CheckPoint 156-590 CTPS Practice Questions

Shared by Osborne on 24-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the purpose of the Profile Cleanup option?

Options:

A- It lets you start over by removing all administrator overrides.
B- It merges protection settings from multiple profiles into the Optimized Profile.
C- It serves as a cleanup policy if none of the protection matches the packets.
D- It eliminates protections automatically which hasn't been used for a predefined amount of time.

Answer:

A

Explanation:

The correct answer is A. It lets you start over by removing all administrator overrides. Profile Cleanup is a profile-maintenance function used when manual IPS protection changes have accumulated and the administrator wants to return the profile to its intended baseline logic. Check Point's IPS Protections documentation describes the Profile Cleanup window as offering actions such as Remove all user modified and Clear all staging, followed by installing the Threat Prevention Policy.

This makes the feature a reset and hygiene mechanism, not a rulebase cleanup rule. It removes administrator-level overrides that may have been introduced during tuning, temporary mitigation, testing, exception handling, or staged rollout of protections. Option B is incorrect because Profile Cleanup does not merge settings from several profiles into the Optimized Profile. Option C is incorrect because unmatched traffic handling is controlled by policy/rule behavior, not by Profile Cleanup. Option D is incorrect because protections are not automatically removed based on usage age by this option. The administrative value of Profile Cleanup is control: it lets the security architect re-align a profile with its default or intended activation criteria. Reference topics: IPS Protections, Activation Overrides, Profile Cleanup, Staging, Threat Prevention Policy installation.

Question 2

Question Type: MultipleChoice

What is the purpose of the Packet Capture Track option?

Options:

A- You can visualize traffic information with a third-party XDR tool.
B- The security Gateway sends a packet capture file along with the log file. The former can by analyzed with an external tool, such as WireShark.
C- You can specify the time after which the connection has to be reinitialized.
D- You can specify a threshold value which serves as a limit after which the connection will be reset.

Answer:

B

Explanation:

The correct answer is B. The Security Gateway sends a packet capture file along with the log file. The former can be analyzed with an external tool, such as Wireshark. Packet Capture is a tracking enhancement used when logs alone are not enough to understand the traffic that triggered a security event. Check Point documentation explains that Packet Capture lets administrators capture network traffic and that the packet-capture content provides greater insight into the traffic that generated the log. When this feature is activated, the Security Gateway sends a packet-capture file with the log to the Log Server.

This is especially useful for IPS and Threat Prevention troubleshooting because analysts can inspect payload structure, headers, protocol behavior, retransmissions, and exact traffic context behind a prevention or detection event. Packet captures can then be opened in external protocol-analysis tools such as Wireshark for deeper investigation. Option A is incorrect because Packet Capture is not specifically an XDR visualization feature. Option C is unrelated to tracking and describes a timeout-style behavior. Option D describes threshold/reset logic, not packet evidence collection. Reference topics: Packet Capture Track option, Logs & Monitor, Threat Prevention event analysis, IPS troubleshooting, packet-level evidence.

Question 3

Question Type: MultipleChoice

Which protection setting is generally the LEAST resource intensive?

Options:

A- Prevent
B- Inspect
C- Detect
D- Inactive

Answer:

D

Explanation:

The correct answer is D. Inactive. A protection set to Inactive is not enforced for matching traffic, so it does not impose the same inspection and enforcement cost as active protection states. Check Point documentation explains that a Threat Prevention profile determines which protections are activated and which Software Blades are enabled for a rule or policy. The protections a profile activates depend on factors such as performance impact, threat severity, confidence level, and blade-specific settings. Check Point best-practice material also describes that administrators may tune IPS profiles and set protections to prevent, detect, or inactive.

The relative resource logic is direct: Prevent is usually the most expensive because the gateway must inspect and enforce a blocking action inline. Inspect and Detect still require traffic analysis and matching logic, even if the final result is logging rather than prevention. Inactive removes the protection from enforcement consideration, making it the lowest resource option. This does not mean administrators should disable protections indiscriminately; Inactive should be used only when justified by risk, false-positive analysis, performance tuning, or compensating controls. Reference topics: IPS profile tuning, activation settings, performance impact, Prevent/Detect/Inactive behavior, Threat Prevention optimization.

Question 4

Question Type: MultipleChoice

What is the primary benefit of DNS Trap?

Options:

A- Infected host identification
B- Blocking known bad URLs
C- Blocking outbound malicious DNS queries
D- Blocking inbound malicious DNS queries

Answer:

A

Explanation:

The correct answer is A. Infected host identification. Malware DNS Trap is designed to help identify compromised clients by redirecting malicious DNS resolution to a controlled false IP address and then observing which internal hosts attempt to connect to that trap address. Check Point's R81.20 Threat Prevention guide states that Malware DNS Trap can be used to detect compromised clients by checking logs with connection attempts to the false IP address. It also notes that internal DNS servers can be added to better identify the origin of malicious DNS requests.

This makes the primary operational benefit host attribution. While DNS security can block or prevent malicious DNS-related activity, DNS Trap's distinctive value is showing which internal endpoint is likely infected or attempting malicious communication. Option B is more aligned with URL Filtering or URL reputation, not DNS Trap. Option C describes a blocking outcome, but it misses the key trap mechanism and attribution purpose. Option D is incorrect because the usual DNS Trap use case concerns internal clients generating suspicious outbound DNS or follow-up connections, not inbound malicious DNS queries. Reference topics: Malware DNS Trap, Anti-Bot & Advanced DNS, false IP address, compromised-client detection, infected-host investigation.

Question 5

Question Type: MultipleChoice

What are the three Preconfigured Threat Prevention Profiles?

Options:

A- Inbound, Outbound, Etherbound.
B- Perimeter, Datacenter, East-West Communication.
C- North-South, East-West, Lateral Movement.
D- Basic, Optimized, Strict.

Answer:

D

Explanation:

The correct answer is D. Basic, Optimized, Strict. Check Point supplies out-of-the-box Threat Prevention profiles to give administrators predefined security/performance baselines. The official Threat Prevention Profiles section states that administrators can clone a selected profile but cannot change the out-of-the-box profiles: Basic, Optimized, and Strict.

These profiles represent different operating postures. Basic is designed for reliable protection with lower performance impact. Optimized is the default-style balanced approach, providing strong protection for common products and protocols while preserving gateway performance. Strict provides wider coverage and more aggressive protection selection, but can increase inspection cost and may require closer tuning. The other answer choices describe architectural traffic directions or deployment zones, not the official preconfigured profile names. ''Perimeter,'' ''Datacenter,'' and ''East-West'' are useful design concepts, especially in modern segmentation and Autonomous Threat Prevention discussions, but they are not the three preconfigured Custom Threat Prevention profiles in this question. From a certification perspective, the distinction matters because profiles are selected as the Action in Threat Prevention rules and determine which protections and blades are active. Reference topics: Threat Prevention Profiles, out-of-the-box profiles, Basic profile, Optimized profile, Strict profile, profile cloning.

Question 6

Question Type: MultipleChoice

In Anti-Virus, What is one of the benefits of Deep Scanning?

Options:

A- Best performance
B- Minimal resource utilization
C- Minimal buffering
D- Thorough protection

Answer:

D

Explanation:

The correct answer is D. Thorough protection. Deep Scanning is selected when the organization wants broader and more complete Anti-Virus inspection, even at the cost of additional processing. Check Point's Anti-Virus settings documentation shows that administrators can

configure file handling to process file types known to contain malware, process specific file-type families, or process all file types. It also states that enabling deep inspection scanning impacts performance.

This is the key tradeoff: Deep Scanning improves protection depth by expanding the set of files and content types subjected to inspection, but it is not the best choice for minimal latency or lowest resource consumption. Options A, B, and C are therefore incorrect because Deep Scanning is not primarily a performance optimization. It can require more CPU, memory, buffering, file classification, and scanning time, especially when paired with archive scanning, HTTPS Inspection, or large file transfers. Its benefit is security completeness: it reduces blind spots by inspecting more file content and providing stronger protection against malware hidden in less common or less obvious file types. Reference topics: Anti-Virus Settings, File Types, Deep Inspection Scanning, process all file types, performance impact, thorough malware protection.

Question 7

Question Type: MultipleChoice

What kind of blade is the IPS considered?

Options:

A- Preventative
B- Pre-infection
C- Inline
D- Post-infection

Answer:

B

Explanation:

The correct answer is B. Pre-infection. IPS is categorized as a pre-infection Threat Prevention blade because its primary role is to stop exploitation attempts before the protected host becomes compromised. Check Point's Threat Prevention guide describes IPS as protection against malicious and unwanted network traffic, focusing on application and server vulnerabilities, in-the-wild attacks, exploit kits, and malicious attackers. The same guide distinguishes Anti-Bot & Advanced DNS as post-infection detection of bots on hosts, while Anti-Virus is described as pre-infection detection and blocking of malware at the gateway.

IPS belongs in the pre-infection stage because it prevents the exploit chain from succeeding. It inspects network traffic for vulnerability exploitation, protocol abuse, malformed payloads,

known CVE exploitation attempts, server attacks, client attacks, and suspicious patterns that could lead to compromise. ''Preventative'' is broadly true as an English description, but it is not the specific Check Point lifecycle classification tested here. ''Inline'' describes where a security function may sit in traffic flow, not the infection-stage category. ''Post-infection'' is associated with Anti-Bot, which detects and blocks command-and-control communications after a host shows signs of compromise. Reference topics: IPS Software Blade, pre-infection prevention, exploit protection, Threat Prevention architecture, Anti-Bot post-infection contrast.