DUMPSBOSS.

Check Point Certified Troubleshooting AdministratorR81.20 (CCTA)

Checkpoint 156-582

Version Demo

Total Demo Questions: 9

Total Premium Questions: 93

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Troubleshooting	49
Topic 2, SmartConsole Troubleshooting	11
Topic 3, Policy Management Troubleshooting	16
Topic 4, Monitoring ClusterXL Connections	2
Topic 5, Identity Awareness Troubleshooting	1
Topic 6, VPN Troubleshooting	3
Topic 7, HTTPS Inspection Troubleshooting	1
Topic 8, Troubleshooting Issues with Acceleration	6
Topic 9, Mix Questions	4
Total	93

QUESTION NO: 1

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: A

Explanation:

Your account has classification permission to Viewer is correct because the Viewer classification in Check Point User Center is intended for read-only access. A Viewer can view account, product, and license information, but cannot perform licensing operations such as adding, attaching, detaching, upgrading, or otherwise modifying licenses. Consequently, the portal disables the licensing action controls, which appear greyed out. Licensing tasks require an account classification that grants licensing-management privileges, assigned by the applicable User Center account administrator. The key troubleshooting point is to verify the User Center classification associated with the logged-in Check Point account and request an appropriate licensing role if gateway-license actions are required. Support-contact status is used for entitlement and interaction with Check Point support services; it is not the permission model that enables license-management controls in User Center. Check Point's User Center is the portal used to manage products, licenses, and account-related assets: Check Point User Center. For account access and entitlement assistance, use the Check Point Support Center.

QUESTION NO: 2

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: D

Explanation:

Valid service contracts must be stored on the Security Management Server before they can be downloaded to a Security Gateway. In Check Point environments, contracts are centrally managed through SmartConsole/SmartUpdate on the Security Management Server. The management server retrieves and maintains contract entitlement information, then distributes the applicable contract data to gateways. This process allows gateways to validate entitlement for licensed services and supported updates, including Threat Prevention capabilities that depend on an active contract. Centralized contract management also gives administrators one authoritative location to view contract status, update contract data, and distribute it to the relevant managed gateways. A gateway does not independently act as the initial repository for service-contract information; it receives the relevant data after the management system has obtained and stored it. This design is consistent with the SmartUpdate workflow, in which licenses and contracts are managed centrally and then applied or downloaded to Security Gateways as needed. See Check Point's R81.20 SmartConsole Administration Guide: SmartUpdate and the Check Point service-contract management guidance.

QUESTION NO: 3

A filtered tcpdump shows the affected packets entering and leaving a Security Gateway, but the same traffic does not appear in a standard fw monitor capture. Which condition most likely explains this result?

A. The packets are encrypted by IPsec VPN.

B. The gateway has no active connection entry.

C. The traffic is handled by SecureXL acceleration.

D. The gateway cannot send logs to the Log Server.

ANSWER: C

Explanation:

Traffic that is handled by **SecureXL acceleration** can bypass portions of the firewall inspection path where a standard `fw monitor` capture obtains visibility. Consequently, an interface-level tcpdump can show packets entering and leaving the gateway while those packets are not seen in the expected fw monitor output.

This does not by itself prove that the access-control policy allowed the traffic, that the connection is absent from the connection table, or that a logging failure occurred. The decisive distinction is between an interface capture and a kernel inspection-path capture in an environment where traffic can be accelerated.

QUESTION NO: 4

What is the difference between the “Super User" and “Read Write All" SmartConsole permission profiles?

A. “Read Write All" has the extra ability to make changes within the Gaia operating system

B. “Super User” has the extra ability to administer other administrative accounts

C. “Super User” has the extra ability to make changes within the Gaia operating system

D. “Super User" had the extra ability of being able to use the Management API

ANSWER: B

Explanation:

“Super User” has the extra ability to administer other administrative accounts. In SmartConsole, the Super User permission profile has full read/write access to Security Management functionality and includes administrative-control permissions for SmartConsole administrators and their permission profiles. This enables a Super User to create, modify, and delete administrator accounts, as well as assign the access rights that determine what those administrators can manage.

“Read Write All” is intended to provide broad operational read/write access across the managed environment, such as working with policy and configuration data, without granting the authority to administer the SmartConsole administrator population itself. Separating administrator-account management from general configuration access supports least-privilege administration: an operator can perform normal management work without being able to elevate access or alter another administrator’s privileges. Gaia operating-system administration is controlled through Gaia authentication and its own role-based access controls; it is not the distinguishing SmartConsole permission-profile capability described here.

Check Point documents SmartConsole administrator permissions and predefined permission profiles in its Security Management Administration Guide: Managing Administrators and Permission Profiles.

QUESTION NO: 5

What Check Point process controls logging?

A. CPWD

B. FWD

C. CPD

D. CPM

ANSWER: B

Explanation:

FWD is the Check Point Firewall Daemon and is the process associated with Check Point logging services. On a Security Gateway, it handles log-generation-related activity and forwards log records to the configured Security Management Server or Log Server. On management components, FWD participates in receiving, processing, and making log data available to SmartConsole and other Check Point logging tools. This makes FWD the relevant process to examine when troubleshooting log transmission, log collection, or failures involving Check Point log services.

Check Point's logging architecture is based on Security Gateways creating records for traffic and security events, then sending those records to a Log Server for storage and analysis. Because FWD is the daemon that supports this Check Point logging communication and service functionality, its status is directly relevant when logs are not arriving or are not being processed as expected. Administrators can review Check Point process status with the CPWD monitoring framework, but the logging function itself is provided by FWD. See the Check Point R81.20 Logging and Monitoring Administration Guide and the R81.20 CLI Reference Guide for Check Point service and logging architecture details.

QUESTION NO: 6

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

ANSWER: B

Explanation:

Run `netstat -anp | grep :257` in expert mode on the Log server to check whether Security Gateways have established log-forwarding connections to that Log Server. Check Point uses TCP port 257 for the gateway-to-Log Server logging connection. The `netstat` output shows listening and active network sockets; an active entry for port 257, typically with an `ESTABLISHED` state, confirms that a gateway is currently connected. The peer address shown in the output can be matched to the gateway's IP address, allowing the administrator to validate the status of a particular gateway connection. Expert mode is required because `netstat` is a Gaia operating-system command and is not a CLISH command. The `-a` switch displays all sockets, `-n` preserves numeric addresses and port numbers, and `-p` displays the associated process information where available. This is therefore a direct server-side verification of the logging transport path. Check Point's documented port information is available in the R81.20 Network Ports documentation; Gaia command-mode context is described in the R81.20 CLI Reference Guide.

QUESTION NO: 7

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

A. fw -p -o switch

B. fw logswitch

C. Install security policy

D. fw switchlog

ANSWER: B

Explanation:

The correct command is `fw logswitch`. Run on a Check Point Security Gateway, it instructs the gateway's logging process to close the current active log file and begin writing new log records to a newly created log file. This is useful when an administrator needs to rotate logs manually for troubleshooting, log collection, archival, or to make the current log file available for review without waiting for an automatic log rotation event. The command affects the active log file on the gateway; it does not install or modify the Access Control policy. Check Point documents `fw logswitch` in the Security Management Administration Guide command reference as the procedure for closing the current log file and opening a new one. Appropriate permissions and access to the gateway's expert-mode command line are required to execute it. For operational context and the current command syntax, see the Check Point R81.20 Security Management Administration Guide: Managing Logs and the R81.20 CLI Reference Guide: Log Management Commands.

QUESTION NO: 8

An administrator successfully installs a revised Access Control Policy on a Security Gateway. Which command can be used on the gateway to verify the installed policy name and installation information?

A. fw ctl pstat

B. fw stat

C. cpwd_admin list

D. cplic print -x

ANSWER: B

Explanation:

fw stat displays information about the policy installed on the Security Gateway, including the policy name and installation-related details. It is useful for confirming that the gateway is enforcing the expected policy after an installation operation.

`fw ctl pstat` displays kernel and memory-related status information, not the installed policy identity. `cpwd_admin list` checks Check Point process status, and `cplic print -x` displays license information.

QUESTION NO: 9

An fw monitor capture for a test packet shows the packet at the i and I inspection points, but it does not appear at o or O. What is the correct conclusion?

A. The packet passed inbound inspection but did not reach the outbound inspection path.

B. The packet was accepted and transmitted from the egress interface.

C. The packet never entered the Security Gateway kernel.

D. The packet was captured only after outbound inspection.

ANSWER: A

Explanation:

The packet **passed inbound inspection but did not reach the outbound inspection path**. The lowercase `i` point is pre-inbound and uppercase `I` is post-inbound. The packet therefore entered the firewall kernel and progressed through inbound processing. Its absence from both `o` and `O` means that it was not observed on the outbound portion of the fw monitor chain.

The capture alone does not establish one specific root cause, such as a routing problem or a policy drop. It does, however, precisely narrow the investigation to processing that occurs after inbound inspection and before outbound inspection.