Number: 156-315.81
Passing Score: 800
Time Limit: 120
File Version: 14.5

Exam Code: 156-315.81
Exam Name: Check Point Certified Security Expert R81

Exam A

QUESTION 1
Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?

A. 50%
B. 75%
C. 80%
D. 15%

Correct Answer: D
Section:
Explanation:
Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to a certain threshold. In this case, the correct threshold is specified as option D: 15%.
So, when the available disk space reaches or falls below 15%, old log entries should be deleted to free up space.
Options A, B, and C do not represent the recommended threshold for deleting old log entries according to Check Point's best practices.
Topic 2, Exam Pool B

QUESTION 2
SmartEvent has several components that function together to track security threats. What is the function of the Correlation Unit as a component of this architecture?

A. Analyzes each log entry as it arrives at the log server according to the Event Policy. When a threat pattern is identified, an event is forwarded to the SmartEvent Server.
B. Correlates all the identified threats with the consolidation policy.
C. Collects syslog data from third party devices and saves them to the database.
D. Connects with the SmartEvent Client when generating threat reports.

Correct Answer: A
Section:
Explanation:
The Correlation Unit in SmartEvent architecture has the function of analyzing each log entry as it arrives at the log server according to the Event Policy. When it identifies a threat pattern, it forwards an event to the SmartEvent Server. This is an essential function in threat detection and analysis, as it helps in identifying and alerting about security threats based on the configured policies.
Option A correctly describes the function of the Correlation Unit, making it the verified answer.

QUESTION 3
SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

A. This statement is true because SecureXL does improve all traffic.
B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
C. This statement is true because SecureXL does improve this traffic.
D. This statement is false because encrypted traffic cannot be inspected.

Correct Answer: C
Section:
Explanation:

SecureXL is a performance-enhancing technology used in Check Point firewalls. It improves the throughput of both non-encrypted firewall traffic and encrypted VPN traffic. The statement in option C is true because SecureXL does improve both types of traffic by offloading processing to dedicated hardware acceleration, optimizing firewall and VPN operations.
Option C correctly states that SecureXL improves this traffic, making it the verified answer.

QUESTION 4
What component of R81 Management is used for indexing?

A. DBSync
B. API Server
C. fwm
D. SOLR

Correct Answer: D
Section:
Explanation:
The component of R81 Management that is used for indexing is SOLR. SOLR is an open-source enterprise search platform that provides fast and scalable indexing and searching capabilities. SOLR is used by SmartConsole to index the objects and rules in the security policy, as well as the logs and events in SmartLog and SmartEvent. SOLR enables quick and easy access to the relevant information in the management database.
Reference:Check Point Security Expert R81 Course, SOLR Troubleshooting

QUESTION 5
After making modifications to the $CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?

A. cvpnd_restart
B. cvpnd_restart
C. cvpnd restart
D. cvpnrestart

Correct Answer: B
Section:
Explanation:
The cvpnd_restart command is used to restart the daemon after making modifications to the $CVPNDIR/conf/cvpnd.C file. The cvpnd daemon is responsible for managing the communication between the Check Point components and the Content Vectoring Protocol (CVP) server. The CVP server is an external server that provides content inspection and filtering services for Check Point gateways. The $CVPNDIR/conf/cvpnd.C file contains the configuration settings for the cvpnd daemon, such as the CVP server IP address, port number, timeout value, and debug level.
Reference:Check Point Security Expert R81 Course, Content Inspection Using ICAP, cvpnd daemon debug file

QUESTION 6
SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

A. Threat Emulation
B. Mobile Access
C. Mail Transfer Agent
D. Threat Cloud

Correct Answer: B
Section:
Explanation:
Mobile Access is not part of the SandBlast component. Mobile Access is a software blade that provides secure remote access to corporate resources from various devices, such as smartphones, tablets, and laptops. Mobile Access supports different connectivity methods, such as SSL VPN, IPsec VPN, and Mobile Enterprise Application Store (MEAS). Mobile Access also integrates with Mobile Threat Prevention (MTP) to protect mobile devices

from malware and network attacks.
Reference:Check Point Security Expert R81 Course, Mobile Access Administration Guide, SandBlast Mobile Datasheet

QUESTION 7
With Mobile Access enabled, administrators select the web-based and native applications that can be accessed by remote users and define the actions that users can perform the applications. Mobile Access encrypts all traffic using:

A. HTTPS for web-based applications and 3DES or RC4 algorithm for native applications. For end users to access the native applications, they need to install the SSL Network Extender.
B. HTTPS for web-based applications and AES or RSA algorithm for native applications. For end users to access the native application, they need to install the SSL Network Extender.
C. HTTPS for web-based applications and 3DES or RC4 algorithm for native applications. For end users to access the native applications, no additional software is required.
D. HTTPS for web-based applications and AES or RSA algorithm for native applications. For end users to access the native application, no additional software is required.

Correct Answer: A
Section:
Explanation:
Mobile Access encrypts all traffic using HTTPS for web-based applications and 3DES or RC4 algorithm for native applications. For end users to access the native applications, they need to install the SSL Network Extender, which is a lightweight VPN client that creates a secure SSL tunnel to the Mobile Access gateway. The SSL Network Extender supports various types of native applications, such as email clients, file sharing, and remote desktop.
Reference:Mobile Access Administration Guide,SSL Network Extender

QUESTION 8
What is the benefit of ''tw monitor'' over ''tcpdump''?

A. ''fw monitor'' reveals Layer 2 information, while ''tcpdump'' acts at Layer 3.
B. ''fw monitor'' is also available for 64-Bit operating systems.
C. With ''fw monitor'', you can see the inspection points, which cannot be seen in ''tcpdump''
D. ''fw monitor'' can be used from the CLI of the Management Server to collect information from multiple gateways.

Correct Answer: C
Section:
Explanation:
The benefit of fw monitor over tcpdump is that with fw monitor, you can see the inspection points, which cannot be seen in tcpdump. Inspection points are the locations in the firewall kernel where packets are inspected by the security policy and other software blades. Fw monitor allows you to capture packets at different inspection points and see how they are processed by the firewall. Tcpdump, on the other hand, is a generic packet capture tool that only shows the packets as they enter or leave the network interface.
Reference:Check Point Security Expert R81 Course,fw monitor, tcpdump

QUESTION 9
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.

Correct Answer: D
Section:
Explanation:
Threat Extraction is a software blade that delivers PDF versions of original files with active content removed. Active content, such as macros, scripts, or embedded objects, can be used by attackers to deliver malware or exploit vulnerabilities. Threat Extraction removes or sanitizes the active content from the files and converts them to PDF format, which is safer and more compatible. Threat Extraction can also work together with Threat

Emulation to provide both clean and original files to the users.
Reference:Check Point Security Expert R81 Course, Threat Extraction Administration Guide

QUESTION 10
Which command gives us a perspective of the number of kernel tables?

A. fw tab -t
B. fw tab -s
C. fw tab -n
D. fw tab -k

Correct Answer: B
Section:
Explanation:
The command 'fw tab -s' is used to display information about the state of various kernel tables in a Check Point firewall. It provides a perspective on the number and status of these tables, which can be helpful for troubleshooting and monitoring firewall performance.
Option B correctly identifies the command that gives a perspective of the number of kernel tables, making it the verified answer.

QUESTION 11
When simulating a problem on ClusterXL cluster with cphaprob --d STOP -s problem -t 0 register, to initiate a failover on an active cluster member, what command allows you remove the problematic state?

A. cphaprob --d STOP unregister
B. cphaprob STOP unregister
C. cphaprob unregister STOP
D. cphaprob --d unregister STOP

Correct Answer: A
Section:
Explanation:
When simulating a problem on a ClusterXL cluster with the command 'cphaprob --d STOP -s problem -t 0 register' to initiate a failover on an active cluster member, you can use the command 'cphaprob --d STOP unregister' to remove the problematic state and return the cluster to normal operation.
Option A correctly identifies the command that allows you to remove the problematic state, making it the verified answer.

QUESTION 12
How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

A. Install appliance TE250X on SpanPort on LAN switch in MTA mode.
B. Install appliance TE250X in standalone mode and setup MTA.
C. You can utilize only Check Point Cloud Services for this scenario.
D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance.

Correct Answer: C
Section:
Explanation:
To deploy a TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway, you can utilize Check Point Cloud Services. In this scenario, you can leverage cloud-based email security services provided by Check Point without the need for an on-premises Security Gateway.
Option C correctly states that you can use only Check Point Cloud Services for this scenario, making it the verified answer.

QUESTION 13
What is the main difference between Threat Extraction and Threat Emulation?

A. Threat Emulation never delivers a file and takes more than 3 minutes to complete.
B. Threat Extraction always delivers a file and takes less than a second to complete.
C. Threat Emulation never delivers a file that takes less than a second to complete.
D. Threat Extraction never delivers a file and takes more than 3 minutes to complete.

Correct Answer: B
Section:
Explanation:
Threat Extraction (Answer B): Threat Extraction always delivers a file, but it removes potentially malicious content from the file before delivering it to the user. It is designed to provide a safe version of the file quickly, taking less than a second to complete.
Threat Emulation (Option A): Threat Emulation does not deliver the original file to the user until it has been thoroughly analyzed for threats. It may take more than 3 minutes to complete the analysis. The emphasis here is on safety and thorough inspection, which may result in a longer processing time.
Therefore, Option B correctly describes the main difference between Threat Extraction and Threat Emulation.

QUESTION 14
You find one of your cluster gateways showing ''Down'' when you run the ''cphaprob stat'' command. You then run the ''clusterXL_admin up'' on the down member but unfortunately the member continues to show down.
What command do you run to determine the cause?

A. cphaprob --f register
B. cphaprob --d --s report
C. cpstat --f all
D. cphaprob --a list

Correct Answer: D
Section:
Explanation:
To determine the cause of a cluster gateway showing 'Down' despite running 'clusterXL_admin up' on the down member, you can run the following command:

```
css                                                    Copy code

cphaprob -a list
```

This command will provide a list of cluster members along with their statuses and can help diagnose the issue with the down member.

QUESTION 15
In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
C. Mail, Block Source, Block Destination, External Script, SNMP Trap
D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Correct Answer: A
Section:
Explanation:

In SmartEvent, the administrator can configure different types of automatic reactions, which include:
Mail notifications
Blocking the source of the event
Blocking the event activity
Running an external script
Sending an SNMP trap
So, the correct answer is 'Mail, Block Source, Block Event Activity, External Script, SNMP Trap.'

QUESTION 16
Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

A. mgmt_cli add-host ''Server_1'' ip_address ''10.15.123.10'' --format txt
B. mgmt_cli add host name ''Server_1'' ip-address ''10.15.123.10'' --format json
C. mgmt_cli add object-host ''Server_1'' ip-address ''10.15.123.10'' --format json
D. mgmt._cli add object ''Server-1'' ip-address ''10.15.123.10'' --format json

Correct Answer: B
Section:
Explanation:
The correct syntax to import a host object using mgmt_cli ismgmt_cli add host name <name> ip-address <ip-address> --format <format>1. The name and ip-address parameters are mandatory, while the format parameter is optional and can be either json or txt.The other options are incorrect because they either use wrong parameters, wrong hyphens, or wrong object types.
Reference:1: Check Point Resource Library2

QUESTION 17
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

Correct Answer: A
Section:
Explanation:
The correct steps to configure the HTTPS Inspection Policy in Check Point R81 are as follows1:
Go toManage&Settings > Blades > HTTPS Inspection > Configurein SmartDashboard.
EnableHTTPS Inspectionand select thePolicytab.
Create a newHTTPS Inspection Layeror edit an existing one.
Define therulesfor inspecting HTTPS traffic based on the source, destination, service, and action.
Install thepolicyon the relevant gateways.
The other options are incorrect because they either use wrong blade names, wrong menu options, or wrong configuration steps.
Reference:1: LAB:25 How to Configure HTTPS Inspection in Check Point Firewall R81(https://www.youtube.com/watch?v=NCvV7-R9ZgU)

QUESTION 18
You want to store the GAIA configuration in a file for later reference. What command should you use?

A. write mem <filename>
B. show config --f <filename>

C. save config --o <filename>
D. save configuration <filename>

Correct Answer: D
Section:
Explanation:
The correct command to store the GAIA configuration in a file issave configuration <filename>1.This will create a file with the current system level configuration in the home directory of the current user1.The other commands are incorrect because they either do not exist or do not save the configuration to a file.
Reference:1: Backing up Gaia system level configuration(https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk102234)

QUESTION 19
How do Capsule Connect and Capsule Workspace differ?

A. Capsule Connect provides a Layer3 VPN. Capsule Workspace provides a Desktop with usable applications.
B. Capsule Workspace can provide access to any application.
C. Capsule Connect provides Business data isolation.
D. Capsule Connect does not require an installed application at client.

Correct Answer: A
Section:
Explanation:
Capsule Connect and Capsule Workspace are both components of Check Point's remote access solution, but they serve different purposes and have distinct features:
A) Capsule Connect provides a Layer 3 VPN, which allows remote users to connect securely to their corporate network. It typically provides network-level access, allowing users to access resources on the corporate network. On the other hand, Capsule Workspace provides a secure workspace environment, including a virtual desktop with usable applications. It is more focused on providing application-level access to users in a secure manner.
B) This statement is partially true. Capsule Workspace is designed to provide secure access to a wide range of applications and resources, not limited to specific applications.
C) Capsule Connect does provide business data isolation by creating a secure VPN tunnel for remote users, ensuring that their network traffic is isolated from the public internet.
D) Capsule Connect usually requires an installed application or VPN client on the client device to establish a secure connection to the corporate network. This statement is not entirely accurate because an installed application or client is typically required.
Therefore, option A is the correct answer as it accurately distinguishes between Capsule Connect and Capsule Workspace based on their primary functionalities.

QUESTION 20
John detected high load on sync interface. Which is most recommended solution?

A. For short connections like http service -- delay sync for 2 seconds
B. Add a second interface to handle sync traffic
C. For short connections like http service -- do not sync
D. For short connections like icmp service -- delay sync for 2 seconds

Correct Answer: A
Section:
Explanation:
When John detects a high load on the sync interface, the recommended solution is to implement a delay in the sync process for short-lived connections like HTTP. Here's an explanation of each option:
A) Delaying the sync for 2 seconds for short connections like HTTP services is a common practice to reduce the load on the sync interface. This allows the interface to handle the incoming connections more effectively.
B) Adding a second interface to handle sync traffic might be a viable solution, but it can be more complex and costly compared to implementing a delay for short connections.
C) Not syncing short connections like HTTP services is not a recommended approach because it may lead to synchronization issues and potential data inconsistencies between cluster members.
D) Delaying the sync for ICMP (ping) services is not a common practice and may not effectively address the high load issue on the sync interface.
Therefore, option A is the most recommended solution as it addresses the issue by introducing a delay for short-lived connections, optimizing the sync process without causing synchronization problems.

QUESTION 21
Which of these is an implicit MEP option?

A. Primary-backup
B. Source address based
C. Round robin
D. Load Sharing

Correct Answer: A
Section:
Explanation:
Implicit MEP (Multicast Ethernet Point) options refer to the way multicast traffic is handled within a network. In this case, the question is asking about an implicit MEP option, and the correct answer is:
A) Primary-backup: This is an implicit MEP option where one switch (primary) forwards multicast traffic while the other switch (backup) does not forward the traffic. It is used to ensure redundancy in case the primary switch fails.
B) Source address-based, C. Round-robin, and D. Load Sharing are not implicit MEP options; they are different methods of handling multicast traffic and do not describe the concept of primary-backup.
Therefore, option A is the correct answer as it represents an implicit MEP option.

QUESTION 22
Which Check Point daemon monitors the other daemons?

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

Correct Answer: C
Section:
Explanation:
The Check Point daemon that monitors the other daemons is cpwd (Check Point Watchdog). It is responsible for monitoring the health and status of various Check Point daemons and processes running on the Security Gateway. If any daemon or process stops responding or encounters an issue, cpwd can restart it to ensure the continued operation of the Security Gateway.

QUESTION 23
What is the least amount of CPU cores required to enable CoreXL?

A. 2
B. 1
C. 4
D. 6

Correct Answer: A
Section:
Explanation:
The least amount of CPU cores required to enable CoreXL is2. CoreXL is a technology that improves the performance of Security Gateways by using multiple CPU cores to process traffic in parallel. CoreXL requires at least two CPU cores, one for SND (Secure Network Distributor) and one for a Firewall instance. The other options are either too few or too many CPU cores for enabling CoreXL.
Reference: [Check Point R81 SecureXL Administration Guide], [Check Point R81 Performance Tuning Administration Guide]

QUESTION 24
You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
B. Create a separate Security Policy package for each remote Security Gateway.
C. Create network objects that restricts all applicable rules to only certain networks.
D. Run separate SmartConsole instances to login and configure each Security Gateway directly.

Correct Answer: B
Section:
Explanation:
To simplify security administration when working with multiple Security Gateways enforcing an extensive number of rules, you would choose to create a separate Security Policy package for each remote Security Gateway. A Security Policy package is a set of rules and objects that can be assigned to one or more Security Gateways.This allows you to manage different policies for different gateways from the same Management Server1. The other options are either not effective or not feasible for simplifying security administration.
Reference:Check Point R81 Security Management Administration Guide

QUESTION 25
Which of the following authentication methods ARE NOT used for Mobile Access?

A. RADIUS server
B. Username and password (internal, LDAP)
C. SecurID
D. TACACS+

Correct Answer: D
Section:
Explanation:
TACACS+ is not an authentication method that is used for Mobile Access.Mobile Access supports the following authentication methods: username and password (internal, LDAP, or RADIUS), certificate, SecurID, DynamicID, and SMS2.TACACS+ is a protocol that provides access control for routers, network access servers, and other network devices, but it is not supported by Mobile Access3.
Reference:Check Point R81 Mobile Access Administration Guide, TACACS+ - Wikipedia

QUESTION 26
What is the correct command to observe the Sync traffic in a VRRP environment?

A. fw monitor --e ''accept[12:4,b]=224.0.0.18;''
B. fw monitor --e ''accept port(6118;''
C. fw monitor --e ''accept proto=mcVRRP;''
D. fw monitor --e ''accept dst=224.0.0.18;''

Correct Answer: D
Section:
Explanation:
The correct command to observe the Sync traffic in a VRRP environment isfw monitor --e ''accept dst=224.0.0.18;''. This command captures the packets that have the destination IP address of 224.0.0.18, which is the multicast address used by VRRP for synchronization. The other commands are either not valid or not specific to VRRP Sync traffic.
Reference: [Check Point R81 ClusterXL Administration Guide], Check Point R81 Performance Tuning Administration Guide

QUESTION 27
What has to be taken into consideration when configuring Management HA?

A. The Database revisions will not be synchronized between the management servers

B. SmartConsole must be closed prior to synchronized changes in the objects database
C. If you wanted to use Full Connectivity Upgrade, you must change the Implied Rules to allow FW1_cpredundant to pass before the Firewall Control Connections.
D. For Management Server synchronization, only External Virtual Switches are supported. So, if you wanted to employ Virtual Routers instead, you have to reconsider your design.

Correct Answer: A
Section:
Explanation:
When configuring Management HA, you have to take into consideration that the Database revisions will not be synchronized between the management servers. Database revisions are snapshots of the database that are created manually or automatically when installing a policy or saving changes. They are stored locally on each management server and are not replicated by Management HA. The other options are either not true or not relevant to Management HA.
Reference:Check Point R81 Installation and Upgrade Guide

QUESTION 28
Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?

A. Check Point Remote User
B. Check Point Capsule Workspace
C. Check Point Mobile Web Portal
D. Check Point Capsule Remote

Correct Answer: C
Section:
Explanation:
Check Point Mobile Web Portal is a Mobile Access Application that allows a secure container on mobile devices to give users access to internal websites, file shares and emails. The Mobile Web Portal is a web-based application that can be accessed from any browser on any device. It provides a user-friendly interface to access various resources on the corporate network without requiring a VPN client or additional software installation. The Mobile Web Portal supports authentication methods such as user name and password, certificate, one-time password (OTP), etc. The Mobile Web Portal also supports security features such as encryption, data leakage prevention (DLP), threat prevention, etc.
Reference:R81 Mobile Access Administration Guide

QUESTION 29
Which of the following process pulls application monitoring status?

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

Correct Answer: D
Section:
Explanation:
The process that pulls application monitoring status iscpd. cpd is a daemon that runs on Check Point products and performs various tasks related to management communication, policy installation, license verification, logging, etc. cpd also monitors the status of other processes and applications on the system and reports it to the management server. cpd uses SNMP to collect information from various sources, such as blades, gateways, servers, etc. You can view the application monitoring status in SmartConsole by using theGateways & Serverstab in theLogs & Monitorview.
Reference: Check Point Processes and Daemons

QUESTION 30
Identify the API that is not supported by Check Point currently.

A. R81 Management API-
B. Identity Awareness Web Services API
C. Open REST API
D. OPSEC SDK

Correct Answer: C
Section:
Explanation:
Check Point currently supports four types of APIs: R81 Management API, Identity Awareness Web Services API, OPSEC SDK, and Gaia REST API. The Open REST API is not a valid option.Reference:Check Point APIs

QUESTION 31
SandBlast Mobile identifies threats in mobile devices by using on-device, network, and cloud-based algorithms and has four dedicated components that constantly work together to protect mobile devices and their data. Which component is NOT part of the SandBlast Mobile solution?

A. Management Dashboard
B. Gateway
C. Personal User Storage
D. Behavior Risk Engine

Correct Answer: C
Section:
Explanation:
SandBlast Mobile has four components: Management Dashboard, Gateway, Behavior Risk Engine, and On-Device Network Protection. Personal User Storage is not part of the SandBlast Mobile solution.Reference:SandBlast Mobile Architecture

QUESTION 32
What are the different command sources that allow you to communicate with the API server?

A. SmartView Monitor, API_cli Tool, Gaia CLI, Web Services
B. SmartConsole GUI Console, mgmt_cli Tool, Gaia CLI, Web Services
C. SmartConsole GUI Console, API_cli Tool, Gaia CLI, Web Services
D. API_cli Tool, Gaia CLI, Web Services

Correct Answer: B
Section:
Explanation:
You can communicate with the API server using three command sources: SmartConsole GUI Console, mgmt_cli Tool, and Gaia CLI. Web Services are not a command source, but a way to access the API server using HTTP requests.Reference:Check Point Management APIs

QUESTION 33
What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?

A. Anti-Bot is the only countermeasure against unknown malware
B. Anti-Bot is the only protection mechanism which starts a counter-attack against known Command & Control Centers
C. Anti-Bot is the only signature-based method of malware protection.
D. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command & Control Center.

Correct Answer: D
Section:
Explanation:
Anti-Bot is a post-infection malware protection that detects and blocks botnet communications from infected hosts to Command & Control servers. It is different from other Threat Prevention mechanisms that prevent malware from entering the network or executing on the hosts.Reference:Anti-Bot Software Blade

QUESTION 34
Which TCP-port does CPM process listen to?

A. 18191
B. 18190
C. 8983
D. 19009

Correct Answer: D
Section:
Explanation:
The CPM process is the core process of the Security Management Server that handles all management operations. It listens to TCP-port 19009 by default.Reference:CPM process

QUESTION 35
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(clish)19+
D. Sending API commands over an http connection using web-services

Correct Answer: D
Section:
Explanation:
The Management API supports three methods of communication: mgmt_cli command, SmartConsole GUI dialog box, and Gaia CLI. Sending API commands over an http connection using web-services is not a supported method.Reference:Check Point Management APIs

QUESTION 36
Your manager asked you to check the status of SecureXL, and its enabled templates and features. What command will you use to provide such information to manager?

A. fw accel stat
B. fwaccel stat
C. fw acces stats
D. fwaccel stats

Correct Answer: B
Section:
Explanation:
The fwaccel stat command displays the status of SecureXL, and its enabled templates and features. The other commands are either incorrect or incomplete.Reference: [SecureXL Commands]

QUESTION 37
SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user's machine via the web browser. What are the two modes of SNX?

A. Application and Client Service
B. Network and Application
C. Network and Layers
D. Virtual Adapter and Mobile App

Correct Answer: B
Section:
Explanation:
SSL Network Extender (SNX) has two modes of operation: Network Mode and Application Mode. Network Mode provides full network connectivity to the remote user, while Application Mode provides access to specific applications on the corporate network.Reference: [SSL Network Extender]

QUESTION 38
Which command would disable a Cluster Member permanently?

A. clusterXL_admin down
B. cphaprob_admin down
C. clusterXL_admin down-p
D. set clusterXL down-p

Correct Answer: C
Section:
Explanation:
The clusterXL_admin down -p command disables a Cluster Member permanently, meaning that it will not rejoin the cluster even after a reboot. The other commands either disable a Cluster Member temporarily or are invalid.Reference: [ClusterXL Administration Guide]

QUESTION 39
Which two of these Check Point Protocols are used by SmartEvent Processes?

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

Correct Answer: D
Section:
Explanation:
SmartEvent Processes use two Check Point Protocols: ELA (Event Log Agent) and CPLOG (Check Point Log). ELA collects logs from Security Gateways and forwards them to the Log Server. CPLOG is used by the Log Server to communicate with the SmartEvent Server.Reference: [SmartEvent Architecture]

QUESTION 40
Fill in the blank: The tool _____ generates a R81 Security Gateway configuration report.

A. infoCP
B. infoview
C. cpinfo
D. fw cpinfo

Correct Answer: C
Section:
Explanation:
The cpinfo tool generates a R81 Security Gateway configuration report that includes information about the hardware, operating system, product version, patches, and configuration settings.Reference:cpinfo - Check Point Support Center

QUESTION 41
Which of these statements describes the Check Point ThreatCloud?

A. Blocks or limits usage of web applications
B. Prevents or controls access to web sites based on category
C. Prevents Cloud vulnerability exploits
D. A worldwide collaborative security network

Correct Answer: D
Section:
Explanation:
The Check Point ThreatCloud is a worldwide collaborative security network that collects and analyzes threat data from millions of sensors, security gateways, and other sources, and delivers real-time threat intelligence and protection to Check Point products.Reference:Check Point ThreatCloud

QUESTION 42
Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every

A. 15 sec
B. 60 sec
C. 5 sec
D. 30 sec

Correct Answer: B
Section:
Explanation:
Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every 60 seconds based on the current traffic load. This ensures optimal performance and load balancing of SecureXL instances.Reference:SecureXL Mechanism

QUESTION 43
Which command will allow you to see the interface status?

A. cphaprob interface
B. cphaprob --I interface
C. cphaprob --a if
D. cphaprob stat

Correct Answer: C
Section:
Explanation:
The cphaprob -a if command displays the interface status of all cluster members, including the interface name, IP address, state, monitor mode, and sync status.Reference:cphaprob - Check Point Support Center

QUESTION 44

Which command can you use to enable or disable multi-queue per interface?

A. cpmq set
B. Cpmqueue set
C. Cpmq config
D. St cpmq enable

Correct Answer: A
Section:
Explanation:
The cpmq set command enables or disables multi-queue per interface. Multi-queue is a feature that allows distributing the network traffic among several CPU cores, improving the throughput and performance of the Security Gateway.Reference:Multi-Queue

QUESTION 45
To help SmartEvent determine whether events originated internally or externally you must define using the Initial Settings under General Settings in the Policy Tab. How many options are available to calculate the traffic direction?

A. 5 Network; Host; Objects; Services; API
B. 3 Incoming; Outgoing; Network
C. 2 Internal; External
D. 4 Incoming; Outgoing; Internal; Other

Correct Answer: D
Section:
Explanation:
To help SmartEvent determine whether events originated internally or externally, you must define the traffic direction using the Initial Settings under General Settings in the Policy Tab. There are four options available to calculate the traffic direction: Incoming, Outgoing, Internal, and Other. Incoming means the source is external and the destination is internal. Outgoing means the source is internal and the destination is external. Internal means both the source and the destination are internal. Other means both the source and the destination are external.Reference:SmartEvent R81 Administration Guide

QUESTION 46
There are 4 ways to use the Management API for creating host object with R81 Management API. Which one is NOT correct?

A. Using Web Services
B. Using Mgmt_cli tool
C. Using CLISH
D. Using SmartConsole GUI console
E. Events are collected with SmartWorkflow from Trouble Ticket systems

Correct Answer: E
Section:
Explanation:
There are four ways to use the Management API for creating host object with R81 Management API: Using Web Services, Using mgmt_cli tool, Using CLISH, and Using SmartConsole GUI console. Events are collected with SmartWorkflow from Trouble Ticket systems is not a correct option.Reference:Check Point Management APIs

QUESTION 47
CoreXL is supported when one of the following features is enabled:

A. Route-based VPN
B. IPS
C. IPv6
D. Overlapping NAT

Correct Answer: B
Section:
Explanation:
CoreXL is supported when one of the following features is enabled: IPS. CoreXL does not support Check Point Suite with these features: Route-based VPN, IPv6, Overlapping NAT, QoS, Content Awareness, Application Control, URL Filtering, Identity Awareness, HTTPS Inspection, DLP, Anti-Bot, Anti-Virus, Threat Emulation.Reference:CoreXL

QUESTION 48
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 multik pq enable

Correct Answer: C
Section:
Explanation:
To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. You can enable them by using the command fw ctl multik set_mode 9. This command sets the SecureXL mode to 9, which means that Priority Queues are enabled and Dynamic Dispatcher is fully enabled.Reference:SecureXL Mechanism

QUESTION 49
Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidates management console. CPM allows the GUI client and management server to communicate via web services using _____.

A. TCP port 19009
B. TCP Port 18190
C. TCP Port 18191
D. TCP Port 18209

Correct Answer: A
Section:
Explanation:
Check Point Management (cpm) is the main management process that provides the architecture for a consolidated management console. CPM allows the GUI client and management server to communicate via web services using TCP port 19009 by default.Reference:CPM process

QUESTION 50
Which command is used to set the CCP protocol to Multicast?

A. cphaprob set_ccp multicast
B. cphaconf set_ccp multicast
C. cphaconf set_ccp no_broadcast

D. cphaprob set_ccp no_broadcast

Correct Answer: B
Section:
Explanation:
The cphaconf set_ccp multicast command is used to set the Cluster Control Protocol (CCP) to Multicast mode. This mode allows cluster members to communicate with each other using multicast packets. The other commands are either incorrect or set the CCP to Broadcast mode.Reference:ClusterXL Administration Guide

QUESTION 51
Which packet info is ignored with Session Rate Acceleration?

A. source port ranges
B. source ip
C. source port
D. same info from Packet Acceleration is used

Correct Answer: C
Section:
Explanation:
Session Rate Acceleration is a SecureXL feature that accelerates the establishment of new connections by bypassing the inspection of the first packet of each session. Session Rate Acceleration ignores the source port information of the packet, as well as the destination port ranges, protocol type, and VPN information. The other packet info is used by Packet Acceleration, which is another SecureXL feature that accelerates the forwarding of subsequent packets of an established connection.Reference:SecureXL Mechanism

QUESTION 52
Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?

A. Synchronized
B. Never been synchronized
C. Lagging
D. Collision

Correct Answer: D
Section:
Explanation:
The least ideal Synchronization Status for Security Management Server High Availability deployment is Collision. This status indicates that both members have modified the same object independently, resulting in a conflict that needs to be resolved manually. The other statuses are either normal or indicate a temporary delay in synchronization.Reference:High Availability Administration Guide

QUESTION 53
During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

A. Host having a Critical event found by Threat Emulation
B. Host having a Critical event found by IPS
C. Host having a Critical event found by Antivirus
D. Host having a Critical event found by Anti-Bot

Correct Answer: D
Section:
Explanation:

The host having a Critical event found by Anti-Bot should be remediated first, as it indicates that the host is infected by a botnet malware that is communicating with a Command and Control server. This poses a serious threat to the network security and data integrity. The other events may indicate potential malware infection or attack attempts, but not necessarily successful ones.Reference:Threat Prevention Administration Guide

QUESTION 54
In R81 spoofing is defined as a method of:

A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
B. Hiding your firewall from unauthorized users.
C. Detecting people using false or wrong authentication logins
D. Making packets appear as if they come from an authorized IP address.

Correct Answer: D
Section:
Explanation:
In R81, spoofing is defined as a method of making packets appear as if they come from an authorized IP address. Spoofing can be used by attackers to bypass security policies or hide their identity. Check Point firewalls use anti-spoofing mechanisms to prevent spoofed packets from entering or leaving the network.Reference:Security Gateway R81 Administration Guide:

QUESTION 55
Connections to the Check Point R81 Web API use what protocol?

A. HTTPS
B. RPC
C. VPN
D. SIC

Correct Answer: A
Section:
Explanation:
Connections to the Check Point R81 Web API use the HTTPS protocol. The Web API is a RESTful web service that allows you to perform management tasks on the Security Management Server using HTTP requests.Reference:Check Point Management APIs

QUESTION 56
Which command lists all tables in Gaia?

A. fw tab --t
B. fw tab --list
C. fw-tab --s
D. fw tab -1

Correct Answer: C
Section:
Explanation:
The fw tab -s command lists all tables in Gaia. The fw tab command displays information about the firewall tables, such as connections, NAT translations, SAM rules, etc. The -s option shows a summary of all tables.Reference:fw tab - Check Point Support Center

QUESTION 57
What is true about the IPS-Blade?

A. In R81, IPS is managed by the Threat Prevention Policy
B. In R81, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
C. In R81, IPS Exceptions cannot be attached to ''all rules''
D. In R81, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Correct Answer: A
Section:
Explanation:
In R81, IPS is managed by the Threat Prevention Policy. The Threat Prevention Policy is a unified policy that allows you to configure and enforce IPS, Anti-Bot, Anti-Virus, Threat Emulation, and Threat Extraction settings in one place.Reference:Threat Prevention Administration Guide

QUESTION 58
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.

Correct Answer: A
Section:
Explanation:
Detecting and blocking malware by correlating multiple detection engines before users are affected is not a feature associated with the Check Point URL Filtering and Application Control Blade. This feature is part of the Check Point SandBlast Network solution, which uses Threat Emulation and Threat Extraction technologies to prevent zero-day attacks. The other features are part of the URL Filtering and Application Control Blade, which allows you to control access to web applications and sites based on various criteria.Reference:URL Filtering and Application Control Administration Guide

QUESTION 59
What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?

A. Stateful Mode
B. VPN Routing Mode
C. Wire Mode
D. Stateless Mode

Correct Answer: C
Section:
Explanation:
Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of 'Wire Mode'.

QUESTION 60
What Factor preclude Secure XL Templating?

A. Source Port Ranges/Encrypted Connections
B. IPS
C. ClusterXL in load sharing Mode

D. CoreXL

Correct Answer: A
Section:
Explanation:
SecureXL Templating is a feature that accelerates the processing of packets that belong to the same connection or session by creating a template for the first packet and applying it to the subsequent packets. SecureXL Templating is precluded by factors that prevent the creation of a template, such as source port ranges, encrypted connections, NAT, QoS, etc.Reference:SecureXL Mechanism

QUESTION 61
In order to get info about assignment (FW, SND) of all CPUs in your SGW, what is the most accurate CLI command?

A. fw ctl sdstat
B. fw ctl affinity --l --a --r --v
C. fw ctl multik stat
D. cpinfo

Correct Answer: B
Section:
Explanation:
The fw ctl affinity -l -a -r -v command is the most accurate CLI command to get info about assignment (FW, SND) of all CPUs in your SGW. This command displays the affinity settings of all interfaces and processes in a verbose mode, including the Firewall (FW) and Secure Network Distributor (SND) instances.Reference:CoreXL Administration Guide

QUESTION 62
Check Pont Central Deployment Tool (CDT) communicates with the Security Gateway / Cluster Members over Check Point SIC _____ .

A. TCP Port 18190
B. TCP Port 18209
C. TCP Port 19009
D. TCP Port 18191

Correct Answer: D
Section:
Explanation:
Check Point Central Deployment Tool (CDT) communicates with the Security Gateway / Cluster Members over Check Point SIC using TCP port 18191 by default. CDT is a tool that allows you to perform simultaneous configuration changes on multiple gateways or clusters using predefined commands or scripts.Reference:Check Point Central Deployment Tool (CDT)

QUESTION 63
The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

A. Secure Internal Communication (SIC)
B. Restart Daemons if they fail
C. Transfers messages between Firewall processes
D. Pulls application monitoring status

Correct Answer: D
Section:
Explanation:
The CPD daemon is a Firewall Kernel Process that does not pull application monitoring status. The CPD daemon is responsible for Secure Internal Communication (SIC), restarting daemons if they fail, transferring messages

between Firewall processes, and managing policy installation.Reference:CPD process

QUESTION 64
What is not a component of Check Point SandBlast?

A. Threat Emulation
B. Threat Simulator
C. Threat Extraction
D. Threat Cloud

Correct Answer: B
Section:
Explanation:
Threat Simulator is not a component of Check Point SandBlast. Check Point SandBlast is a solution that provides advanced protection against zero-day threats using four components: Threat Emulation, Threat Extraction, Threat Cloud, and Threat Prevention.Reference:Check Point SandBlast Network

QUESTION 65
Tom has been tasked to install Check Point R81 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

A. One machine, but it needs to be installed using SecurePlatform for compatibility purposes.
B. One machine
C. Two machines
D. Three machines

Correct Answer: C
Section:
Explanation:
Tom will need two machines to install Check Point R81 in a distributed deployment, if he does not include a SmartConsole machine in his calculations. A distributed deployment consists of a Security Management Server that manages one or more Security Gateways. Therefore, Tom will need one machine for the Security Management Server and another machine for the Security Gateway. The other options are either too few or too many machines for a distributed deployment.
Reference: Check Point R81 Installation and Upgrade Guide

QUESTION 66
You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines a(n) _____ or _____ action for the file types.

A. Inspect/Bypass
B. Inspect/Prevent
C. Prevent/Bypass
D. Detect/Bypass

Correct Answer: A
Section:
Explanation:
You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines anInspectorBypassaction for the file types.The Inspect action means that the file will be sent to the Threat Emulation engine for analysis, and the Bypass action means that the file will not be sent and will be allowed or blocked based on other Threat Prevention blades1. The other options are not valid actions for file types in Threat Prevention profiles.
Reference:Check Point R81 Threat Prevention Administration Guide

QUESTION 67
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. Security Gateway
E. SmartEvent

Correct Answer: D
Section:
Explanation:
When doing a Stand-Alone Installation, you would install the Security Management Server with the Security Gateway as the other Check Point architecture component.A Stand-Alone Installation is where the Security Management Server and the Security Gateway are installed on the same machine2. The other options are either not Check Point architecture components, or not suitable for a Stand-Alone Installation.
Reference:Check Point R81 Installation and Upgrade Guide

QUESTION 68
On R81.20 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

A. 18210
B. 18184
C. 257
D. 18191

Correct Answer: B
Section:
Explanation:
On R81.20, when configuring Third-Party devices to read the logs using the LEA (Log Export API), the default Log Server uses port18184. This port can be changed using thelea_servercommand in expert mode. The other ports are either not related to LEA, or used for different purposes, such as 18210 for CPMI, 257 for FW1_log, and 18191 for SIC.
Reference: [Check Point R81 Logging and Monitoring Administration Guide], [Check Point Ports Used for Communication by Various Check Point Modules]

QUESTION 69
The Correlation Unit performs all but the following actions:

A. Marks logs that individually are not events, but may be part of a larger pattern to be identified later.
B. Generates an event based on the Event policy.
C. Assigns a severity level to the event.
D. Takes a new log entry that is part of a group of items that together make up an event, and adds it to an ongoing event.

Correct Answer: C
Section:
Explanation:
The Correlation Unit in Check Point Security Management performs several actions, but it does not assign a severity level to the event. The Correlation Unit is responsible for identifying patterns in logs, marking logs that are part of larger patterns, generating events based on the Event policy, and adding new log entries to ongoing events. However, assigning a severity level to an event is typically done through the Event policy configuration, not by the Correlation Unit.

QUESTION 70
What is the difference between SSL VPN and IPSec VPN?

A. IPSec VPN does not require installation of a resilient 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.

Correct Answer: D
Section:
Explanation:
The main difference between SSL VPN (Secure Sockets Layer Virtual Private Network) and IPSec VPN (Internet Protocol Security Virtual Private Network) is in the way they operate:
SSL VPN typically does not require the installation of a resident VPN client. It often relies on a web browser to establish the VPN connection, making it more convenient for remote users who may not want to install dedicated VPN software.
IPSec VPN, on the other hand, often requires the installation of a resident VPN client on the user's device to establish the VPN connection. This client software is necessary for configuring and managing the VPN connection.
Option C, stating that SSL VPN and IPSec VPN are the same, is incorrect because they have distinct characteristics as described above.
Option A is incorrect because it inaccurately suggests that IPSec VPN does not require a resident VPN client, which is not true in most cases.
Option B is incorrect because it wrongly claims that SSL VPN requires the installation of a resident VPN client.

QUESTION 71
Which of the following will NOT affect acceleration?

A. Connections destined to or originated from the Security gateway
B. A 5-tuple match
C. Multicast packets
D. Connections that have a Handler (ICMP, FTP, H.323, etc.)

Correct Answer: B
Section:
Explanation:
Check Point's SecureXL technology, which is responsible for acceleration, has certain limitations and conditions under which acceleration may not occur. In this context, the question is asking about factors that will NOT affect acceleration.
Option B, 'A 5-tuple match,' will not affect acceleration. A 5-tuple match refers to the matching of source IP, source port, destination IP, destination port, and protocol. SecureXL can accelerate traffic that matches these criteria, but it's not a factor that hinders acceleration.
Options A, C, and D can all affect acceleration:
Option A mentions 'Connections destined to or originated from the Security gateway,' which implies that SecureXL acceleration can apply to these connections.
Option C mentions 'Multicast packets,' and SecureXL may have limitations in handling multicast traffic efficiently.
Option D mentions 'Connections that have a Handler (ICMP, FTP, H.323, etc.),' and certain protocols (such as FTP) may require special handling and might not be fully accelerated by SecureXL.

QUESTION 72
The following command is used to verify the CPUSE version:

A. HostName:0>show installer status build
B. [Expert@HostName:0]#show installer status
C. [Expert@HostName:0]#show installer status build
D. HostName:0>show installer build

Correct Answer: A
Section:
Explanation:

The correct command to verify the CPUSE (Check Point Update Service Engine) version is:

```lua
HostName:0> show installer status build
```

Option B is incorrect because it uses the '[Expert@HostName:0]#' prompt, which is typically used for expert mode commands, but the CPUSE version can be checked using the 'show installer status build' command in standard mode.
Option C is incorrect because it uses the '[Expert@HostName:0]#' prompt, and while it includes the 'build' parameter, it's not the standard command to check the CPUSE version.
Option D is incorrect because it uses the 'HostName:0>' prompt, but it lacks the 'show' command and uses 'build' instead of 'status build.'

QUESTION 73
What is the difference between an event and a log?

A. Events are generated at gateway according to Event Policy
B. A log entry becomes an event when it matches any rule defined in Event Policy
C. Events are collected with SmartWorkflow form Trouble Ticket systems
D. Log and Events are synonyms

Correct Answer: B
Section:
Explanation:
The difference between an event and a log is that a log entry becomes an event when it matches any rule defined in Event Policy. A log entry is a record of a network activity that is generated by a Security Gateway or a Management Server. An event is a log entry that meets certain criteria and triggers an action or a notification. The other options are either not true or not accurate definitions of events and logs.
Reference: Check Point R81 Logging and Monitoring Administration Guide

QUESTION 74
What are the attributes that SecureXL will check after the connection is allowed by Security Policy?

A. Source address, Destination address, Source port, Destination port, Protocol
B. Source MAC address, Destination MAC address, Source port, Destination port, Protocol
C. Source address, Destination address, Source port, Destination port
D. Source address, Destination address, Destination port, Protocol

Correct Answer: A
Section:
Explanation:
The attributes that SecureXL will check after the connection is allowed by Security Policy areSource address, Destination address, Source port, Destination port, Protocol. These are the five tuple parameters that define a connection and are used by SecureXL to accelerate the traffic.The other options are either missing some of the parameters or include irrelevant ones, such as MAC addresses1.
Reference:Check Point R81 SecureXL Administration Guide

QUESTION 75
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.

Correct Answer: A
Section:
Explanation:
The statement that is not true about Delta synchronization isUsing UDP Multicast or Broadcast on port 8161. Delta synchronization is a mechanism that transfers only the changes in the kernel tables between cluster members, instead of sending the entire tables.It uses UDP Multicast or Broadcast on port8116, not 81612. The other statements are true about Delta synchronization.
Reference:Check Point R81 ClusterXL Administration Guide

QUESTION 76
The Event List within the Event tab contains:

A. a list of options available for running a query.
B. the top events, destinations, sources, and users of the query results, either as a chart or in a tallied list.
C. events generated by a query.
D. the details of a selected event.

Correct Answer: C
Section:
Explanation:
The Event List within the Event tab containsevents generated by a query. The Event List shows the events that match the query criteria, such as time range, filter, and aggregation.The events can be sorted by different columns, such as severity, time, action, and source3. The other options are either not part of the Event tab or not related to the Event List.
Reference:Check Point R81 Logging and Monitoring Administration Guide

QUESTION 77
Which statement is correct about the Sticky Decision Function?

A. It is not supported with either the Performance pack of a hardware based accelerator card
B. Does not support SPI's when configured for Load Sharing
C. It is automatically disabled if the Mobile Access Software Blade is enabled on the cluster
D. It is not required L2TP traffic

Correct Answer: A
Section:
Explanation:
The statement that is correct about the Sticky Decision Function isIt is not supported with either the Performance pack of a hardware based accelerator card. The Sticky Decision Function (SDF) is a feature that ensures that packets from the same connection are handled by the same cluster member in a Load Sharing configuration.However, SDF is not compatible with SecureXL acceleration, which is enabled by default or by using a Performance pack or a hardware based accelerator card4. The other statements are either incorrect or outdated about SDF.
Reference:Check Point R81 ClusterXL Administration Guide,Sticky Decision Function - Check Point CheckMates

QUESTION 78
Which statement is true regarding redundancy?

A. System Administrators know when their cluster has failed over and can also see why it failed over by using the cphaprob --f if command.
B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
C. Machines in a ClusterXL High Availability configuration must be synchronized.
D. Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.

Correct Answer: D
Section:

Explanation:
The statement that is true regarding redundancy isBoth ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments. ClusterXL and VRRP are two technologies that provide high availability and load sharing for Security Gateways.They are both supported by Gaia OS and can be deployed on various platforms5. The other statements are either false or incomplete regarding redundancy.
Reference:Check Point R81 ClusterXL Administration Guide, Check Point R81 Gaia Administration Guide

QUESTION 79
NAT rules are prioritized in which order?
1. Automatic Static NAT
2. Automatic Hide NAT
3. Manual/Pre-Automatic NAT
4. Post-Automatic/Manual NAT rules

A. 1, 2, 3, 4
B. 1, 4, 2, 3
C. 3, 1, 2, 4
D. 4, 3, 1, 2

Correct Answer: A
Section:
Explanation:
NAT rules are prioritized in the following order:
Automatic Static NAT: This is the highest priority NAT rule and it translates the source or destination IP address to a different IP address without changing the port number. It is configured in the network object properties.
Automatic Hide NAT: This is the second highest priority NAT rule and it translates the source IP address and port number to a different IP address and port number. It is configured in the network object properties.
Manual/Pre-Automatic NAT: This is the third highest priority NAT rule and it allows you to create custom NAT rules that are not possible with automatic NAT. It is configured in the NAT policy rulebase before the automatic NAT rules.
Post-Automatic/Manual NAT rules: This is the lowest priority NAT rule and it allows you to create custom NAT rules that are not possible with automatic NAT. It is configured in the NAT policy rulebase after the automatic NAT rules.

QUESTION 80
In R81, how do you manage your Mobile Access Policy?

A. Through the Unified Policy
B. Through the Mobile Console
C. From SmartDashboard
D. From the Dedicated Mobility Tab

Correct Answer: A
Section:
Explanation:
In R81, you can manage your Mobile Access Policy through the Unified Policy. The Unified Policy is a single policy that combines access control, threat prevention, data protection, and identity awareness. You can create rules for mobile access in the Unified Policy rulebase and apply them to mobile devices, users, and applications. You can also use the Mobile Access blade to configure additional settings for mobile access, such as authentication methods, VPN settings, and application portal.

QUESTION 81
R81.20 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. Versions R75 and higher

Correct Answer: C
Section:
Explanation:
R81.20 management server can manage gateways with versions R75.20 and higher. However, some features may not be supported on older gateway versions. For example, R81 introduces a new feature called Infinity Threat Prevention, which requires R81 gateways to work properly. Therefore, it is recommended to upgrade your gateways to the latest version to take advantage of all the new features and enhancements in R81.

QUESTION 82
Which command can you use to verify the number of active concurrent connections?

A. fw conn all
B. fw ctl pstat
C. show all connections
D. show connections

Correct Answer: B
Section:
Explanation:
The commandfw ctl pstatcan be used to verify the number of active concurrent connections on a gateway. This command displays various statistics about the firewall kernel, such as memory usage, CPU utilization, packet rates, and connection table information. The output of this command includes a line that shows the current number of connections and the peak number of connections since the last reboot. For example:

```
Connections all in all: 1234/8192 (15%) at peak: 2345
```

This means that there are currently 1234 active connections out of a maximum of 8192 connections, which is 15% of the connection table capacity. The peak number of connections since the last reboot was 2345.

QUESTION 83
Which of the following statements is TRUE about R81 management plug-ins?

A. The plug-in is a package installed on the Security Gateway.
B. Installing a management plug-in requires a Snapshot, just like any upgrade process.
C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
D. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

Correct Answer: C
Section:
Explanation:
A management plug-in is a software component that interacts with a Security Management Server to provide new features and support for new products. A management plug-in can extend the functionality of SmartConsole, SmartDashboard, SmartView Monitor, SmartView Tracker, SmartEvent, SmartReporter, SmartProvisioning, SmartUpdate, and other management tools. A management plug-in can also add new objects, policies, rules, actions, reports, views, and wizards to the management system. Some examples of management plug-ins are CloudGuard Controller, SandBlast Agent, Endpoint Security Server, Threat Extraction for Web, etc.

QUESTION 84
How can SmartView application accessed?

A. http://<Security Management IP Address>/smartview
B. http://<Security Management IP Address>:4434/smartview/

C. https://<Security Management IP Address>/smartview/
D. https://<Security Management host name>:4434/smartview/

Correct Answer: C
Section:
Explanation:
SmartView is a web-based application that allows you to view and analyze logs, reports, and events from multiple Check Point products. You can access SmartView by using the following URL:

```
https://<Security Management IP Address>/smartview/
```

You need to use HTTPS protocol and the default port 443. You also need to enter the IP address of the Security Management Server that hosts the SmartView application. You cannot use the host name of the Security Management Server or a different port number.
Reference:SmartView R81 Administration Guide

QUESTION 85
What command verifies that the API server is responding?

A. api stat
B. api status
C. show api_status
D. app_get_status

Correct Answer: B
Section:
Explanation:
The API server is a service that runs on the Security Management Server and enables external applications to communicate with the Check Point management database using REST APIs. You can verify that the API server is responding by using the following command in Expert mode:

```
api status
```

This command will display the current status of the API server, such as running, stopped, or initializing. It will also show the API version, port number, and SSL certificate information.
Reference:Check Point R81 REST API Reference Guide

QUESTION 86
Which features are only supported with R81.20 Gateways but not R77.x?

A. Access Control policy unifies the Firewall, Application Control & URL Filtering, Data Awareness, and Mobile Access Software Blade policies.
B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
C. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
D. Time object to a rule to make the rule active only during specified times.

Correct Answer: C
Section:
Explanation:
The features that are only supported with R81.20 Gateways and not with R77.x are described in option C:
'C. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.'
This feature, known as Rule Base Layers, allows for greater flexibility and control in organizing and prioritizing security rules within the rule base.

Options A, B, and D do not specifically pertain to features introduced in R81.20 and are available in earlier versions as well.

QUESTION 87
Which CLI command will reset the IPS pattern matcher statistics?

A. ips reset pmstat
B. ips pstats reset
C. ips pmstats refresh
D. ips pmstats reset

Correct Answer: D
Section:
Explanation:
The CLI command to reset the IPS (Intrusion Prevention System) pattern matcher statistics is option D: ips pmstats reset. This command will reset the statistics related to the IPS pattern matcher.
Options A, B, and C are not the correct syntax for resetting the IPS pattern matcher statistics.

QUESTION 88
When requiring certificates for mobile devices, make sure the authentication method is set to one of the following, Username and Password, RADIUS or _____.

A. SecureID
B. SecurID
C. Complexity
D. TacAcs

Correct Answer: B
Section:
Explanation:
When requiring certificates for mobile devices, the authentication method should be set to one of the following:
Username and Password
RADIUS
SecurID (RSA SecurID)
So, the correct answer is option B, 'SecurID.'
Options A, C, and D are not standard authentication methods for mobile devices in this context.

QUESTION 89
When Dynamic Dispatcher is enabled, connections are assigned dynamically with the exception of:

A. Threat Emulation
B. HTTPS
C. QOS
D. VoIP

Correct Answer: D
Section:
Explanation:
When Dynamic Dispatcher is enabled, it dynamically assigns connections, but there are exceptions. The exception mentioned in the question is:
VoIP (Option D): VoIP connections are an exception when Dynamic Dispatcher is enabled. They are not assigned dynamically but follow a different rule set to ensure quality and reliability for VoIP traffic.
The other options, Threat Emulation (Option A), HTTPS (Option B), and QoS (Option C), are dynamically assigned when Dynamic Dispatcher is enabled.

QUESTION 90
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

Correct Answer: A
Section:
Explanation:
Check Point SandBlast Zero-Day Protection offers flexibility in implementation to meet individual business needs. One of the deployment options for Check Point SandBlast Zero-Day Protection is:
Smart Cloud Services (Option A): Smart Cloud Services allow organizations to leverage cloud-based threat intelligence and protection services provided by Check Point.
The other options, Load Sharing Mode Services (Option B), Threat Agent Solution (Option C), and Public Cloud Services (Option D), may also be components of a security strategy, but they are not specific deployment options for Check Point SandBlast Zero-Day Protection.

QUESTION 91
Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs
B. Capsule Cloud
C. Capsule Enterprise
D. Capsule Workspace

Correct Answer: C
Section:
Explanation:
Check Point Capsule is a suite of solutions designed to provide comprehensive mobile security and secure access. The components of Check Point Capsule include:
Capsule Docs (Option A): A component that secures document sharing and protects sensitive data.
Capsule Cloud (Option B): A component that provides cloud-based security services.
Capsule Workspace (Option D): A component that provides secure workspace on mobile devices.
Option C, 'Capsule Enterprise,' is not a recognized component of Check Point Capsule based on the available information. Therefore, it is the correct answer as the component that is NOT part of Check Point Capsule.

QUESTION 92
What is the purpose of Priority Delta in VRRP?

A. When a box up, Effective Priority = Priority + Priority Delta
B. When an Interface is up, Effective Priority = Priority + Priority Delta
C. When an Interface fail, Effective Priority = Priority -- Priority Delta
D. When a box fail, Effective Priority = Priority -- Priority Delta

Correct Answer: C
Section:
Explanation:
Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP.
If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will begin to send out its own HELLO packet.
Once the master sees this packet with a priority greater than its own, then it releases the VIP.

QUESTION 93
Which statements below are CORRECT regarding Threat Prevention profiles in Smart Dashboard?

A. You can assign only one profile per gateway and a profile can be assigned to one rule Only.
B. You can assign multiple profiles per gateway and a profile can be assigned to one rule only.
C. You can assign multiple profiles per gateway and a profile can be assigned to one or more rules.
D. You can assign only one profile per gateway and a profile can be assigned to one or more rules.

Correct Answer: C
Section:
Explanation:
In SmartDashboard, Threat Prevention profiles can be assigned to one or more rules. This means that you can have multiple profiles assigned to a single gateway, and each of these profiles can be associated with one or more rules. This allows for granular control over threat prevention settings for different rules or scenarios.

QUESTION 94
Using ClusterXL, what statement is true about the Sticky Decision Function?

A. Can only be changed for Load Sharing implementations
B. All connections are processed and synchronized by the pivot
C. Is configured using cpconfig
D. Is only relevant when using SecureXL

Correct Answer: A
Section:
Explanation:
The Sticky Decision Function in ClusterXL is primarily used in Load Sharing implementations. In Load Sharing, the pivot member is responsible for determining the destination of new connections and ensures that traffic from the same source IP address is directed to the same cluster member. This ensures session stickiness for the same source IP, improving load sharing efficiency.

QUESTION 95
What is the name of the secure application for Mail/Calendar for mobile devices?

A. Capsule Workspace
B. Capsule Mail
C. Capsule VPN
D. Secure Workspace

Correct Answer: A
Section:
Explanation:
The secure application for Mail/Calendar for mobile devices in Check Point is called 'Capsule Workspace.' Capsule Workspace provides secure access to email and calendar data on mobile devices while maintaining security policies and controls.

QUESTION 96
Where do you create and modify the Mobile Access policy in R81?

A. SmartConsole
B. SmartMonitor

C. SmartEndpoint
D. SmartDashboard

Correct Answer: A
Section:
Explanation:
In R81, the Mobile Access policy is created and modified in SmartConsole. SmartConsole is the management interface for configuring and managing various security policies, including Mobile Access policies.

QUESTION 97
SmartConsole R81 requires the following ports to be open for SmartEvent R81 management:

A. 19090,22
B. 19190,22
C. 18190,80
D. 19009,443

Correct Answer: D
Section:
Explanation:
To use SmartConsole R81 for managing SmartEvent R81, you need to have the following ports open:
Port 19009 for communication over HTTPS (443)
Port 19009 for communication over HTTP (80)
These ports are necessary for the SmartConsole to communicate with SmartEvent for management and monitoring purposes.

QUESTION 98
Which configuration file contains the structure of the Security Server showing the port numbers, corresponding protocol name, and status?

A. $FWDIR/database/fwauthd.conf
B. $FWDIR/conf/fwauth.conf
C. $FWDIR/conf/fwauthd.conf
D. $FWDIR/state/fwauthd.conf

Correct Answer: C
Section:
Explanation:
The configuration file that contains the structure of the Security Server showing the port numbers, corresponding protocol name, and status is $FWDIR/conf/fwauthd.conf. This file is used for configuring authentication services in Check Point Security Servers.

QUESTION 99
What API command below creates a new host with the name ''New Host'' and IP address of ''192.168.0.10''?

A. new host name ''New Host'' ip-address ''192.168.0.10''
B. set host name ''New Host'' ip-address ''192.168.0.10''
C. create host name ''New Host'' ip-address ''192.168.0.10''
D. add host name ''New Host'' ip-address ''192.168.0.10''

Correct Answer: D
Section:

Explanation:
The API command to create a new host with the name 'New Host' and IP address '192.168.0.10' is:

```csharp
add host name "New Host" ip-address "192.168.0.10"
```

This command adds a host object with the specified name and IP address to the Check Point configuration.

QUESTION 100
The essential means by which state synchronization works to provide failover in the event an active member goes down, _____ is used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster.

A. ccp
B. cphaconf
C. cphad
D. cphastart

Correct Answer: A
Section:
Explanation:
The essential means by which state synchronization works to provide failover in the event an active member goes down,ccpis used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster. Ccp stands for Cluster Control Protocol, and it is a proprietary protocol that runs on UDP port 8116. Ccp is responsible for exchanging state information, health checks, load balancing decisions, and synchronization network configuration between cluster members.The other options are either commands or daemons that are related to cluster operations, but not the protocol itself.

QUESTION 101
Which statement is most correct regarding about ''CoreXL Dynamic Dispatcher''?

A. The CoreXL FW instanxces assignment mechanism is based on Source MAC addresses, Destination MAC addresses
B. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores
C. The CoreXL FW instances assignment mechanism is based on IP Protocol type
D. The CoreXl FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type

Correct Answer: B
Section:
Explanation:
The statement that is most correct regarding about ''CoreXL Dynamic Dispatcher'' is: The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores. CoreXL Dynamic Dispatcher is a feature that allows the Security Gateway to dynamically assign connections to the most available CoreXL FW instance, based on the CPU core utilization. This improves the performance and load balancing of the Security Gateway, especially when handling connections with different processing requirements.The other statements are either incorrect or describe the CoreXL Static Dispatcher mechanism, which assigns connections based on a hash function of the Source IP, Destination IP, and IP Protocol type.

QUESTION 102
What CLI command compiles and installs a Security Policy on the target's Security Gateways?

A. fwm compile
B. fwm load
C. fwm fetch
D. fwm install

Correct Answer: B
Section:
Explanation:
The CLI command that compiles and installs a Security Policy on the target's Security Gateways isfwm load. Fwm stands for FireWall Management, and it is a command that allows administrators to perform various management tasks on the Security Management Server or Multi-Domain Server. Fwm load takes two arguments: the name of the Security Policy and the name or IP address of the target Security Gateway or Gateway Cluster. For example:
[Expert@SMS]# fwm load Standard_Policy fw1
This command will compile and install the Standard_Policy on the Security Gateway named fw1. The other commands are either invalid or perform different functions.

QUESTION 103
Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R81.20. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.
What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?

A. Pamela should check SecureXL status on DMZ Security gateway and if it's turned ON. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.
B. Pamela should check SecureXL status on DMZ Security Gateway and if it's turned OFF. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.
C. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
D. Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.

Correct Answer: A
Section:
Explanation:
The best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic is: Pamela should check SecureXL status on DMZ Security gateway and if it's turned ON. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures. SecureXL is a technology that accelerates network traffic processing by offloading intensive operations from the Firewall kernel to a dedicated SecureXL device. However, this also means that some traffic might not be seen by fw monitor, which is a tool that captures packets at different inspection points in the Firewall kernel. Therefore, to ensure that fw monitor captures all traffic, SecureXL should be turned OFF before using fw monitor. The other suggestions are either incorrect or less effective in capturing traffic.

QUESTION 104
Fill in the blank: The ''fw monitor'' tool can be best used to troubleshoot _____.

A. AV issues
B. VPN errors
C. Network traffic issues
D. Authentication issues

Correct Answer: C
Section:
Explanation:
The ''fw monitor'' tool can be best used to troubleshootnetwork traffic issues. Fw monitor is a tool that allows administrators to capture packets at different inspection points in the Firewall kernel, and apply filters and flags to analyze the traffic. Fw monitor can help troubleshoot network connectivity problems, packet drops, NAT issues, VPN issues, and more. The other options are either not related or less suitable for fw monitor.

QUESTION 105
For Management High Availability, which of the following is NOT a valid synchronization status?

A. Collision
B. Down
C. Lagging

D. Never been synchronized

Correct Answer: B
Section:
Explanation:
For Management High Availability, the valid synchronization status options are:
A) Collision
B) Down
C) Lagging
D) Never been synchronized
In this context, 'Down' indicates that the synchronization is not functioning correctly or that the standby management server is not reachable. This is a valid synchronization status, so the answer is not B.

QUESTION 106
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.

Correct Answer: C
Section:
Explanation:
Multiple administrators can connect to a Security Management Server at the same time. Each administrator has their own username and works in a session that is independent of other administrators. This allows for collaboration and simultaneous management tasks by different administrators.

QUESTION 107
Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?

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

Correct Answer: D
Section:
Explanation:
Firewall Management (fwm) is available on any management product, including Multi-Domain and on products that requite direct GUI access, such as SmartEvent, It provides the following:
-- GUI Client communication
-- Database manipulation
-- Policy Compilation
-- Management HA sync

QUESTION 108
To add a file to the Threat Prevention Whitelist, what two items are needed?

A. File name and Gateway

B. Object Name and MD5 signature
C. MD5 signature and Gateway
D. IP address of Management Server and Gateway

Correct Answer: B
Section:
Explanation:
To add a file to the Threat Prevention Whitelist, you need two items:
B) Object Name and MD5 signature
You need the Object Name to identify the file or object you want to whitelist, and the MD5 signature to specify the unique hash value of that file. The MD5 signature ensures that the specific file you want to whitelist is identified accurately.

QUESTION 109
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

Correct Answer: D
Section:
Explanation:
The proxy ARP configuration is stored under the following file: $FWDIR/conf/local.arp on the gateway This file, local.arp, contains the proxy ARP configuration for the Security Gateway. It is used to configure ARP (Address Resolution Protocol) settings for network communication.

QUESTION 110
What information is NOT collected from a Security Gateway in a Cpinfo?

A. Firewall logs
B. Configuration and database files
C. System message logs
D. OS and network statistics

Correct Answer: A
Section:
Explanation:
In a Cpinfo (Checkpoint information) command, various information is collected from a Security Gateway. However, firewall logs are NOT collected from a Security Gateway in a Cpinfo.
A) Firewall logs
The Cpinfo command typically collects information such as configuration and database files, system message logs, OS and network statistics, but it does not include firewall logs. Firewall logs are usually obtained separately using other methods or tools.

QUESTION 111
SandBlast appliances can be deployed in the following modes:

A. using a SPAN port to receive a copy of the traffic only
B. detect only
C. inline/prevent or detect

D. as a Mail Transfer Agent and as part of the traffic flow only

Correct Answer: C
Section:
Explanation:
SandBlast appliances can be deployed in the following modes:
C) Inline/prevent or detect
SandBlast appliances can be deployed in an inline mode where they actively inspect and prevent or detect malicious traffic. In this mode, the appliance sits in the network traffic path and can take actions to block or detect threats in real-time.

QUESTION 112
Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enabled which path is handling the traffic?

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

Correct Answer: A
Section:
Explanation:
When traffic from source 192.168.1.1 is going to www.google.com, and the Application Control Blade on the gateway is inspecting the traffic with acceleration enabled, it is handled by the Slow Path.
A) Slow Path
The Slow Path is responsible for handling traffic that requires full inspection by various security blades, including the Application Control Blade. Acceleration may offload some processing to the Medium Path or Fast Path, but the Slow Path is still involved in deeper inspection.

QUESTION 113
How do you enable virtual mac (VMAC) on-the-fly on a cluster member?

A. cphaprob set int fwha_vmac_global_param_enabled 1
B. clusterXL set int fwha_vmac_global_param_enabled 1
C. fw ctl set int fwha_vmac_global_param_enabled 1
D. cphaconf set int fwha_vmac_global_param_enabled 1

Correct Answer: C
Section:
Explanation:
To enable VMAC mode on a cluster member, you need to set the value of the global kernel parameterfwha_vmac_global_param_enabledto 1. This can be done on-the-fly using the commandfw ctl set int fwha_vmac_global_param_enabled 1on all cluster members. This command does not require a reboot or a policy installation. VMAC mode allows the cluster to use a virtual MAC address for its virtual IP addresses, which reduces the number of gratuitous ARP packets sent upon failover and avoids ARP cache issues on some routers and switches.
Reference:How to enable ClusterXL Virtual MAC (VMAC) mode

QUESTION 114
Which command is used to obtain the configuration lock in Gaia?

A. Lock database override
B. Unlock database override
C. Unlock database lock

D. Lock database user

Correct Answer: A
Section:
Explanation:
Which command is used to obtain the configuration lock in Gaia? The command that is used to obtain the configuration lock in Gaia islock database override. This command allows a user to take over the configuration lock from another user who is currently logged in with read/write access. The other user will be forced to logout and will lose any unsaved changes. This command should be used with caution and only when necessary.
Reference:Gaia Administration Guide R81, page 15.

QUESTION 115
What is the default shell for the command line interface?

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

Correct Answer: B
Section:
Explanation:
What is the default shell for the command line interface? The default shell for the command line interface isClish. Clish is a shell that provides a menu-based interface for configuring various system settings, such as network interfaces, routing, DNS, NTP, SNMP, SSH, etc. Clish also provides help and completion features for easier navigation. To switch from Clish to Expert mode, which allows running Linux commands, use the commandexpert.
Reference:Gaia Administration Guide R81, page 29.

QUESTION 116
You plan to automate creating new objects using new R81 Management API. You decide to use GAIA CLI for this task.
What is the first step to run management API commands on GAIA's shell?

A. mgmt_admin@teabag > id.txt
B. mgmt_login
C. login user admin password teabag
D. mgmt_cli login user ''admin'' password ''teabag'' > id.txt

Correct Answer: B
Section:
Explanation:
You plan to automate creating new objects using new R81 Management API. You decide to use GAIA CLI for this task.
The first step to run management API commands on GAIA's shell ismgmt_login. This command allows you to login to the management server and obtain a session ID, which is required for running other management API commands. You can also specify the user name and password as parameters, or enter them interactively. The session ID is stored in the file$CPDIR/tmp/.api_sessionby default, unless you specify a different file name.
Reference:R81 Management API Reference Guide, page 15.

QUESTION 117
On R81.20 the IPS Blade is managed by:

A. Threat Protection policy
B. Anti-Bot Blade
C. Threat Prevention policy
D. Layers on Firewall policy

Correct Answer: C
Section:
Explanation:
On R81.20 the IPS Blade is managed by theThreat Prevention policy. The Threat Prevention policy is a unified policy that includes Anti-virus, IPS, Anti-bot, and Threat Emulation software blades. The IPS blade provides protection against network attacks and exploits by inspecting the traffic and blocking malicious packets. The IPS blade can be configured with different profiles and exceptions to suit different security needs.
Reference:R81 Threat Prevention Administration Guide, page 15.

QUESTION 118
When users connect to the Mobile Access portal they are unable to open File Shares.
Which log file would you want to examine?

A. cvpnd.elg
B. httpd.elg
C. vpnd.elg
D. fw.elg

Correct Answer: A
Section:
Explanation:
When users connect to the Mobile Access portal they are unable to open File Shares.
The log file that you would want to examine iscvpnd.elg. This log file contains information about the Mobile Access VPN daemon, which handles the connections from the Mobile Access portal to the internal resources, such as File Shares, Web Applications, etc. The log file is located in the directory$FWDIR/log/on the Security Gateway. You can use the commandfw log -f cvpnd.elgto view the log file in real time.
Reference:R81 Mobile Access Administration Guide, page 255.

QUESTION 119
What is the correct order of the default ''fw monitor'' inspection points?

A. i, o, l, O
B. i, l, o, O
C. 1, 2, 3, 4
D. l, i, O, o

Correct Answer: B
Section:
Explanation:
https://community.checkpoint.com/t5/General-Topics/Check-Point-Inspection-points-iIoO/td-p/34938
The default order of the 'fw monitor' inspection points is:
i (input): this is the first inspection point, where packets enter the firewall.
l (local): this is the second inspection point, where packets are processed locally by the firewall, before being forwarded to the next hop.
o (output): this is the third inspection point, where packets are sent out to their final destination.
O (offload): this is the fourth inspection point, where packets are offloaded to hardware acceleration for faster processing.

QUESTION 120
What is the default size of NAT table fwx_alloc?

A. 20000
B. 35000
C. 25000

D. 10000

Correct Answer: C
Section:
Explanation:
What is the default size of NAT table fwx_alloc? The default size of NAT table fwx_alloc is25000. This table stores the connections that require NAT translation by the Security Gateway. The size of this table can be changed by using the commandfw ctl set int fwx_alloc <value>, where <value> is the desired number of connections. The maximum value is 65535. To make this change permanent, you need to add this command to the file$FWDIR/conf/fwaffinity.confon the Security Gateway.
Reference: [R81 Performance Tuning Administration Guide], page 126.

QUESTION 121
What are types of Check Point APIs available currently as part of R81.20 code?

A. Security Gateway API Management API, Threat Prevention API and Identity Awareness Web Services API
B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
C. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API
D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Correct Answer: B
Section:
Explanation:
What are types of Check Point APIs available currently as part of R81.20 code?
The types of Check Point APIs available currently as part of R81.20 code are:
Management API: This API allows you to automate and orchestrate various management tasks, such as creating and modifying objects, installing policies, generating reports, etc. The Management API can be accessed via CLI, Web Services, or GUI clients.
Threat Prevention API: This API allows you to interact with the Threat Prevention software blades, such as Anti-Virus, Anti-Bot, Threat Emulation, etc. The Threat Prevention API can be used to query and update indicators, upload files for emulation, retrieve verdicts and reports, etc.
Identity Awareness Web Services API: This API allows you to integrate external identity sources with the Identity Awareness software blade, which provides identity-based access control for network traffic. The Identity Awareness Web Services API can be used to send identity and session information to the Security Gateway, query identity information from the Security Gateway, etc.
OPSEC SDK API: This API allows you to develop custom applications that can communicate with Check Point products using the OPSEC protocol. The OPSEC SDK API supports various OPSEC services, such as LEA, CPMI, SAM, ELA, UFP, etc.
Reference:R81 Management API Reference Guide, page 7; [R81 Threat Prevention API Reference Guide], page 7; [R81 Identity Awareness Administration Guide], page 105; [OPSEC SDK R81 Documentation Package].

QUESTION 122
To accelerate the rate of connection establishment, SecureXL groups all connection that match a particular service and whose sole differentiating element is the source port. The type of grouping enables even the very first packets of a TCP handshake to be accelerated. The first packets of the first connection on the same service will be forwarded to the Firewall kernel which will then create a template of the connection. Which of the these is NOT a SecureXL template?

A. Accept Template
B. Deny Template
C. Drop Template
D. NAT Template

Correct Answer: B
Section:
Explanation:
SecureXL templates are a mechanism to accelerate the rate of connection establishment by grouping connections that match a particular service and whose sole differentiating element is the source port. SecureXL templates enable even the very first packets of a TCP handshake to be accelerated, without waiting for the Firewall kernel to create a connection entry. The first packets of the first connection on the same service will be forwarded to the Firewall kernel, which will then create a template of the connection. The template will contain all the relevant information for the connection, such as source and destination IP addresses, destination port, NAT

information, policy decision, etc. The template will be used by SecureXL to handle subsequent connections on the same service, without involving the Firewall kernel. This reduces the CPU load and increases the throughput. There are three types of SecureXL templates: Accept, Drop, and NAT. Accept templates are used for connections that are allowed by the Firewall policy. Drop templates are used for connections that are blocked by the Firewall policy. NAT templates are used for connections that require NAT translation. Deny templates are not a valid type of SecureXL template.

QUESTION 123
Which of the following is NOT a type of Check Point API available in R81.x?

A. Identity Awareness Web Services
B. OPSEC SDK
C. Mobile Access
D. Management

Correct Answer: C
Section:
Explanation:
Check Point API is a set of web services that enable the usage of functions and commands in a dynamic and automated fashion. Check Point API is available in different types, each serving a different purpose and functionality.According to the Check Point Resource Library1, the following are the types of Check Point API available in R81.x:
Identity Awareness Web Services: This type of API allows external applications to send identity and location information to the Security Gateway, which can then use this information for policy enforcement. Identity Awareness Web Services can be used for scenarios such as guest registration, captive portal, identity agents, etc.
OPSEC SDK: This type of API provides a framework for developing applications that interact with Check Point products using the OPSEC (Open Platform for Security) protocol. OPSEC SDK can be used for scenarios such as log export, event management, anti-virus integration, etc.
Management: This type of API allows external applications to perform management operations on the Check Point Management server using RESTful web services. Management API can be used for scenarios such as policy installation, object creation, configuration backup, etc.
Mobile Access is not a type of Check Point API, but rather a feature that provides secure remote access to corporate resources from various devices. Mobile Access uses SSL VPN technology and supports different authentication methods and access scenarios.

QUESTION 124
When an encrypted packet is decrypted, where does this happen?

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

Correct Answer: A
Section:
Explanation:
When an encrypted packet is received by a Check Point Security Gateway, it is decrypted according to the security policy. The security policy defines the rules and settings for encryption and decryption of traffic, such as the encryption algorithm, the encryption domain, the pre-shared secret or certificate, etc. The security policy is enforced by the Firewall kernel, which is responsible for decrypting the packets before passing them to the inbound chain for further inspection. The inbound chain consists of various inspection modules that apply security checks and actions on the decrypted packets. The outbound chain is the reverse process, where the packets are inspected and then encrypted according to the security policy before being sent out.

QUESTION 125
John is using Management H

A. Which Smartcenter should be connected to for making changes?
B. secondary Smartcenter
C. active Smartenter

D. connect virtual IP of Smartcenter HA
E. primary Smartcenter

Correct Answer: B
Section:
Explanation:
Management HA is a feature that allows the Security Management server to have one or more backup Standby Security Management servers that are ready to take over in case of failure1. The Active Security Management server is the one that handles all the management operations, such as policy installation, object creation, configuration backup, etc. The Standby Security Management servers are synchronized with the Active Security Management server and store the same data, such as databases, certificates, CRLs, etc.The Standby Security Management servers can also perform some operations, such as fetching a Security Policy or retrieving a CRL1.
To make changes to the system, such as editing objects or policies, the administrator needs to connect to the Active Security Management server. This is because the Active Security Management server is the only one that can modify the data and synchronize it with the Standby Security Management servers.The administrator can use SmartConsole to connect to the Active Security Management server by entering its IP address or hostname1.
The administrator can also use SmartDashboard to connect to the Active Security Management server by selecting Policy > Management High Availability.This shows information about the Security Management server that includes its peers - displayed with the name, status and type of Security Management server1.
The other options are incorrect because:
A) secondary Smartcenter: This is a synonym for a Standby Security Management server, which cannot be used to make changes to the system.
C) connect virtual IP of Smartcenter HA: This is not a valid option because there is no virtual IP for Smartcenter HA. Each Security Management server has its own IP address and hostname.
D) primary Smartcenter: This is a synonym for the Active Security Management server, but it is not the correct term to use. The term primary implies that there is only one Active Security Management server, which is not true.The administrator can put the Active Security Management server on standby and promote a Standby Security Management server to active at any time1.

QUESTION 126
You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Correct Answer: B
Section:
Explanation:
User-mode processes are processes that run in the user space of the operating system, as opposed to kernel-mode processes that run in the kernel space. User-mode processes are usually less privileged and have less access to system resources than kernel-mode processes. Check Point products use both user-mode and kernel-mode processes to provide various functionalities and services.
The following are some of the user-mode processes that can be seen on the management server and gateway:
fwd: This process is responsible for policy installation, logging, and communication with other Check Point components. It runs on both the management server and gateway.
cpd: This process is responsible for licensing, certificate management, and communication with SmartConsole. It runs on both the management server and gateway.
cpwd: This process is responsible for monitoring and restarting other processes. It runs on both the management server and gateway.
The following is a user-mode process that can only be seen on the management server:
fwm: This process is responsible for managing the security policy database, compiling the security policy, and generating reports. It runs only on the management server.
Therefore, the correct answer is B)

QUESTION 127
What scenario indicates that SecureXL is enabled?

A. Dynamic objects are available in the Object Explorer
B. SecureXL can be disabled in cpconfig
C. fwaccel commands can be used in clish
D. Only one packet in a stream is seen in a fw monitor packet capture

Correct Answer: C
Section:
Explanation:
SecureXL is a technology that accelerates the performance of the Check Point Security Gateway by offloading CPU-intensive operations from the Firewall kernel to the SecureXL device. SecureXL can handle various types of traffic, such as TCP, UDP, ICMP, non-IP, VPN, NAT, etc. SecureXL can also work with various features, such as CoreXL, ClusterXL, QoS, etc.
One way to indicate that SecureXL is enabled is to use thefwaccelcommands in clish. Clish is a command-line shell that provides a user-friendly interface for configuring and managing Check Point products. Thefwaccelcommands are used to control and monitor SecureXL operations, such as enabling or disabling SecureXL, viewing SecureXL statistics, managing SecureXL templates, etc. For example, the commandfwaccel statshows the status of SecureXL, such as whether it is on or off, how many packets are accelerated or not accelerated, etc.
The other options are not valid indicators of SecureXL being enabled:
A) Dynamic objects are available in the Object Explorer: Dynamic objects are objects that represent IP addresses that change over time, such as VPN clients, DHCP clients, etc. Dynamic objects are available in the Object Explorer regardless of whether SecureXL is enabled or not.
B) SecureXL can be disabled in cpconfig: Cpconfig is a command-line tool that allows you to configure various settings of Check Point products, such as administrator password, GUI clients, SNMP extension, etc. SecureXL can be disabled in cpconfig only if it was enabled before. Therefore, this option does not indicate that SecureXL is enabled.
D) Only one packet in a stream is seen in a fw monitor packet capture: Fw monitor is a command-line tool that allows you to capture and analyze network traffic passing through the Security Gateway. Fw monitor shows the traffic at different inspection points in the Firewall kernel. If SecureXL is enabled, some packets may be accelerated by SecureXL and bypass the Firewall kernel inspection. Therefore, fw monitor may not see all packets in a stream. However, this does not mean that only one packet in a stream will be seen by fw monitor. Some packets may still go through the Firewall kernel inspection and be seen by fw monitor. Therefore, this option does not indicate that SecureXL is enabled.
Therefore, the correct answer is C.

QUESTION 128
What processes does CPM control?

A. Object-Store, Database changes, CPM Process and web-services
B. web-services, CPMI process, DLEserver, CPM process
C. DLEServer, Object-Store, CP Process and database changes
D. web_services, dle_server and object_Store

Correct Answer: D
Section:
Explanation:
CPM stands for Check Point Management, which is a process that runs on the Security Management server and controls the management operations, such as policy installation, object creation, configuration backup, etc. CPM also controls other processes that are related to the management functions, such as:
web_services: This process is responsible for providing web services for the communication between SmartConsole and the Security Management server. It handles requests from SmartConsole clients and forwards them to CPM or other processes.
dle_server: This process is responsible for managing the log files and indexes. It handles queries from SmartLog and SmartEvent and provides log data to CPM or other processes.
object_Store: This process is responsible for storing and retrieving objects from the database. It handles requests from CPM or other processes and provides object data.
Therefore, the correct answer is D)
The other options are incorrect because:
A) Object-Store, Database changes, CPM Process and web-services: This option includes some processes that are controlled by CPM, such as Object-Store, CPM Process, and web-services, but it also includes Database changes, which is not a process but an action performed by CPM or other processes.
B) web-services, CPMI process, DLEserver, CPM process: This option includes some processes that are controlled by CPM, such as web-services, DLEserver, and CPM process, but it also includes CPMI process, which is not a process but a protocol used by CPM or other processes to communicate with each other.
C) DLEServer, Object-Store, CP Process and database changes: This option includes some processes that are controlled by CPM, such as DLEServer and Object-Store, but it also includes CP Process and database changes, which are not processes but a generic term for any Check Point process and an action performed by CPM or other processes respectively.

QUESTION 129
Which Check Point software blades could be enforced under Threat Prevention profile using Check Point R81.20 SmartConsole application?

A. IPS, Anti-Bot, URL Filtering, Application Control, Threat Emulation.

B. Firewall, IPS, Threat Emulation, Application Control.
C. IPS, Anti-Bot, Anti-Virus, Threat Emulation, Threat Extraction.
D. Firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation.

Correct Answer: C
Section:
Explanation:
The Threat Prevention profile in Check Point R81.20 SmartConsole application allows you to enforce the following software blades: IPS, Anti-Bot, Anti-Virus, Threat Emulation, and Threat Extraction. These software blades provide comprehensive protection against various types of threats, such as network attacks, malware, ransomware, phishing, and zero-day exploits. You can configure the profile settings for each software blade, such as the action to take, the protection scope, and the exceptions.
Reference:Check Point Security Expert R81 Course,Threat Prevention Administration Guide

QUESTION 130
When gathering information about a gateway using CPINFO, what information is included or excluded when using the ''-x'' parameter?

A. Includes the registry
B. Gets information about the specified Virtual System
C. Does not resolve network addresses
D. Output excludes connection table

Correct Answer: B
Section:
Explanation:
The cpinfo command is a tool that collects diagnostic data from a Check Point gateway or management server. The data includes configuration files, logs, status reports, and more. The cpinfo output can be used for troubleshooting or sent to Check Point support for analysis. The -x parameter is used to get information about the specified Virtual System on a VSX gateway. A Virtual System is a virtualized firewall instance that runs on a VSX gateway and has its own security policy and objects.
Reference:Check Point Security Expert R81 Course,cpinfo Utility,VSX Administration Guide

QUESTION 131
Security Checkup Summary can be easily conducted within:

A. Summary
B. Views
C. Reports
D. Checkups

Correct Answer: B
Section:
Explanation:
Security Checkup Summary can be easily conducted within Views. Views is a feature in SmartConsole that allows you to create customized dashboards and reports based on various security data sources, such as logs, events, audit trails, and more. You can use Views to perform a Security Checkup Summary, which is a comprehensive analysis of your network security posture and potential risks. You can use predefined templates or create your own views to generate the summary.
Reference:Check Point Security Expert R81 Course, Views Administration Guide

QUESTION 132
What command can you use to have cpinfo display all installed hotfixes?

A. cpinfo -hf

B. cpinfo --y all
C. cpinfo --get hf
D. cpinfo installed_jumbo

Correct Answer: B
Section:
Explanation:
The command cpinfo -y all can be used to have cpinfo display all installed hotfixes. Cpinfo is a tool that collects diagnostic data from a Check Point gateway or management server. The data includes configuration files, logs, status reports, and more. The -y parameter is used to specify which sections of data to include in the cpinfo output. The value all means to include all sections, including the hotfixes section, which shows the list of hotfixes installed on the system.
Reference:Check Point Security Expert R81 Course, cpinfo Utility

QUESTION 133
Using Threat Emulation technologies, what is the best way to block .exe and .bat file types?

A. enable DLP and select.exe and .bat file type
B. enable .exe & .bat protection in IPS Policy
C. create FW rule for particular protocol
D. tecli advanced attributes set prohibited_file_types exe.bat

Correct Answer: A
Section:
Explanation:
The best way to block .exe and .bat file types using Threat Emulation technologies is toenable DLP and select .exe and .bat file type. DLP stands for Data Loss Prevention, and it is a feature that allows administrators to define rules and actions to protect sensitive data from unauthorized access or transfer. One of the DLP rule conditions is File Type, which can be used to block or alert on specific file types, such as .exe and .bat, that may contain malicious code or scripts. The other options are either not related to Threat Emulation technologies, or not effective in blocking .exe and .bat file types.
Topic 3, Exam Pool C

QUESTION 134
What is the recommended number of physical network interfaces in a Mobile Access cluster deployment?

A. 4 Interfaces -- an interface leading to the organization, a second interface leading to the internet, a third interface for synchronization, a fourth interface leading to the Security Management Server.
B. 3 Interfaces -- an interface leading to the organization, a second interface leading to the Internet, a third interface for synchronization.
C. 1 Interface -- an interface leading to the organization and the Internet, and configure for synchronization.
D. 2 Interfaces -- a data interface leading to the organization and the Internet, a second interface for synchronization.

Correct Answer: B
Section:
Explanation:
According to the Check Point R81 Mobile Access Administration Guide, the recommended number of physical network interfaces in a Mobile Access cluster deployment isthree. One interface should be connected to the organization network, one interface should be connected to the Internet, and one interface should be used for synchronization between cluster members.This configuration provides optimal performance and security for Mobile Access traffic.

QUESTION 135
Which process handles connection from SmartConsole R81?

A. fwm
B. cpmd

C. cpm
D. cpd

Correct Answer: C
Section:
Explanation:
The process that handles connection from SmartConsole R81 iscpm. Cpm stands for Check Point Management, and it is the main process that runs on the Security Management Server and interacts with SmartConsole clients. Cpm is responsible for managing policies, objects, logs, tasks, and other management functions.The other processes are either obsolete or irrelevant for SmartConsole connection.

QUESTION 136
What is the command to show SecureXL status?

A. fwaccel status
B. fwaccel stats -m
C. fwaccel -s
D. fwaccel stat

Correct Answer: D
Section:
Explanation:
The command to show SecureXL status isfwaccel stat. This command displays information about SecureXL acceleration, such as the number of accelerated and non-accelerated connections, the reason for non-acceleration, and the SecureXL device name and mode.The other commands are either invalid or show different statistics.

QUESTION 137
The SmartEvent R81 Web application for real-time event monitoring is called:

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

Correct Answer: B
Section:
Explanation:
The SmartEvent R81 Web application for real-time event monitoring is calledSmartEventWeb. SmartEventWeb is a web-based interface that allows administrators to view and analyze security events from various sources, such as logs, reports, incidents, and indicators. SmartEventWeb provides dashboards, widgets, filters, and drill-down options to help administrators gain insights into their security posture. The other options are either incorrect or refer to different applications.

QUESTION 138
What will SmartEvent automatically define as events?

A. Firewall
B. VPN
C. IPS
D. HTTPS

Correct Answer: C
Section:

Explanation:
SmartEvent automatically defines events based onIPS(Intrusion Prevention System) alerts. IPS is a feature that detects and prevents malicious network traffic based on predefined or custom signatures. IPS alerts are generated when IPS detects an attack or an anomaly that matches a signature. SmartEvent collects and correlates IPS alerts from different gateways and displays them as events in SmartEventWeb. The other options are not automatically defined as events by SmartEvent.

QUESTION 139
With MTA (Mail Transfer Agent) enabled the gateways manages SMTP traffic and holds external email with potentially malicious attachments. What is required in order to enable MTA (Mail Transfer Agent) functionality in the Security Gateway?

A. Threat Cloud Intelligence
B. Threat Prevention Software Blade Package
C. Endpoint Total Protection
D. Traffic on port 25

Correct Answer: B
Section:
Explanation:
To enable MTA (Mail Transfer Agent) functionality in the Security Gateway, theThreat Prevention Software Blade Packageis required. The Threat Prevention Software Blade Package includes the Anti-Virus, Anti-Bot, and Threat Emulation blades, which can scan and hold external email with potentially malicious attachments. The MTA functionality allows the Security Gateway to act as an SMTP relay between the mail server and the Internet, and apply Threat Prevention policies to the email traffic.The other options are either not related or not sufficient to enable MTA functionality. R

QUESTION 140
What is not a purpose of the deployment of Check Point API?

A. Execute an automated script to perform common tasks
B. Create a customized GUI Client for manipulating the objects database
C. Create products that use and enhance the Check Point solution
D. Integrate Check Point products with 3rd party solution

Correct Answer: B
Section:
Explanation:
The deployment of Check Point API does not have the purpose of creating a customized GUI Client for manipulating the objects database. The Check Point API is a web service that allows external applications to interact with the Check Point management server using standard methods such as HTTP(S) requests and JSON objects. The Check Point API can be used to execute an automated script to perform common tasks, create products that use and enhance the Check Point solution, and integrate Check Point products with 3rd party solutions.However, creating a customized GUI Client for manipulating the objects database is not a supported or intended use case of the Check Point API.

QUESTION 141
You need to change the number of firewall Instances used by CoreXL. How can you achieve this goal?

A. edit fwaffinity.conf; reboot required
B. cpconfig; reboot required
C. edit fwaffinity.conf; reboot not required
D. cpconfig; reboot not required

Correct Answer: B
Section:
Explanation:

To change the number of firewall instances used by CoreXL, thecpconfigcommand must be used, followed by a reboot. CoreXL is a technology that improves the performance of the Security Gateway by using multiple cores to handle concurrent connections. The number of firewall instances determines how many cores are dedicated to CoreXL. The cpconfig command allows the administrator to configure various settings on the Security Gateway, including the number of firewall instances. After changing this setting, a reboot is required for the changes to take effect. The other commands are either incorrect or do not require a reboot.

QUESTION 142
Fill in the blank: Identity Awareness AD-Query is using the Microsoft _____ API to learn users from AD.

A. WMI
B. Eventvwr
C. XML
D. Services.msc

Correct Answer: A
Section:
Explanation:
Identity Awareness AD-Query is using the MicrosoftWMIAPI to learn users from AD. WMI stands for Windows Management Instrumentation, and it is an API that allows remote management and monitoring of Windows systems. Identity Awareness AD-Query is a feature that enables the Security Gateway to query Active Directory servers for user and computer information, such as login events, group membership, and IP addresses. By using the WMI API, Identity Awareness AD-Query can receive real-time notifications from Active Directory servers without installing any agents or scripts on them.

QUESTION 143
Which is not a blade option when configuring SmartEvent?

A. Correlation Unit
B. SmartEvent Unit
C. SmartEvent Server
D. Log Server

Correct Answer: B
Section:
Explanation:
SmartEvent Unitis not a blade option when configuring SmartEvent. SmartEvent is a unified security event management solution that provides visibility, analysis, and reporting of security events across multiple Check Point products. SmartEvent consists of three main components: SmartEvent Server, Correlation Unit, and Log Server. SmartEvent Server is responsible for storing and displaying security events in SmartConsole and SmartEventWeb. Correlation Unit is responsible for collecting and correlating logs from various sources and generating security events based on predefined or custom scenarios. Log Server is responsible for receiving and indexing logs from Security Gateways and other Check Point modules. SmartEvent Unit is not a valid component or blade of SmartEvent.

QUESTION 144
In which formats can Threat Emulation forensics reports be viewed in?

A. TXT, XML and CSV
B. PDF and TXT
C. PDF, HTML, and XML
D. PDF and HTML

Correct Answer: C
Section:
Explanation:
The formats in which Threat Emulation forensics reports can be viewed in arePDF, HTML, and XML. Threat Emulation is a feature that detects and prevents zero-day attacks by emulating files in a sandbox environment and analyzing their behavior. Threat Emulation generates forensics reports that provide detailed information about the emulated files, such as verdict, severity, activity summary, screenshots, network activity, registry activity, file

activity, and process activity. These reports can be viewed in PDF, HTML, or XML formats from SmartConsole or SmartView.

QUESTION 145
In ClusterXL Load Sharing Multicast Mode:

A. only the primary member received packets sent to the cluster IP address
B. only the secondary member receives packets sent to the cluster IP address
C. packets sent to the cluster IP address are distributed equally between all members of the cluster
D. every member of the cluster received all of the packets sent to the cluster IP address

Correct Answer: D
Section:
Explanation:
In ClusterXL Load Sharing Multicast Mode,every member of the cluster receives all of the packets sent to the cluster IP address. This mode uses multicast MAC addresses to distribute packets to all cluster members. Each member decides whether to accept or reject the packet based on a load balancing algorithm.This mode provides better performance and scalability than Unicast mode, but requires a switch that supports multicast MAC addresses.

QUESTION 146
What kind of information would you expect to see using the sim affinity command?

A. The VMACs used in a Security Gateway cluster
B. The involved firewall kernel modules in inbound and outbound packet chain
C. Overview over SecureXL templated connections
D. Network interfaces and core distribution used for CoreXL

Correct Answer: D
Section:
Explanation:
The kind of information that you would expect to see using thesim affinitycommand isnetwork interfaces and core distribution used for CoreXL. Sim affinity is a command that allows administrators to view and modify the CPU core affinity of network interfaces and SecureXL instances. CoreXL is a technology that improves the performance of the Security Gateway by using multiple cores to handle concurrent connections.The sim affinity command can show which network interfaces and SecureXL instances are bound to which CPU cores, and allow administrators to change the affinity settings.

QUESTION 147
What cloud-based SandBlast Mobile application is used to register new devices and users?

A. Check Point Protect Application
B. Management Dashboard
C. Behavior Risk Engine
D. Check Point Gateway

Correct Answer: D
Section:
Explanation:
The cloud-based SandBlast Mobile application that is used to register new devices and users isCheck Point Gateway. Check Point Gateway is a web portal that allows administrators to enroll devices and users into the SandBlast Mobile service, which is a cloud-based solution that protects mobile devices from advanced threats. Check Point Gateway also allows administrators to configure policies, monitor device status, and generate reports for SandBlast Mobile.

QUESTION 148

What is the responsibility of SOLR process on R81.20 management server?

A. Validating all data before it's written into the database
B. It generates indexes of data written to the database
C. Communication between SmartConsole applications and the Security Management Server
D. Writing all information into the database

Correct Answer: B
Section:
Explanation:
The responsibility of SOLR process on R81.20 management server isto generate indexes of data written to the database. SOLR is an open source search platform that provides fast and scalable indexing and querying capabilities. SOLR is used by the R81.20 management server to index data such as logs, objects, policies, tasks, and events, and to enable quick and efficient searches on this data by SmartConsole and SmartView applications.

QUESTION 149
In the Firewall chain mode FFF refers to:

A. Stateful Packets
B. No Match
C. All Packets
D. Stateless Packets

Correct Answer: C
Section:
Explanation:
In the Firewall chain mode FFF refers toall packets. Firewall chain mode is a feature that allows administrators to define how packets are processed by different firewall kernel modules in inbound and outbound directions. FFF is one of the predefined chain modes that applies all firewall kernel modules (Firewall, VPN, IPS, etc.) to all packets, regardless of their state or connection. This mode provides maximum security, but also consumes more CPU resources.

QUESTION 150
Which file gives you a list of all security servers in use, including port number?

A. $FWDIR/conf/conf.conf
B. $FWDIR/conf/servers.conf
C. $FWDIR/conf/fwauthd.conf
D. $FWDIR/conf/serversd.conf

Correct Answer: C
Section:
Explanation:
The file that gives you a list of all security servers in use, including port number, is$FWDIR/conf/fwauthd.conf. Security servers are processes that handle application-level protocols such as HTTP, FTP, SMTP, etc., and perform security checks on them. Fwauthd.conf is a configuration file that defines which security servers are enabled, which ports they listen on, and which inspection points they are attached to.

QUESTION 151
Which of the following commands shows the status of processes?

A. cpwd_admin -l
B. cpwd -l

C. cpwd admin_list
D. cpwd_admin list

Correct Answer: D
Section:
Explanation:
The command that shows the status of processes iscpwd_admin list. Cpwd_admin is a command that allows administrators to manage processes that are registered with the Check Point WatchDog (CPWD) daemon. CPWD is a daemon that monitors the health of critical processes on the Security Gateway or Management Server, and restarts them if they fail or stop responding. Cpwd_admin list shows the process name, PID, status, start time, monitor status, and number of restarts for each process registered with CPWD.

QUESTION 152
What is the valid range for VRID value in VRRP configuration?

A. 1 - 254
B. 1 - 255
C. 0 - 254
D. 0 - 255

Correct Answer: B
Section:
Explanation:
The valid range for VRID value in VRRP configuration is1 - 255. VRID stands for Virtual Router ID, and it is a number that identifies a virtual router in a VRRP cluster. A VRRP cluster consists of one or more routers that share a virtual IP address and provide redundancy and load balancing for network traffic. Each router in the cluster must have a unique VRID value, and the VRID value must match the VRID value configured on the interface that connects to the VRRP cluster.The VRID value can be any number from 1 to 255, inclusive.

QUESTION 153
What is true of the API server on R81.20?

A. By default the API-server is activated and does not have hardware requirements.
B. By default the API-server is not active and should be activated from the WebUI.
C. By default the API server is active on management and stand-alone servers with 16GB of RAM (or more).
D. By default, the API server is active on management servers with 4 GB of RAM (or more) and on stand-alone servers with 8GB of RAM (or more).

Correct Answer: D
Section:
Explanation:
The true statement about the API server on R81.20 is: By default, the API server is active on management servers with 4 GB of RAM (or more) and on stand-alone servers with 8GB of RAM (or more). The API server is a web service that allows external applications to interact with the Check Point management server using standard methods such as HTTP(S) requests and JSON objects. The API server is enabled by default on R81.20 management servers that have at least 4 GB of RAM, and on stand-alone servers that have at least 8 GB of RAM.The API server can also be manually enabled or disabled from the WebUI or the CLI.

QUESTION 154
To ensure that VMAC mode is enabled, which CLI command should you run on all cluster members?

A. fw ctl set int fwha vmac global param enabled
B. fw ctl get int 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

Correct Answer: D
Section:
Explanation:
To ensure that VMAC mode is enabled, the CLI command that should be run on all cluster members isfw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1. VMAC mode is a feature that allows ClusterXL to use virtual MAC addresses for cluster interfaces, instead of physical MAC addresses. This improves the failover performance and compatibility of ClusterXL with switches and routers. To check if VMAC mode is enabled, the command fw ctl get int fwha_vmac_global_param_enabled can be used, which returns 1 if VMAC mode is enabled, and 0 if VMAC mode is disabled.

QUESTION 155
For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

A. 20 minutes
B. 15 minutes
C. Admin account cannot be unlocked automatically
D. 30 minutes at least

Correct Answer: D
Section:
Explanation:
For best practices, the recommended time for automatic unlocking of locked admin accounts is30 minutes at least. Admin accounts can be locked due to failed login attempts, password expiration, or manual locking by another admin. To prevent unauthorized access or brute force attacks, locked admin accounts should not be unlocked automatically too soon. The recommended minimum time for automatic unlocking is 30 minutes, which can be configured from the SmartConsole under Manage > Permissions and Administrators > Advanced > Unlock locked administrators after.

QUESTION 156
Which is NOT a SmartEvent component?

A. SmartEvent Server
B. Correlation Unit
C. Log Consolidator
D. Log Server

Correct Answer: C
Section:
Explanation:
Log Consolidatoris NOT a SmartEvent component. SmartEvent is a unified security event management solution that provides visibility, analysis, and reporting of security events across multiple Check Point products. SmartEvent consists of three main components: SmartEvent Server, Correlation Unit, and Log Server. SmartEvent Server is responsible for storing and displaying security events in SmartConsole and SmartEventWeb. Correlation Unit is responsible for collecting and correlating logs from various sources and generating security events based on predefined or custom scenarios. Log Server is responsible for receiving and indexing logs from Security Gateways and other Check Point modules. Log Consolidator is not a valid component or blade of SmartEvent.

QUESTION 157
Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all the following except:

A. Create new dashboards to manage 3rd party task
B. Create products that use and enhance 3rd party solutions
C. Execute automated scripts to perform common tasks
D. Create products that use and enhance the Check Point Solution

Correct Answer: A
Section:

Explanation:
Check Point APIs let system administrators and developers make changes to the security policy with CLI tools and web-services. You can use an API to:
* Use an automated script to perform common tasks
* Integrate Check Point products with 3rd party solutions
* Create products that use and enhance the Check Point solution

QUESTION 158
When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:

A. All UDP packets
B. All IPv6 Traffic
C. All packets that match a rule whose source or destination is the Outside Corporate Network
D. CIFS packets

Correct Answer: D
Section:
Explanation:
When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:CIFS packets. SecureXL is a technology that accelerates network traffic processing by offloading intensive operations from the Firewall kernel to a dedicated SecureXL device. However, some packets cannot be accelerated by SecureXL due to various reasons, such as unsupported features, security policy settings, or protocol limitations. One example of packets that cannot be accelerated by SecureXL are CIFS packets, which are used for file sharing and access over SMB protocol. CIFS packets are not accelerated by SecureXL because they require stateful inspection by the Firewall kernel.

QUESTION 159
On what port does the CPM process run?

A. TCP 857
B. TCP 18192
C. TCP 900
D. TCP 19009

Correct Answer: D
Section:
Explanation:
The port that the CPM process runs on isTCP 19009. CPM stands for Check Point Management, and it is the main process that runs on the Security Management Server and interacts with SmartConsole clients. CPM is responsible for managing policies, objects, logs, tasks, and other management functions. CPM listens on TCP port 19009 for incoming connections from SmartConsole clients.The other ports are either used by other processes or not related to CPM.

QUESTION 160
What is the SandBlast Agent designed to do?

A. Performs OS-level sandboxing for SandBlast Cloud architecture
B. Ensure the Check Point SandBlast services is running on the end user's system
C. If malware enters an end user's system, the SandBlast Agent prevents the malware from spreading with the network
D. Clean up email sent with malicious attachments

Correct Answer: C
Section:
Explanation:

The SandBlast Agent is designed toprevent malware from spreading within the networkif it enters an end user's system. SandBlast Agent is a lightweight endpoint security solution that protects devices from advanced threats such as ransomware, phishing, zero-day attacks, and data exfiltration. SandBlast Agent uses various technologies such as behavioral analysis, anti-exploitation, anti-ransomware, threat emulation, threat extraction, and forensics to detect and block malware before it can harm the device or the network.The other options are either not the main purpose or not the functionality of SandBlast Agent.

QUESTION 161
What is correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution?

A. Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure.
B. Security Gateway failover as well as Security Management Server failover is a manual procedure.
C. Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.
D. Security Gateway failover as well as Security Management Server failover is an automatic procedure.

Correct Answer: A
Section:
Explanation:
The correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution is:Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure. Security Gateway failover is a feature that allows a cluster of Security Gateways to provide high availability and load balancing for network traffic. If one Security Gateway fails or becomes unreachable, another Security Gateway in the cluster automatically takes over its role and handles the traffic without interrupting the service. Security Management Server failover is a feature that allows a backup Security Management Server to take over the role of the primary Security Management Server in case of failure or disaster. However, this feature requires manual intervention to activate the backup server and restore the database from a backup file.

QUESTION 162
SandBlast agent extends 0 day prevention to what part of the network?

A. Web Browsers and user devices
B. DMZ server
C. Cloud
D. Email servers

Correct Answer: A
Section:
Explanation:
SandBlast agent extends zero-day prevention toweb browsers and user devices. Zero-day prevention is a capability that protects devices from unknown and emerging threats that exploit vulnerabilities that have not been patched or disclosed. SandBlast Agent provides zero-day prevention by using various technologies such as threat emulation, threat extraction, anti-exploitation, anti-ransomware, and behavioral analysis. SandBlast Agent protects web browsers and user devices from malicious downloads, phishing links, drive-by downloads, browser exploits, malicious scripts, and more.

QUESTION 163
What command would show the API server status?

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

Correct Answer: C
Section:
Explanation:
The command that would show the API server status isapi status. API stands for Application Programming Interface, and it is a web service that allows external applications to interact with the Check Point management server

using standard methods such as HTTP(S) requests and JSON objects. API status is a command that shows the current status of the API server, such as whether it is enabled or disabled, running or stopped, listening on which port, using which certificate, etc. The other commands are either invalid or perform different functions.

QUESTION 164
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

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

Correct Answer: C
Section:
Explanation:
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. The option that can be added to each Log, Detailed Log and Extended Log isAccounting/Suppression. Accounting/Suppression is a feature that allows administrators to control how often logs are generated for certain rules or connections. Accounting means that logs are generated periodically based on a specified interval or volume. Suppression means that logs are generated only for the first and last packet of a connection or session. Accounting/Suppression can be added to any tracking option to reduce the number of logs and save disk space.

QUESTION 165
Which file contains the host address to be published, the MAC address that needs to be associated with the IP Address, and the unique IP of the interface that responds to ARP request?

A. /opt/CPshrd-R81/conf/local.arp
B. /var/opt/CPshrd-R81/conf/local.arp
C. $CPDIR/conf/local.arp
D. $FWDIR/conf/local.arp

Correct Answer: D
Section:
Explanation:
The file that contains the host address to be published, the MAC address that needs to be associated with the IP address, and the unique IP of the interface that responds to ARP request is$FWDIR/conf/local.arp. Local.arp is a configuration file that defines static ARP entries for hosts behind NAT devices. This file allows the Security Gateway to respond to ARP requests for NATed hosts with the correct MAC address, and to publish the NATed IP address instead of the real IP address.The other files are either not related or not valid.

QUESTION 166
With SecureXL enabled, accelerated packets will pass through the following:

A. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
B. Network Interface Card, Check Point Firewall Kernal, and the Acceleration Device
C. Network Interface Card and the Acceleration Device
D. Network Interface Card, OSI Network Layer, and the Acceleration Device

Correct Answer: C
Section:
Explanation:
With SecureXL enabled, accelerated packets will pass through the following:Network Interface Card and the Acceleration Device. SecureXL is a technology that accelerates network traffic processing by offloading intensive operations from the Firewall kernel to a dedicated SecureXL device. Accelerated packets are packets that match certain criteria and can be handled by SecureXL without involving the Firewall kernel. These packets bypass the OSI Network Layer, OS IP Stack, and Check Point Firewall Kernel, and are processed directly by the Network Interface Card and the Acceleration Device.The other options are either incorrect or describe non-accelerated packets.

QUESTION 167
Which command would you use to set the network interfaces' affinity in Manual mode?

A. sim affinity -m
B. sim affinity -l
C. sim affinity -a
D. sim affinity -s

Correct Answer: D
Section:
Explanation:
The command that would be used to set the network interfaces' affinity in Manual mode issim affinity -s. Sim affinity is a command that allows administrators to view and modify the CPU core affinity of network interfaces and SecureXL instances. Core affinity is a feature that binds network interfaces and SecureXL instances to specific CPU cores, which improves the performance and load balancing of the Security Gateway. Sim affinity -s sets the network interfaces' affinity in Manual mode, which means that administrators can manually assign network interfaces to CPU cores. The other options are either invalid or perform different functions.

QUESTION 168
You notice that your firewall is under a DDoS attack and would like to enable the Penalty Box feature, which command you use?

A. sim erdos --e 1
B. sim erdos -- m 1
C. sim erdos --v 1
D. sim erdos --x 1

Correct Answer: A
Section:
Explanation:
The command that would be used to enable the Penalty Box feature issim erdos -e 1. Penalty Box is a feature that protects the Security Gateway from DDoS attacks by dropping packets from sources that send excessive traffic. Sim erdos is a command that allows administrators to configure and manage the Penalty Box feature. Sim erdos -e 1 enables the Penalty Box feature on the Security Gateway. The other options are either invalid or perform different functions.

QUESTION 169
Which of the following is NOT an option to calculate the traffic direction?

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

Correct Answer: D
Section:
Explanation:
The option that is NOT an option to calculate the traffic direction isOutgoing. Traffic direction is a parameter that determines how traffic is classified as internal or external based on its source and destination. Traffic direction can be calculated using three options: Incoming, Internal, or External. Incoming means that traffic is classified as internal if its destination is one of the Security Gateway's interfaces, and external otherwise. Internal means that traffic is classified as internal if its source or destination belongs to one of the internal networks defined in the topology, and external otherwise. External means that traffic is classified as internal if both its source and destination belong to one of the internal networks defined in the topology, and external otherwise. Outgoing is not a valid option to calculate traffic direction.

QUESTION 170
What command lists all interfaces using Multi-Queue?

A. cpmq get
B. show interface all
C. cpmq set
D. show multiqueue all

Correct Answer: A
Section:
Explanation:
The command that lists all interfaces using Multi-Queue iscpmq get. Multi-Queue is a feature that allows network interfaces to use multiple transmit and receive queues, which improves the performance and scalability of the Security Gateway by distributing the network load among several CPU cores. Cpmq is a command that allows administrators to configure and manage Multi-Queue settings on network interfaces. Cpmq get lists all interfaces using Multi-Queue and shows their queue count and core distribution.

QUESTION 171
When deploying SandBlast, how would a Threat Emulation appliance benefit from the integration of ThreatCloud?

A. ThreatCloud is a database-related application which is located on-premise to preserve privacy of company-related data
B. ThreatCloud is a collaboration platform for all the CheckPoint customers to form a virtual cloud consisting of a combination of all on-premise private cloud environments
C. ThreatCloud is a collaboration platform for Check Point customers to benefit from VMWare ESXi infrastructure which supports the Threat Emulation Appliances as virtual machines in the EMC Cloud
D. ThreatCloud is a collaboration platform for all the Check Point customers to share information about malicious and benign files that all of the customers can benefit from as it makes emulation of known files unnecessary

Correct Answer: D
Section:
Explanation:
ThreatCloud is a collaboration platform for all the Check Point customers to share information about malicious and benign files that all of the customers can benefit from as it makes emulation of known files unnecessary. ThreatCloud is a cloud-based service that collects and analyzes threat intelligence from multiple sources, such as Check Point products, third-party vendors, open sources, and customers. ThreatCloud provides real-time updates and feeds to Check Point products, such as SandBlast, which is a solution that detects and prevents zero-day attacks by emulating files in a sandbox environment. By integrating with ThreatCloud, a Threat Emulation appliance can benefit from the shared information about malicious and benign files, and avoid emulating files that are already known to be safe or harmful. This can improve the performance and efficiency of the Threat Emulation appliance.The other options are either incorrect or not relevant to ThreatCloud or Threat Emulation.

QUESTION 172
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

A. Dropped without sending a negative acknowledgment
B. Dropped without logs and without sending a negative acknowledgment
C. Dropped with negative acknowledgment
D. Dropped with logs and without sending a negative acknowledgment

Correct Answer: D
Section:
Explanation:
For packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are dropped with logs and without sending a negative acknowledgment. Firewall Kernel Inspection is the process of applying security policies and rules to network traffic by the Firewall kernel module. If a packet does not match any rule or matches a rule with an action of Drop or Reject, the packet is dropped by the Firewall kernel module. The difference between Drop and Reject is that Drop silently discards the packet without informing the sender, while Reject discards the packet and sends a negative acknowledgment (such as an ICMP message) to the sender. However, both Drop and Reject actions generate logs that record the details of the dropped packets, such as source, destination, protocol, port, rule number, etc. The other options are either incorrect or describe different scenarios.

QUESTION 173

Vanessa is firewall administrator in her company. Her company is using Check Point firewall on a central and several remote locations which are managed centrally by R77.30 Security Management Server. On central location is installed R77.30 Gateway on Open server. Remote locations are using Check Point UTM-1570 series appliances with R75.30 and some of them are using a UTM-1-Edge-X or Edge-W with latest available firmware. She is in process of migrating to R81.
What can cause Vanessa unnecessary problems, if she didn't check all requirements for migration to R81?

A. Missing an installed R77.20 Add-on on Security Management Server
B. Unsupported firmware on UTM-1 Edge-W appliance
C. Unsupported version on UTM-1 570 series appliance
D. Unsupported appliances on remote locations

Correct Answer: A
Section:
Explanation:
What can cause Vanessa unnecessary problems, if she didn't check all requirements for migration to R81, is missing an installed R77.20 Add-on on Security Management Server. R77.20 Add-on is a package that adds new features and enhancements to R77 Security Management Server, such as support for new appliances, Gaia OS features, VPN features, etc. One of the requirements for migrating to R81 from R77 Security Management Server is to have R77.20 Add-on installed on the server. If Vanessa did not check this requirement and tried to migrate without R77.20 Add-on, she would encounter errors and failures during the migration process. The other options are either not relevant or not problematic for migration to R81.

QUESTION 174
Please choose the path to monitor the compliance status of the Check Point R81.20 based management.

A. Gateways & Servers --> Compliance View
B. Compliance blade not available under R81.20
C. Logs & Monitor --> New Tab --> Open compliance View
D. Security & Policies --> New Tab --> Compliance View

Correct Answer: C
Section:
Explanation:
The path to monitor the compliance status of the Check Point R81.20 based management is Logs & Monitor > New Tab > Open compliance View. Compliance View is a feature that allows administrators to monitor and assess the compliance level of their Check Point products and security policies based on best practices and industry standards. Compliance View provides a dashboard that shows the overall compliance status, compliance score, compliance trends, compliance issues, compliance reports, and compliance blades for different security aspects, such as data protection, threat prevention, identity awareness, etc. To access Compliance View in R81.20 SmartConsole, administrators need to go to Logs & Monitor > New Tab > Open compliance View. The other options are either incorrect or not available in R81.20.

QUESTION 175
Fill in the blank: The R81 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows then as prioritized security events.

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

Correct Answer: B
Section:
Explanation:
The R81 SmartConsole, SmartEvent GUI client, and SmartView Web Application consolidate billions of logs and show them as prioritized security events. The SmartView Web Application is a web-based interface that allows you to access the SmartEvent Server from any browser.You can use the SmartView Web Application to view and analyze security events, generate reports, and configure SmartEvent settings12.

QUESTION 176
Office mode means that:

A. SecurID client assigns a routable MAC address. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
B. Users authenticate with an Internet browser and use secure HTTPS connection.
C. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
D. Allows a security gateway to assign a remote client an IP address. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Correct Answer: D
Section:
Explanation:
Office mode is a feature that allows a security gateway to assign a remote client an IP address from a network that is protected by the security gateway. This way, the remote client can access resources on the internal network as if it was physically connected to it. The IP address is assigned to the remote client after the user authenticates for a tunnel, and it is routable, meaning that it can be reached by other hosts on the network.Office mode is useful for scenarios where the remote client needs to use applications that rely on IP addresses, such as VoIP or file sharing12.

QUESTION 177
When attempting to start a VPN tunnel, in the logs the error ''no proposal chosen'' is seen numerous times. No other VPN-related entries are present.
Which phase of the VPN negotiations has failed?

A. IKE Phase 1
B. IPSEC Phase 2
C. IPSEC Phase 1
D. IKE Phase 2

Correct Answer: A
Section:
Explanation:
The error ''no proposal chosen'' indicates that the VPN gateway did not find a matching proposal for the IKE Phase 1 negotiation. This phase is responsible for establishing a secure channel between the VPN peers, using a pre-shared secret or a certificate. The proposal consists of parameters such as encryption algorithm, hash algorithm, Diffie-Hellman group, and lifetime.If the VPN gateway does not receive a proposal that matches its own configuration, it will reject the connection attempt and log the error ''no proposal chosen''1.
To troubleshoot this issue, one should verify that the VPN peers have the same IKE Phase 1 settings, such as:
The same pre-shared secret or certificate
The same encryption algorithm (e.g., AES-256)
The same hash algorithm (e.g., SHA-256)
The same Diffie-Hellman group (e.g., Group 14)
The same lifetime (e.g., 86400 seconds)
One can use the commandvpn tuon the VPN gateway to view the current IKE Phase 1 settings and compare them with the other peer.Alternatively, one can use the SmartConsole to check the VPN community properties and the gateway object properties for the IKE Phase 1 settings2.

QUESTION 178
Which of the following Windows Security Events will not map a username to an IP address in Identity Awareness?

A. Kerberos Ticket Renewed
B. Kerberos Ticket Requested
C. Account Logon
D. Kerberos Ticket Timed Out

Correct Answer: D

Section:
Explanation:
Identity Awareness maps usernames to IP addresses by collecting Windows Security Events from Active Directory Domain Controllers. These events include Account Logon, Kerberos Ticket Requested, and Kerberos Ticket Renewed. These events indicate that a user has successfully authenticated to the domain and obtained a Kerberos ticket for accessing network resources. Identity Awareness can use these events to associate the username with the source IP address of the authentication request.
However, Kerberos Ticket Timed Out is not a Windows Security Event that Identity Awareness can use to map usernames to IP addresses. This event indicates that a user's Kerberos ticket has expired and needs to be renewed. This event does not contain the source IP address of the user, only the username and the ticket information. Therefore, Identity Awareness cannot use this event to map a username to an IP address.
1, Training & Certification | Check Point Software, section ''Security Expert R81.20 (CCSE) Core Training''
2, Certified Security Expert (CCSE) R81.20 Course Overview, page 1
3, Check Point Certified Security Expert R81, page 5
5, Identity Awareness Administration Guide R81, section ''How Identity Awareness Collects Identities''

QUESTION 179
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____ .

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

Correct Answer: B
Section:
Explanation:
Browser-based Authentication is a method of acquiring identities from unidentified users by sending them to a web page where they can log in and authenticate.Browser-based Authentication uses two techniques to acquire identities: Captive Portal and Transparent Kerberos Authentication1.
Captive Portal is a simple method that attempts authentication through a web interface before granting a user access to Intranet resources. When a user tries to access a protected resource, they are redirected to a web page where they have to enter their credentials. The credentials are verified by the Identity Awareness Security Gateway or an external authentication server.If the authentication is successful, the user's identity is associated with their IP address and they are allowed to access the resource12.
Transparent Kerberos Authentication is a more seamless method that leverages the existing Kerberos infrastructure in the network. When a user tries to access a protected resource, the Identity Awareness Security Gateway intercepts the Kerberos ticket request and extracts the user's identity from it. The user's identity is then associated with their IP address and they are allowed to access the resource without any additional prompts.This method requires that the Identity Awareness Security Gateway is configured as a trusted proxy in the Active Directory domain12.
Therefore, the correct answer is B) Browser-based Authentication sends users to a web page to acquire identities using Captive Portal and Transparent Kerberos Authentication.
1, THE IMPORTANCE OF ACCESS ROLES - Check Point Software, page 2
2, Browser-based Authentication Check Point - Bing
3, How to Configure Client Authentication - Check Point Software, page 1
4, Identity Sources - Check Point Software
5, Configuring Browser-Based Authentication - Check Point Software
6, Two Factor Authentication - Check Point Software

QUESTION 180
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

Correct Answer: B
Section:

Explanation:
The software blade package that uses CPU-level and OS-level sandboxing in order to detect and block malware is the Next Generation Threat Emulation.This package is part of the Check Point SandBlast Zero-Day Protection solution, which protects organizations against unknown malware, zero-day threats and targeted attacks, and prevents infections from undiscovered exploits1.
CPU-level and OS-level sandboxing are two techniques that Check Point uses to analyze files and objects for malicious behavior. CPU-level inspection is a unique technology that detects malware at the pre-infection stage by examining the CPU instructions that the file executes.This allows Check Point to identify and block malware that tries to evade detection by using obfuscation, encryption, or polymorphism12.
OS-level sandboxing is a complementary technology that runs files and objects in a virtualized environment and monitors their behavior for malicious indicators.This allows Check Point to detect and block malware that tries to exploit vulnerabilities in the operating system or applications, or that performs malicious actions such as downloading additional payloads, modifying system settings, or communicating with command and control servers12.
Therefore, the correct answer is B) The Next Generation Threat Emulation software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.
1, Understanding SandBlast - Check Point Software Technologies
2, HOW TO CHOOSE YOUR NEXT SANDBOXING SOLUTION - Check Point Software
3, CHECK POINT + SERVICENOW
4, Check Point Quantum Edge Datasheet

QUESTION 181
Which tool is used to enable ClusterXL?

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

Correct Answer: B
Section:
Explanation:
The tool that is used to enable ClusterXL is cpconfig.ClusterXL is a software-based Load Sharing and High Availability solution that distributes network traffic between clusters of redundant Security Gateways1.ClusterXL can be enabled on Check Point Security Gateways running on Gaia OS, SecurePlatform OS, IPSO OS, or X-Series XOS2.
To enable ClusterXL, the administrator must run the cpconfig command on each cluster member and select the option to enable ClusterXL. This will prompt the administrator to choose the ClusterXL mode (High Availability or Load Sharing) and the Cluster Control Protocol (CCP) mode (Broadcast or Multicast).After enabling ClusterXL, the administrator must reboot the cluster members for the changes to take effect34.
Therefore, the correct answer is B) The tool that is used to enable ClusterXL is cpconfig.
1, Introduction to ClusterXL - Check Point Software
2, ClusterXL Requirements and Compatibility - Check Point Software
3, Configuring ClusterXL - Check Point Software
4, How to configure ClusterXL - Check Point Software Technologies

QUESTION 182
How many policy layers do Access Control policy support?

A. 2
B. 4
C. 1
D. 3

Correct Answer: A
Section:
Explanation:
The Access Control policy supports two policy layers. These are the Network layer and the Application & URL Filtering layer. The Network layer contains rules that control the network traffic based on the source, destination, service, and action.The Application & URL Filtering layer contains rules that control the application and web access based on the application, site category, and user identity12.
The Access Control policy can also use inline layers, which are sub-policies that are embedded within a rule.Inline layers allow more granular control over specific traffic or scenarios, such as VPN, Mobile Access, or different

user groups13.However, inline layers are not considered as separate policy layers, but rather as extensions of the parent rule4.
Therefore, the correct answer is A. The Access Control policy supports two policy layers.
1, Policy Layers in R80.x - Check Point CheckMates
2, Access Control policies, layers, and rules | Check Point Firewall ...
3, Chapter 8: Introduction to Policies, Layers, and Rules - Check Point ...
4, Creating an Access Control Policy - Check Point Software

QUESTION 183
One of major features in R81 SmartConsole is concurrent administration.
Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

A. A lock icon shows that a rule or an object is locked and will be available.
B. AdminA and AdminB are editing the same rule at the same time.
C. A lock icon next to a rule informs that any Administrator is working on this particular rule.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Correct Answer: B
Section:
Explanation:
One of the major features in R81 SmartConsole is concurrent administration. This feature allows multiple administrators to work on the same Security Policy simultaneously, without blocking each other or creating conflicts.Concurrent administration improves the efficiency and productivity of security management operations1.
However, not all of the options given are possible considering that AdminA, AdminB and AdminC are editing the same Security Policy. The correct answer is B) AdminA and AdminB are editing the same rule at the same time. This is not possible because concurrent administration uses a locking mechanism to prevent multiple administrators from modifying the same rule or object at the same time. When an administrator clicks on a rule or an object, it becomes locked and a lock icon appears next to it.The lock icon shows the name of the administrator who is working on that rule or object, and prevents other administrators from editing it until it is unlocked12.
Therefore, the other options are possible considering that AdminA, AdminB and AdminC are editing the same Security Policy.Option A is possible because a lock icon shows that a rule or an object is locked and will be available when the administrator who locked it finishes working on it or logs out of SmartConsole12.Option C is possible because a lock icon next to a rule informs that any administrator is working on this particular rule, and hovering over the lock icon will show the name of that administrator12.Option D is possible because AdminA, AdminB and AdminC are editing three different rules at the same time, which does not create any conflicts or blockages12.

QUESTION 184
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. 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
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0set static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
D. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

Correct Answer: A
Section:
Explanation:
To set the IP address and default gateway of the Management interface on a Check Point appliance, you can use the following commands:
set interface Mgmt ipv4-address 192.168.80.200 mask-length 24- This command sets the IPv4 address of the Management interface to 192.168.80.200 and the subnet mask to 255.255.255.0 (24 bits).
set static-route default nexthop gateway address 192.168.80.1 on- This command sets the default gateway to 192.168.80.1 and enables the static route.
save config- This command saves the configuration changes to the appliance.
These commands are documented in theCheck Point appliance initial installationguide, which you can find in the web search results.
The other options are incorrect because they use invalid syntax or parameters for the commands. For example, option B usesadd static-routeinstead ofset static-route, option C uses0.0.0.0.instead of0.0.0.0, and option D usesadd static-route defaultinstead ofset static-route default.

QUESTION 185
Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward.
What will happen to the changes already made?

A. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.
B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
C. Tom's changes will be lost since he lost connectivity and he will have to start again.
D. Tom will have to reboot his SmartConsole computer, clear to cache, and restore changes.

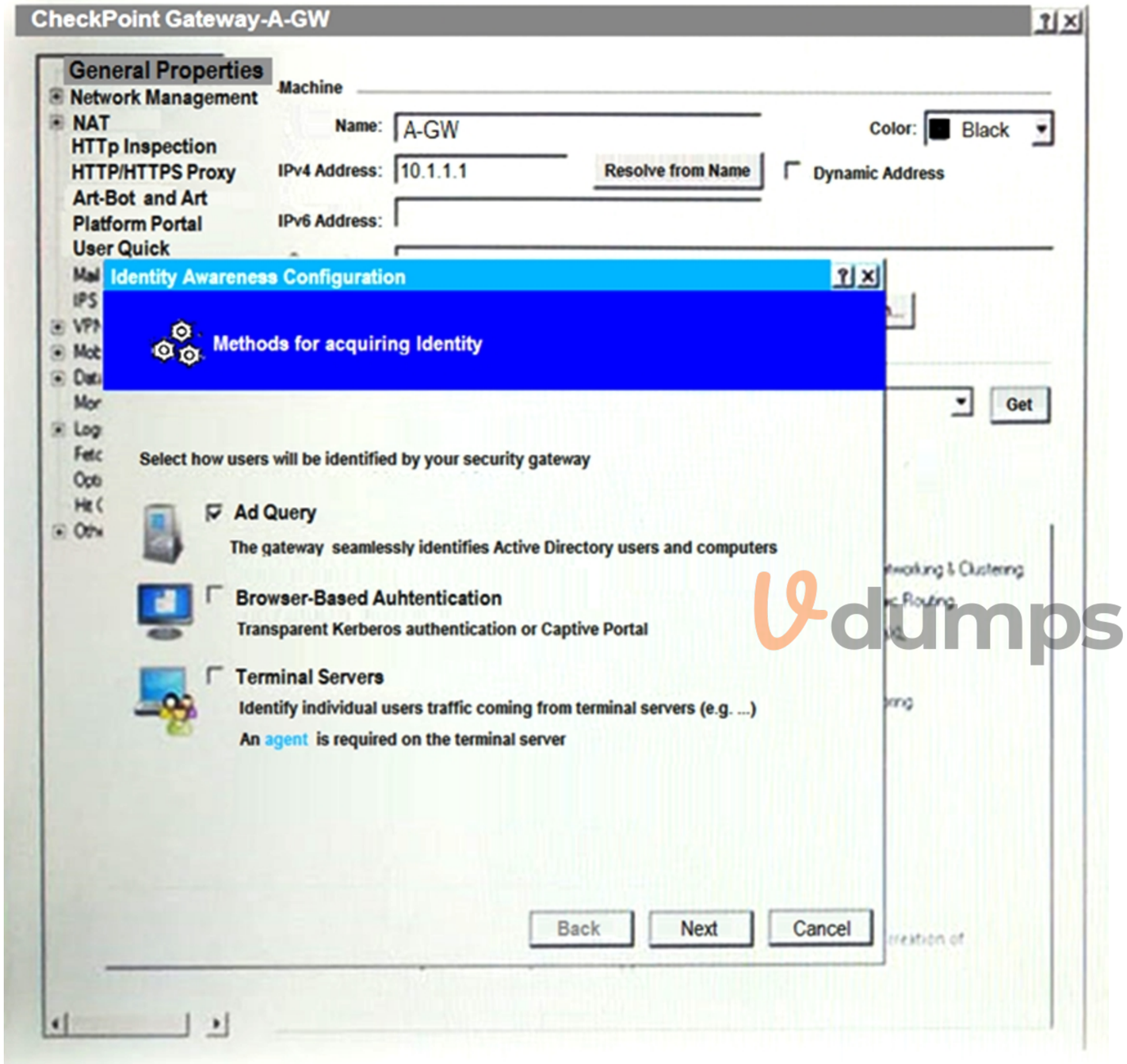
Correct Answer: A
Section:
Explanation:
Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.
This is because SmartConsole has a feature called Concurrent Administration, which allows multiple administrators to work on the same Security Policy simultaneously, without blocking each other or creating conflicts.
Concurrent Administration uses a locking mechanism to prevent multiple administrators from modifying the same rule or object at the same time. When an administrator clicks on a rule or an object, it becomes locked and a lock icon appears next to it.The lock icon shows the name of the administrator who is working on that rule or object, and prevents other administrators from editing it until it is unlocked12.
Concurrent Administration also has a feature called Session Persistence, which preserves the changes made by an administrator in case of a network failure or a SmartConsole crash. When an administrator reconnects to the Management Server after a network failure or a SmartConsole crash, they can resume their work from where they left off, without losing any changes.The changes are stored locally on the administrator's machine until they are published to the Management Server13.
Therefore, if Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity, his changes will not be lost. They will be stored locally on his machine and he can resume his work when he reconnects to the Management Server.

QUESTION 186
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

Correct Answer: C
Section:
Explanation:
The key C is used to save the current CPView page in a filename format cpview_''cpview process ID''.cap'number of captures'. This is a feature of CPView that allows the user to capture the current page for later analysis or troubleshooting. The file is saved in the /var/log directory on the Security Gateway.
Reference:Check Point Resource Library, page 3.
Topic 4, Exam Pool D

QUESTION 187
On the following picture an administrator configures Identity Awareness:



After clicking ''Next'' the above configuration is supported by:

A. Kerberos SSO which will be working for Active Directory integration
B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user.
C. Obligatory usage of Captive Portal.
D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication.

Correct Answer: B
Section:
Explanation:
After clicking ''Next'', the above configuration is supported by Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user. This is a feature of Identity Awareness that allows the Security Gateway to identify users and machines on the network and enforce security policies based on their identity.The administrator can configure Identity Awareness to use various methods for acquiring identity, including Active Directory integration, browser-based authentication, terminal servers, and transparent authentication1.
Reference:Check Point Resource Library, page 3.

QUESTION 188
Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

A. assign privileges to users.
B. edit the home directory of the user.
C. add users to your Gaia system.
D. assign user rights to their home directory in the Security Management Server.

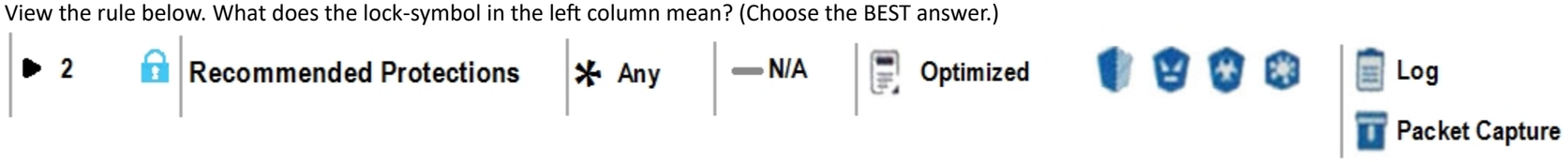
Correct Answer: D
Section:
Explanation:
The WebUI can be used to manage user accounts and assign privileges to users. It can also add users to your Gaia system and edit the home directory of the user.However, it cannot assign user rights to their home directory in the Security Management Server1.
Reference:Check Point Resource Library, page 3.

QUESTION 189
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

Correct Answer: B
Section:
Explanation:
In the Check Point Security Management Architecture, both the Security Management Server and Security Gateway can store logs.The Security Management Server stores logs related to management activities, while the Security Gateway stores logs related to network traffic1.
Reference:Check Point Resource Library, page 3.

QUESTION 190
View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)



A. The current administrator has read-only permissions to Threat Prevention Policy.
B. Another user has locked the rule for editing.

C. Configuration lock is present. Click the lock symbol to gain read-write access.
D. The current administrator is logged in as read-only because someone else is editing the policy.

Correct Answer: B
Section:
Explanation:
The lock symbol in the left column of the rule means that another user has locked the rule for editing. This is to prevent multiple users from editing the same rule at the same time and causing conflicts.
Reference: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TP-Policy/TP-Policy-Edit-Rules.htm

QUESTION 191
By default, which port does the WebUI listen on?

A. 80
B. 4434
C. 443
D. 8080

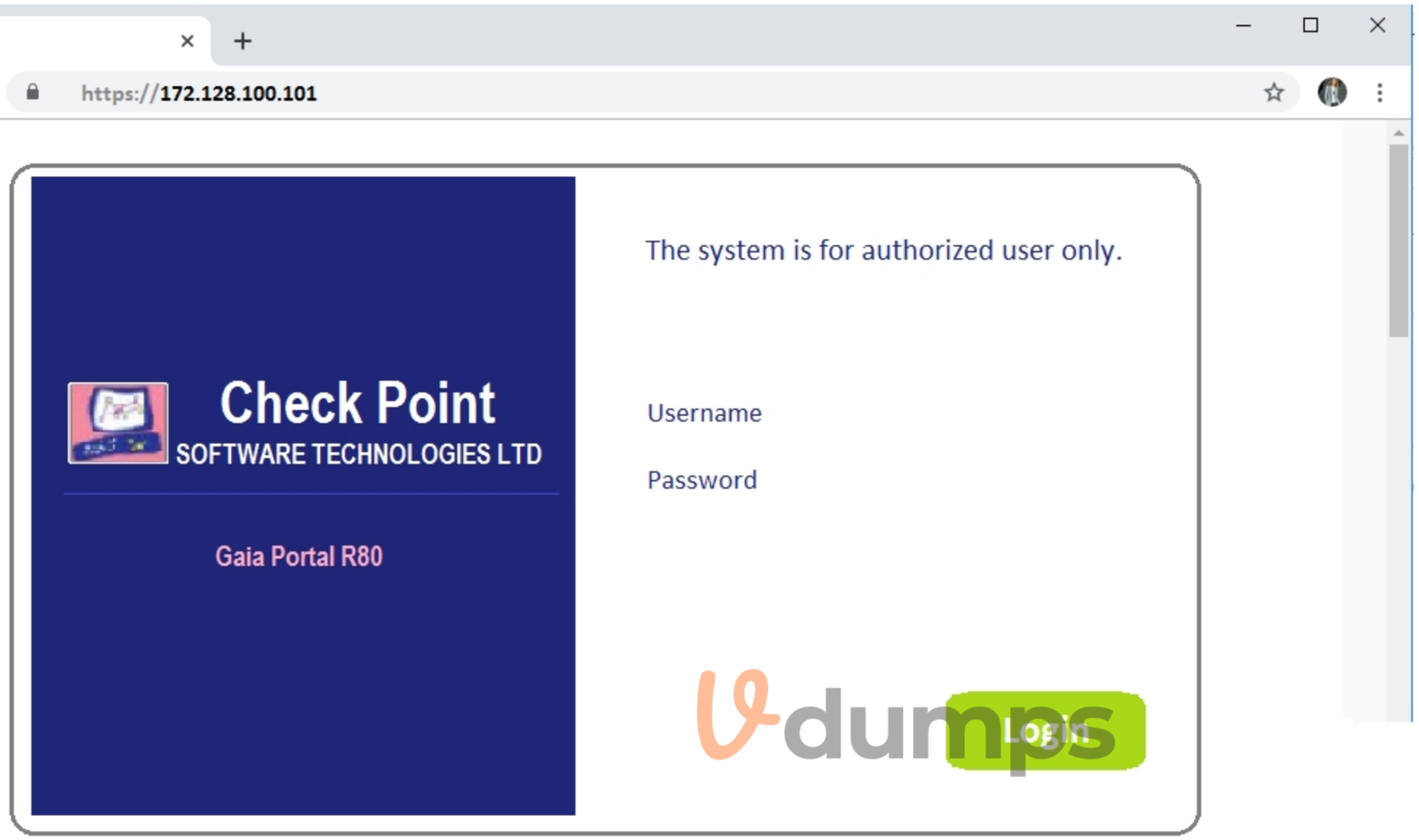
Correct Answer: C
Section:
Explanation:
The default port for the Gaia WebUI Portal is HTTPS 443. This is the standard port for secure web communication over SSL/TLS. Changing the port may cause inconsistency with the settings on the SmartConsole and is not recommended unless necessary. To change the port, you can use the CLISH commandset web ssl-port and save the configuration.
Reference:13

QUESTION 192
Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

A. To satellites through center only
B. To center only
C. To center and to other satellites through center
D. To center, or through the center to other satellites, to Internet and other VPN targets

Correct Answer: D
Section:
Explanation:
This VPN routing option uses VPN routing for every connection a satellite gateway handles, regardless of the destination. This means that all traffic from the satellite gateway will go through the VPN tunnel to the center gateway, and then be routed to the appropriate destination, whether it is another satellite, the Internet, or another VPN target. This option provides the highest level of security and control, but also consumes more bandwidth and processing power.

QUESTION 193
Kofi, the administrator of the ALPHA Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?



A. set web ssl-port <new port number>
B. set Gaia-portal port <new port number>
C. set Gaia-portal https-port <new port number>
D. set web https-port <new port number>

Correct Answer: A
Section:
Explanation:
The CLISH command to change the default Gaia WebUI Portal port number isset web ssl-port <new port number>. This command will change the port that the WebUI listens on for HTTPS connections. After changing the port, you need to save the configuration withsave configand verify that the change was applied withshow web ssl-port. You also need to update the Main URL in the Platform Portal section of the gateway object in SmartConsole and install the policy.

QUESTION 194
Joey want to configure NTP on R81 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

A. https://<Device_IP_Adress>
B. http://<Device IP_Address>:443
C. https://<Device_IP_Address>:10000

D. https://<Device_IP_Address>:4434

Correct Answer: A
Section:
Explanation:
The correct address to access the Web UI for Gaia platform via browser is https://<Device_IP_Adress>. This will open the Gaia Portal login page, where you can enter your username and password to access the Gaia configuration options. By default, the Web UI listens on port 443 for HTTPS connections, but you can change it using the CLISH commandset web ssl-port .

QUESTION 195
The ''Hit count'' feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits if the Track option is set to ''None''?

A. No, it will work independently. Hit Count will be shown only for rules Track option set as Log or alert.
B. Yes it will work independently as long as ''analyze all rules'' tick box is enabled on the Security Gateway.
C. No, it will not work independently because hit count requires all rules to be logged.
D. Yes it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways.

Correct Answer: D
Section:
Explanation:
The Hit Count feature allows tracking the number of connections that each rule matches, regardless of the Track option set for the rule. When you enable Hit Count, the Security Management Server collects the data from supported Security Gateways and displays it in SmartConsole. You can use the Hit Count feature to optimize your rule base by identifying unused or rarely used rules, or rules that match too many connections.

QUESTION 196
Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or _____ .

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

Correct Answer: C
Section:
Explanation:
Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or on specific tunnels in the community. Permanent VPN tunnels are always active and prevent VPN tunnel negotiation failures due to idle time or traffic volume. You can configure permanent VPN tunnels in SmartConsole by selecting the Permanent Tunnel option in the VPN Community Properties window.

QUESTION 197
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 Licenses are installed via Gaia on Security Gateways
D. True, Central License can be installed with CPLIC command on a Security Gateway

Correct Answer: D
Section:
Explanation:
In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway using the CPLIC command. The CPLIC command allows you to add, delete, or list Central Licenses on a Security Gateway from the

command line. You need to provide the IP address of the Security Management Server and the license string as parameters for the CPLIC command.

QUESTION 198
In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

A. Pentagon
B. Combined
C. Meshed
D. Star

Correct Answer: D
Section:
Explanation:
A star VPN community is a type of VPN community that allows a central gateway to create VPN tunnels with multiple satellite gateways or hosts, but does not allow satellite gateways or hosts to create VPN tunnels with each other. This type of community is suitable for hub-and-spoke topologies, where the central gateway acts as the hub and the satellite gateways or hosts act as the spokes. The central gateway can initiate or terminate VPN traffic to any satellite member, but the satellite members can only initiate or terminate VPN traffic to the central gateway.

QUESTION 199
When a packet arrives at the gateway, the gateway checks it against the rules in the hop Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

A. If the Action is Accept, the gateway allows the packet to pass through the gateway.
B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.
C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.
D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

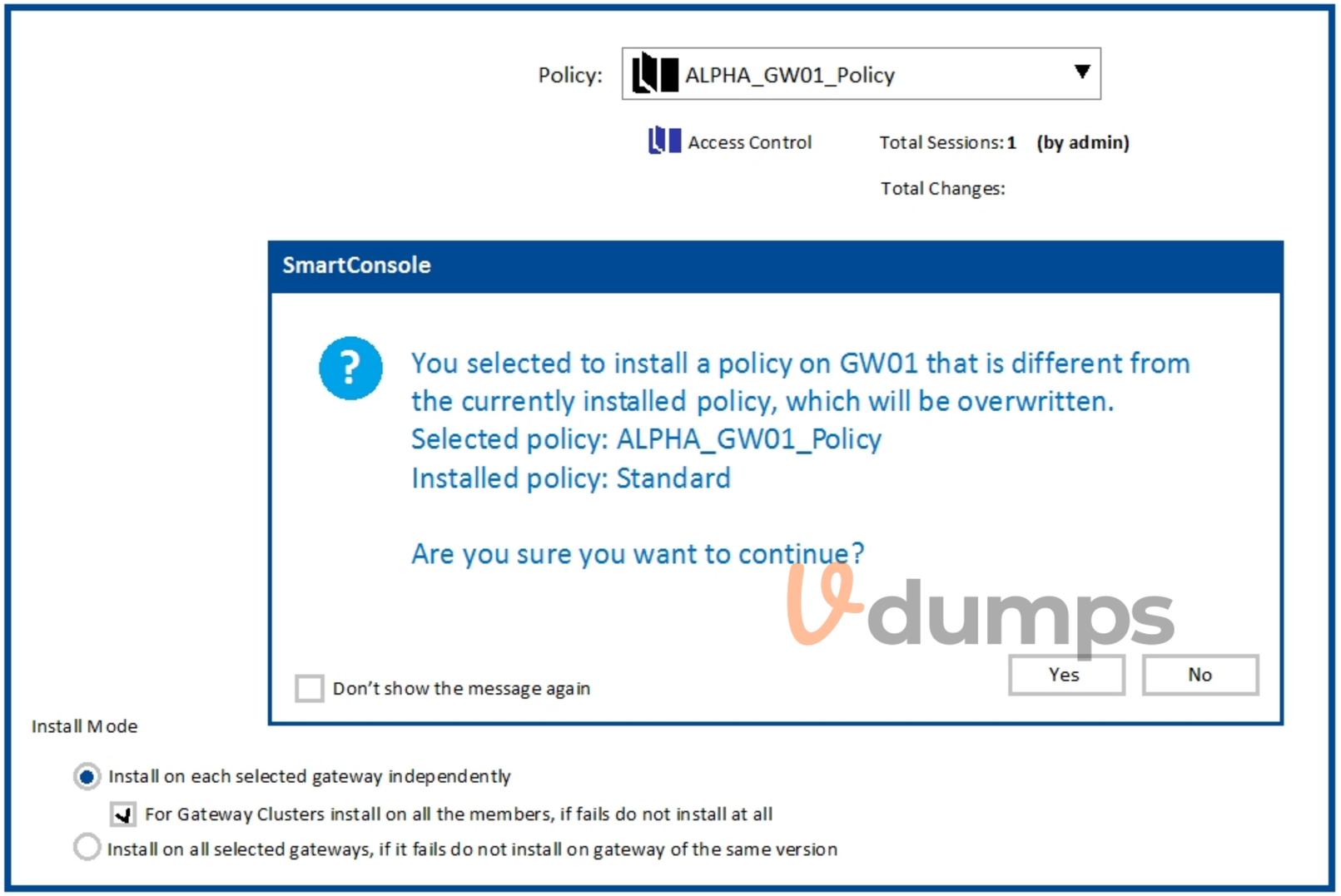
Correct Answer: C
Section:
Explanation:
When a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom, and enforces the first rule that matches the packet. The order of rule enforcement depends on the action of the matching rule. If the action is Accept, the gateway allows the packet to pass through the gateway, but also continues to check rules in the next Policy Layer down. If the action is Drop, Reject, or Encrypt, the gateway applies that action to the packet and stops checking rules in that Policy Layer and any subsequent Policy Layers. If there is no matching rule in a Policy Layer, the gateway applies the Implicit Clean-up Rule for that Policy Layer, which is usually Drop.

QUESTION 200
Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

A. UserCheck
B. Active Directory Query
C. Account Unit Query
D. User Directory Query

Correct Answer: B
Section:
Explanation:
Active Directory Query is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers by querying domain controllers for security event logs. The Security Gateway sends a WMI query to each domain controller and receives a WMI event when a user logs in, logs out, or unlocks their computer. The Security Gateway then maps IP addresses to user names based on these events. Active Directory Query does not require any software installation on domain controllers or clients, but it requires certain permissions and configurations on the domain controllers

QUESTION 201
Why would an administrator see the message below?



A. A new Policy Package created on both the Management and Gateway will be deleted and must be backed up first before proceeding.
B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
D. A new Policy Package created on the Gateway and transferred to the Management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Correct Answer: B
Section:
Explanation:
A Policy Package is a set of rules and settings that define how a Security Gateway enforces security on traffic that passes through it. A Policy Package can be created on either the Management Server or the Security Gateway, but it must be installed on both to take effect. When a new Policy Package is created on the Management Server, it must be installed on an existing Security Gateway that has a different Policy Package installed. The message below warns the administrator that installing a new Policy Package will overwrite the existing one on the Security Gateway.
https://www.bing.com/images/blob?bcid=qMoRhR0dzSkGmg

The message also advises the administrator to back up their existing configuration before proceeding with the installation.

QUESTION 202
Which command is used to add users to or from existing roles?

A. Add rba user <User Name> roles <List>
B. Add rba user <User Name>
C. Add user <User Name> roles <List>
D. Add user <User Name>

Correct Answer: A
Section:
Explanation:
The command to add users to or from existing roles isadd rba user <User Name> roles <List>. This command allows you to assign one or more roles to a user in the Gaia database. Roles are collections of permissions that define what actions a user can perform on the system. You can use predefined roles or create your own custom roles. To remove a role from a user, you can use the commanddelete rba user <User Name> roles <List>.

QUESTION 203
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

Correct Answer: C
Section:
Explanation:
The option that allows traffic to VPN gateways in specific VPN communities is Specific VPN Communities. This option lets you specify which VPN communities are allowed or denied by the rule. A VPN community is a group of VPN gateways or hosts that share the same VPN policy and keys. You can create different types of VPN communities, such as star, meshed, or remote access, depending on your network topology and security requirements. You can also use tags to group VPN gateways or hosts into logical categories.

QUESTION 204
Fill in the blank: An identity server uses a _____ for user authentication.

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

Correct Answer: D
Section:
Explanation:
An identity server uses a token for user authentication. A token is a piece of data that contains information about the user's identity, such as their username, email, roles, and claims. A token is digitally signed by the identity server and can be verified by the relying party (the application or service that needs to authenticate the user). A token can be issued in different formats, such as JSON Web Token (JWT) or Security Assertion Markup Language (SAML). A token can also have different lifetimes, such as short-lived access tokens or long-lived refresh tokens.

QUESTION 205
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

Correct Answer: B
Section:
Explanation:
Resource is not an objects category in SmartConsole. Objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories, such as Network Object, Host, Gateway, Service, Time Object, Custom Application / Site, Limit, and Group. A resource is a type of object that represents an application or content that is accessible through HTTP or HTTPS protocols. A resource can be used to define access rules for users who connect through Identity Awareness or Mobile Access blades.

QUESTION 206
DLP and Geo Policy are examples of what type of Policy?

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

Correct Answer: B
Section:
Explanation:
DLP and Geo Policy are examples of Shared Policies. Shared Policies are policies that can be applied to multiple gateways or clusters, regardless of their Access Control policy. Shared Policies allow administrators to manage common security settings across different gateways or clusters, such as Data Loss Prevention, Geo Protection, Threat Prevention, HTTPS Inspection, etc.
Reference:R81 Security Management Administration Guide, page 31.

QUESTION 207
Fill in the blank: The IPS policy for pre-R81 gateways is installed during the _____ .

A. Firewall policy install
B. Threat Prevention policy install
C. Anti-bot policy install
D. Access Control policy install

Correct Answer: C
Section:
Explanation:
The IPS policy for pre-R81 gateways is installed during the Anti-bot policy install. The Anti-bot policy install includes both Anti-bot and IPS protections for pre-R81 gateways, since they share the same inspection engine. For R81 and above gateways, the IPS policy is installed separately as part of the Threat Prevention policy install, which also includes Anti-virus and Threat Emulation protections.
Reference:R81 Threat Prevention Administration Guide, page 15.

QUESTION 208
How many users can have read/write access in Gaia at one time?

A. Infinite

B. One
C. Three
D. Two

Correct Answer: B
Section:
Explanation:
How many users can have read/write access in Gaia at one time? Only one user can have read/write access in Gaia at one time. This is to prevent conflicts and inconsistencies in the configuration changes made by different users. If another user tries to login with read/write access while a user is already logged in, they will receive a warning message and will be given the option to either login with read-only access or force the other user to logout.
Reference: [Gaia Administration Guide R81], page 15.

QUESTION 209
Which software blade does NOT accompany the Threat Prevention policy?

A. Anti-virus
B. IPS
C. Threat Emulation
D. Application Control and URL Filtering

Correct Answer: D
Section:
Explanation:
Which software blade does NOT accompany the Threat Prevention policy? Application Control and URL Filtering software blade does not accompany the Threat Prevention policy. The Threat Prevention policy is a unified policy that includes Anti-virus, IPS, Anti-bot, and Threat Emulation software blades. Application Control and URL Filtering software blade is part of the Access Control policy, which is a separate policy that controls network access based on users, applications, content, and other criteria.
Reference:R81 Security Management Administration Guide, page 29.

QUESTION 210
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.

Correct Answer: B
Section:
Explanation:
Check Point ClusterXL Active/Active deployment is used when there is Load Sharing solution set up. Load Sharing is a ClusterXL mode that allows distributing the network traffic between all cluster members, while still providing high availability in case of failures. Load Sharing can be configured as either Unicast or Multicast, depending on the network topology and switches support.
Reference:R81 ClusterXL Administration Guide, page 9.

QUESTION 211
To optimize Rule Base efficiency, the most hit rules should be where?

A. Removed from the Rule Base.
B. Towards the middle of the Rule Base.

C. Towards the top of the Rule Base.
D. Towards the bottom of the Rule Base.

Correct Answer: C
Section:
Explanation:
To optimize Rule Base efficiency, the most hit rules should be towards the top of the Rule Base. This is because the Rule Base is processed from top to bottom, and the first rule that matches the traffic is applied. Therefore, placing the most hit rules at the top reduces the number of rules that need to be checked and improves the performance of the firewall.
Reference:R81 Security Management Administration Guide, page 97.

QUESTION 212
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

Correct Answer: D
Section:
Explanation:
What two ordered layers make up the Access Control Policy Layer? Network and Application Control are the two ordered layers that make up the Access Control Policy Layer. The Network layer controls network access based on source, destination, service, time, etc. The Application Control layer controls application access based on users, groups, applications, content categories, etc. The Network layer is always processed before the Application Control layer.
Reference:R81 Security Management Administration Guide, page 29.

QUESTION 213
Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is ____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

A. Accept; redirect
B. Accept; drop
C. Redirect; drop
D. Drop; accept

Correct Answer: D
Section:
Explanation:
In the Network policy layer, the default action for the Implied last rule isdropall traffic. However, in the Application Control policy layer, the default action isacceptall traffic. The Implied last rule is a rule that is automatically added at the end of each policy layer and defines what to do with traffic that does not match any of the user-defined rules. The default actions for each policy layer can be changed in the Global Properties or in the layer properties.
Reference:R81 Security Management Administration Guide, page 30.

QUESTION 214
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links.
Which component of SandBlast protection is her company using on a Gateway?

A. SandBlast Threat Emulation

B. SandBlast Agent
C. Check Point Protect
D. SandBlast Threat Extraction

Correct Answer: D
Section:
Explanation:
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links.
The component of SandBlast protection that her company is using on a Gateway isSandBlast Threat Extraction. SandBlast Threat Extraction is a software blade that provides protection against malicious files by removing potentially risky elements, such as macros, embedded objects, scripts, etc. The sanitized files are delivered to the users with a notification about the removed elements. SandBlast Threat Extraction can also reconstruct the original files after they are scanned by SandBlast Threat Emulation, which is another software blade that provides protection against malicious files by emulating them in a virtual sandbox and analyzing their behavior.
Reference:R81 Threat Prevention Administration Guide, page 37.

QUESTION 215
If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is necessary to be completed for it to function properly?

A. Nothing - the proxy ARP is automatically handled in the R81 version
B. Add the proxy ARP configurations in a file called /etc/conf/local.arp
C. Add the proxy ARP configurations in a file called $FWDIR/conf/local.arp
D. Add the proxy ARP configurations in a file called $CPDIR/conf/local.arp

Correct Answer: C
Section:
Explanation:
If an administrator wants to add manual NAT for addresses not owned by the Check Point firewall, they also need to add the proxy ARP configurations in a file called$FWDIR/conf/local.arp. This file contains the mappings between the IP addresses and the MAC addresses of the NATed hosts. The proxy ARP feature allows the firewall to answer ARP requests on behalf of the NATed hosts and forward the traffic to them. The local.arp file needs to be edited manually and reloaded with the commandarp -f $FWDIR/conf/local.arp.
Reference:R81 Security Management Administration Guide, page 1014.

QUESTION 216
How many interfaces can you configure to use the Multi-Queue feature?

A. 10 interfaces
B. 3 interfaces
C. 4 interfaces
D. 5 interfaces

Correct Answer: D
Section:
Explanation:
How many interfaces can you configure to use the Multi-Queue feature? You can configure up to5 interfacesto use the Multi-Queue feature. Multi-Queue is a performance enhancement feature that allows distributing the network traffic among multiple CPU cores, instead of using a single core for all traffic. Multi-Queue can be enabled on interfaces that have high traffic load and support multiple receive/transmit queues. Multi-Queue can be configured via SmartConsole or via CLI with the commandsim affinity -m.
Reference:R81 Performance Tuning Administration Guide, page 18.

QUESTION 217
Which firewall daemon is responsible for the FW CLI commands?

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

Correct Answer: A
Section:
Explanation:
Which firewall daemon is responsible for the FW CLI commands? The firewall daemon that is responsible for the FW CLI commands isfwd. This daemon handles the communication between the firewall kernel and the user space processes, such as SmartConsole, SmartView Tracker, etc. The FW CLI commands are used to control and monitor various aspects of the firewall, such as connections, policy installation, logs, NAT, etc. The FW CLI commands are executed with the prefixfw, such asfw stat,fw tab,fw monitor, etc.
Reference:R81 Command Line Interface Reference Guide, page 13.

QUESTION 218
How long may verification of one file take for Sandblast Threat Emulation?

A. up to 1 minutes
B. within seconds cleaned file will be provided
C. up to 5 minutes
D. up to 3 minutes

Correct Answer: D
Section:
Explanation:
How long may verification of one file take for SandBlast Threat Emulation? Verification of one file may take up to3 minutesfor SandBlast Threat Emulation. SandBlast Threat Emulation is a software blade that provides protection against malicious files by emulating them in a virtual sandbox and analyzing their behavior. The emulation time depends on various factors, such as file size, file type, emulation mode, etc. The default emulation time limit is 180 seconds, but it can be changed in the Threat Prevention policy settings.
Reference: [R81 Threat Prevention Administration Guide], page 39.

QUESTION 219
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

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

Correct Answer: B
Section:
Explanation:
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new CPU to replace the existing single core CPU. After installation, the administrator needs to perform some additional tasks for it to function properly.
The tasks that the administrator needs to perform are:
Go to Clish-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
Go to SmartConsole | Install Security Policy
The first task is to enable and configure CoreXL, which is a performance enhancement feature that allows running multiple instances of the firewall kernel on multiple CPU cores. CoreXL can be enabled and configured via

cpconfig, which is a utility that provides a menu-based interface for various system settings. After enabling CoreXL, the administrator needs to reboot the Security Gateway for the changes to take effect.
The second task is to install the security policy on the Security Gateway via SmartConsole, which is a unified graphical user interface for managing Check Point products. Installing the security policy will activate the CoreXL instances and distribute the traffic among them.
Reference:R81 Performance Tuning Administration Guide, page 15;R81 Security Management Administration Guide, page 83.

QUESTION 220
GAIA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the:

A. Check Point Update Service Engine
B. Check Point Software Update Agent
C. Check Point Remote Installation Daemon (CPRID)
D. Check Point Software Update Daemon

Correct Answer: A
Section:
Explanation:
GAIA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as theCheck Point Update Service Engine. This agent allows you to download and install software updates, hotfixes, upgrade packages, etc., from Check Point servers or from a local repository. The Check Point Update Service Engine can be accessed via SmartConsole or via WebUI or CLI on GAIA.
Reference: [Gaia Administration Guide R81], page 77.

QUESTION 221
Hit Count is a feature to track the number of connections that each rule matches, which one is not benefit of Hit Count.

A. Better understand the behavior of the Access Control Policy
B. Improve Firewall performance - You can move a rule that has hot count to a higher position in the Rule Base
C. Automatically rearrange Access Control Policy based on Hit Count Analysis
D. Analyze a Rule Base - You can delete rules that have no matching connections

Correct Answer: C
Section:
Explanation:
Hit Count is a feature to track the number of connections that each rule matches, which can help to optimize the Rule Base efficiency and analyze the network traffic behavior. The benefit that is not provided by Hit Count isautomatically rearrange Access Control Policy based on Hit Count Analysis. Hit Count does not change the order of the rules automatically, but it allows the administrator to manually move the rules up or down based on the hit count statistics. The administrator can also use the SmartOptimize feature to get suggestions for improving the Rule Base order and performance.
Reference:R81 Security Management Administration Guide, page 97.

QUESTION 222
You need to change the MAC-address on eth2 interface of the gateway. What command and what mode will you use to achieve this goal?

A. set interface eth2 mac-addr 11:11:11:11:11:11; CLISH
B. ifconfig eth1 hw 11:11:11:11:11:11; expert
C. set interface eth2 hw-addr 11:11:11:11:11:11; CLISH
D. ethtool -i eth2 mac 11:11:11:11:11:11; expert

Correct Answer: A
Section:
Explanation:
You need to change the MAC-address on eth2 interface of the gateway. The command and the mode that you will use to achieve this goal areset interface eth2 mac-addr 11:11:11:11:11:11; CLISH. This command allows you to

change the MAC address of an interface in GAIA, which can be useful for replacing a faulty network card or cloning another device. The command is executed in CLISH mode, which is a shell that provides a menu-based interface for configuring various system settings. To apply the changes, you need to save the configuration and restart the interface.
Reference:Gaia Administration Guide R81, page 31.

QUESTION 223
The Check Point history feature in R81 provides the following:

A. View install changes and install specific version
B. View install changes
C. Policy Installation Date, view install changes and install specific version
D. Policy Installation Date only

Correct Answer: A
Section:
Explanation:
The Check Point history feature in R81 provides the following functions:
View install changes: This function allows you to view the changes that were made in each policy installation, such as added, modified, or deleted rules, objects, settings, etc. You can also compare the changes between different policy installations and filter them by various criteria.
Install specific version: This function allows you to install a specific version of the policy from the history, which can be useful for reverting to a previous policy or testing different policies. You can also view the changes that will be applied by installing a specific version before installing it.
Reference:R81 Security Management Administration Guide, page 85.

QUESTION 224
You are the administrator for ABC Corp. You have logged into your R81 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.
What does this mean?

A. This rule No. 6 has been marked for deletion in your Management session.
B. This rule No. 6 has been marked for deletion in another Management session.
C. This rule No. 6 has been marked for editing in your Management session.
D. This rule No. 6 has been marked for editing in another Management session.

Correct Answer: C
Section:
Explanation:
You are the administrator for ABC Corp. You have logged into your R81 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.
This means that rule No.6 has been marked for editing in your Management session. In R81, every administrator works in a session that is independent of other administrators. Changes made by one administrator are not visible to others until they are published. When you edit a rule, it is marked with a pencil icon to indicate that it has been modified in your session. You can also lock a rule to prevent other administrators from editing it until you unlock it or publish your session.
Reference:R81 Security Management Administration Guide, page 43.

QUESTION 225
SandBlast agent extends 0-day prevention to what part of the network?

A. Web Browsers and user devices
B. DMZ server
C. Cloud
D. Email servers

Correct Answer: A
Section:
Explanation:
SandBlast Agent is a comprehensive endpoint security solution that extends 0-day prevention to web browsers and user devices. It protects against advanced threats such as ransomware, phishing, and zero-day attacks by using a combination of static, dynamic, and behavioral analysis.
Reference: [SandBlast Agent Datasheet]

QUESTION 226
What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?

A. Use Multi-Domain Management Server.
B. Choose different setting for log storage and SmartEvent db
C. Install Management and SmartEvent on different machines.
D. it is not possible.

Correct Answer: C
Section:
Explanation:
The recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days is to install Management and SmartEvent on different machines. This is because SmartLog and SmartEvent use different databases and storage methods, and having them on separate machines allows for better performance and scalability.
Reference: [SmartLog Administration Guide]

QUESTION 227
The log server sends what to the Correlation Unit?

A. Authentication requests
B. CPMI dbsync
C. Logs
D. Event Policy

Correct Answer: C
Section:
Explanation:
The log server sends logs to the Correlation Unit. The Correlation Unit analyzes the logs and generates events based on the event policy. The events are then sent to the SmartEvent Server, which displays them in the SmartEvent GUI.
Reference: [SmartEvent Administration Guide]

QUESTION 228
SmartEvent uses it's event policy to identify events. How can this be customized?

A. By modifying the firewall rulebase
B. By creating event candidates
C. By matching logs against exclusions
D. By matching logs against event rules

Correct Answer: D
Section:
Explanation:

SmartEvent uses its event policy to identify events. The event policy can be customized by matching logs against event rules. Event rules define the conditions and actions for generating events. You can create, edit, delete, enable, or disable event rules in the SmartEvent Policy tab of the SmartConsole.
Reference: [SmartEvent Administration Guide]

QUESTION 229
When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, which of the following query syntax would you use?

A. Toni? AND 10.0.4.210 NOT 10.0.4.76
B. To** AND 10.0.4.210 NOT 10.0.4.76
C. Ton* AND 10.0.4.210 NOT 10.0.4.75
D. 'Toni' AND 10.0.4.210 NOT 10.0.4.76

Correct Answer: D
Section:
Explanation:
When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, you would use the following query syntax:
''Toni'' AND 10.0.4.210 NOT 10.0.4.76
This query will match logs that contain the exact phrase ''Toni'' and the IP address 10.0.4.210, but not the IP address 10.0.4.76. The quotation marks around ''Toni'' ensure that only logs with that exact word are matched, not variations like Toni? or To**. The AND operator combines two conditions that must both be true, while the NOT operator excludes logs that match a certain condition.
Reference: [SmartLog User Guide]

QUESTION 230
Check Point Support in many cases asks you for a configuration summary of your Check Point system. This is also called:

A. cpexport
B. sysinfo
C. cpsizeme
D. cpinfo

Correct Answer: D
Section:
Explanation:
Check Point Support in many cases asks you for a configuration summary of your Check Point system. This is also called cpinfo. Cpinfo is a utility that collects diagnostic data on a Check Point gateway, management server, or log server. It generates a file that contains information such as product version, license details, OS details, network configuration, installed hotfixes, status of Check Point processes, firewall tables, etc. This file can be used by Check Point Support to troubleshoot issues or analyze performance.
Reference: [Cpinfo Utility]

QUESTION 231
How does the Anti-Virus feature of the Threat Prevention policy block traffic from infected websites?

A. By dropping traffic from websites identified through ThreatCloud Verification and URL Caching
B. By dropping traffic that is not proven to be from clean websites in the URL Filtering blade
C. By allowing traffic from websites that are known to run Antivirus Software on servers regularly
D. By matching logs against ThreatCloud information about the reputation of the website

Correct Answer: D
Section:
Explanation:

The Anti-Virus feature of the Threat Prevention policy blocks traffic from infected websites by matching logs against ThreatCloud information about the reputation of the website. ThreatCloud is a collaborative network that collects and analyzes threat data from millions of sources worldwide. It assigns a reputation score to each website based on its malicious activity and behavior. If a website has a low reputation score, it is considered infected and blocked by the Anti-Virus blade.
Reference:Training & Certification | Check Point Software, CCSE section

QUESTION 232
What level of CPU load on a Secure Network Distributor would indicate that another may be necessary?

A. Idle <20%
B. USR <20%
C. SYS <20%
D. Wait <20%

Correct Answer: A
Section:
Explanation:
The CPU load on a Secure Network Distributor (SND) indicates how much processing power is available for distributing traffic among cluster members. If the CPU load is high, it means that the SND is overloaded and cannot handle more traffic efficiently. A good indicator of SND overload is when the Idle CPU percentage is less than 20%. In this case, you may need to add another SND to balance the load or optimize your cluster configuration.
Reference:Getting Started - Check Point Software, section ''Monitoring ClusterXL Status''

QUESTION 233
What is required for a certificate-based VPN tunnel between two gateways with separate management systems?

A. Mutually Trusted Certificate Authorities
B. Shared User Certificates
C. Shared Secret Passwords
D. Unique Passwords

Correct Answer: A
Section:
Explanation:
A certificate-based VPN tunnel between two gateways with separate management systems requires mutually trusted certificate authorities. This means that each gateway must have a certificate issued by a certificate authority (CA) that the other gateway trusts. The CA can be either an internal CA or an external CA. The CA issues certificates that contain the public key and identity information of the gateway. The gateway uses its private key to sign and encrypt the VPN traffic. The other gateway can verify the signature and decrypt the traffic using the public key in the certificate. This ensures the authenticity, integrity, and confidentiality of the VPN tunnel.
Remote Access VPN R81.20 Administration Guide, page 12
DeepDive Webinar - R81.20 Seamless VPN Connection to Public Cloud, slide 9

QUESTION 234
When performing a minimal effort upgrade, what will happen to the network traffic?

A. All connections that were initiated before the upgrade will be dropped, causing network downtime
B. All connections that were initiated before the upgrade will be handled normally
C. All connections that were initiated before the upgrade will be handled by the standby gateway
D. All connections that were initiated before the upgrade will be handled by the active gateway

Correct Answer: B
Section:
Explanation:

A minimal effort upgrade is a process of upgrading the Security Gateway software without changing the configuration or policy. It is done by using the CPUSE (Check Point Update Service Engine) tool, which is available in the Gaia Portal or CLI. The CPUSE tool performs a pre-upgrade verification to check the compatibility and readiness of the system for the upgrade. If the verification passes, the CPUSE tool installs the new software package and reboots the system. During the reboot, there is a short network downtime, but it does not affect the existing connections. All connections that were initiated before the upgrade will be handled normally by the upgraded gateway. The minimal effort upgrade preserves the existing configuration and policy, so there is no need to reinstall the policy or reconfigure the gateway after the upgrade.
Check Point Upgrade Path and Management Servers and Security Gateways Compatibility Maps, section ''Minimal Effort Upgrade''
INSTALLATION AND UPGRADE GUIDE R81, page 21-22

QUESTION 235
Which command will reset the kernel debug options to default settings?

A. fw ctl dbg -a 0
B. fw ctl dbg resetall
C. fw ctl debug 0
D. fw ctl debug set 0

Correct Answer: C
Section:
Explanation:
The commandfw ctl debug 0will reset the kernel debug options to default settings. This command will disable all the debug flags and clear the debug buffer. It is recommended to use this command before and after performing a kernel debug, to avoid any interference or confusion with other debug outputs. The commandfw ctl debug 0is also equivalent tofw ctl debug -buf 0.
Best Practices - HTTPS Inspection - Check Point Software, section ''How to perform a Kernel Debug''
LOGGINGAND MONITORING R81 - Check Point Software, page 104

QUESTION 236
When defining QoS global properties, which option below is not valid?

A. Weight
B. Authenticated timeout
C. Schedule
D. Rate

Correct Answer: D
Section:
Explanation:
QoS global properties are the settings that apply to all QoS rules and QoS interfaces on the Security Gateway.They include the following options12:
Weight: This is the relative importance of a QoS rule compared to other QoS rules. A higher weight means a higher priority. The default weight is 1, and the maximum weight is 1000.
Authenticated timeout: This is the time period in seconds that a connection remains in the QoS rule after the last packet is sent or received. The default timeout is 600 seconds, and the minimum timeout is 60 seconds.
Schedule: This is the time period in which a QoS rule is active. You can define a schedule for each day of the week, or use the default schedule of always active.
Rate: This is not a valid option for QoS global properties. Rate is an option for QoS rule action, which defines the maximum bandwidth allocated for a QoS rule. The rate can be specified in Kbps, Mbps, or percentage of interface speed.

QUESTION 237
Which command shows only the table names of all kernel tables?

A. fwtab-t
B. fw tab -s
C. fw tab -n
D. fw tab -k

Correct Answer: B
Section:
Explanation:
The commandfw tabis used to display the contents of the kernel tables1. The command has several options that can modify the output.The option-sshows only the table names and the number of entries in each table1. For example:

```
[Expert@HostName]# fw tab -s
HOSTS (1): 1
RESOLV (2): 0
SERVICES (3): 0
SERVICES_UDP (4): 0
SERVICES_TCP (5): 0
...
```

The option-tshows the contents of a specific table, given by its name or ID1. For example:

```
[Expert@HostName]# fw tab -t connections
ID | Name
0 | connections
#VALS | #PEAK | #SLINKS
0 | 0 | 0
```

The option-nshows the numeric values of the fields in the tables, instead of resolving them to names1. For example:

```
[Expert@HostName]# fw tab -n -t connections
ID | Name
0 | connections
#VALS | #PEAK | #SLINKS
0 | 0 | 0
SRC IP | DST IP | SRC PORT | DST PORT | PROTO | TIMEOUT | KBUF | STATE | EXPDATE | TYPE
...
```

The option-kshows the kernel references for each entry in the table1. For example:

```
[Expert@HostName]# fw tab -k -t connections
ID | Name
0 | connections
#VALS | #PEAK | #SLINKS
0 | 0 | 0
SRC IP | DST IP | SRC PORT | DST PORT | PROTO | TIMEOUT | KBUF | STATE | EXPDATE ...
10.1.1.1 -> 10.2.2.2 : 1234 -> 80 : TCP : 3600 : 0x00000000 : ESTABLISHED : 1599999999
...
```

Therefore, the correct answer is B, as it shows only the table names of all kernel tables.

QUESTION 238
When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. What is this setting called and what are you defining?

A. Network, and defining your Class A space
B. Topology, and you are defining the Internal network
C. Internal addresses you are defining the gateways

D. Internal network(s) you are defining your networks

Correct Answer: D
Section:
Explanation:
When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. This setting is called Internal network(s) and you are defining your networks. You can specify one or more networks or IP addresses that are considered internal for SmartEvent. This helps SmartEvent to determine the direction of the traffic (inbound, outbound, or internal) and generate events accordingly.
Reference: [SmartEvent Administration Guide]

QUESTION 239
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

Correct Answer: B
Section:
Explanation:
Rugged appliances are small appliances with ruggedized hardware that are designed for harsh environments. Like Quantum Spark appliances, they use Gaia embedded as their operating system. Gaia embedded is a lightweight version of Gaia that supports a subset of features and commands.
Reference: [Check Point R81 Gaia Embedded Administration Guide]

QUESTION 240
What is the biggest benefit of policy layers?

A. To break one policy into several virtual policies
B. Policy Layers and Sub-Policies enable flexible control over the security policy
C. They improve the performance on OS kernel version 3.0
D. To include Threat Prevention as a sub policy for the firewall policy

Correct Answer: B
Section:
Explanation:
The biggest benefit of policy layers is that they enable flexible control over the security policy. Policy layers and sub-policies allow administrators to break one policy into several virtual policies, each with its own set of rules and actions. Policy layers can be ordered, shared, and reused across different policies. Policy layers can also include Threat Prevention as a sub-policy for the firewall policy.
Reference: [Check Point R81 Security Management Guide]

QUESTION 241
What ports are used for SmartConsole to connect to the Security Management Server?

A. CPMI (18190)
B. ICA_Pull (18210), CPMI (18190) https (443)
C. CPM (19009), CPMI (18190) https (443)
D. CPM (19009), CPMI (18190) CPD (18191)

Correct Answer: C

Section:
Explanation:
The correct answer is C) CPM (19009), CPMI (18190) https (443).
SmartConsole is a client application that connects to the Security Management Server to manage and configure the security policy and objects. SmartConsole uses three ports to communicate with the Security Management Server1:
CPM (19009): This port is used for the communication between the SmartConsole client and the Check Point Management (CPM) process on the Security Management Server. The CPM process handles the database operations and the policy installation.
CPMI (18190): This port is used for the communication between the SmartConsole client and the Check Point Management Interface (CPMI) process on the Security Management Server. The CPMI process handles the authentication and encryption of the SmartConsole sessions.
https (443): This port is used for the communication between the SmartConsole client and the web server on the Security Management Server. The web server provides the SmartConsole GUI and the SmartConsole extensions.
The other options are incorrect because they either include ports that are not used by SmartConsole or omit ports that are used by SmartConsole.
SmartConsole R81.20 - Check Point Software1

QUESTION 242
After upgrading the primary security management server from R80.40 to R81.10 Bob wants to use the central deployment in SmartConsole R81.10 for the first time. How many installations (e.g. Jumbo Hotfix, Hotfixes or Upgrade Packages) can run of such at the same time:

A. Up to 5 gateways
B. only 1 gateway
C. Up to 10 gateways
D. Up to 3 gateways

Correct Answer: C
Section:
Explanation:
According to the Check Point R81.20 documentation, the central deployment feature allows you to install up to 10 packages simultaneously on multiple gateways1.
Reference
1:Check Point R81.20 Administration Guide, page 35.