CheckPoint

156-590

Check Point Certified Threat Prevention Specialist Exam

Questions & Answers (Demo)

Version: 4.0

Question: 1

Which process is responsible for Archive Scanning?

A. zipscn

B. psl_dlp

C. gzscn_proc

D. dlpu

Answer: A

Explanation:

The correct answer is A. zipscn. Archive Scanning is part of the Anti-Virus file-inspection workflow, where compressed archives must be unpacked and inspected before the gateway can make a final malware-prevention decision. Check Point documentation describes Archive Scanning as the configuration area used to define how the ThreatSpect engine unpacks and scans file archives. It also defines controls such as how long archive processing may continue and what action is taken if the maximum scan time is exceeded. In the Threat Prevention Administration Guide, enabling archive scanning is described as an Anti-Virus setting in which the Anti-Virus engine unpacks archives and applies proactive heuristics, with an explicit note that this feature can impact network performance.

The process name associated with this archive-processing function is zipscn. The distractors do not fit the archive-scanning function: psl_dlp and dlpu are associated with DLP/user-space processing contexts, while gzscn_proc is not the named Archive Scanning process for this blade function. Reference topics: Anti-Virus Settings, Archive Scanning, ThreatSpect engine, archive unpacking, proactive heuristics.

Question: 2

That Tracking option can be used to capture additional data for analysis by Check Point TAC?

A. Alert

B. Forensics

C. SNMP

D. User Defined

Answer: B

Explanation:

The correct answer is B. Forensics. In Threat Prevention policy tracking, Forensics is the tracking option intended to enrich Threat Prevention logs with additional investigation data. Check Point documentation states that the Forensics option adds fields to the Threat Prevention logs, and that this extra information provides a deeper understanding of an attack. The Monitoring Threat Prevention section further explains that Advanced Forensics Details can appear in logs for supported protocols such as DNS, FTP, SMTP, HTTP, and HTTPS, and that this additional information is used by Check Point researchers to analyze attacks.

This is why Forensics is the correct TAC-oriented tracking choice. Alert is a notification-style tracking action, not a deep forensic enrichment mechanism. SNMP sends a management notification, and User Defined invokes administrator-defined alert handling rather than supplying advanced attack-analysis fields. In operational troubleshooting, Forensics is valuable because it preserves richer evidence around the inspected connection, affected blade, protocol behavior, and detection context. Reference topics: Threat Prevention Policy Track Options, Advanced Forensics Details, Logs & Monitor, TAC escalation analysis.

Question: 3

What is the purpose of the Profile Cleanup option?

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: 4

Which is NOT true of Threat Prevention policy application?

A. Only applied after traffic is accepted by Access Control Policy

B. Traffic is matched against all applicable layers at the same time

C. Only applies first matched rule

D. Applied as ordered layer

Answer: B

Explanation:

The correct answer is B. Traffic is matched against all applicable layers at the same time. Threat Prevention policy evaluation is not best described as a flat simultaneous match against all applicable layers. Check Point documentation explains that Threat Prevention Policy Layers are Ordered Layers, and that each ordered layer calculates its action separately from the other layers. In a single-layer policy package, the enforced rule is the first matched rule. In multiple-layer policy behavior, matching and enforcement are determined by the layer calculations and the applicable action logic, rather than by one undifferentiated simultaneous match model.

Option A is true because Threat Prevention inspection is applied after the Access Control policy allows the connection; traffic dropped or rejected by Access Control does not proceed to Threat Prevention enforcement. Option C is true for a single Threat Prevention layer because the first matching rule is enforced. Option D is also true because Threat Prevention uses ordered policy-layer behavior. The false statement is therefore option B. Reference topics: Threat Prevention Policy,

Ordered Layers, first-match rule behavior, Access Control before Threat Prevention, multi-layer enforcement logic.

Question: 5

What is the recommended setting for Anti-Virus and why?

A. Background because it is Post-infection

B. Hold because it is Pre-infection and inspects a limited subset of traffic

C. Hold because it inspects a limited subset of traffic

D. Background because it inspects a large subset of traffic

Answer: D

Explanation:

The correct answer is D. Background because it inspects a large subset of traffic. Anti-Virus is a pre-infection Threat Prevention blade that can inspect broad user traffic categories, including web and file-transfer flows. Because the inspection scope can be large, the selected enforcement behavior directly affects latency, user experience, and gateway resource consumption. Check Point documentation identifies Anti-Virus as a blade that scans protocols such as HTTP/HTTPS, FTP, SMB, and mail-related traffic depending on configuration, with additional protocol support documented for IMAP and POP3.

The Background setting is recommended in this context because it avoids unnecessarily holding a large volume of traffic while inspection continues. Hold mode is stricter because it delays delivery until inspection completes or a timeout condition is reached, but that strictness can introduce user-facing delay when applied broadly. Option A is incorrect because Anti-Virus is not post-infection; it prevents malware before user impact. Options B and C are incorrect because they associate Hold mode with a limited inspection scope, while Anti-Virus commonly applies to a large and performance-sensitive traffic set. Reference topics: Anti-Virus Settings, protocol inspection scope, Background versus Hold behavior, performance impact, pre-infection prevention.