Practice With CheckPoint 156-590 Mock Test

Shared by Vega on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What Track - Settings Forensics does not?

Options:

A- When enabled, advanced forensics detailed information is included in logs.
B- Check Point researchers use advanced forensics details for troubleshooting and attack analysis.
C- Forensics details also include Security Gateway statistics, which are sent to the Check Point Cloud.
D- Communicate forensics data collected to Government Agencies.

Answer:

D

Explanation:

The correct answer is D. Communicate forensics data collected to Government Agencies. The Forensics tracking option exists to enrich Threat Prevention logs with deeper technical context for analysis and troubleshooting. Check Point documentation states that the Forensics option adds fields to Threat Prevention logs and that the additional information gives a deeper understanding of an attack. The Monitoring Threat Prevention guidance also explains that Advanced Forensics Details can include protocol-specific details for DNS, FTP, SMTP, HTTP, and HTTPS, and that this information is used by Check Point researchers to analyze attacks.

The purpose is security analysis, incident investigation, and support-quality evidence collection, not government reporting. Options A and B accurately describe the function of Forensics tracking. Option C reflects the broader idea that forensic and diagnostic details may include gateway-related technical data for Check Point analysis, depending on configuration and feature behavior. Option D is the false statement because Check Point Threat Prevention Forensics is not defined as a mechanism for transmitting collected forensic data to government agencies. In production, enabling Forensics should be treated as a deliberate logging and privacy decision because it may add protocol and transaction context to logs. Reference topics: Threat Prevention Track Options, Forensics tracking, Advanced Forensics Details, Logs & Monitor, attack analysis.

Question 2

Question Type: MultipleChoice

What is the action for newly updated protections which is set in Staging Mode?

Options:

A- Detect
B- Bypass
C- None
D- Prevent

Answer:

A

Explanation:

The correct answer is A. Detect. IPS Staging Mode is designed to introduce newly updated protections safely by observing their effect before enforcing active prevention. Check Point documentation states that when newly updated protections are set to Staging Mode, they remain in staging until the administrator changes their configuration. The default action for protections in staging mode is Detect, and this can be changed manually in the IPS Protections page. The R81.20 guide states the same behavior: newly updated protections in staging mode remain there until changed, and their default action is Detect.

This behavior is important during IPS lifecycle management because new signatures can introduce unexpected matches in production traffic. Detect mode allows the gateway to log and expose what the protection would have matched while avoiding immediate blocking. That gives administrators time to validate logs, tune exceptions, confirm confidence level, and assess business impact before switching to Prevent. Bypass would skip inspection and is not the staging default. None is not the default action. Prevent may be the final desired enforcement state, but staging intentionally avoids immediate prevention until analysis is complete. Reference topics: IPS Updates Policy, Staging Mode, Newly Updated Protections, Detect action, IPS protection rollout.

Question 3

Question Type: MultipleChoice

What is the name of the default Threat Prevention Profile?

Options:

A- Basic
B- Standard
C- Strict
D- Optimized

Answer:

D

Explanation:

The correct answer is D. Optimized. In Check Point Threat Prevention, profiles define how the gateway applies protections across blades such as IPS, Anti-Bot, Anti-Virus, Threat Emulation, and Threat Extraction. The default profile is Optimized, because it balances effective security with acceptable gateway performance. Check Point documentation states that the Optimized profile is activated by default and that it gives excellent security with good gateway performance.

This design reflects the practical tradeoff in enterprise Threat Prevention: not every protection should be enabled at the most aggressive setting on every gateway, because high-impact protections can increase CPU consumption, latency, and inspection overhead. The Optimized profile uses criteria such as protection severity, confidence, and performance impact to activate protections that are broadly useful without creating unnecessary operational cost. Basic is less aggressive and is intended for lower-impact protection coverage. Strict provides wider coverage but can affect performance more significantly. Standard is not one of the default Threat Prevention profiles in this context. Reference topics: Threat Prevention Profiles, default profile behavior, Optimized Protection Profile settings, blade activation, security/performance balance.

Question 4

Question Type: MultipleChoice

What is necessary to do in order for the IPS Core Protection to take effect?

Options:

A- Nothing is to be done, since the Core Protection settings are immediately active.
B- Install the Access Control Policy.
C- Install the Threat Prevention Policy.
D- Perform 'Install Database' on the Management Server.

Answer:

C

Explanation:

The correct answer is C. Install the Threat Prevention Policy. IPS Core Protections are part of the Threat Prevention policy domain, so changing them in SmartConsole is not enough by itself. The updated configuration must be compiled and installed to the relevant Security Gateways through the Threat Prevention Policy installation process. Check Point's IPS Protections documentation shows the workflow for editing core protections: go to Security Policies > Threat Prevention > Custom Policy Tools > IPS Protections, filter for Type Core, edit the required core protection settings, and then Install the Threat Prevention policy.

This directly eliminates the other options. The setting is not immediately active because gateways enforce installed policy, not merely edited management configuration. Install Database updates the management database but does not push enforcement logic to the Security Gateway. Install Access Control Policy applies firewall/access-layer logic, but IPS Core Protections belong to the Threat Prevention policy. In operational terms, this separation allows administrators to install Threat Prevention changes without necessarily reinstalling Access Control, reducing disruption and keeping blade changes scoped to the correct policy package. Reference topics: IPS Protections, Core IPS Protections, Custom Policy Tools, Threat Prevention Policy installation, enforcement lifecycle.

Question 5

Question Type: MultipleChoice

What is a distinct limitation of Active Streaming compared to Passive Streaming in conjunction with Anti-Virus?

Options:

A- Only scheduled scans are possible.
B- File size limits.
C- There is no limitation.

D- Only a subset of file types supported.

Answer:

D

Explanation:

The correct answer is D. Only a subset of file types supported. In Check Point traffic inspection architecture, Passive Streaming and Active Streaming are stream-handling mechanisms used by content-inspection components. Passive Streaming allows inspection of traffic as a stream is observed, while Active Streaming is more intrusive because the gateway can actively participate in traffic handling, buffering, or modification. In Anti-Virus inspection, this distinction matters because file classification and supported file handling depend on the inspection mechanism and file-type processing model. Check Point's Anti-Virus settings expose file-type controls, including processing file-type families and configuring actions per file type. Check Point's Security Gateway documentation also identifies CPAS as Check Point Active Streaming and PSL as Passive Streaming Layer, with MUX selecting between passive and active streaming for application traffic.

The exam distinction is that Active Streaming does not provide unrestricted Anti-Virus inspection coverage across every possible file type; its limitation is that only a subset of file types is supported. Option A is wrong because Anti-Virus inspection is not limited to scheduled scans. Option B is not the distinct comparative limitation in this context. Option C is incorrect because there is a documented architectural distinction between the two streaming approaches. Reference topics: CPAS, PSL, MUX, Anti-Virus file-type processing, content inspection architecture.

Question 6

Question Type: MultipleChoice

What does ThreatCloud DGA Protection defend against?

Options:

A- Known malicious IPs
B- Infected URLs
C- Infected files
D- Newly created domains

Answer:

D

Explanation:

The correct answer is D. Newly created domains. DGA means Domain Generation Algorithm, a technique used by malware to algorithmically create large numbers of domain names for command-and-control communication. Instead of hardcoding one static C2 domain, a bot can generate many possible domains over time, making takedown and static blocking much harder. Check Point's Network Security Software Bundles datasheet states that Check Point AI Deep Learning blocks the latest DNS attacks, including Tunneling and Domain Generation Algorithm/DGA, and specifically blocks connections to the newest generation of malicious domains created via DGA.

This explains why the correct exam option is ''newly created domains.'' Known malicious IP blocking is a reputation and IP intelligence function, but it is not the specific purpose of DGA protection. Infected URLs and infected files are handled by URL reputation, Anti-Virus, Threat Emulation, and related Threat Prevention functions. DGA protection focuses on DNS-layer behavior and suspicious or algorithmically generated domain use, especially when malware attempts to contact rotating or recently generated domains for C2, payload retrieval, or data exfiltration. In operational terms, DGA protection is part of Anti-Bot and Advanced DNS defense, helping detect compromised hosts even when the malware infrastructure changes rapidly. Reference topics: ThreatCloud, DGA Protection, Advanced DNS, Anti-Bot, DNS C2 prevention.