CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

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

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

Answer: B

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

NEW QUESTION 2
An administrator wishes to enable Identity Awareness on the Check Point firewalls. However they allow users to use company issued or personal laptops. Since the administrator cannot manage the personal laptops, which of the following methods would BEST suit this company?

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

Answer: B

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

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

Answer: C

NEW QUESTION 4
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 5
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 6
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 7
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 8
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 9
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 10
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
In a Distributed deployment, the Security Gateway and the Security Management software are installed on what platforms?

A. Different computers or appliances.
B. The same computer or appliance.
C. Both on virtual machines or both on appliances but not mixed.
D. In Azure and AWS cloud environments.

Answer: A

Explanation:
"The Security Management ServerClosed (1) and the Security GatewayClosed (3) are installed on different computers, with a network connection (2)."
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION 11
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 12
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 14
The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?

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

Answer: A

NEW QUESTION 18
Which statement is NOT TRUE about Delta synchronization?

A. Using UDP Multicast or Broadcast on port 8161
B. Using UDP Multicast or Broadcast on port 8116
C. Quicker than Full sync
D. Transfers changes in the Kernel tables between cluster members

Answer: A

NEW QUESTION 20
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 22
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 27
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

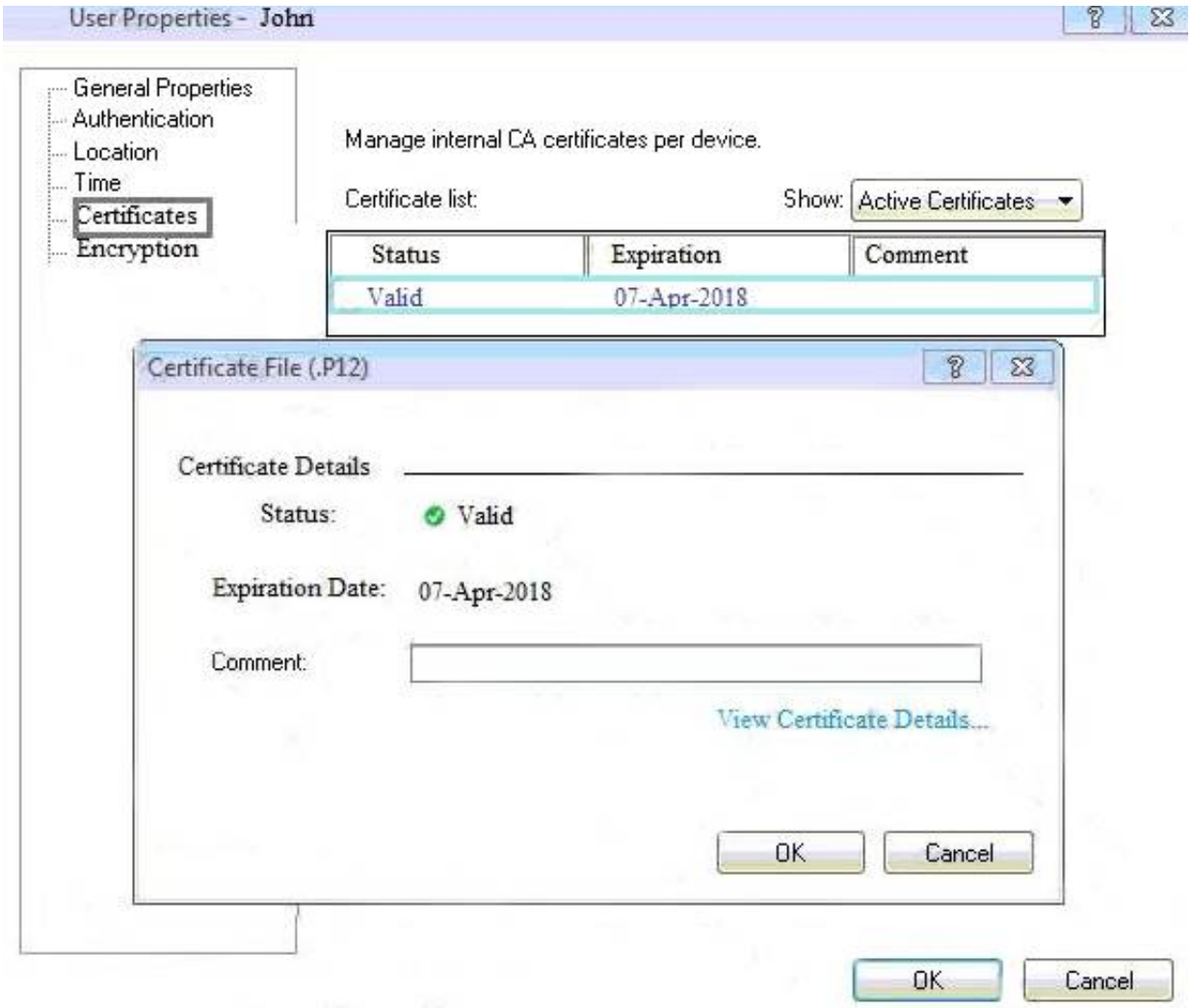
Explanation:
UserCheck alerts users while attemping to browse a suspicious/blocked or otherwise policy-limited website through a message in their web browsers shown before the actual page loads.

NEW QUESTION 28
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 32
You can see the following graphic:



What is presented on it?

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

Answer: A

NEW QUESTION 34
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 35
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 39
What is the purpose of the CPCA process?

A. Monitoring the status of processes
B. Sending and receiving logs
C. Communication between GUI clients and the SmartCenter server
D. Generating and modifying certificates

Answer: D

NEW QUESTION 42
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 45
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 49
Which path below is available only when CoreXL is enabled?

A. Slow path
B. Firewall path
C. Medium path
D. Accelerated path

Answer: C

NEW QUESTION 52
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 56
Fill in the blanks: Default port numbers for an LDAP server is _____ for standard connections and _____ SSL connections.

A. 675, 389
B. 389, 636
C. 636, 290
D. 290, 675

Answer: B

Explanation:
A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS.

NEW QUESTION 58
To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway does what with the data?

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

Answer: B

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

NEW QUESTION 62
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 63
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 66
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 67
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 72
In Unified SmartConsole Gateways and Servers tab you can perform the following functions EXCEPT _____.

A. Upgrade the software version
B. Open WebUI
C. Open SSH
D. Open service request with Check Point Technical Support

Answer: C

NEW QUESTION 77
Fill in the blank: Service blades must be attached to a _____.

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

Answer: A

NEW QUESTION 80
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 85
Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 88
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 92
In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:

A. 3rd Party integration of CLI and API for Gateways prior to R80.
B. A complete CLI and API interface using SSH and custom CPCode integration.
C. 3rd Party integration of CLI and API for Management prior to R80.
D. A complete CLI and API interface for Management with 3rd Party integration.

Answer: B

NEW QUESTION 96
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 97
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 102
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 105
Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

A. Centos Linux
B. Gaia embedded
C. Gaia
D. Red Hat Enterprise Linux version 5

Answer: B

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

NEW QUESTION 106
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 111
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 114
What is the BEST method to deploy Identity Awareness for roaming users?

A. Use Office Mode
B. Use identity agents
C. Share user identities between gateways
D. Use captive portal

Answer: B

Explanation:
Using Endpoint Identity Agents give you:

NEW QUESTION 119
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 120
In order to see real-time and historical graph views of Security Gateway statistics in SmartView Monitor, what feature needs to be enabled on the Security Gateway?

A. Logging & Monitoring
B. None - the data is available by default
C. Monitoring Blade
D. SNMP

Answer: C

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

NEW QUESTION 122
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 126
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 127
A network administrator has informed you that they have identified a malicious host on the network, and instructed you to block it. Corporate policy dictates that firewall policy changes cannot be made at this time. What tool can you use to block this traffic?

A. Anti-Bot protection
B. Anti-Malware protection
C. Policy-based routing
D. Suspicious Activity Monitoring (SAM) rules

Answer: D

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

NEW QUESTION 132
What is the default shell for the command line interface?

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

Answer: A

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

NEW QUESTION 134
SmartEvent does NOT use which of the following procedures to identity events:

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

Answer: C

NEW QUESTION 136
What data MUST be supplied to the SmartConsole System Restore window to restore a backup?

A. Server, Username, Password, Path, Version
B. Username, Password, Path, Version
C. Server, Protocol, Username, Password, Destination Path
D. Server, Protocol, Username, Password, Path

Answer: D

Explanation:
References:

NEW QUESTION 137
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

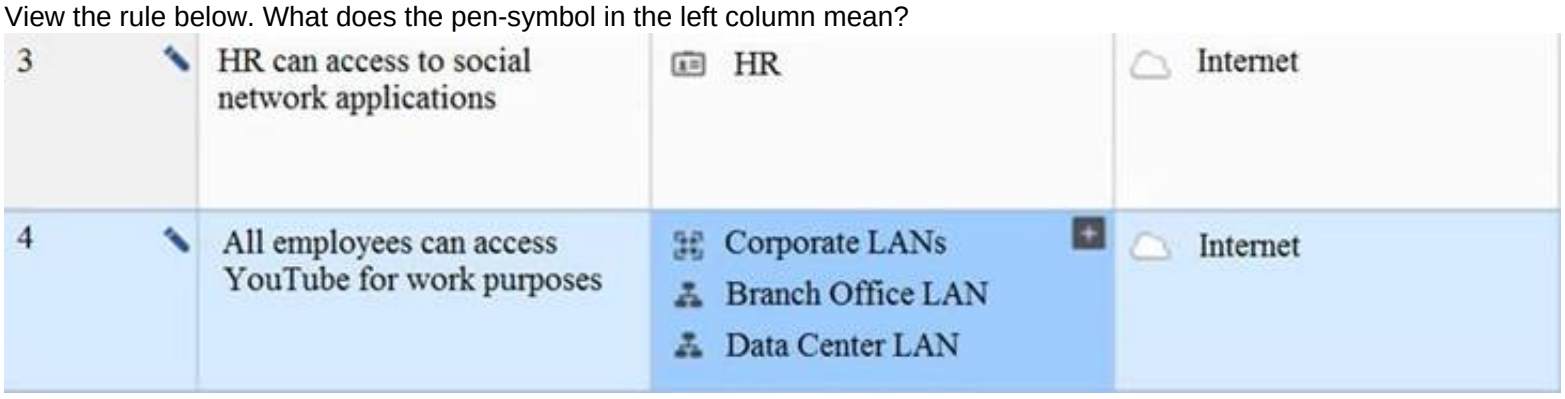
Answer: C

NEW QUESTION 139
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 140
View the rule below. What does the pen-symbol in the left column mean?



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 145
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 148
Where is the “Hit Count” feature enabled or disabled in SmartConsole?

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

Answer: B

Explanation:
References:

NEW QUESTION 149
Your internal networks 10.1.1.0/24, 10.2.2.0/24 and 192.168.0.0/16 are behind the Internet Security Gateway. Considering that Layer 2 and Layer 3 setup is correct, what are the steps you will need to do in SmartConsole in order to get the connection working?

A. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway’s external IP.3. Publish and install the policy.
B. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish the policy.
C. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish and install the policy.
D. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway’s external IP.3. Publish the policy.

Answer: C

NEW QUESTION 150
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 155
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 159
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 162
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 167
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 171
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 175
Fill in the blank: The position of an implied rule is manipulated in the _____ window.

A. NAT
B. Firewall
C. Global Properties
D. Object Explorer

Answer: C

Explanation:

"Note - In addition, users can access the Implied Rules configurations through Global Properties and use the implied policy view below Configuration."
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 180
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 185
Which option will match a connection regardless of its association with a VPN community?

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

Answer: B

NEW QUESTION 190
In _____ NAT, the _____ is translated.

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

Answer: A

NEW QUESTION 195
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 200
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 205
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 209

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 212
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 214
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 217
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 221
What are the Threat Prevention software components available on the Check Point Security Gateway?

A. IPS, Threat Emulation and Threat Extraction
B. IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction
C. IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction
D. IDS, Forensics, Anti-Virus, Sandboxing

Answer: C

NEW QUESTION 222
R80.10 management server can manage gateways with which versions installed?

A. Versions R77 and higher
B. Versions R76 and higher
C. Versions R75.20 and higher
D. Version R75 and higher

Answer: B

NEW QUESTION 224
Application Control/URL filtering database library is known as:

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

D. Application Library

Answer: B

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

NEW QUESTION 229
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 234
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 235
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 237
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 240
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 244
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 248
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 249
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 250
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 254
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 257
Which of the following situations would not require a new license to be generated and installed?

A. The Security Gateway is upgraded.
B. The existing license expires.
C. The license is upgraded.
D. The IP address of the Security Management or Security Gateway has changed.

Answer: A

NEW QUESTION 260
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 262
After the initial installation on Check Point appliance, you notice that the Management interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
B. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

Answer: A

NEW QUESTION 263

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 267
Fill in the blanks: The Application Layer Firewalls inspect traffic through _____ the layer(s) of the TCP/IP model and up to and including the _____ layer.

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

Answer: C

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

NEW QUESTION 269
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 271
What are the three types of UserCheck messages?

A. inform, ask, and block
B. block, action, and warn
C. action, inform, and ask
D. ask, block, and notify

Answer: A

Explanation:
Inform User Inform
Shows when the action for the ruleClosed is inform. It informs users what the company policy is for that site. Blocked Message
Block
Shows when a request is blocked. Ask User
Ask
Shows when the action for the rule is ask. It informs users what the company policy is for that site and they must click OK to continue to the site.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_DataLossPrevention_AdminGuide/

NEW QUESTION 275
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 280
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 282
To view the policy installation history for each gateway, which tool would an administrator use?

A. Revisions
B. Gateway installations
C. Installation history
D. Gateway history

Answer: C

NEW QUESTION 283
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 284
To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?

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

Answer: B

NEW QUESTION 285
When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, what does that indicate?

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

Answer: D

NEW QUESTION 287
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 291
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 294
The competition between stateful inspection and proxies was based on performance, protocol support, and security. Considering stateful Inspections and Proxies, which statement is correct?

A. Stateful Inspection is limited to Layer 3 visibility, with no Layer 4 to Layer 7 visibility capabilities.
B. When it comes to performance, proxies were significantly faster than stateful inspection firewalls.
C. Proxies offer far more security because of being able to give visibility of the payload (the data).
D. When it comes to performance, stateful inspection was significantly faster than proxies.

Answer: C

NEW QUESTION 299
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 304
Check Point ClusterXL Active/Active deployment is used when:

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

Answer: D

NEW QUESTION 308
Which tool allows for the automatic updating of the Gaia OS and Check Point products installed on the Gaia OS?

A. CPASE - Check Point Automatic Service Engine
B. CPAUE - Check Point Automatic Update Engine
C. CPDAS - Check Point Deployment Agent Service
D. CPUSE - Check Point Upgrade Service Engine

Answer: D

Explanation:
Check Point Update Service Engine (CPUSE), also known as Deployment Agent [DA], is an advanced and intuitive mechanism for software deployment on Gaia OS, which supports deployments of single HotFixes (HF), of HotFix Accumulators (Jumbo), and of Major Versions.
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 309
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 312
Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the _____ algorithm.

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

Answer: A

NEW QUESTION 314
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 315
A Check Point Software license consists of two components, the Software Blade and the Software Container. There are _____ types of Software Containers:

_____ .

A. Two; Security Management and Endpoint Security
B. Two; Endpoint Security and Security Gateway
C. Three; Security Management, Security Gateway, and Endpoint Security
D. Three; Security Gateway, Endpoint Security, and Gateway Management

Answer: C

Explanation:
There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security. Ref: https://downloads.checkpoint.com/dc/download.htm?ID=11608

NEW QUESTION 319
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 323
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 326
Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

A. ThreatWiki
B. Whitelist Files
C. AppWiki
D. IPS Protections

Answer: A

NEW QUESTION 328
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 331
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 335
URL Filtering cannot be used to:

A. Control Bandwidth issues
B. Control Data Security
C. Improve organizational security

D. Decrease legal liability

Answer: D

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

NEW QUESTION 339
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 343
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 345
What are the three deployment options available for a security gateway?

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

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/86429.htm

NEW QUESTION 347
What key is used to save the current CPView page in a filename format cpview_“cpview process ID”. cap”number of captures”?

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

Answer: C

NEW QUESTION 350
Which of the following is NOT a role of the SmartCenter:

A. Status monitoring
B. Policy configuration
C. Certificate authority
D. Address translation

Answer: C

NEW QUESTION 353
What command from the CLI would be used to view current licensing?

A. license view
B. fw ctl tab -t license -s
C. show license -s
D. cplic print

Answer: D

NEW QUESTION 354

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 358
Which option, when applied to a rule, allows all encrypted and non-VPN traffic that matches the rule?

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

Answer: B

NEW QUESTION 359
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 360
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 362
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 365
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 369
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 370
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 372
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 375
In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

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

Answer: C

NEW QUESTION 379
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 381
What is the most recommended installation method for Check Point appliances?

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

Answer: C

NEW QUESTION 384
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 386
Fill in the blank: Once a certificate is revoked from the Security GateWay by the Security Management Server, the certificate information is _____.

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

Answer: D

NEW QUESTION 387
Which of the following is NOT an identity source used for Identity Awareness?

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

Answer: B

NEW QUESTION 392
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 394
Which of the following log queries would show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1?

A. src:192.168.1.1 OR dst:172.26.1.1 AND action:Drop
B. src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop
C. 192.168.1.1 AND 172.26.1.1 AND drop
D. 192.168.1.1 OR 172.26.1.1 AND action:Drop

Answer: B

NEW QUESTION 398
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 401
Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

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

Answer: D

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

NEW QUESTION 403
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 407
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 411
What are the three deployment considerations for a secure network?

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

Answer: A

NEW QUESTION 416
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 419
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 422
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 425
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 429
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 434
Fill in the blank: To create policy for traffic to or from a particular location, use the _____ .

A. DLP shared policy
B. Geo policy shared policy
C. Mobile Access software blade
D. HTTPS inspection

Answer: B

Explanation:
Shared Policies
The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. T are shared between all Policy packages.
Shared policies are installed with the Access Control Policy. Software Blade
Description Mobile Access
Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP
Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy
Create a policy for traffic to or from specific geographical or political locations.

NEW QUESTION 439
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

A. Smart Cloud Services
B. Load Sharing Mode Services
C. Threat Agent Solution
D. Public Cloud Services

Answer: A

NEW QUESTION 444
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 446
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 450
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 453
Which policy type is used to enforce bandwidth and traffic control rules?

A. Access Control
B. Threat Emulation
C. Threat Prevention
D. QoS

Answer: D

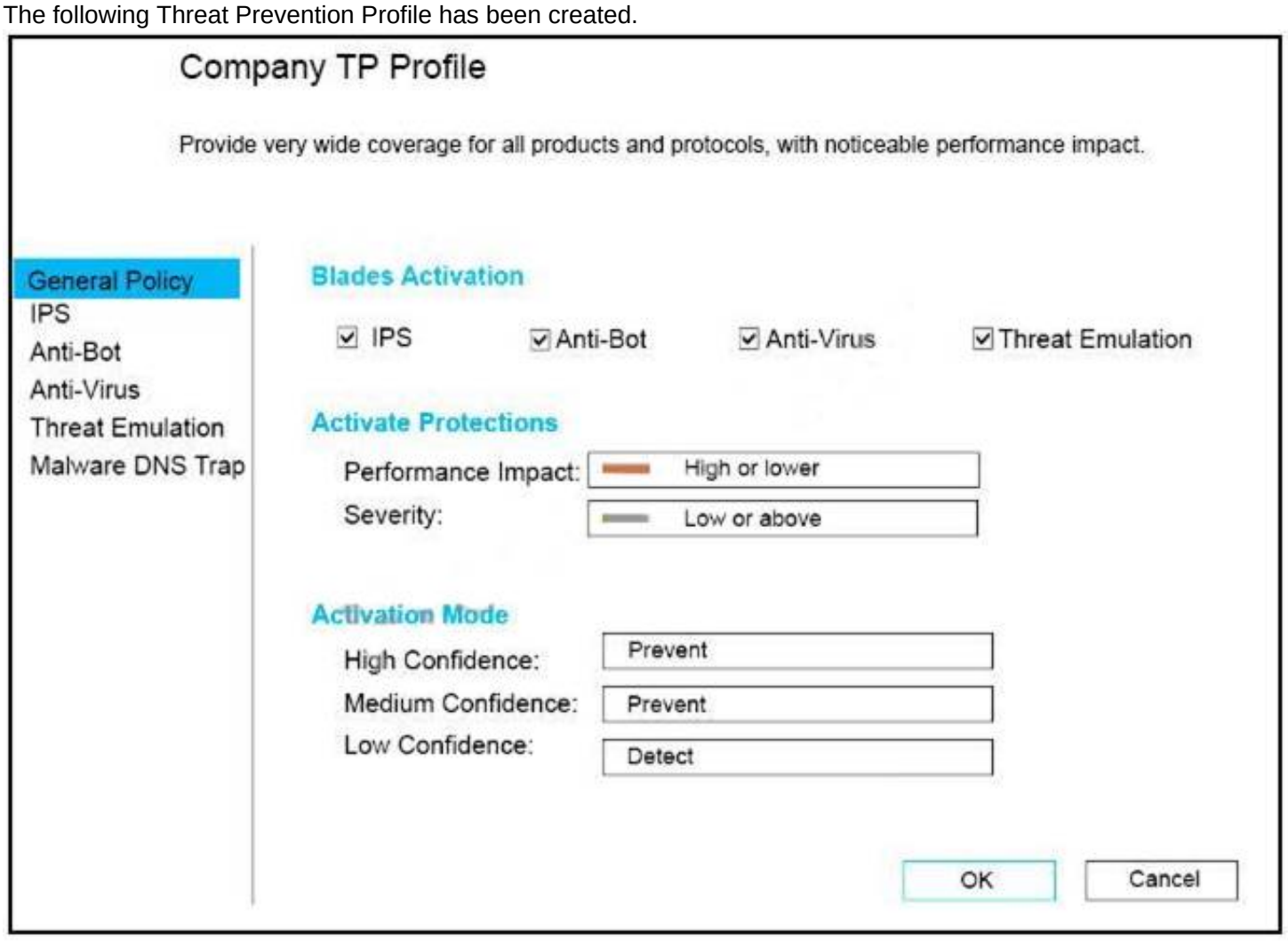
Explanation:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_QoS_AdminGuide/html_fram

NEW QUESTION 454
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 456
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 460
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 462
Which of the following is NOT a valid configuration screen of an Access Role Object?

A. Users
B. Networks
C. Time
D. Machines

Answer: C

NEW QUESTION 467
How are the backups stored in Check Point appliances?

A. Saved as*.tar under /var/log/CPbackup/backups
B. Saved as*tgz under /var/CPbackup
C. Saved as*tar under /var/CPbackup
D. Saved as*tgz under /var/log/CPbackup/backups

Answer: B

Explanation:
Backup configurations are stored in: /var/CPbackup/backups/

NEW QUESTION 471
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 473
After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

A. Security Gateway IP-address cannot be changed without re-establishing the trust
B. The Security Gateway name cannot be changed in command line without re-establishing trust
C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust
D. The Security Management Server IP-address cannot be changed without re-establishing the trust

Answer: A

NEW QUESTION 476
What Check Point tool is used to automatically update Check Point products for the Gaia OS?

A. Check Point INSPECT Engine
B. Check Point Upgrade Service Engine
C. Check Point Update Engine
D. Check Point Upgrade Installation Service

Answer: B

NEW QUESTION 477
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 482
Phase 1 of the two-phase negotiation process conducted by IKE operates in _____ mode.

A. Main
B. Authentication
C. Quick
D. High Alert

Answer: A

Explanation:
Phase I modes
Between Security Gateways, there are two modes for IKE phase I. These modes only apply to IKEv1:

NEW QUESTION 483
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 487
What are the steps to configure the HTTPS Inspection Policy?

A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
D. Go to Application&url filtering blade > Https Inspection > Policy

Answer: C

NEW QUESTION 488
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

156-215.81 Practice Exam Features:

* 156-215.81 Questions and Answers Updated Frequently

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

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

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