

CheckPoint.156-583.v2026-10-27.q70

Exam Code:	156-583
Exam Name:	Check Point Certified Troubleshooting Administrator - R82 (CCTA)
Certification Provider:	CheckPoint
Free Question Number:	70
Version:	v2026-10-27
# of views:	102
# of Questions views:	708
https://www.freecram.net/torrent/CheckPoint.156-583.v2026-10-27.q70.html	

NEW QUESTION: 1

Which daemon handles HTTPS Inspection on a Security Gateway?

- A. wstlsd
- B. httpsd
- C. rad
- D. cvpnd

Answer: (SHOW ANSWER)

The wstlsd daemon performs TLS termination and inspection tasks for HTTPS Inspection. Certificate validation failures and handshake errors are typically investigated through its debug output.

NEW QUESTION: 2

After deploying a Hide NAT for a new network, users are unable to access the Internet. What command would you use to check the internal NAT behavior?

- A. cp ctl kdebug + xlate xltrc nat
- B. fw ctl zdebug + xlate xltrc nat
- C. cp ctl zdebug + xlate xltrc nat
- D. fw ctl kdebug + xlate xltrc nat

Answer: (SHOW ANSWER)

To troubleshoot NAT behavior, especially after deploying a Hide NAT configuration, the fw ctl zdebug + xlate xltrc nat command is used. This command provides detailed debug information about NAT translations, allowing administrators to verify that internal addresses are being correctly translated and that the NAT rules are functioning as intended.

NEW QUESTION: 3

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

Answer: C ([LEAVE A REPLY](#))

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.

NEW QUESTION: 4

UserCenter/PartnerMAP access is based on what criteria?

- A. The certification level achieved by employees of an organization.
- B. User permissions assigned to company contacts.
- C. The certification level achieved by the partner.
- D. The level of Support purchased by a company manager.

Answer: ([SHOW ANSWER](#)**)**

Access to UserCenter and PartnerMAP is primarily based on the user permissions assigned to company contacts. These permissions dictate what information and functionalities users can access within the portals, ensuring that only authorized personnel can view or manage specific aspects of the Check Point services and products.

NEW QUESTION: 5

A packet is dropped even though a rule explicitly allows it. Debug shows: "Dropped by fwpsl." What is the cause?

- A. IPS
- B. HTTPS Inspection
- C. Anti-Spoofing
- D. ThreatCloud reputation

Answer: ([SHOW ANSWER](#)**)**

"fwpsl" = packet is dropped by PSL (inspection) often due to ThreatCloud reputation.

NEW QUESTION: 6

Which utility collects configuration files, logs, and diagnostic data from a Check Point system for analysis by Support?

- A. cpinfo
- B. cpview
- C. cpstat
- D. sysconfig

Answer: ([SHOW ANSWER](#))

The cpinfo utility gathers a comprehensive snapshot of the system, including registry, policy, licensing, and log information. The resulting file can be examined locally with CPInfoView or uploaded to Check Point Support.

NEW QUESTION: 7

Which command shows the distribution of connections across CoreXL firewall instances?

- A. fw ctl multik stat
- B. fw ctl affinity -l
- C. fw ctl pstat
- D. cpstat fw -f instances

Answer: ([SHOW ANSWER](#))

The fw ctl multik stat command lists each CoreXL firewall worker instance along with its connection count and CPU. A heavily unbalanced distribution suggests an elephant flow or a hashing problem worth investigating further.

NEW QUESTION: 8

An administrator wants to see every packet dropped by the firewall kernel along with the reason for the drop. Which command should be used?

- A. fw ctl zdebug + drop
- B. fw monitor -e "accept;"
- C. fw ctl pstat
- D. fwaccel stats -d

Answer: ([SHOW ANSWER](#))

The drop flag in the kernel debug prints each dropped packet together with the rule or reason code that caused the drop. This is one of the fastest ways to identify whether traffic loss is caused by policy, anti-spoofing, or another kernel-level inspection.

NEW QUESTION: 9

The URL filtering cache limit exceeded. What issues can this cause?

- A. When URL filtering cache exceeds the limit, it will be disabled temporarily to overcome instability of the system
- B. RAD process will spawn multiple times to help populate the cache
- C. Resource Advisor (RAD) process on the Security Gateway consumes close to 100 percent of the CPU
- D. Nothing, the Security Gateway dynamically raises the cache when needed

Answer: ([SHOW ANSWER](#))

When the URL filtering cache limit is exceeded, the Resource Advisor (RAD) process can consume nearly 100% of the CPU. This high CPU usage can lead to system instability and degrade the performance of the Security Gateway. It is crucial to monitor and manage cache

limits to prevent such performance issues, ensuring that the URL filtering functionality operates smoothly without overloading system resources.

NEW QUESTION: 10

Which command manages the Internal Certificate Authority and can be used to revoke or re-issue certificates?

- A. `cpca_client`
- B. `cpca_admin`
- C. `cp_conf ca`
- D. `vpn_crl_zap`

Answer: ([SHOW ANSWER](#))

The `cpca_client` command provides options to create, revoke, and list certificates issued by the ICA. It is commonly used when SIC or VPN certificate problems require a certificate to be reissued.

NEW QUESTION: 11

Which command displays a summary of accelerated versus non-accelerated traffic statistics on a gateway?

- A. `fwaccel stats -s`
- B. `fwaccel stat`
- C. `fwaccel conns`
- D. `fw ctl multik stat`

Answer: A ([LEAVE A REPLY](#))

The `fwaccel stats -s` command shows the percentage of packets handled by the accelerated path, the medium path, and the firewall path. A very low acceleration percentage points to rules, blades, or connection types that prevent offloading.

NEW QUESTION: 12

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

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 13

Which daemon is responsible for the categorization requests used by Application Control and URL Filtering?

- A. RAD
- B. TED
- C. WSTLSD
- D. CPRID

Answer: ([SHOW ANSWER](#))

The Resource Advisor (RAD) daemon queries the Check Point cloud for site categorization and application signatures. Its debug output is written to \$FWDIR/log/rad.elg, and rad_admin can be used to display statistics about requests and cache hits.

NEW QUESTION: 14

Which pair of commands starts and stops the SmartEvent processes?

- A. cpwd_admin start and cpwd_admin stop
- B. cpstart and cpstop
- C. smartevent start and smartevent stop
- D. evstart and evstop

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 15

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 16

What is the impact of an expired or missing contract file?

- A. The existing protection settings will be removed in SmartConsole but protections are still being enforced by the Security Gateway.
- B. The existing protection settings display in SmartConsole remain and during policy install the Security Gateway asks the administrator to put a new contract file during policy install.
- C. The existing protection settings display in SmartConsole remain and the Security Gateway will use a 14-day EVAL free license instead.

D. The existing protection settings display in SmartConsole remain but are not being enforced by the Security Gateway.

Answer: ([SHOW ANSWER](#))

When a contract file expires or is missing, the existing protection settings continue to display in SmartConsole but are no longer enforced by the Security Gateway. This means that while the administrative interface still shows the security configurations, the actual enforcement of those policies is halted, potentially leaving the network vulnerable until the contract is renewed or replaced.

Valid 156-583 Dumps shared by ExamDiscuss.com for Helping Passing 156-583 Exam! ExamDiscuss.com now offer the **newest 156-583 exam dumps**, the ExamDiscuss.com 156-583 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 156-583 dumps with Test Engine here:
<https://www.examdisscuss.com/CheckPoint/exam/156-583/premium/> (**143** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 17

You need to verify the license on Security Gateway. What command can you use from the command line?

- A.** cplic -l
- B.** cplic print
- C.** cplic list
- D.** sh lic stat

Answer: ([SHOW ANSWER](#))

To verify the license on a Security Gateway, the cplic print command is used. This command displays the current licensing information, including the status and details of installed licenses, ensuring that the gateway has the necessary permissions and features enabled for its operation.

NEW QUESTION: 18

Select the correct statement about service contracts.

- A.** Valid service contracts must be stored only on the Security Gateways that have Threat Prevention blades enabled
- B.** Service contracts are provided on paper only
- C.** Valid service contracts are only stored and required on the Primary Security Management Server and never downloaded on any other system
- D.** Valid service contracts must be stored on the Security Management Server before they can be downloaded to a Security Gateway

Answer: ([SHOW ANSWER](#))

Service contracts in Check Point environments must be stored on the Security Management Server before they can be downloaded to any Security Gateway. This centralized approach ensures that all gateways receive consistent and authorized contract information, which is essential for maintaining compliance and enabling the required security features across the network.

NEW QUESTION: 19

Which command is used in R82 to display Multi-Queue configuration and per-interface queue assignment?

- A. mq_mng -o
- B. cpmq get
- C. sim affinity -l
- D. fw ctl affinity -q

Answer: ([SHOW ANSWER](#))

The mq_mng utility manages and reports Multi-Queue in current versions, replacing the older cpmq commands. Its output shows which interfaces have Multi-Queue enabled and how the receive queues map to CPU cores.

NEW QUESTION: 20

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

Answer: ([SHOW ANSWER](#))

The correct inspection flow using fw monitor is:

- (i) - pre-inbound: Before the packet enters the inbound processing path.
- (l) - 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.

NEW QUESTION: 21

What is the default protection profile for Autonomous Threat Prevention?

- A. Perimeter
- B. Guest
- C. Internal
- D. Bypass

Answer: A ([LEAVE A REPLY](#))

The Perimeter protection profile is the default setting for Autonomous Threat Prevention in Check Point environments. This profile is designed to provide robust security measures at the network's perimeter, effectively mitigating threats and ensuring that incoming traffic is thoroughly inspected and filtered based on established security policies.

NEW QUESTION: 22

What is the maximum kernel debug buffer size that can be allocated with `fw ctl debug -buf`?

- A. 1024
- B. 8192
- C. 16384
- D. 32768

Answer: ([SHOW ANSWER](#))

The kernel debug buffer can be set up to 32768 KB using `fw ctl debug -buf 32768`. A larger buffer reduces the risk of losing debug messages on a busy gateway, at the cost of additional kernel memory consumption.

NEW QUESTION: 23

Which fw monitor option is used to specify an INSPECT filter expression directly on the command line?

- A. -f
- B. -e
- C. -m
- D. -x

Answer: ([SHOW ANSWER](#))

The -e option accepts an inline INSPECT expression, for example `fw monitor -e "accept host(1.1.1.1);"`. The -f option is used instead when the filter is stored in a file, which is convenient for long or reusable expressions.

NEW QUESTION: 24

Which log file contains the debug output of the fwd daemon?

- A. `$FWDIR/log/fw.elg`
- B. `$FWDIR/log/fwd.elg`
- C. `$FWDIR/log/cpd.elg`
- D. `$CPDIR/log/fwd.log`

Answer: ([SHOW ANSWER](#))

Each Check Point user mode process writes its debug output to a matching .elg file in `$FWDIR/log` or `$CPDIR/log`. For fwd, which handles log forwarding and several policy-related functions, the file is `$FWDIR/log/fwd.elg`.

NEW QUESTION: 25

An administrator needs to capture traffic on a Gaia gateway while minimizing the CPU impact of the capture itself. Besides using tcpdump with the appropriate option, which alternative capture tool is designed for lower overhead on the accelerated path?

- A. cppcap
- B. fw monitor
- C. snoop
- D. tshark

Answer: ([SHOW ANSWER](#))

The cppcap tool was introduced as a lightweight capture utility that works with the acceleration path and imposes less overhead than tcpdump on busy gateways. It also allows capture on multiple interfaces with filtering, making it well suited to production troubleshooting.

NEW QUESTION: 26

Which Layer of the OSI Model is responsible for routing?

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

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 27

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

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 28

After deploying a new Static NAT configuration, traffic is not getting through. What command would you use to troubleshoot internal problems with the NAT traffic?

- A. fw ctl kdebug + xlate xltrc nat

- B. cp ctl zdebug + xlate xltrc nat
- C. fw ctl zdebug + xlate xltrc nat
- D. cp ctl kdebug + xlate xltrc nat

Answer: ([SHOW ANSWER](#))

To troubleshoot internal problems with NAT traffic after deploying a Static NAT configuration, the fw ctl zdebug + xlate xltrc nat command is utilized. This command provides detailed debugging information related to NAT translations, helping administrators identify and resolve issues within the NAT process.

NEW QUESTION: 29

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: ([SHOW ANSWER](#))

The command fw monitor -p all initiates packet capturing across all 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: 30

Users cannot reach their VPN site through the cluster VIP. Traffic works when connecting to each individual node.

- A. ARP cache wrong
- B. VIP missing topology configuration
- C. SNAT misconfigured
- D. CCP in wrong mode

Answer: ([SHOW ANSWER](#))

VIP route or topology wrong → cluster doesn't forward traffic.

NEW QUESTION: 31

SecureXL is enabled, but traffic is not accelerated. Why?

- A. Kinetics disabled
- B. Rulebase using objects not template-compatible
- C. HTTPS Inspection enabled
- D. Wrong CPUID fix

Answer: ([SHOW ANSWER](#))

SecureXL templates break on:
time object rules
identity rules

services with QOS

Template fallback → slow path.

Valid 156-583 Dumps shared by ExamDiscuss.com for Helping Passing 156-583 Exam! ExamDiscuss.com now offer the **newest 156-583 exam dumps**, the ExamDiscuss.com 156-583 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 156-583 dumps with Test Engine here:

<https://www.examdiscuss.com/CheckPoint/exam/156-583/premium/> (143 Q&As Dumps,

35%OFF Special Discount Code: freecram)

NEW QUESTION: 32

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: 33

Which process indexes log files so that SmartConsole Logs and Monitor views return fast search results?

- A. log_indexer
- B. fwd
- C. cpd
- D. cpsead

Answer: (SHOW ANSWER)

The log_indexer process reads log files and builds the index used for searching in the Logs and Monitor view. If logs are visible in the raw files but searches return nothing, the indexer is a primary suspect.

NEW QUESTION: 34

SmartConsole closes immediately, what is the most likely reason?

- A. The process crashed in kernel space

- B. The process crashed in user space
- C. The user idle time expired and SmartConsole disconnected the user
- D. The Security Management server rejected the client connection

Answer: ([SHOW ANSWER](#))

If SmartConsole closes immediately, the most likely cause is that the process crashed in user space. User space crashes typically occur due to application-level errors, such as bugs or corrupted files, leading to the abrupt termination of the application. Kernel space crashes are less common and usually affect the entire system rather than a single application.

NEW QUESTION: 35

SmartEvent shows logs from gateways, but no Events are generated. Why?

- A. Indexing disabled
- B. Correlation Unit not SIC-authenticated
- C. Wrong Event Policy
- D. Wrong GW object type

Answer: ([SHOW ANSWER](#))

SmartEvent needs an active Correlation Policy. Without it: raw logs only.

NEW QUESTION: 36

What Check Point process controls logging?

- A. CPWD
- B. FWD
- C. CPD
- D. CPM

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 37

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

Answer: C ([LEAVE A REPLY](#))

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.

NEW QUESTION: 38

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: ([SHOW ANSWER](#))

To prevent false positives in IPS, using the Recommended IPS profile is 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: 39

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: ([SHOW ANSWER](#))

The delete threshold cannot be more than 25 percent of the disk. Automatically delete logs if less than 12GB are available. It is recommended to delete the old files when disk space is below 15-20 percent.

NEW QUESTION: 40

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

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 41

Which command is used to reset SIC on a Security Gateway from the CLI?

- A. cp_conf sic init
- B. sic_reset
- C. cpca_client reset
- D. fw sic -r

Answer: ([SHOW ANSWER](#))

The cp_conf sic init command re-initializes SIC with a new one-time password on the gateway. The corresponding certificate must then be reset on the management server object before trust can be re-established.

NEW QUESTION: 42

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 43

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

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 44

A file bypasses Threat Emulation for specific users only. Most likely cause?

- A. Wrong blade order
- B. IA identity roles applied

C. TE only runs on cloud

D. Bad routing

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 45

Which command displays all processes that are monitored and restarted by the Check Point WatchDog?

A. cpwd_admin list

B. cpstat wd

C. fw ctl pstat

D. ps -ef | grep cpwd

Answer: ([SHOW ANSWER](#)**)**

The cpwd_admin list command shows each WatchDog-monitored process, its PID, state, number of restarts, and the time of the last start. A high or increasing restart counter is a strong indicator of an unstable process that requires further debugging.

NEW QUESTION: 46

Which pair of commands starts and stops the SmartEvent processes?

A. evstart and evstop

B. cpstart and cpstop

C. smartevent start and smartevent stop

D. cpwd_admin start and cpwd_admin stop

Answer: ([SHOW ANSWER](#)**)**

The evstart and evstop commands control the SmartEvent correlation and analysis processes independently of the main Check Point services. This allows SmartEvent to be restarted without disrupting the rest of the management server.

Valid 156-583 Dumps shared by ExamDiscuss.com for Helping Passing 156-583 Exam! ExamDiscuss.com now offer the **newest 156-583 exam dumps**, the ExamDiscuss.com 156-583 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 156-583 dumps with Test Engine here:

<https://www.examdumps.com/CheckPoint/exam/156-583/premium/> (143 Q&As Dumps,

35%OFF Special Discount Code: freecram)

NEW QUESTION: 47

You need to capture NAT information into packet capture, what tool is the best suitable for this task?

A. tcpdump

B. fw monitor

- C. cppcap
- D. fw ctl zdebug + xlate xltrc nat

Answer: ([SHOW ANSWER](#))

fw monitor is 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: 48

Which command displays the inspection chain modules that a packet traverses inside the gateway?

- A. fw ctl chain
- B. fw ctl debug -m
- C. fw monitor -p all
- D. fw ctl conn

Answer: ([SHOW ANSWER](#))

The fw ctl chain command lists the ordered chain modules, such as SecureXL, VPN, and the firewall virtual machine, with their positions. This information is essential when using fw monitor with the -p option to capture at a specific chain position.

NEW QUESTION: 49

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: ([SHOW ANSWER](#))

To generate a capture file directly from fw monitor that can be opened in Wireshark, you use the -o option to write to an output file.

The filter expression must follow the Inspect syntax accept <expression>; and be quoted properly on the command line (e.g. fw monitor -e "accept host 1.2.3.4;" -o output.cap).

Using shell redirection (> or >>) is not the recommended/expected method for this exam-style question, and -file is not a valid option, whereas -o is.

NEW QUESTION: 50

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 51

A VPN tunnel intermittently fails after renegotiation. Debug shows: "Invalid SPI."

- A.** Routing missing
- B.** DPD disabled
- C.** Wrong Phase-2 timers
- D.** NAT-T misconfigured

Answer: ([SHOW ANSWER](#))

On rekey mismatch, gateways accept wrong SPI → drop packets.

NEW QUESTION: 52

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: ([SHOW ANSWER](#))

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: 53

Which command repairs a corrupted log file and rebuilds its pointer file?

- A.** fw repairlog
- B.** fw logswitch -r
- C.** fw log -f
- D.** log_indexer -rebuild

Answer: ([SHOW ANSWER](#))

The fw repairlog command rebuilds the pointer file associated with a log file so that it can be read again by log viewers. Corruption commonly follows an abrupt shutdown or a disk space exhaustion event on the log server.

NEW QUESTION: 54

Which of the following files is commonly associated with troubleshooting crashes on a system such as SmartConsole?

- A. CPMILdump
- B. fw monitor
- C. crash dump
- D. tcpdump

Answer: ([SHOW ANSWER](#))

A crash dump file is typically generated when an application like SmartConsole crashes. This file contains detailed information about the state of the system at the time of the crash, which is invaluable for diagnosing the cause of the failure. Analyzing crash dumps helps developers and support teams identify and fix underlying issues.

NEW QUESTION: 55

Which process on an R82 Security Management Server handles communication with SmartConsole clients?

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

Answer: ([SHOW ANSWER](#))

CPM (Check Point Management) is the main management process in R80 and above, including R82. It handles SmartConsole sessions, policy operations, and database transactions. Its debug output is written to \$FWDIR/log/cpm.elg, which is the first place to look for SmartConsole connectivity or session errors.

NEW QUESTION: 56

Which environment variable is set to enable maximum verbosity when debugging a Check Point user mode process?

- A. CPDEBUG_ALL=5
- B. TDERROR_ALL_ALL=5
- C. FW_DEBUG_LEVEL=5
- D. DEBUG_LEVEL_ALL=5

Answer: ([SHOW ANSWER](#))

User mode debugging is controlled by TDERROR variables, where TDERROR_ALL_ALL=5 sets the highest verbosity for all modules of the process. More targeted variables can be used to limit output to a specific component and reduce noise.

NEW QUESTION: 57

Application Control and URL Filtering update files are located in which directory?

- A. SCPDIR/appi/update
- B. SFWDIR/conf/update
- C. SCPDIR/apci/update
- D. SFWDIR/appi/update/

Answer: ([SHOW ANSWER](#))

Update files for Application Control and URL Filtering are typically stored in the SFWDIR/appi/update/ directory. This location houses the latest updates and definitions required for the proper functioning of these security features, ensuring that the gateway can effectively control applications and filter URLs based on the latest threat intelligence.

NEW QUESTION: 58

Policy installation fails randomly after making changes. No SIC errors.

- A. Corrupted \$FWDIR/policy
- B. Threat + Access layers mismatch
- C. Time drift between manager and GW
- D. Log server overloaded

Answer: ([SHOW ANSWER](#))

Time affecting SIC certificates causes intermittent policy install failures.

NEW QUESTION: 59

A cluster behaves correctly, but occasionally both members show Active state. Traffic still works. Root cause?

- A. SmartTasks
- B. Policy mismatch
- C. Broadcast/multicast dropped for CCP
- D. SecureXL template corruption

Answer: ([SHOW ANSWER](#))

If CCP heartbeats cannot pass, appliances believe the other is dead.

NEW QUESTION: 60

In fw monitor output, which inspection point represents the packet after the outbound firewall inspection but before it leaves the interface?

- A. i
- B. l
- C. o
- D. O

Answer: ([SHOW ANSWER](#))

Lowercase o is the pre-outbound point immediately before the outbound virtual machine, while uppercase O is the post-outbound point just before the packet exits the interface. Seeing a packet at o but not at O indicates it was dropped during outbound inspection.

NEW QUESTION: 61

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

Answer: (SHOW ANSWER)

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.

Valid 156-583 Dumps shared by ExamDiscuss.com for Helping Passing 156-583 Exam! ExamDiscuss.com now offer the **newest 156-583 exam dumps**, the ExamDiscuss.com 156-583 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 156-583 dumps with Test Engine here:
<https://www.examdisscuss.com/CheckPoint/exam/156-583/premium/> (143 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 62

Which command displays the internal firewall kernel statistics, including memory usage, connection counts, and hash table information?

- A. fw ctl pstat
- B. fw ctl iflist
- C. fw ctl chain
- D. fw tab -s

Answer: (SHOW ANSWER)

The fw ctl pstat command reports kernel memory allocation, connection table usage, sync status, and inspection statistics. Memory failures or a connections table nearing its limit are frequently identified from this output.

NEW QUESTION: 63

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 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.

NEW QUESTION: 64

Which command is used to view real-time and historical performance statistics on a Check Point gateway through a menu-driven interface?

- A. cpview
- B. cpstat
- C. top
- D. sar

Answer: ([SHOW ANSWER](#)**)**

CPView provides a navigable, continuously refreshed display of CPU, memory, network, and blade statistics. It also supports a history mode that allows an administrator to review recorded statistics from a past time window.

NEW QUESTION: 65

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

Answer: ([SHOW ANSWER](#)**)**

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.

NEW QUESTION: 66

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

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 67

Which command lists the critical devices (pnodes) that are being monitored by ClusterXL?

- A. cphaprob -a if
- B. cphaprob list
- C. cphaprob syncstat
- D. cphaconf show

Answer: ([SHOW ANSWER](#))

The cphaprob list command displays every registered critical device, its status, and the number of failures allowed before a failover occurs. A device reported as problematic here usually explains why a member left the Active state.

NEW QUESTION: 68

Which command shows the installed licenses and contracts on a Check Point device?

- A. cplicenses print -x
- B. cplic print-s
- C. fwlic print -x
- D. cplic print-x

Answer: ([SHOW ANSWER](#))

The cplic print-x command is used to display the installed licenses and contracts on a Check Point device. This command provides detailed information about the licenses, including their status, expiration dates, and associated features, enabling administrators to manage and verify their licensing effectively.

NEW QUESTION: 69

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: ([SHOW ANSWER](#))

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: 70

Where can a Check Point customer find information about product licenses they own, download product manuals, and get information about product support expiration?

- A. Smart Console
- B. PartnerMAP portal
- C. UserCenter portal
- D. In security management server via CLI and executing command cplic print

Answer: C ([LEAVE A REPLY](#))

The UserCenter portal is the central hub where Check Point customers can access detailed information about their product licenses, download product manuals, and obtain information regarding product support expiration. This online portal provides a comprehensive view of all licensed products and services, facilitating effective license management and access to essential documentation.

Valid 156-583 Dumps shared by ExamDiscuss.com for Helping Passing 156-583 Exam! ExamDiscuss.com now offer the **newest 156-583 exam dumps**, the ExamDiscuss.com 156-583 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 156-583 dumps with Test Engine here:

<https://www.examdiscuss.com/CheckPoint/exam/156-583/premium/> (143 Q&As Dumps,

35%OFF Special Discount Code: **freecram**)