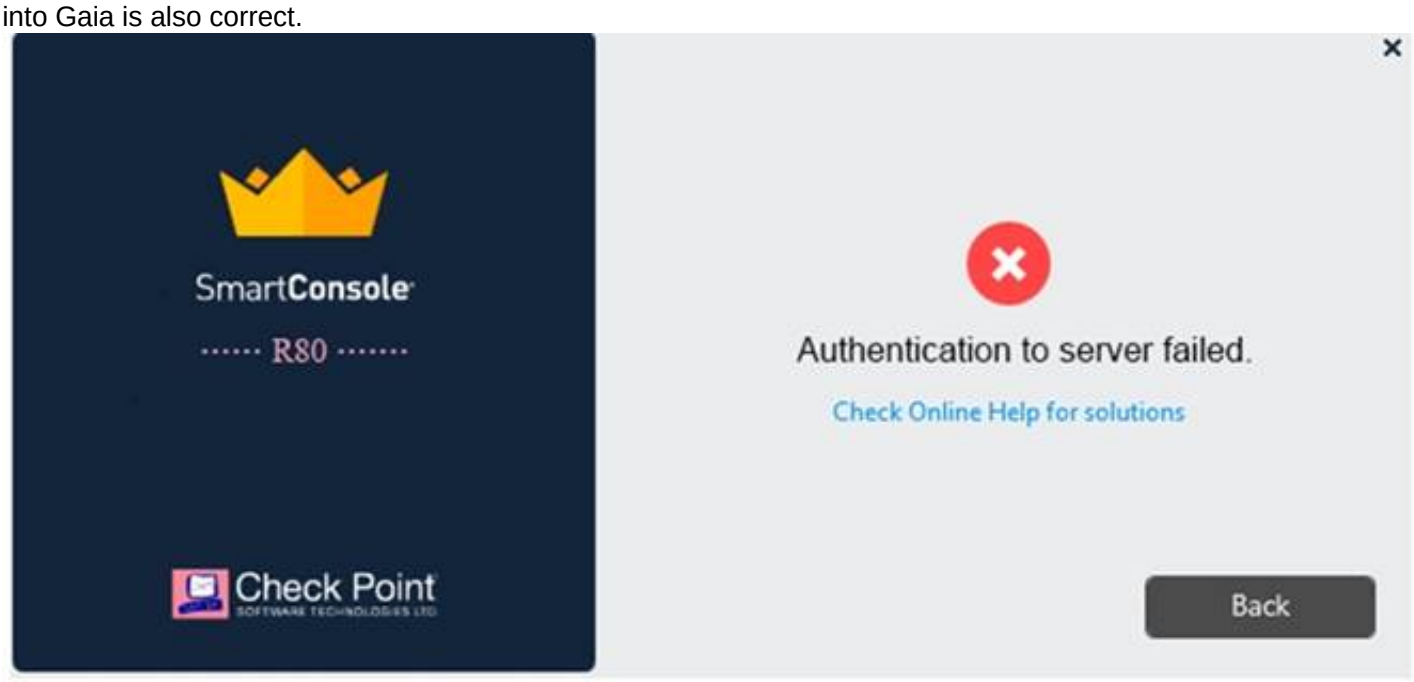
**NEW QUESTION 173**
Check Point ClusterXL Active/Active deployment is used when:

A. Only when there is Multicast solution set up
B. There is Load Sharing solution set up
C. Only when there is Unicast solution set up
D. There is High Availability solution set up

**Answer:** D

**NEW QUESTION 174**

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




What is the most likely reason?

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

**Answer:** B

**NEW QUESTION 179**
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

**NEW QUESTION 183**
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 188**
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 192**
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 196**
Which option in a firewall rule would only match and allow traffic to VPN gateways for one Community in common?

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

**Answer:** C

**NEW QUESTION 198**
Which of the following licenses are considered temporary?

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

**Answer:** A

**NEW QUESTION 199**
When a Security Gateway sends its logs to an IP address other than its own, which deployment option is installed?

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

**Answer:** A

**NEW QUESTION 202**
Which method below is NOT one of the ways to communicate using the Management API's?

A. Typing API commands using the "mgmt_cli" command
B. Typing API commands from a dialog box inside the SmartConsole GUI application
C. Typing API commands using Gaia's secure shell (clash)19+
D. Sending API commands over an http connection using web-services

**Answer:** D

**NEW QUESTION 204**
To enforce the Security Policy correctly, a Security Gateway requires:

A. a routing table
B. awareness of the network topology
C. a Demilitarized Zone
D. a Security Policy install

**Answer:** B

**Explanation:**
The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:

**NEW QUESTION 206**
When should you generate new licenses?

A. Before installing contract files.
B. After an RMA procedure when the MAC address or serial number of the appliance changes.
C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes.
D. Only when the license is upgraded.

**Answer:** C

**NEW QUESTION 210**
Which of the following is NOT a role of the SmartCenter:

A. Status monitoring
B. Policy configuration
C. Certificate authority

D. Address translation

**Answer:** C

**NEW QUESTION 212**
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 215**
Fill in the blank: SmartConsole, SmartEvent GUI client, and _____ allow viewing of billions of consolidated logs and shows them as prioritized security events.

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

**Answer:** A

**Explanation:**
"The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents"
https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=docume

**NEW QUESTION 218**
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 223**
Which firewall daemon is responsible for the FW CLI commands?

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

**Answer:** A

**NEW QUESTION 228**
Fill in the blank: An identity server uses a _____ for user authentication.

A. Shared secret
B. Certificate
C. One-time password
D. Token

**Answer:** A

**NEW QUESTION 229**
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 234**
In which deployment is the security management server and Security Gateway installed on the same appliance?

A. Standalone
B. Remote
C. Distributed
D. Bridge Mode

**Answer:** A

**Explanation:**
https://www.youtube.com/watch?v=BFNnBKQz5HA

**NEW QUESTION 239**
In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

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

**Answer:** C

**NEW QUESTION 243**
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 247**
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 249**
Which of the following is NOT an advantage to using multiple LDAP servers?

A. You achieve a faster access time by placing LDAP servers containing the database at remote sites
B. You achieve compartmentalization by allowing a large number of users to be distributed across several servers
C. Information on a user is hidden, yet distributed across several servers.
D. You gain High Availability by replicating the same information on several servers

**Answer:** C

**NEW QUESTION 250**
Most Check Point deployments use Gaia but which product deployment utilizes special Check Point code (with unification in R81.10)?

A. Enterprise Network Security Appliances
B. Rugged Appliances
C. Scalable Platforms
D. Small Business and Branch Office Appliances

**Answer:** A

**NEW QUESTION 254**
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=

**NEW QUESTION 255**
Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

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

**Answer:** D

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

**NEW QUESTION 256**
To view statistics on detected threats, which Threat Tool would an administrator use?

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

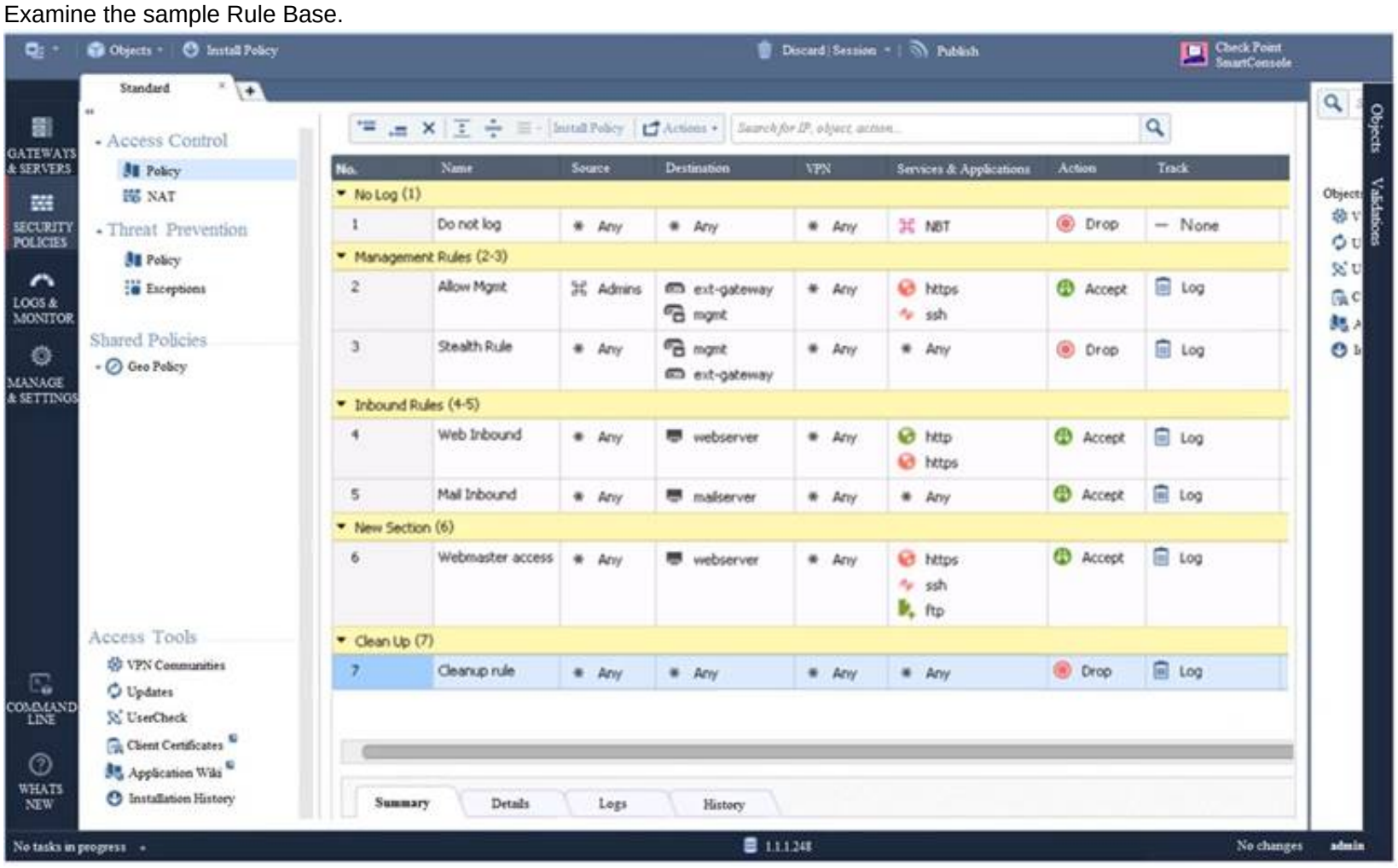
**Answer:** D

**NEW QUESTION 261**
Which SmartConsole tab is used to monitor network and security performance?

A. Manage & Settings
B. Security Policies
C. Gateway & Servers
D. Logs & Monitor

**Answer:** D

**NEW QUESTION 265**
Examine the sample Rule Base.




What will be the result of a verification of the policy from SmartConsole?

A. No errors or Warnings
B. Verification Erro
C. Empty Source-List in Rule 5 (Mail Inbound)
D. Verification Erro
E. Rule 4 (Web Inbound) hides Rule 6 (Webmaster access)
F. Verification Erro
G. Rule 7 (Clean-Up Rule) hides Implicit Clean-up Rule

**Answer:** C

**NEW QUESTION 266**
What command would show the API server status?

A. cpm status

B. api restart
C. api status
D. show api status

**Answer:** D

**NEW QUESTION 267**
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 268**
When using Monitored circuit VRRP, what is a priority delta?

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

**Answer:** C

**NEW QUESTION 269**
Which of the following is NOT a policy type available for each policy package?

A. Threat Emulation
B. Access Control
C. Desktop Security
D. Threat Prevention

**Answer:** A

**Explanation:**
References:

**NEW QUESTION 271**
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

**NEW QUESTION 275**
What is UserCheck?

A. Messaging tool user to verify a user’s credentials
B. Communication tool used to inform a user about a website or application they are trying to access
C. Administrator tool used to monitor users on their network
D. Communication tool used to notify an administrator when a new user is created

**Answer:** B

**Explanation:**
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T

**NEW QUESTION 277**
.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons 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