

# Intrusion Prevention System (IPS)

Expected Time: 45 Minutes

## Introduction

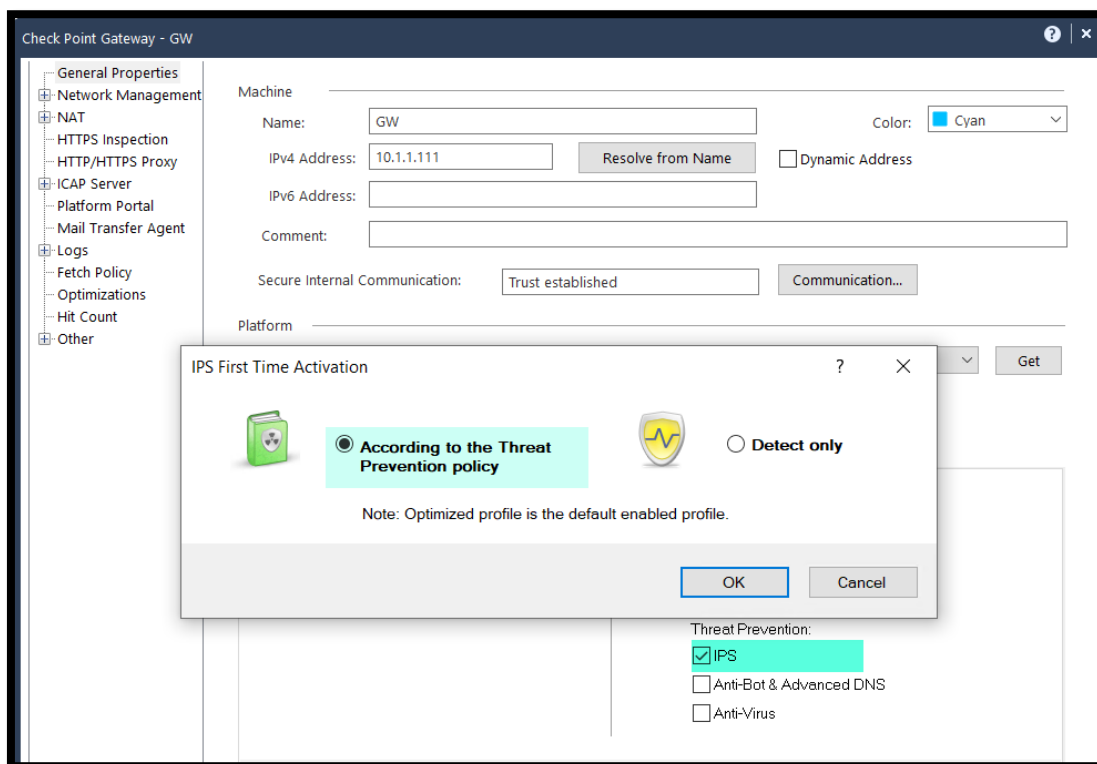
Intrusion Prevention Systems detect or prevent attempts to exploit weaknesses in vulnerable systems or applications, protecting you in the race to exploit the latest breaking threat.

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.

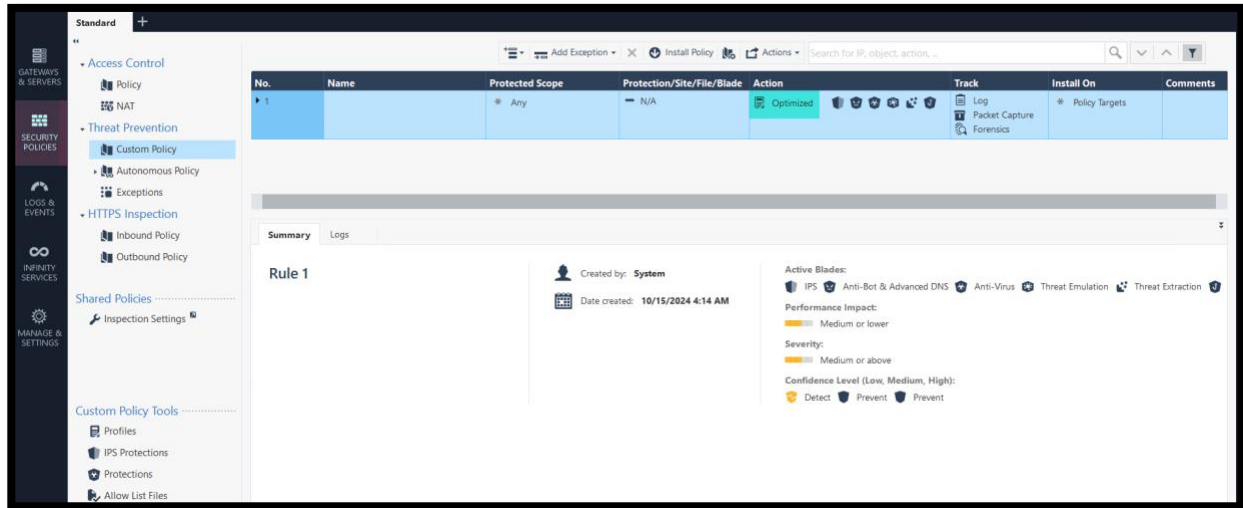
## Exercise 1: Onboarding

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

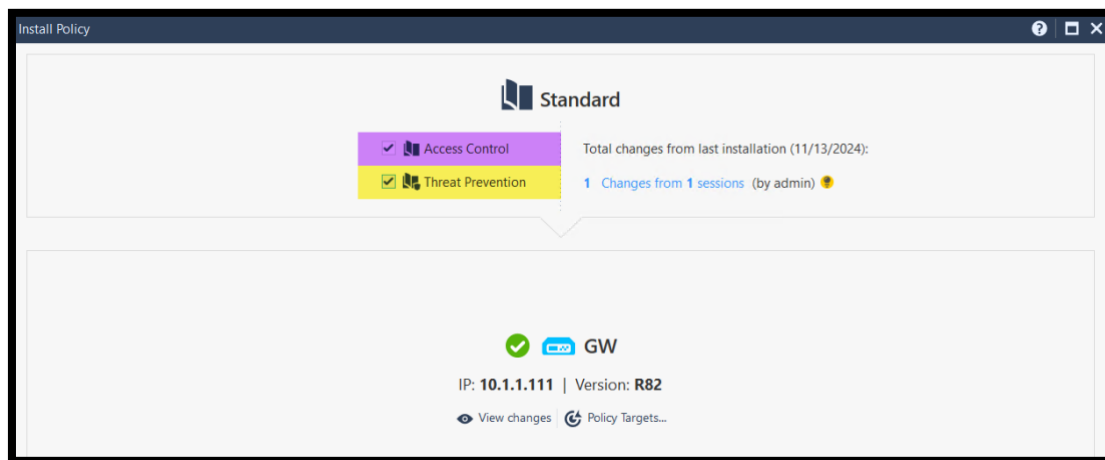
1. Edit the **GW** object and enable the **IPS** blade According to the Threat Prevention Policy.



- 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.



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

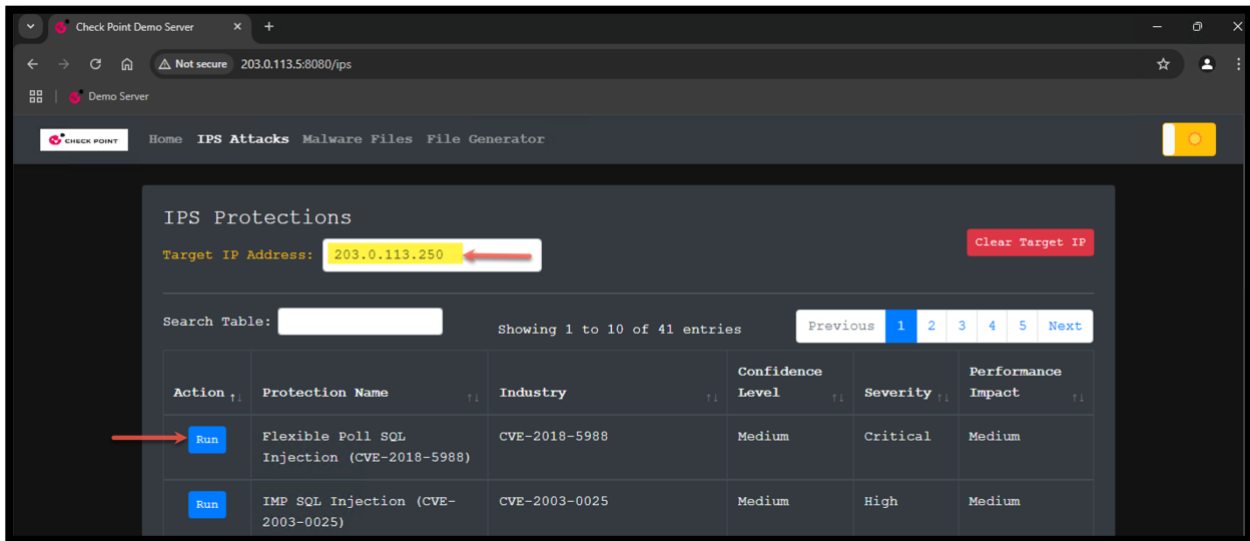


- From **win\_client**, Open the browser and browse to the Demo Server at <http://203.0.113.5:8080>

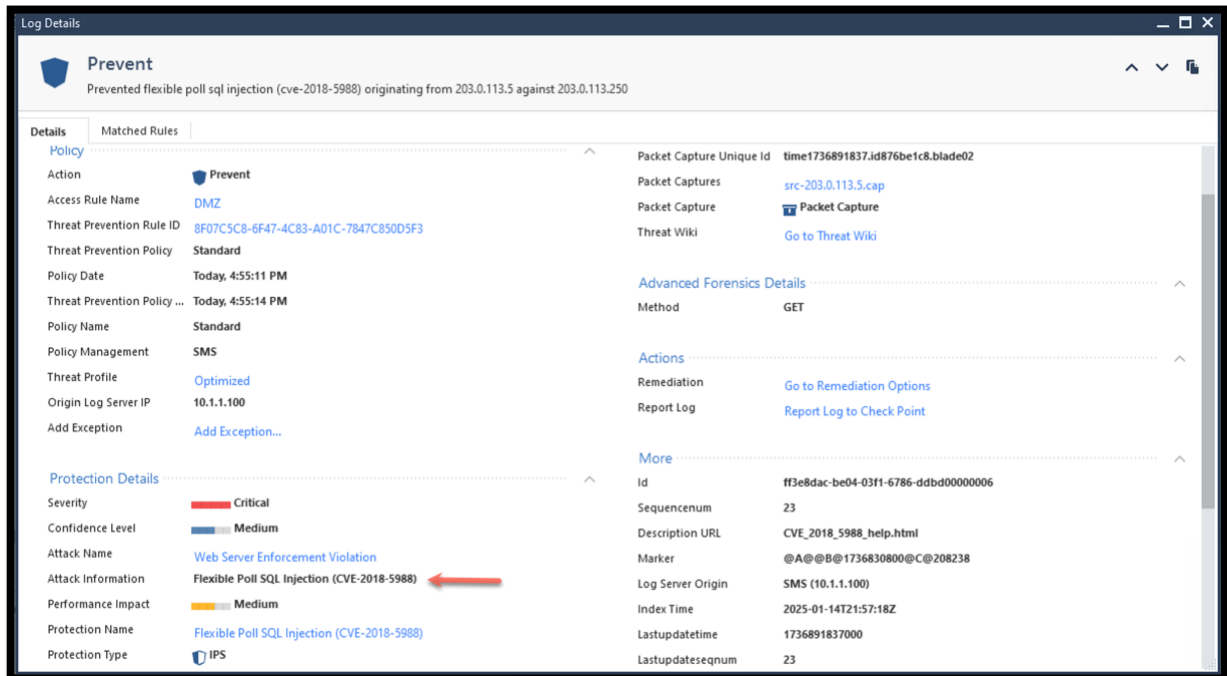
#### Notes:

- 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.

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



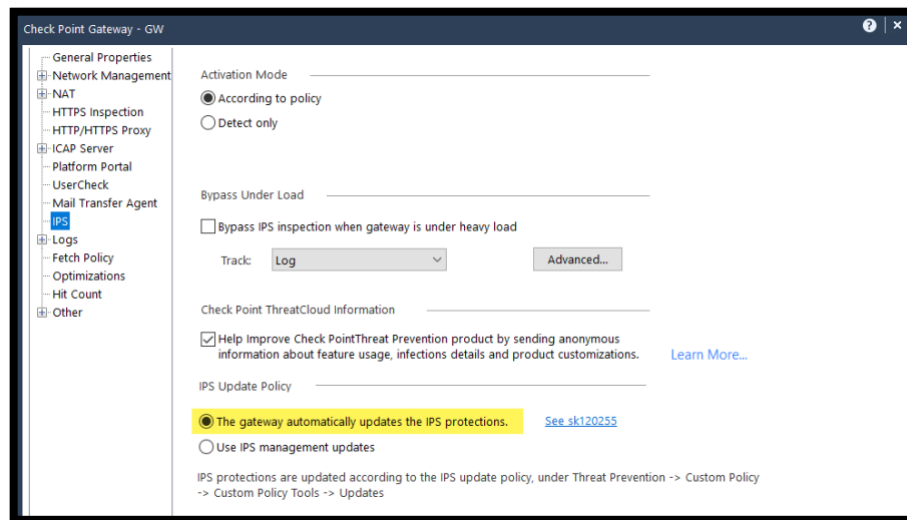
- Filter the logs in SmartConsole to show logs from **IPS** only. Notice that the attack we triggered generated a log and the **Packet Capture** is attached to the log.



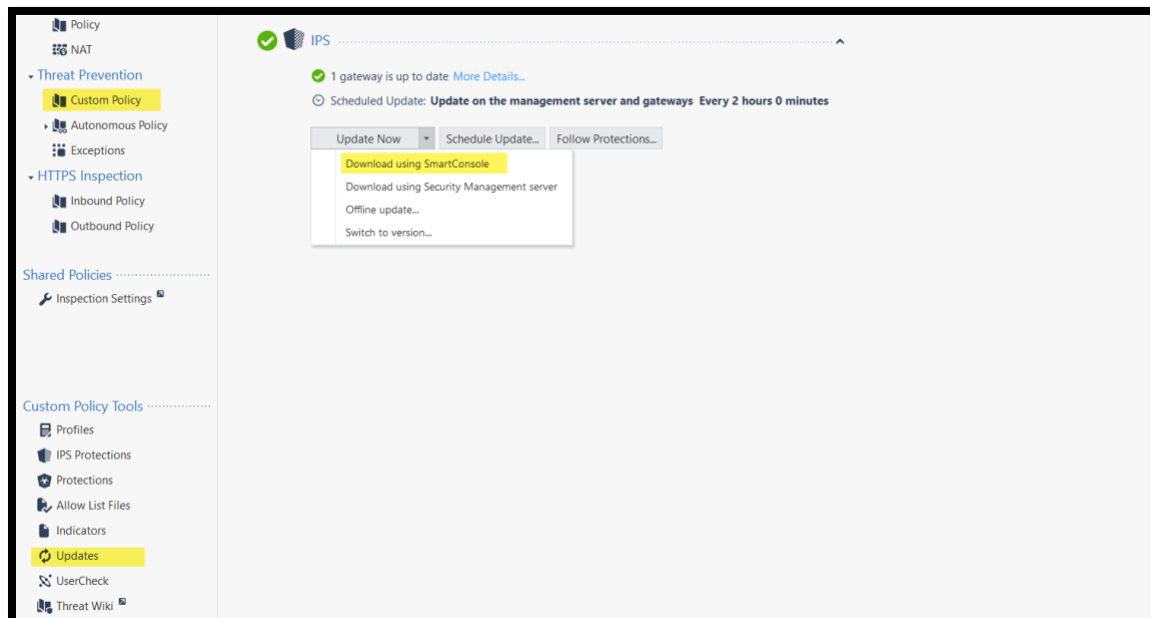
## Exercise 2: Updates

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.

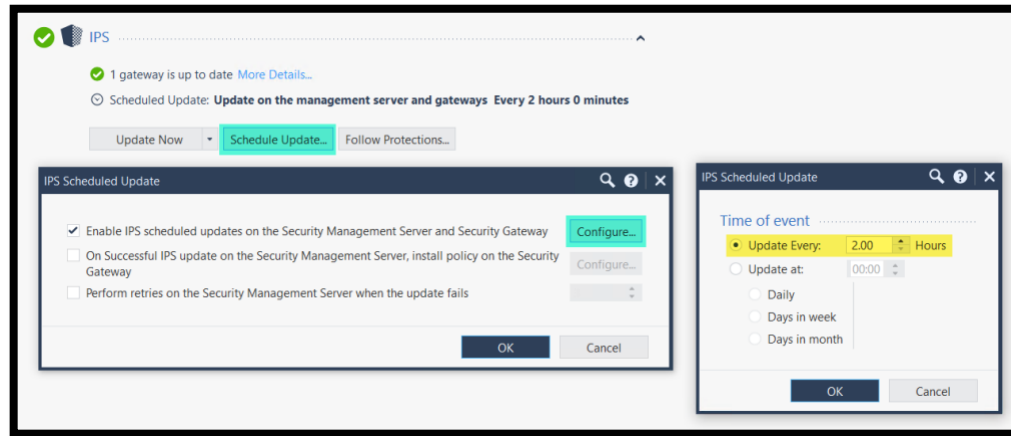
1. Open the **GW** object and review the **IPS Update Policy** settings for the GW. Notice that by default, the GW will try to update the IPS protections automatically. Read [SK120225](#) for more details.



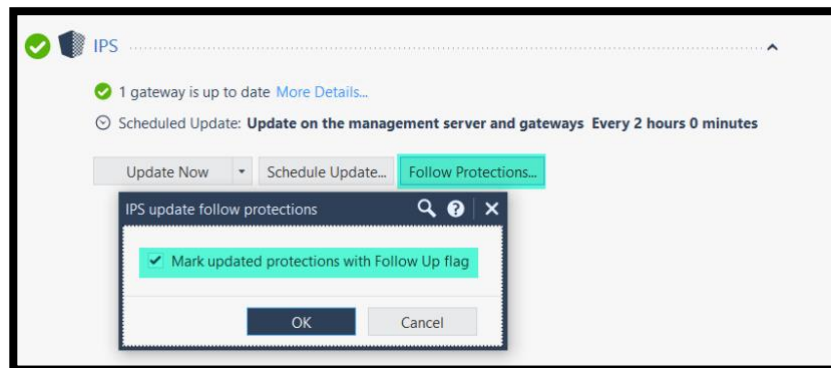
2. While in the Custom Threat Prevention Policy View, click updates and review the available methods to update IPS. Update using SmartConsole.



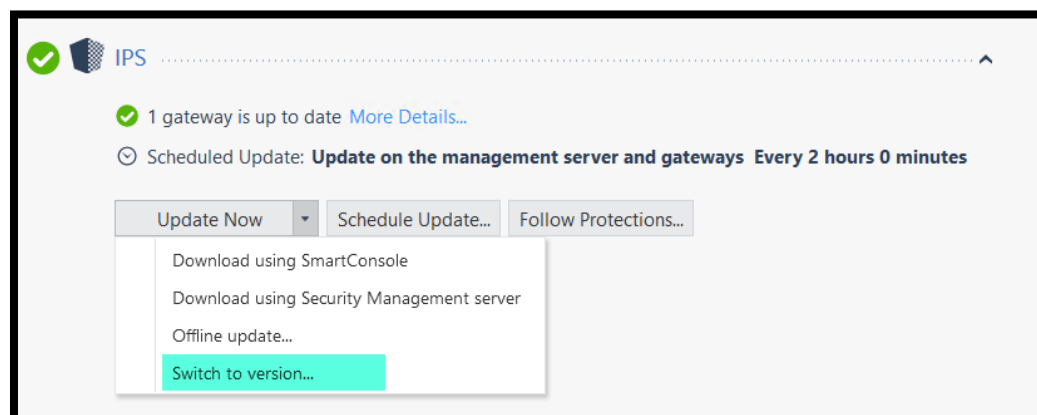
- Review the scheduled updates. By default, the security management and security gateways check for updates every 2 hours.



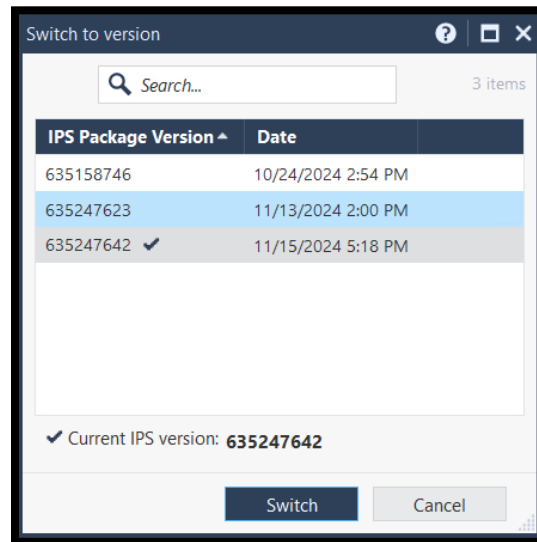
- To be able to tell which protection were updated, they are marked by default. Review the settings under “Follow Protections”.



- 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**



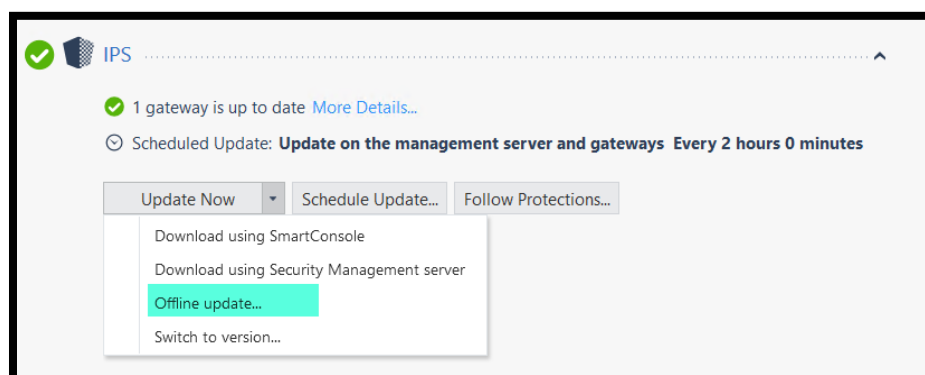
- From the list of versions, select the version to revert to and click Switch.



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

Security Management R80	
Offline Update	sd_updates.upf
MD5	MD5
Version Information	Version Information

- 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 for IPS Protections. A yellow banner at the top states: "IPS protections are not up-to-date, automatically updated gateways may have a newer database version of IPS protections." Below this, a table lists various protections. The 'SQL Injection' protection is highlighted in blue. The interface includes a left sidebar with navigation options like 'Access Control', 'Threat Prevention', and 'Shared Policies'. On the right, there are filters for 'Performance Impact', 'Type', 'Severity', and 'Confidence Level'. The 'SQL Injection' protection details are shown at the bottom, including its CVE references and severity levels.

Protection	Industry Reference	Release	Updated	Performance Impact	Severity	Confidence Level	Optimized
Mismatched Replies	None	N/A	N/A	Low	Critical	Medium	See Details
Multiple Vendor ICMP Connection Reset...	CVE-2004-0790	2/27/2010	4/29/2013	Low	Critical	Medium	See Details
Multiple Vendor ICMP Source Quench De...	CVE-2004-0791	2/27/2010	2/27/2010	Low	Critical	Medium	See Details
Ping of Death	CVE-1999-0128	N/A	N/A	Low	Critical	Medium	See Details
Samba Long CIFS Passwords Buffer Overr...	CVE-1999-0182	1/1/2006	N/A	Low	Critical	Medium	See Details
Scrambling	CVE-2007-3898 CVE-20...	N/A	N/A	Low	Critical	Medium	See Details
SMTP STARTTLS Command	None	N/A	N/A	Low	Critical	Medium	See Details
Spoofed Reset	CVE-2004-0230	N/A	4/12/2015	Low	Critical	Medium	See Details
SQL Injection	CVE-2005-0537	N/A	N/A	Low	Critical	Medium	See Details
Sweep Scan	None	N/A	N/A	Low	Critical	Medium	See Details
Tear Drop	CAN-1999-0258 CAN...	N/A	N/A	Low	Critical	Medium	See Details
Time to Live (TTL) Masking	None	N/A	N/A	Low	Critical	Medium	See Details
Unknown SMTP Commands	None	N/A	N/A	Low	Critical	Medium	See Details

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

The screenshot shows the Check Point management console interface for IPS Attacks. A yellow banner at the top states: "Triggered 'SQL Injection Scanning Attempt'. 104 - Connection Reset by Peer (Blocked)". Below this, a table lists various attacks. The 'SQL Injection Scanning Attempt' attack is highlighted in blue. The interface includes a top navigation bar with options like 'Home', 'IPS Attacks', 'Malware Files', and 'File Generator'. The 'SQL Injection Scanning Attempt' attack details are shown at the bottom, including its CVE references and severity levels.

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
Run	SQL Injection Scanning Attempt	CVE-2020-13118, CVE-2020-5510, CVE-2021-36748, CVE-2021-43140, CVE-2022-	High	Critical	Medium

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

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...

Details
Logs

Last 24 Hours
Current Protection
Enter search query (Ctrl+F)

Found 1 results (210 ms)

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

- Review the log and the field of each section.

Log Details
Prevent
Prevented sql injection scanning attempt originating from 203.0.113.5 against 203.0.113.250

Details
Matched Rules

Action
Access Rule Name
Threat Prevention Rule ID
Threat Prevention Policy
Policy Date
Threat Prevention Policy D...
Policy Name
Policy Management
Threat Profile
Origin Log Server IP
Add Exception

Protection Details
Severity
Confidence Level
Attack Name
Attack Information
Performance Impact
Protection Name
Protection Type
Industry Reference

Packet Capture Unique Id
Packet Captures
Packet Capture
Threat Wiki
Advanced Forensics Details
MITRE ATT&CK
Initial Access
Actions
Remediation
Report Log
More
Id
Sequencenum
Description URL
Marker
Log Server Origin
Index Time
Lastupdateime

- 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.

Core Protections
General
Gateways
Exceptions

The following protection settings are enforced according to Gateways setting and installed via Acc...

Protection: SQL Injection

SQL Injection
Performance Impact
Severity
Confidence Level

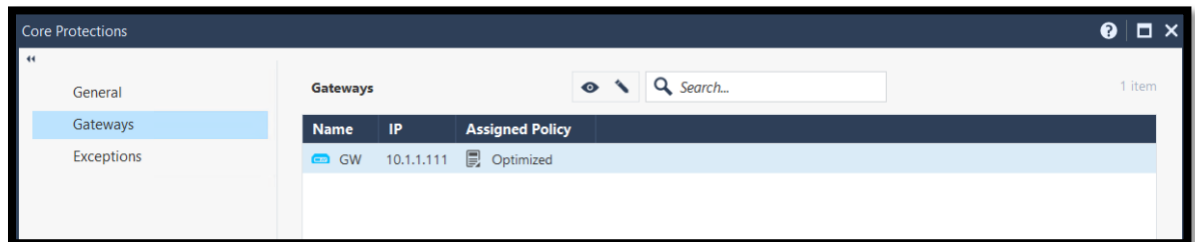
Actions
Search...

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

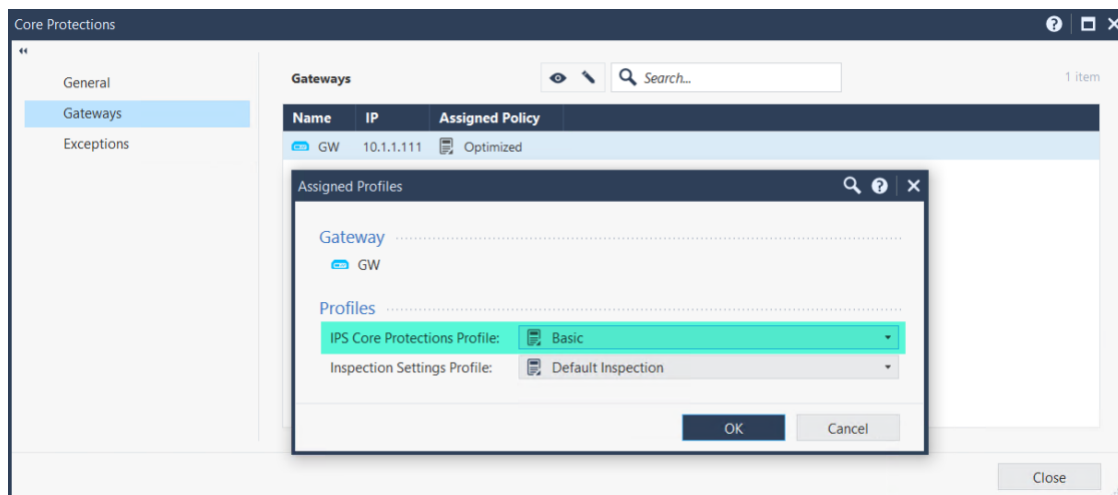
Close



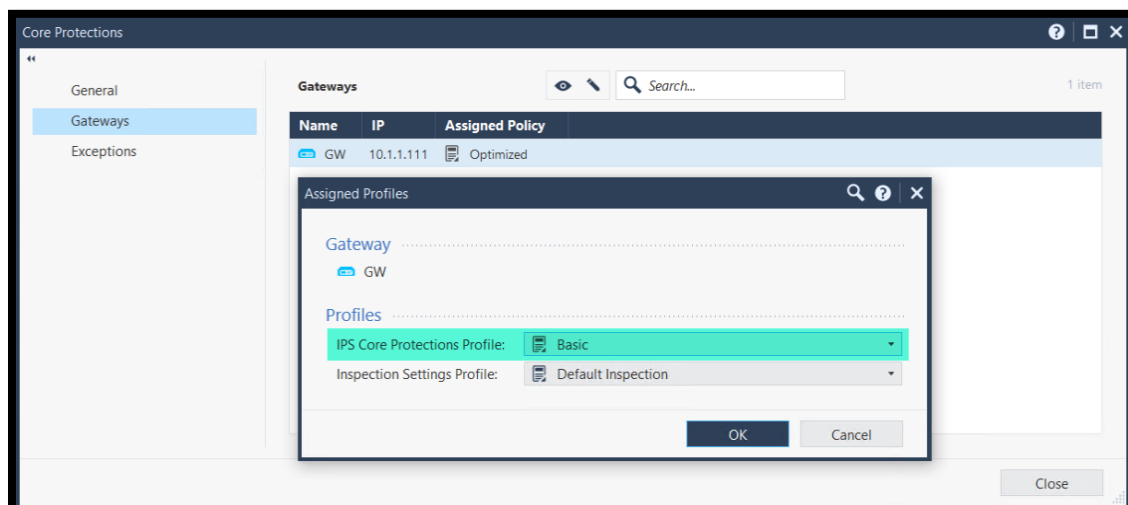
6. Move to the Gateways tab and review the default profile settings. Notice that this profile assignment is independent of the profile assigned in the rule base.



7. Edit the selection and select the Basic profile



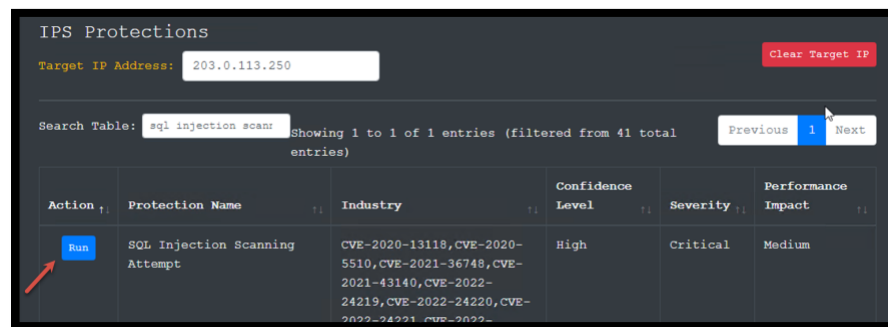
8. Edit the profile selection and select the Basic Profile.



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



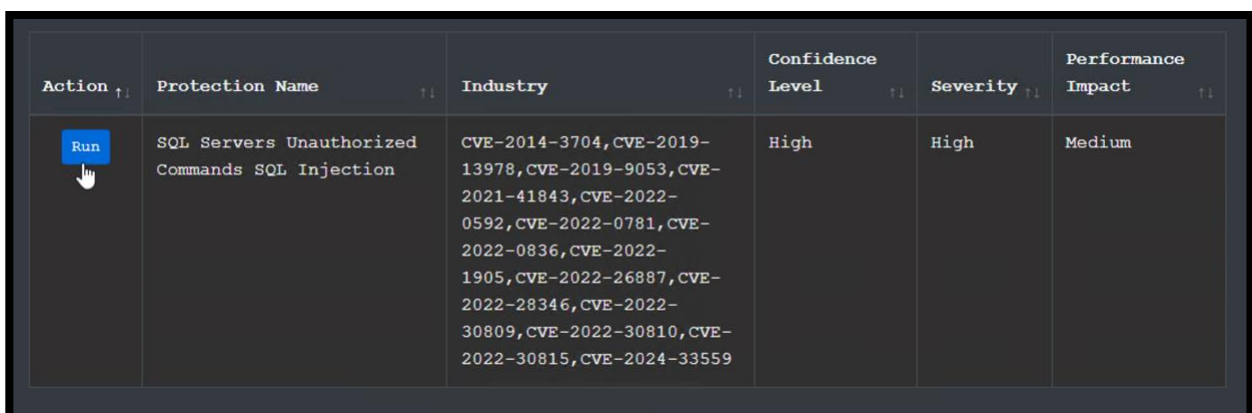
- Try to trigger the same protection we used before in the demo Server (SQL Scanning attempt)



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

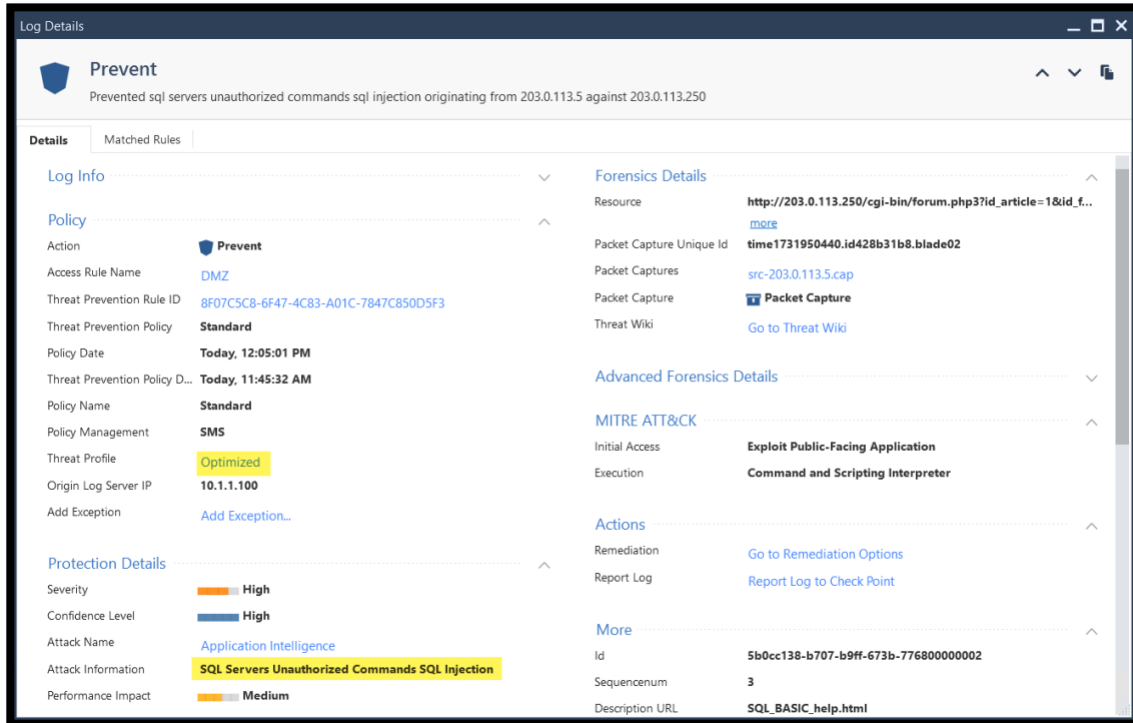
- There will be no new logs since this protection is disabled in the Basic profile which we assigned to the GW.
- Pay extra attention to deactivating protections as it will leave gaps in your security protection.

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





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

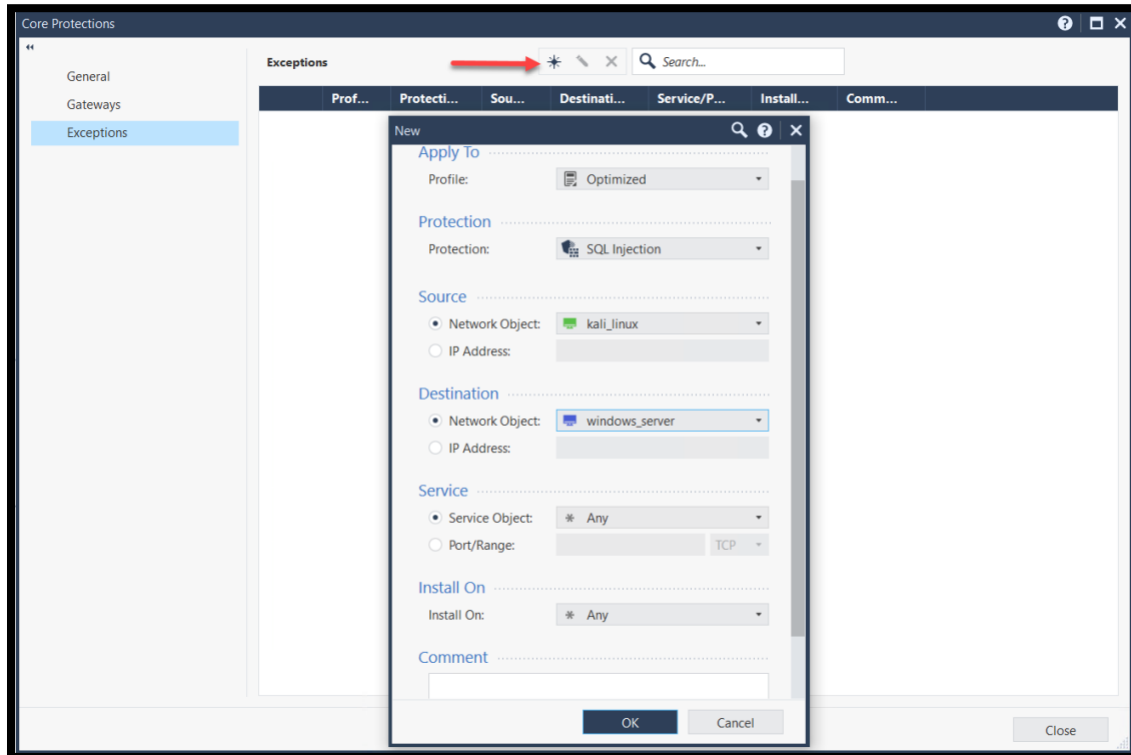
- Check Point provide multiple protections that work in parallel to protect your environment.
- Notice that this protection is managed via the Optimized profile assigned in the rule base and not the Basic profile we assigned to core protections.



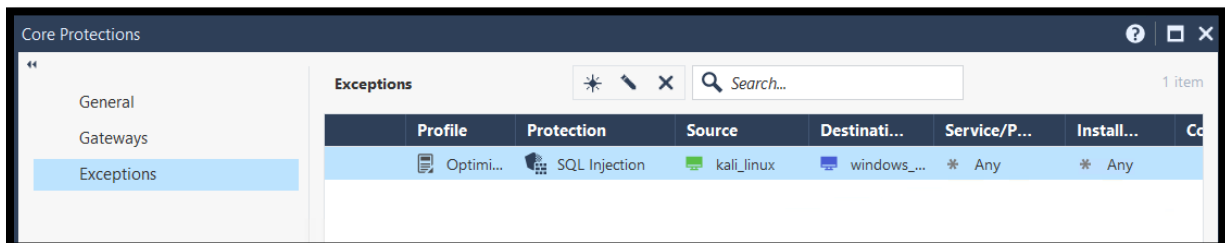
14. Edit the SQL protection settings and assign the **Optimized Profile**.

Gateways			Search...	
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



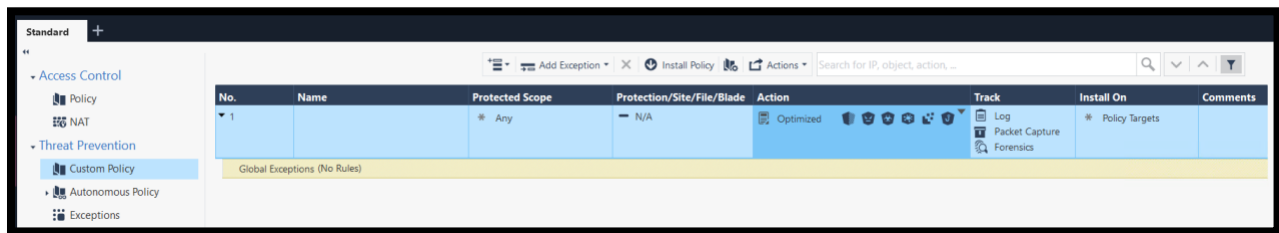
17. Run a new test using the same protection trigger from the demo server.

- 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.

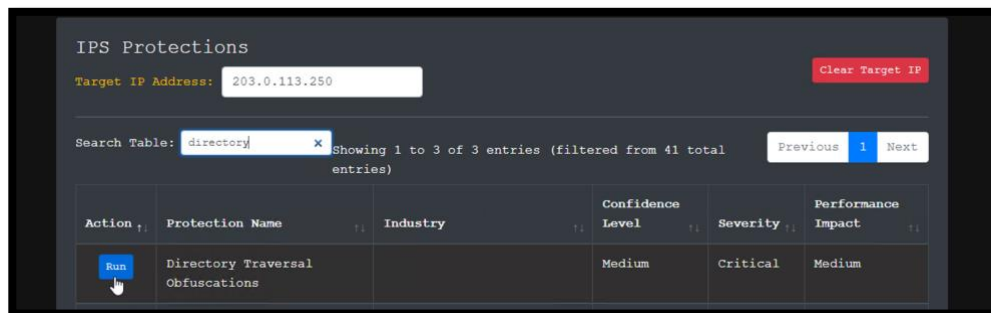
## Exercise 4: Threat Cloud Protections

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

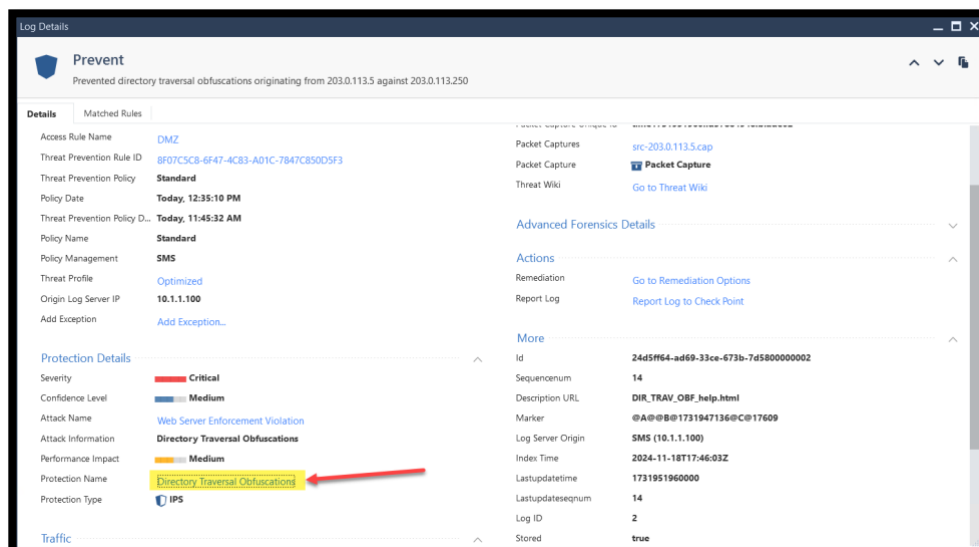
- Review the default rule in the Threat Prevention Custom policy. Notice that the optimized profile is assigned by default.



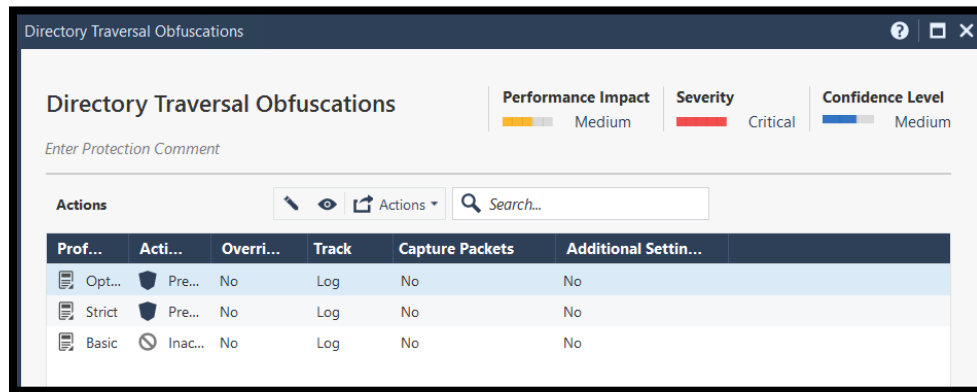
- From the demo server, trigger the protection **Directory Traversal Obfuscation**



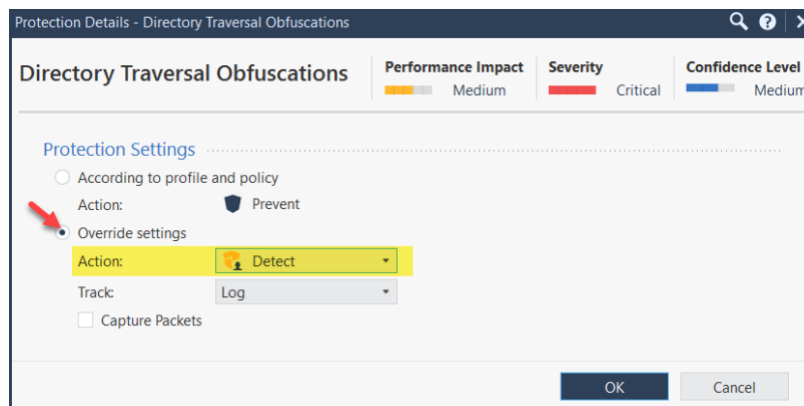
- Review the log and pay attention to the profile.



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.



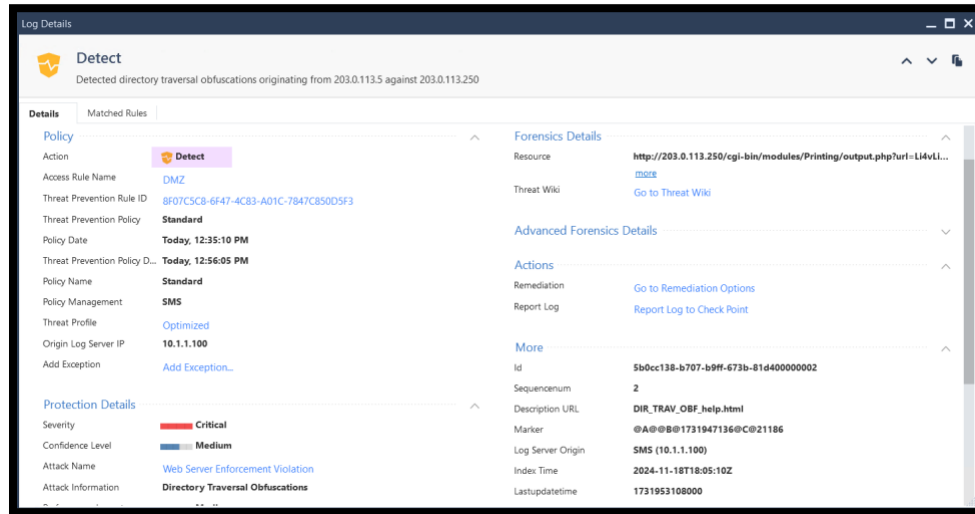
16. While Optimized is selected, edit the settings and change the behavior to detect instead of Prevent.



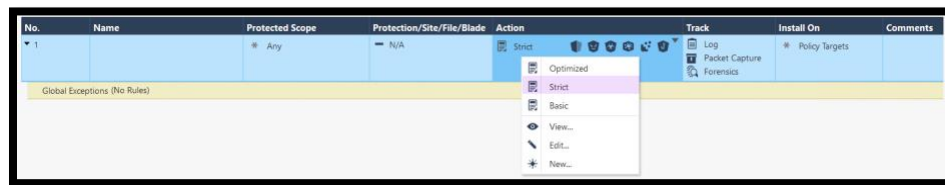
17. Confirm the changes and Install the Threat Prevention Policy.

Actions						
Profile	Acti...	Overri...	Track	Capture Packets	Additional Settin...	
Optimized	Det...	Yes	Log	No	No	
Strict	Pre...	No	Log	No	No	
Basic	Inac...	No	Log	No	No	

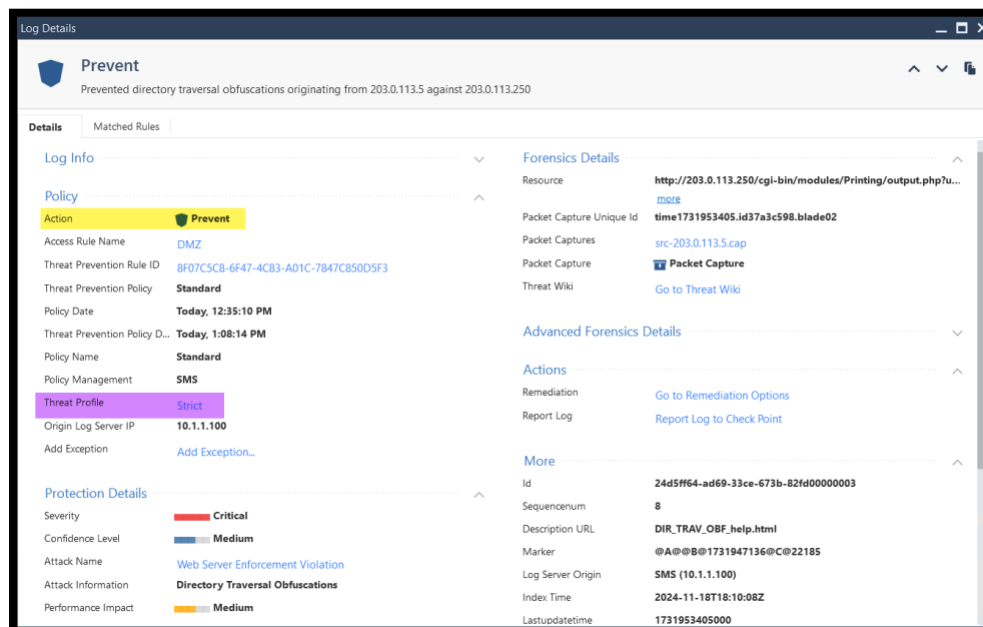
18. Trigger the same protection again and review the logs. You should see a detect log. Note that this is only made for the optimized profile. However, this applies to all hosts and networks.



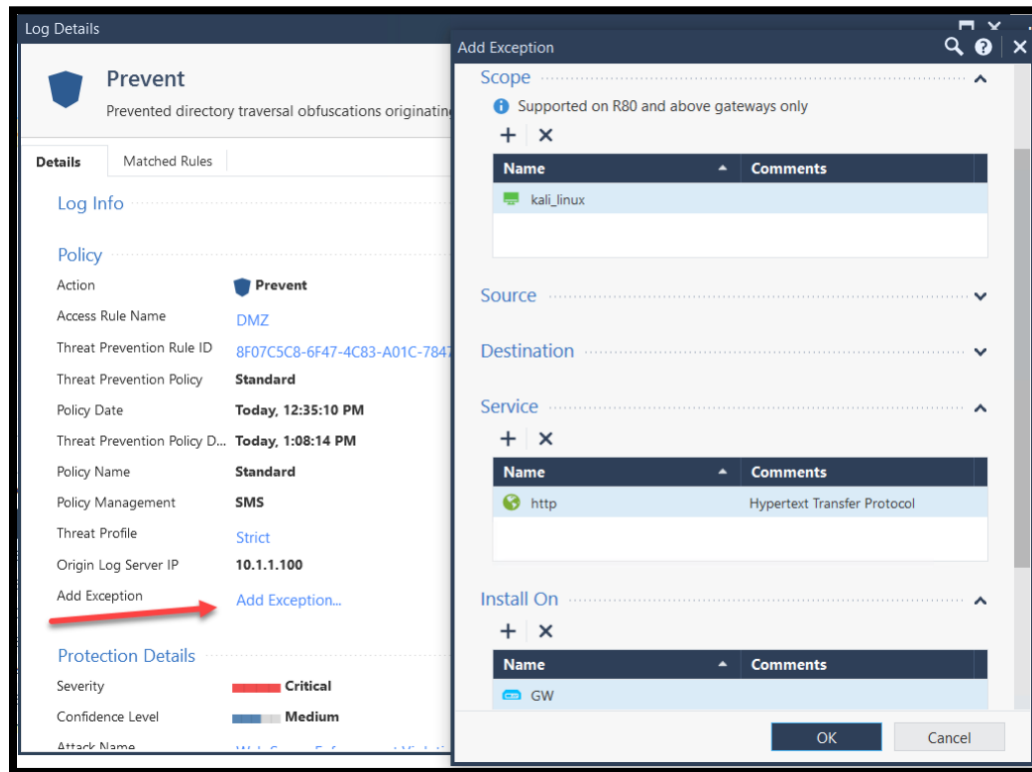
19. Change the profile assigned to the default rule, select the Strict profile and install the Threat Prevention Policy.



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



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

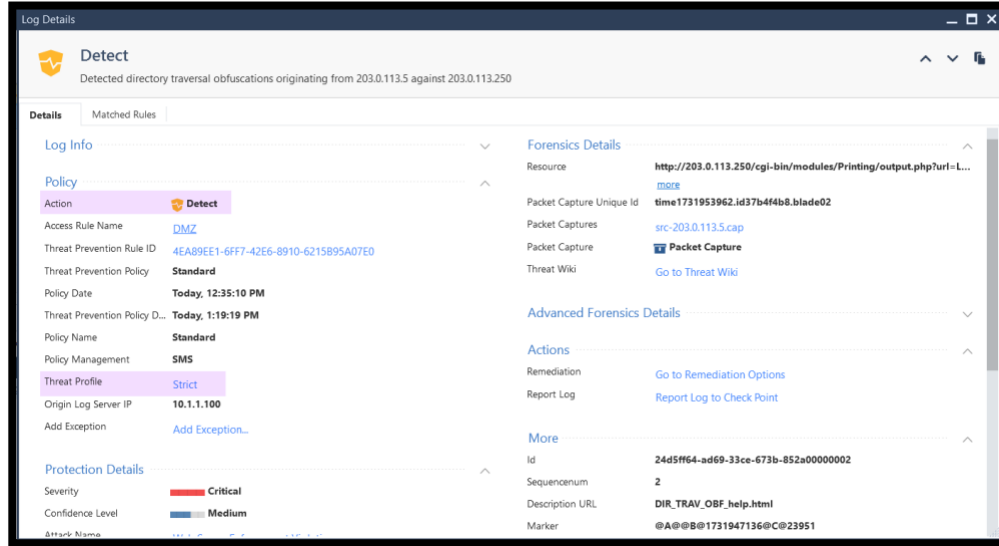


22. Notice that the exception was added to deactivate the protection for a specific source. Change the action to detect and install the Threat Prevention Policy.

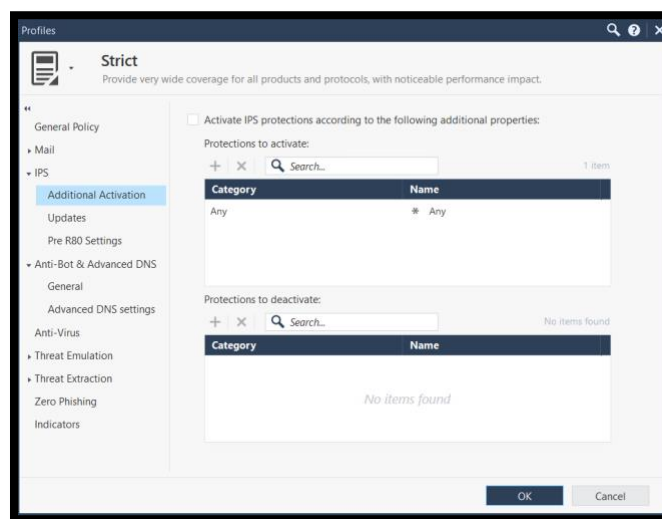
No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track	Install On	Comments
1		* Any	N/A	Strict	Log Packet Capture Forensics	* Policy Targets	
Global Exceptions (No Rules)							
E-1.1		kali_linux	Directory Traversal Obf...	Detect	Log	GW	

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

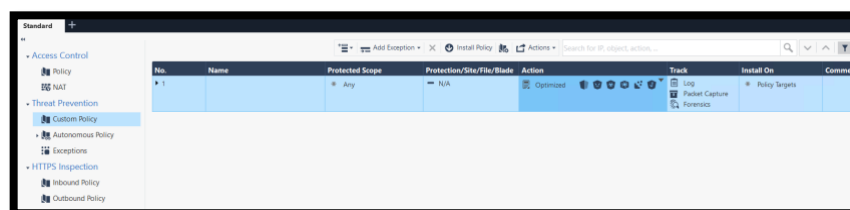




24. View the Strict Profile and navigate through the available features.



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



26. Install the Threat Prevention Policy.