DUMPSARENA

Check Point Certified Threat Prevention Specialist (CTPS)

Checkpoint 156-590

Version Demo

Total Demo Questions: 8

Total Premium Questions: 84

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Threat Prevention Overview	17
Topic 2, Threat Prevention Policy	17
Topic 3, Threat Prevention Profiles	26
Topic 4, Threat Prevention Updates	6
Topic 5, Threat Prevention Monitoring	12
Topic 6, Threat Prevention Troubleshooting	5
Topic 7, Mix Questions	1
Total	84

QUESTION NO: 1

Where is IPS primarily enforced?

A. Post-infection

B. Post-inspection

C. Pre-infection

D. Pre-inspection

ANSWER: C

Explanation:

Pre-infection is correct because the IPS Software Blade is intended to prevent an intrusion from successfully exploiting a vulnerability or abusing a protocol before a protected system is compromised. It examines traffic as it traverses the Security Gateway and applies protections for known vulnerability exploits, protocol anomalies, malicious payloads, and suspicious behavior. When a configured IPS protection detects an attack attempt, the gateway can prevent the relevant traffic from reaching its target, stopping the attack at the network-enforcement point before exploitation can result in unauthorized access, code execution, or malware installation.

This placement makes IPS a preventive control in Check Point's threat-prevention architecture. Its protections are designed to address the attack stage in which an attacker attempts to use a weakness in a client, server, operating system, or application. Administrators configure IPS profiles and actions in Threat Prevention policy, then install that policy on the gateway so enforcement occurs inline for matching connections. Check Point's IPS documentation describes the blade as protecting networks against attacks through signatures and other protections, while its Threat Prevention documentation places IPS among the controls used to block threats before they affect the organization. See Check Point IPS documentation and Check Point Intrusion Prevention System overview.

QUESTION NO: 2

An administrator needs to determine whether a newly enabled IPS protection is causing a noticeable performance impact on a Security Gateway. The administrator also needs to identify whether an increased amount of traffic is being handled in the Firewall-to-Firewall path.

Which command provides the most relevant information?

A. fw stat

B. fwaccel dos rate

C. fwaccel stats

D. cpstop

ANSWER: C

Explanation:

fwaccel stats is correct. The command provides SecureXL acceleration statistics, including information about connections handled in the Firewall-to-Firewall path and the reasons that connections could not be accelerated. This helps an administrator correlate increased F2F handling with inspection and performance behavior.

fwaccel dos rate is used for SecureXL rate-limiting configuration rather than examining acceleration statistics. fw stat displays policy and module information, but it does not provide the relevant F2F acceleration counters. cpstop stops Check Point services and is not a diagnostic command for this purpose.

QUESTION NO: 3

What is the impact of changing the Preconfigured Threat Prevention Profiles?

A. The best practice for all Check Point delivered profiles and object is to first clone them and work on the clones.

B. The impact is minimum if you first delete all of them and then build them from scratch.

C. The impact can be minimized if you use the performance check tool. You can enable it in IPS protections - > actions - > Run Protection performance check tool.

D. There is no performance or security impact in changing the Preconfigured Profiles.

ANSWER: A

Explanation:

The best practice for all Check Point delivered profiles and object is to first clone them and work on the clones. Check Point provides predefined Threat Prevention profiles, including Basic, Optimized, and Strict, as tested baseline configurations that combine Threat Emulation, Anti-Bot, Anti-Virus, IPS, and other applicable protections according to a defined security posture. These out-of-the-box profiles are not intended to be directly edited. Instead, an administrator clones the appropriate predefined profile, gives the clone a meaningful name, adjusts the required protection settings, assigns the cloned profile in the Threat Prevention policy, and installs the policy.

Using a clone preserves the original Check Point baseline for comparison, troubleshooting, and future operational reference. It also allows the organization to tailor enforcement to its own risk tolerance, traffic patterns, and performance requirements without losing the known starting configuration supplied by Check Point. This approach supports controlled change management: changes can be reviewed and tested in the cloned profile before being applied to production policy. Check Point documents the predefined profiles and the cloning workflow in its Threat Prevention Administration Guide: Threat Prevention Profiles and Creating Threat Prevention Profiles.

QUESTION NO: 4

IPS stands for?

A. Invasion Prevention Software

B. Intrusion Prevention System

C. Intrusion Prevention Software

D. Invasion Prevention System

ANSWER: B

Explanation:

Intrusion Prevention System is correct. An IPS is a security control that inspects network traffic and actively detects and prevents malicious activity, such as exploit attempts, protocol violations, and suspicious patterns associated with known threats. Unlike a detection-only capability, an intrusion prevention system can take preventative action according to its configured policy, such as dropping malicious packets, terminating connections, or logging the event for investigation. In Check Point environments, the Intrusion Prevention System is provided through the IPS Software Blade, which uses protections maintained by Check Point and configured in the Threat Prevention policy. Administrators can apply protections based on severity, confidence level, performance impact, and the organization's risk requirements. IPS is therefore the standard industry and Check Point term for this technology, as reflected in Check Point's IPS documentation and its Threat Prevention administration guidance. See Check Point IPS Best Practices and Check Point: What Is an Intrusion Prevention System?.

QUESTION NO: 5

What are the three IPS update options?

A. Auto Update, Policy Update, Update Now

B. Update Now, Schedule Update, Follow Protections

C. Update Now, Schedule Update, Follow policy

D. Manual Update, Scheduled Update, Auto Update

ANSWER: B

Explanation:

Update Now, Schedule Update, Follow Protections is correct because it reflects the operational IPS-protection update and review workflow available in Check Point SmartConsole. **Update Now** lets an administrator retrieve the current IPS protection package immediately, which is useful when newly released protections must be reviewed and deployed without waiting for the normal maintenance cycle. **Schedule Update** defines recurring automatic retrieval of IPS updates so the management environment stays current with newly published signatures, protections, and related IPS metadata. After an IPS update, the updated or newly introduced protections can be identified and reviewed through the follow-up workflow. **Follow Protections** captures this review activity: protections can be marked for follow-up, allowing an administrator to filter and assess changes before deciding how they should be handled in the Threat Prevention policy. This workflow separates obtaining updated protection content from the administrator's policy-review process. To make selected IPS settings effective on Security Gateways, the relevant Threat Prevention policy must then be installed. Check Point documents IPS protection administration and update behavior in its Threat Prevention Administration Guide and provides product-level IPS context at Check Point Threat Prevention.

QUESTION NO: 6

A security analyst is reviewing thousands of related Threat Prevention logs generated during an external attack. The analyst needs the related log records grouped into a meaningful incident view, with the ability to investigate the supporting logs.

Which SmartEvent capability should be used?

A. Generate a SmartEvent Threat Prevention Report.

B. Use SmartEvent event correlation.

C. Export the matching logs to a CSV file.

D. Use only a SmartConsole log query.

ANSWER: B

Explanation:

SmartEvent event correlation is the correct capability. SmartEvent analyzes logs received from Security Gateways and Log Servers, identifies related activity, and presents it as a consolidated security event. The analyst can then investigate the event and review the supporting logs without treating every individual record as an unrelated incident.

A SmartEvent report is intended for formatted, time-based reporting and management summaries. A SmartConsole log query filters raw logs but does not itself correlate them into a consolidated event. Exporting logs to an external file also does not provide SmartEvent correlation.

QUESTION NO: 7

Which protection setting is generally the LEAST resource intensive?

A. Prevent

B. Inspect

C. Detect

D. Inactive

ANSWER: D

Explanation:

Inactive is generally the least resource-intensive protection setting because the specific Threat Prevention protection is disabled. When a protection is inactive, the Security Gateway does not apply that protection's inspection logic, pattern matching, protocol parsing, or enforcement processing to traffic. Consequently, it adds no meaningful per-connection or per-packet processing overhead for that protection. This setting can be appropriate where a protection is not relevant to an organization's environment, where a documented compatibility exception is necessary, or while administrators are deliberately controlling which protections are enabled in a Threat Prevention profile.

Check Point Threat Prevention profiles allow protections to be configured with activation and action settings. An active protection requires the gateway to inspect applicable traffic in order to identify a matching threat or event and potentially generate logs or take an enforcement action. By contrast, an inactive protection is excluded from this processing path. Although overall gateway utilization still depends on the enabled blades, traffic volume, enabled features, logging, and the remaining active protections, disabling one protection minimizes that individual protection's resource use. See Check Point's Threat Prevention Profile documentation and the protection configuration guidance.

QUESTION NO: 8

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: B

Explanation:

Hold because it is Pre-infection and inspects a limited subset of traffic is the recommended setting. Check Point Anti-Virus is a pre-infection protection: its purpose is to identify and block malicious files before they reach the client and can execute. Hold mode supports that objective by retaining the applicable file transfer until the gateway receives a verdict from the Anti-Virus inspection process. A clean result permits delivery, whereas a malicious verdict allows the configured prevention action to be applied before the file is released to the endpoint.

Anti-Virus inspection is applied to supported file-transfer and content protocols rather than indiscriminately examining every flow as a full-session behavioral analysis engine would. This more limited inspection scope makes Hold mode the appropriate recommended trade-off when the security goal is to prevent delivery of infected content. The setting provides a stronger pre-infection control point while preserving the intended Anti-Virus protection workflow. Check Point's Threat Prevention Administration Guide describes Anti-Virus as a protection against malicious files and documents the relevant inspection and policy behavior. See the Check Point R81.20 Threat Prevention Administration Guide and Check Point's Anti-Virus protection overview.