Checkpoint.156-315.81vJun-2024.by.Osis..288q

Number: 156-315.81
Passing Score: 800
Time Limit: 120
File Version: 13.0

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

Exam A

QUESTION 1
What is the command to see cluster status in cli expert mode?

A. fw ctl stat
B. clusterXL stat
C. clusterXL status
D. cphaprob stat

Correct Answer: D
Section:
Explanation:
To see the cluster status in CLI expert mode, you can use the command cphaprob stat. This command displays the status of the Check Point High Availability cluster. It provides information about the state of the cluster members, such as 'Active,' 'Standby,' or 'Collision.'

QUESTION 2
As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

A. That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.
B. Fill Layer4 VPN --SSL VPN that gives users network access to all mobile applications.
C. Full Layer3 VPN --IPSec VPN that gives users network access to all mobile applications.
D. You can make sure that documents are sent to the intended recipients only.

Correct Answer: C
Section:
Explanation:
The feature that provides Full Layer3 VPN --IPSec VPN, giving users network access to all mobile applications, is the correct answer.
Capsule Connect/VPN is used to establish secure VPN connections for mobile devices, and the Full Layer3 VPN (IPSec VPN) option provides comprehensive network access.

QUESTION 3
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:

```
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12

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 13
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 14
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 15
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 16
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 17
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 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43
CPM process stores objects, policies, users, administrators, licenses and management data in a database. The database is:

A. MySQL
B. Postgres SQL
C. MarisDB
D. SOLR

Correct Answer: B
Section:
Explanation:
CPM process stores objects, policies, users, administrators, licenses and management data in a Postgres SQL database.This database is located in$FWDIR/confand can be accessed using thepg_clientcommand2. The other options are not the correct database type for CPM.
Reference:Check Point R81 Security Management Administration Guide

QUESTION 44
If you needed the Multicast MAC address of a cluster, what command would you run?

A. cphaprob --a if
B. cphaconf ccp multicast
C. cphaconf debug data
D. cphaprob igmp

Correct Answer: D
Section:
Explanation:
The commandcphaprob igmpcan be used to display the Multicast MAC address of a cluster.This command shows the IGMP (Internet Group Management Protocol) information for each cluster interface, including the VRID (Virtual Router ID), the Multicast IP address, and the Multicast MAC address3. The other commands do not show the Multicast MAC address information.
Reference:Check Point R81 ClusterXL Administration Guide

QUESTION 45
Which is NOT an example of a Check Point API?

A. Gateway API
B. Management API
C. OPSC SDK
D. Threat Prevention API

Correct Answer: A
Section:
Explanation:
Gateway API is not an example of a Check Point API. Check Point APIs are interfaces that enable interactions with Check Point products using automation scripts or external applications.The examples of Check Point APIs are Management API, OPSEC SDK, Threat Prevention API, Identity Awareness Web Services API, and others4. Gateway API is not a valid Check Point API name.
Reference:Check Point R81 Security Management Administration Guide, Check Point APIs

QUESTION 46
What are the three components for Check Point Capsule?

A. Capsule Docs, Capsule Cloud, Capsule Connect
B. Capsule Workspace, Capsule Cloud, Capsule Connect
C. Capsule Workspace, Capsule Docs, Capsule Connect
D. Capsule Workspace, Capsule Docs, Capsule Cloud

Correct Answer: D
Section:
Explanation:
The three components for Check Point Capsule are Capsule Workspace, Capsule Docs, and Capsule Cloud. Capsule Workspace is a secure container app that allows users to access corporate data and applications from their mobile devices. Capsule Docs is a solution that protects documents with encryption and granular access control. Capsule Cloud is a cloud-based security service that enforces security policies on devices that are outside the corporate network.
Reference: Check Point Capsule

QUESTION 47
Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

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

Correct Answer: B
Section:
Explanation:
The fwd process within the Security Management Server is responsible for the receiving of log records from Security Gateway.The fwd process handles the communication with the Security Gateways and log servers via TCP port 2571.The other processes have different roles, such as logd for writing logs to the database, fwm for handling GUI clients, and cpd for infrastructure tasks2.
Reference:Check Point Ports Used for Communication by Various Check Point Modules,Check Point Processes Cheat Sheet -- LazyAdmins

QUESTION 48
The fwd process on the Security Gateway sends logs to the fwd process on the Management Server via which 2 processes?

A. fwd via cpm

B. fwm via fwd

C. cpm via cpd

D. fwd via cpd

Correct Answer: A
Section:
Explanation:
The fwd process on the Security Gateway sends logs to the fwd process on the Management Server via the cpm process.The cpm process is the main management process that handles database operations, policy installation, and communication with GUI clients via TCP port 190093. The other options are either incorrect or irrelevant to the log flow.
Reference:Certified Security Expert (CCSE) R81.20 Course Overview,Check Point Ports Used for Communication by Various Check Point Modules

QUESTION 49
You have successfully backed up Check Point configurations without the OS information. What command would you use to restore this backup?

A. restore_backup

B. import backup

C. cp_merge

D. migrate import

Correct Answer: D
Section:
Explanation:
The commandmigrate importcan be used to restore a backup of Check Point configurations without the OS information. This command imports the configuration from a file that was created using themigrate exportcommand, which backs up only the Check Point configuration and not the OS settings. The other commands are either not valid or not suitable for restoring a backup without the OS information.
Reference: Check Point R81 Installation and Upgrade Guide

QUESTION 50
The Firewall Administrator is required to create 100 new host objects with different IP addresses. What API command can he use in the script to achieve the requirement?

A. add host name <New HostName> ip-address <ip address>

B. add hostname <New HostName> ip-address <ip address>

C. set host name <New HostName> ip-address <ip address>

D. set hostname <New HostName> ip-address <ip address>

Correct Answer: A
Section:
Explanation:
The API commandadd host name <New HostName> ip-address <ip address>can be used in a script to create 100 new host objects with different IP addresses. This command adds a new host object with the specified name and IP address to the database. The other commands are either not valid or not suitable for creating new host objects.
Reference: Check Point - Management API reference

QUESTION 51
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 52
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 53
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 54
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 55
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 56
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 57
Which of the following will NOT affect acceleration?

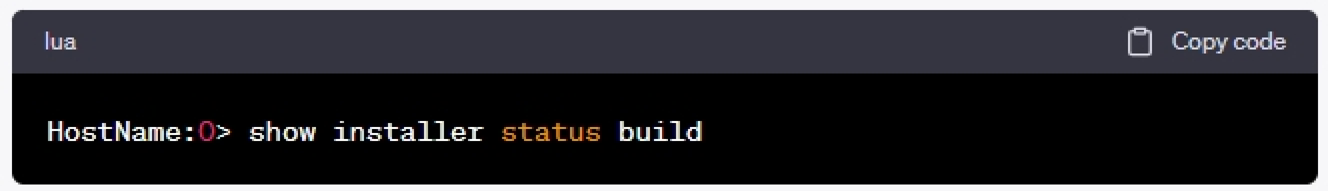
A. Connections destined to or originated from the Security gateway
B. A 5-tuple match
C. Multicast packets
D. Connections that have a Handler (ICMP, FTP, H.323, etc.)

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 58
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:



```
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 59
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 60
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 61
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 62
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 63
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 64
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 65
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 66
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 67
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

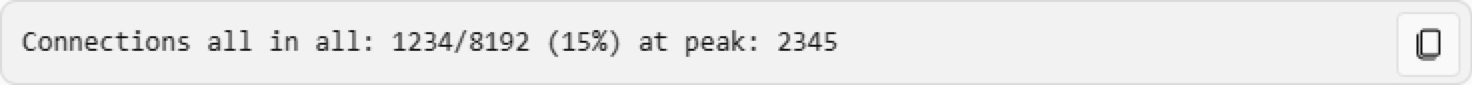
Correct Answer: C
Section:
Explanation:
R81.20 management server can manage gateways with versions R75.20 and higher. However, some features may not be supported on older gateway versions. For example, R81 introduces a new feature called Infinity Threat Prevention, which requires R81 gateways to work 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 68
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 69
Which of the following statements is TRUE about R81 management plug-ins?

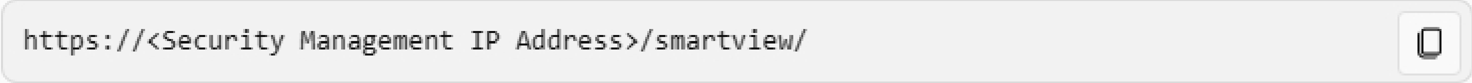
A. The plug-in is a package installed on the Security Gateway.
B. Installing a management plug-in requires a Snapshot, just like any upgrade process.
C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
D. Using a plug-in offers full 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 70
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/
```

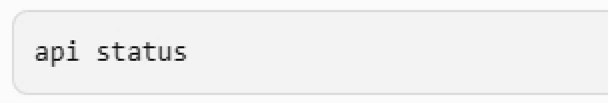
You need to use HTTPS protocol and the default port 443. You also need to enter the IP address of the Security Management Server that hosts the SmartView application. You cannot use the host name of the Security Management Server or a different port number.
Reference:SmartView R81 Administration Guide

QUESTION 71
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 72
Where you can see and search records of action done by R81 SmartConsole administrators?

A. In SmartView Tracker, open active log
B. In the Logs & Monitor view, select "Open Audit Log View"
C. In SmartAuditLog View
D. In Smartlog, all logs

Correct Answer: B
Section:
Explanation:
The Audit Log is a feature that records all the actions performed by R81 SmartConsole administrators, such as logging in, logging out, publishing, installing policy, creating objects, modifying rules, etc. You can see and search records of action done by R81 SmartConsole administrators by following these steps:
In SmartConsole, go toLogs & Monitorview.
In the left pane, selectOpen Audit Log View.
In the right pane, you will see a table that shows all the audit log records. You can filter, sort, group, or search the records by using the toolbar options.
You can also double-click on a record to see more details in a pop-up window.
Reference:R81 Logging and Monitoring Administration Guide

QUESTION 73
Fill in the blank: The R81 utility fw monitor is used to troubleshoot _______________________.

A. User data base corruption
B. LDAP conflicts
C. Traffic issues
D. Phase two key negotiations

Correct Answer: C
Section:
Explanation:
Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The FW Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark.

QUESTION 74
The Firewall kernel is replicated multiple times, therefore:

A. The Firewall kernel only touches the packet if the connection is accelerated

B. The Firewall can run different policies per core

C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out

D. The Firewall can run the same policy on all cores.

Correct Answer: D
Section:
Explanation:
On a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated copy, or instance, runs on one processing core. These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel. When CoreXL is enabled, all the kernel instances in the Security Gateway process traffic through the same interfaces and apply the same security policy.

QUESTION 75
Selecting an event displays its configurable properties in the Detail pane and a description of the event in the Description pane. Which is NOT an option to adjust or configure?

A. Severity

B. Automatic reactions

C. Policy

D. Threshold

Correct Answer: C
Section:
Explanation:
An event is a notification that something significant has occurred on a Check Point product or network. Events are generated by various sources, such as blades, gateways, servers, SmartEvent, etc. You can view and manage events in SmartConsole by using theEventstab in theLogs & Monitorview. Selecting an event displays its configurable properties in the Detail pane and a description of the event in the Description pane. The configurable properties include:
Severity: The level of importance or urgency of the event. You can change the severity of an event by selecting a different value from the drop-down list.
Automatic reactions: The actions that are triggered when an event occurs. You can add, edit, or delete automatic reactions for an event by clicking on the+icon or the pencil icon.
Threshold: The minimum number or frequency of occurrences of an event that triggers an automatic reaction. You can change the threshold of an event by entering a different value in the text box.
The policy is not an option to adjust or configure for an event. The policy is a set of rules that define how to handle events based on their source, type, severity, etc. You can create and manage policies in SmartEvent by using thePoliciestab in theLogs & Monitorview.
Reference:R81 Logging and Monitoring Administration Guide

QUESTION 76
To fully enable Dynamic Dispatcher on a Security Gateway:

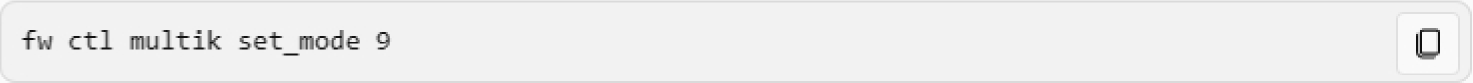
A. run fw ctl multik set_mode 9 in Expert mode and then Reboot.

B. Using cpconfig, update the Dynamic Dispatcher value to ''full'' under the CoreXL menu.

C. Edit/proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot.

D. run fw multik set_mode 1 in Expert mode and then reboot.

Correct Answer: A
Section:
Explanation:
To fully enable Dynamic Dispatcher on a Security Gateway, you need to run the following command in Expert mode then reboot:



```
fw ctl multik set_mode 9
```

This command sets the multi-core mode to 9, which means that Dynamic Dispatcher is enabled without Firewall Priority Queues. Dynamic Dispatcher is a feature that optimizes the performance of Security Gateways with

multiple CPU cores by dynamically allocating traffic to different cores based on their load and priority. Dynamic Dispatcher can improve the throughput and scalability of the Security Gateway, especially for traffic that is not accelerated by SecureXL. The other commands are not valid or do not enable Dynamic Dispatcher.
Reference:R81 Performance Tuning Administration Guide

QUESTION 77
Session unique identifiers are passed to the web api using which http header option?

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

Correct Answer: A
Section:
Explanation:
Session unique identifiers are passed to the web API using theX-chkp-sidHTTP header option. The web API 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. To use the web API, you need to create a session with the management server by sending a login request with your credentials. The management server will respond with a session unique identifier (SID) that represents your session. You need to pass this SID in every subsequent request to the web API using the X-chkp-sid HTTP header option. This way, the management server can identify and authenticate your session and perform the requested operations.
Reference:Check Point R81 REST API Reference Guide

QUESTION 78
Which command shows actual allowed connections in state table?

A. fw tab --t StateTable
B. fw tab --t connections
C. fw tab --t connection
D. fw tab connections

Correct Answer: B
Section:
Explanation:
The correct command to show actual allowed connections in the state table is option B: fw tab --t connections. This command displays the contents of the 'connections' table, which contains information about the active connections being tracked by the firewall.
Option A (fw tab --t StateTable) is incorrect as there is no 'StateTable' table; it should be 'connections.'
Option C (fw tab --t connection) is also incorrect, as it should be 'connections.'
Option D (fw tab connections) is not the correct syntax for the command.

QUESTION 79
What SmartEvent component creates events?

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

Correct Answer: B
Section:

Explanation:
The SmartEvent component that creates events is the Correlation Unit, which is responsible for correlating and analyzing security events to identify patterns and potential threats.
Option A, 'Consolidation Policy,' does not create events but is used to configure policies for event consolidation.
Option C, 'SmartEvent Policy,' is not responsible for creating events but is used to configure policies related to SmartEvent.
Option D, 'SmartEvent GUI,' is the graphical user interface for managing SmartEvent but does not create events itself.

QUESTION 80
Which command collects diagnostic data for analyzing customer setup remotely?

A. cpinfo
B. migrate export
C. sysinfo
D. cpview

Correct Answer: A
Section:
Explanation:
CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).
The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.

QUESTION 81
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 82
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 83
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 84
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 85
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 86
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 87
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 88
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 89
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 90
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 91
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 92
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 93
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 94
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 95
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 96
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 97
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 98
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 99
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 100
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

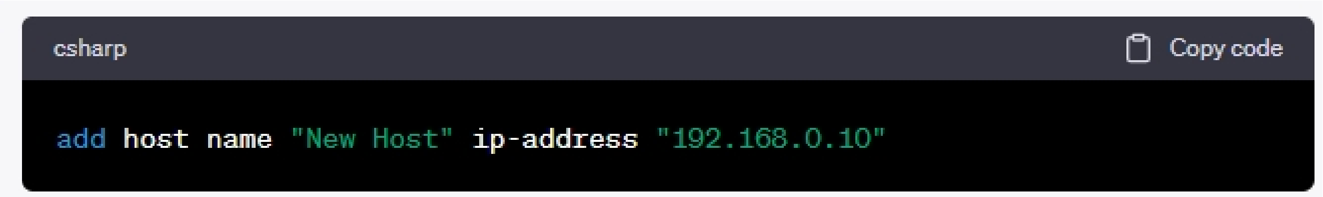
Correct Answer: C
Section:
Explanation:
The configuration file that contains the structure of the Security Server showing the port numbers, corresponding protocol name, and status is $FWDIR/conf/fwauthd.conf. This file is used for configuring authentication services in Check Point Security Servers.

QUESTION 101
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 102
Which command is used to display status information for various components?

A. show all systems
B. show system messages
C. sysmess all
D. show sysenv all

Correct Answer: D
Section:
Explanation:
The command used to display status information for various components is show sysenv all. This command provides comprehensive status information about the system's environment and various components, including hardware and software components. It can be useful for troubleshooting and monitoring the system's health.

QUESTION 103
What are the blades of Threat Prevention?

A. IPS, DLP, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction
B. DLP, AntiVirus, QoS, AntiBot, Sandblast Threat Emulation/Extraction
C. IPS, AntiVirus, AntiBot
D. IPS, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction

Correct Answer: D
Section:
Explanation:
The blades of Threat Prevention in Check Point include:
Intrusion Prevention System (IPS)
AntiVirus
AntiBot
SandBlast Threat Emulation/Extraction
So, the correct answer is D, which includes all the mentioned blades.

QUESTION 104
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 105
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 106
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 107
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 108
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 109
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 110
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 111
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 112
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 113
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 114
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 115
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 116
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 117
Which encryption algorithm is the least secured?

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

Correct Answer: C
Section:
Explanation:
DES (Data Encryption Standard) is a symmetric block cipher that uses a 56-bit key to encrypt and decrypt 64-bit blocks of data. It was developed by IBM in 1975 and adopted by the US government as a standard for encryption. However, DES has been proven to be insecure and vulnerable to various attacks, such as brute force, differential cryptanalysis, and linear cryptanalysis. A brute force attack can break DES in a matter of hours using modern hardware. Differential cryptanalysis can reduce the number of keys to be searched by a factor of four, and linear cryptanalysis can reduce it by a factor of two. Therefore, DES is the least secure encryption algorithm among the options given.

QUESTION 118
What is the command to check the status of the SmartEvent Correlation Unit?

A. fw ctl get int cpsead_stat
B. cpstat cpsead
C. fw ctl stat cpsemd
D. cp_conf get_stat cpsemd

Correct Answer: B
Section:
Explanation:
The SmartEvent Correlation Unit is responsible for analyzing the log entries and identifying events from them.It runs on the Log Server machine or on a dedicated machine1. To check the status of the SmartEvent Correlation Unit, you can use the commandcpstat cpseadon the machine where it is installed.This command will show you information such as the number of logs processed, the number of events generated, the CPU and memory usage, and the status of the connection to the SmartEvent Server23.

QUESTION 119
You need to see which hotfixes are installed on your gateway, which command would you use?

A. cpinfo --h all
B. cpinfo --o hotfix
C. cpinfo --l hotfix
D. cpinfo --y all

Correct Answer: D
Section:
Explanation:
The commandcpinfo --y alldisplays information about all the hotfixes that are installed on the gateway1.This command also shows the hotfix ID, description, installation date, and status for each hotfix2. The other commands are not valid options for this task.The commandcpinfo --h allshows the hardware information of the gateway3. The commandscpinfo --o hotfixandcpinfo --l hotfixdo not exist and will return an error message.

QUESTION 120
: 156
VPN Link Selection will perform the following when the primary VPN link goes down?

A. The Firewall will drop the packets.
B. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.
C. The Firewall will send out the packet on all interfaces.
D. The Firewall will inform the client that the tunnel is down.

Correct Answer: B
Section:
Explanation:
VPN Link Selection is a feature that allows the Security Gateway to select the best link for each VPN tunnel based on the network topology and the Link Selection configuration1.When the primary VPN link goes down, the Firewall can update the Link Selection entries to start using a different link for the same tunnel, as long as the remote peer supports this feature and has multiple IP addresses configured2. This way, the VPN tunnel can be maintained without interruption or renegotiation. The other options are not correct because:

A) The Firewall will not drop the packets, but will try to send them over another link if possible.

C) The Firewall will not send out the packet on all interfaces, but will use the routing table to determine the best interface for each destination.

D) The Firewall will not inform the client that the tunnel is down, but will try to keep the tunnel up by switching to another link.

QUESTION 121
Which of the following links will take you to the SmartView web application?

A. https://<Security Management Server host name>/smartviewweb/
B. https://<Security Management Server IP Address>/smartview/
C. https://<Security Management Server host name>smartviewweb

D. https://<Security Management Server IP Address>/smartview

Correct Answer: B
Section:
Explanation:
The SmartView web application is a web-based interface that allows you to view and analyze logs and events from your Security Gateways and Management Servers1. To access the SmartView web application, you need to use the following link: https://<Security Management Server IP Address>/smartview/. This link will prompt you to enter your credentials and then take you to the SmartView dashboard. The other options are not correct because:
A) The link https://<Security Management Server host name>/smartviewweb/ is missing a slash (/) between the host name and smartviewweb.
C) The link https://<Security Management Server host name>smartviewweb is missing a slash (/) after the host name and before smartviewweb.
D) The link https://<Security Management Server IP Address>/smartview is missing a slash (/) at the end.

QUESTION 122
Which directory below contains log files?

A. /opt/CPSmartlog-R81/log
B. /opt/CPshrd-R81/log
C. /opt/CPsuite-R81/fw1/log
D. /opt/CPsuite-R81/log

Correct Answer: C
Section:
Explanation:
The directory /opt/CPsuite-R81/fw1/log contains the log files for the Security Gateway, such as firewall, VPN, IPS, and anti-virus logs1.These log files can be viewed and analyzed using SmartConsole or SmartView2. The other directories are not correct because:
A)The directory /opt/CPSmartlog-R81/log contains the log files for the SmartLog server, which is a separate component that indexes and searches the logs from multiple Security Gateways3.
B)The directory /opt/CPshrd-R81/log contains the log files for the shared components of the Check Point suite, such as cpwd, cpca, cpd, and cpwatchdog4.
D) The directory /opt/CPsuite-R81/log does not exist by default and is not used for logging purposes.

QUESTION 123
Which GUI client is supported in R81?

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

Correct Answer: C
Section:
Explanation:
SmartView Monitor is a GUI client that is supported in R81.It allows you to monitor the network and security performance of your Security Gateways and devices5.You can use it to view real-time statistics, alerts, logs, reports, and graphs6. The other GUI clients are not supported in R81 because:
A)SmartProvisioning was replaced by SmartLSM in R80.20 and later versions7.SmartLSM is a unified solution for managing large-scale deployments of Security Gateways8.
B)SmartView Tracker was replaced by SmartLog in R80 and later versions9.SmartLog is a powerful log analysis tool that enables fast and easy access to log data from multiple Security Gateways10.
D)SmartLog is not a GUI client, but a web-based application that runs on the Security Management Server or Log Server10. You can access it from any web browser or from SmartConsole.

QUESTION 124
From SecureXL perspective, what are the tree paths of traffic flow:

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

Correct Answer: D
Section:
Explanation:
SecureXL is a technology that improves the performance of Security Gateway by offloading the processing of some packets from the Firewall kernel to the SecureXL device driver1.SecureXL can handle packets in three different paths, depending on the type and state of the packet2:
Firewall Path: This is the slowest path, where packets are processed by the Firewall kernel and all the inspection blades. This path is used for packets that require full inspection, such as the first packet of a connection, packets that match a rule with a UTM blade, or packets that are not eligible for acceleration.
Accelerated Path: This is the fastest path, where packets are processed by the SecureXL device driver and bypass the Firewall kernel. This path is used for packets that belong to an established connection that is marked for acceleration, and do not require any further inspection by the Firewall or other blades.
Medium Path: This is a hybrid path, where packets are processed by both the SecureXL device driver and the Firewall kernel, but skip some inspection steps. This path is used for packets that belong to an established connection that is not marked for acceleration, but do not require full inspection by all the blades.
The other options are not correct because:
A) Initial Path; Medium Path; Accelerated Path: There is no such thing as Initial Path in SecureXL terminology. The initial packet of a connection is always handled by the Firewall Path.
B) Layer Path; Blade Path; Rule Path: These are not paths of traffic flow, but components of the unified policy in R80 and above versions.The Layer Path refers to the order of layers in the policy, the Blade Path refers to the order of blades within a layer, and the Rule Path refers to the order of rules within a blade3.
C) Firewall Path; Accept Path; Drop Path: These are not paths of traffic flow, but possible actions that the Firewall can take on a packet. The Firewall Path is one of the paths of traffic flow, but the Accept Path and Drop Path are not.The Accept Path means that the packet is allowed to pass through the Firewall, and the Drop Path means that the packet is blocked by the Firewall4.

QUESTION 125
To enable Dynamic Dispatch on Security Gateway without the Firewall Priority Queues, run the following command in Expert mode and reboot:

A. fw ctl Dyn_Dispatch on
B. fw ctl Dyn_Dispatch enable
C. fw ctl multik set_mode 4
D. fw ctl multik set_mode 1

Correct Answer: C
Section:
Explanation:
Dynamic Dispatch is a feature that enhances CoreXL performance by dynamically assigning new connections to CoreXL FW instances based on their CPU utilization1.To enable Dynamic Dispatch on Security Gateway without enabling Firewall Priority Queues (FPQ), you need to run the commandfw ctl multik set_mode 4in Expert mode and reboot2. This command will set the CoreXL mode to Dynamic Dispatcher without FPQ. The other options are not correct because:
A) fw ctl Dyn_Dispatch on: This command does not exist and will return an error message.
B) fw ctl Dyn_Dispatch enable: This command does not exist and will return an error message.
D)fw ctl multik set_mode 1: This command will set the CoreXL mode to Static Dispatcher without FPQ, which is the default mode2. This mode will use a static hash function to assign new connections to CoreXL FW instances based on their IP addresses and protocol.

QUESTION 126
What is the protocol and port used for Health Check and State Synchronization in ClusterXL?

A. CCP and 18190
B. CCP and 257

C. CCP and 8116

D. CPC and 8116

Correct Answer: C
Section:
Explanation:
ClusterXL is a clustering technology that provides high availability and load sharing for Security Gateways. ClusterXL uses a proprietary protocol called Check Point Cluster Protocol (CCP) to communicate between cluster members. CCP has two main functions: Health Check and State Synchronization. Health Check is the mechanism that monitors the status and availability of each cluster member and determines which member is the active one. State Synchronization is the mechanism that synchronizes the connection and NAT tables between cluster members to ensure a smooth failover in case of a member failure. CCP uses UDP port 8116 for both Health Check and State Synchronization messages. The other options are not correct because:
A) CCP and 18190: This option is incorrect because CCP does not use port 18190. Port 18190 is used by Secure Internal Communication (SIC) between Security Gateways and Management Servers.
B) CCP and 257: This option is incorrect because CCP does not use port 257. Port 257 is used by Check Point Security Management Protocol (CPM) for communication between SmartConsole and Management Servers.
D) CPC and 8116: This option is incorrect because there is no such protocol as CPC in ClusterXL.

QUESTION 127
Which command shows the current connections distributed by CoreXL FW instances?

A. fw ctl multik stat

B. fw ctl affinity -l

C. fw ctl instances -v

D. fw ctl iflist

Correct Answer: A
Section:
Explanation:
CoreXL is a performance-enhancing technology that enables the processing CPU cores to concurrently perform multiple tasks on Security Gateways with multiple CPU cores. CoreXL replicates the Firewall kernel multiple times, creating multiple Firewall instances that run on different CPU cores. These Firewall instances handle traffic concurrently, and each Firewall instance is a complete and independent Firewall inspection kernel. To show the current connections distributed by CoreXL FW instances, you can use the commandfw ctl multik staton the Security Gateway. This command will display information such as the number of connections, packets, bytes, drops, and errors handled by each CoreXL FW instance, as well as the CPU utilization and affinity of each instance. The other options are not correct because:
B) fw ctl affinity -l: This command will show the CPU affinity of all processes and IRQs on the Security Gateway. It will not show the current connections distributed by CoreXL FW instances.
C) fw ctl instances -v: This command will show the details of all CoreXL FW instances on the Security Gateway, such as their ID, type, state, priority, and interfaces. It will not show the current connections distributed by CoreXL FW instances.
D) fw ctl iflist: This command will show the list of all interfaces on the Security Gateway, along with their names

QUESTION 128
What is the purpose of extended master key extension/session hash?

A. UDP VOIP protocol extension

B. In case of TLS1.x it is a prevention of a Man-in-the-Middle attack/disclosure of the client-server communication

C. Special TCP handshaking extension

D. Supplement DLP data watermark

Correct Answer: B
Section:
Explanation:
The extended master key extension/session hash is a feature introduced in TLS 1.3 to prevent a Man-in-the-Middle attack/disclosure of the client-server communication. It works by generating a unique session hash for each connection, which is derived from the master key and other parameters. This session hash is then used to authenticate the application data and the end-of-handshake messages, ensuring that no one can tamper with or eavesdrop on the communication.

Reference:Check Point Security Expert R81 Course, TLS 1.3 RFC

QUESTION 129
In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Wire Mode configuration, chain modules marked with ____________ will not apply.

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

Correct Answer: B
Section:
Explanation:
In the Check Point Firewall Kernel Module, each kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Wire Mode configuration, chain modules marked with 1 will not apply, as they are related to NAT, VPN, or other features that are not supported in Wire Mode. Wire Mode is a mode of operation that allows transparent traffic forwarding without any inspection or modification by the firewall.
Reference:Check Point Security Expert R81 Course, Wire Mode Configuration Guide

QUESTION 130
Which one of the following is true about Capsule Connect?

A. It is a full layer 3 VPN client
B. It offers full enterprise mobility management
C. It is supported only on iOS phones and Windows PCs
D. It does not support all VPN authentication methods

Correct Answer: A
Section:
Explanation:
Capsule Connect is a full layer 3 VPN client that provides secure and seamless remote access to corporate networks from iOS and Android devices. It supports all VPN authentication methods, such as certificates, passwords, tokens, and challenge-response. It also supports split tunneling and seamless roaming.
Reference:Capsule Connect Datasheet,Capsule Connect Administration Guide

QUESTION 131
How often does Threat Emulation download packages by default?

A. Once a week
B. Once an hour
C. Twice per day
D. Once per day

Correct Answer: D
Section:
Explanation:
Threat Emulation downloads packages by default once per day. The packages contain updates for the Threat Emulation engine, signatures, and images. The download frequency can be changed in the Threat Prevention policy settings.
Reference:Threat Emulation Administration Guide,Threat Prevention R81 Release Notes

QUESTION 132

You are investigating issues with to gateway cluster members are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?

A. TCP port 443

B. TCP port 257

C. TCP port 256

D. UDP port 8116

Correct Answer: C
Section:
Explanation:
The FWD daemon uses TCP port 256 to do a Full Synchronization between gateway cluster members. This port is also used for other synchronization types, such as Delta Synchronization and Accelerated Synchronization. The FWD daemon is responsible for synchronizing the connections table, NAT table, and VPN keys between cluster members.
Reference: ClusterXL Administration Guide, SK25977 - Ports Used by Check Point Software

QUESTION 133

Which statement is true about ClusterXL?

A. Supports Dynamic Routing (Unicast and Multicast)

B. Supports Dynamic Routing (Unicast Only)

C. Supports Dynamic Routing (Multicast Only)

D. Does not support Dynamic Routing

Correct Answer: A
Section:
Explanation:
ClusterXL supports Dynamic Routing for both Unicast and Multicast traffic. Dynamic Routing protocols, such as OSPF, BGP, or PIM, can be configured on cluster members to exchange routing information with other routers.
ClusterXL supports two modes of operation for Dynamic Routing: New Mode and Legacy Mode.
Reference: ClusterXL Administration Guide, SK98226 - ClusterXL New Mode Overview

QUESTION 134

Which command shows detailed information about VPN tunnels?

A. cat $FWDIR/conf/vpn.conf

B. vpn tu tlist

C. vpn tu

D. cpview

Correct Answer: B
Section:
Explanation:
The command vpn tu tlist shows detailed information about VPN tunnels, such as the peer IP address, encryption domain, IKE phase 1 and phase 2 status, encryption algorithm, and tunnel uptime. The command vpn tu is an interactive tool that allows users to list, delete, or reconnect VPN tunnels. The command cpview is a real-time performance monitoring tool that shows various statistics about the system and network.
Reference: VPN Administration Guide, SK97638 - What is cpview Utility and How to Use it

QUESTION 135

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 136
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 137
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 138
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 139
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 140
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 141
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 142
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 143
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 144
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 145
What is the port used for SmartConsole to connect to the Security Management Server?

A. CPMI port 18191/TCP

B. CPM port/TCP port 19009

C. SIC port 18191/TCP

D. https port 4434/TCP

Correct Answer: A
Section:
Explanation:
The port used for SmartConsole to connect to the Security Management Server is CPMI port 18191/TCP. CPMI stands for Check Point Management Interface, which is a proprietary protocol that enables secure communication between the SmartConsole and the Security Management Server. CPMI uses SSL encryption and authentication to protect the data exchange.
Reference:Check Point Security Expert R81 Course,SK52421 - Ports used by Check Point software

QUESTION 146
What is considered Hybrid Emulation Mode?

A. Manual configuration of file types on emulation location.

B. Load sharing of emulation between an on premise appliance and the cloud.

C. Load sharing between OS behavior and CPU Level emulation.

D. High availability between the local SandBlast appliance and the cloud.

Correct Answer: B
Section:
Explanation:
Hybrid Emulation Mode is a mode of operation that allows load sharing of emulation between an on premise appliance and the cloud. Emulation is a process that analyzes files for malicious behavior by running them in a virtual sandbox. Hybrid Emulation Mode enables you to optimize the performance and scalability of your Threat Emulation solution by distributing the emulation workload between your local SandBlast appliance and the Check Point cloud service.
Reference:Check Point Security Expert R81 Course,Threat Emulation Administration Guide

QUESTION 147
When setting up an externally managed log server, what is one item that will not be configured on the R81 Security Management Server?

A. IP

B. SIC

C. NAT

D. FQDN

Correct Answer: C
Section:
Explanation:
NAT (Network Address Translation) is one item that will not be configured on the R81 Security Management Server when setting up an externally managed log server. NAT is a technique that allows devices with private IP addresses to communicate with devices with public IP addresses by translating the private addresses to public ones. NAT is not relevant for configuring an externally managed log server, which requires only the IP address, SIC (Secure Internal Communication), and FQDN (Fully Qualified Domain Name) of the log server.
Reference:Check Point Security Expert R81 Course,Logging and Monitoring Administration Guide

QUESTION 148
Customer's R81 management server needs to be upgraded to R81.20. What is the best upgrade method when the management server is not connected to the Internet?

A. Export R81 configuration, clean install R81.20 and import the configuration

B. CPUSE offline upgrade

C. CPUSE online upgrade

D. SmartUpdate upgrade

Correct Answer: C
Section:
Explanation:
CPUSE offline upgrade is the best upgrade method when the management server is not connected to the Internet. CPUSE (Check Point Upgrade Service Engine) is a tool that automates the process of upgrading and installing software packages on Check Point devices. CPUSE can work in online mode or offline mode. Online mode requires an Internet connection to download the packages from Check Point servers. Offline mode allows you to download the packages manually from another device and transfer them to the management server using a USB drive or SCP.
Reference:Check Point Security Expert R81 Course, CPUSE Administration Guide

QUESTION 149
When installing a dedicated R81 SmartEvent server. What is the recommended size of the root partition?

A. Any size

B. Less than 20GB

C. More than 10GB and less than 20GB

D. At least 20GB

Correct Answer: D
Section:
Explanation:
At least 20GB is the recommended size of the root partition when installing a dedicated R81 SmartEvent server. The root partition is the primary partition that contains the operating system files and other essential files for booting and running the system. The SmartEvent server requires at least 20GB of free space on the root partition to install and operate properly. If the root partition size is less than 20GB, you may encounter errors or performance issues with SmartEvent.
Reference:Check Point Security Expert R81 Course, SmartEvent Administration Guide

QUESTION 150
As an administrator, you may be required to add the company logo to reports. To do this, you would save the logo as a PNG file with the name 'cover-company-logo.png' and then copy that image file to which directory on the SmartEvent server?

A. SFWDIR/smartevent/conf

B. $RTDIR/smartevent/conf
C. $RTDIR/smartview/conf
D. $FWDIR/smartview/conf

Correct Answer: C
Section:
Explanation:
To add the company logo to reports, you would save the logo as a PNG file with the name 'cover-company-logo.png' and then copy that image file to the $RTDIR/smartview/conf directory on the SmartEvent server. The $RTDIR is an environment variable that points to the runtime directory of the SmartEvent server, which is usually /opt/CPrt-R81. The smartview/conf directory contains the configuration files for SmartView, which is a web-based interface for viewing reports and dashboards generated by SmartEvent.
Reference:SmartEvent Administration Guide,SK120193 - How to add a company logo to SmartView reports

QUESTION 151
Which one of the following is true about Threat Extraction?

A. Always delivers a file to user
B. Works on all MS Office, Executables, and PDF files
C. Can take up to 3 minutes to complete
D. Delivers file only if no threats found

Correct Answer: A
Section:
Explanation:
Threat Extraction is a software blade that always delivers a file to user. 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. Threat Extraction works on MS Office, PDF, and archive files, but not on executables. Threat Extraction can take up to 3 minutes to complete, depending on the file size and complexity.
Reference:Check Point Security Expert R81 Course,Threat Extraction Administration Guide

QUESTION 152
Which one of the following is true about Threat Emulation?

A. Takes less than a second to complete
B. Works on MS Office and PDF files only
C. Always delivers a file
D. Takes minutes to complete (less than 3 minutes)

Correct Answer: D
Section:
Explanation:
Threat Emulation is a software blade that takes minutes to complete (less than 3 minutes). Threat Emulation analyzes files for malicious behavior by running them in a virtual sandbox. Threat Emulation works on MS Office, PDF, executables, and archive files. Threat Emulation does not always deliver a file, but only if no threats are found or if the user chooses to download the original file after seeing a warning message.
Reference:Check Point Security Expert R81 Course, Threat Emulation Administration Guide

QUESTION 153
Both ClusterXL and VRRP are fully supported by Gaia R81.20 and available to all Check Point appliances. Which the following command is NOT related to redundancy and functions?

A. cphaprob stat
B. cphaprob --a if

C. cphaprob --l list

D. cphaprob all show stat

Correct Answer: D
Section:
Explanation:
The command cphaprob all show stat is not related to redundancy and functions. This command does not exist in ClusterXL or VRRP. The other commands are valid commands for checking the status of cluster members, interfaces, and synchronization. ClusterXL and VRRP are both high availability solutions that provide redundancy and load balancing for Check Point gateways.
Reference:Check Point Security Expert R81 Course, ClusterXL Administration Guide, VRRP Administration Guide

QUESTION 154
What is the purpose of a SmartEvent Correlation Unit?

A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server.

B. The SmartEvent Correlation Unit's task it to assign severity levels to the identified events.

C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.

D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server.

Correct Answer: C
Section:
Explanation:
The purpose of a SmartEvent Correlation Unit is to evaluate logs from the log server component to identify patterns/threats and convert them to events. The SmartEvent Correlation Unit is a software module that runs on the SmartEvent server or on a dedicated server. It applies correlation rules and logic to the logs received from various sources, such as security gateways, endpoints, or third-party devices. It then generates events that represent security incidents or trends that require attention or action.
Reference:Check Point Security Expert R81 Course,SmartEvent Administration Guide

QUESTION 155
What are the main stages of a policy installations?

A. Verification & Compilation, Transfer and Commit

B. Verification & Compilation, Transfer and Installation

C. Verification, Commit, Installation

D. Verification, Compilation & Transfer, Installation

Correct Answer: A
Section:
Explanation:
The main stages of a policy installation are Verification & Compilation, Transfer and Commit. Verification & Compilation is the stage where the Security Management Server checks the validity and consistency of the policy and compiles it into a binary format. Transfer is the stage where the compiled policy is sent to the Security Gateways over a secure channel. Commit is the stage where the Security Gateways activate the new policy and update their connections table accordingly.
Reference:Check Point Security Expert R81 Course,Policy Installation Process

QUESTION 156
What is a best practice before starting to troubleshoot using the ''fw monitor'' tool?

A. Run the command: fw monitor debug on

B. Clear the connections table

C. Disable CoreXL

D. Disable SecureXL

Correct Answer: D
Section:
Explanation:
A best practice before starting to troubleshoot using the fw monitor tool is to disable SecureXL. SecureXL is a performance acceleration solution that optimizes the packet flow through the Security Gateway. However, SecureXL can also bypass some inspection points and cause some packets to be invisible to fw monitor. Therefore, disabling SecureXL can ensure that fw monitor captures all the relevant packets for troubleshooting purposes.
Reference:Check Point Security Expert R81 Course,fw monitor,SecureXL

QUESTION 157
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 158
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 159
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 160
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 161
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 162
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 163
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 164
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 165
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 166
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 167
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 168
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 169
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 170
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 171
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 172
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 173
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 174
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 175
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 176
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 177
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 178
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 179
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 180
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 181
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 182
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 183
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 184
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 185
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 186
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 187
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 188
When using CPSTAT, what is the default port used by the AMON server?

A. 18191
B. 18192
C. 18194
D. 18190

Correct Answer: B
Section:
Explanation:
The default port used by the AMON server when using CPSTAT is 18192. CPSTAT is a command-line tool that allows administrators to monitor various statistics and status information about Check Point products and components, such as CPU usage, memory usage, policy installation, cluster state, etc. CPSTAT uses AMON (Advanced Monitoring) protocol to communicate with AMON server, which is a daemon that runs on Security Gateways or Management Servers and collects and provides AMON data. By default, AMON server listens on TCP port 18192 for incoming CPSTAT requests.

QUESTION 189
Which of the following is NOT an internal/native Check Point command?

A. fwaccel on
B. fw ct1 debug
C. tcpdump
D. cphaprob

Correct Answer: C
Section:
Explanation:
The commandtcpdumpis not an internal/native Check Point command. It is a common command-line tool that captures and analyzes network traffic. The other commands are internal/native Check Point commands that perform various functions. For example:
fwaccel onenables SecureXL acceleration on the Security Gateway.
fw ctl debugsets the debug flags for the Firewall kernel module.
cphaprobdisplays the status and information about ClusterXL or VRRP members.

QUESTION 190
What are the minimum open server hardware requirements for a Security Management Server/Standalone in R81?

A. 2 CPU cores, 4GB of RAM and 15GB of disk space
B. 8 CPU cores, 16GB of RAM and 500 GB of disk space
C. 4 CPU cores, 8GB of RAM and 500GB of disk space
D. 8 CPU cores, 32GB of RAM and 1 TB of disk space

Correct Answer: C
Section:
Explanation:
The minimum open server hardware requirements for a Security Management Server/Standalone in R81 are:
CPU: Intel Core i5-4590 or equivalent (4 cores)
Memory: 8 GB RAM
Disk space: 500 GB
The other options do not match the minimum requirements. Option A has insufficient CPU cores, memory and disk space. Option B has excessive CPU cores and disk space. Option D has excessive CPU cores, memory and disk space.

QUESTION 191
The ''MAC magic'' value must be modified under the following condition:

A. There is more than one cluster connected to the same VLAN
B. A firewall cluster is configured to use Multicast for CCP traffic
C. There are more than two members in a firewall cluster
D. A firewall cluster is configured to use Broadcast for CCP traffic

Correct Answer: A
Section:
Explanation:
Comprehensive and Detailed Explanation: The ''MAC magic'' value, also known as the ''Cluster Global ID'', is a mechanism that identifies different clusters on the same network segment. It is used to prevent MAC address conflicts and ensure proper load balancing among cluster members. The ''MAC magic'' value is a hexadecimal number that is appended to the virtual MAC address of the cluster interface. By default, the ''MAC magic'' value is set to 1 for all clusters, but it must be changed manually if there is more than one cluster connected to the same VLAN. Otherwise, the clusters will not be able to communicate with each other or with external hosts.
The ''MAC magic'' value does not need to be modified under the other conditions listed in the question. The firewall cluster can use either Broadcast or Multicast for CCP traffic without affecting the ''MAC magic'' value. The number of members in a firewall cluster also does not affect the ''MAC magic'' value, as long as they belong to the same cluster and have the same Cluster Global ID.

QUESTION 192
What is the correct description for the Dynamic Balancing / Split feature?

A. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
B. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND's. The interface must support Multi-Queue. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
C. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND's. The interface must support Multi-Queue. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)
D. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)

Correct Answer: D
Section:
Explanation:
The correct description for the Dynamic Balancing / Split feature is:
Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load.
It is only available on Quantum Appliances (not on Quantum Spark or Open Server)
The Dynamic Balancing / Split feature is a performance-enhancing daemon that balances the load between CoreXL SNDs and CoreXL Firewalls. It monitors the average CPU utilization of CoreXL Firewall and SND instances and automatically increases or decreases the number of CoreXL Firewall instances.The Dynamic Balancing Daemon (dsd) has three stages in each iteration: Examine the current CPU utilization, Calculate the optimal split, and Apply the new split1.
The Dynamic Balancing / Split feature is supported on Check Point Appliances, such as Quantum Appliances, Quantum Maestro, Quantum Security Gateways, and Quantum LightSpeed Appliances in KPPAK mode2. It is not supported on Quantum Spark appliances, which are designed for small and medium businesses. It is also not supported on Open Server platforms, which are general-purpose servers that run Check Point software on top of third-party operating systems.

QUESTION 193
Which command shows the current Security Gateway Firewall chain?

A. show current chain
B. show firewall chain
C. fw ctl chain
D. fw ctl firewall-chain

Correct Answer: C
Section:

QUESTION 194
You want to allow your Mobile Access Users to connect to an internal file share. Adding the Mobile Application 'File Share' to your Access Control Policy in the SmartConsole didn't work. You will be only allowed to select Services for the 'Service & Application' column How to fix it?

A. A Quantum Spark Appliance is selected as Installation Target for the policy packet.
B. The Mobile Access Blade is not enabled for the Access Control Layer of the policy.
C. The Mobile Access Policy Source under Gateway properties Is set to Legacy Policy and not to Unified Access Policy.
D. The Mobile Access Blade is not enabled under Gateway properties.

Correct Answer: C
Section:

QUESTION 195
What are not possible commands to acquire the lock in order to make changes in Clish or Web GUI?

A. set config-lock on override
B. Click the Lock icon in the WebUI
C. 'set rbac rw = 1''
D. lock database override

Correct Answer: C
Section:

QUESTION 196
When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

A. Syslog
B. SNMPTrap
C. Block Source
D. Mail

Correct Answer: B
Section:

QUESTION 197

What is the recommended way to have a redundant Sync connection between the cluster nodes?

A. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define two Sync interfaces per node. Connect both Sync interfaces without using a switch.
B. Use a group of bonded interfaces. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define a Virtual IP for the Sync interface.
C. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define two Sync interfaces per node. Use two different Switches to connect both Sync interfaces.
D. Use a group of bonded interfaces connected to different switches. Define a dedicated sync interface, only one interface per node using the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management.

Correct Answer: D
Section:
Explanation:
The recommended way to have a redundant Sync connection between the cluster nodes is to use a group of bonded interfaces connected to different switches. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management, you should define a dedicated sync interface, only one interface per node.

QUESTION 198
There are multiple types of licenses for the various VPN components and types. License type related to management and functioning of Remote Access VPNs are - which of the following license requirement statement is NOT true:

A. MobileAccessLicense This license is required on the Security Gateway for the following Remote Access solutions
B. EndpointPolicyManagementLicense The Endpoint Security Suite includes blades other than the Remote Access VPN, hence this license is required to manage the suite
C. EndpointContainerLicense The Endpoint Software Blade Licenses does not require an Endpoint Container License as the base
D. IPSecVPNLicense * This license is installed on the VPN Gateway and is a basic requirement for a Remote Access VPN solution

Correct Answer: C
Section:
Explanation:
The Endpoint Policy Management License is required for managing the Endpoint Security Suite, which includes blades such as the Remote Access VPN. The IPSec VPN License is installed on the VPN Gateway and is a basic requirement for a Remote Access VPN solution. The MobileAccessLicense is required on the Security Gateway for the following Remote Access solutions.

QUESTION 199
What is false regarding a Management HA environment?

A. Only one Management Server should be active, while any others be in standby mode
B. It is not necessary to establish SIC between the primary and secondary management server, since the latter gets the exact same copy of the management database from the prior.
C. SmartConsole can connect to any management server in Readonly mode.
D. Synchronization will occur automatically with each Publish event if the Standby servers are available.

Correct Answer: B
Section:
Explanation:
It is false that it is not necessary to establish SIC between the primary and secondary management server, since the latter gets the exact same copy of the management database from the prior. In fact, SIC is required between the primary and secondary management server for Management HA to work properly. SIC ensures secure communication between the management servers and allows the standby server to receive updates from the active server. Without SIC, the standby server will not be able to synchronize with the active server and will not be ready to take over in case of a failover.
Solved: Management HA - Check Point CheckMates, section ''Synchronizing Active and Standby Servers''
CheckPoint Management Server R81 HA Configuration | Udemy, section ''How to set it up in the PNET lab environment''
Check Point R81, section ''Management High Availability''

QUESTION 200

Which Check Point process provides logging services, such as forwarding logs from Gateway to Log Server, providing Log Export API (LEA) & Event Logging API (EL-A) services.

A. DASSERVICE
B. FWD
C. CPVIEWD
D. CPD

Correct Answer: B
Section:
Explanation:
The FWD process provides logging services, such as forwarding logs from Gateway to Log Server, providing Log Export API (LEA) and Event Logging API (EL-A) services. The FWD process is responsible for sending logs from the Security Gateway to the Security Management Server or Log Server, and for fetching logs from the Security Management Server or Log Server to SmartConsole. The FWD process also handles the communication with external logging applications that use the LEA or EL-A protocols.
FWD process does not work after reboot - Check Point CheckMates, section ''FWD process does not work after reboot''
Check Point R81, section ''Logging and Monitoring''
CoreXL Dynamic Dispatcher - Check Point Software, section ''Example of output''

QUESTION 201
Which process handles connection from SmartConsole R81?

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

Correct Answer: C
Section:
Explanation:
The CPM process handles connection from SmartConsole R81. The CPM process is the main process of the Security Management Server and the Multi-Domain Security Management Server. It is responsible for managing the database, handling policy installation, communicating with SmartConsole clients, and providing REST API services. The CPM process runs on port 19009 and uses the CPD process as a proxy for communication with other processes.
Check Point Processes and Daemons, section ''CPM''
Check Point R81, section ''SmartConsole''
Check Point R81.20, section ''REST API''

QUESTION 202
Which of the following Central Deployment is NOT a limitation in R81.20 SmartConsole?

A. Security Gateway Clusters in Load Sharing mode
B. Dedicated Log Server
C. Dedicated SmartEvent Server
D. Security Gateways/Clusters in ClusterXL HA new mode

Correct Answer: A
Section:
Explanation:
Security Gateway Clusters in Load Sharing mode are not supported by the Central Deployment feature in R81.20 SmartConsole.According to the Check Point R81.20 Known Limitations article1, Central Deployment in SmartConsole does not support:

Connection from SmartConsole Client to the Management Server through a proxy server. In this case, use the applicable API command
ClusterXL in Load Sharing mode
VRRP Cluster
Installation of a package on a VSX VSLS Cluster that contains more than 3 members.
On Multi-Domain Servers: Global Domain, or the MDS context
Standalone server
Standby Security Management Server or Multi-Domain Security Management
Scalable Platforms 40000 / 60000
SMB Appliances
The other options are supported by the Central Deployment feature in R81.20 SmartConsole. Dedicated Log Server, Dedicated SmartEvent Server, and Security Gateways/Clusters in ClusterXL HA new mode can be selected as targets for installing packages using the Central Deployment wizard.

QUESTION 203
What is 'Accelerated Policy Installation'?

A. Starting R81, the Desktop Security Policy installation process is accelerated thereby reducing the duration of the process significantly
B. Starting R81, the QoS Policy installation process is accelerated thereby reducing the duration of the process significantly
C. Starting R81, the Access Control Policy installation process is accelerated thereby reducing the duration of the process significantly
D. Starting R81, the Threat Prevention Policy installation process is accelerated thereby reducing the duration of the process significantly

Correct Answer: C
Section:
Explanation:
Starting R81, the Access Control Policy installation process is accelerated thereby reducing the duration of the process significantly.According to the Check Point R81 Security Management Administration Guide1, Accelerated Install Policy is a new feature in R81 that optimizes common use-cases and drastically speeds up the installation with up to 90% improvement. Policy installation is accelerated depending on the changes that were made to the Access Control policy since the last installation. When the policy installation is accelerated, the icon will appear under the ''Install Policy Acceleration'' column in the Install Policy window.
Accelerated Install Policy - Check Point Software, section ''Accelerated Install Policy''

QUESTION 204
What is Dynamic Balancing?

A. It is a ClusterXL feature that switches an HA cluster into an LS cluster if required to maximize throughput
B. It is a feature that uses a daemon to balance the required number of firewall instances and SNDs based on the current load
C. It is a new feature that is capable of dynamically reserve the amount of Hash kernel memory to reflect the resource usage necessary for maximizing the session rate.
D. It is a CoreXL feature that assigns the SND to network interfaces to balance the RX Cache of the interfaces

Correct Answer: B
Section:
Explanation:
Dynamic Balancing is a feature that uses a daemon to balance the required number of firewall instances and SNDs based on the current load. It dynamically changes the split between CoreXL SNDs and CoreXL Firewalls and does not require a reboot or cause an outage. It monitors the system and makes changes as needed to optimize the performance of the Security Gateway. It is supported on Check Point Appliances with R80.40 and higher versions.
Reference:Dynamic Balancing for CoreXL - Check Point Software,Dynamic Balancing available on R80.40 - Check Point CheckMates,CLI R81.20 Reference Guide - Check Point Software,Performance Tuning R81.20 Administration Guide - Check Point Software

QUESTION 205
What is false regarding prerequisites for the Central Deployment usage?

A. The administrator must have write permission on SmartUpdate
B. Security Gateway must have the latest CPUSE Deployment Agent
C. No need to establish SIC between gateways and the management server, since the CDT tool will take care about SIC automatically.
D. The Security Gateway must have a policy installed

Correct Answer: C
Section:
Explanation:
Establishing SIC between gateways and the management server is a prerequisite for Central Deployment usage, as the CDT tool will not take care of this automatically1.The administrator must have write permission on SmartUpdate, the Security Gateway must have the latest CPUSE Deployment Agent, and the Security Gateway must have a policy installed2.These are the basic requirements for using the Central Deployment Tool (CDT), which is a utility that lets you manage a deployment of software packages from your Management Server to the multiple managed Security gateways and cluster members at the same time2.The CDT can perform various actions, such as installation of software packages, taking snapshots, running shell scripts, pushing/pulling files, and automating the RMA backup and restore process2.The CDT is supported on Check Point Appliances with R80.40 and higher versions2.
Reference:How to keep your Security Gateways up to date - Check Point Software,Central Deployment Tool (CDT) - Check Point CheckMates.

QUESTION 206
Main Mode in IKEv1 uses how many packages for negotiation?

A. 4
B. depends on the make of the peer gateway
C. 3
D. 6

Correct Answer: D
Section:
Explanation:
Main Mode in IKEv1 usessix packetsfor negotiation1. Main Mode is the default mode for IKE phase I, which establishes a secure channel between the peers.Main Mode performs the following steps2:
The peers exchange their security policies and agree on a common set of parameters.
The peers generate a shared secret key using the Diffie-Hellman algorithm.
The peers authenticate each other using pre-shared keys, digital signatures, or public key encryption. Main Mode is partially encrypted, from the point at which the shared DH key is known to both peers2.Main Mode provides more security than Aggressive Mode, which uses only three packets for negotiation, but is faster and simpler2.
Reference:Check Point gateways always send main IP address as IKE Main Mode ID - Check Point Software,IPsec and IKE - Check Point Software

QUESTION 207
What component of Management is used tor indexing?

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

Correct Answer: D
Section:
Explanation:
The component of Management that is used for indexing isSOLR1.SOLR is an open source enterprise search platform that provides indexing and searching capabilities for various types of data2.Check Point uses SOLR to index logs, objects, policies, and other data that are stored in the Security Management Server or the Multi-Domain Security Management Server3.SOLR enables fast and efficient searches in SmartConsole, SmartLog, SmartView, and other applications3.SOLR also supports advanced features such as full-text search, faceted search, highlighting, spell checking, and geospatial search2.
Reference:Check Point R81.20 Known Limitations - Check Point Software,SOLR - The Enterprise Search Platform,Check Point R81.20 Logging and Monitoring Administration Guide - Check Point Software

QUESTION 208
What mechanism can ensure that the Security Gateway can communicate with the Management Server with ease in situations with overwhelmed network resources?

A. The corresponding feature is new to R81.20 and is called 'Management Data Plane Separation'
B. The corresponding feature is called 'Dynamic Dispatching'
C. There is a feature for ensuring stable connectivity to the management server and is done via Priority Queuing.
D. The corresponding feature is called 'Dynamic Split'

Correct Answer: A
Section:
Explanation:
The mechanism that can ensure that the Security Gateway can communicate with the Management Server with ease in situations with overwhelmed network resources is calledManagement Data Plane Separation (MDPS)1. MDPS is a feature that allows a Security Gateway to have isolated Management and Data networks. The network system of each domain (plane) is independent and includes interfaces, routes, sockets, and processes. The Management Plane is a domain that accesses, provisions, and monitors the Security Gateway.The Data Plane is a domain that handles all other traffic1.MDPS has the following benefits2:
It improves the performance and stability of the Security Gateway by separating the management traffic from the data traffic.
It enhances the security of the Security Gateway by preventing any packet from crossing between the planes.
It simplifies the network configuration and troubleshooting by having separate routing tables for each plane. MDPS is supported on Check Point Appliances with R80.40 and higher versions1.It is also supported on Quantum Maestro and Quantum Scalable Chassis with R81.20 and higher versions3.MDPS can be configured using Gaia Clish commands or Gaia Portal1.
Reference:Management Data Plane Separation (MDPS) - Check Point Software,Tip of the Week: Management Data Plane Separation - Check Point CheckMates,Management Data Plane Separation (MDPS) on Maestro R81.20 - Check Point Software

QUESTION 209
What a valid SecureXL paths in R81.20?

A. F2F (Slow path). Templated Path. PQX and F2V
B. F2F (Slow path). PXL, QXL and F2V
C. F2F (Slow path), Accelerated Path, PQX and F2V
D. F2F (Slow path), Accelerated Path, Medium Path and F2V

Correct Answer: D
Section:
Explanation:
The valid SecureXL paths in R81.20 areF2F (Slow path), Accelerated Path, Medium Path and F2V1.SecureXL is a technology that accelerates the performance of the Security Gateway by offloading CPU-intensive operations to the SecureXL device2.SecureXL uses different paths to process packets, depending on the type and state of the connection3.The SecureXL paths are3:
F2F (Slow path): This path handles packets that require a full inspection by the Firewall kernel. It is the slowest path, but it supports all features and blades. Examples of packets that use this path are packets that belong to a new connection, packets that match a rule with UTM blades, or packets that require address translation.
Accelerated Path: This path handles packets that belong to an established connection that does not require any further inspection by the Firewall kernel. It is the fastest path, but it supports only a limited set of features and blades. Examples of packets that use this path are packets that match an accept rule with no UTM blades, or packets that match a rule with SecureXL acceleration enabled.
Medium Path: This path handles packets that belong to an established connection that requires some inspection by the Firewall kernel, but not a full inspection. It is faster than the F2F path, but slower than the Accelerated path. It supports more features and blades than the Accelerated path, but less than the F2F path. Examples of packets that use this path are packets that match a rule with IPS or Anti-Bot blades, or packets that require NAT templates.
F2V: This path handles packets that are encapsulated or decapsulated by the VPN kernel. It is faster than the F2F path, but slower than the Accelerated path. It supports VPN features such as encryption, decryption, encapsulation, and decapsulation.
Reference:R81.x Security Gateway Architecture (Logical Packet Flow) - Check Point CheckMates,SecureXL Mechanism in R80.10 and above - Check Point Software,SecureXL - Check Point Software

QUESTION 210
The admin lost access to the Gaia Web Management Interface but he was able to connect via ssh. How can you check if the web service is enabled, running and which port is used?

A. In expert mode run #netstat -tulnp | grep httpd to see if httpd is up and to get the port number. In dish run >show web daemon-enable to see if the web daemon is enabled.
B. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in use. In expert mode run #netstat -anp | grep httpd to see if the httpd is up
C. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in use. In expert mode run #netstat -anp | grep httpd2 to see if the httpd2 is up
D. In expert mode run #netstat -tulnp | grep httpd2 to see if httpd2 is up and to get the port number. In dish run >show web daemon-enable to see if the web daemon is enabled.

Correct Answer: C
Section:
Explanation:
The correct way to check if the web service is enabled, running and which port is used is to use option C. In dish, runshow web ssl-portto see if the web daemon is enabled and which port is in use.In expert mode, runnetstat -anp | grep httpd2to see if the httpd2 is up1.The httpd2 service is responsible for the Gaia Web Management Interface2.If the web daemon is disabled, you can enable it by runningset web daemon-enable onin dish3.If the httpd2 service is down, you can start it by runningservice httpd2 startin expert mode4.
Reference:Gaia WebUI and CLI - Check Point CheckMates,Gaia R81.20 Administration Guide - Check Point Software,Gaia R81 Administration Guide - Check Point Software,How to restart Gaia Portal (WebUI) process - Check Point Software

QUESTION 211
A user complains that some Internet resources are not available. The Administrator is having issues seeing it packets are being dropped at the firewall (not seeing drops in logs). What is the solution to troubleshoot the issue?

A. run fw unloadlocal' on the relevant gateway and check the ping again
B. run 'cpstop' on the relevant gateway and check the ping again
C. run ''fw log' on the relevant gateway
D. run ''fw ctl zdebug drop' on the relevant gateway

Correct Answer: D
Section:
Explanation:
The solution to troubleshoot the issue of some Internet resources being unavailable is to runfw ctl zdebug dropon the relevant gateway1.This command lists all dropped packets in real time and explains the reasons for the drop2.It is a powerful tool that can help diagnose connectivity problems and firewall policy issues3.To use this command, you need to access the gateway in expert mode and runfw ctl zdebug + drop2.You can also filter the output by using grep with an IP address or a keyword, for example:fw ctl zdebug + drop | grep 10.10.10.10orfw ctl zdebug + drop | grep SYN3.This command is a wrapper for the full debugs, and it will run the debug commands for you and will allow you to run debug from one debug module only4.By default, it will use a small debug buffer but if you wish, you can provide the-bufoption to use your own size4.To stop the command, press Ctrl+C and then runfw ctl debug 0to reset the debug state3.
Note: Running this command may affect the performance of the firewall, so use it with caution and only when necessary3.
Reference:Solved: is it possible /supported to run fw ctl zdebug on ... - Check ...,How to use the fw ctl zdebug command to view drops on the Security Gateway,Troubleshooting dropped packets in Checkpoint using zdebug,''fw ctl zdebug'' - Helpful Command Combinations - Check Point CheckMates

QUESTION 212
What are possible Automatic Reactions in SmartEvent?

A. Mail. SNMP Trap, Block Source. Block Event Activity, External Script
B. Web Mail. Block Destination, SNMP Trap. SmartTask
C. Web Mail, Block Service. SNMP Trap. SmartTask, Geo Protection
D. Web Mail, Forward to SandBlast Appliance, SNMP Trap, External Script

Correct Answer: A
Section:
Explanation:
The possible Automatic Reactions in SmartEvent areMail, SNMP Trap, Block Source, Block Event Activity, and External Script1.Automatic Reactions are actions that SmartEvent can perform automatically when a specific event occurs2.They can help you respond quickly and efficiently to security incidents and threats2.The Automatic Reactions are1:
Mail: This reaction sends an email notification to a specified recipient with the details of the event. You can customize the subject and the body of the email, and use variables to include relevant information.

SNMP Trap: This reaction sends an SNMP trap to a specified SNMP server with the details of the event. You can customize the OID and the community string of the trap, and use variables to include relevant information.
Block Source: This reaction blocks the source IP address of the event from accessing your network for a specified duration. You can choose to block the source on all gateways or on specific gateways. You can also choose to block the source on a specific port or service.
Block Event Activity: This reaction blocks the specific activity that triggered the event from occurring again for a specified duration. You can choose to block the activity on all gateways or on specific gateways. You can also choose to block the activity on a specific port or service.
External Script: This reaction runs an external script on a specified server with the details of the event as arguments. You can use any script that can be executed by the operating system of the server, such as bash, perl, python, etc. You can use variables to include relevant information in the script arguments.

QUESTION 213
Which of the following processes pulls the application monitoring status from gateways?

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

Correct Answer: A
Section:
Explanation:
The process that pulls the application monitoring status from gateways iscpd1.The cpd process is responsible for the communication between the Security Management Server and the Security Gateway2.It handles tasks such as policy installation, status reporting, logging, and synchronization2.The cpd process also monitors the application status of the Security Gateway, such as CPU, memory, disk space, and processes3.The cpd process sends this information to the Security Management Server, which displays it in SmartConsole and SmartView Monitor3.

QUESTION 214
Which of the following statements about SecureXL NAT Templates is true?

A. NAT Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup. These are enabled by default and work only if Accept Templates are enabled.
B. DROP Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup. These are disabled by default and work only if NAT Templates are disabled.
C. NAT Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup. These are disabled by default and work only if Accept Templates are disabled.
D. ACCEPT Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup. These are disabled by default and work only if NAT Templates are disabled.

Correct Answer: A
Section:
Explanation:
NAT Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup.These are enabled by default and work only if Accept Templates are enabled1.According to the web search results, NAT Templates are a feature of SecureXL that accelerates the performance of the Security Gateway by offloading CPU-intensive operations to the SecureXL device2.NAT Templates are supported for Static NAT and Hide NAT using the existing SecureXL Templates mechanism1.NAT Templates are disabled by default on Check Point Security Gateway R80.10 and below, but they are not relevant to SecureXL in versions R80.20 and above, as all template handling has moved to the Firewall1.NAT Templates can be enabled or disabled by setting the relevant kernel parameters in $FWDIR/boot/modules/fwkern.conf file1.

QUESTION 215
Is it possible to establish a VPN before the user login to the Endpoint Client?

A. yes, you had to set neo_remember_user_password to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_remember_user_password attribute in the trac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway

B. no, the user must login first.

C. yes. you had to set neo_always_connected to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_always_connected attribute in the trac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway

D. yes, you had to enable Machine Authentication in the Gateway object of the Smart Console

Correct Answer: D
Section:
Explanation:
You can establish a VPN before the user login to the Endpoint Client by enabling Machine Authentication in the Gateway object of the Smart Console1.Machine Authentication is a feature that allows you to authenticate with a machine certificate and establish a VPN tunnel before the Windows Logon2.This feature provides the following benefits2:
It enhances the security of the VPN connection by verifying the identity of the machine before allowing access to the network.
It simplifies the user experience by eliminating the need to enter credentials twice (once for the VPN and once for the Windows Logon).
It enables seamless connectivity to the network resources and domain services, such as Group Policy, login scripts, and mapped drives. Machine Authentication is supported on Check Point Endpoint Security Client for Windows with E80.71 and higher versions2.It requires a hotfix on top of R77.30 jumbo 286 on the Security Gateway2.To configure Machine Authentication, you need to do the following steps2:
Generate and distribute machine certificates to the Endpoint machines using a trusted Certificate Authority (CA).
Enable Machine Authentication in the Gateway object of the Smart Console and select the CA that issued the machine certificates.
Install policy on the Security Gateway and reboot it.
Enable Machine Authentication in the Endpoint Security Client and select the machine certificate to use.

QUESTION 216
After having saved the Clish Configuration with the 'save configuration config.txt' command, where can you find the config.txt file?

A. You will find it in the home directory of your user account (e.g. /home/admin/)

B. You can locate the file via SmartConsole > Command Line.

C. You have to launch the WebUI and go to 'Config' -> 'Export Config File' and specifiy the destination directory of your local file system.

D. You cannot locate the file in the file system since Clish does not have any access to the bash file system

Correct Answer: A
Section:
Explanation:
You will find the config.txt file in the home directory of your user account (e.g./home/admin/)1.Thesave configuration config.txtcommand is a Clish command that saves the current Gaia configuration to a text file2.The file is stored in the home directory of the user who executed the command, and it can be accessed by using thecatorlesscommands in expert mode1.The file can also be transferred to another machine by using thescporsftpcommands1.The config.txt file contains the Clish commands that are needed to restore the Gaia configuration to the same state as when the file was saved2.The file can be used for backup, migration, or troubleshooting purposes2.

QUESTION 217
How can you switch the active log file?

A. Run fw logswitch on the gateway

B. Run fwm logswitch on the Management Server

C. Run fwm logswitch on the gateway

D. Run fw logswitch on the Management Server

Correct Answer: D
Section:
Explanation:
You can switch the active log file by runningfw logswitchon the Management Server1.This command closes the current log file and creates a new one2.It is useful for archiving or backing up log files, or for creating a new log

file for a specific time period2.You can also schedule the log switch to occur automatically at a regular interval, such as daily, weekly, or monthly2.To run this command, you need to access the Management Server in expert mode and runfw logswitch1. You can also use the SmartView Tracker to switch the active log file from the GUI.To do this, go to the Network & Endpoint tab, click on the File menu, and select Switch Active File...3.

QUESTION 218
Which of the following Check Point commands is true to enable Multi-Version Cluster (MVC)?

A. Check Point Security Management HA (Secondary): set cluster member mvc on
B. Check Point Security Gateway Only: set cluster member mvc on
C. Check Point Security Management HA (Primary): set cluster member mvc on
D. Check Point Security Gateway Cluster Member: set cluster member mvc on

Correct Answer: D
Section:
Explanation:
You can enable Multi-Version Cluster (MVC) by runningset cluster member mvc onon the Check Point Security Gateway Cluster Member1.MVC is a feature that allows you to upgrade a Security Gateway Cluster to a higher version without downtime2.It works by upgrading one cluster member at a time, while the other cluster members continue to operate with the lower version2.MVC supports upgrading from R80.40 and above to R81 and above2.To use MVC, you need to do the following steps2:
Enable MVC on each cluster member by runningset cluster member mvc onin Clish and rebooting the gateway.
Install the higher version on one cluster member using CPUSE or ISO image.
Install policy on the upgraded cluster member and verify that it works properly.
Repeat the previous steps for the remaining cluster members until all of them are upgraded.
Disable MVC on each cluster member by runningset cluster member mvc offin Clish and rebooting the gateway.

QUESTION 219
Bob needs to know if Alice was configuring the new virtual cluster interface correctly. Which of the following Check Point commands is true?

A. cphaprob-aif
B. cp hap rob state
C. cphaprob list
D. probcpha -a if

Correct Answer: A
Section:
Explanation:
You can use thecphaprob -a ifcommand to check the status of the virtual cluster interface1.This command displays the state, virtual IP address, and physical IP address of each cluster interface2.It also shows the load balancing method, the load on each interface, and the active member for each interface2. This command can help you verify that Alice configured the virtual cluster interface correctly and that it is working properly.To run this command, you need to access the cluster member in Clish and runcphaprob -a if1.

QUESTION 220
What is the amount of Priority Queues by default?

A. There are 8 priority queues and this number cannot be changed.
B. There is no distinct number of queues since it will be changed in a regular basis based on its system requirements.
C. There are 7 priority queues by default and this number cannot be changed.
D. There are 8 priority queues by default, and up to 8 additional queues can be manually configured

Correct Answer: D
Section:

Explanation:
There are 8 priority queues by default, and up to 8 additional queues can be manually configured1.Priority Queues are a feature of SecureXL that accelerates the performance of the Security Gateway by offloading CPU-intensive operations to the SecureXL device2.Priority Queues are used to prioritize traffic when the Security Gateway is stressed and needs to drop packets2.By default, there are 8 priority queues, each with a different priority level and type of connections2.You can manually configure up to 8 additional queues by setting the relevant kernel parameters in $FWDIR/boot/modules/fwkern.conf file1.You can also customize the queue length, the load balancing method, and the services that are considered as control connections1.

QUESTION 221
Bob is asked by Alice to disable the SecureXL mechanism temporary tor further diagnostic by their Check Point partner. Which of the following Check Point Command is true:

A. fwaccel suspend
B. fwaccel standby
C. fwaccel off
D. fwaccel templates

Correct Answer: C
Section:
Explanation:
You can disable the SecureXL mechanism temporarily for further diagnostic by runningfwaccel offon the Security Gateway1.This command disables SecureXL, which is an acceleration solution that maximizes the performance of the Firewall by offloading CPU-intensive operations to the SecureXL device2.Disabling SecureXL can help you troubleshoot connectivity or policy issues, as it forces all traffic to go through the Firewall kernel and bypass the SecureXL device1.To run this command, you need to access the Security Gateway in expert mode and runfwaccel off1.To enable SecureXL again, you can runfwaccel on1.Note that disabling SecureXL may affect the performance of the Security Gateway, so use it with caution and only when necessary1.

QUESTION 222
You had setup the VPN Community VPN-Stores'with 3 gateways. There are some issues with one remote gateway(1.1.1.1) and an your local gateway. What will be the best log filter to see only the IKE Phase 2 agreed networks for both gateways

A. action:'Key Install' AND 1.1.1.1 AND Main Mode
B. action:'Key Install- AND 1.1.1.1 ANDQuick Mode
C. Blade:'VPN' AND VPN-Stores AND Main Mode
D. Blade:'VPN' AND VPN-Stores AND Quick Mode

Correct Answer: B
Section:
Explanation:
The best log filter to see only the IKE Phase 2 agreed networks for both gateways is B.action:''Key Install'' AND 1.1.1.1 AND Quick Mode1.This filter will show you the logs that indicate the successful establishment of IKE Phase 2, which is also known as Quick Mode2.In this phase, the Security Gateway and the remote gateway negotiate the IPSec Security Associations (SAs) and exchange the encryption keys for the VPN tunnel2.The action:''Key Install'' field shows that the SAs were installed successfully3.The 1.1.1.1 field shows that the logs are related to the remote gateway with that IP address3.The Quick Mode field shows that the logs are related to IKE Phase 2, as opposed to Main Mode, which is IKE Phase 13.To use this filter, you need to go to SmartConsole, open SmartLog, and enter the filter expression in the search box3.

QUESTION 223
Besides fw monitor, what is another command that can be used to capture packets?

A. arp
B. traceroute
C. tcpdump
D. ping

Correct Answer: C

Section:
Explanation:
Tcpdump is a tool that captures and analyzes network traffic on a given interface2.It can be used to troubleshoot connectivity or performance issues, or to inspect the content of the packets2.To use tcpdump, you need to access the Security Gateway in expert mode and runtcpdump -i <interface> [options] [filter]2.You can specify various options and filters to customize the output, such as source or destination IP address, port number, protocol, packet size, etc2.You can also save the captured packets to a file for later analysis by using the-woption2.For more information about tcpdump, you can runman tcpdumpor visit the official website3.

QUESTION 224
What are the modes of SandBlast Threat Emulation deployment?

A. Cloud, Smart-1 and Hybrid
B. Cloud. OpenServer and Vmware
C. Cloud, Appliance and Private
D. Cloud, Appliance and Hybrid

Correct Answer: D
Section:
Explanation:
SandBlast Threat Emulation is a technology that protects against zero-day and unknown malware by inspecting files in a secure sandbox environment and emulating their behavior.SandBlast Threat Emulation can be deployed in three modes: Cloud, Appliance and Hybrid1.
Cloud mode: The files are sent to the Check Point cloud service for emulation. This mode does not require any additional hardware or software installation. It is the easiest and most cost-effective way to deploy SandBlast Threat Emulation.
Appliance mode: The files are sent to a dedicated appliance (TE1000X, TE2500X, or TE100X) for emulation. This mode provides the highest level of performance and scalability, as well as data privacy and compliance. It is suitable for large organizations with high security and throughput requirements.
Hybrid mode: The files are first sent to the Check Point cloud service for emulation, and if the cloud service cannot determine the verdict, they are then sent to a dedicated appliance for further analysis. This mode combines the benefits of both cloud and appliance modes, offering fast response time and high accuracy.

QUESTION 225
Which command lists firewall chain?

A. fwctl chain
B. fw list chain
C. fw chain module
D. fw tab -t chainmod

Correct Answer: A
Section:
Explanation:
The command that lists firewall chain isfw ctl chain1.This command displays the list of chain modules that are registered on the Security Gateway2.Chain modules are components of the Firewall kernel that inspect and process packets according to the security policy and other features3.The order of the chain modules determines the order of the packet inspection and processing3.Thefw ctl chaincommand can help you troubleshoot connectivity or performance issues, or to verify that a feature is enabled or disabled on the Security Gateway2.To run this command, you need to access the Security Gateway in expert mode and runfw ctl chain1.

QUESTION 226
Which Queue in the Priority Queue has the maximum priority?

A. High Priority
B. Control
C. Routing
D. Heavy Data Queue

Correct Answer: C
Section:
Explanation:
The Priority Queue is a feature that allows the firewall to prioritize certain types of traffic over others, such as control and routing traffic, when the CPU load is high.The Priority Queue has four levels of priority: Control, Routing, High Priority and Heavy Data Queue1. The Control level has the highest priority and is reserved for firewall control traffic, such as policy installation and synchronization. The Routing level has the second highest priority and is used for routing protocols, such as OSPF and BGP. The High Priority level has the third highest priority and is used for user-defined traffic that needs to be prioritized, such as VoIP or video conferencing.The Heavy Data Queue level has the lowest priority and is used for bulk data transfer, such as FTP or HTTP2. Therefore, the correct answer is C.

QUESTION 227
What is the purpose of the command 'ps aux | grep twd'?

A. You can check the Process ID and the processing time of the twd process.
B. You can convert the log file into Post Script format.
C. You can list all Process IDs for all running services.
D. You can check whether the IPS default setting is set to Detect or Prevent mode

Correct Answer: A
Section:
Explanation:
The command ''ps aux | grep twd'' is used to check the process ID and the processing time of the twd process on the Security Gateway. The ps command displays information about the active processes on the system. The aux option shows all processes for all users, including those without a controlling terminal.The grep command filters the output of the ps command by searching for the pattern ''twd'', which is the name of the process that handles VPN traffic encryption and decryption1.The output of the command shows the process ID, CPU usage, memory usage, start time, and other details of the twd process2. Therefore, the correct answer is A.

QUESTION 228
What is the minimum number of CPU cores required to enable CoreXL?

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

Correct Answer: C
Section:
Explanation:
CoreXL is a technology that improves the performance of the Security Gateway by utilizing multiple CPU cores for processing traffic. CoreXL creates multiple instances of the firewall kernel (fwk) that run in parallel on different CPU cores.The number of kernel instances can be configured using the cpconfig command on the Security Gateway3.The minimum number of CPU cores required to enable CoreXL is 2, as one core is reserved for SND (Secure Network Distributor) and one core is used for running a kernel instance4. If the Security Gateway has only one CPU core, CoreXL cannot be enabled. Therefore, the correct answer is C.

QUESTION 229
You want to gather data and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

A. Check Point Capsule Cloud
B. Sandblast Mobile Protect
C. SecuRemote
D. SmartEvent Client Info

Correct Answer: B
Section:

Explanation:
SandBlast Mobile Protect is an application that provides comprehensive protection for mobile devices against cyber threats. SandBlast Mobile Protect is a lightweight app that does not affect the device performance or battery life.It monitors network traffic, device behavior, and installed apps to detect and prevent attacks such as phishing, malware, ransomware, botnets, and man-in-the-middle5.SandBlast Mobile Protect also integrates with Check Point's ThreatCloud intelligence network to provide real-time threat information and updates6. Therefore, the correct answer is B)

QUESTION 230
Secure Configuration Verification (SCV), makes sure that remote access client computers are configured in accordance with the enterprise Security Policy. Bob was asked by Alice to implement a specific SCV configuration but therefore Bob needs to edit and configure a specific Check Point file. Which location file and directory is true?

A. $FWDIR/conf/client.scv
B. $CPDIR/conf/local.scv
C. $CPDIR/conf/client.svc
D. $FWDIR/conf/local.scv

Correct Answer: D
Section:
Explanation:
Secure Configuration Verification (SCV) is a feature that allows the Mobile Access Gateway to check the compliance of remote access clients with the enterprise security policy before granting them access to internal resources.SCV checks can be defined in a file named local.scv, which is located in the $FWDIR/conf directory on the Mobile Access Gateway1.The file can be edited manually or using the SCV Editor tool2. Therefore, the correct answer is D)

QUESTION 231
What are the services used for Cluster Synchronization?

A. 256H-CP tor Full Sync and 8116/UDP for Delta Sync
B. 8116/UDP for Full Sync and Delta Sync
C. TCP/256 for Full Sync and Delta Sync
D. No service needed when using Broadcast Mode

Correct Answer: A
Section:
Explanation:
Cluster Synchronization is a mechanism that allows cluster members to share state information and maintain a consistent security policy. Cluster Synchronization uses two types of synchronization: Full Synchronization and Delta Synchronization. Full Synchronization transfers the entire Security Policy and state tables from one cluster member to another. Delta Synchronization transfers only the changes in the state tables.Cluster Synchronization uses two services for communication: TCP port 256 (CPHA) for Full Synchronization and UDP port 8116 for Delta Synchronization3. Therefore, the correct answer is A.

QUESTION 232
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

A. After upgrading the hardware, increase the number of kernel instances using cpconfig
B. Hyperthreading must be enabled in the bios to use CoreXL
C. Run cprestart from dish
D. Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores.

Correct Answer: A
Section:
Explanation:

https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminGuide/Content/Topics-PTG/CoreXL-Configuring-IPv4-and-IPv6-CoreXL-FW-instances.htm?Highlight=Configuring%20the%20Number%20of%20IPv4%20CoreXL%20Firewall%20Instances R81 https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_PerformanceTuning_AdminGuide/Topics-PTG/CoreXL-Configuring-IPv4-and-IPv6-CoreXL-FW-instances.htm cpconfig -> Enter the number of the Check Point CoreXL option. (Enter 1 to select Change the number of firewall instances. OR Enter 2 for the option Change the number of IPv6 firewall instances.) -> Enter the total number of IPv4 (IPv6) CoreXL Firewall instances you wish the Security Gateway to run. Follow the instructions on the screen. -> Exit from the cpconfig menu. - Reboot the Security Gateway.

QUESTION 233

Mobile Access Gateway can be configured as a reverse proxy for Internal Web Applications Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. Which of the following Check Point command is true for enabling the Reverse Proxy:

A. ReverseCLIProxy

B. ReverseProxyCLI

C. ReverseProxy

D. ProxyReverseCLI

Correct Answer: C

Section:

Explanation:

Mobile Access Gateway can be configured as a reverse proxy for internal web applications. Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. The Security Gateway then forwards the requests to the internal web servers and returns the responses to the users.To enable reverse proxy mode on the Mobile Access Gateway, the administrator needs to run the ReverseProxy command on the command line interface of the Security Gateway5. Therefore, the correct answer is C.

QUESTION 234

What should the admin do in case the Primary Management Server is temporary down?

A. Use the VIP in SmartConsole you always reach the active Management Server.

B. The Secondary will take over automatically Change the IP in SmartConsole to logon to the private IP of the Secondary Management Server.

C. Run the 'promote_util' to activate the Secondary Management server

D. Logon with SmartConsole to the Secondary Management Server and choose 'Make Active' under Actions in the HA Management Menu

Correct Answer: A

Section:

Explanation:

High Availability (HA) is a deployment scenario where two or more Security Management Servers are configured to work together as a cluster. One server acts as the Primary server and handles all management operations, while another server acts as the Secondary server and serves as a backup. If the Primary server fails, the Secondary server takes over and becomes active. The cluster members communicate using a Virtual IP (VIP) address, which is used by SmartConsole to connect to the active server. If the Primary server is temporarily down, the administrator does not need to do anything, as SmartConsole will automatically connect to the VIP address and reach the Secondary server that has become active. Therefore, the correct answer is A.

QUESTION 235

According to the policy installation flow the transfer state (CPTA) is responsible for the code generated by the FWM. On the Security Gateway side a process receives them and first stores them Into a temporary directory. Which process is true for receiving these Tiles;

A. FWD

B. CPD

C. FWM

D. RAD

Correct Answer: A

Section:
Explanation:
FWD is a process that runs on both Security Management Server and Security Gateway. On Security Management Server, FWD handles logging and communication with SmartConsole.On Security Gateway, FWD receives policy files from FWM (the policy compiler process on Security Management Server) and stores them in a temporary directory before installing them on the firewall kernel7. Therefore, FWD is responsible for receiving policy files from FWM on Security Gateway side. The correct answer is A.

QUESTION 236
The customer has about 150 remote access user with a Windows laptops. Not more than 50 Clients will be connected at the same time. The customer want to use multiple VPN Gateways as entry point and a personal firewall. What will be the best license for him?

A. He will need Capsule Connect using MEP (multiple entry points).
B. Because the customer uses only Windows clients SecuRemote will be sufficient and no additional license is needed
C. He will need Harmony Endpoint because of the personal firewall.
D. Mobile Access license because he needs only a 50 user license, license count is per concurrent user.

Correct Answer: C
Section:
Explanation:
Harmony Endpoint is a solution that provides comprehensive protection for endpoint devices against cyber threats. Harmony Endpoint includes a personal firewall that controls the network traffic to and from the endpoint device, based on predefined rules and policies.Harmony Endpoint also integrates with Check Point's VPN solutions to provide secure remote access to corporate resources1. Therefore, the customer will need Harmony Endpoint because of the personal firewall requirement.

QUESTION 237
Bob has finished io setup provisioning a secondary security management server. Now he wants to check if the provisioning has been correct. Which of the following Check Point command can be used to check if the security management server has been installed as a primary or a secondary security management server?

A. cpprod_util MgmtIsPrimary
B. cpprod_util FwIsSecondary
C. cpprod_util MgmtIsSecondary
D. cpprod_util FwIsPrimary

Correct Answer: A
Section:
Explanation:
The cpprod_util command is a utility that provides information about the installed Check Point products and their versions.The cpprod_util MgmtIsPrimary option checks if the Security Management Server is installed as a primary or a secondary server in a High Availability cluster2. If the server is primary, the command returns ''yes''. If the server is secondary, the command returns ''no''. Therefore, Bob can use this command to verify the provisioning of the secondary Security Management Server.

QUESTION 238
What are the three SecureXL Templates available in R81.20?

A. PEP Templates. QoS Templates. VPN Templates
B. Accept Templates. Drop Templates. NAT Templates
C. Accept Templates. Drop Templates. Reject Templates
D. Accept Templates. PDP Templates. PEP Templates

Correct Answer: B
Section:

Explanation:

SecureXL is a technology that improves the performance of the Security Gateway by offloading CPU-intensive operations to a dedicated hardware or software module. SecureXL uses templates to accelerate traffic processing based on predefined patterns and conditions.SecureXL supports three types of templates: Accept Templates, Drop Templates, and NAT Templates3.

Accept Templates are used to accelerate traffic that matches an Accept rule in the Security Policy. Accept Templates bypass most of the inspection stages and send packets directly to the network interface.

Drop Templates are used to accelerate traffic that matches a Drop rule in the Security Policy. Drop Templates drop packets without sending them to the firewall kernel for inspection.

NAT Templates are used to accelerate traffic that requires Network Address Translation (NAT). NAT Templates perform NAT operations without sending packets to the firewall kernel.

Therefore, the correct answer is B)

QUESTION 239

Which one is not a valid Package Option In the Web GUI for CPUSE?

A. Clean Install

B. Export Package

C. Upgrade

D. Database Conversion to R81.20 only

Correct Answer: B

Section:

Explanation:

CPUSE (Check Point Upgrade Service Engine) is a tool that allows users to download, import, install, and uninstall software packages on Gaia OS. CPUSE has a web-based user interface that can be accessed through Gaia Portal.CPUSE offers four package options in the web GUI for different purposes4:

Clean Install - This option performs a clean installation of a Major Version package, which erases all existing configuration and data on the system.

Export Package - This option exports a package from CPUSE repository to an external location for backup or transfer purposes.

Upgrade - This option performs an upgrade of a Major Version package or a Minor Version package, which preserves the existing configuration and data on the system.

Database Conversion - This option converts the database schema of a Major Version package to match the current version.

Therefore, the correct answer is B)

QUESTION 240

Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently capable of issuing and managing certificate. Alice uses the Check Point command 'cpconfig'' to run the Check Point Security Management Server configuration tool on both Check Point Management HA instances 'Primary & Secondary' Which configuration option does she need to look for:

A. Certificate's Fingerprint

B. Random Pool

C. CA Authority

D. Certificate Authority

Correct Answer: D

Section:

Explanation:

Certificate Authority (CA) is a service that issues and manages digital certificates for secure communication between Check Point components. CA can be installed on a Security Management Server or on a dedicated server. CA can be configured as primary or secondary in a High Availability cluster. The cpconfig command is used to run the Check Point Configuration Tool on Gaia OS, which allows users to configure various settings for Check Point products.One of the configuration options is Certificate Authority, which shows if CA is installed on the server and if it is primary or secondary5. Therefore, Alice needs to look for this option to check the CA status.

QUESTION 241

What API command below creates a new host object with the name 'My Host' and IP address of '192 168 0 10'?

A. set host name 'My Host' ip-address '192.168.0.10'

B. new host name 'My Host' ip-address '192 168.0.10'

C. create host name 'My Host' ip-address '192.168 0.10'

D. mgmt.cli -m <mgmt ip> add host name 'My Host' ip-address '192.168.0 10'

Correct Answer: A
Section:
Explanation:
Check Point API is an interface that allows users to automate tasks and manage Check Point products using RESTful web service calls. Check Point API uses JSON format for requests and responses.To create a new host object with the name ''My Host'' and IP address of ''192.168.0.10'', users need to use the set host command with the name and ip-address parameters6. The command syntax is:
set host name ''My Host'' ip-address ''192.168.0.10''
Therefore, the correct answer is A.

QUESTION 242
What does Backward Compatibility mean upgrading the Management Server and how can you check it?

A. The Management Server is able to manage older Gateways. The lowest supported version is documented in the Installation and Upgrade Guide

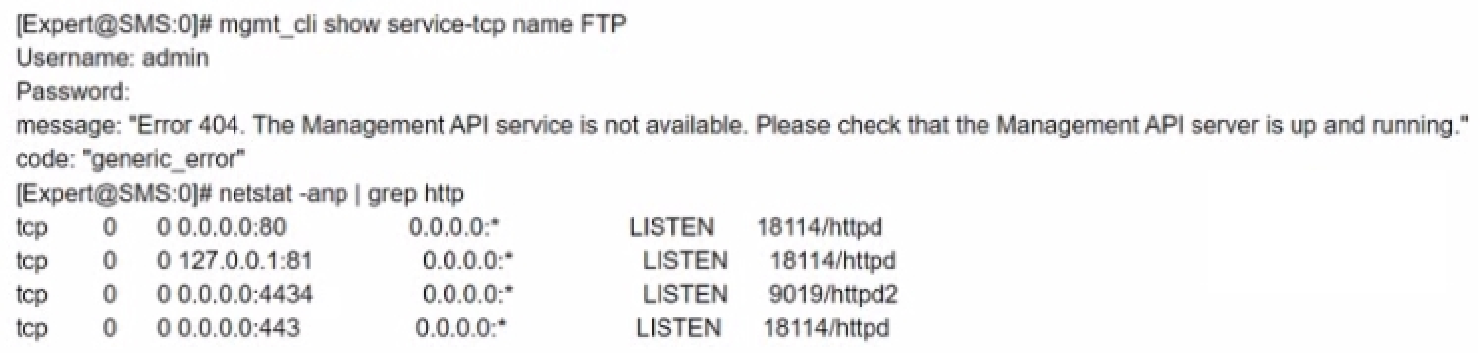
B. The Management Server is able to manage older Gateways The lowest supported version is documented in the Release Notes

C. You will be able to connect to older Management Server with the SmartConsole. The lowest supported version is documented in the Installation and Upgrade Guide

D. You will be able to connect to older Management Server with the SmartConsole The lowest supported version is documented in the Release Notes

Correct Answer: B
Section:
Explanation:
Backward Compatibility means that the Management Server is able to manage older Gateways. The lowest supported version is documented in the Release Notes of each version. The Installation and Upgrade Guide only provides information about how to install or upgrade the Management Server and the Gateways, not about the compatibility between them.
Reference:Check Point R81 Release Notes, page 6.

QUESTION 243
The admin is connected via ssh lo the management server. He wants to run a mgmt_dl command but got a Error 404 message. To check the listening ports on the management he runs netstat with the results shown below.
What can be the cause for the issue?



```
[Expert@SMS:0]# mgmt_cli show service-tcp name FTP
Username: admin
Password:
message: "Error 404. The Management API service is not available. Please check that the Management API server is up and running."
code: "generic_error"
[Expert@SMS:0]# netstat -anp | grep http
tcp      0      0 0.0.0.0:80            0.0.0.0:*          LISTEN     18114/httpd
tcp      0      0 127.0.0.1:81          0.0.0.0:*          LISTEN     18114/httpd
tcp      0      0 0.0.0.0:4434          0.0.0.0:*          LISTEN     9019/httpd2
tcp      0      0 0.0.0.0:443           0.0.0.0:*          LISTEN     18114/httpd
```

A. Wrong Management API Access setting^for Ihe client IP To correct it go to SmartConsole / Management & Settings / Blades / Management API and press 'Advanced Settings..' and choose GUI clients or ALL IP's.

B. The API didn't run on the default port check it with api status' and add '-port 4434' to the mgmt_clt command.

C. The management permission in the user profile is mrssing. Go to SmartConsole / Management & Settings I Permissions & Administrators / Permission Profiles. Select the profile of the user and enable 'Management API Login' under Management Permissions

D. The API is not running, the services shown by netstat are the gaia services. To start the API run 'api start'

Correct Answer: D
Section:
Explanation:

The error message ''Error 404. The Management API server is not available. Please check that the Management API server is up and running.'' indicates that the API is not running on the Management Server. The netstat command shows that there is no process listening on port 4434, which is the default port for the API. To start the API, the command 'api start' should be used. The other options are not relevant to this issue.
Reference:Check Point R81 Installation and Upgrade Guide, page 18.

QUESTION 244
What is a possible command to delete all of the SSH connections of a gateway?

A. fw sam -I dport 22
B. fw ctl conntab -x -dpott=22
C. fw tab -t connections -x -e 00000016
D. fwaccel dos config set dport ssh

Correct Answer: A
Section:
Explanation:
The command 'fw sam -I dport 22' will delete all of the SSH connections of a gateway by adding a temporary rule to the Security Policy that blocks traffic with destination port 22. The other commands are not valid or do not have the same effect.
Reference:Check Point R81 Command Line Interface Reference Guide, page 101.

QUESTION 245
What are the two types of tests when using the Compliance blade?

A. Policy-based tests and Global properties
B. Global tests and Object-based tests
C. Access Control policy analysis and Threat Prevention policy analysis
D. Tests conducted based on the IoC XMfcfile and analysis of SOLR documents

Correct Answer: B
Section:
Explanation:
The Check Point Compliance Blade has a library of Check Point-defined tests to use as a baseline for good gateway and policy configuration. A Best Practice test is related to specified regulations in different regulatory standards. It describes compliance status and recommends corrective steps. Global Tests - Examine all applicable configuration settings in the organization. Object-based Tests - Examine the configuration settings for specified objects (gateways, profiles and other objects)
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120256

QUESTION 246
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 by the active gateway
C. All connections that were initiated before the upgrade will be handled normally
D. All connections that were initiated before the upgrade will be handled by the standby gateway

Correct Answer: B
Section:
Explanation:
All connections that were initiated before the upgrade will be handled by the active gateway.According to the Check Point documentation1, a minimal effort upgrade is a procedure that allows you to upgrade each Security Gateway individually, without affecting the cluster operation. The active gateway continues to handle the traffic while the standby gateway is upgraded, and then they switch roles.This way, there is no network downtime and

no need to synchronize the cluster members before or after the upgrade1.However, some connections may be dropped during the switch-over, so it is recommended to use a connectivity upgrade or a zero downtime upgrade for mission-critical environments2.

QUESTION 247
Which two Cluster Solutions are available under R81.20?

A. ClusterXL and NSRP
B. VRRPandHSRP
C. VRRP and IP Clustering
D. ClusterXL and VRitP

Correct Answer: D
Section:
Explanation:
ClusterXL and VRRP are the two cluster solutions that are available under R81.20.According to the ClusterXL R81.20 Administration Guide1, ClusterXL is a Check Point software-based clustering solution that provides high availability and load sharing for Check Point Security Gateways and Cluster Members. ClusterXL supports two modes: High Availability and Load Sharing. In High Availability mode, all Cluster Members are connected to the same network segment and share a virtual IP address. One member is active and handles all traffic, while the others are in standby mode and ready to take over in case of a failure. In Load Sharing mode, all Cluster Members are active and share the traffic load according to a predefined algorithm.ClusterXL supports both unicast and multicast modes for Load Sharing1.
VRRP (Virtual Router Redundancy Protocol) is an industry standard protocol that provides high availability for routers or firewalls by creating a virtual router with a virtual IP address that is shared by a group of routers or firewalls. One router or firewall is elected as the master and handles all traffic directed to the virtual IP address, while the others are backups that monitor the master and take over if it fails.VRRP can be used with Check Point Security Gateways to provide redundancy and failover for external interfaces1.
NSRP (NetScreen Redundancy Protocol) is a proprietary protocol developed by Juniper Networks that provides high availability and load balancing for NetScreen firewalls.NSRP is not supported by Check Point products2.
HSRP (Hot Standby Router Protocol) is a Cisco proprietary protocol that provides high availability for routers by creating a virtual router with a virtual IP address that is shared by a group of routers. One router is elected as the active router and handles all traffic directed to the virtual IP address, while another router is elected as the standby router and monitors the active router and takes over if it fails. HSRP is not supported by Check Point products.
IP Clustering is a feature of Linux Virtual Server (LVS) that provides high availability and load balancing for IP-based services by creating a cluster of real servers that are accessed through a virtual IP address. The cluster is managed by a director that routes requests to the real servers according to a scheduling algorithm. IP Clustering is not supported by Check Point products.

QUESTION 248
Which is the command to identify the NIC driver before considering about the employment of the Multi-Queue feature?

A. show interface eth0 mq
B. ethtool A eth0
C. ifconfig -i eth0 verbose
D. ip show Int eth0

Correct Answer: B
Section:
Explanation:
The command to identify the NIC driver before considering about the employment of the Multi-Queue feature isethtool -i eth0, whereeth0is the name of the network interface.This command displays the information about the driver and firmware version of the NIC, as well as other details such as bus-info and supported features1.The Multi-Queue feature requires a NIC driver that supports multiple transmit and receive queues2.

QUESTION 249
An established connection is going to www.google.com. The Application Control Blade Is inspecting the traffic. If SecureXL and CoreXL are both enabled, which path is handling the traffic?

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

D. Accelerated Path

Correct Answer: D
Section:
Explanation:
The traffic is handled by the Accelerated Path.According to the R81.x Security Gateway Architecture (Logical Packet Flow)1, the Accelerated Path is the fastest path for processing packets, as it bypasses most of the inspection and uses SecureXL to accelerate the traffic.The Accelerated Path is used for connections that are established, compliant with the security policy, and do not require any content inspection or NAT1.
The Application Control blade inspects the traffic based on the application identity, which is determined by the Application Control Software Blade in the Medium Path1.However, once the application identity is established, the connection can be offloaded to SecureXL and handled by the Accelerated Path2.This way, the Application Control blade can improve performance and reduce CPU consumption2.
The other paths are not used for this traffic because:
The Slow Path is used for packets that are not compliant with the security policy, require stateful inspection or NAT, or are not supported by SecureXL1.This path involves the most inspection and processing, and is therefore the slowest3.
The Fast Path is used for packets that are trusted and do not require any inspection or NAT.This path bypasses both SecureXL and the Firewall kernel, and uses a kernel module called simfast to forward the packets directly to the network interface driver4.This path is not enabled by default, and requires manual configuration of rules to define which traffic can use it4.
The Medium Path is used for packets that require content inspection, such as IPS, Anti-Virus, Anti-Bot, URL Filtering, or Application Control1.This path uses SecureXL to accelerate some parts of the inspection, but still involves some processing by the Firewall kernel3.This path is only used for the first few packets of a connection until the application identity is established, and then the connection can be offloaded to the Accelerated Path2.

QUESTION 250
SecureXL is able to accelerate the Connection Rate using templates. Which attributes are used in the template to identify the connection?

A. Source address. Destination address. Source Port, Destination port
B. Source address. Destination address. Destination port
C. Source address. Destination address. Destination port. Pro^col
D. Source address. Destination address. Source Port, Destination port. Protocol

Correct Answer: D
Section:
Explanation:
SecureXL uses templates to accelerate the connection rate by creating a connection entry in the SecureXL Connections Table without notifying the Firewall kernel for a predefined period of time1.This reduces the load on the Firewall kernel and improves the performance of new connections1.SecureXL uses five attributes to identify a connection and create a template: source address, destination address, source port, destination port, and protocol2.These attributes form a unique 5-tuple that defines a connection2.

QUESTION 251
Which Correction mechanisms are available with ClusterXL under R81.20?

A. Correction Mechanisms are only available of Maestro Hyperscale Orchestrators
B. Pre-Correction and SDF (Sticky Decision Function)
C. SDF (Sticky Decision Function) and Flush and ACK
D. Dispatcher (Early Correction) and Firewall (Late Correction)

Correct Answer: C
Section:
Explanation:
SDF (Sticky Decision Function) and Flush and ACK are the two correction mechanisms that are available with ClusterXL under R81.20.According to the ClusterXL R81.20 Administration Guide1, correction mechanisms are methods that ClusterXL uses to prevent or recover from out-of-state situations, which occur when different Cluster Members have different information about the connections that they handle1.ClusterXL supports two types of correction mechanisms: SDF and Flush and ACK1.
SDF (Sticky Decision Function) is a mechanism that ensures that packets of the same connection are always handled by the same Cluster Member, regardless of the load balancing algorithm. SDF uses a hash table that maps each connection to a specific Cluster Member, based on the 5-tuple of source IP, destination IP, source port, destination port, and protocol.SDF prevents out-of-state situations by avoiding the switch of Cluster Members for existing connections1.

Flush and ACK is a mechanism that synchronizes the connection tables of different Cluster Members when an out-of-state situation is detected. Flush and ACK works as follows:
When a Cluster Member receives a packet that belongs to an unknown connection, it sends a Flush message to all other Cluster Members, asking them to delete the connection from their tables.
When a Cluster Member receives a Flush message, it checks if it has the connection in its table. If it does, it deletes the connection and sends an ACK message to the sender of the Flush message, indicating that it has performed the deletion.
When a Cluster Member receives an ACK message, it creates a new connection entry in its table for the packet that triggered the Flush message, and processes the packet normally.
If a Cluster Member does not receive any ACK message within a timeout period, it assumes that no other Cluster Member has the connection, and creates a new connection entry in its table for the packet that triggered the Flush message1.

QUESTION 252
Which upgrade method you should use upgrading from R80.40 to R81.20 to avoid any downtime?

A. Zero Downtime Upgrade (ZDU)
B. Connectivity Upgrade (CU)
C. Minimal Effort Upgrade (ME)
D. Multi-Version Cluster Upgrade (MVC)

Correct Answer: D
Section:
Explanation:
The correct upgrade method for upgrading from R80.40 to R81.20 without any downtime is the Multi-Version Cluster Upgrade (MVC). MVC is a new feature in R80.40 that replaces the deprecated Connectivity Upgrade (CU). MVC allows you to upgrade cluster members to a newer version without losing connectivity and test the new version on some of the cluster members before you decide to upgrade the rest of the cluster members. MVC synchronizes connections between cluster members that run different versions and ensures that the cluster remains operational during the upgrade process. MVC is intended only to test the current configuration in the newer version and not to change the security policy and install it on cluster members with different software versions. MVC is disabled by default and can be enabled on each cluster member individually. MVC has some limitations, such as not supporting VSX clusters, IPS blade, or SecureXL acceleration.
Multi-Version Cluster (MVC) replaces Connectivity Upgrade (CU) in R80.40
Multi-Version Cluster (MVC) Upgrade
Configuring the Multi-Version Cluster Mechanism

QUESTION 253
How can you see historical data with cpview?

A. cpview -f <timestamp>
B. cpview -e <timestamp>
C. cpview -t <timestamp>
D. cpview -d <timestamp>

Correct Answer: C
Section:
Explanation:
To see historical data with cpview, you can use the cpview -t <timestamp> command, where <timestamp> is the date and time you want to view. For example, cpview -t Jan 01 2023 12:00:00 will show you the cpview data for January 1st, 2023 at noon. You can also enter a partial date, such as Jan 02, to see the data for the whole day.This feature is available in R77.10 and higher versions of Check Point software1.You can also access the historical data by pressing the ''t'' key while running cpview in live mode and entering the desired date and time1.The historical data is stored in the CPViewDB.dat file in the /var/log/CPView_history directory on your gateway2.You can export this file and import it into other tools for visualization, such as Grafana3.

QUESTION 254
Alice & Bob are concurrently logged In via SSH on the same Check Point Security Gateway as user 'admin* however Bob was first logged in and acquired the lock Alice Is not aware that Bob is also togged in to the same Security Management Server as she is but she needs to perform very urgent configuration changes - which of the following GAIAclish command is true for overriding Bobs configuration database lock:

A. lock database override
B. unlock override database
C. unlock database override
D. database unlock override

Correct Answer: A
Section:
Explanation:
To override Bob's configuration database lock, Alice can use the commandlock database overridein the clish shell. This command will transfer the lock from Bob to Alice and allow her to make the urgent configuration changes. However, this command should be used with caution, as it may cause conflicts or inconsistencies if Bob and Alice are working on the same objects or policies.It is recommended to communicate with other administrators before using this command and to release the lock as soon as possible after finishing the changes1. The other commands are not valid in clish and will result in an error message.

QUESTION 255
What command is used to manually failover a cluster during a zero-downtime upgrade?

A. set cluster member down
B. cpstop
C. clusterXL_admin down
D. set clusterXL down

Correct Answer: C
Section:
Explanation:
To manually failover a cluster during a zero-downtime upgrade, you can use the commandclusterXL_admin downon the active cluster member. This command will gracefully change the state of the cluster member to down and trigger a failover to the standby cluster member. This way, you can upgrade the cluster member that is now down without affecting the traffic processed by the other cluster member. You can then use the commandclusterXL_admin upto bring the upgraded cluster member back online and repeat the process for the other cluster member.This command is useful for testing and debugging purposes and does not survive reboot unless you add the-poption or use theset cluster member admin down/up permanentcommand in clish1. The other commands are not valid for initiating a manual failover. Theset cluster member downcommand is used to remove a cluster member from a cluster. Thecpstopcommand is used to stop all Check Point services on a gateway. Theset clusterXL downcommand does not exist.

QUESTION 256
Packet acceleration (SecureXL) identities connections by several attributes. Which of the attributes is NOT used for identifying connection?

A. Source Port
B. TCP Acknowledgment Number
C. Source Address
D. Destination Address

Correct Answer: B
Section:
Explanation:
SecureXL does not use the TCP acknowledgment number as an attribute for identifying connections. SecureXL is a technology that accelerates the performance of the firewall by offloading some of the traffic processing from the firewall kernel to a more efficient path.SecureXL identifies connections by five attributes: source address, destination address, source port, destination port, and protocol1. These attributes are also known as the 5-tuple or the connection key. SecureXL uses these attributes to match packets to existing connections and apply the appropriate security policy and actions.SecureXL does not need to inspect the TCP sequence or acknowledgment numbers, as they are irrelevant for the connection identification and security enforcement2.The TCP sequence and acknowledgment numbers are used by the TCP protocol to ensure reliable and ordered delivery of data between endpoints

QUESTION 257
What is required for a site-to-site VPN tunnel that does not use certificates?

A. Pre-Shared Secret
B. RSA Token
C. Unique Passwords
D. SecureID

Correct Answer: A
Section:
Explanation:
A pre-shared secret is a secret key that is shared between the two VPN peers before establishing a secure connection. It is used to authenticate the VPN peers and encrypt the VPN traffic. A pre-shared secret is required for a site-to-site VPN tunnel that does not use certificates, because certificates are another way of authenticating the VPN peers using public key cryptography. Without certificates, the VPN peers need to have a common secret key that only they know.
Reference:Check Point R81 VPN Administration Guide, page 13

QUESTION 258
Using AD Query, the security gateway connections to the Active Directory Domain Controllers using what protocol?

A. Windows Management Instrumentation (WMI)
B. Hypertext Transfer Protocol Secure (HTTPS)
C. Lightweight Directory Access Protocol (LDAP)
D. Remote Desktop Protocol (RDP)

Correct Answer: A
Section:
Explanation:

Windows Management Instrumentation (WMI) is a protocol that allows remote management and monitoring of Windows systems. It is used by AD Query to connect to the Active Directory Domain Controllers and query them for user and computer information. AD Query uses WMI to get real-time updates on user logon events, group membership changes, and computer status changes. WMI is not the same as LDAP, which is a protocol for accessing and modifying directory services. HTTPS and RDP are also different protocols that are not used by AD Query.
Reference:Check Point R81 Identity Awareness Administration Guide, page 17

QUESTION 259
Name the file that is an electronically signed file used by Check Point to translate the features in the license into a code?

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

Correct Answer: B
Section:
Explanation:
cp.macro is an electronically signed file used by Check Point to translate the features in the license into a code. It is located in the $FWDIR/conf directory on the Security Management Server. The cp.macro file contains a list of features and their corresponding codes, which are used to generate the license file (.lic) based on the contract file (.xml). The license file (.lic) is then installed on the Security Gateway or Security Management Server to activate the licensed features.
Reference:Check Point R81 Licensing and Contract Administration Guide, page 10

QUESTION 260
What technologies are used to deny or permit network traffic?

A. Stateful Inspection, Firewall Blade, and URL/Application Blade
B. Packet Filtering, Stateful Inspection, and Application Layer Firewall
C. Firewall Blade, URL/Application Blade, and IPS
D. Stateful Inspection, URL/Application Blade, and Threat Prevention

Correct Answer: B
Section:
Explanation:
Packet filtering, stateful inspection, and application layer firewall are technologies used to deny or permit network traffic based on different criteria. Packet filtering is a basic firewall technology that examines the header of each packet and compares it to a set of rules to decide whether to allow or drop it. Stateful inspection is an advanced firewall technology that tracks the state and context of each connection and applies security rules based on the connection information. Application layer firewall is a firewall technology that inspects the content and behavior of applications and protocols at the application layer of the OSI model and enforces granular policies based on the application identity, user identity, and content type.
Reference:Check Point R81 Firewall Administration Guide, page 9-10

QUESTION 261
Which is the lowest gateway version supported by R81.20 management server?

A. R77.30
B. R80.20
C. R77
D. R65

Correct Answer: A
Section:
Explanation:
The lowest gateway version supported by R81.20 management server is R77.30.According to the Check Point Release Map1, you can upgrade to R81.20 from R77.30, R80, R80.10, R80.20.M1, R80.20, R80.20SP, R80.20.M2, R80.20 3.10, R80.30, R80.30 3.10, R80.30SP, R80.40, R81 and R81.20. However, to upgrade from R77.30, R80 and R80.10, you first need to upgrade to R80.40.For more information, you can refer to the Check Point R81.20 (Titan) Release Home page2or the Certified Security Expert (CCSE) R81.20 Course Overview3.

QUESTION 262
Which Mobile Access Solution is clientless?

A. Mobile Access Portal
B. Checkpoint Mobile
C. Endpoint Security Suite
D. SecuRemote

Correct Answer: A
Section:
Explanation:
Mobile Access Portal is a clientless solution that provides secure web access to corporate resources from any device and any browser. Mobile Access Portal uses SSL encryption and authentication to protect the data and the identity of the users. Mobile Access Portal supports various types of web applications, such as webmail, file shares, intranet sites, and web-based applications.
The references are:
Check Point Certified Security Expert R81.20 (CCSE) Core Training, slide 15
Check Point R81 Mobile Access Blade Administration Guide, page 7
[Check Point Mobile Access Software Blade]

QUESTION 263
In CoreXL, the Firewall kernel is replicated multiple times. Each replicated copy or instance can perform the following:

A. The Firewall kernel only touches the packet if the connection is accelerated
B. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
C. The Firewall can run the same policy on all cores
D. The Firewall can run different policies per core

Correct Answer: C
Section:
Explanation:
CoreXL is a performance-enhancing technology that enables the Security Gateway to utilize multiple CPU cores for processing traffic. CoreXL creates multiple instances of the Firewall kernel, each running on a separate CPU core. Each Firewall instance can handle traffic concurrently and independently, applying the same security policy to the packets that are assigned to it. CoreXL does not allow different policies per core, as this would create inconsistency and complexity in the security enforcement.
The references are:
Best Practices - Security Gateway Performance
Check Point Certified Security Expert R81.20 (CCSE) Core Training, slide 16
Check Point R81 Quantum Security Gateway Guide, page 42

QUESTION 264
What are scenarios supported by the Central Deployment in SmartConsole?

A. Installation of Jumbo Hotfix on a ClusterXL environment in High Availability Mode
B. Upgrading a Dedicated SmartEvent Server
C. Upgrading a Dedicated Log Server to R81
D. Upgrading a Standalone environment

Correct Answer: A
Section:

QUESTION 265
Identity Awareness allows the Security Administrator to configure network access based on which of the following?

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

Correct Answer: D
Section:
Explanation:
Implied rules are predefined rules that are automatically added to the Access Control rulebase by the Security Management Server. Implied rules allow the control connections that are essential for the functionality and security of the Check Point products, such as communication between the Security Gateway and the Security Management Server, synchronization between cluster members, logging, VPN, and ICMP. Implied rules are not visible in the SmartConsole, but they can be viewed and modified using the Global Properties window.
The references are:
Check Point Certified Security Expert R81.20 (CCSE) Core Training, slide 12
Check Point R81 Quantum Security Gateway Guide, page 141
Check Point R81 Firewall Administration Guide, page 21

QUESTION 266
By default, what type of rules in the Access Control rulebase allow the control connections?

A. Implicit Rules
B. Explicitly Implied Rules
C. Implied Rules
D. Explicit Rules

Correct Answer: C
Section:

QUESTION 267
The installation of a package via SmartConsole CANNOT be applied on

A. A single Security Gateway
B. A full Security Cluster (All Cluster Members included)
C. Multiple Security Gateways and/or Clusters
D. R81.20 Security Management Server

Correct Answer: A
Section:

QUESTION 268
Which type of Endpoint Identity Agent includes packet tagging and computer authentication?

A. Full
B. Custom
C. Light
D. Complete

Correct Answer: A
Section:
Explanation:
The type of Endpoint Identity Agent that includes packet tagging and computer authentication is Full. Packet tagging is a feature that allows the Endpoint Identity Agent to add a tag to the packets sent by the user's device, which contains the user's identity information. This way, the Security Gateway can identify the user without requiring additional authentication methods. Computer authentication is a feature that allows the Endpoint Identity Agent to authenticate the user's device using a certificate, which ensures that only authorized devices can access the network resources. The Full Endpoint Identity Agent supports both packet tagging and computer authentication, as well as other features such as Single Sign-On (SSO), Multi-Factor Authentication (MFA), and VPN.
The references are:
Check Point R81 Identity Awareness Administration Guide, page 15
Endpoint Identity Agent - Check Point CheckMates
Check Point Identity Agent - All flavors for Windows OS in a single package (Full, Light, v1 and v2 for Terminal Server)

QUESTION 269
What kind of information would you expect to see when using the 'sim affinity -I' command?

A. Overview over SecureXL templated connections
B. The VMACs used in a Security Gateway cluster

C. Affinity Distribution

D. The involved firewall kernel modules in inbound and outbound packet chain

Correct Answer: C
Section:
Explanation:
The ''sim affinity -l'' command is a command that displays the affinity distribution of the Security Gateway's interfaces. Affinity distribution is the assignment of CPU cores to handle the traffic from different interfaces. The ''sim affinity -l'' command shows the following information for each interface:
The interface name, such as eth0, eth1, etc.
The interface index, such as 0, 1, 2, etc.
The interface type, such as physical, bond, VLAN, etc.
The interface state, such as up or down
The interface speed, such as 1000 Mbps, 10000 Mbps, etc.
The interface MTU, such as 1500, 9000, etc.
The interface MAC address, such as 00:11:22:33:44:55
The interface IP address, such as 192.168.1.1, 10.0.0.1, etc.
The interface affinity mask, such as 0x00000001, 0x00000002, etc. The affinity mask is a hexadecimal value that represents the CPU cores that are assigned to handle the traffic from the interface. For example, 0x00000001 means that only CPU core 0 is assigned, 0x00000003 means that CPU cores 0 and 1 are assigned, and so on.
The ''sim affinity -l'' command can help you to monitor and optimize the performance of your Security Gateway by showing you how the traffic load is distributed among the CPU cores. You can also use the ''sim affinity'' command with other options to change the affinity settings of the interfaces or the firewall instances. For more information, you can refer to the Check Point R81.20 (Titan) Resolved Issues and Enhancements1 or the Solved: Sim Affinity - Check Point CheckMates2.

QUESTION 270
Where is the license for Check Point Mobile users installed?

A. The Primary Gateway

B. The Standby Gateway

C. The Endpoint Server

D. The Security Management Server

Correct Answer: D
Section:
Explanation:
The license for Check Point Mobile users is installed on the Security Management Server. Check Point Mobile is a client application that allows remote users to securely access corporate resources from their mobile devices. To use Check Point Mobile, you need to have a valid license for the Mobile Access Software Blade on the Security Management Server. The license determines the number of concurrent users that can connect to the Security Gateway using Check Point Mobile. You can view and manage the license from the SmartConsole or the CPUSE WebUI. For more information, you can refer to the Check Point R81 Mobile Access Blade Administration Guide1 or the Check Point Cybersecurity BootCamp R81.20 -- CCSA & CCSE Training2.

QUESTION 271
There are 4 ways to use the Management API for creating host object with the Management API. Which one is NOT correct?

A. Using cpconfig

B. Using CLISH

C. Using SmartConsole GUI console

D. Using Web Services

Correct Answer: A
Section:

QUESTION 272
Which is the command to identify the NIC driver before considering about the employment of the Multi-Queue feature?

A. ip show int eth0
B. show interface eth0 mq
C. ifconfig -i eth0 verbose
D. ethtool -i eth0

Correct Answer: D
Section:

QUESTION 273
Name the authentication method that requires token authenticator.

A. SecureID
B. DynamicID
C. Radius
D. TACACS

Correct Answer: A
Section:
Explanation:
The correct answer is A) SecureID.
SecureID is an authentication method that uses a token-based system to generate one-time passwords (OTPs) for users. Users need to have a physical or software token that displays a code that changes periodically. The code is used along with a personal identification number (PIN) to authenticate the user.
DynamicID is another authentication method that uses OTPs, but it does not require a token. Instead, it sends the OTP to the user's email or phone number.
Radius and TACACS are protocols that allow remote authentication of users through a centralized server. They do not use tokens, but they can support different types of authentication methods, such as passwords, certificates, or OTPs.
Certified Security Expert (CCSE) R81.20 Course Overview1
What Is Token-Based Authentication? | Okta2

QUESTION 274
Identity Awareness lets an administrator easily configure network access and auditing based on three items. Choose the correct statement.

A. Network location, the identity of a user and the identity of a machine.
B. Geographical location, the identity of a user and the identity of a machine.
C. Network location, the identity of a user and the active directory membership.
D. Network location, the telephone number of a user and the UID of a machine.

Correct Answer: A
Section:
Explanation:
The correct answer is A. Network location, the identity of a user and the identity of a machine.
Identity Awareness allows you to easily configure network access and auditing based on three items: network location, the identity of a user and the identity of a machine1. This enables you to create granular and accurate identity-based policies that control who can access what, when and how. You can also monitor and log user and machine activities for compliance and auditing purposes.
Geographical location, the telephone number of a user and the UID of a machine are not the items that Identity Awareness uses to identify and authorize users and machines.
Identity Awareness - Check Point Software1

QUESTION 275
Which of the following cannot be configured in an Access Role Object?

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

Correct Answer: D
Section:
Explanation:
The verified answer is D) Time.
An Access Role object is a logical representation of a set of users, machines, or networks that can be used in the security policy1. An Access Role object can include the following components1:
Networks: IP addresses or network objects that define the source or destination of the traffic.
Machines: Specific hosts or machine groups that are identified by their MAC addresses or certificates.
Users: Specific users or user groups that are authenticated by one or more identity sources, such as Active Directory, LDAP, or Identity Awareness.
Time is not a component of an Access Role object, and it cannot be configured in it. Time is a separate object type that can be used to define the validity period of a rule or a policy2.
LDAP group vs Access role objects - Check Point CheckMates3
THE IMPORTANCE OF ACCESS ROLES - Check Point Software1
Time Objects - Check Point Software2

QUESTION 276
While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?

A. Security Gateway is not part of the Domain
B. SmartConsole machine is not part of the domain
C. Identity Awareness is not enabled on Global properties
D. Security Management Server is not part of the domain

Correct Answer: B
Section:
Explanation:
The verified answer is B) SmartConsole machine is not part of the domain.
The Identity Awareness wizard uses the SmartConsole machine to detect the windows domain by querying the Active Directory server using DCOM protocol1. If the SmartConsole machine is not part of the domain, the query will fail and the wizard will not automatically detect the domain. The user will have to manually enter the domain name and credentials to proceed with the configuration.
The Security Gateway, the Security Management Server, and the Identity Awareness global properties do not affect the domain detection by the wizard. However, they are required for other aspects of the Identity Awareness blade, such as AD Query, Identity Collector, and Browser-Based Authentication2.
Identity Awareness Configuration wizard authentication fails3
Identity Awareness - Check Point Software4

QUESTION 277
Which command collects diagnostic data for analyzing a customer setup remotely?

A. cpv
B. cpinfo
C. migrate export
D. sysinfo

Correct Answer: B
Section:
Explanation:
The verified answer is B) cpinfo.
cpinfo is a command that collects diagnostic data for analyzing a customer setup remotely. It is an auto-updatable utility that runs on the customer's machine and uploads the data to Check Point servers. The data includes information about the system, the security policy, the objects, and the logs. Check Point support engineers can use the DiagnosticsView utility to open the cpinfo file and view the customer's configuration and environment settings1.
migrate export is a command that exports the Check Point configuration and database files to a compressed file. It is used for backup and migration purposes, not for remote analysis2.
sysinfo is a command that displays basic information about the system, such as the hostname, the OS version, the CPU model, and the memory size. It does not collect or upload any data to Check Point servers3.
cpv is not a valid command in Check Point.
Support, Support Requests, Training ... - Check Point Software1
Migrate export - Check Point Software
sysinfo - Check Point Software

QUESTION 278
Alice was asked by Bob to implement the Check Point Mobile Access VPN blade - therefore are some basic configuration steps required - which statement about the configuration steps is true?

A. 1. Add a rule in the Access Control Policy and install policy 2. Configure Mobile Access parameters in Security Gateway object 3. Enable Mobile Access blade on the Security Gateway object and complete the wizard 4. Connect to the Mobile Access Portal
B. 1. Connect to the Mobile Access Portal 2. Enable Mobile Access blade on the Security Gateway object and complete the wizard 3. Configure Mobile Access parameters in Security Gateway object 4. Add a rule in the Access Control Policy and install policy
C. 1. Configure Mobile Access parameters in Security Gateway object 2. Enable Mobile Access blade on the Security Gateway object and complete the wizard 3. Add a rule in the Access Control Policy and install policy 4. Connect to the Mobile Access Portal
D. 1. Enable Mobile Access blade on the Security Gateway object and complete the wizard 2. Configure Mobile Access parameters in Security Gateway object 3. Add a rule in the Access Control Policy and install policy 4. Connect to the Mobile Access Portal

Correct Answer: D
Section:
Explanation:
The verified answer is D) 1. Enable Mobile Access blade on the Security Gateway object and complete the wizard 2. Configure Mobile Access parameters in Security Gateway object 3. Add a rule in the Access Control Policy and install policy 4. Connect to the Mobile Access Portal
The basic configuration steps for the Check Point Mobile Access VPN blade are as follows1:
Enable Mobile Access blade on the Security Gateway object and complete the wizard: This step activates the Mobile Access blade on the selected gateway and guides you through the initial configuration, such as defining the portal name, the certificate, and the authentication methods.
Configure Mobile Access parameters in Security Gateway object: This step allows you to customize the Mobile Access settings, such as defining the supported applications, the access roles, the client settings, and the advanced options.
Add a rule in the Access Control Policy and install policy: This step creates a rule that allows the traffic from the Mobile Access portal to the protected resources and installs the policy on the gateway.
Connect to the Mobile Access Portal: This step verifies that the Mobile Access portal is accessible and functional from a web browser or a mobile device.
The other options are incorrect because they do not follow the correct order or include the necessary steps.
Mobile Access Administration Guide R81 - Check Point Software1

QUESTION 279
What destination versions are supported for a Multi-Version Cluster Upgrade?

A. R77.30 and later
B. R80.10 and Later
C. R70 and Later
D. R76 and later

Correct Answer: B
Section:
Explanation:
The correct answer is B) R80.10 and later.
According to the Check Point documentation1, the Multi-Version Cluster Upgrade (MVC) is a new feature in R80.40 and higher that replaces the Connectivity Upgrade (CU) method. MVC allows you to upgrade a cluster to a newer version without a loss in connectivity and test the new version on some of the cluster members before you decide to upgrade the rest of the cluster members. The MVC feature supports the following destination versions2:
R80.10
R80.20
R80.30
R80.40
R81
R81.20
The other options are incorrect because they are either not supported by MVC or they are older than the source version (R80.40).
Multi-Version Cluster (MVC) replaces Connectivity Upgrade (CU) in R80.401
ClusterXL upgrade methods and paths2

QUESTION 280
Which of the following is true regarding the Proxy ARP feature for Manual NAT?

A. The local.arp file must always be configured
B. Automatic proxy ARP configuration can be enabled
C. fw ctl proxy should be configured
D. Translate Destination on Client Side should be configured

Correct Answer: B
Section:
Explanation:
The verified answer is B) Automatic proxy ARP configuration can be enabled.
Proxy ARP is a feature that allows a gateway to respond to ARP requests on behalf of another IP address that is not on the same network segment. Proxy ARP is required for manual NAT rules when the NATed IP addresses are not routed to the gateway1.
By default, proxy ARP for manual NAT rules has to be configured manually by editing the local.arp file or using the CLISH commands on the gateway2. However, since R80.10, there is an option to enable automatic proxy ARP configuration for manual NAT rules by modifying the files $CPDIR/tmp/.CPprofile.sh and $CPDIR/tmp/.CPprofile.csh on the gateway3.
fw ctl proxy is a command that displays the proxy ARP table on the gateway, but it does not configure proxy ARP4.
Translate Destination on Client Side is a NAT option that determines whether the destination IP address is translated before or after the routing decision. It does not affect proxy ARP.
Configuring Proxy ARP for Manual NAT - Check Point Software1
R80.10: Automatic Proxy ARP with Manual NAT rules - checkpoint<dot>engineer2
Automatic creation of Proxy ARP for Manual NAT rules on Security Gateway R80.103
fw ctl proxy - Check Point Software
NAT Properties - Check Point Software

QUESTION 281
What are the Threat Prevention software components available on the Check Point Security Gateway?

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

Correct Answer: C
Section:
Explanation:
The Threat Prevention software components available on the Check Point Security Gateway are IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction. These components provide comprehensive protection against various types of cyber threats, such as network attacks, malware, ransomware, phishing, zero-day exploits, data leakage, and more. IPS is a network security component that detects and prevents malicious traffic based on signatures, behavioral patterns, and anomaly detection. Anti-Bot is a network security component that detects and blocks botnet communications and command-and-control servers. Anti-Virus is a network security component that scans files for known viruses, worms, and trojans. Threat Emulation is a network security component that emulates files in a sandbox environment to detect unknown malware and prevent zero-day attacks. Threat Extraction is a network security component that removes malicious content from files and delivers clean files to users.
Reference: [Check Point R81 Threat Prevention Administration Guide], page 9-10

QUESTION 282
Alice & Bob are going to deploy Management Data Plane Separation (MDPS) for all their Check Point Security Gateway(s)/Cluster(s). Which of the following statement is true?

A. Each network environment is dependent and includes interfaces, routes, sockets, and processes
B. Management Plane -- To access, provision and monitor the Security Gateway
C. Data Plane -- To access, provision and monitor the Security Gateway
D. Management Plane -- for all other network traffic and processing

Correct Answer: B
Section:
Explanation:
Management Data Plane Separation (MDPS) is a feature that allows the separation of the management plane and the data plane on a Security Gateway or a cluster. The management plane is responsible for accessing, provisioning and monitoring the Security Gateway, while the data plane is responsible for all other network traffic and processing.Each network environment is independent and includes interfaces, routes, sockets, and processes1.
Reference:Check Point R81 Administration Guide

QUESTION 283
In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

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

Correct Answer: C
Section:
Explanation:
In order for changes made to policy to be enforced by a Security Gateway, an administrator must perform the action of installing policy. Installing policy is the process of transferring the policy package from the Security Management Server to the Security Gateway. Publishing changes is the process of saving changes to the database and making them available to other administrators.Saving changes is the process of saving changes to a session without publishing them2.
Reference:Check Point R81 Security Management Guide

QUESTION 284
The Check Point installation history feature in provides the following:

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

D. View install changes

Correct Answer: C
Section:
Explanation:
The Check Point installation history feature provides the following:
Policy Installation Date: The date and time when the policy was installed on the Security Gateway.
View install changes: The ability to view the differences between two policy versions that were installed on the Security Gateway.
Install specific version: The ability to install a specific policy version from the installation history on the Security Gateway3.
Reference:Check Point R81 SmartConsole Guide

QUESTION 285
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 286
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 287
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 288
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.