

CheckPoint.156-581.v2023-02-13.q31

Exam Code:	156-581
Exam Name:	Check Point Certified Troubleshooting Administrator - R81
Certification Provider:	CheckPoint
Free Question Number:	31
Version:	v2023-02-13
# of views:	854
# of Questions views:	2458
https://www.dumpsfiles.com/files/CheckPoint/156-581/CheckPoint.156-581.v2023-02-13.q31	

NEW QUESTION: 1

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 2

During the policy installation process, compiled policies are located in three different directories, which directory contains the last policy which was compiled successfully on the management side?

- A. \$FWDIR/log/fwd.elg
- B. \$FWDIR/state/local/FW1
- C. \$FWDIR/state/<gateway_name>/FW1
- D. \$FWDIR/state_tmp/FW1

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 3

Which of the following kernel tables can provide useful information in troubleshooting Hide NAT port exhaustion?

- A. connections
- B. fw_nat
- C. fwx_alloc
- D. nat_entries

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 4

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. Valid service contracts are only stored and required on Primary Security Management Server and never downloaded on any other system
- C. Service contracts are provided on paper only
- D. Valid service contracts must be stored on the Security Management Server before they can be downloaded to a Security Gateway

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

NEW QUESTION: 5

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

- A. CLISH
- B. snoop
- C. wireshark
- D. CLI

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

NEW QUESTION: 6

Which version of SmartConsole is recommended?

- A. The latest release based on the version running on the management server
- B. The latest release based on the version running on the most up-to-date gateway
- C. The latest release available
- D. The latest stable release available

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

NEW QUESTION: 7

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. <SmartConsole Directory>\Crash_report\data\
- B. <SmartFirewall Directory>\data\crash_report\
- C. <SmartConsole Directory>\data\Crash_report\
- D. <FW1 Directory>\data\crash_report

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

NEW QUESTION: 8

The Identity Awareness process that receives identity data from the identity sources and organizes it in tables before forwarding the data to the enforcement module is called

- A. iaforward
- B. pdp
- C. pep
- D. iasend

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

NEW QUESTION: 9

The customer is using Check Point appliances that were configured long ago by third-party administrators. Current policy includes different enabled IPS protections and Bypass Under Load function. Bypass Under Load is configured to disable IPS inspections if CPU and Memory usage is higher than 80%. The Customer reports that IPS protections are not working at all regardless of CPU and Memory usage. What is a possible reason of such behavior?

- A. The kernel parameter `ids_assume_stress` is set to 0
- B. The kernel parameter `ids_tolerance_stress` is set to 10
- C. The kernel parameter `ids_tolerance_no_stress` is set to 10
- D. The kernel parameter `ids_assume_stress` is set to 1

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

NEW QUESTION: 10

What are the available types of licenses in Check Point?

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

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

NEW QUESTION: 11

Is it possible to analyze ICMP packets with tcpdump?

- A. Yes, tcpdump is not limited to tcp specific issues
- B. No, tcpdump works from layer 4. ICMP is located in the network layer (layer 3), therefore is not applicable to this scenario
- C. No, since ICMP does not have any source or destination ports, but specification of port numbers is mandatory
- D. No, use fw monitor instead

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

NEW QUESTION: 12

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

- A. `cplic print -x`
- B. `fwlic print -x`
- C. `cplicenses print -x`

D. cplic print -s

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

NEW QUESTION: 13

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 kdebug + xlate xltrc nat

C. cp ctt zdebug + xlate xltrc nat

D. fw ctl zdebug + xlate xltrc nat

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 14

In what formats can you export license status?

A. PDF, CSV, DLL

B. CSV, PDF, Template

C. Word, PDF, exe

D. CSV, Word, Notepad

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 15

IPS detection incorporates 4 layers. Which of the following is NOT a layer in IPS detection?

A. Protocol Parsers

B. Protections

C. Context Management

D. Detections

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

NEW QUESTION: 16

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. solr

C. dlpd

D. cpm

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

156-581 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com 156-581 dumps with Test Engine here:
<https://www.trainingdump.com/CheckPoint/156-581-practice-exam-dumps.html> (93 Q&As
Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

What is true concerning fw monitor?

- A. fwmonitor is available on all platforms and even the syntax is the same on all gateways
- B. fw monitor is available on all management server platforms and the syntax is the same everywhere
- C. tcpdump syntax can be used in fw monitor for deeper analysis
- D. fwmonitor has been obsoleted by tcpdump with R80.10

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

NEW QUESTION: 18

What would be the most likely response when attempting to use SmartConsole to connect to a management server with the wrong credentials?

- A. "invalid username or password"
- B. "Server down on unresponsive"
- C. "Incorrect name or IP address"
- D. "Authentication to server failed"

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

NEW QUESTION: 19

The default time out for policy installation is

- A. 150 seconds
- B. 300 seconds
- C. 90 seconds
- D. 600 seconds

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

NEW QUESTION: 20

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

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

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

NEW QUESTION: 21

Which of the following would be the most appropriate command in debugging a HideNAT issue?

- A. fw ctl zdebug + fwalloc hidenat
- B. fw ctl zdebug + dynamic natips natports
- C. fw ctl zdebug + xlate xltrc nat
- D. fw ctl zdebug + fwn allnat

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

NEW QUESTION: 22

Performing NAT on the Client Side means that translation of all packets will occur?

- A. Prior to any routing taking place
- B. In the firewall kernel closest to the initiator of the connection
- C. In the inbound firewall kernel instance
- D. After the packets have already been routed

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

NEW QUESTION: 23

What are the four ways to insert an FW Monitor into the firewall kernel chain?

- A. Relative position using geolocation, relative position using inertial navigation, absolute position, all positions
- B. Absolute position using location, absolute position using alias, relative position, all positions
- C. Absolute position using location, relative position using alias, general position, all positions
- D. Relative position using location, relative position using alias, absolute position. all positions

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

NEW QUESTION: 24

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

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

NEW QUESTION: 25

Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?

- A. \$FWDIR/conf/install_firewall_tmp/ANTIMALWARE/conf/
- B. \$FWDIR/log/install_manager_tmp/ANTIMALWARE/log/
- C. \$CPDIR/conf/install_manager_tmp/ANTIMALWARE/conf/

D. \$FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 26

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

- A. .cap
- B. .exe
- C. .pcap
- D. .tgz

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

NEW QUESTION: 27

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

- A. \$FWDIR/log/fwm.elg
- B. \$FWDIR/log/fwd.elg
- C. \$CPDIR/log/cpd.elg
- D. \$MDS_FWDIR/log/cpm.elg

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

NEW QUESTION: 28

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. fwm, TCP 18190
- C. fwm, TCP 257
- D. cpm, 19009

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

NEW QUESTION: 29

Which command do you need to execute to insert fw monitor after TCP streaming (out) in the outbound chain using absolute position? Given the chain was 1ffffe0, select the correct answer.

- A. fw monitor -po 1ffffe0
- B. fw monitor -pO -ox1ffffe0
- C. fw monitor -pO ox1ffffe0
- D. fw monitor -po -0x1ffffe0

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

NEW QUESTION: 30

One of most common reasons that firewall administrator couldn't login anymore into a newly installed R80.x Security Management via SmartConsole is, that the 15-day trial license was expired. How can the firewall administrator install a valid license on the security management, if he only has access to the management via SmartConsole or via Gaia Portal?

- A.** The Firewall administrator should run SmartDistributor.exe, located in, login and install the valid license on management server.
- B.** The Firewall administrator should run SmartProvider.exe, located in, login and install the valid license on management server.
- C.** The Firewall administrator should run SmartUpdate.exe, located in \bin\, login and install the valid license on management server.
- D.** The Firewall administrator should run GuidBedit.exe, located in \, login and install the valid license on management server

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

NEW QUESTION: 31

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

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

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

Valid 156-581 Dumps shared by TrainingDump.com for Helping Passing 156-581 Exam! TrainingDump.com now offer the **newest 156-581 exam dumps**, the TrainingDump.com 156-581 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com 156-581 dumps with Test Engine here:
<https://www.trainingdump.com/CheckPoint/156-581-practice-exam-dumps.html> (**93 Q&As** Dumps, **40%OFF** Special Discount: **Exam-Tests**)

Valid 156-581 Dumps shared by TrainingDump.com for Helping Passing 156-581 Exam! TrainingDump.com now offer the **newest 156-581 exam dumps**, the TrainingDump.com 156-581 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com 156-581 dumps with Test Engine here:
<https://www.trainingdump.com/CheckPoint/156-581-practice-exam-dumps.html> (**93 Q&As** Dumps, **40%OFF** Special Discount: **Exam-Tests**)