CheckPoint.156-590.v2026-06-11.q47

Exam Code:	156-590
Exam Name:	Check Point Certified Threat Prevention Specialist (CTPS)
Certification Provider:	CheckPoint
Free Question Number:	47
Version:	v2026-06-11
# of views:	123
# of Questions views:	470
https://www.freepdfdumps.com/CheckPoint.156-590.v2026-06-11.q47.html	

NEW QUESTION: 1
Task: Validate Anti-Virus updates are recent.
Answer:
See the Explanation.Explanation:
1- Use SmartConsole > Gateways > Threat Prevention > Updates.
2- Confirm update timestamp is recent.
3- SSH into Gateway and run cpstat anti-virus.
4- Run: cat $FWDIR/tmp/antivirus_status.xml to verify signature version.
5- Confirm no update errors in $FWDIR/log/antivirus_update.elg.

NEW QUESTION: 2
Task: Set Anti-Virus protections to prevent downloads of known malware in the same profile.
Answer:
See the Explanation.Explanation:
1- Edit Corporate_TP_Strict > Anti-Virus tab.
2- Enable protection against malicious files and emails.
3- Set confidence level High and Medium to Prevent.
4- Enable file scanning on protocols like HTTP, SMTP, FTP.
5- Save and close.

NEW QUESTION: 3
Task: Assign Anti-Bot and Anti-Virus profiles to a Threat Prevention policy rule.
Answer:
See the Explanation.Explanation:
1- Open Threat Prevention > Policy.
2- Add a rule with appropriate Source, Destination, Services.

3- Under "Profile," assign the custom AV/AB profile.
4- Set Action to "Accept" and Track to "Log."
5- Publish and install the policy.

NEW QUESTION: 4
Task: Roll back IPS protections to a previous version.
Answer:
See the Explanation.Explanation:
1- Go to Threat Prevention > Updates.
2- Click "View Versions" under IPS.
3- Select an older version and click "Install."
4- Monitor status and confirm with ips stat.
5- Document rollback for audit purposes.

NEW QUESTION: 5
Task: Manually trigger an IPS update from SmartConsole.
Answer:
See the Explanation.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.

NEW QUESTION: 6
Task: Simulate false positive and create a detection-only override.
Answer:
See the Explanation.Explanation:
1- Generate test traffic causing a prevent log in SmartConsole.
2- Identify the IPS protection name.
3- Add an exception for that IP or subnet with action "Detect."
4- Re-test traffic and verify logs reflect "Detect."
5- Document the false positive and report to Check Point if needed.

NEW QUESTION: 7
Task: Enable SSH and HTTP monitoring on Gateway.
Answer:
See the Explanation.Explanation:
1- SSH into the Gateway.
2- Run: cpconfig and choose "Enable WebUI."
3- Open firewall rule for ports 22 and 443.

4- Confirm access via browser and SSH client.
5- Check SmartConsole > Logs for connection attempts.

NEW QUESTION: 8
Task: Confirm IPS protections are correctly layered when using shared layers.
Answer:
See the Explanation.Explanation:
1- Go to Threat Prevention Policy > Layers tab.
2- Confirm shared layer is attached to Threat Prevention layer.
3- Double-check profile bindings per rule.
4- Publish and install to apply globally.
5- Use logs to validate consistent protection across gateways.

NEW QUESTION: 9
Task: Simulate a port scan and verify IPS logs.
Answer:
See the Explanation.Explanation:
1- From a test machine, run: nmap .
2- On SmartConsole, go to Logs & Monitor.
3- Filter logs for blade:"IPS" and source IP of test machine.
4- Confirm log action is "Prevented" or "Detected."
5- Open the log to analyze the protection triggered.

NEW QUESTION: 10
Task: Create an exception for Anti-Virus detection on a custom port.
Answer:
See the Explanation.Explanation:
1- Open Threat Prevention > Protections.
2- Choose "Anti-Virus Protections" and select the one triggered.
3- Add Exception: Service/Port = custom (e.g., 8081).
4- Set action to "Detect" for this exception.
5- Publish changes and validate behavior in logs.

NEW QUESTION: 11
Task: Export IPS protections list to CSV for audit.
Answer:
See the Explanation.Explanation:
1- In SmartConsole, open Threat Tools > IPS Protections.
2- Use filters to narrow scope.
3- Click "Export" > Choose CSV.
4- Save locally and open to review.

5- Check for inactive or outdated protections.

NEW QUESTION: 12
Task: Check the current IPS protection version on the Security Gateway.
Answer:
See the Explanation.Explanation:
1- Open SmartConsole > Gateways & Servers.
2- Select the gateway and go to the "Threat Prevention" tab.
3- Note the IPS database version and timestamp.
4- On CLI: run ips stat to cross-verify.
5- Ensure version matches the latest published by Check Point.

NEW QUESTION: 13
Task: Use SmartConsole to verify that the correct profile is applied to gateway traffic.
Answer:
See the Explanation.Explanation:
1- Generate traffic that matches the Threat Prevention rule.
2- Go to Logs & Monitor, search by source/destination.
3- Confirm the Profile name in the log entry under Threat Prevention details.
4- Cross-reference with the rule base.
5- Adjust rules if wrong profile is triggered.

NEW QUESTION: 14
Task: Compare two custom profiles for audit validation.
Answer:
See the Explanation.Explanation:
1- Export both profiles via SmartConsole.
2- Use external diff tool or compare policy settings manually.
3- Focus on blade settings, confidence levels, and exceptions.
4- Document differences and justify configuration choices.
5- Store comparison for audit records.

NEW QUESTION: 15
Task: Create a new Threat Prevention profile in SmartConsole.
Answer:
See the Explanation.Explanation:
1- Go to Threat Prevention > Profiles.
2- Click "New Profile" and name it.
3- Adjust IPS, Anti-Bot, and AV settings to "Prevent" or "Detect."
4- Save and assign it to relevant policy layers.
5- Publish and install policy.

NEW QUESTION: 16
Task: Check the health of the Threat Prevention blades.
Answer:
See the Explanation.Explanation:
1- SSH into the Gateway.
2- Run: cpview > Threat Prevention section.
3- Check CPU, memory, and update status.
4- Look for blade-specific errors or crashes.
5- Use cpstat threat-prevention for CLI summary.

NEW QUESTION: 17
Task: Enable "Update Automatically" for IPS database.
Answer:
See the Explanation.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.

NEW QUESTION: 18
Task: Verify if a specific IPS protection is active.
Answer:
See the Explanation.Explanation:
1- Go to Threat Tools > IPS Protections.
2- Use the filter to search by name or CVE ID.
3- Confirm status is "Active" and assigned to profile.
4- Double-click to view scope and affected profiles.
5- Confirm via SmartConsole logs if it triggered recently.

NEW QUESTION: 19

Task: Check if Anti-Bot is blocking known Command and Control (C&C) traffic.

Answer:

See the Explanation.Explanation:

1- Simulate traffic to a test C&C domain (in a safe lab).

2- Monitor logs with: blade:"Anti-Bot" and action:"Prevented".

3- Confirm the threat name and DNS/IP contacted.

4- Check confidence level = High.

5- Ensure profile is set to "Prevent" for high-confidence threats.

NEW QUESTION: 20

Task: Simulate a file download test and confirm Anti-Virus prevention using the custom profile.

Answer:

See the Explanation.Explanation:

1- Use EICAR test file in a browser.

2- Confirm file is blocked and logs show blade:"Anti-Virus" and action:"Prevented".

3- Confirm the active profile name matches your custom profile.

4- Check logs for file hash and signature info.

5- Document success as part of validation.

NEW QUESTION: 21

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

Answer:

See the Explanation.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.

NEW QUESTION: 22

Task: Create a custom Threat Prevention profile named Corporate_TP_Strict in SmartConsole.

Answer:

See the Explanation.Explanation:

1- Go to Threat Prevention > Profiles.

2- Click "New Profile", name it Corporate_TP_Strict.

3- In the base profile, select Optimized as a starting point.

4- Enable IPS, Anti-Bot, Anti-Virus, Threat Emulation, and Threat Extraction.

5- Save the profile for later assignment to a policy rule.

NEW QUESTION: 23
Task: Validate policy enforcement of a specific IPS profile.
Answer:
See the Explanation.Explanation:
1- Trigger test traffic that matches a rule using the profile.
2- SmartConsole > Logs > Filter by Profile name.
3- Confirm protections are applied with expected action.
4- Use fw stat on gateway to view loaded policy.
5- Ensure profile assignment is correct in the policy rule.

NEW QUESTION: 24
Task: View and interpret Threat Prevention event in SmartEvent.
Answer:
See the Explanation.Explanation:
1- Open SmartEvent > Events tab.
2- Filter by Category: Threat Prevention.
3- Open a specific event to see attack vector, target IP, and action.
4- Click "Show Packet Data" to analyze payload.
5- Cross-reference with IPS protections.

NEW QUESTION: 25
Task: Configure automatic IPS updates via SmartConsole.
Answer:
See the Explanation.Explanation:
1- Open SmartConsole > Threat Prevention > Updates.
2- Enable "Check for updates automatically."
3- Set schedule (e.g., daily at 2:00 AM).
4- Enable "Install updates automatically" for production or testing only.
5- Click OK and publish changes.

NEW QUESTION: 26
Task: Revert a mistakenly modified IPS protection to its default state.
Answer:
See the Explanation.Explanation:
1- Go to IPS Protections > Locate modified entry.
2- Click "Revert to Check Point default."
3- Confirm action and apply changes.
4- Publish and install policy.
5- Log actions confirm protection now behaves as default.

NEW QUESTION: 27

Task: Exclude traffic to internal update servers from Anti-Virus scanning.

Answer:

See the Explanation.Explanation:

1- Open Threat Prevention Policy.

2- Add a rule: Source = Internal Gateway, Destination = AV Server.

3- Assign a profile with AV blade disabled.

4- Set Track = Log and Action = Accept.

5- Place rule before general AV rule, publish, and install.

NEW QUESTION: 28

Task: Tune a Threat Prevention profile by converting medium-confidence threats from Detect to Prevent.

Answer:

See the Explanation.Explanation:

1- Open the profile in SmartConsole.

2- Under each blade (AV, AB, IPS), change Medium confidence action from "Detect" to "Prevent."

3- Save, publish, and install the policy.

4- Monitor post-deployment logs for increased blocks.

5- Revert individual settings if false positives increase.

NEW QUESTION: 29

Task: Create a Threat Prevention profile exclusively for outbound traffic.

Answer:

See the Explanation.Explanation:

1- Clone the "Optimized" profile > name it Outbound_Profile.

2- Disable Threat Emulation and Extraction.

3- Enable IPS, Anti-Bot, Anti-Virus.

4- Apply only to Internet-bound rules.

5- Use action: Prevent for known C&C and malware traffic.

NEW QUESTION: 30

Task: Troubleshoot policy installation failure.

Answer:

See the Explanation.Explanation:

1- In SmartConsole, attempt policy install again and note error.

2- View install_policy.elg in $FWDIR/log/.

3- Verify SIC is active.

4- Ensure policy contains no rulebase errors.

5- Re-push after resolving syntax or connectivity issues.

NEW QUESTION: 31
Task: Enable logging of blocked malware downloads in the profile.
Answer:
See the Explanation.Explanation:
1- Edit the custom profile > Anti-Virus tab.
2- Ensure action for medium/high confidence is set to Prevent.
3- Enable Track = Log.
4- Save and push policy.
5- Review logs by filtering blade:"Anti-Virus" and action:"Prevented".

NEW QUESTION: 32
Task: Assign the custom profile to a Threat Prevention policy rule.
Answer:
See the Explanation.Explanation:
1- Open Threat Prevention > Policy.
2- Add a new rule or edit an existing one.
3- In the Profile column, select Corporate_TP_Strict.
4- Set Track to Log and Action to Accept.
5- Publish and install the Threat Prevention policy.

NEW QUESTION: 33
Task: Enable automatic email alerts for critical IPS events.
Answer:
See the Explanation.Explanation:
1- Open SmartEvent or SmartConsole > Logs & Monitor.
2- Go to Automatic Reactions > New Reaction.
3- Set condition: blade=IPS AND severity=Critical.
4- Choose Action: Send Email > Configure recipient.
5- Save and test by generating a trigger.

NEW QUESTION: 34
Task: Add a comment in a Threat Prevention profile to indicate usage purpose.

Answer:

See the Explanation.Explanation:

1- Open the custom profile (e.g., Corporate_TP_Strict).

2- Add a note in the description field: e.g., "Used for internal office users."

3- Save changes.

4- Optionally add version info or change history.

5- Use this for future auditing and documentation.

NEW QUESTION: 35

Task: Apply different IPS profiles based on network zone using policy layers.

Answer:

See the Explanation.Explanation:

1- Create multiple Threat Prevention profiles per zone (DMZ, Internal, External).

2- In Threat Prevention Policy, add separate rules by source zone.

3- Apply respective profile in each rule.

4- Publish and install the policy.

5- Monitor logs to verify zone-specific detection.

NEW QUESTION: 36

Task: Create a custom Threat Prevention profile enabling only Anti-Bot and Anti-Virus protections.

Answer:

See the Explanation.Explanation:

1- Go to Threat Prevention > Profiles.

2- Click "New Profile," name it (e.g., "AV_AB_Only").

3- Enable "Anti-Bot" and "Anti-Virus"; disable IPS and TE.

4- Set Action to "Prevent" for high/medium confidence threats.

5- Save and apply this profile to your Threat Prevention rule.

NEW QUESTION: 37

Task: Validate Anti-Bot blade updates on the Gateway.

Answer:

See the Explanation.Explanation:

1- SSH into the Gateway.

2- Run: cpstat threat-emulation and cpstat anti-bot.

3- Check SmartConsole > Gateways > Updates tab.

4- Validate signature update timestamps.

5- Ensure outbound connectivity to Check Point update servers.

NEW QUESTION: 38

Task: Configure Anti-Bot in the Corporate_TP_Strict profile to prevent all high-confidence threats.

Answer:

See the Explanation.Explanation:

1- Edit the Corporate_TP_Strict profile.

2- Navigate to the Anti-Bot tab.

3- Set High Confidence to Prevent.

4- Set Medium Confidence to Detect or Prevent, depending on policy.

5- Save and publish changes.

NEW QUESTION: 39

Task: Configure inspection settings for mobile VPN users.

Answer:

See the Explanation.Explanation:

1- Go to Threat Prevention > Inspection Settings.

2- Add a new exception group for mobile user IP pool.

3- Set reduced inspection sensitivity for this group.

4- Save, publish, and test VPN user traffic.

5- Ensure logs still show critical threats being detected.

NEW QUESTION: 40

Task: Verify Anti-Virus scan mode is set to "Stream-Based" on the gateway.

Answer:

See the Explanation.Explanation:

1- In SmartConsole, go to Gateway > Threat Prevention tab.

2- Locate Anti-Virus scan mode settings.

3- Ensure "Stream-Based" is selected (not Hold-Mode).

4- If needed, change the scan mode and reinstall policy.

5- Verify with cpview under Threat Prevention section.

NEW QUESTION: 41

Task: Verify if Anti-Bot and Anti-Virus protections are active on a Security Gateway.

Answer:

See the Explanation.Explanation:

1- SSH into the gateway.

2- Run: cpstat antimalware and cpstat anti-bot.

3- Confirm both blades are "Active" and signatures are "Up-to-date."

4- Check with cpview > Threat Prevention section.

5- Use watch -n 5 cpstat antimalware to monitor real-time status.

NEW QUESTION: 42

Task: Validate the IPS update server connectivity from the gateway.

Answer:

See the Explanation.Explanation:

1- SSH into the gateway.

2- Use: curl -v https://updates.checkpoint.com

3- Confirm DNS resolves and certificate is valid.

4- Check proxy settings if blocked.

5- Verify SmartConsole > Gateways > Update section reflects success.

NEW QUESTION: 43

Task: Enable Threat Prevention debug mode for troubleshooting.

Answer:

See the Explanation.Explanation:

1- SSH into the Gateway.

2- Run: tecli debug on or pdp debug on.

3- Reproduce the issue.

4- View logs in $FWDIR/log/.

5- Disable debug mode: tecli debug off.

NEW QUESTION: 44

Task: Enable DNS reputation protection under Anti-Bot in a custom profile.

Answer:

See the Explanation.Explanation:

1- Edit your custom Threat Prevention profile.

2- Under the Anti-Bot section, enable DNS Reputation.

3- Set to Prevent on High Confidence queries.

4- Ensure "Inspect DNS traffic" is enabled.

5- Save and apply the profile.

NEW QUESTION: 45

Task: Enable Anti-Bot and Anti-Virus software blades on a Security Gateway.

Answer:

See the Explanation.Explanation:

1- Open SmartConsole > Gateways & Servers.

2- Double-click the relevant Security Gateway.

3- Under the "General Properties" tab, enable "Anti-Bot" and "Anti-Virus."

4- Click OK > Publish the changes.

5- Install the Access Control and Threat Prevention policy.

NEW QUESTION: 46

Task: Verify IPS protections are being enforced.

Answer:
See the Explanation.Explanation:
1- Open SmartConsole > Logs.
2- Filter: blade:"IPS" and action:"Prevented".
3- Confirm matching protections from the active profile.
4- View details: CVE, protocol, action, confidence level.
5- Export log details for auditing.

NEW QUESTION: 47
Task: Configure exceptions for Anti-Virus to ignore a known safe file hash.
Answer:
See the Explanation.Explanation:
1- Open SmartConsole > Threat Prevention > Protections.
2- Go to "Anti-Virus" protections.
3- Create a new exception using file hash under "Files & Hashes."
4- Set action to "Ignore" or "Detect."
5- Save, apply to profile, publish, and install policy.

Valid 156-590 Dumps shared by Actual4test.com for Helping Passing 156-590 Exam! Actual4test.com now offer the **newest 156-590 exam dumps**, the Actual4test.com 156-590 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 156-590 dumps with Test Engine here: https://www.actual4test.com/156-590_examcollection.html (**78** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)