CheckPoint.156-582.v2025-08-25.q27

Exam Code:	156-582
Exam Name:	Check Point Certified Troubleshooting Administrator - R81.20
Certification Provider:	CheckPoint
Free Question Number:	27
Version:	v2025-08-25
# of views:	155
# of Questions views:	270
https://www.exam-tests.com/156-582-exam/CheckPoint.156-582.v2025-08-25.q27.html	

NEW QUESTION: 1
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
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 2
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
Answer: C (LEAVE A REPLY)

To troubleshoot why the Security Management Server is not receiving logs from the Security Gateway or Cluster, you should verify the status of theFWDprocess. 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.

NEW QUESTION: 3
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.
Answer: D (LEAVE A REPLY)
To enableAutonomous Threat Preventionon a Security Gateway, navigate to theGateway and Serversview in SmartConsole, enable the feature, and thenselect 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.

NEW QUESTION: 4
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
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 5

What are two types of SAs in the VPN negotiation?
A. IKE and VPND SA
B. IKE SA and VPN SA
C. IKE SA and IPsec SA
D. VPN SA and Main SA
Answer: C (LEAVE A REPLY)
In VPN negotiations, there are two primary types of Security Associations (SAs):
* IKE SA (Internet Key Exchange Security Association): Establishes the secure channel for negotiating IPsec parameters.
* IPsec SA (IP Security Security Association): Defines the parameters for the actual encrypted communication.
These SAs work together to ensure secure and authenticated VPN connections between gateways.

NEW QUESTION: 6
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
Answer: C (LEAVE A REPLY)
In SmartConsole, when accessing theLicense 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.

NEW QUESTION: 7
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
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 8
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
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 9
How do you verify that Proxy ARP entries are loaded into the kernel?
A. fw ctl arp
B. show arp dynamic all
C. This information can be viewed in the logs, under NAT section of log, field: Proxy ARP entry
D. fw ctl get arp list all
Answer: A (LEAVE A REPLY)
Thefw ctl arpcommand is used to verify that Proxy ARP entries are loaded into the kernel. This command provides detailed information about the current ARP table, including any Proxy ARP entries that have been established for NAT configurations. Ensuring that these entries are present confirms that the system is correctly handling ARP requests for NATed addresses.

NEW QUESTION: 10
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
Answer: D (LEAVE A REPLY)
Port18191is 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.

NEW QUESTION: 11
Which of the following is NOT an account user classification?
A. Licensers
B. Manager
C. Viewer
D. Administrator
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 12
For Threat Prevention, which process is enabled when the Policy Conversion process has debug turned on using the INTERNAL_POLICY_LOADING=1 command?
A. fwm
B. cpm
C. solr
D. dlpd
Answer: (SHOW ANSWER)
When thePolicy Conversionprocess has debugging enabled using theINTERNAL_POLICY_LOADING=1 command, thefwm(Firewall Manager) process is also enabled for detailed debugging. This allows administrators to monitor and troubleshoot the policy loading and conversion process more effectively, ensuring that policies are correctly applied and enforced.

NEW QUESTION: 13
What is the correct process for GUI connectivity issues with SmartConsole troubleshooting?
A. Processes (FWM and CPM), Connectivity, GUI clients, Certificate, Authentication
B. First troubleshoot Authentication and then the rest
C. Reinstall the SmartConsole and check if it's running properly
D. Connectivity, Processes (FWM and CPM), GUI clients, Certificate, Authentication
Answer: (SHOW ANSWER)
The correct troubleshooting process for GUI connectivity issues with SmartConsole involves the following steps in order:
* Connectivity: Ensure that the network connection between SmartConsole and the Management Server is stable.

* Processes (FWM and CPM): Verify that critical processes like FWM (Firewall Manager) and CPM (Check Point Management) are running correctly.
* GUI Clients: Check the client-side configurations and ensure that SmartConsole is properly installed and configured.
* Certificate: Ensure that the necessary certificates for secure communication are valid and correctly installed.
* Authentication: Confirm that user authentication mechanisms are functioning as expected.
Following this structured approach ensures that all potential issues are systematically addressed.

NEW QUESTION: 14
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
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 15
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
Answer: D (LEAVE A REPLY)
Wiresharkis 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.

NEW QUESTION: 16

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%

Answer: B (LEAVE A REPLY)

TheDelete thresholdfor managing locally stored logs on a Security Gateway should not exceed75%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.

Valid 156-582 Dumps shared by BraindumpsPass.com for Helping Passing 156-582 Exam! BraindumpsPass.com now offer the **newest 156-582 exam dumps**, the BraindumpsPass.com 156-582 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com 156-582 dumps with Test Engine here: https://www.braindumpspass.com/CheckPoint/156-582-practice-exam-dumps.html (**77** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 17

Services with expired licenses and contracts have,

A. full functionality for 90 days after they expire

B. full functionality for 45 days after they expire

C. no functionality

D. limited functionality

Answer: (SHOW ANSWER)

When licenses and contracts expire, services continue to operate withlimited functionality. This means that while some basic operations might still be available, advanced features and protections are disabled until the licenses are renewed or updated. This approach prevents complete loss of functionality while prompting administrators to address licensing issues.

NEW QUESTION: 18

When is the Enable Bypass Under Load used in IPS?

A. When the threshold is reached for connections and throughput

B. When there is a problem with IPS and connectivity cannot be guaranteed

C. When the threshold is reached for CPU and memory

D. When there is an ongoing attack, the Security Gateway puts its state to maintenance mode to prevent attackers from breaching the network

Answer: C (LEAVE A REPLY)
Enable Bypass Under Loadin Intrusion Prevention Systems (IPS) is used when the system reaches high thresholds for CPU and memory usage. This feature allows the IPS to bypass certain processing to maintain overall system performance and ensure that essential network functions continue operating smoothly despite resource constraints.

NEW QUESTION: 19
Which of the following is the most significant impact of not having a valid Policy Management license installed on a management server?
A. Inability to make rule changes
B. Inability to install policies
C. Inability to review logs
D. Inability to log in to SmartConsole
Answer: B (LEAVE A REPLY)
Without avalid Policy Management licenseinstalled on the management server, administrators areunable to install policiesto the Security Gateways. This prevents the deployment of updated security rules and configurations, leaving the network potentially vulnerable to threats. Other functionalities like making rule changes or reviewing logs might still be accessible, but the core capability to enforce policies is compromised.

NEW QUESTION: 20
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
Answer: D (LEAVE A REPLY)
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 usesthe -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.

NEW QUESTION: 21
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
Answer: D (LEAVE A REPLY)

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.

NEW QUESTION: 22
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
Answer: (SHOW ANSWER)
To verifySmart Contractson a Security Gateway,
thecpconfigandcontracts_mgmtcommands 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.

NEW QUESTION: 23
What are some measures you can take to prevent IPS false positives?
A. Capture packets, Update the IPS database, and Back up custom IPS files
B. Use Recommended IPS profile
C. Use IPS only in Detect mode
D. Exclude problematic services from being protected by IPS (sip, H.323, etc.)
Answer: B (LEAVE A REPLY)
To preventfalse positivesin IPS, using theRecommended IPS profileis an effective measure. This profile is optimized based on best practices and the latest threat intelligence, reducing the likelihood of legitimate traffic being mistakenly identified as malicious. While other options like capturing packets and updating the IPS database are also important, adhering to recommended profiles ensures a balanced and accurate detection mechanism.

NEW QUESTION: 24
After manipulating the rulebase and objects with SmartConsole the application crashes and closes immediately. To troubleshoot, you will need to review the crash report. In which directory on the host PC will you find this report?
A. <SmartFirewall Directory>\data\crash_report\
B. <SmartConsole Directory>\data\crash_report\

C. <FW1 Directory>\data\crash_report
D. <SmartConsole Directory>\crash_report\data\
Answer: (SHOW ANSWER)
Crash reports for SmartConsole are typically located in the <SmartConsole Directory>\data \crash_report\ directory on the host PC. Reviewing these reports provides insights into why the application crashed, including error messages and stack traces, which are essential for diagnosing and resolving the underlying issues.

NEW QUESTION: 25
How many captures does the command "fw monitor -p all" take?
A. All 15 of the inbound and outbound modules
B. The -p option takes the same number of captures, but gathers all of the data packet
C. 1 from every inbound and outbound module of the chain
D. All 4 points of the fw VM modules
Answer: A (LEAVE A REPLY)
The commandfw monitor -p allinitiates packet capturing acrossall 15 inbound and outbound modules within the Check Point inspection chain. This comprehensive capture allows for thorough analysis of packet flow and behavior at every stage of processing, facilitating detailed troubleshooting and performance evaluation.

NEW QUESTION: 26
You need to capture NAT information into packet capture, what tool is the best suitable for this task?
A. fw monitor
B. fw ctl zdebug + xlate xltrc nat
C. cppcap
D. tcpdump
Answer: A (LEAVE A REPLY)
fw monitoris the most suitable tool for capturing NAT information within packet captures. It allows administrators to specify NAT-related filters and capture detailed information about how packets are being translated as they pass through the firewall. This capability is essential for diagnosing and resolving NAT- related issues effectively.

NEW QUESTION: 27
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
Answer: B (LEAVE A REPLY)

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.

Valid 156-582 Dumps shared by BraindumpsPass.com for Helping Passing 156-582 Exam! BraindumpsPass.com now offer the **newest 156-582 exam dumps**, the BraindumpsPass.com 156-582 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com 156-582 dumps with Test Engine here: https://www.braindumpspass.com/CheckPoint/156-582-practice-exam-dumps.html (**77** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)