Vendor: Check Point

Exam Code: 156-590

Exam Name: Check Point Certified Threat Prevention Specialist (CTPS)

Version: DEMO

QUESTION 1
What does the IPS Follow Protections feature do?

A. Automatically activates new protections based on profile
B. Flags newly downloaded protections for review
C. Generates a report of activity from new protections
D. Highlights log entries for new protections

Answer: A
Explanation:
IPS protections are governed by Threat Prevention profiles, and those profiles determine which protections are activated for a rule or policy. Check Point documentation states that a Threat Prevention profile determines which protections are activated and which Software Blades are enabled for the specified rule or policy. For newly downloaded IPS protections, Check Point documents that automatic IPS update behavior can use the profile settings as the default action for those newly downloaded protections.

QUESTION 2
SecureXL full acceleration happens on which component?

A. irq
B. snd
C. dynamic dispatcher
D. cpu core

Answer: B
Explanation:
In Check Point performance architecture, SND means Secure Network Distributor. It is the CoreXL component that receives traffic from network interfaces, performs SecureXL acceleration where possible, and distributes non-accelerated traffic to CoreXL Firewall instances for deeper inspection. Check Point's Performance Tuning documentation describes CoreXL SND as responsible for processing incoming traffic, securely accelerating authorized packets when SecureXL is enabled, and distributing non-accelerated packets between Firewall kernel instances.

QUESTION 3
What is the main purpose of IPS Implied Exceptions?

A. This defines the handling of traffic if no IPS rule applied to the appropriate packets.
B. This defines the handling of traffic if you do not have an IPS Policy as part of an ordered layer.
C. This feature is to prevent IPS Enforcement to interfere with important Security Gateway operations, such as Control Connections.
D. This defines the handling of traffic if you do not have an IPS Policy as part of an Inline layer.

Answer: C
Explanation:
IPS Implied Exceptions are designed as safeguard exceptions for traffic that is necessary for the Security Gateway, management, or Check Point infrastructure to operate correctly. The purpose is not to define general unmatched-traffic behavior. Instead, they prevent IPS enforcement from disrupting essential control-plane and gateway-related communications. Check Point's Threat Prevention exception documentation shows that IPS exceptions are a formal part of policy tuning and that exception changes are enforced through policy installation.

QUESTION 4
At what point is the Anti-Bot blade enforced?

A. Pre-infection
B. Post-infection
C. Pre-inspection
D. Post-inspection

Answer: B
Explanation:
Anti-Bot is the Threat Prevention blade focused on identifying and stopping bot-infected hosts after compromise indicators appear. Check Point documentation explicitly describes Anti-Bot as performing post-infection detection of bots on hosts and preventing bot damage by blocking command-and-control communications. The broader Threat Prevention guide also lists Anti-Bot as post-infection detection and explains that it uses ThreatCloud intelligence and multiple detection methods to identify bot activity.

QUESTION 5
What is/are the enabled by default protocols supported by the Antivirus Blade?

A. HTTP/HTTPS, FTP, SMB, SMTP
B. HTTP/HTTPS, FTP, SMB
C. HTTP/HTTPS
D. HTTP/HTTPS, FTP

Answer: C
Explanation:
The course-guide answer identifies HTTP/HTTPS as the Anti-Virus protocols enabled by default. Architecturally, this reflects the most common perimeter malware-delivery path: users downloading web content from the Internet. HTTP is naturally visible to the gateway, while HTTPS requires HTTPS Inspection to expose encrypted file transfers and web objects for Anti-Virus inspection. Check Point documentation notes that most traffic is HTTPS rather than HTTP and recommends enabling HTTPS Inspection to maximize the effectiveness of Threat Prevention Software Blades.

QUESTION 6
What is necessary to activate the exception to all Security Gateways?

A. Install Database is sufficient.
B. You have to re-install the Threat Prevention policy.
C. You have to re-install the Access Control policy.
D. The changes will be applied immediately, so no need to do anything.

Answer: B
Explanation:
Threat Prevention exceptions are policy constructs, so they must be compiled and installed to the relevant Security Gateways before they affect enforcement. Check Point documentation for creating IPS exceptions shows the workflow: create or configure the exception rule, click OK, and then Install Policy. The Custom Threat Prevention guide also explains that Threat Prevention blades have a dedicated Threat Prevention policy and that this policy can be installed separately

from Access Control. It explicitly recommends installing only the Threat Prevention policy to minimize performance impact on Security Gateways.

QUESTION 7
What kind of information is stored in the Audit Log?

A. An audit log is a record of actions taken by administrators.
B. An audit log is a record of system event logs on the Security Management Server.
C. An audit log is a portion of the traffic log which has been filtered by filter expression defined by the administrator.
D. An audit log is a record of system event logs on the Security Gateway.

Answer: A
Explanation:
In Check Point management architecture, audit logs are different from traffic logs, threat logs, or operating-system event logs. A traffic log records inspected network connections and blade decisions. A threat log records Threat Prevention detections, preventions, packet captures, forensic details, and blade-specific events. An audit log records administrative activity performed in the management environment. The uploaded Check Point glossary material defines an Audit Log as a log that contains administrator actions on a Management Server, including login and logout, creation or modification of an object, and installation of a policy.

QUESTION 8
Which process is responsible for communication with the Check Point ThreatCloud for the sake of Anti-Virus Protection Update?

A. The CPAS Daemon (cpasd)
B. The Resource Advisor Daemon (RAD)
C. The PSL AV-Daemon (pslavd)
D. The Threat Emulation Daemon "ted"

Answer: A
Explanation:
In the course-guide context, cpasd is the process associated with Anti-Virus communication toward Check Point ThreatCloud for protection-update and classification purposes. The functional reason is that Anti-Virus file inspection depends on Check Point's ThreatSpect and ThreatCloud intelligence pipeline. Check Point documentation explains that each Security Gateway has a Malware database and a local cache; when the cache has no answer, it queries the ThreatCloud repository. For Anti-Virus, the signature is sent for file classification.

QUESTION 9
Core Activation Exceptions are applied to what?

A. Protection Groups
B. Threat Cloud
C. Inspection Settings
D. Individual Protections

Answer: D
Explanation:
Core Activation Exceptions are used to override activation behavior at the protection level, not at

a broad ThreatCloud, inspection-engine, or protection-group abstraction. The official IPS profile settings documentation explains that the Additional Activation section gives administrators granular control to select IPS protections to activate or deactivate. It states that activated protections are enforced by gateways, while deactivated protections are not enforced, regardless of the general profile protection settings.

QUESTION 10
Using IPS can send a large part of traffic to F2F path.
Which command can you use to enforce traffic quotas?

A. fw dos rate
B. fwaccel rate
C. fw ctl dos
D. fwaccel dos rate

Answer: D
Explanation:
When IPS or other Threat Prevention inspection causes significant traffic to leave the fully accelerated SecureXL path and move to F2F, the gateway can experience higher CPU utilization because more packets require Firewall kernel processing. The fwaccel dos rate command belongs to SecureXL DoS and rate-limiting controls. Check Point's Performance Tuning guide defines fwaccel dos rate and fwaccel6 dos rate as commands that show and install the Rate Limiting policy in SecureXL. It also notes that the feature is enabled by default without rules.

QUESTION 11
What happens to traffic that matches the Access Control Policy but not the Threat Prevention Policy?

A. It is dropped and logged.
B. It is accepted and logged.
C. It is accepted.
D. The traffic is not dropped. It is simply not inspected by the Threat Prevention Engine.

Answer: D
Explanation:
It is simply not inspected by the Threat Prevention Engine. Access Control and Threat Prevention are separate enforcement stages. The Access Control policy first decides whether the connection is allowed, rejected, or dropped. If Access Control accepts the connection, Threat Prevention is then applied only if the connection matches a Threat Prevention rule and therefore receives a Threat Prevention profile. Check Point documentation describes Threat Prevention policy as the mechanism used to activate only the protections needed and prevent attacks that most threaten the network. It also explains that Threat Prevention policy layers calculate their action separately and that in a single layer, the first matched rule is enforced.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**