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
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 3
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 4
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

NEW QUESTION 5
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 6
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 7
When URL Filtering is set, what identifying data gets sent to the Check Point Online Web Service?

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

D. The URL and IP address are sent to the Check Point Online Web Service

Answer: C

NEW QUESTION 8
Fill in the blanks: Gaia can be configured using _______ the ________.

A. Command line interface; WebUI
B. Gaia Interface; GaiaUI
C. WebUI; Gaia Interface
D. GaiaUI; command line interface

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/C

NEW QUESTION 9
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 10
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 10
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 12
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

NEW QUESTION 17
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

NEW QUESTION 21

URL Filtering employs a technology, which educates users on web usage policy in real time. What is the name of that technology?

A. WebCheck
B. UserCheck
C. Harmony Endpoint
D. URL categorization

Answer: B

Explanation:
UserCheck alerts users while attemping to browse a suspicious/blocked or otherwise policy-limited website through a message in their web browsers shown before the actual page loads.

NEW QUESTION 22
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 27
Which tool allows you to monitor the top bandwidth on smart console?

A. Logs & Monitoring
B. Smart Event
C. Gateways & Severs Tab
D. SmartView Monitor

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 29
What is the purpose of the Clean-up Rule?

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

Answer: A

Explanation:
These are basic access control rules we recommend for all Rule Bases:
There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

NEW QUESTION 33
Fill in the blank: In Security Gateways R75 and above, SIC uses ________ for encryption.

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

Answer: A

NEW QUESTION 34
Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

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

Answer: D

NEW QUESTION 37
John is the administrator of a R80 Security Management server managing r R77.30 Check Point Security Gateway. John is currently updating the network objects and amending the rules using SmartConsole. To make John’s changes available to other administrators, and to save the database before installing a policy, what must John do?

A. Logout of the session
B. File > Save
C. Install database
D. Publish the session

Answer: D

Explanation:
Installing and Publishing
It is important to understand the differences between publishing and installing. You must do this:
After you did this: Publish
Opened a session in SmartConsole and made changes.
The Publish operation sends all SmartConsole modifications to other administrators, and makes the changes you made in a private session public.
Install the database
Modified network objects, such as servers, users, services, or IPS profiles, but not the Rule Base. Updates are installed on management servers and log servers.
Install a policy Changed the Rule Base.
The Security Management Server installs the updated policy and the entire database on Security Gateways (even if you did not modify any network objects).

NEW QUESTION 38
When a SAM rule is required on Security Gateway to quickly block suspicious connections which are not restricted by the Security Policy, what actions does the administrator need to take?

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

Answer: A

Explanation:
A Security GatewayClosed with SAM enabled has Firewall rules to block suspicious connections that are not restricted by the security policyClosed. These rules are applied immediately (policy installation is not required).
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 42
Core Protections are installed as part of what Policy?

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

Answer: A

Explanation:
Core protections - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy. ThreatCloud protections - Updated from the Check Point cloud, (see Updating IPS Protections). These protections are part of the Threat Prevention policy.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To

NEW QUESTION 45
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 47
Which is NOT an encryption algorithm that can be used in an IPSEC Security Association (Phase 2)?

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

Answer: B

NEW QUESTION 50

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

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

Answer: A

NEW QUESTION 55
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 57
Fill in the blank: _______ is the Gaia command that turns the server off.

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

Answer: C

NEW QUESTION 61
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 62
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 64
Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 68
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 70
Which two Identity Awareness daemons are used to support identity sharing?

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

Answer: D

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

NEW QUESTION 71
Both major kinds of NAT support Hide and Static NAT. However, one offers more flexibility. Which statement is true?

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

Answer: A

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

NEW QUESTION 74
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 75
Can multiple administrators connect to a Security Management Server at the same time?

A. No, only one can be connected
B. Yes, all administrators can modify a network object at the same time
C. Yes, every administrator has their own username, and works in a session that is independent of other administrators
D. Yes, but only one has the right to write

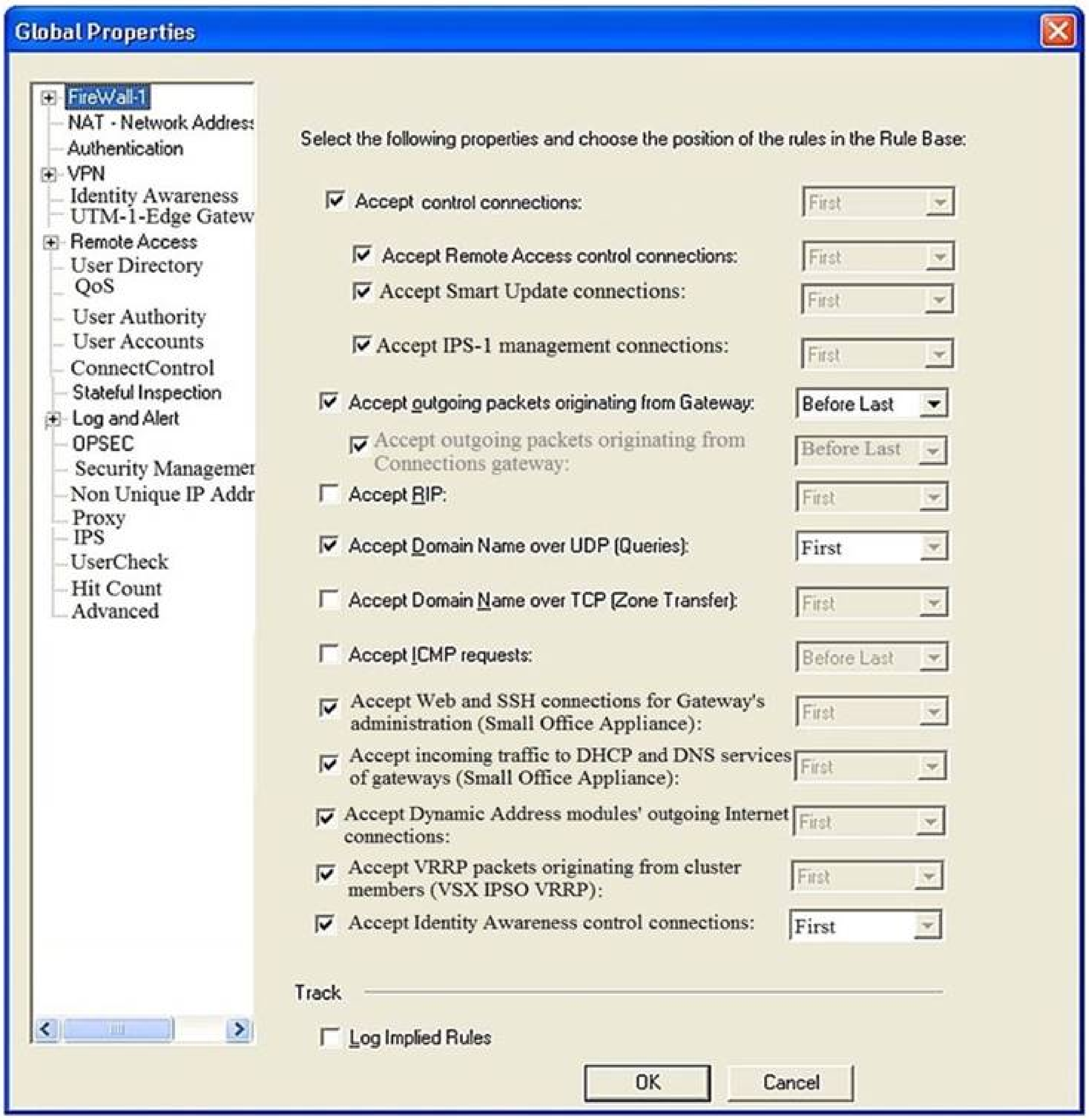
Answer: C

NEW QUESTION 80
You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

A. restore_backup
B. import backup
C. cp_merge
D. migrate import

Answer: A

NEW QUESTION 83
Consider the Global Properties following settings:



Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept control connections: First

☑ Accept Remote Access control connections: First

☑ Accept Smart Update connections: First

☑ Accept IPS-1 management connections: First

☑ Accept outgoing packets originating from Gateway: Before Last

☑ Accept outgoing packets originating from Connections gateway: Before Last

□ Accept RIP: First

☑ Accept Domain Name over UDP (Queries): First

□ Accept Domain Name over TCP (Zone Transfer): First

□ Accept ICMP requests: Before Last

☑ Accept Web and SSH connections for Gateway's administration (Small Office Appliance): First

☑ Accept incoming traffic to DHCP and DNS services of gateways (Small Office Appliance): First

☑ Accept Dynamic Address modules' outgoing Internet connections: First

☑ Accept VRRP packets originating from cluster members (VSX IPSO VRRP): First

☑ Accept Identity Awareness control connections: First

Track

□ Log Implied Rules

The selected option “Accept Domain Name over UDP (Queries)” means:

A. UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy.
B. All UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
C. No UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
D. All UDP Queries will be accepted by the traffic allowed by first explicit rule written by Administrator in a Security Policy.

Answer: A

NEW QUESTION 88
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 89
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 92
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 95
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 98
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 101
What is the default tracking option of a rule?

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

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 104
Stateful Inspection compiles and registers connections where?

A. Connection Cache
B. State Cache
C. State Table
D. Network Table

Answer: C

NEW QUESTION 108
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 109
Which backup utility captures the most information and tends to create the largest archives?

A. backup
B. snapshot
C. Database Revision
D. migrate export

Answer: B

NEW QUESTION 113
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

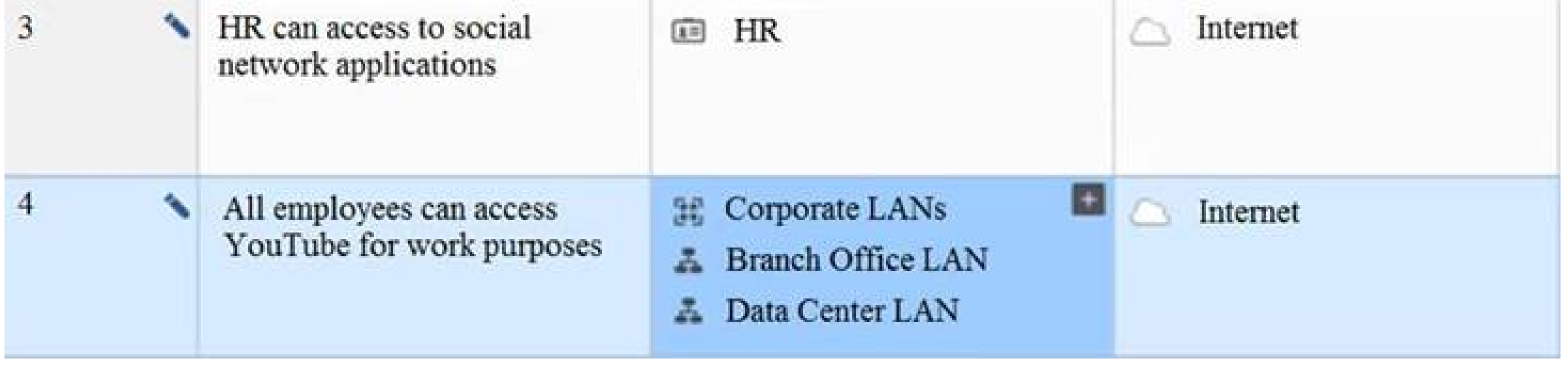
NEW QUESTION 117
Which SmartConsole application shows correlated logs and aggregated data to provide an overview of potential threats and attack patterns?

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

Answer: A

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

NEW QUESTION 118
View the rule below. What does the pen-symbol in the left column mean?



3 ✎	HR can access to social network applications	HR	Internet
4 ✎	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN Data Center LAN	Internet

A. Those rules have been published in the current session.
B. Rules have been edited by the logged in administrator, but the policy has not been published yet.
C. Another user has currently locked the rules for editing.
D. The configuration lock is presen
E. Click the pen symbol in order to gain the lock.

Answer: B

NEW QUESTION 121
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 122
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

NEW QUESTION 123

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

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

Answer: B

NEW QUESTION 126
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 129
The SmartEvent R80 Web application for real-time event monitoring is called:

A. SmartView Monitor
B. SmartEventWeb
C. There is no Web application for SmartEvent
D. SmartView

Answer: B

NEW QUESTION 132
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 136
Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

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

Answer: B

NEW QUESTION 140
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 144
You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Answer: B

NEW QUESTION 145

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=

NEW QUESTION 149
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 154
How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 156
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 157
To increase security, the administrator has modified the Core protection ‘Host Port Scan’ from ‘Medium’ to ‘High’ Predefined Sensitivity. Which Policy should the administrator install after Publishing the changes?

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

Answer: D

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

NEW QUESTION 162
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 166
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 169
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 174
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 177
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 180
Which of the following commands is used to verify license installation?

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

Answer: B

NEW QUESTION 184
Fill in the blank: When a policy package is installed, _______ are also distributed to the target installation Security Gateways.

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

Answer: A

Explanation:
A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:
The installation process:
If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.

NEW QUESTION 188
Which of the following is considered to be the more secure and preferred VPN authentication method?

A. Password
B. Certificate
C. MD5
D. Pre-shared secret

Answer: B

Explanation:
References:

NEW QUESTION 192
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 193
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 197
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 199
One of major features in R80.x SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?

A. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.
B. AdminA and AdminB are editing the same rule at the same time.
C. AdminB sees a pencil icon next the rule that AdminB is currently editing.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Answer: B

NEW QUESTION 201
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 206
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

NEW QUESTION 207
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 212
Which of the following commands is used to monitor cluster members?

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

Answer: A

NEW QUESTION 214
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 219
Where can administrator edit a list of trusted SmartConsole clients?

A. cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server.
B. In cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server, in SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
C. WebUI client logged to Security Management Server, SmartDashboard: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients, via cpconfig on a Security Gateway.
D. Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.

Answer: B

NEW QUESTION 220
Why is a Central License the preferred and recommended method of licensing?

A. Central Licensing is actually not supported with Gaia.
B. Central Licensing is the only option when deploying Gaia
C. Central Licensing ties to the IP address of a gateway and can be changed to any gateway if needed.
D. Central Licensing ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it changes.

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To

NEW QUESTION 225
What kind of NAT enables Source Port Address Translation by default?

A. Automatic Static NAT
B. Manual Hide NAT
C. Automatic Hide NAT
D. Manual Static NAT

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 230

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 234
When should you generate new licenses?

A. Before installing contract files.
B. After a device upgrade.
C. When the existing license expires, license is upgraded or the IP-address associated with the license changes.
D. Only when the license is upgraded.

Answer: C

NEW QUESTION 239
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 241
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 246
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 250
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

NEW QUESTION 254
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 257
Which icon in the WebUI indicates that read/write access is enabled?

A. Pencil
B. Padlock
C. Book
D. Eyeglasses

Answer: A

NEW QUESTION 258
Fill in the blanks: There are ______ types of software containers ______.

A. Three; security management, Security Gateway, and endpoint security
B. Three; Security gateway, endpoint security, and gateway management
C. Two; security management and endpoint security
D. Two; endpoint security and Security Gateway

Answer: A

Explanation:
There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security.

NEW QUESTION 259
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 260
Which key is created during Phase 2 of a site-to-site VPN?

A. Pre-shared secret
B. Diffie-Hellman Public Key
C. Symmetrical IPSec key
D. Diffie-Hellman Private Key

Answer: C

NEW QUESTION 263
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

NEW QUESTION 264
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 269
In the Check Point Security Management Architecture, which component(s) can store logs?

A. SmartConsole
B. Security Management Server and Security Gateway
C. Security Management Server
D. SmartConsole and Security Management Server

Answer: B

NEW QUESTION 272
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

A. Accounting
B. Suppression
C. Accounting/Suppression
D. Accounting/Extended

Answer: C

NEW QUESTION 273
When changes are made to a Rule base, it is important to _______ to enforce changes.

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

Answer: C

NEW QUESTION 278
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 281
There are four policy types available for each policy package. What are those policy types?

A. Access Control, Threat Prevention, Mobile Access and HTTPS Inspection
B. Access Control, Custom Threat Prevention, Autonomous Threat Prevention and HTTPS Inspection
C. There are only three policy types: Access Control, Threat Prevention and NAT.
D. Access Control, Threat Prevention, NAT and HTTPS Inspection

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 284
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

NEW QUESTION 287
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 290
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

NEW QUESTION 294
Which of the following is NOT supported by Bridge Mode on the Check Point Security Gateway?

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

Answer: D

Explanation:
NAT rules (specifically, Firewall kernel in logs shows the traffic as accepted, but Security Gateway does not actually forward it). For more information, see sk106146. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION 298
What default layers are included when creating a new policy layer?

A. Application Control, URL Filtering and Threat Prevention
B. Access Control, Threat Prevention and HTTPS Inspection
C. Firewall, Application Control and IPSec VPN
D. Firewall, Application Control and IPS

Answer: B

NEW QUESTION 301
What object type would you use to grant network access to an LDAP user group?

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

Answer: B

NEW QUESTION 306
Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

A. Export R80 configuration, clean install R80.10 and import the configuration
B. CPUSE online upgrade
C. CPUSE offline upgrade
D. SmartUpdate upgrade

Answer: C

NEW QUESTION 307
Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays ________ for the given VPN tunnel.

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

Answer: A

NEW QUESTION 308
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 310
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 314
How is communication between different Check Point components secured in R80? As with all questions, select the best answer.

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

Answer: B

NEW QUESTION 316
Which application is used for the central management and deployment of licenses and packages?

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

Answer: C

NEW QUESTION 321
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 323
True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway

A. True, CLI is the prefer method for Licensing
B. False, Central License are handled via Security Management Server
C. False, Central License are installed via Gaia on Security Gateways
D. True, Central License can be installed with CPLIC command on a Security Gateway

Answer: D

NEW QUESTION 324
What is the Transport layer of the TCP/IP model responsible for?

A. It transports packets as datagrams along different routes to reach their destination.
B. It manages the flow of data between two hosts to ensure that the packets are correctly assembled and delivered to the target application.
C. It defines the protocols that are used to exchange data between networks and how host programs interact with the Application layer.
D. It deals with all aspects of the physical components of network connectivity and connects with different network types.

Answer: B

NEW QUESTION 325
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 328
Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 330
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

NEW QUESTION 331
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 332
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 333
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 336
When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

A. Security Management Server’s /home/.fgpt file and is available for future SmartConsole authentications.
B. Windows registry is available for future Security Management Server authentications.
C. There is no memory used for saving a fingerprint anyway.
D. SmartConsole cache is available for future Security Management Server authentications.

Answer: D

NEW QUESTION 337
Security Gateway software blades must be attached to what?

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

Answer: B

Explanation:
Security Management and Security Gateway Software Blades must be attached to a Software Container to be licensed.
https://downloads.checkpoint.com/dc/download.htm?ID=11608

NEW QUESTION 341
Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

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

Answer: D

NEW QUESTION 344
Which tool is used to enable cluster membership on a Gateway?

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

Answer: B

Explanation:
References:

NEW QUESTION 345
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 348
How many users can have read/write access in Gaia Operating System at one time?

A. One
B. Three
C. Two
D. Infinite

Answer: A

Explanation:
if another user has r/w access, you need to use "lock database override" or "unlock database" to claim r/w access. Ref:
https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_Gaia_AdminGuide/html

NEW QUESTION 352
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 355
Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

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

Answer: A

NEW QUESTION 357
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 360
Security Zones do no work with what type of defined rule?

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

Answer: B

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

NEW QUESTION 361
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 363
Access roles allow the firewall administrator to configure network access according to:

A. remote access clients.
B. a combination of computer or computer groups and networks.
C. users and user groups.
D. All of the above.

Answer: D

Explanation:
To create an access role:
The Access Role window opens.
Your selection is shown in the Networks node in the Role Preview pane.
A window opens. You can search for Active Directory entries or select them from the list. You can search for AD entries or select them from the list.
The access role is added to the Users and Administrators tree.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 364
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 367
From SecureXL perspective, what are the tree paths of traffic flow:

A. Initial Path; Medium Path; Accelerated Path
B. Layer Path; Blade Path; Rule Path
C. Firewall Path; Accept Path; Drop Path
D. Firewall Path; Accelerated Path; Medium Path

Answer: D

NEW QUESTION 370
Fill in the blank: An Endpoint identity agent uses a _______ for user authentication.

A. Shared secret
B. Token
C. Username/password or Kerberos Ticket
D. Certificate

Answer: C

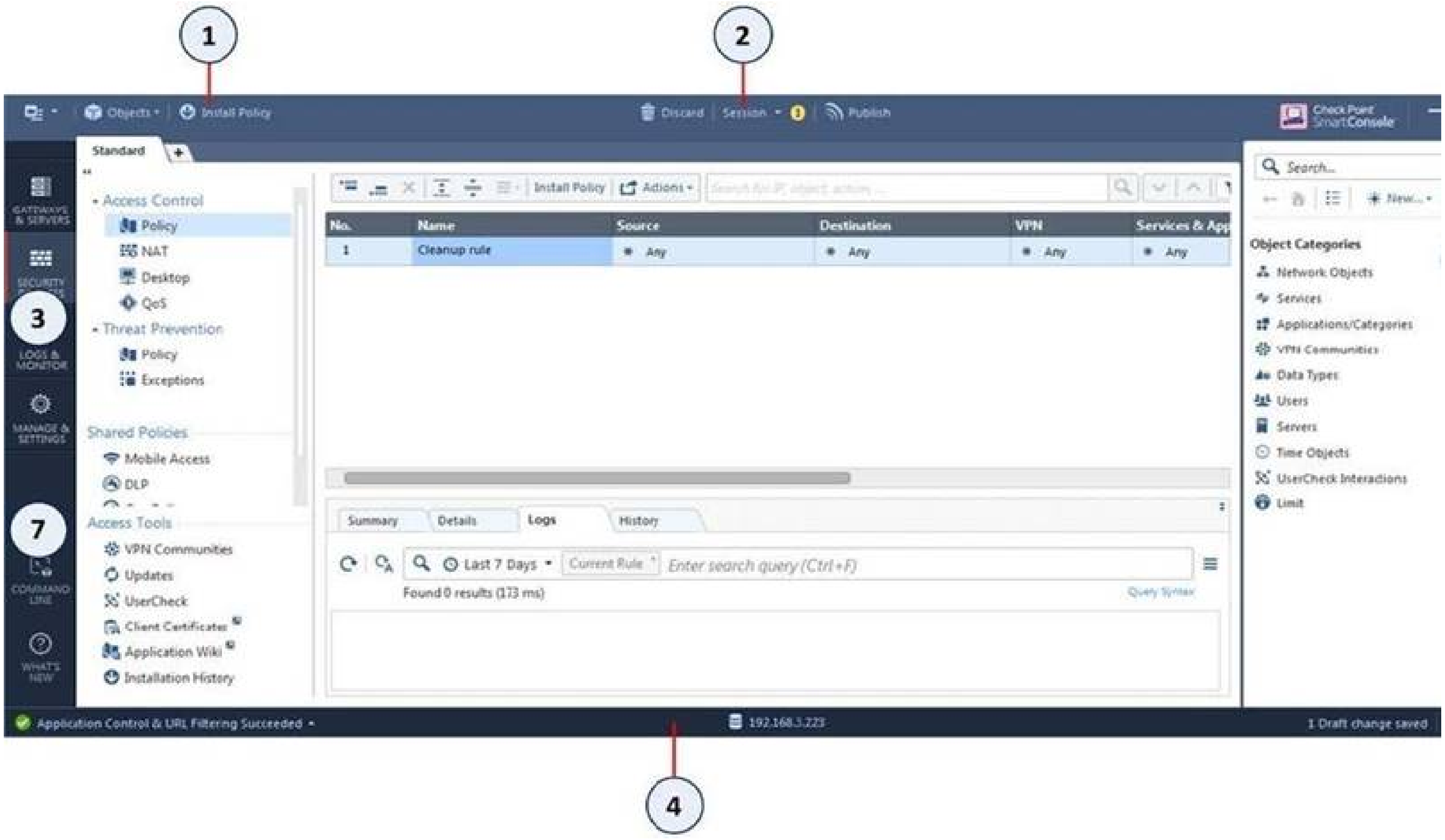
Explanation:
Two ways of auth: Username/Password in Captive Portal or Transparent Kerberos Auth through Kerberos Ticket.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 374
Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

A. Manage and Command Line
B. Logs and Monitor
C. Security Policies
D. Gateway and Servers

Answer: A

Explanation:



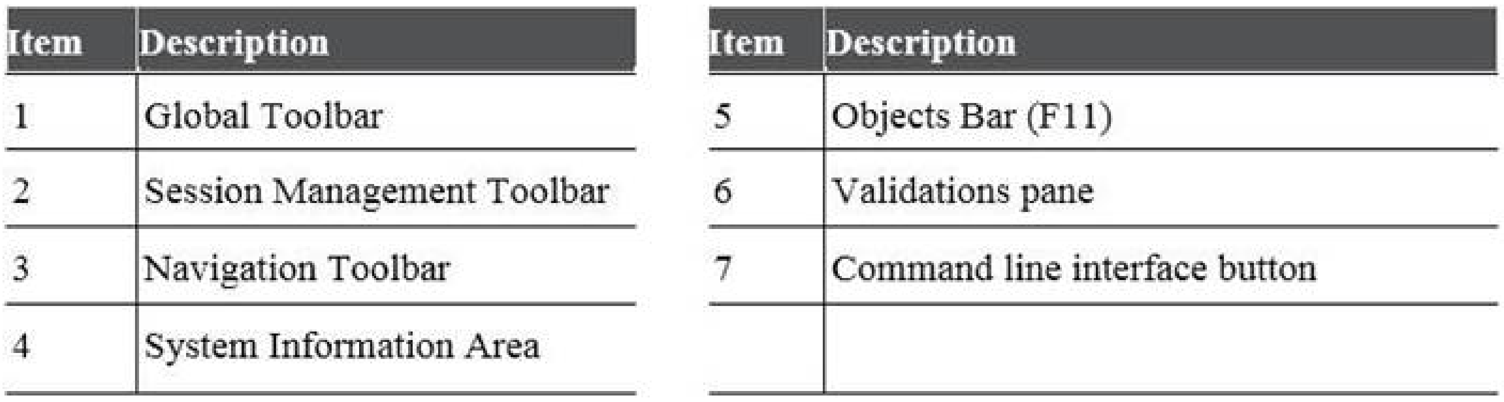
No.	Name	Source	Destination	VPN	Services & App
1	Cleanup rule	Any	Any	Any	Any

Found 0 results (173 ms)

Application Control & URL Filtering Succeeded

192.168.3.223

1 Draft change saved



Item	Description
1	Global Toolbar
2	Session Management Toolbar
3	Navigation Toolbar
4	System Information Area

Item	Description
5	Objects Bar (F11)
6	Validations pane
7	Command line interface button

NEW QUESTION 378
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

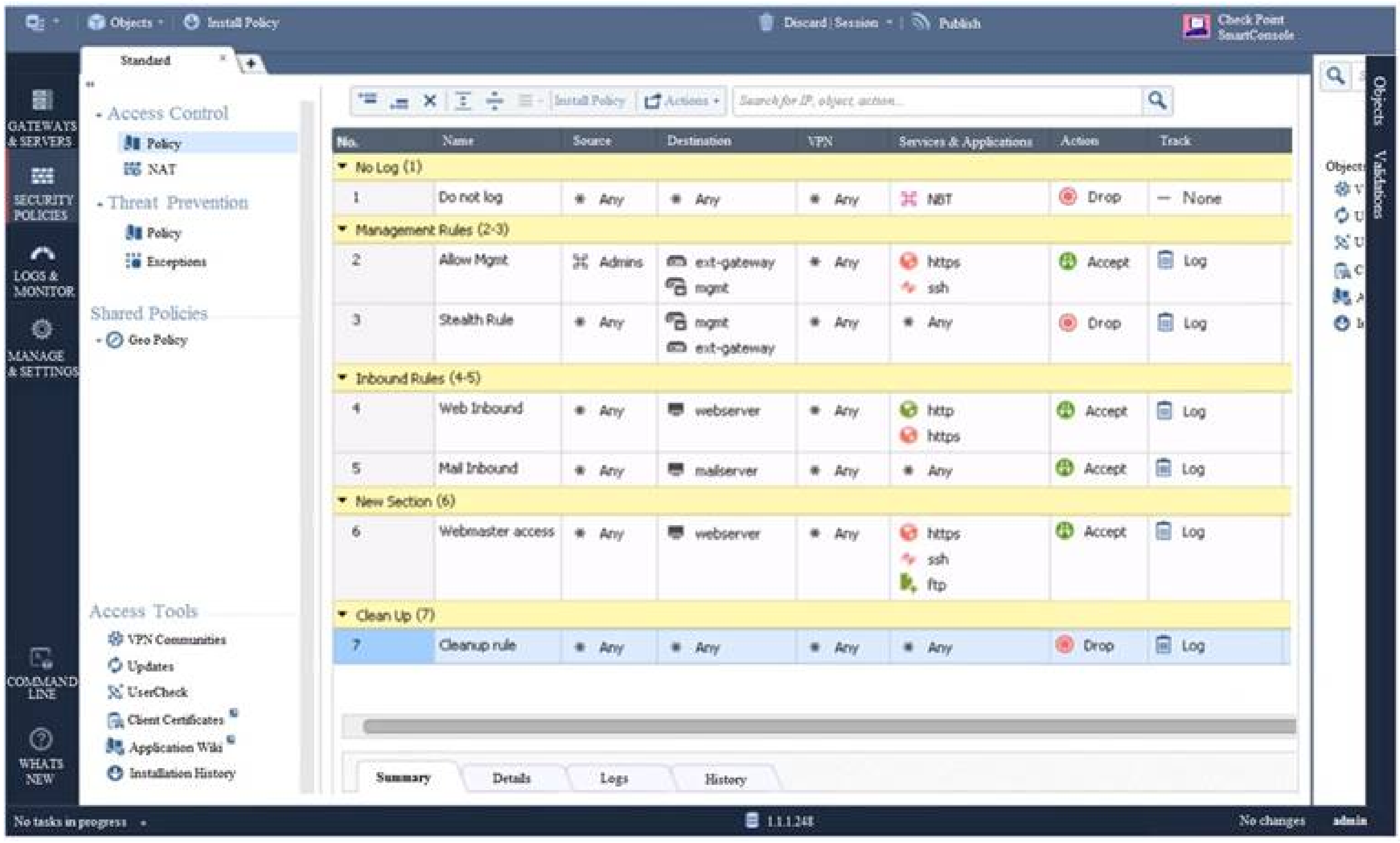
NEW QUESTION 379
Which is a main component of the Check Point security management architecture?

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 383
Examine the sample Rule Base.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
No Log (1)							
1	Do not log	Any	Any	Any	NBT	Drop	None
Management Rules (2-3)							
2	Allow Mgmt	Admins	ext-gateway mgmt	Any	https ssh	Accept	Log
3	Stealth Rule	Any	mgmt ext-gateway	Any	Any	Drop	Log
Inbound Rules (4-5)							
4	Web Inbound	Any	webserver	Any	http https	Accept	Log
5	Mail Inbound	Any	mailserver	Any	Any	Accept	Log
New Section (6)							
6	Webmaster access	Any	webserver	Any	https ssh ftp	Accept	Log
Clean Up (7)							
7	Cleanup rule	Any	Any	Any	Any	Drop	Log

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 386
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 387
Which of the following is NOT supported by Bridge Mode Check Point Security Gateway

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

Answer: C

NEW QUESTION 389
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 393
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

NEW QUESTION 395
What is a role of Publishing?

A. The Publish operation sends the modifications made via SmartConsole in the private session and makes them public
B. The Security Management Server installs the updated policy and the entire database on Security Gateways
C. The Security Management Server installs the updated session and the entire Rule Base on Security Gateways
D. Modifies network objects, such as servers, users, services, or IPS profiles, but not the Rule Base

Answer: A

NEW QUESTION 397
Identity Awareness allows the Security Administrator to configure network access based on which of the following?

A. Name of the application, identity of the user, and identity of the machine
B. Identity of the machine, username, and certificate
C. Network location, identity of a user, and identity of a machine
D. Browser-Based Authentication, identity of a user, and network location

Answer: C

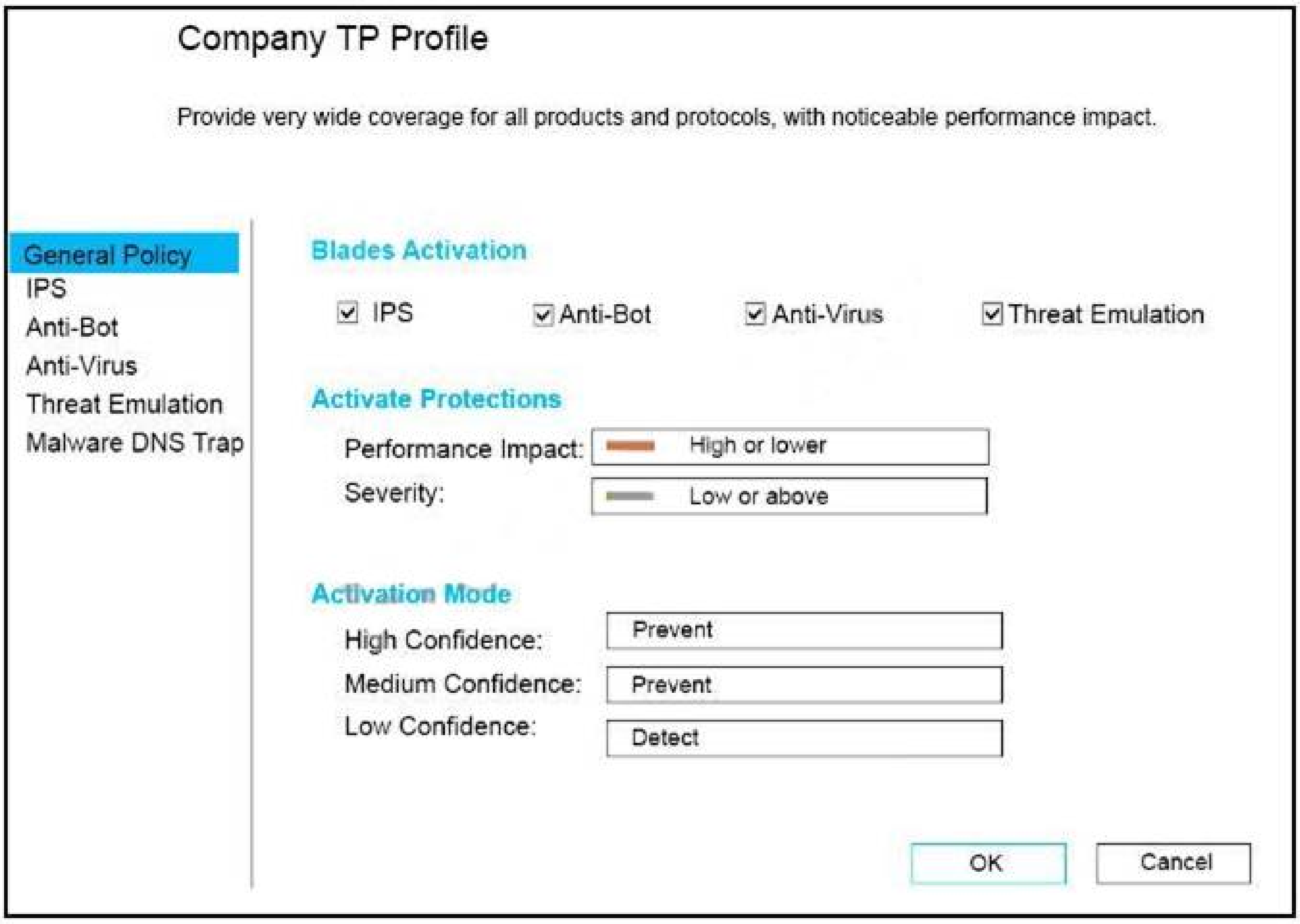
NEW QUESTION 398
What command would show the API server status?

A. cpm status

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

Answer: D

NEW QUESTION 399
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.

Blades Activation

☑ IPS ☑ Anti-Bot ☑ Anti-Virus ☑ Threat Emulation

Activate Protections

Performance Impact: High or lower
Severity: Low or above

Activation Mode

High Confidence: Prevent
Medium Confidence: Prevent
Low Confidence: Detect

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 400
The purpose of the Communication Initialization process is to establish a trust between the Security Management Server and the Check Point gateways. Which statement best describes this Secure Internal
Communication (SIC)?

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

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 403
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 408
What is the difference between SSL VPN and IPSec VPN?

A. IPSec VPN does not require installation of a resident VPN client
B. SSL VPN requires installation of a resident VPN client

C. SSL VPN and IPSec VPN are the same
D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser

Answer: D

NEW QUESTION 409
Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or _______.

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

Answer: C

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

NEW QUESTION 414
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 418
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 422
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 427
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 432
Can you use the same layer in multiple policies or rulebases?

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

D. Yes - but it must be copied and pasted with a different name.

Answer: A

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

NEW QUESTION 433
When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

A. Any size
B. Less than 20GB
C. More than 10GB and less than 20 GB
D. At least 20GB

Answer: D

NEW QUESTION 436
Fill in the blank: With the User Directory Software Blade, you can create user definitions on a(n) _______ Server.

A. SecurID
B. LDAP
C. NT domain
D. SMTP

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 438
......

Relate Links

100% Pass Your 156-215.81 Exam with Exambible Prep Materials

https://www.exambible.com/156-215.81-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/