Check Point

156-590

Check Point Certified Threat Prevention Specialist (CTPS)

Latest Version: 6.0

Question: 1

Task: Manually trigger an IPS update from SmartConsole.

A. See the Explanation.

Answer: A

Explanation:
1- Go to Threat Prevention > Updates.
2- Click “Check Now” under IPS section.
3- Wait for update to complete and view the status log.
4- On the gateway, check $FWDIR/log/ips_update.elg for details.
5- Confirm the update applied with ips stat.

Question: 2

Task: Enable “Update Automatically” for IPS database.

A. See the Explanation.

Answer: A

Explanation:
1- Go to Threat Prevention > Updates in SmartConsole.
2- Enable "Check for updates automatically."
3- Set interval (e.g., every 6 hours).
4- Tick “Install updates automatically” with warning prompt.
5- Click OK, publish, and monitor update logs.

Question: 3

Task: Configure General Protections for all protocols.

A. See the Explanation.

Answer: A

Explanation:
1- Open Threat Prevention > Profiles > Edit selected profile.
2- Navigate to General Protections tab.

3- Enable protections like “Protocol Anomaly” or “Malicious Mail Content.”
4- Set actions to Prevent/Detect based on severity.
5- Save and assign the profile to your policy.

Question: 4

Task: Configure a specific protection for DNS tunneling detection.

A. See the Explanation.

Answer: A

Explanation:
1- Go to Threat Tools > IPS Protections.
2- Search for "DNS tunneling" and select it.
3- Set action to "Prevent" and tag it for monitoring.
4- Add it to your active IPS profile.
5- Confirm with SmartConsole logs if any events occur post-enforcement.

Question: 5

Task: Clone a built-in IPS profile and tailor it to internal services.

A. See the Explanation.

Answer: A

Explanation:
1- Open Threat Prevention > Profiles.
2- Select “Optimized” > Right-click > Clone.
3- Rename it (e.g., “Internal_Services_Profile”).
4- Disable protections unnecessary for internal traffic (e.g., HTTP-related).
5- Save, apply to Threat Prevention policy layer.

Question: 6

Task: Export current IPS protections list with their actions for audit.

A. See the Explanation.

Answer: A

Explanation:
1- Go to Threat Tools > IPS Protections.
2- Use filter or leave default.

3- Click “Export > CSV.”
4- Choose file name and download location.
5- Open CSV and sort by Action or Performance Impact for analysis.

Question: 7

Task: Analyze IPS logs for common attacks detected in the past 7 days.

A. See the Explanation.

Answer: A

Explanation:
1- Open SmartConsole > Logs & Monitor.
2- Use filter: blade:IPS AND last 7 days.
3- Sort by “Attack Name” or “Destination.”
4- Identify frequently triggered protections.
5- Consider raising their severity or blocking source IPs if needed.

Question: 8

Task: Create a protection exception for an IPS protection triggered during backup scans.

A. See the Explanation.

Answer: A

Explanation:
1- Go to IPS Protections > Filter the protection name.
2- Click “Add Exception.”
3- Define the backup server's IP as source.
4- Set Action to "Detect" or "Inactive."
5- Save, publish, and recheck log results.

Question: 9

Task: Create a Threat Prevention rule targeting internal traffic with minimal IPS coverage.

A. See the Explanation.

Answer: A

Explanation:
1- Go to Threat Prevention > Policy.
2- Add a rule: Source=Internal Networks, Dest=Internal Networks.

3- Attach a custom profile with minimal protections.
4- Set Action=Accept and Track=Log.
5- Install the policy and test by generating benign internal traffic.

Question: 10

Task: Use CLI to test connectivity with IPS update servers.

A. See the Explanation.

Answer: A

Explanation:
1- SSH into the Gateway.
2- Run: curl -v https://updates.checkpoint.com.
3- Confirm certificate and connection success.
4- Run ips update now for manual update.
5- Check /opt/CPsuite-R81/fw1/log/ips_update.elg for result.