Exam Questions 156-215.81

Check Point Certified Security Administrator R81

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

NEW QUESTION 1
An administrator wishes to enable Identity Awareness on the Check Point firewalls. However they allow users to use company issued or personal laptops. Since the administrator cannot manage the personal laptops, which of the following methods would BEST suit this company?

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

Answer: B

NEW QUESTION 2
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 3
What is the best sync method in the ClusterXL deployment?

A. Use 1 cluster + 1st sync
B. Use 1 dedicated sync interface
C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
D. Use 2 clusters + 1st sync + 2nd sync

Answer: B

NEW QUESTION 4
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 5
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 6
Which of the following is NOT a component of a Distinguished Name?

A. Common Name
B. Country
C. User container
D. Organizational Unit

Answer: C

NEW QUESTION 7
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 8
Name one limitation of using Security Zones in the network?

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

Answer: B

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

NEW QUESTION 9
When enabling tracking on a rule, what is the default option?

A. Accounting Log
B. Extended Log
C. Log
D. Detailed Log

Answer: C

NEW QUESTION 10
What are the types of Software Containers?

A. Smart Console, Security Management, and Security Gateway
B. Security Management, Security Gateway, and Endpoint Security
C. Security Management, Log & Monitoring, and Security Policy
D. Security Management, Standalone, and Security Gateway

Answer: B

NEW QUESTION 10
A SAM rule Is implemented to provide what function or benefit?

A. Allow security audits.
B. Handle traffic as defined in the policy.
C. Monitor sequence activity.
D. Block suspicious activity.

Answer: D

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

NEW QUESTION 12
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 15
Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?

A. All options stop Check Point processes
B. backup
C. migrate export
D. snapshot

Answer: D

NEW QUESTION 18
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 20
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 24
John is using Management HA. Which Smartcenter should be connected to for making changes?

A. secondary Smartcenter
B. active Smartcenter
C. connect virtual IP of Smartcenter HA
D. primary Smartcenter

Answer: B

NEW QUESTION 28
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 31
What is the main difference between Static NAT and Hide NAT?

A. Static NAT only allows incoming connections to protect your network.
B. Static NAT allow incoming and outgoing connection
C. Hide NAT only allows outgoing connections.
D. Static NAT only allows outgoing connection
E. Hide NAT allows incoming and outgoing connections.
F. Hide NAT only allows incoming connections to protect your network.

Answer: B

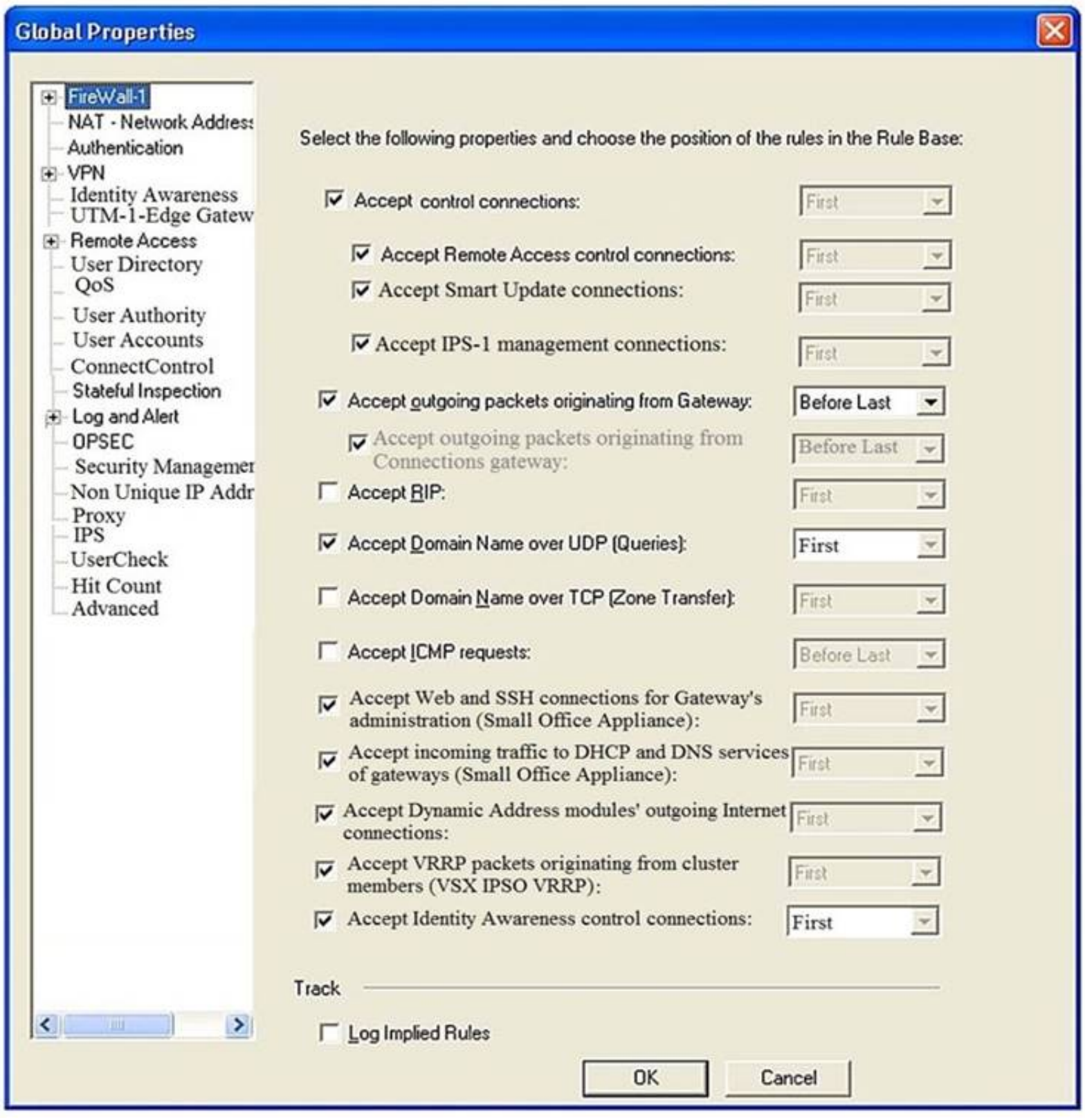
Explanation:
Hide NAT only translates the source address to hide it behind a gateway.

NEW QUESTION 32
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 33
Consider the Global Properties following settings:



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 34
Gaia has two default user accounts that cannot be deleted. What are those user accounts?

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

Answer: D

NEW QUESTION 37
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 38

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 43
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 47
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 48
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 52
You have discovered suspicious activity in your network. What is the BEST immediate action to take?

A. Create a policy rule to block the traffic.
B. Create a suspicious action rule to block that traffic.
C. Wait until traffic has been identified before making any changes.
D. Contact ISP to block the traffic.

Answer: B

NEW QUESTION 57
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 58
What SmartEvent component creates events?

A. Consolidation Policy

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

Answer: B

NEW QUESTION 62
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 66
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 71
What two ordered layers make up the Access Control Policy Layer?

A. URL Filtering and Network
B. Network and Threat Prevention
C. Application Control and URL Filtering
D. Network and Application Control

Answer: D

NEW QUESTION 76
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 80
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 82
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 83
A stateful inspection firewall works by registering connection data and compiling this information. Where is the information stored?

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

Answer: B

Explanation:
The information stored in the state tables provides cumulative data that can be used to evaluate future connections.....
https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-stateful-firewall/

NEW QUESTION 88
What is the purpose of a Stealth Rule?

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

Answer: C

NEW QUESTION 92
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 95
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 99
What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

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

Answer: D

NEW QUESTION 103
Which one of the following is a way that the objects can be manipulated using the new API integration in R80 Management?

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

Answer: B

NEW QUESTION 106
In SmartConsole, on which tab are Permissions and Administrators defined?

A. Manage and Settings
B. Logs and Monitor
C. Security Policies
D. Gateways and Servers

Answer: A

NEW QUESTION 111
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 116
To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members? Choose the best answer.

A. fw ctl set int fwha vmac global param enabled
B. fw ctl get int fwha vmac global param enabled; result of command should return value 1
C. cphaprob –a if
D. fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1

Answer: B

NEW QUESTION 117
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 122
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 125
Which of the following commands is used to monitor cluster members in CLI?

A. show cluster state
B. show active cluster
C. show clusters
D. show running cluster

Answer: A

NEW QUESTION 128
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 131
Which two of these Check Point Protocols are used by ?

A. ELA and CPD
B. FWD and LEA
C. FWD and CPLOG
D. ELA and CPLOG

Answer: B

NEW QUESTION 134
When comparing Stateful Inspection and Packet Filtering, what is a benefit that Stateful Inspection offers over Packer Filtering?

A. Stateful Inspection offers unlimited connections because of virtual memory usage.
B. Stateful Inspection offers no benefits over Packet Filtering.
C. Stateful Inspection does not use memory to record the protocol used by the connection.
D. Only one rule is required for each connection.

Answer: D

NEW QUESTION 137
When an encrypted packet is decrypted, where does this happen?

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

Answer: A

NEW QUESTION 142
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 147
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 149
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 152
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 153
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 156
DLP and Geo Policy are examples of what type of Policy?

A. Inspection Policies
B. Shared Policies
C. Unified Policies
D. Standard Policies

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_NextGenSecurityGateway_G

NEW QUESTION 160
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 163
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 167
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 168
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 172
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 174
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 176
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 181
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 184
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 185
Which two Identity Awareness commands are used to support identity sharing?

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

Answer: A

NEW QUESTION 187
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 192
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 197
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 202
What is the main objective when using Application Control?

A. To filter out specific content.
B. To assist the firewall blade with handling traffic.
C. To see what users are doing.
D. Ensure security and privacy of information.

Answer: A

Explanation:
https://www.checkpoint.com/cyber-hub/network-security/what-is-application-control/

NEW QUESTION 203
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 205
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 206
Which Identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

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

Answer: C

Explanation:
Endpoint Identity Agents and Browser-Based Authentication - When a high level of security is necessary.
Captive Portal is used for distributing the Endpoint Identity Agent. IP Spoofing protection can be set to prevent packets from being IP spoofed.

NEW QUESTION 207
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 211
Which of the following cannot be configured in an Access Role Object?

A. Networks
B. Users

C. Time
D. Machines

Answer: C

Explanation:
Access Role objects includes one or more of these objects: Networks.
Users and user groups. Computers and computer groups. Remote Access Clients.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 216
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 219
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 220
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 222
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 224
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 228
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 230
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

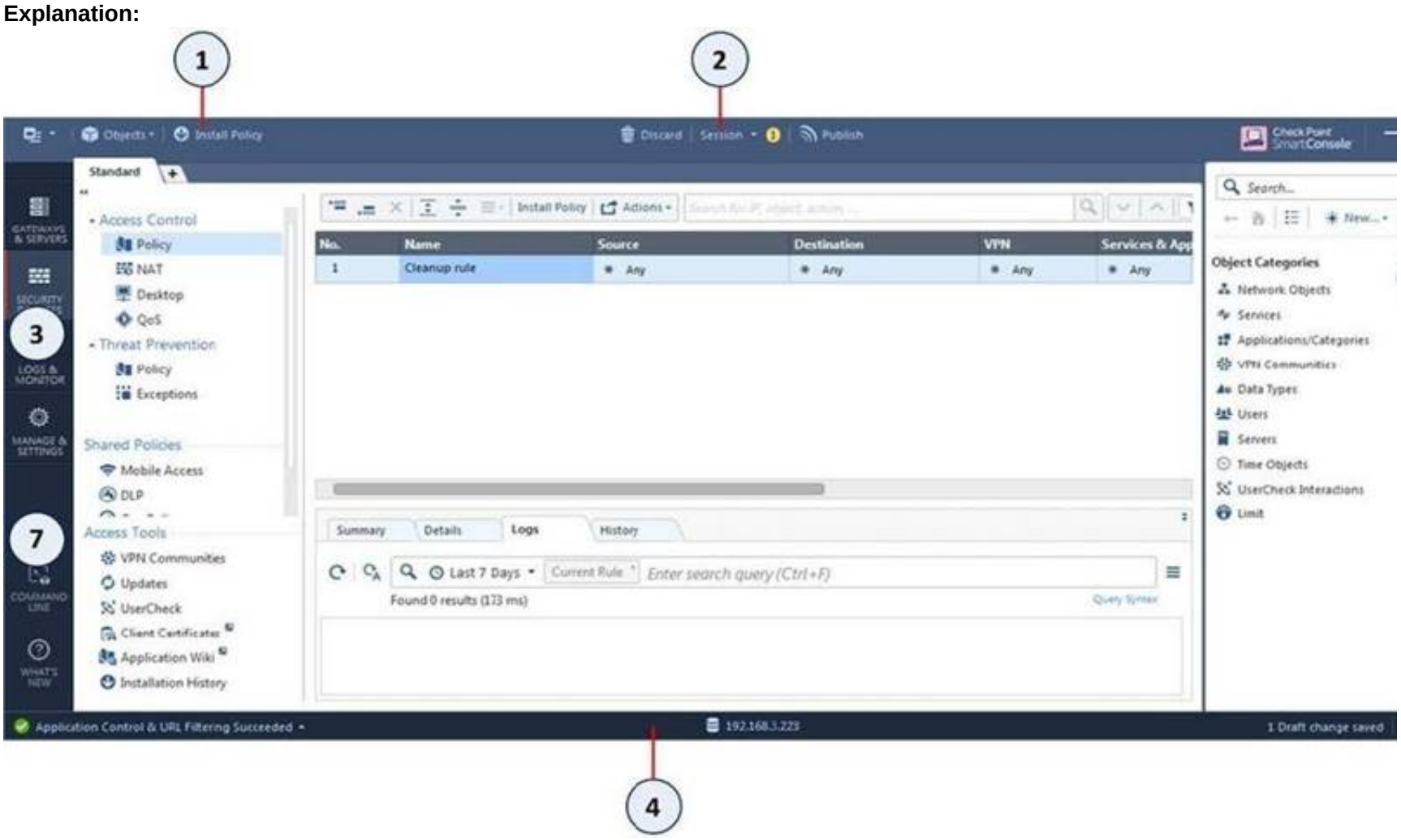
Answer: D

NEW QUESTION 232
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:



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 234
Name the utility that is used to block activities that appear to be suspicious.

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

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_CLI_ReferenceGuide/Topics-CLIG

NEW QUESTION 236
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 240
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 243
What are the three main components of Check Point security management architecture?

A. SmartConsole, Security Management, and Security Gateway
B. Smart Console, Standalone, and Security Management
C. SmartConsole, Security policy, and Logs & Monitoring
D. GUI-Client, Security Management, and Security Gateway

Answer: A

NEW QUESTION 246
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 247
Log query results can be exported to what file format?

A. Word Document (docx)
B. Comma Separated Value (csv)
C. Portable Document Format (pdf)
D. Text (txt)

Answer: B

NEW QUESTION 251
Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

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

Answer: B

Explanation:
The first rule is the automatic rule for the Accept All Encrypted Traffic feature. The Firewalls for the Security Gateways in the BranchOffices and LondonOffices

VPN communities allow all VPN traffic from hosts in clients in these communities. Traffic to the Security Gateways is dropped. This rule is installed on all Security Gateways in these communities.
* 2. Site to site VPN - Connections between hosts in the VPN domains of all Site to Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.
* 3. Remote access - Connections between hosts in the VPN domains of RemoteAccess VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

NEW QUESTION 252
Which statement describes what Identity Sharing is in Identity Awareness?

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

Answer: C

Explanation:
Identity Sharing
Best Practice - In environments that use many Security Gateways and AD Query, we recommend that you set only one Security Gateway to acquire identities from a given Active Directory domain controller for each physical site. If more than one Security Gateway gets identities from the same AD server, the AD server can become overloaded with WMI queries.
Set these options on the Identity Awareness > Identity Sharing page of the Security Gateway object:

NEW QUESTION 257
Which of the following is NOT an option to calculate the traffic direction?

A. Incoming
B. Internal
C. External
D. Outgoing

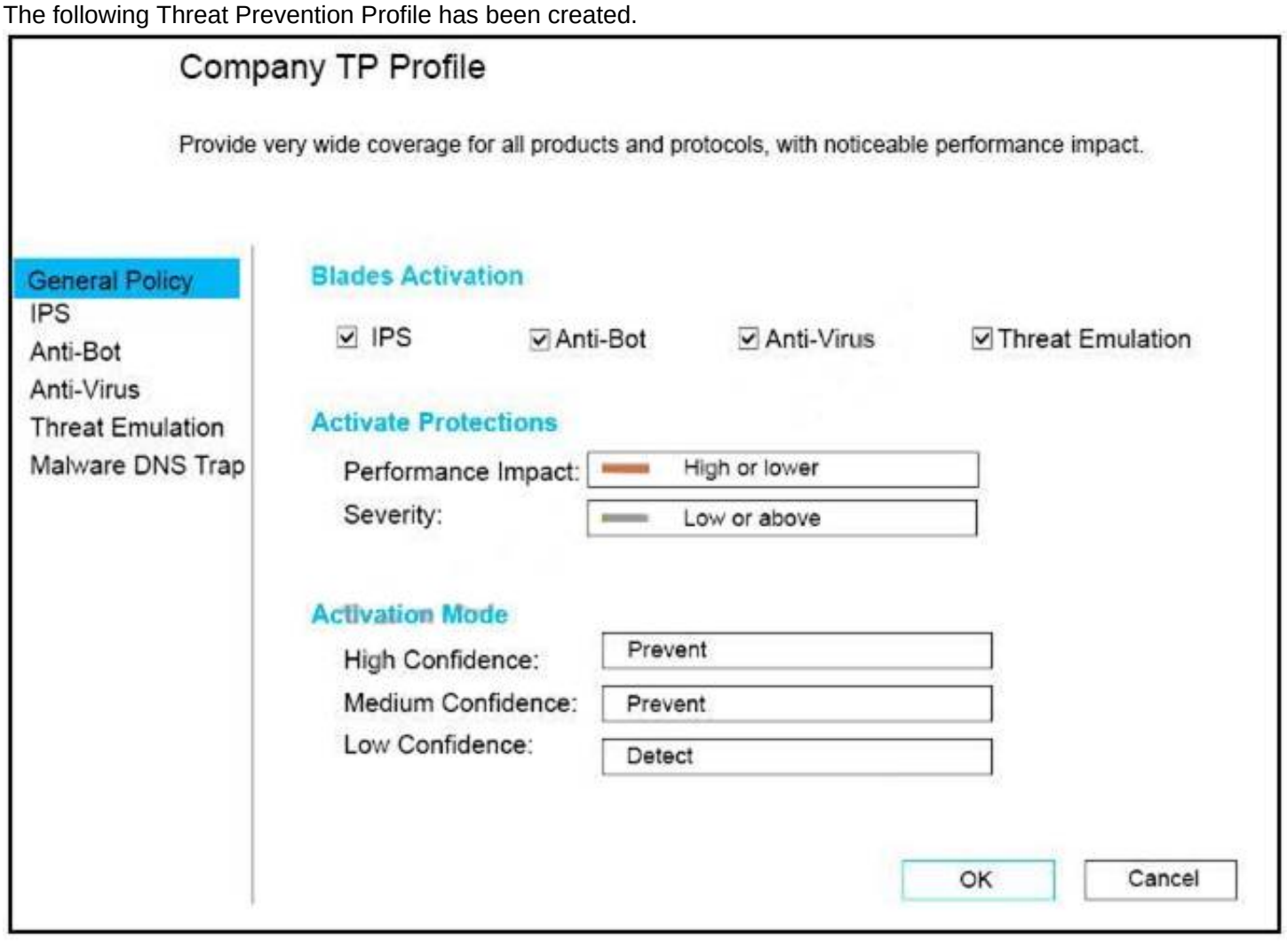
Answer: D

NEW QUESTION 260
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 261
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.



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 264
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 267
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

A. Application Control
B. Threat Emulation
C. Anti-Virus
D. Advanced Networking Blade

Answer: B

NEW QUESTION 268
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 269
You have enabled "Extended Log" as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

A. Identity Awareness is not enabled.
B. Log Trimming is enabled.
C. Logging has disk space issues
D. Content Awareness is not enabled.

Answer: D

NEW QUESTION 270
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 274
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 278

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.81 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.81 Product From:

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

Money Back Guarantee

156-215.81 Practice Exam Features:

* 156-215.81 Questions and Answers Updated Frequently

* 156-215.81 Practice Questions Verified by Expert Senior Certified Staff

* 156-215.81 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-215.81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year