

Intrusion Prevention System (IPS)

Expected Time: 45 Minutes

Introduction

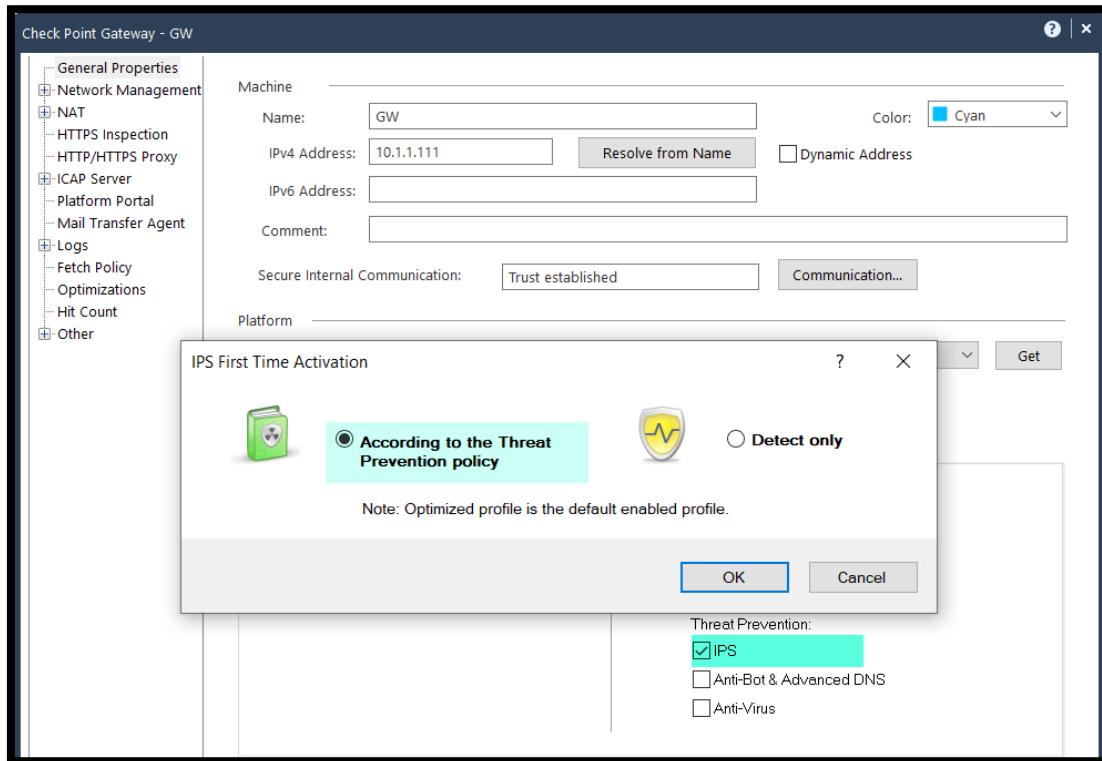
Intrusion Prevention Systems detect or prevent attempts to exploit weaknesses in vulnerable systems or applications, protecting you in the race to exploit the latest breaking threat.

Check Point IPS protections in our Next Generation Firewall are updated automatically. Whether the vulnerability was released years ago, or a few minutes ago, your organization is protected.

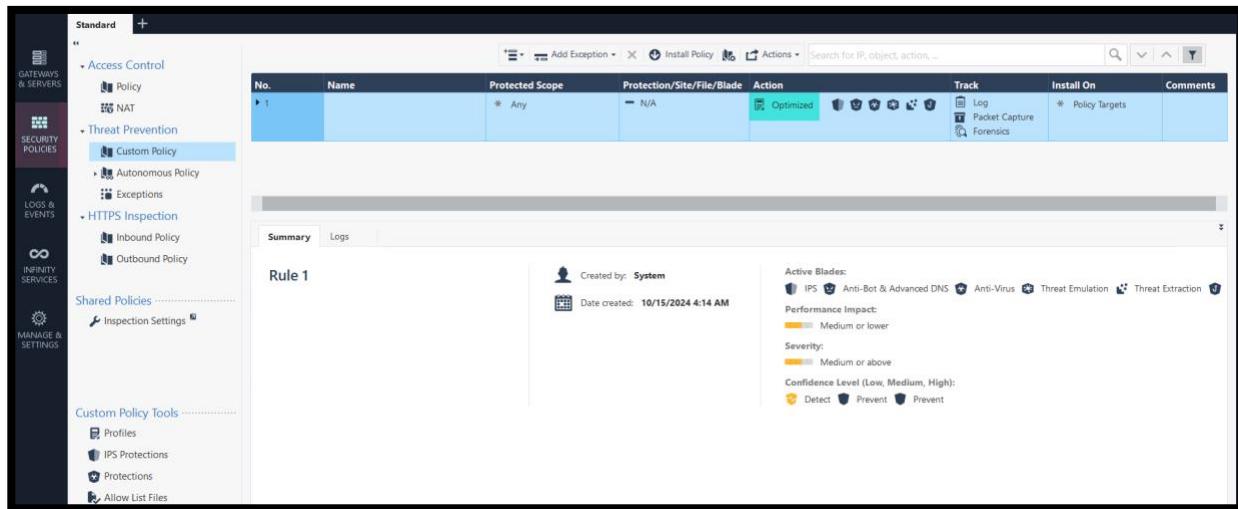
Exercise 1: Onboarding

The Check Point IPS blade can prevent exploitation attempts out of the box. In this exercise, we will activate the IPS blade and confirm its functionality.

1. Edit the **GW** object and enable the **IPS** blade According to the Threat Prevention Policy.

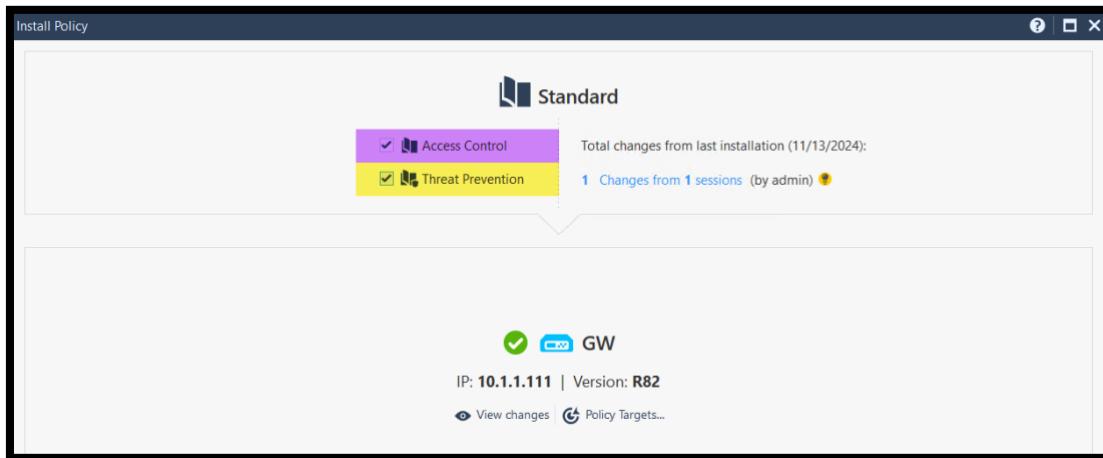


2. Under the Custom **Threat Prevention** Policy. Notice that the **Optimized** profile is assigned by default. It is optimized for good security while making sure the performance is not greatly affected.



No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track	Install On	Comments
1		* Any	N/A	Optimized	Log Packet Capture Forensics	* Policy Targets	

3. Install the **Access Control** and **Threat Prevention** Policy.

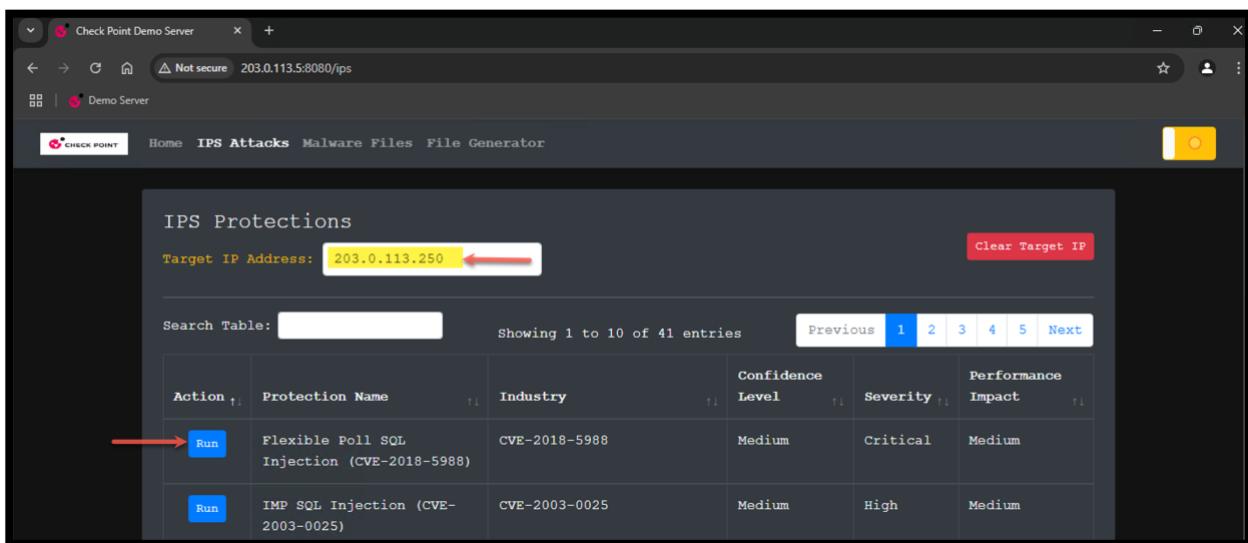


4. From **win_client**, Open the browser and browse to the Demo Server at <http://203.0.113.5:8080>

Notes:

- This server is installed on the Kali Linux machine.
- The target of those attacks will be set to the windows server machine at the public address 203.0.113.250. this address is translated o the GW to the real address 10.1.2.250.
- Attacks are based on HTTP calls.

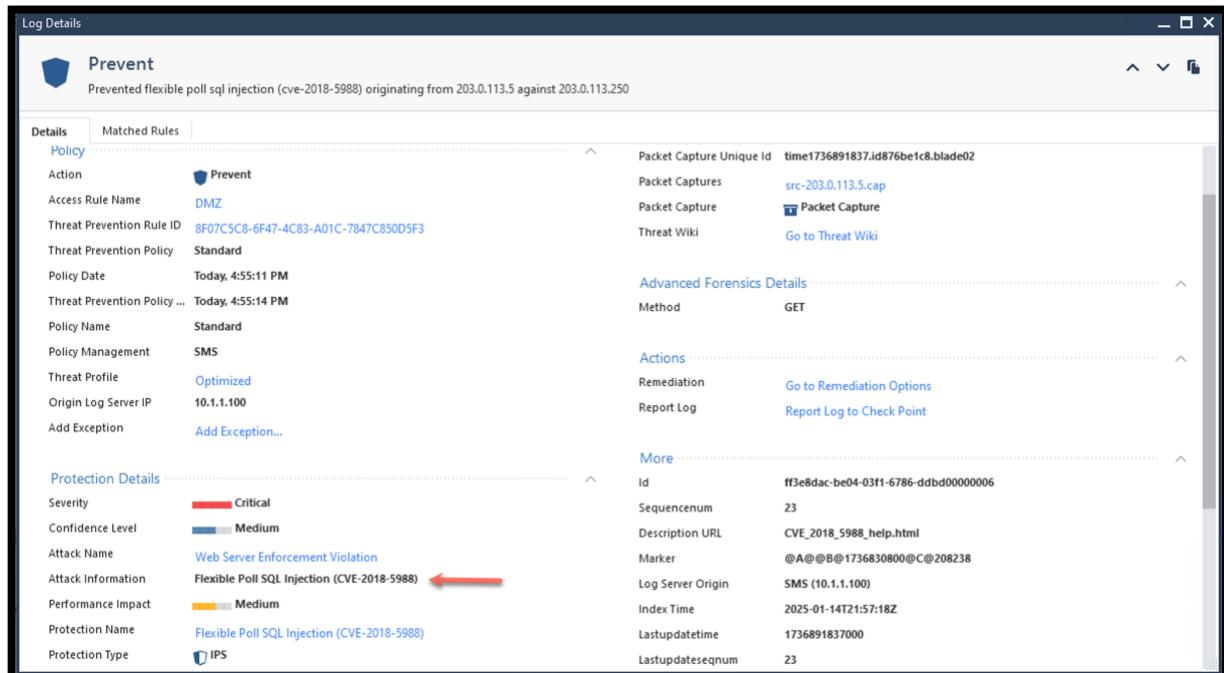
5. Click **Run** to trigger the first protection in the list.



The screenshot shows the 'IPS Protections' page in the Check Point SmartConsole. The target IP address is set to 203.0.113.250. The table lists two entries:

Action	Protection Name	Industry	Confidence Level	Severity	Performance Impact
Run	Flexible Poll SQL Injection (CVE-2018-5988)	CVE-2018-5988	Medium	Critical	Medium
Run	IMP SQL Injection (CVE-2003-0025)	CVE-2003-0025	Medium	High	Medium

6. Filter the logs in SmartConsole to show logs from **IPS** only. Notice that the attack we triggered generated a log and the **Packet Capture** is attached to the log.



The screenshot shows the 'Log Details' page for a prevented attack. The attack information is:

Attack Information: Flexible Poll SQL Injection (CVE-2018-5988) ←

The 'Details' tab shows the following details:

- Action: Prevent
- Access Rule Name: DMZ
- Threat Prevention Rule ID: BF07C5C8-6F47-4C83-A01C-7847C850D5F3
- Threat Prevention Policy: Standard
- Policy Date: Today, 4:55:11 PM
- Threat Prevention Policy ...: Today, 4:55:14 PM
- Policy Name: Standard
- Policy Management: SMS
- Threat Profile: Optimized
- Origin Log Server IP: 10.1.1.100
- Add Exception: Add Exception...

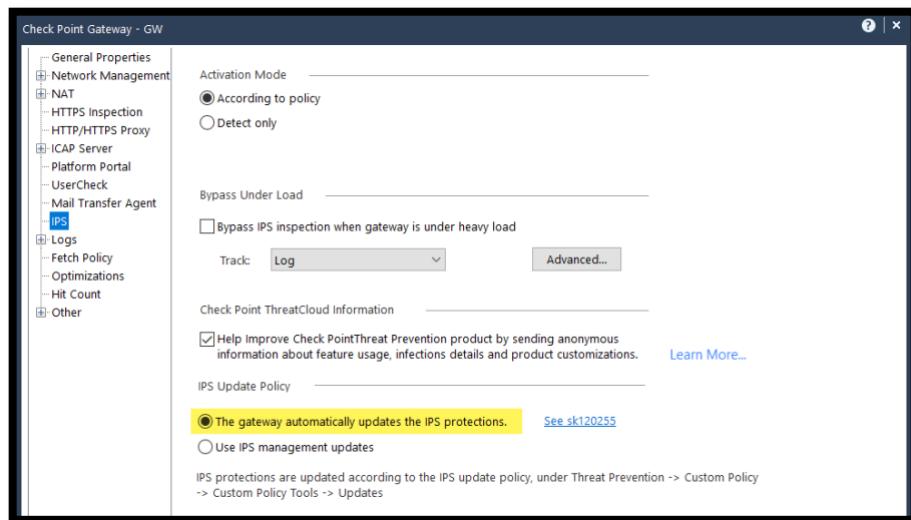
The 'Protection Details' section shows:

- Severity: Critical
- Confidence Level: Medium
- Attack Name: Web Server Enforcement Violation
- Attack Information: Flexible Poll SQL Injection (CVE-2018-5988) ←
- Performance Impact: Medium
- Protection Name: Flexible Poll SQL Injection (CVE-2018-5988)
- Protection Type: IPS

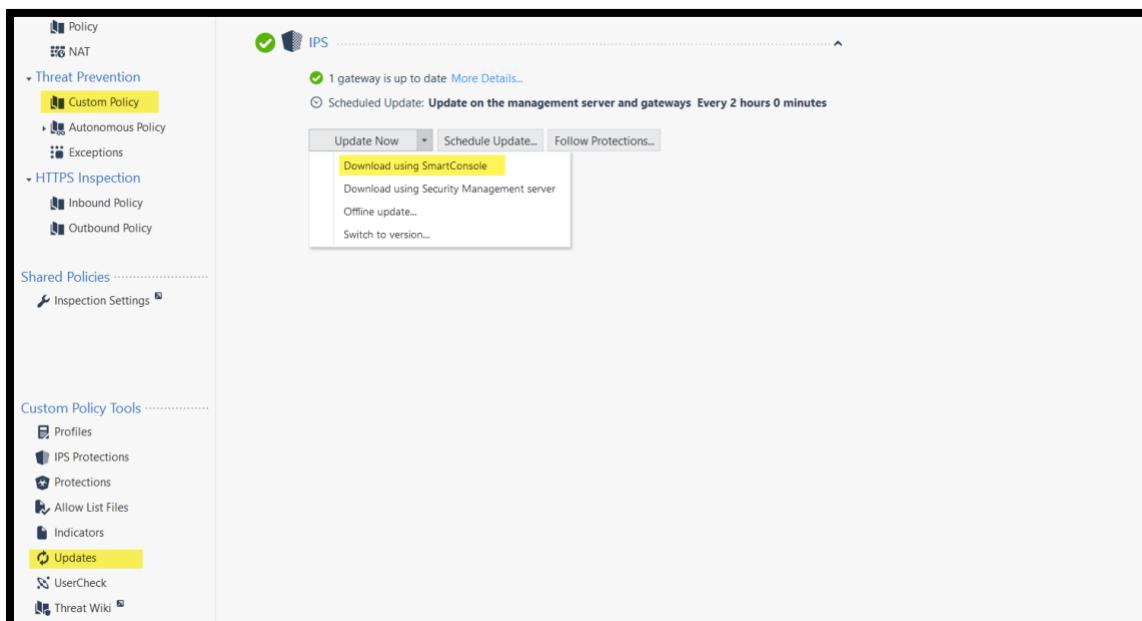
Exercise 2: Updates

It is essential to keep the IPS engine up to date with the latest protections and signatures. This exercise will review the main update features and procedures.

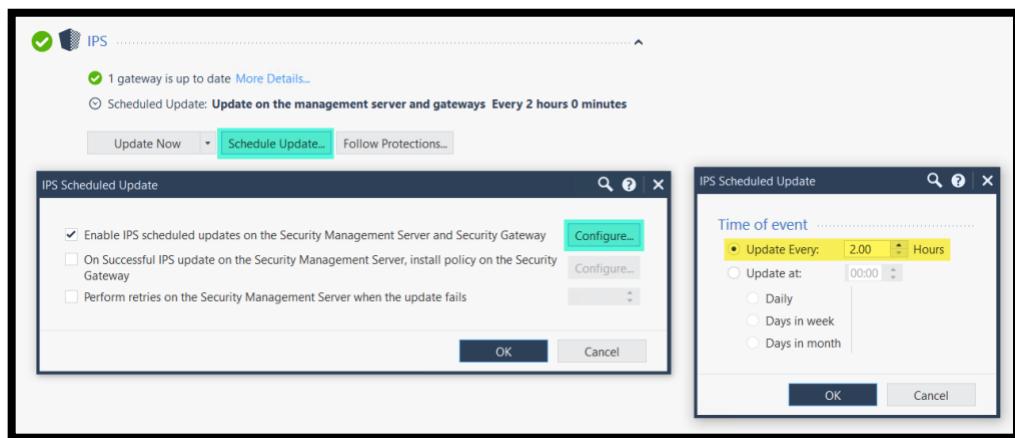
1. Open the **GW** object and review the **IPS Update Policy** settings for the GW. Notice that by default, the GW will try to update the IPS protections automatically. Read [SK120225](#) for more details.



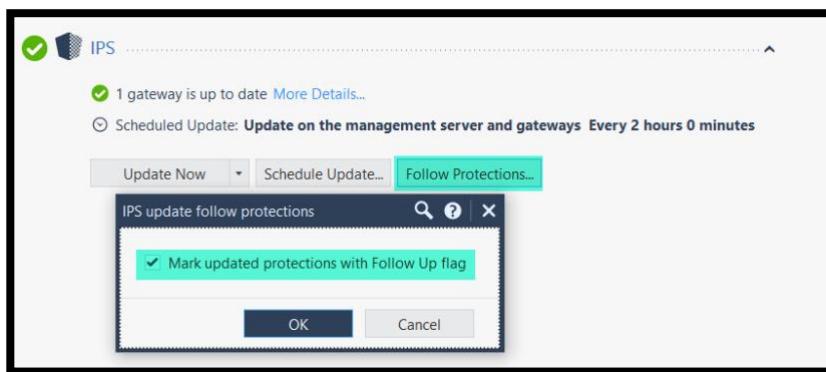
2. While in the Custom Threat Prevention Policy View, click updates and review the available methods to update IPS. Update using SmartConsole.



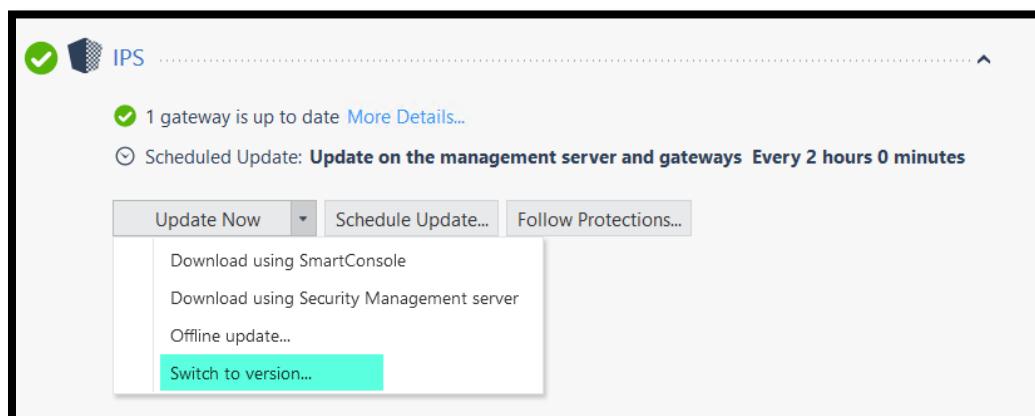
3. Review the scheduled updates. By default, the security management and security gateways check for updated every 2 hours.



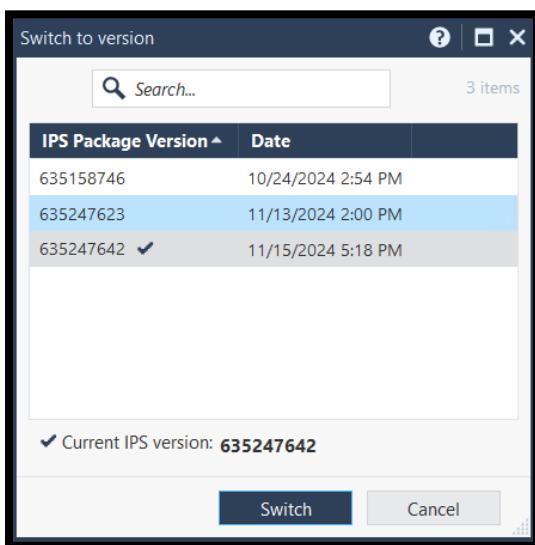
4. To be able to tell which protection were updated, they are marked by default. Review the settings under “Follow Protections”.



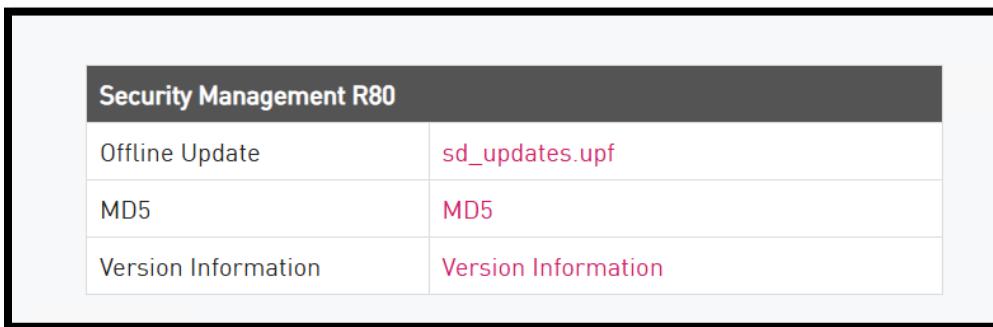
5. In case you updated IPS and for any reason you would like to revert to one of the older versions, navigate to the list of updated under: **Update Now -> Switch to version**



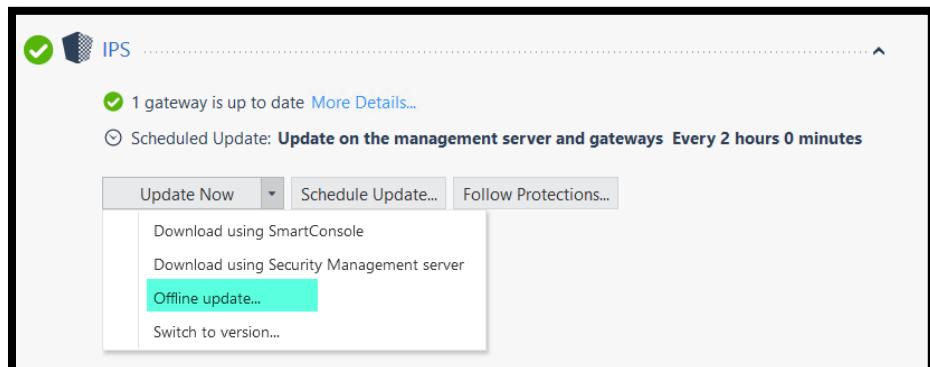
6. From the list of versions, select the version to revert to and click Switch.



7. In case this is an isolated environment, we can download the IPS update via
<https://advisories.checkpoint.com/ips-offline-updates/>



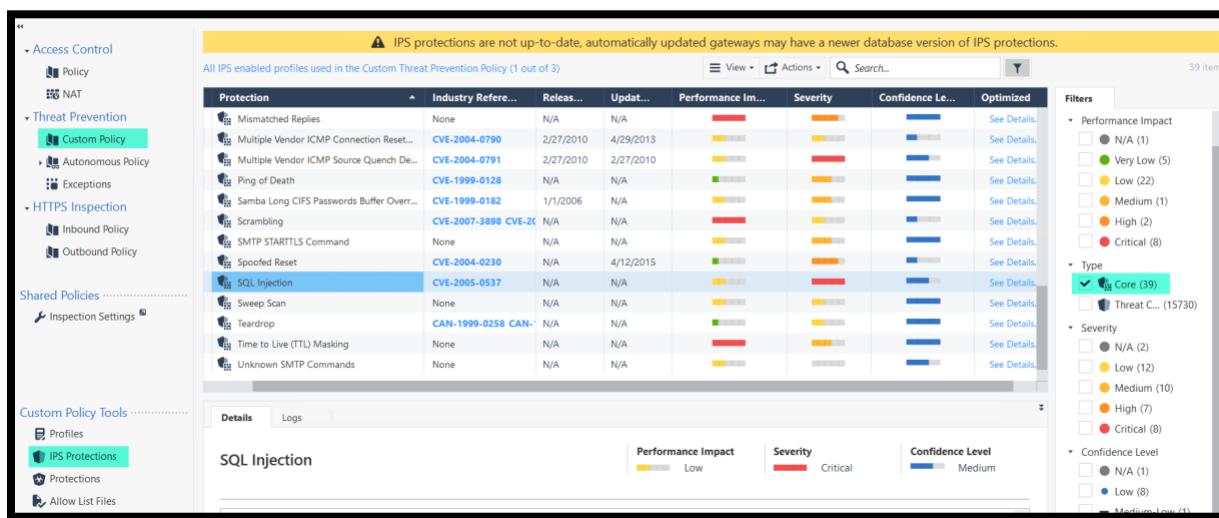
8. When Offline Updates is selected from the drop-down menu, you will be asked to point to the update file location.



Exercise 3: Core Protections

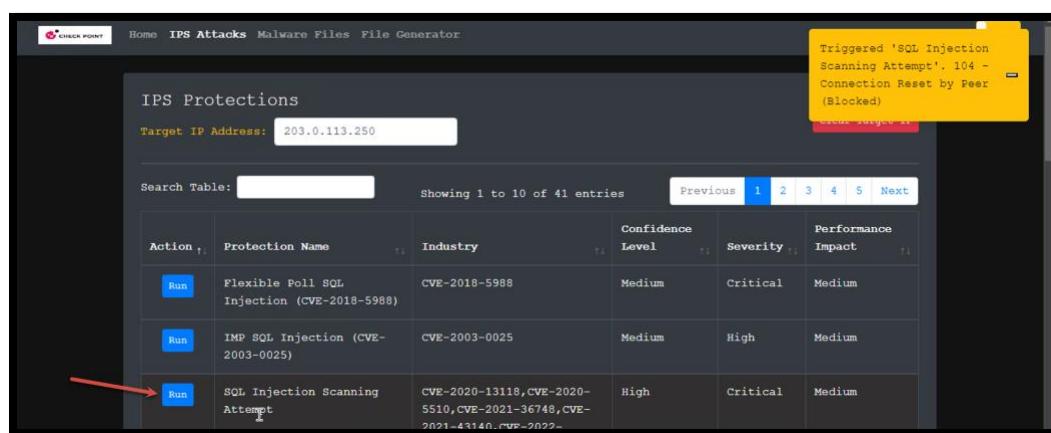
Core Protections are a set of protections that are installed via the Access policy, non-updatable and are managed separately from the **Threat Cloud Protections**. In this exercise, we will learn how to handle the Core Protections.

1. Open the **IPS Protections** tab and filter the protections to show **Core** protections only. Notice that the icon for the core protections differ from the **Threat Cloud** protections.



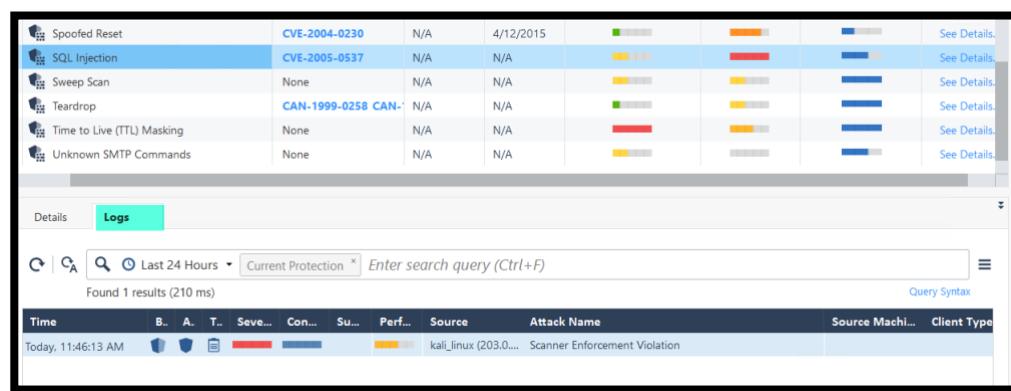
The screenshot shows the Check Point Management Console interface. On the left, there's a navigation sidebar with sections like 'Access Control', 'Policy', 'NAT', 'Threat Prevention' (with 'Custom Policy' selected), 'Autonomous Policy', 'Exceptions', 'HTTPS Inspection', 'Inbound Policy', and 'Outbound Policy'. Below that is 'Shared Policies' and 'Inspection Settings'. On the right, the main area displays a table titled 'IPS protections are not up-to-date, automatically updated gateways may have a newer database version of IPS protections.' It lists various protection entries with columns for 'Protection', 'Industry Reference', 'Release Date', 'Update Date', 'Performance Impact', 'Severity', 'Confidence Level', and 'Optimized'. A specific row for 'SQL Injection' (CVE-2005-0537) is highlighted in blue. At the bottom, there's a 'Logs' tab and a legend for 'Performance Impact' (Low, Medium, High, Critical) and 'Confidence Level' (Medium, Low). On the far right, there are 'Filters' for 'Type' (Core selected), 'Performance Impact' (N/A, Very Low, Low, Medium, High, Critical), 'Severity' (N/A, Low, Medium, High, Critical), and 'Confidence Level' (N/A, Low, Medium).

2. From the Demo Server, trigger one of the SQL attacks. For example, trigger the protection SQL Injection scanning attempt.



The screenshot shows the 'IPS Attacks' tab. At the top, it says 'Triggered 'SQL Injection scanning Attempt''. Below that, it shows 'Target IP Address: 203.0.113.250'. The main area is titled 'IPS Protections' and shows a table with columns: Action, Protection Name, Industry, Confidence Level, Severity, and Performance Impact. There are three rows: 'Flexible Poll SQL Injection (CVE-2018-5988)', 'IMP SQL Injection (CVE-2003-0025)', and 'SQL Injection Scanning Attempt'. The last row has a red arrow pointing to its 'Run' button. A yellow callout box at the top right says 'Triggered 'SQL Injection scanning Attempt''. 104 - Connection Reset by Peer (Blocked)'.

3. Look for the SQL protection in the Core protections list and select the log tab to see logs related to this protection.



The screenshot shows a security dashboard with a table of detected attacks and a detailed log entry.

Attacks Table:

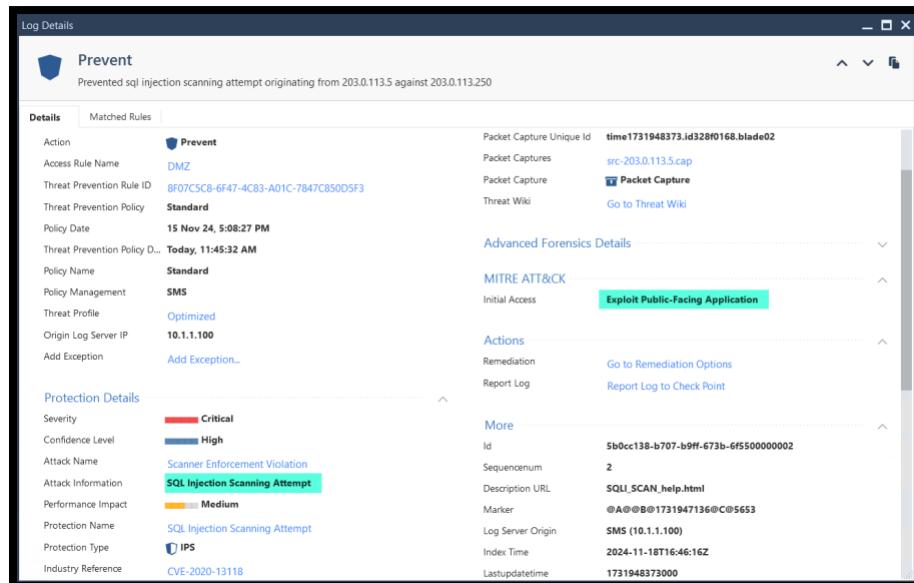
Attack Type	CVE ID	Status	Last Seen	Actions
Spoofed Reset	CVE-2004-0230	N/A	4/12/2015	[See Details]
SQL Injection	CVE-2005-0537	N/A	N/A	[See Details]
Sweep Scan	None	N/A	N/A	[See Details]
Teardrop	CAN-1999-0258 CAN-	N/A	N/A	[See Details]
Time to Live (TTL) Masking	None	N/A	N/A	[See Details]
Unknown SMTP Commands	None	N/A	N/A	[See Details]

Log Entry:

Logs tab selected. Last 24 Hours search results (210 ms).

Time	B..	A..	T..	Sev..	Con..	Perf..	Source	Attack Name	Source Machi...	Client Type
Today, 11:46:13 AM	██████████	██████████	██████████	██████████	██████████	██████████	kali_linux (203.0....)	Scanner Enforcement Violation		

4. Review the log and the field of each section.



The screenshot shows a detailed log entry for a SQL injection attempt.

Prevent: Prevented sql injection scanning attempt originating from 203.0.113.5 against 203.0.113.250

Details:

- Action: Prevent
- Access Rule Name: DMZ
- Threat Prevention Rule ID: BF07C5CB-6F47-4C83-A01C-7847C850D5F3
- Threat Prevention Policy: Standard
- Policy Date: 15 Nov 24, 5:08:27 PM
- Threat Prevention Policy D.: Today, 11:45:32 AM
- Policy Name: Standard
- Policy Management: SMS
- Threat Profile: Optimized
- Origin Log Server IP: 10.1.1.100
- Add Exception: Add Exception...

Protection Details:

- Severity: Critical
- Confidence Level: High
- Attack Name: Scanner Enforcement Violation
- Attack Information: SQL Injection Scanning Attempt
- Performance Impact: Medium
- Protection Name: SQL Injection Scanning Attempt
- Protection Type: IPS
- Industry Reference: CVE-2020-13118

Advanced Forensics Details:

- Packet Capture Unique Id: time1731948373.id3280168.blade02
- Packet Captures: src-203.0.113.5.cap
- Packet Capture: Packet Capture
- Threat Wiki: Go to Threat Wiki

MITRE ATT&CK:

- Initial Access: Exploit Public-Facing Application

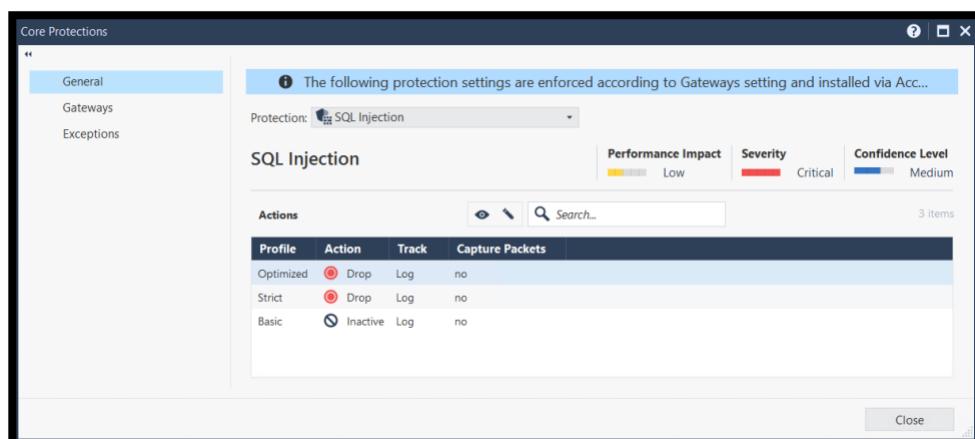
Actions:

- Remediation: Go to Remediation Options
- Report Log: Report Log to Check Point

More:

- Id: 5b0cc138-b707-b9ff-673b-6f5500000002
- Sequencenum: 2
- Description URL: SQL_SCAN_help.html
- Marker: @A@B@1731947136@C@5653
- Log Server Origin: SMS (10.1.1.100)
- Index Time: 2024-11-18T16:46:16Z
- LastupdateTime: 1731948373000

5. Open the SQL Protection and review the default action per profile. Notice that the SQL Injection Core Protection is disabled by default in the Basic profile.



The screenshot shows the Core Protections interface for SQL Injection.

Core Protections: General selected.

Protection: SQL Injection

SQL Injection:

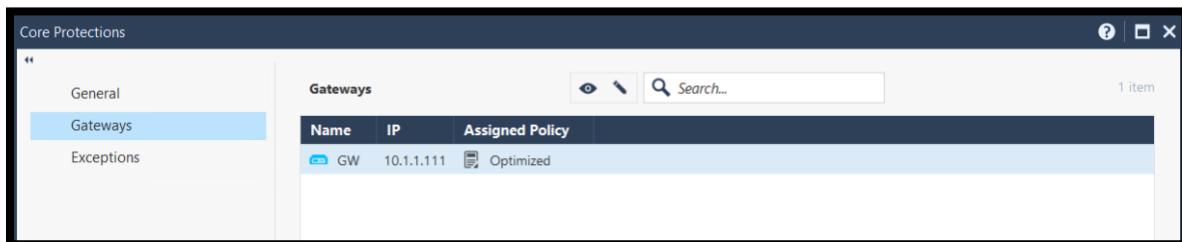
Performance Impact: Low (Yellow), Severity: Critical (Red), Confidence Level: Medium (Blue).

Actions:

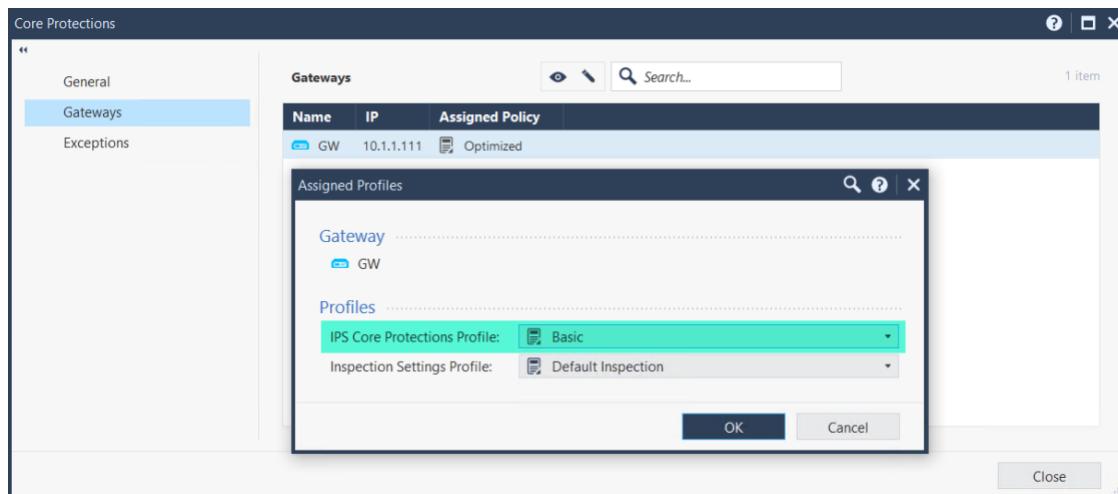
Profile	Action	Track	Capture Packets
Optimized	Drop	Log	no
Strict	Drop	Log	no
Basic	Inactive	Log	no

3 items.

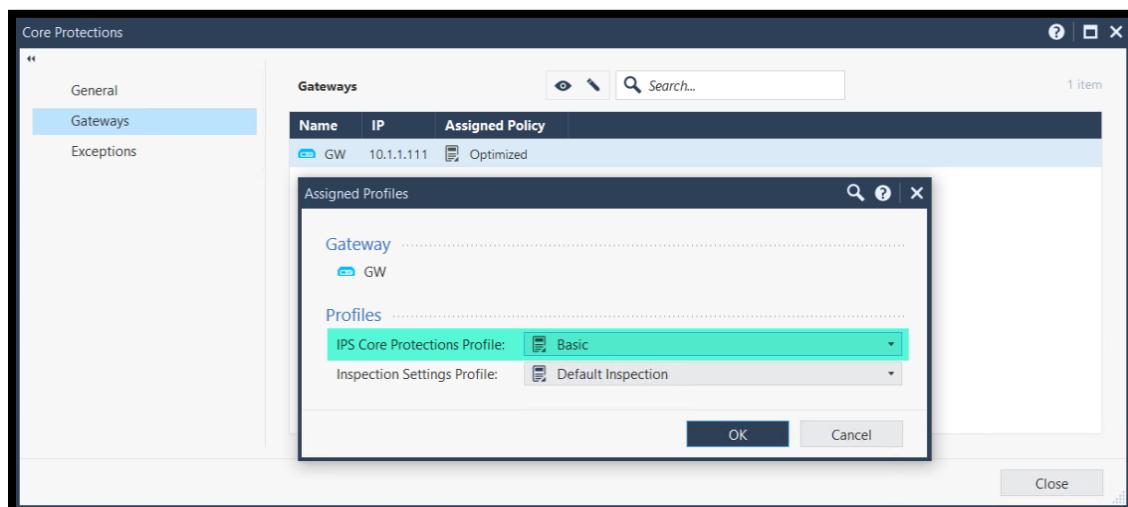
6. Move to the Gateways tab and review the default profile settings. Notice that this profile assignment is independent of the profile assigned in the rule base.



7. Edit the selection and select the Basic profile



8. Edit the profile selection and select the Basic Profile.



9. Install the Access Policy. Remember that Core protections are enforced using the Access Policy and do not require Threat Prevention Policy Install.



10. Try to trigger the same protection we used before in the demo Server (SQL Scanning attempt)

IPS Protections					
Target IP Address: 203.0.113.250					
Search Table: sql injection scan Showing 1 to 1 of 1 entries (filtered from 41 total entries) Previous 1 Next					
Action	Protection Name	Industry	Confidence Level	Severity	Performance Impact
Run	SQL Injection Scanning Attempt	CVE-2020-13118, CVE-2020-5510, CVE-2021-36748, CVE-2021-43140, CVE-2022-24219, CVE-2022-24220, CVE-2022-24221, CVE-2022-	High	Critical	Medium

11. Review the logs and notice that no new protection logs were generated as expected.

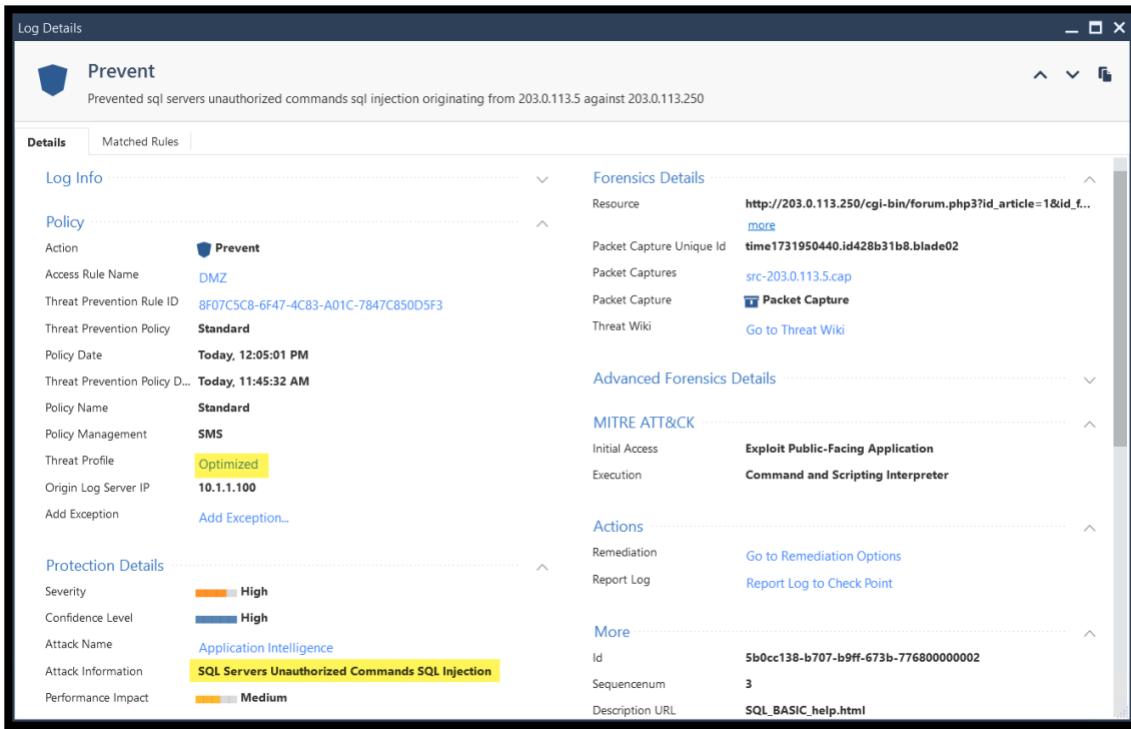
- There will be no new logs since this protection is disabled in the Basic profile which we assigned to the GW.
- Pay extra attention to deactivating protections as it will leave gaps in your security protection.

12. Run a different attack, this time trigger the protection **SQL Servers Unauthorized Commands SQL Injection**.

Action	Protection Name	Industry	Confidence Level	Severity	Performance Impact
Run	SQL Servers Unauthorized Commands SQL Injection	CVE-2014-3704, CVE-2019-13978, CVE-2019-9053, CVE-2021-41843, CVE-2022-0592, CVE-2022-0781, CVE-2022-0836, CVE-2022-1905, CVE-2022-26887, CVE-2022-28346, CVE-2022-30809, CVE-2022-30810, CVE-2022-30815, CVE-2024-33559	High	High	Medium

13. Review the relevant logs. Notice that a different protection was triggered. However, this protection is a different SQL injection provided by Threat Cloud.

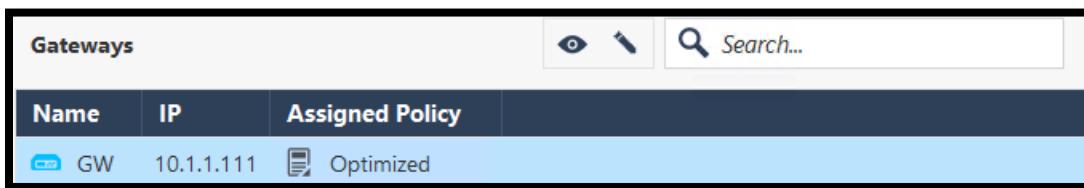
- Check Point provide multiple protections that work in parallel to protect your environment.
- Notice that this protection is managed via the Optimized profile assigned in the rule base and not the Basic profile we assigned to core protections.



The screenshot shows the 'Log Details' window with a 'Prevent' action taken against an SQL injection attempt. Key details include:

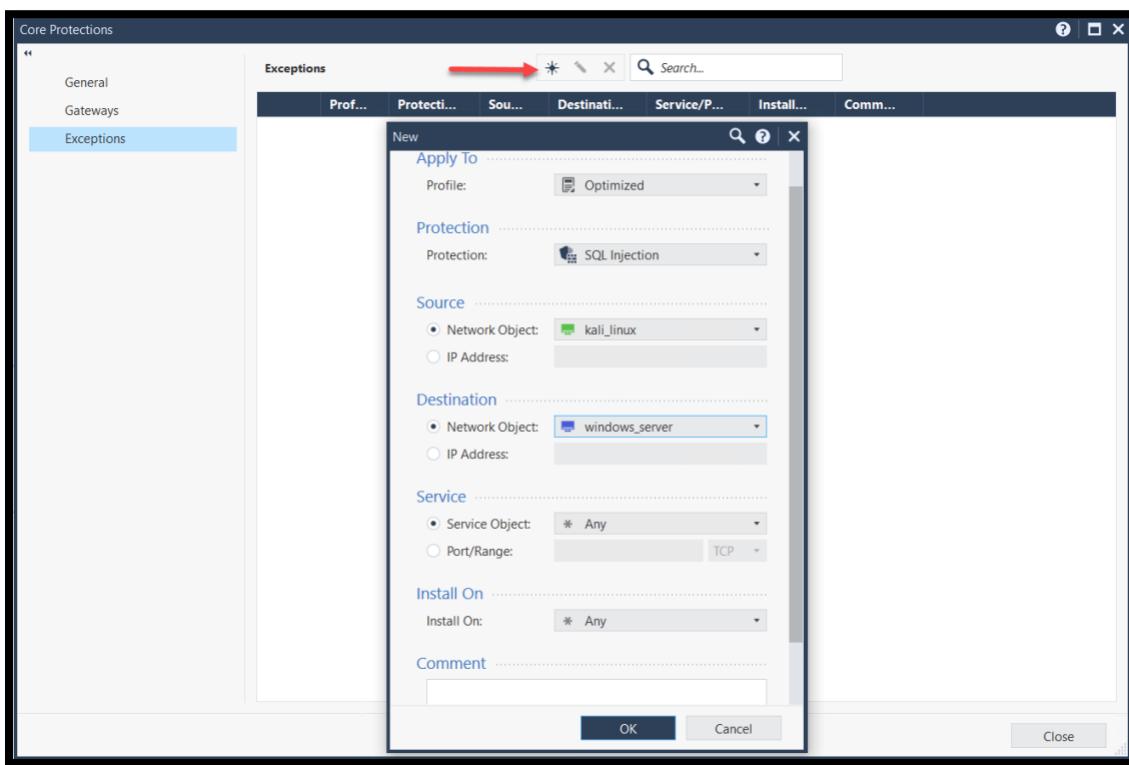
- Prevent**: Action taken.
- Prevented sql servers unauthorized commands sql injection originating from 203.0.113.5 against 203.0.113.250**: Description of the event.
- Details** tab selected.
- Log Info** section shows the event occurred **Today, 12:05:01 PM**.
- Policy** section shows the policy was **Standard** and the threat prevention rule ID was **8F07C5C8-6F47-4C83-A01C-7847C8500DF3**.
- Forensics Details** section includes a **Resource** URL (http://203.0.113.250/cgi-bin/forum.php3?id_article=1&id_f...) and a **Packet Capture Unique Id** ([time1731950440.id428b31b8.blade02](#)).
- Actions** section includes links to [Go to Remediation Options](#) and [Report Log to Check Point](#).
- More** section shows the **Id** is **5b0cc138-b707-b9ff-673b-776800000002**.

14. Edit the SQL protection settings and assign the **Optimized Profile**.

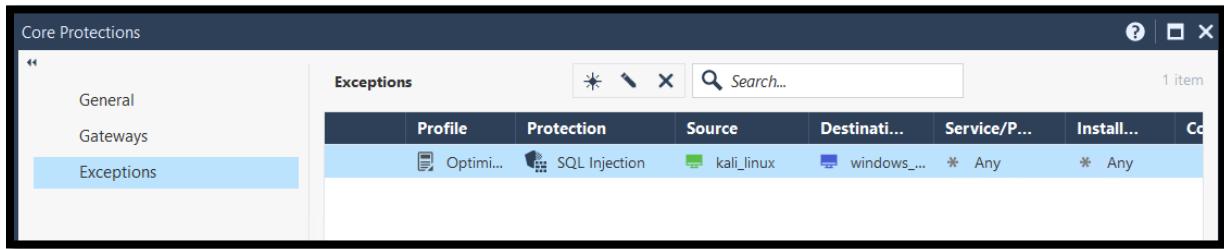


Name	IP	Assigned Policy
GW	10.1.1.111	Optimized

15. Under the **Exceptions** tab, add a new exception to override the default behaviour.



16. Review the list of exceptions and install the Access Policy



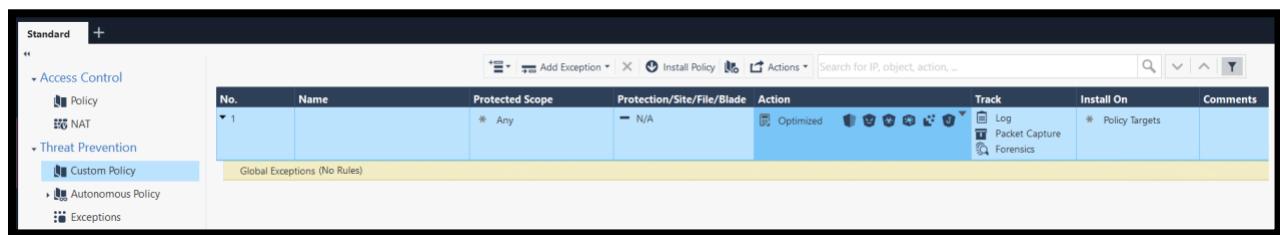
17. Run a new test using the same protection trigger from the demo server.

- Notice that the protection is no longer triggered since we added an exception.
- Making exception is a preferred method in most cases. Add an exception specific to a host or network.
- Like the behavior above, other protection might still drop the traffic as this is a multi-layer protection layer environment.

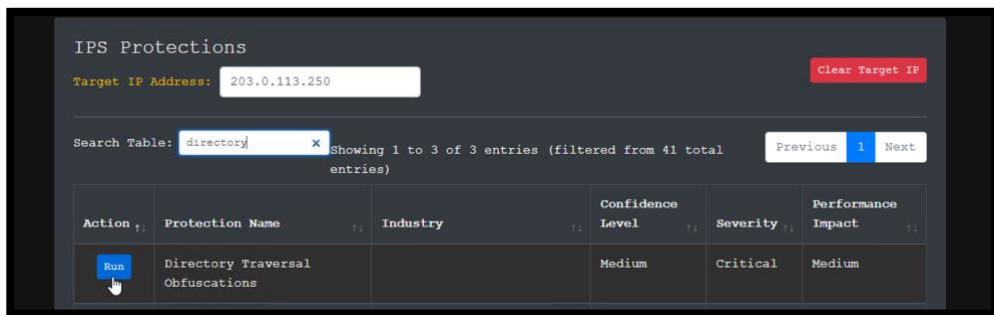
Exercise 4: Threat Cloud Protections

Threat Cloud Protections are updated regularly by the Check Point research team. Those protections are dynamic with new protections added regularly.

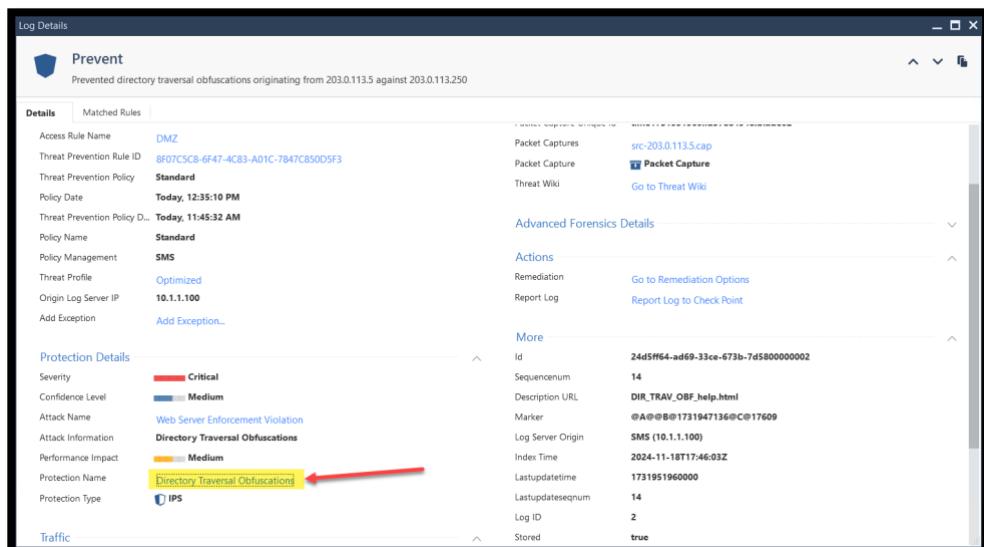
- Review the default rule In the Threat Prevention Custom policy. Notice that the optimized profile is assigned by default.



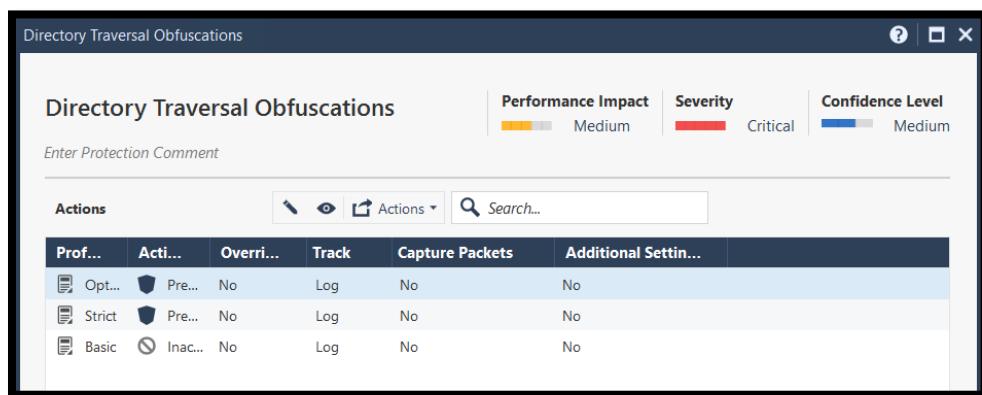
- From the demo server, trigger the protection **Directory Traversal Obfuscation**



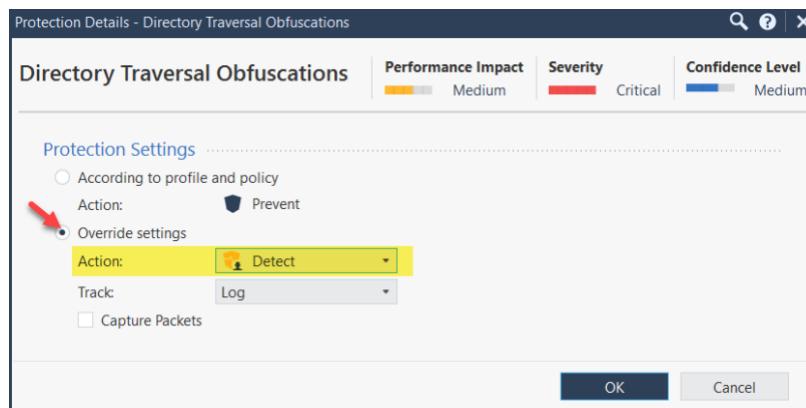
- Review the log and pay attention to the profile.



15. Click on the highlighted protection name link. This will open the corresponding protection window. Notice that this protection is set to prevent mode by default for the Strict and Optimized profiles.



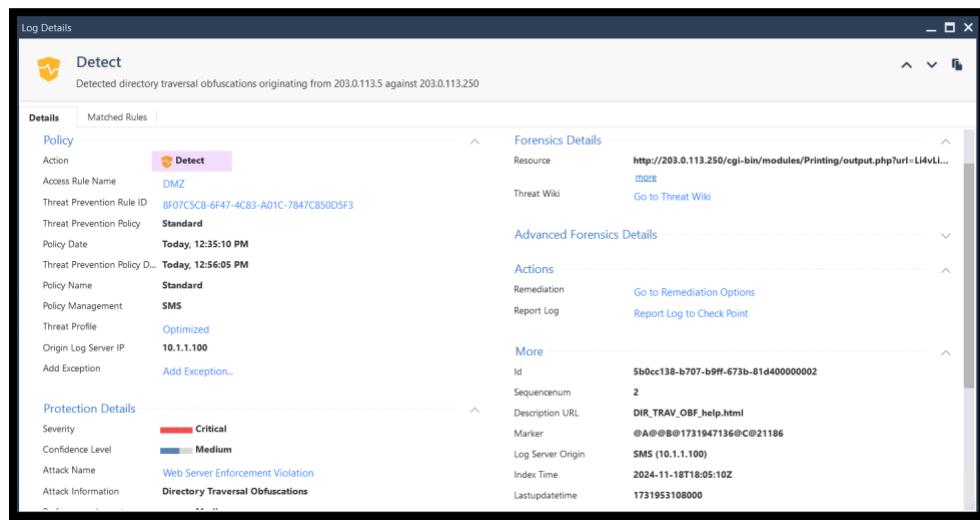
16. While Optimized is selected, edit the settings and change the behavior to detect instead of Prevent.



17. Confirm the changes and Install the Threat Prevention Policy.

Profile	Action	Override	Track	Capture Packets	Additional Settings
Optimized	Det...	Yes	Log	No	No
Strict	Pre...	No	Log	No	No
Basic	Inac...	No	Log	No	No

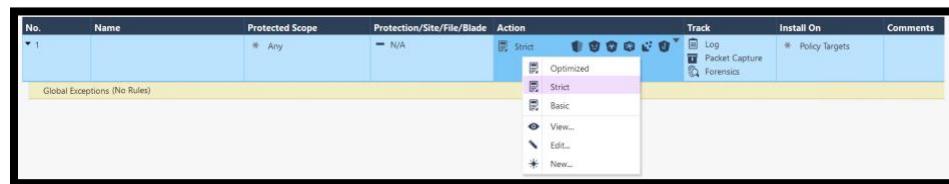
18. Trigger the same protection again and review the logs. You should see a detect log. Note that this is only made for the optimized profile. However, this applies to all hosts and networks.



The screenshot shows the 'Log Details' window for a 'Detect' event. The event details are as follows:

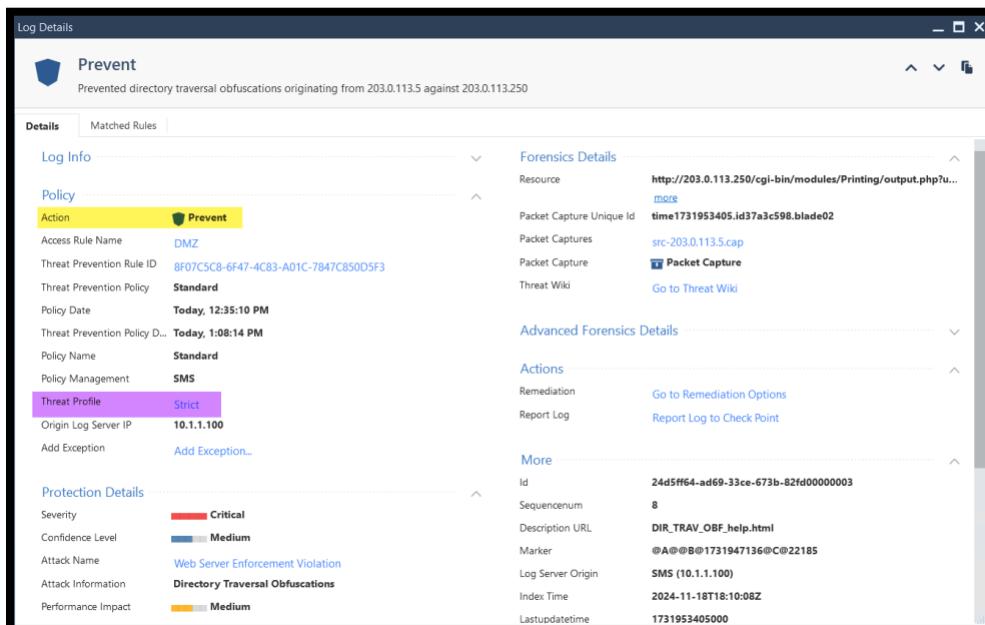
- Action:** Detect
- Resource:** http://203.0.113.250/cgi-bin/modules/Printing/output.php?url=Lj4vL...
- Threat Wiki:** Go to Threat Wiki
- Policy:** Standard
- Policy Date:** Today, 12:35:10 PM
- Threat Prevention Policy Date:** Today, 12:56:05 PM
- Policy Name:** Standard
- Policy Management:** SMS
- Threat Profile:** Optimized
- Origin Log Server IP:** 10.1.1.100
- Add Exception:** Add Exception...
- Protection Details:**
 - Severity:** Critical
 - Confidence Level:** Medium
 - Attack Name:** Web Server Enforcement Violation
 - Attack Information:** Directory Traversal Obfuscations
- Forensics Details:**
 - Resource:** http://203.0.113.250/cgi-bin/modules/Printing/output.php?url=Lj4vL...
 - Threat Wiki:** Go to Threat Wiki
- Advanced Forensics Details:**
 - Actions:**
 - Remediation: Go to Remediation Options
 - Report Log: Report Log to Check Point
- More:**
 - Id:** 5b0cc138-b707-b9ff-673b-81d400000002
 - Sequencenum:** 2
 - Description URL:** DIR_TRAV_OBF_help.html
 - Marker:** @A@B@1731947136@C@21186
 - Log Server Origin:** SMS (10.1.1.100)
 - Index Time:** 2024-11-18T18:05:10Z
 - Lastupdatedtime:** 1731953108000

19. Change the profile assigned to the default rule, select the Strict profile and install the Threat Prevention Policy.



The screenshot shows the 'Action' dropdown menu for a rule. The 'Strict' option is highlighted. Other options visible include Optimized, Basic, View..., Edit..., and New... .

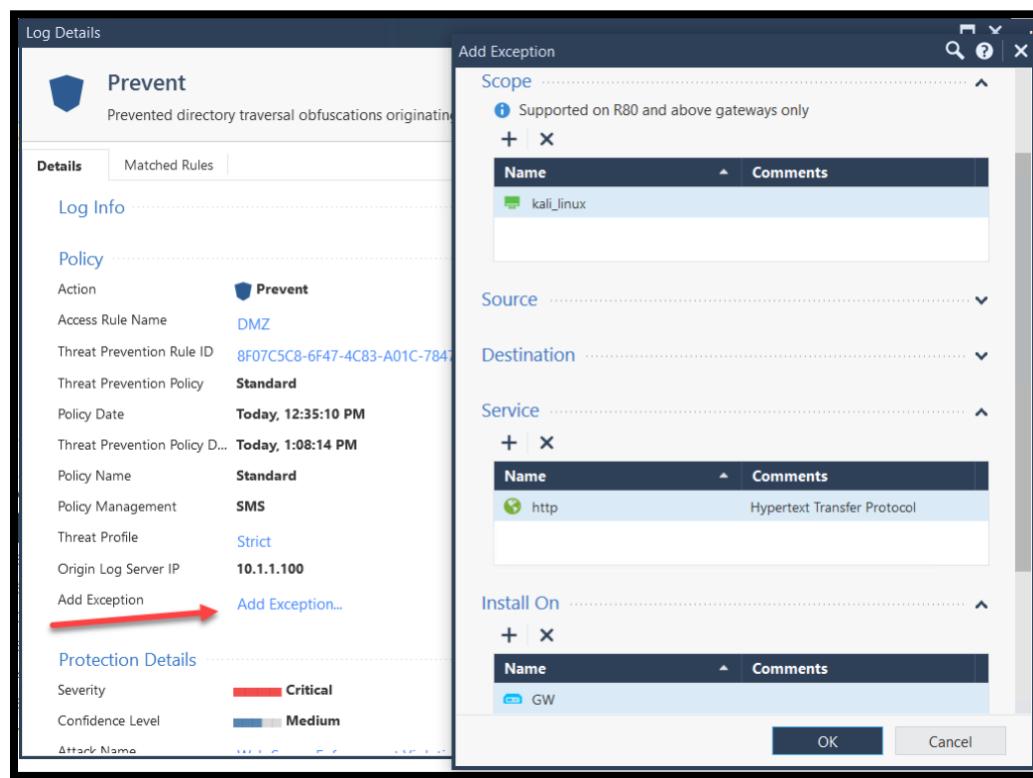
20. Trigger the same protection again. Review the logs and notice that the traffic is now prevented by the Strict profile.



The screenshot shows the 'Log Details' window for a 'Prevent' event. The event details are as follows:

- Action:** Prevent
- Resource:** http://203.0.113.250/cgi-bin/modules/Printing/output.php?url=Lj4vL...
- Threat Wiki:** Go to Threat Wiki
- Policy:** Standard
- Policy Date:** Today, 12:35:10 PM
- Threat Prevention Policy Date:** Today, 1:08:14 PM
- Policy Name:** Standard
- Policy Management:** SMS
- Threat Profile:** Strict
- Origin Log Server IP:** 10.1.1.100
- Add Exception:** Add Exception...
- Protection Details:**
 - Severity:** Critical
 - Confidence Level:** Medium
 - Attack Name:** Web Server Enforcement Violation
 - Attack Information:** Directory Traversal Obfuscations
 - Performance Impact:** Medium
- Forensics Details:**
 - Resource:** http://203.0.113.250/cgi-bin/modules/Printing/output.php?url=Lj4vL...
 - Threat Wiki:** Go to Threat Wiki
- Advanced Forensics Details:**
 - Actions:**
 - Remediation: Go to Remediation Options
 - Report Log: Report Log to Check Point
- More:**
 - Id:** 24d5f64-ad69-33ce-673b-82fd00000003
 - Sequencenum:** 8
 - Description URL:** DIR_TRAV_OBF_help.html
 - Marker:** @A@B@1731947136@C@22185
 - Log Server Origin:** SMS (10.1.1.100)
 - Index Time:** 2024-11-18T18:10:06Z
 - Lastupdatedtime:** 1731953405000

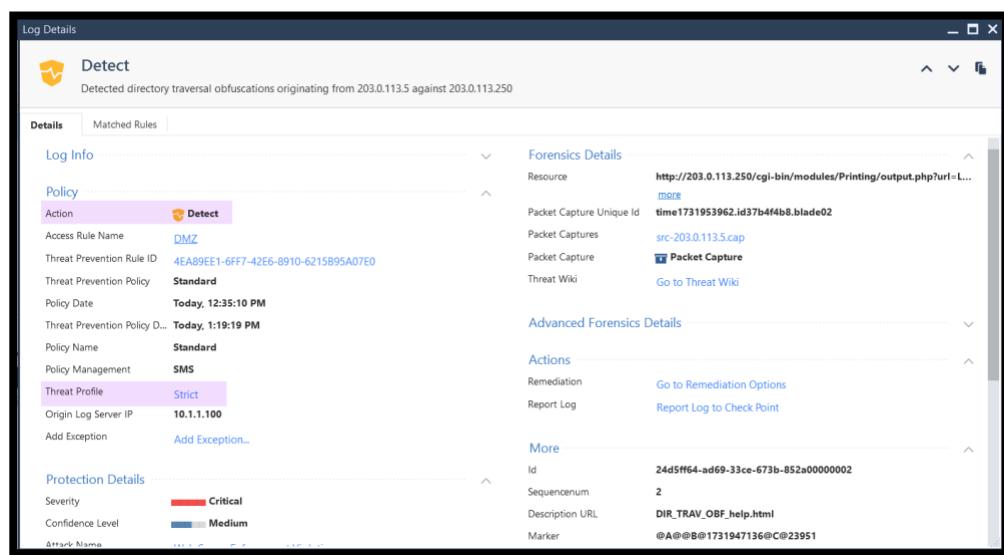
21. Use the Add Exception feature from the log to add an exception to the rule base.



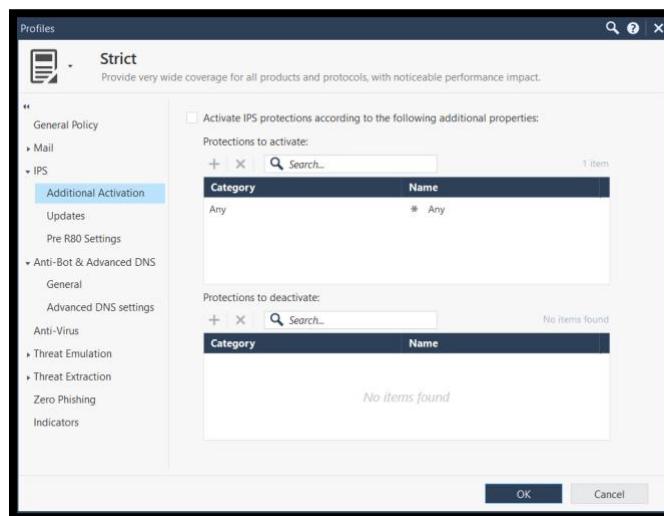
22. Notice that the exception was added to deactivate the protection for a specific source. Change the action to detect and install the Threat Prevention Policy.

No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track	Install On	Comments
1		* Any	- N/A	Strict	Log Packet Capture Forensics	* Policy Targets	
Global Exceptions (No Rules)							
E-1.1	kali_linux	Directory Traversal Obf...	Detect		Log	GW	

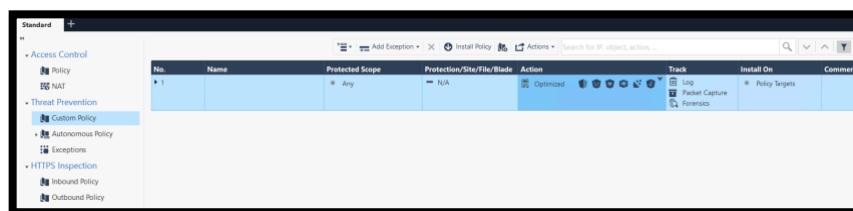
23. Review the detect log and notice that we now have an exception for a specific host.



24. View the Strict Profile and navigate through the available features.



25. Change the Threat Rule and assign the Optimized profile and remove the Exception.



26. Install the Threat Prevention Policy.

End of Lab 5