# Regular Free Updates 156-582 Dumps Real Exam Questions Test Engine Feb 19, 2025 [Q28-Q44


**Regular Free Updates 156-582 Dumps Real Exam Questions Test Engine Feb 19, 2025 Practice Test Questions Verified Answers As Experienced in the Actual Test!**

## CheckPoint 156-582 Exam Syllabus Topics:

TopicDetailsTopic 1- Troubleshooting NAT: This section of the exam measures the skills of Check Point security administrators and covers troubleshooting Network Address Translation (NAT) configurations. It emphasizes understanding NAT rules, translations, and common pitfalls.Topic 2- Troubleshooting SmartConsole: This section of the exam measures the skills of Check Point security professionals and covers troubleshooting techniques specific to SmartConsole, the management interface for Check Point products.Topic 3- Fundamentals of Traffic Monitoring: This section of the exam measures the skills of Check Point security administrators and covers essential techniques for monitoring network traffic. It includes understanding traffic flows, analyzing logs, and identifying anomalies.Topic 4- Autonomous Threat Prevention Troubleshooting: This section of the exam measures the skills of Check Point security administrators and covers troubleshooting techniques for autonomous threat prevention systems. It emphasizes understanding threat detection mechanisms and response actions.Topic 5- Log Collection: This section of the exam measures the skills of Check Point security administrators and covers methods for collecting and managing logs from various security devices.Topic 6- Introduction to Troubleshooting: This section of the exam measures the skills of Check Point security administrators and covers the foundational concepts of troubleshooting within network security environments. It introduces the principles and

methodologies used to identify and resolve issues effectively. A key skill assessed is the ability to apply systematic approaches to diagnose problems.

**NO.28** When running a debug with fw monitor, which parameter will create a more verbose output?
* -I
* -i
* V
* -D

The-Dparameter in thefw monitorcommand is used to enablemore verbose output. This parameter increases the level of detail provided in the debug output, allowing administrators to gain deeper insights into packet processing and troubleshooting network issues more effectively.

**NO.29** Application Control and URL Filtering update files are located in which directory?
* SCPDIR/appi/update
* SFWDIR/conf/update
* SCPDIR/apci/update
* SFWDIR/appi/update/

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

**NO.30** What are two types of SAs in the VPN negotiation?
* IKE and VPND SA
* IKE SA and VPN SA
* IKE SA and IPsec SA
* VPN SA and Main SA

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.

**NO.31** Which of the following is true about tcpdump?
* The tcpdump can only capture TCP packets and not UDP packets
* A tcpdump session can be initiated from the SmartConsole
* The tcpdump has to be run from clish mode in Gaia
* Running tcpdump without the correct switches will negatively impact the performance of the Firewall

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.

**NO.32** What is the name of a protocol for VPN establishment and negotiation?
* NAT-T
* IPsec

* VPN
* IKE

IKE (Internet Key Exchange)is the protocol used for establishing and negotiating VPN connections. It facilitates the negotiation of cryptographic keys and the authentication of the communicating parties, forming the foundation for secure IPsec VPN tunnels. While IPsec is the suite used for securing communications, IKE specifically handles the establishment and negotiation aspects.

**NO.33** How do you verify that Proxy ARP entries are loaded into the kernel?

* fw ctl arp
* show arp dynamic all
* This information can be viewed in the logs, under NAT section of log, field: Proxy ARP entry
* fw ctl get arp list all

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.

**NO.34** What are the available types of licenses in Check Point?

* Evaluation, Perpetual, Trial, Subscription
* Evaluation, Perpetual, Test, Free
* Free, Evaluation, Annual, Lifetime
* Annual, Perpetual, Test, Free

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.

**NO.35** Which of the following is NOT an account user classification?

* Licensers
* Manager
* Viewer
* Administrator

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.

**NO.36** Select the correct statement about service contracts.

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

Service contractsin Check Point environments must be stored on theSecurity Management Serverbefore 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.

**NO.37** The communication between the Security Management Server and Security Gateway to forward logs is done using the following process and port number:
* fwd, TCP 257
* cpm, 19009
* fwm, TCP 18190
* fwm, TCP 257

TheFWDprocess communicates between the Security Management Server and the Security Gateway to forward logs usingTCP 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.

**NO.38** What is the impact of an expired or missing contract file?
* The existing protection settings will be removed in SmartConsole but protections are still being enforced by the Security Gateway.
* 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.
* The existing protection settings display in SmartConsole remain and the Security Gateway will use a 14- day EVAL free license instead.
* The existing protection settings display in SmartConsole remain but are not being enforced by the Security Gateway.

When a contract file expires or is missing, theexisting protection settingscontinue to display in SmartConsole butare no longer enforcedby 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.

**NO.39** Which of the following System Monitoring Commands (Linux) shows process resource utilization, as well as CPU and memory utilization?
* df
* free
* ps
* top

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.

**NO.40** Which of the following is a valid way to capture packets on Check Point gateways?
* Firewall logs
* Wireshark
* tcpdump
* Network taps

tcpdumpis 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.

**NO.41** Which command shows the installed licenses and contracts on a Check Point device?
* cplicenses print -x
* cplic print-s
* fwlic print -x
* cplic print-x

Thecplic print-xcommand 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.

**NO.42** Running tcpdump causes a significant increase on CPU usage, what other option should you use?
* fw monitor
* Wait for out of business hours to do a packet capture
* cppcap
* You need to use tcpdump with -e option to decrease the length of packet in captures and it will utilize the less CPU
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.

**NO.43** 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?
* 19009
* 18190
* 18210
* 18191
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.

**NO.44** What are some measures you can take to prevent IPS false positives?
* Capture packets, Update the IPS database, and Back up custom IPS files
* Use Recommended IPS profile
* Use IPS only in Detect mode
* Exclude problematic services from being protected by IPS (sip, H.323, etc.)
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.