Checkpoint.156-582.by.Endy.40q

Number: 156-582
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 156-582

Exam Name: Check Point Certified Troubleshooting Administrator - R81.20

Exam A

QUESTION 1
Check Point provides tools & commands to help you identify issues about products and applications. Which Check Point command can help you display status and statistics information for various Check Point products and applications?

A. cpstat

B. CP-stat

C. CPview

D. fwstat

Correct Answer: A
Section:
Explanation:
The cpstat command is a versatile tool provided by Check Point to display status and statistics for various Check Point products and applications. It offers insights into system performance, service statuses, and resource utilization, which are essential for diagnosing and resolving issues effectively.

QUESTION 2
Running tcpdump causes a significant increase in CPU usage, what other option should you use?

A. o

B. O

C. I

D. i

Correct Answer: C
Section:
Explanation:
(Note: The provided multiple-choice options for this question appear to be incomplete or incorrect. The best practice and commonly recommended alternative to tcpdump on Check Point to reduce CPU usage is cppcap. If we assume option 'C' corresponds to using cppcap, we select that.)
Given the context, the correct answer is C, assuming it refers to cppcap. cppcap is optimized for packet capturing in Check Point environments and is less CPU-intensive compared to tcpdump.

QUESTION 3
You tested the connection from source to destination and you are not able to find logs in your Security Management. What is the best possible reason?

A. The FWM process crashed on Security Management, therefore logging will not work.

B. There is not enough storage in Security Management, so the logs can't be stored.

C. The logging blade was not enabled on Security Gateway.

D. The gateway is logging locally.

Correct Answer: C
Section:
Explanation:
If logs are not appearing in the Security Management despite successful traffic flow, the most likely reason is that the logging blade is not enabled on the Security Gateway. Without enabling the logging functionality, the gateway will not send logs to the Security Management Server, even though the traffic itself is passing through successfully.

QUESTION 4
You need to switch the active log file on the Security Gateway. What is the correct command?

A. fw -p -o <log file> switch
B. fw logswitch
C. Install security policy
D. fw switchlog

Correct Answer: B
Section:
Explanation:
The fw logswitch command is used to switch the active log file on a Check Point Security Gateway. This command forces the gateway to start writing logs to a new file, which is useful for log management and troubleshooting purposes. Other options listed are either incorrect or do not perform the log-switching function.

QUESTION 5
Customer wants to use autonomous threat prevention. How do you enable it?

A. Enable Autonomous Threat Prevention on the Security Gateway from the SmartConsole: Gateway and Servers view and enable IPS on the Security Gateway by the command: ips on.
B. Enable Autonomous Threat Prevention on the Security Gateway from the SmartConsole: Gateway and Servers view, the default profile Strict Security will be selected.
C. Enable Autonomous Threat Prevention on the Security Gateway from the SmartConsole: Gateway and Servers view, inspection profile is not needed, the Security Gateway will automatically select the best profile according to deployment.
D. Enable Autonomous Threat Prevention on the Security Gateway from the SmartConsole: Gateway and Servers view, then select inspection profile.

Correct Answer: D
Section:
Explanation:
To enable Autonomous Threat Prevention on a Security Gateway, navigate to the Gateway and Servers view in SmartConsole, enable the feature, and then select an appropriate inspection profile. Selecting the inspection profile allows administrators to define the level of threat prevention and customize the security measures based on the organization's specific needs and deployment scenarios.

QUESTION 6
What are the available types of licenses in Check Point?

A. Evaluation, Perpetual, Trial, Subscription
B. Evaluation, Perpetual, Test, Free
C. Free, Evaluation, Annual, Lifetime
D. Annual, Perpetual, Test, Free

Correct Answer: A
Section:
Explanation:
Check Point offers several types of licenses to cater to different customer needs:
Evaluation: Short-term licenses for testing and evaluation purposes.
Perpetual: Licenses that are valid indefinitely, typically involving a one-time purchase.
Trial: Temporary licenses that allow full functionality for a limited period.
Subscription: Licenses that are valid for a specific duration (e.g., annual) and require renewal.
These licensing options provide flexibility for organizations to choose based on their operational requirements and budget constraints.

QUESTION 7

When accessing License Status In Smart Console, what information is available?

A. Blade Name, License Status, Expiration Date, Additional info
B. Expiration Date, Status, SKU, Signature Key
C. Blade Name, Expiration Date, Attached to, Status
D. License Status, Blade Name, Report available, Download

Correct Answer: C
Section:
Explanation:
In SmartConsole, when accessing the License Status, the following information is available:
Blade Name: Identifies the specific security blade the license pertains to.
Expiration Date: Indicates when the license will expire.
Attached to: Shows which device or component the license is attached to.
Status: Reflects the current state of the license (e.g., active, expired).
This information helps administrators monitor and manage their licenses effectively, ensuring that all security features remain operational.

QUESTION 8
What are the commands to verify the Smart Contracts on the Security Gateway?

A. cpconfig and contracts_mgmt
B. cpconfig and cpcontract
C. cpinfo and cplic
D. contractjtil and cplic

Correct Answer: A
Section:
Explanation:
To verify Smart Contracts on a Security Gateway, the cpconfig and contracts_mgmt commands are used.
cpconfig: Allows configuration and verification of various Check Point settings, including licensing and contract details.
contracts_mgmt: Specifically manages and verifies contract information, ensuring that the correct licenses and contracts are in place for the deployed security features.
These commands are essential for ensuring that the Security Gateway has the necessary contracts to enforce security policies effectively.

QUESTION 9
Which of the following CLI commands is best to use for getting a quick look at appliance performance information in Gaia?

A. fw stat
B. fw monitor
C. cpview
D. cphaprob stat

Correct Answer: C
Section:
Explanation:
The cpview command in Gaia provides a real-time, comprehensive view of the system's performance metrics, including CPU usage, memory utilization, and network statistics. This makes it the best choice for quickly assessing the performance of a Check Point appliance. Other commands like fw stat and fw monitor are more focused on firewall statistics and traffic monitoring, respectively. cphaprob stat is used for High Availability status checks, not general performance metrics.

QUESTION 10

You want to work with a license for your gateway in User Center portal, but all options are greyed out. What is the reason?

A. Your account has classification permission to Viewer
B. Your account has classification permission to Licenser
C. You are not defined as Support Contact
D. Your account does not have any rights

Correct Answer: C
Section:
Explanation:
When all licensing options are greyed out in the User Center portal, it typically indicates that the user does not have the necessary permissions to manage licenses. Specifically, the user might not be defined as a Support Contact, which is required to perform licensing actions. Being a Viewer or Licenser does not grant full access to manage licenses, and having no rights would also restrict access, but the most precise reason in this context is the lack of a Support Contact definition.

QUESTION 11

What is the process of intercepting and logging traffic?

A. Debugging
B. Forensics Analysis
C. Logging
D. Packet Capturing

Correct Answer: D
Section:
Explanation:
Packet capturing involves intercepting and logging network traffic as it traverses the network. Tools like fw monitor and tcpdump are commonly used for this purpose in Check Point environments. While logging (Option C) refers to recording events, packet capturing specifically deals with the interception and detailed logging of network packets for analysis.

QUESTION 12

Which of the following is NOT an account user classification?

A. Licensers
B. Manager
C. Viewer
D. Administrator

Correct Answer: A
Section:
Explanation:
In Check Point's user classification for the User Center portal, typical roles include Manager, Viewer, and Administrator. 'Licensers' is not a standard user classification. Instead, licensing roles are usually managed under broader administrative categories. Therefore, 'Licensers' is not recognized as a distinct user classification.

QUESTION 13

You want to collect diagnostics data to include with an SR (Service Request). What command or utility best meets your needs?

A. cpconfig

B. cpinfo
C. cpplic
D. contracts_mgmt

Correct Answer: B
Section:
Explanation:
The cpinfo command is designed to collect comprehensive diagnostic information from a Check Point gateway or management server. This data is essential when submitting a Service Request (SR) to Check Point Support, as it includes configuration details, logs, and system information. cpconfig is used for configuration, cpplic manages licenses, and contracts_mgmt handles contract management, none of which are specifically tailored for collecting diagnostic data for SRs.

QUESTION 14
During a problem isolation with the OSI model, what layer will you investigate when the issue is ARP or MAC address?

A. Network level
B. Layer 2
C. Physical
D. Layer 3

Correct Answer: B
Section:
Explanation:
ARP (Address Resolution Protocol) and MAC (Media Access Control) addresses operate at Layer 2 of the OSI model, which is the Data Link Layer. This layer is responsible for node-to-node data transfer and handling MAC addressing. Issues with ARP or MAC addresses indicate problems at this specific layer, necessitating an investigation into Layer 2.

QUESTION 15
Check Point's self-service knowledge base of technical documents and tools covers everything from articles describing how to fix specific issues, understand error messages and to how to plan and perform product installation and upgrades. This knowledge base is called:

A. SupportCenterBase
B. SecureDocs
C. SupportDocs
D. SecureKnowledge

Correct Answer: D
Section:
Explanation:
Check Point's self-service knowledge base is known as SecureKnowledge. It provides a comprehensive repository of technical documents, guides, troubleshooting steps, and tools necessary for managing and resolving issues related to Check Point products. The other options listed are either incorrect or do not represent the official name of Check Point's knowledge base.

QUESTION 16
Which of the following System Monitoring Commands (Linux) shows process resource utilization, as well as CPU and memory utilization?

A. df
B. free
C. ps
D. top

Correct Answer: D
Section:
Explanation:
The top command in Linux provides a real-time, dynamic view of system processes, showing CPU and memory usage among other metrics. It is the most suitable command for monitoring process resource utilization continuously. In contrast, df displays disk space usage, free shows memory usage, and ps provides a snapshot of current processes but without the dynamic, real-time monitoring that top offers.

QUESTION 17
What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

A. .pea
B. .exe
C. .cap
D. .tgz

Correct Answer: C
Section:
Explanation:
The .cap file extension is commonly used for packet capture files that can be imported and analyzed in Wireshark. When using fw monitor, specifying the output file with a .cap extension ensures compatibility with Wireshark for detailed packet analysis. Other extensions like .exe and .tgz are not suitable for packet captures, and .pea is not a standard extension for this purpose.

QUESTION 18
How many different types of Service Requests exist?

A. 4
B. 2
C. 3
D. 5

Correct Answer: A
Section:
Explanation:
Check Point categorizes Service Requests (SRs) into four main types: Technical Support, Product Enhancement, Billing and Licensing, and Other Services. Each type caters to different aspects of customer needs, ensuring that users can address a wide range of issues and requests through the appropriate channels.

QUESTION 19
When opening a new Service Request, what feature is in place to help guide you through the process?

A. The SmartConsole Help feature
B. The TAC chat room
C. An SR wizard
D. An SR API

Correct Answer: C
Section:
Explanation:
When opening a new Service Request (SR) in Check Point's User Center portal, an SR wizard guides users through the process. This wizard assists in collecting necessary information, categorizing the request appropriately, and ensuring that all required details are provided to expedite the resolution process. The SR wizard simplifies the SR creation process, making it more user-friendly and efficient.

QUESTION 20
Which of the following is NOT a way to insert fw monitor into the chain when troubleshooting packets throughout the chain?

A. Relative position using id
B. Absolute position
C. Relative position using location
D. Relative position using alias

Correct Answer: D
Section:
Explanation:
When using fw monitor for packet capture in Check Point environments, packets can be monitored at various points in the inspection chain. The insertion methods include specifying a relative position using an identifier (id), using an absolute position, or specifying the position based on location within the chain. However, using an alias to determine the relative position is not a recognized method for inserting fw monitor into the inspection chain.

QUESTION 21
Which Layer of the OSI Model is responsible for routing?

A. Network
B. Transport
C. Session
D. Data link

Correct Answer: A
Section:
Explanation:
Routing decisions are made at the Network Layer (Layer 3) of the OSI model. This layer is responsible for determining the best path for data packets to travel from the source to the destination across multiple networks. Protocols like IP (Internet Protocol) operate at this layer, handling addressing and routing functions essential for network communication.

QUESTION 22
The communication between the Security Management Server and Security Gateway to forward logs is done using the following process and port number:

A. fwd, TCP 257
B. cpm, 19009
C. fwm, TCP 18190
D. fwm, TCP 257

Correct Answer: A
Section:
Explanation:
The FWD process communicates between the Security Management Server and the Security Gateway to forward logs using TCP port 257. This port is designated for log transmission, ensuring that logs are efficiently and securely sent from the gateway to the management server for centralized analysis and storage.

QUESTION 23
Where would you look to find the error log file to investigate a logging issue on the Security Management Server?

A. SFWDIR/log/fwd.elg

B. SCPDIR/log/cpd.elg
C. SMDS_FWDIR/log/cpm.elg
D. SFWDIR/log/fwm.elg

Correct Answer: A
Section:
Explanation:
The error log file for logging issues on the Security Management Server is located at SFWDIR/log/fwd.elg. This file contains detailed error messages and diagnostic information related to the FWD process, which is responsible for log forwarding. Reviewing this file can help identify and resolve issues preventing logs from being correctly transmitted.

QUESTION 24
Which is the correct 'fw monitor' syntax for creating a capture file for loading it into Wireshark?

A. fw monitor -e 'accept <FILTER EXPRESSION*;' > Output.cap
B. This cannot be accomplished as it is not supported with R80.10
C. fw monitor -e 'accept <FILTER EXPRESSION^' -o Output.cap
D. fw monitor -e 'accept <FILTER EXPRESSION*;' -file Output.cap

Correct Answer: D
Section:
Explanation:
The correct syntax for using fw monitor to create a capture file compatible with Wireshark involves specifying the filter expression and the output file with the .cap extension. Option D correctly uses the -e flag for the filter expression and the -file flag to specify the output file, ensuring the captured data can be seamlessly imported into Wireshark for analysis.

QUESTION 25
What is the most efficient way to view large fw monitor captures and run filters on the file?

A. snoop
B. CLI
C. CLISH
D. Wireshark

Correct Answer: D
Section:
Explanation:
Wireshark is the most efficient tool for viewing large fw monitor capture files. It provides powerful filtering capabilities, a user-friendly interface, and detailed packet analysis features that make handling large datasets manageable. While CLI tools like snoop and fw monitor offer basic packet viewing, they lack the advanced filtering and visualization options that Wireshark provides.

QUESTION 26
Running tcpdump causes a significant increase on CPU usage, what other option should you use?

A. fw monitor
B. Wait for out of business hours to do a packet capture
C. cppcap
D. You need to use tcpdump with -e option to decrease the length of packet in captures and it will utilize the less CPU

Correct Answer: C

Section:
Explanation:
When tcpdump causes high CPU usage, an alternative is to use cppcap, which is optimized for capturing packets with lower CPU overhead in Check Point environments. cppcap is designed to work efficiently with Check Point's infrastructure, reducing the performance impact compared to generic tools like tcpdump.

QUESTION 27
Which of the following is a valid way to capture packets on Check Point gateways?

A. Firewall logs
B. Wireshark
C. tcpdump
D. Network taps

Correct Answer: C
Section:
Explanation:
tcpdump is a valid and commonly used tool for capturing packets on Check Point gateways. It allows administrators to capture and analyze network traffic directly from the command line. While Wireshark can be used to analyze the captured packets, the actual capture is typically performed using tcpdump. Network taps are hardware devices and not software methods, and firewall logs provide event logging rather than packet-level capture.

QUESTION 28
Which of the following is true about tcpdump?

A. The tcpdump can only capture TCP packets and not UDP packets
B. A tcpdump session can be initiated from the SmartConsole
C. The tcpdump has to be run from clish mode in Gaia
D. Running tcpdump without the correct switches will negatively impact the performance of the Firewall

Correct Answer: D
Section:
Explanation:
Running tcpdump without appropriate filtering or with verbose options can lead to excessive CPU usage and impact the performance of the firewall. It is essential to use specific switches and filters to limit the scope of the capture to necessary traffic only, thereby minimizing the performance overhead. Contrary to Option A, tcpdump can capture various types of packets, including TCP and UDP. Option B is incorrect as tcpdump is run from the command line, not initiated directly from SmartConsole. Option C is partially true but not as directly relevant as the impact on performance.

QUESTION 29
What is a primary advantage of using the fw monitor tool?

A. It is menu-driven, making it easy to configure
B. It can capture packets in various positions as they move through the firewall
C. It has no negative impact on firewall performance
D. It always captures all packets hitting the physical layer

Correct Answer: B
Section:
Explanation:
The primary advantage of using the fw monitor tool is its ability to capture packets at multiple inspection points within the firewall's processing chain. This allows for detailed analysis of how packets are handled at different stages, facilitating effective troubleshooting and performance optimization. While fw monitor is efficient, it can still impact performance if not used judiciously, and it does not capture all physical layer traffic unless specifically configured to do so.

QUESTION 30
After reviewing the Install Policy report and error codes listed in it, you need to check if the policy installation port is open on the Security Gateway. What is the correct port to check?

A. 19009
B. 18190
C. 18210
D. 18191

Correct Answer: D
Section:
Explanation:
Port 18191 is used by Check Point for communication between the Security Management Server and the Security Gateway during policy installations. Ensuring that this port is open and not blocked by any firewall rules is crucial for successful policy deployment. Other ports listed serve different functions within the Check Point ecosystem.

QUESTION 31
Which of the following allows you to capture packets at four inspection points as they traverse a Check Point gateway?

A. tcpdump
B. Firewall logs
C. Kernel debugs
D. fw monitor

Correct Answer: D
Section:
Explanation:
The fw monitor tool allows packet capture at multiple inspection points within a Check Point gateway, typically four in total. This capability provides comprehensive visibility into how packets are processed as they move through different stages of the firewall's inspection chain, facilitating effective troubleshooting and analysis.

QUESTION 32
What is the port for the Log Collection on Security Management Server?

A. 18191
B. 443
C. 258
D. 257

Correct Answer: D
Section:
Explanation:
Port 257 is used for log collection on the Security Management Server. This port facilitates the transmission of log data from Security Gateways to the Management Server, ensuring that logs are centralized for monitoring, analysis, and reporting.

QUESTION 33
What Check Point process controls logging?

A. CPWD
B. FWD

C. CPD

D. CPM

Correct Answer: B
Section:
Explanation:
The FWD (Firewall Daemon) process is responsible for controlling logging in Check Point environments. It manages the creation, storage, and transmission of logs from Security Gateways to the Security Management Server, ensuring that all relevant security events are recorded and available for analysis.

QUESTION 34
As a security administrator/engineer in your company, you have noticed that your HQ Check Point Security Management Server is not receiving logs from your HQ Check Point Gateway/Cluster. To investigate this issue in the command line, you will need to verify which process is running?

A. cpm

B. cpd

C. fwd

D. fwm

Correct Answer: C
Section:
Explanation:
To troubleshoot why the Security Management Server is not receiving logs from the Security Gateway or Cluster, you should verify the status of the FWD process. The fwd daemon handles log forwarding and ensures that logs are transmitted from the gateway to the management server. Checking if fwd is running and functioning correctly is essential for resolving log transmission issues.

QUESTION 35
How would you check the connection status of a gateway to the Log server?

A. Run netstat -anp | grep :257 in CLISH on Log server

B. Run netstat -anp | grep :257 in expert mode on Log server

C. Run netstat -anp | grep :18187 in expert mode on Log server

D. Run netstat -anp | grep :18187 in CLISH on Log server

Correct Answer: B
Section:
Explanation:
To check the connection status between a gateway and the Log server, use the netstat -anp | grep :257 command in expert mode on the Log server. This command filters the network connections to display only those related to port 257, which is used for log collection. Running it in expert mode provides the necessary privileges to view detailed network information.

QUESTION 36
When managing the disk space for locally stored logs, the Delete threshold for the gateway cannot be more than what percentage of the total disk space?

A. 10%

B. 75%

C. 50%

D. 25%

Correct Answer: B
Section:

Explanation:
The Delete threshold for managing locally stored logs on a Security Gateway should not exceed 75% of the total disk space. This threshold ensures that there is ample space for new logs while preventing the disk from becoming overly full, which could lead to system instability or loss of logging capabilities.

QUESTION 37
To verify that communication is working between the Security Management Server and the Security Gateway, which service port should be checked?

A. 257
B. 18209
C. 259
D. 19009

Correct Answer: A
Section:
Explanation:
Port 257 is used for log collection and communication between the Security Management Server and the Security Gateway. Verifying that this port is open and accessible ensures that logs are successfully transmitted from the gateway to the management server, facilitating effective monitoring and analysis.

QUESTION 38
You want to print the status of WatchDog-monitored processes. What command best meets your needs?

A. cpwd_admin list
B. tcpdump
C. cppcap
D. cpplic print

Correct Answer: A
Section:
Explanation:
The cpwd_admin list command is used to display the status of processes monitored by the WatchDog service in Check Point. WatchDog ensures that critical processes are running and restarts them if they fail, maintaining the stability and security of the gateway.

QUESTION 39
The Check Point FW Monitor tool captures and analyzes incoming packets at multiple points in the traffic inspections. Which of the following is the correct inspection flow for traffic?

A. (i) - pre-inbound, (I) - post-inbound, (o) - pre-outbound, (O) - post-outbound
B. (o) - pre-outbound, (O) - post-inbound, (i) - pre-inbound, (I) - post-inbound
C. (O) - post-outbound, (o) - pre-outbound, (I) - post-inbound, (i) - pre-inbound
D. (1) - pre-inbound, (i) - post-inbound, (O) - pre-outbound, (o) - post-outbound

Correct Answer: A
Section:
Explanation:
The correct inspection flow using fw monitor is:
(i) - pre-inbound: Before the packet enters the inbound processing path.
(I) - post-inbound: After the inbound processing.
(o) - pre-outbound: Before the packet enters the outbound processing path.
(O) - post-outbound: After the outbound processing.

This sequence ensures that packets are captured and analyzed at all critical points during their traversal through the firewall.

QUESTION 40
What does the FWD daemon instruct the gateway to do when communication issues between the gateway and SMS/Log Server occur?

A. It instructs the gateway to continue forwarding logs to SMS/Log Server and the logs will be stored in a holding queue for the server until communication is restored.
B. It instructs the gateway to stop logging until it can restore communication.
C. It instructs the gateway to store logs locally as it continues to try to restore communication.
D. It instructs the gateway to only log a specified number of logs as defined in the Security Policy.

Correct Answer: C
Section:
Explanation:
When there are communication issues between the Security Gateway and the Security Management Server (SMS)/Log Server, the FWD daemon directs the gateway to store logs locally. This ensures that logging continues without interruption, and the logs are queued until communication with the SMS/Log Server is re-established, preventing any loss of log data.