

Intrusion Prevention System (IPS)

Introduction

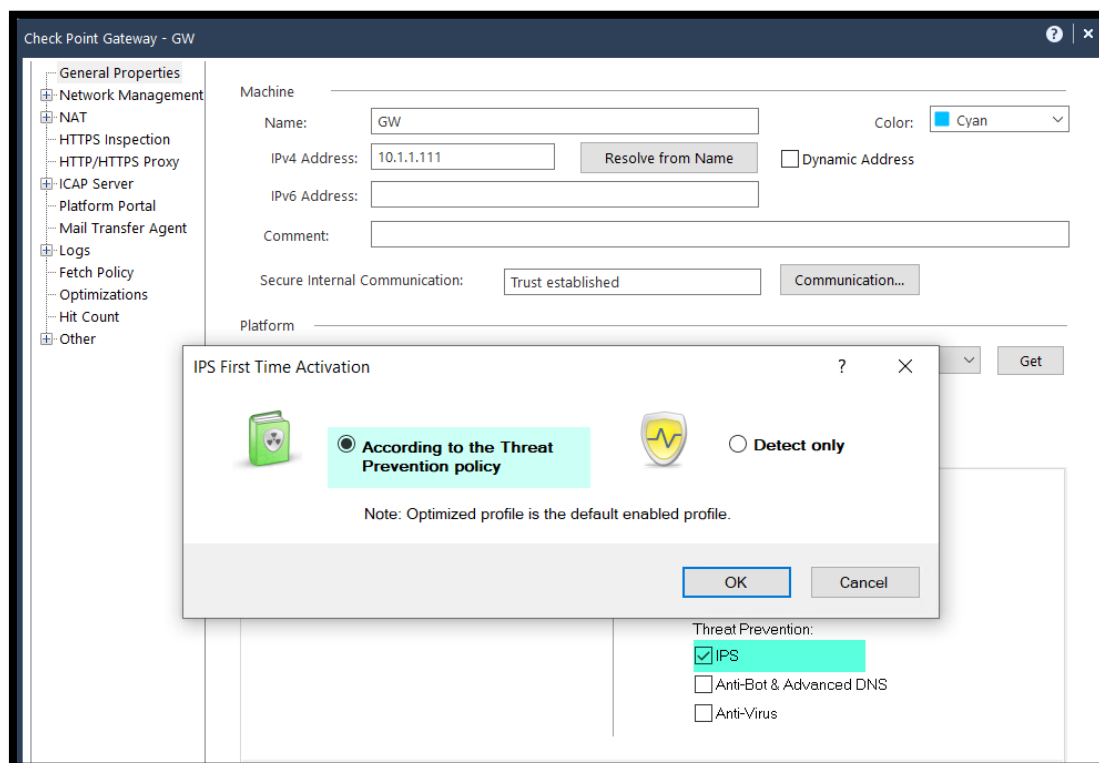
Intrusion Prevention Systems detect or prevent attempts to exploit weaknesses in vulnerable systems or applications, protecting you in the race to exploit the latest breaking threat.

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.

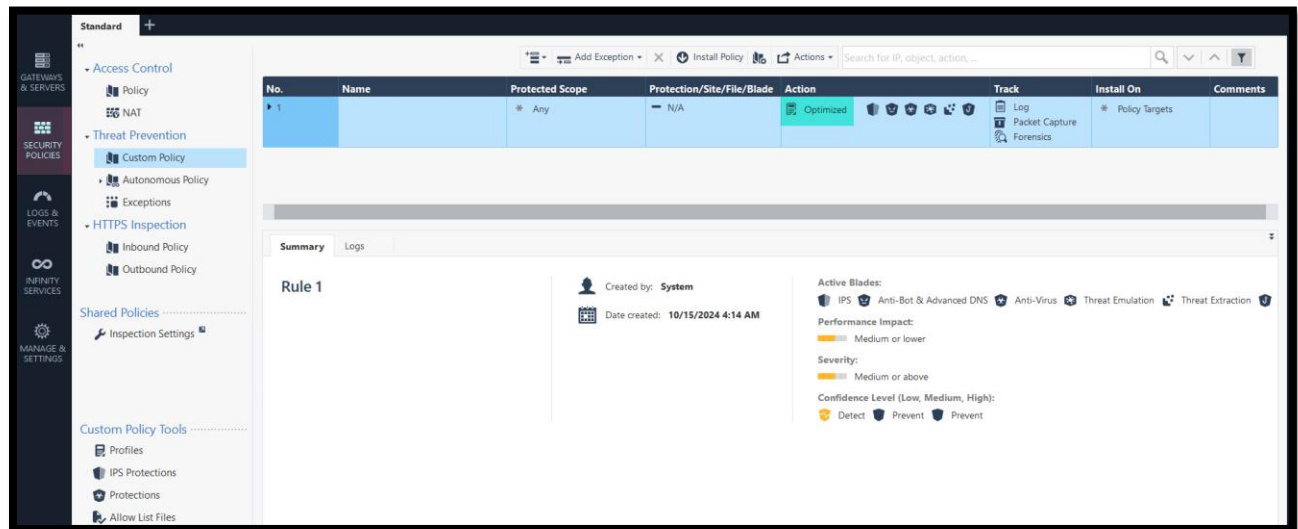
Exercise 1: Onboarding

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.

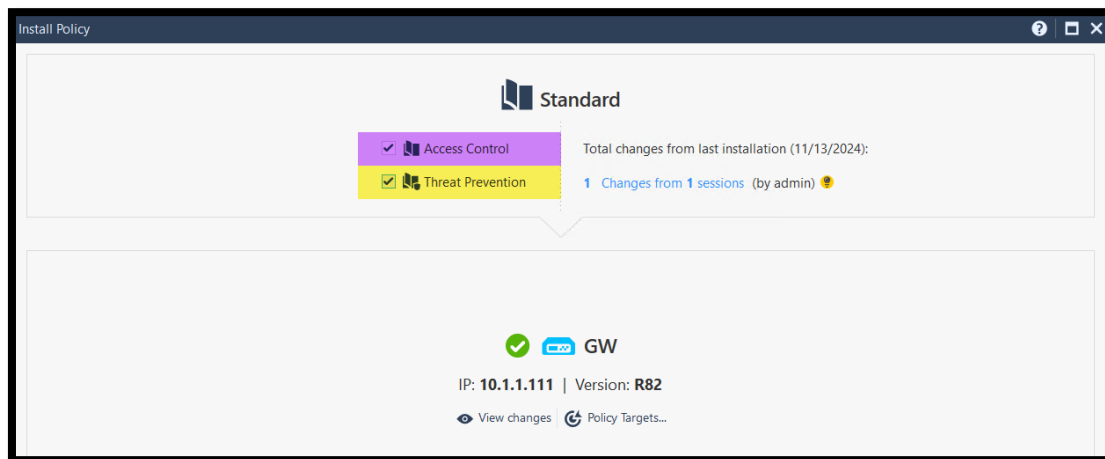
1. Edit the GW object and enable the IPS blade according to the Threat Prevention Policy.



- Under the Custom Threat Prevention Policy, notice that a customized profile is assigned by default. It is customized for good security while making sure the performance is not greatly affected.



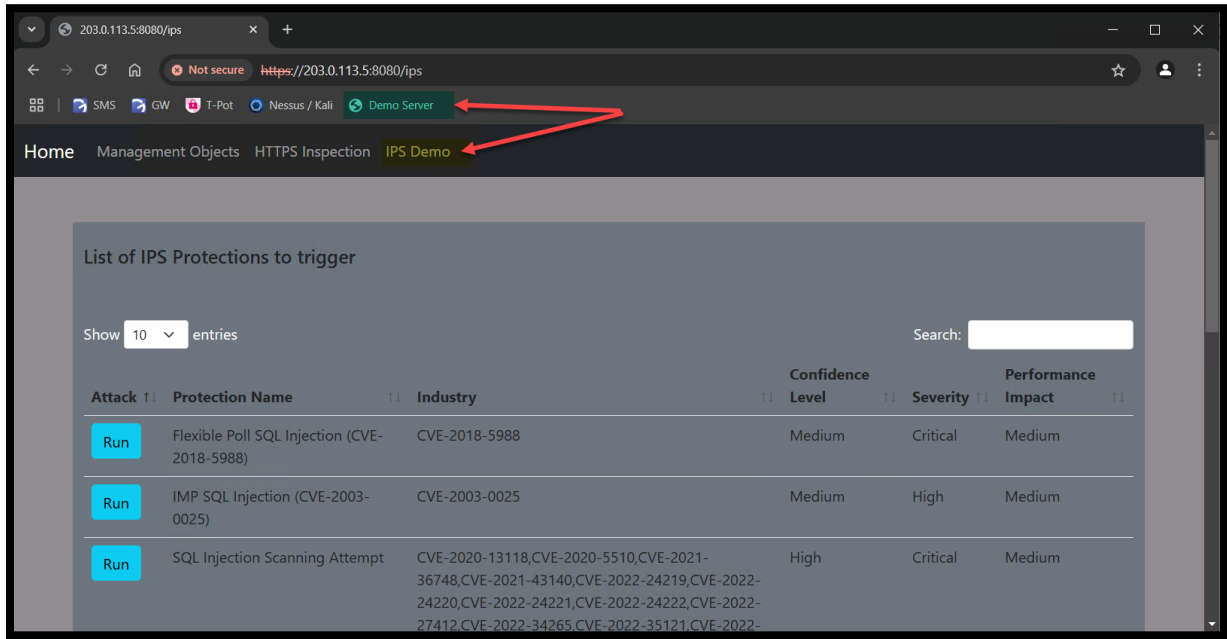
- Install the Access and Threat Prevention Policy.



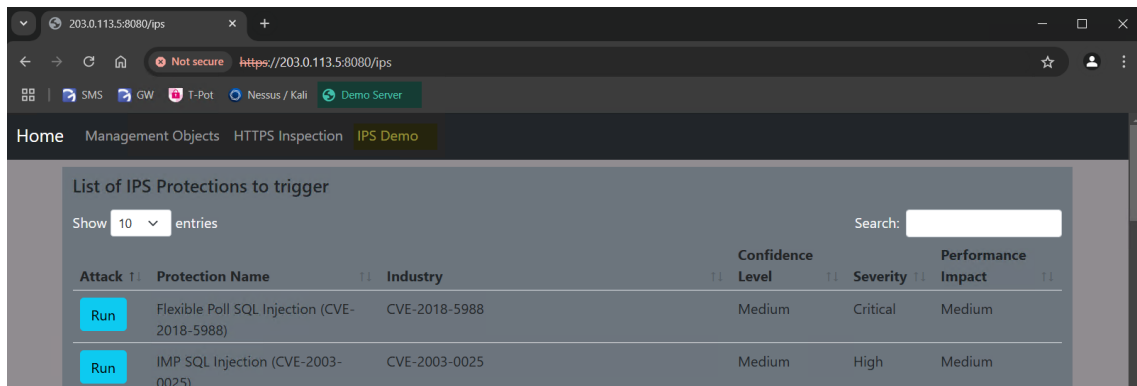
- Open the browser and browse to the demo server at 203.0.113.5:8080

Notes:

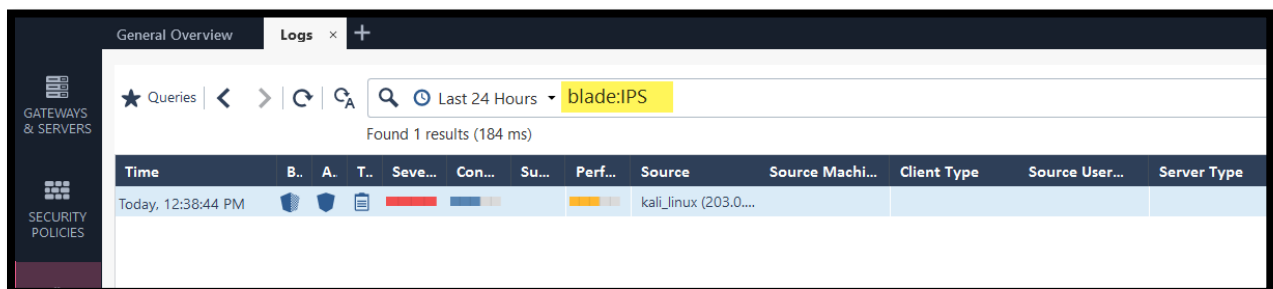
- This server is installed on the Kali Linux machine.
- The target of those attacks is set to the windows server machine at the public address 203.0.113.250. this address is translated o the GW to the real address 10.1.2.250.
- Attacks are based on HTTP calls.



- Click Run to trigger the first protection in the list. Do not expect a response. It's a fire and forget based attacks demo attack.



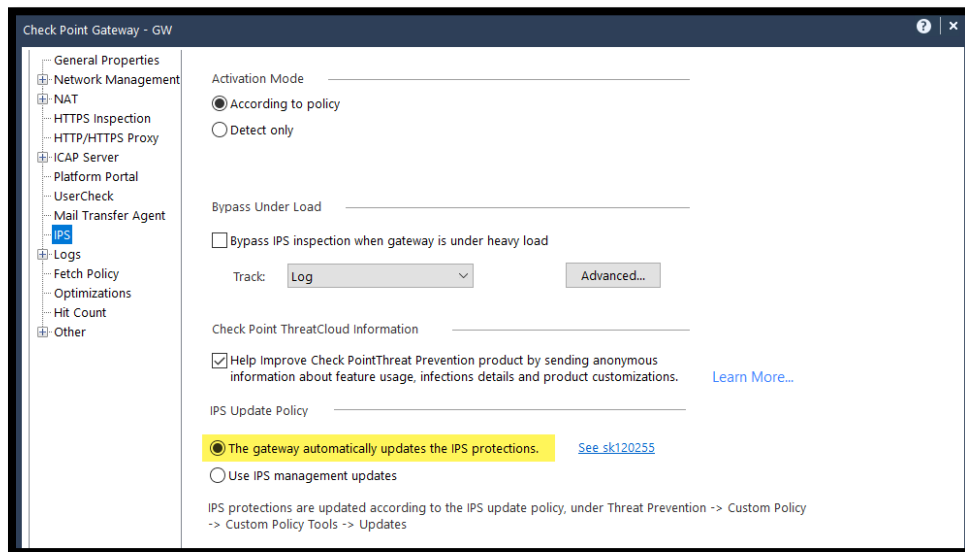
- Filter the logs in SmartConsole to show logs from IPS only. Notice that the attack we triggered generated a log already.



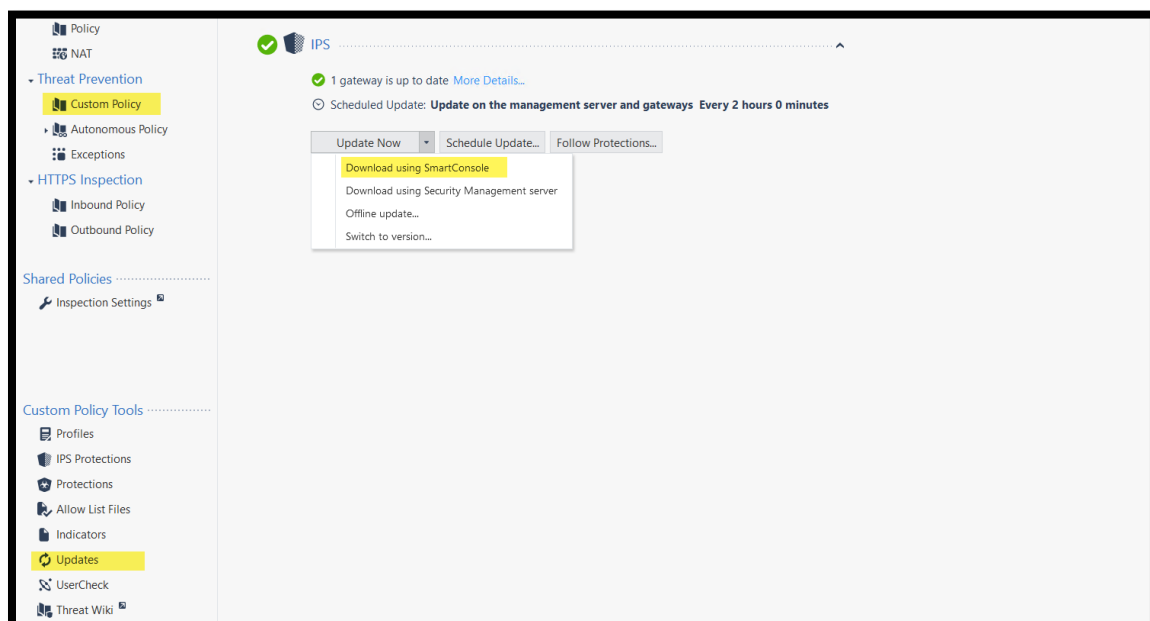
Exercise 2: Updates

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.

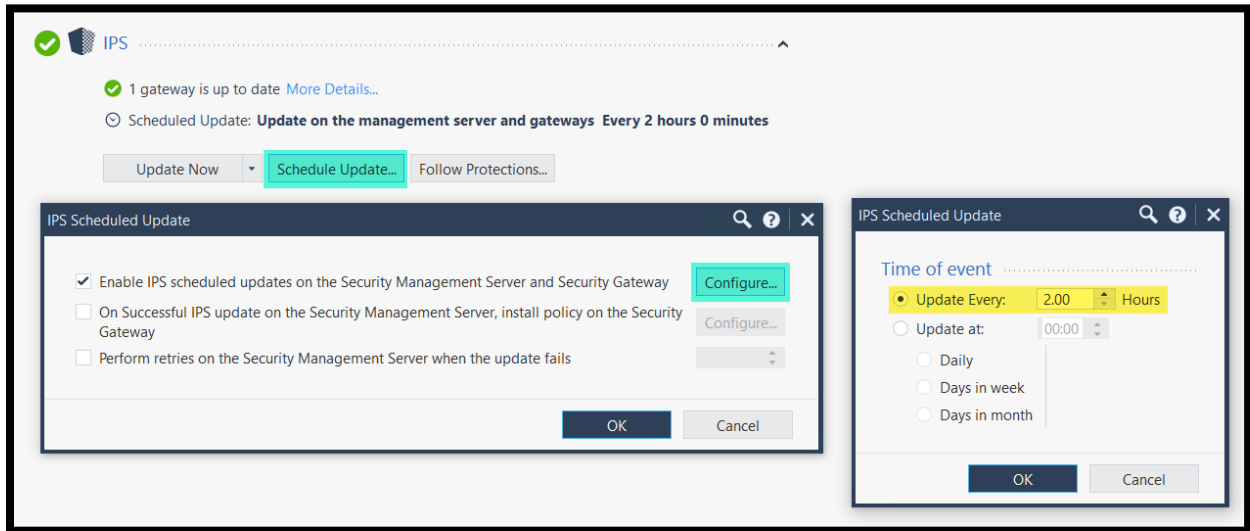
1. Open the GW object and review the IPS update settings for the GW. Notice that by default, the GW will try to update the IPS protections automatically. Read [SK120225](#) for more details.



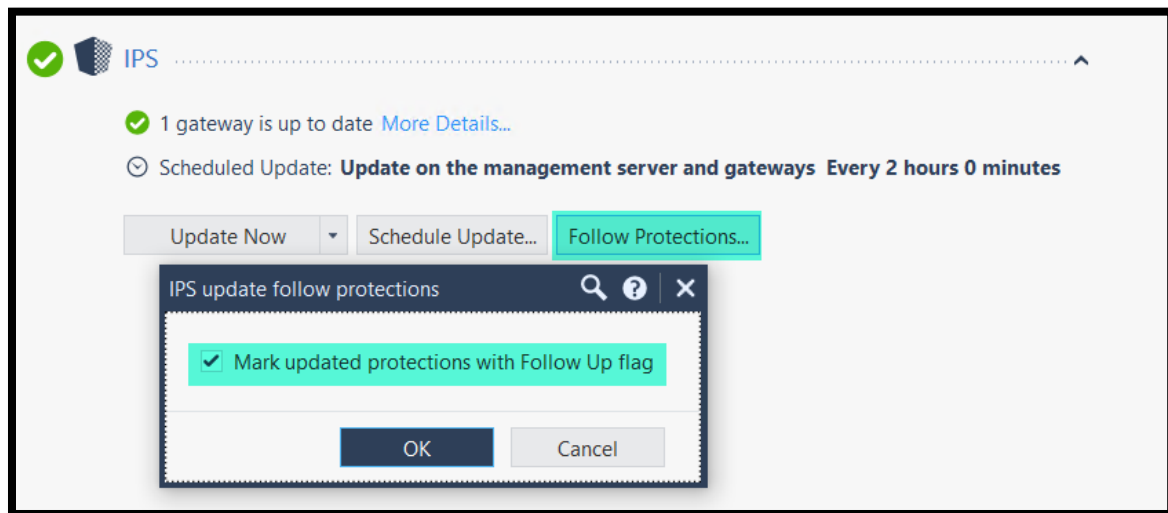
2. While in the Custom Threat Prevention Policy View, click updates and review the available methods to update IPS. Update using SmartConsole.



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

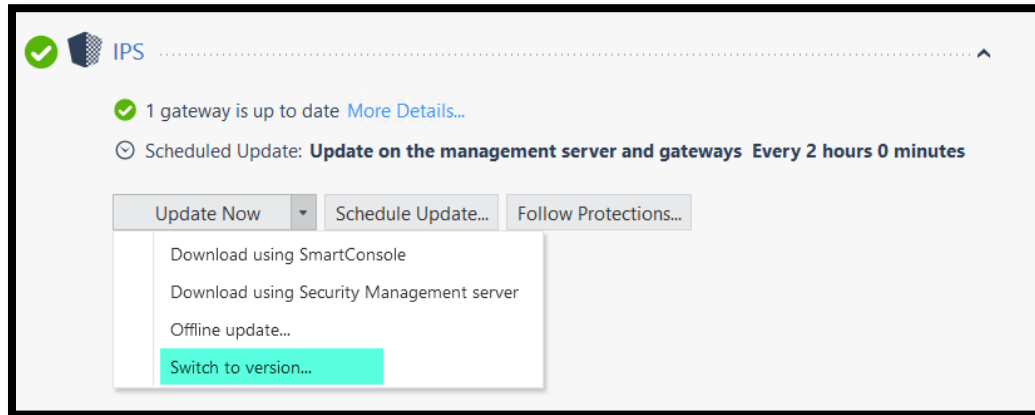


- To be able to tell which protection were updated, they are marked by default. Review the settings under "Follow Protections".

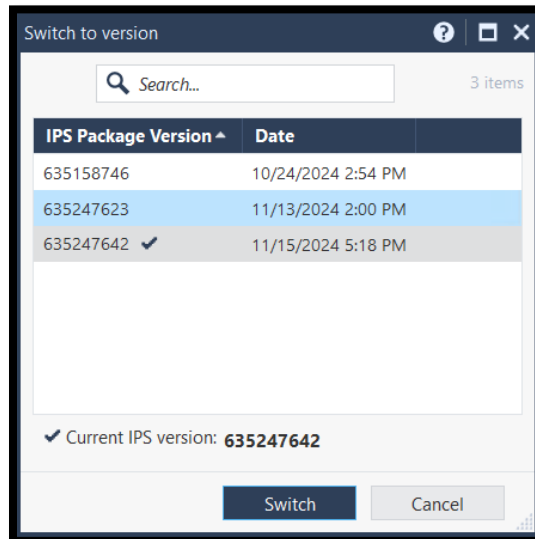


- In case you updated IPS and for any reason you would like to revert to one of the older versions, navigate to the list of updated under:

Update now -> Switch to version



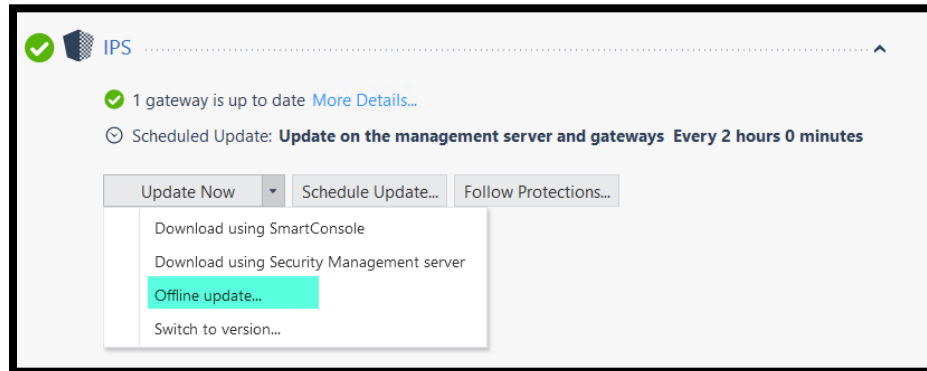
6. From the list of versions, select the version to revert to and click Switch.



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

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

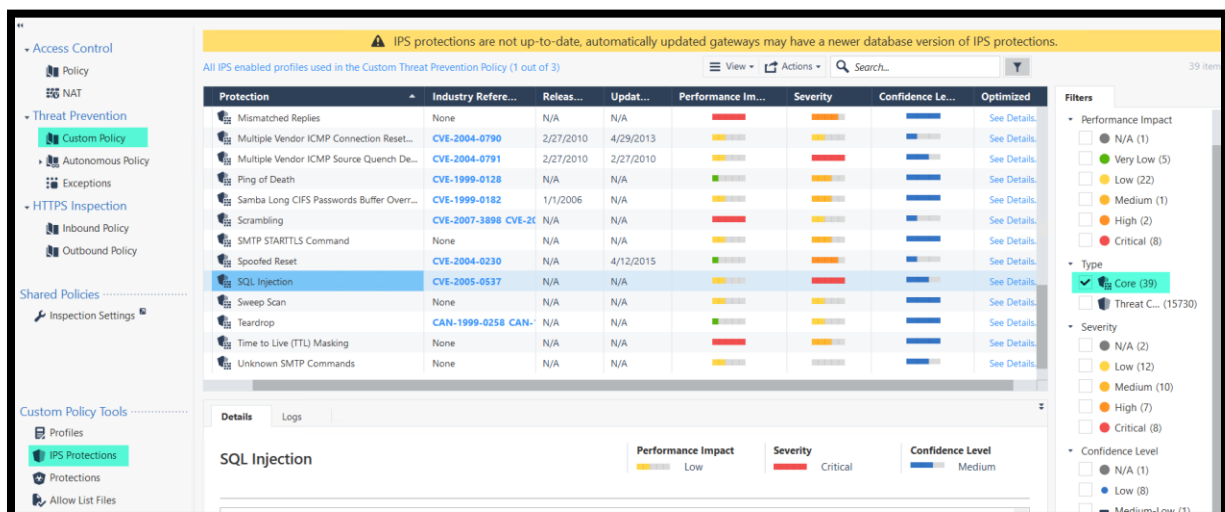
- When Offline Updates is selected from the drop-down menu, you will be asked to point to the update file location.



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.

- Open the IPS protection tab and filter the protections to show Core protections only. Notice that the icon for the core protections differ from the threat Cloud protections.



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

Attack	Protection Name	Industry	Level	Severity	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-2022-24219,CVE-2022-24220,CVE-2022-24221,CVE-2022-24222,CVE-2022-27412,CVE-2022-34265,CVE-2022-35121,CVE-2022-36669,CVE-2022-47862,CVE-2023-24780	High	Critical	Medium

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

	SQL Injection	CVE-2005-0537	N/A	N/A	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	See Details.
	Sweep Scan	None	N/A	N/A	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	See Details.
	Teardrop	CAN-1999-0258 CAN-	N/A	N/A	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	See Details.
	Time to Live (TTL) Masking	None	N/A	N/A	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	See Details.
	Unknown SMTP Commands	None	N/A	N/A	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	See Details.

Details		Logs	
---------	--	-------------	--

			Last 24 Hours		Current Protection	<input type="text" value="Enter search query (Ctrl+F)"/>	
--	--	--	---------------	--	--------------------	--	--

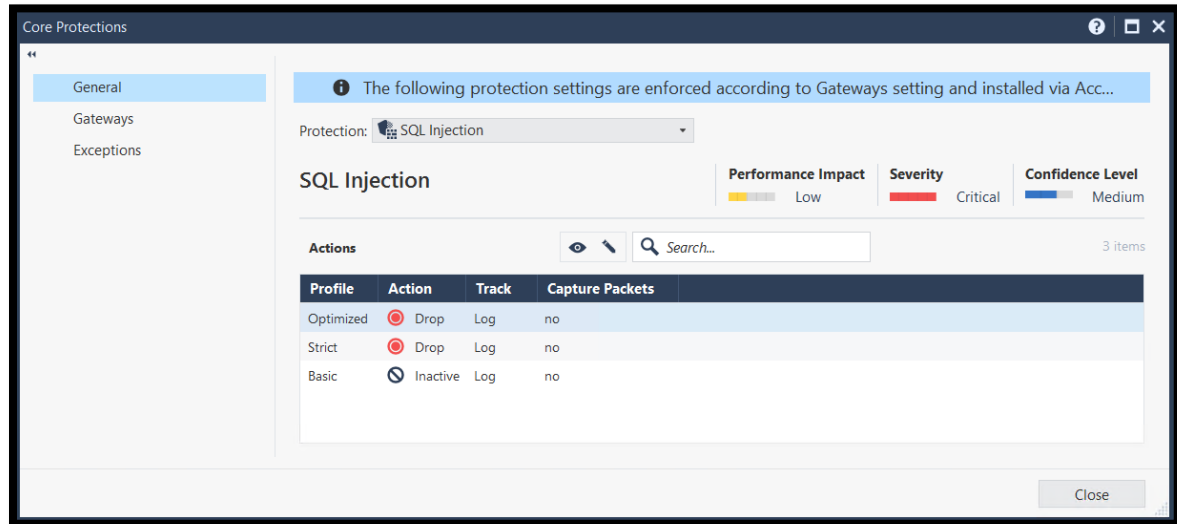
Found 1 results (210 ms) [Query Syntax](#)

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

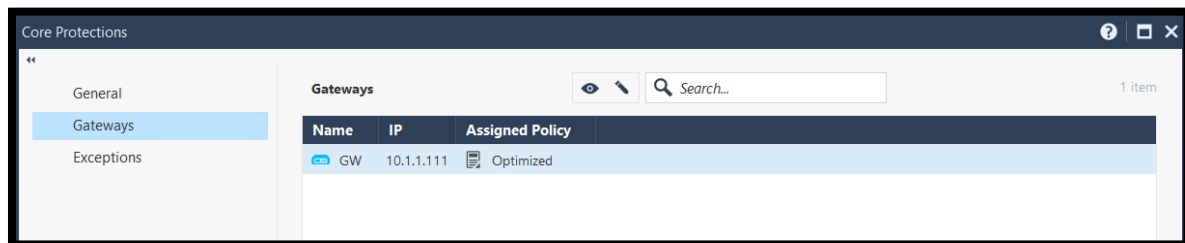
- Review the log and the field of each section.

Log Details		Prevent	
Prevented sql injection scanning attempt originating from 203.0.113.5 against 203.0.113.250			
Details		Matched Rules	
Action		Packet Capture Unique Id	time1731948373.id328f0168.blade02
Access Rule Name	DMZ	Packet Captures	src-203.0.113.5.cap
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-A01C-7847C850D5F3	Packet Capture	
Threat Prevention Policy	Standard	Threat Wiki	Go to Threat Wiki
Policy Date	15 Nov 24, 5:08:27 PM	Advanced Forensics Details	
Threat Prevention Policy D...	Today, 11:45:32 AM	MITRE ATT&CK	
Policy Name	Standard	Initial Access	
Policy Management	SMS	Exploit Public-Facing Application	
Threat Profile	Optimized	Actions	
Origin Log Server IP	10.1.1.100	Remediation	
Add Exception	Add Exception...	Go to Remediation Options	
Protection Details		Report Log	
Severity	<div><div></div></div> Critical	Report Log to Check Point	
Confidence Level	<div><div></div></div> High	More	
Attack Name	Scanner Enforcement Violation	Id	
Attack Information	SQL Injection Scanning Attempt	5b0cc138-b707-b9ff-673b-6f5500000002	
Performance Impact	<div><div></div></div> Medium	Sequencenum	
Protection Name	SQL Injection Scanning Attempt	2	
Protection Type		Description URL	
Industry Reference	CVE-2020-13118	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	
		Lastupdateime	
		1731948373000	

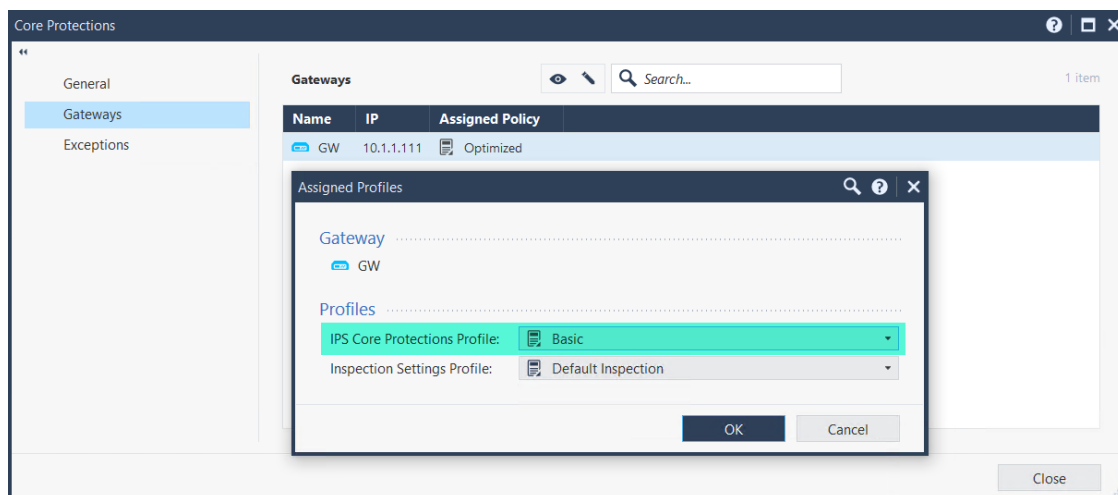
- Open the SQL Protection and review the default action per profile. Notice that the SQL Injection Core Protection is disabled by default in the Basic profile.



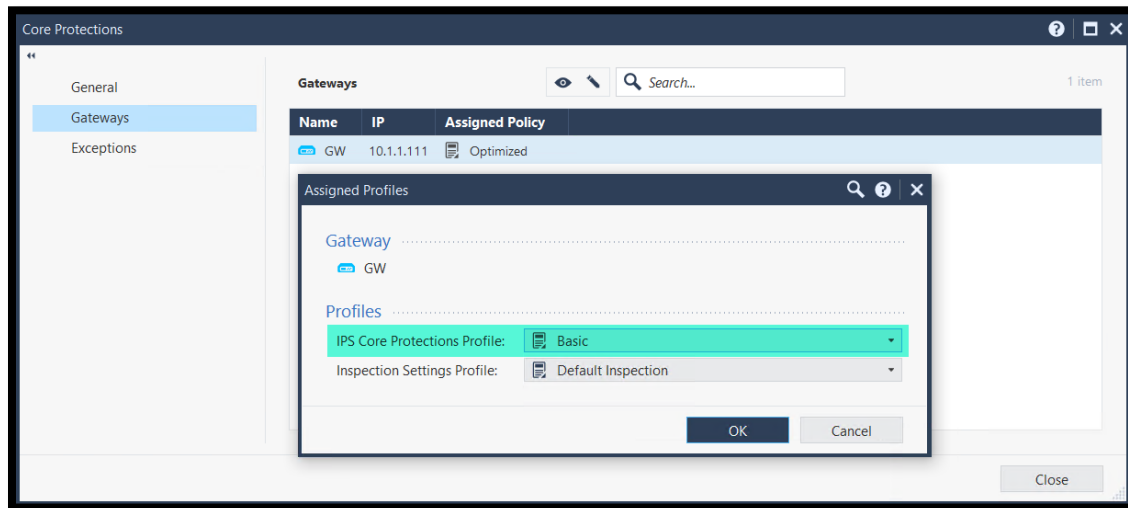
- Move to the Gateways tab and review the default profile settings. Notice that this profile assignment is independent of the profile assigned in the rule base.



- 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.



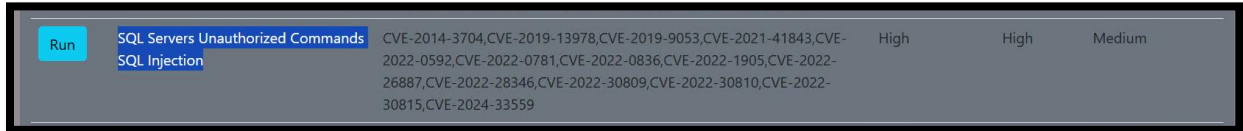
10. Try to trigger the same protection we used before in the demo Server (SQL Scanning attempt)

Attack	Protection Name	Industry	Level	Severity	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-2022-24219,CVE-2022-24220,CVE-2022-24221,CVE-2022-24222,CVE-2022-27412,CVE-2022-34265,CVE-2022-35121,CVE-2022-36669,CVE-2022-47862,CVE-2023-24780	High	Critical	Medium

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

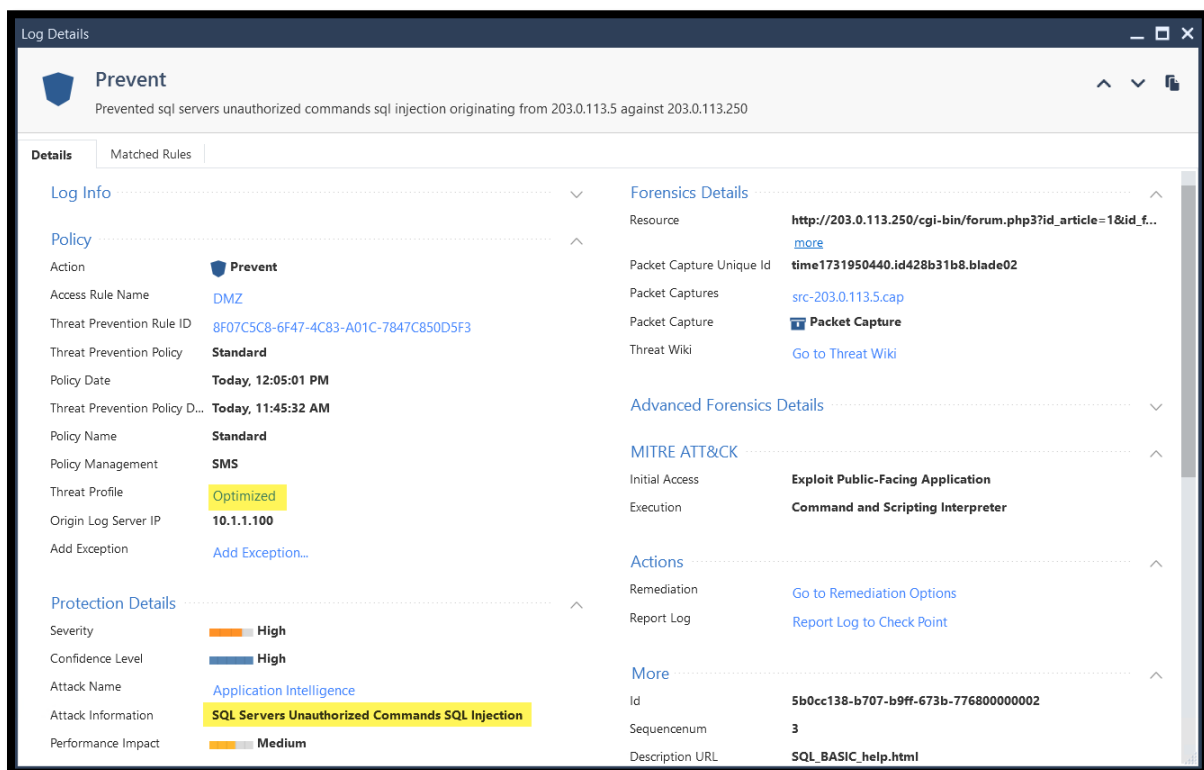
- There will be no new logs since this protection is disabled in the Basic profile which we assigned to the GW.
- Pay extra attention to deactivating protections as it will leave gaps in your security protection.

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

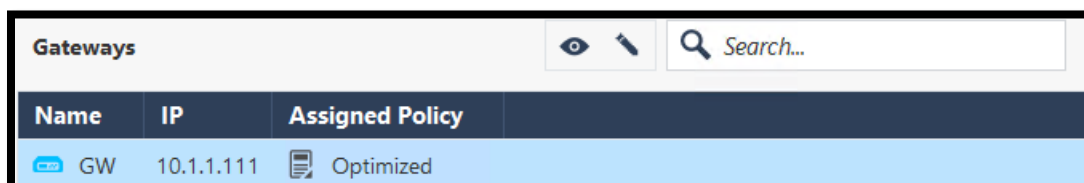


13. Review the logs. Notice that a different protection was triggered. However, this protection is a different SQL injection provided by Threat Cloud.

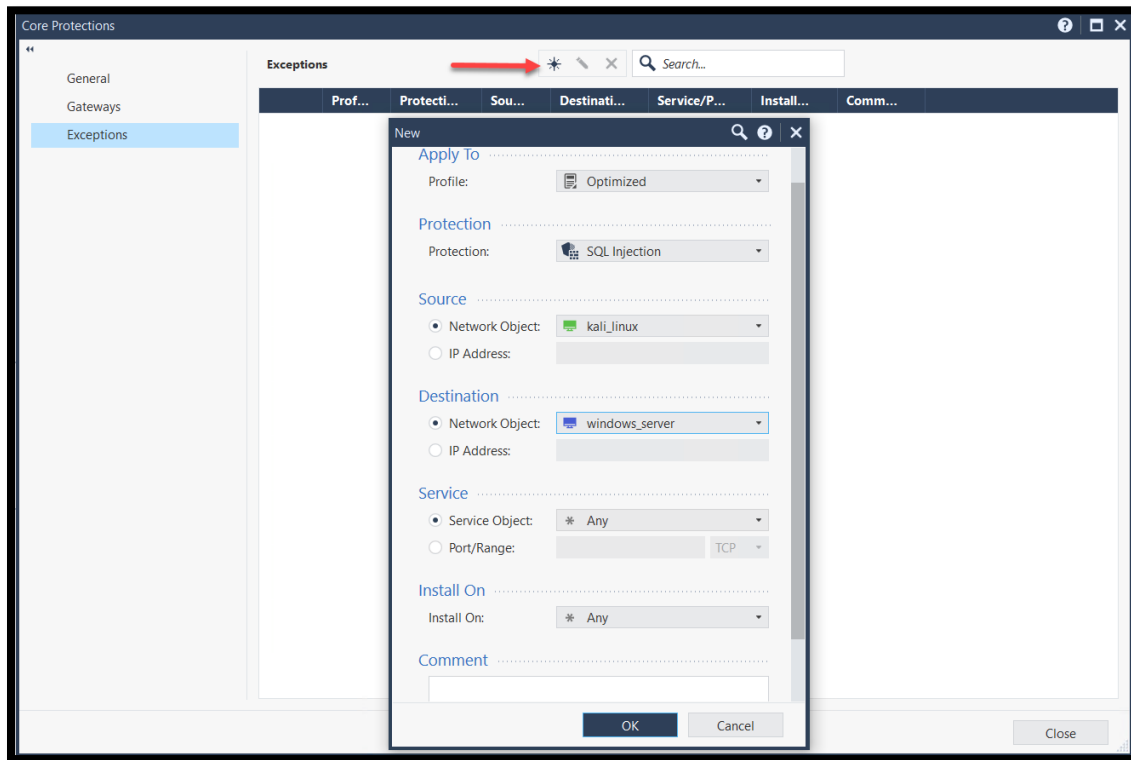
- Check Point provide multiple protections that work in parallel to protect your environment.
- Notice that this protection is managed via the Optimized profile assigned in the rule base and not the Basic profile we assigned to core protections.



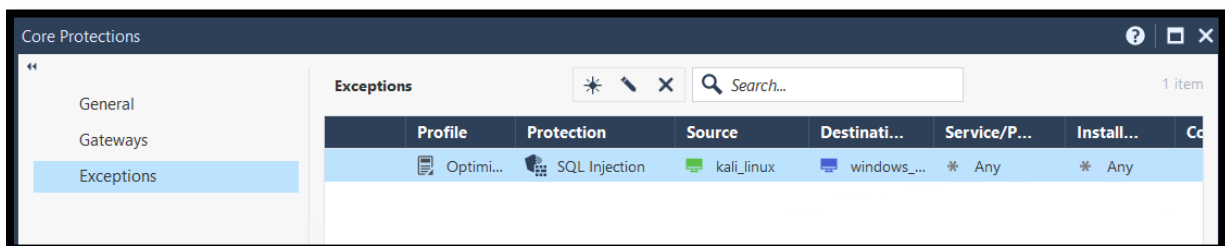
14. Edit the SQLW protection settings and assign the optimized profile.



15. Under the Exception tab, add a new exception to



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



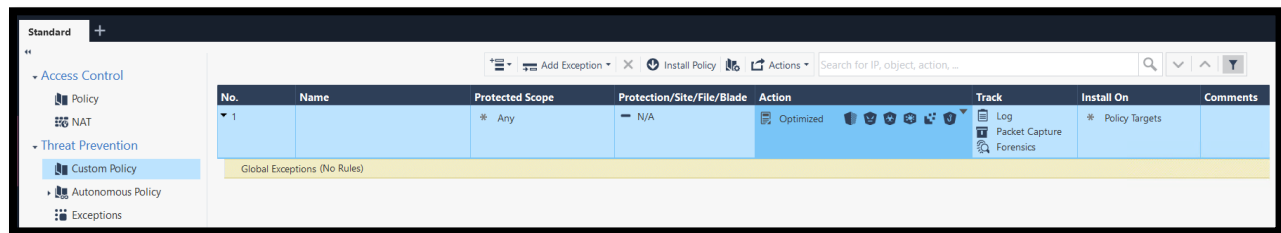
17. Run a new test using the same protection trigger from the demo server.

- 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.
- Similar to the behavior above, Other protection might still drop the traffic as this is a multi-layer protection layer environemnt.

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.

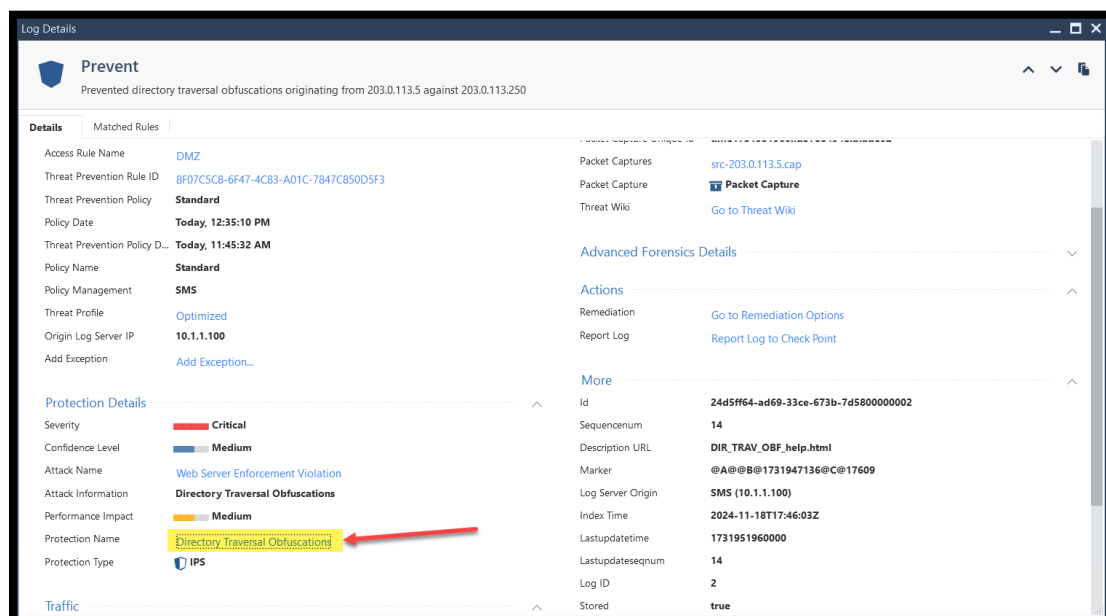
1. Review the default rule in the Threat Prevention Custom policy. Notice that the optimized profile is assigned by default.



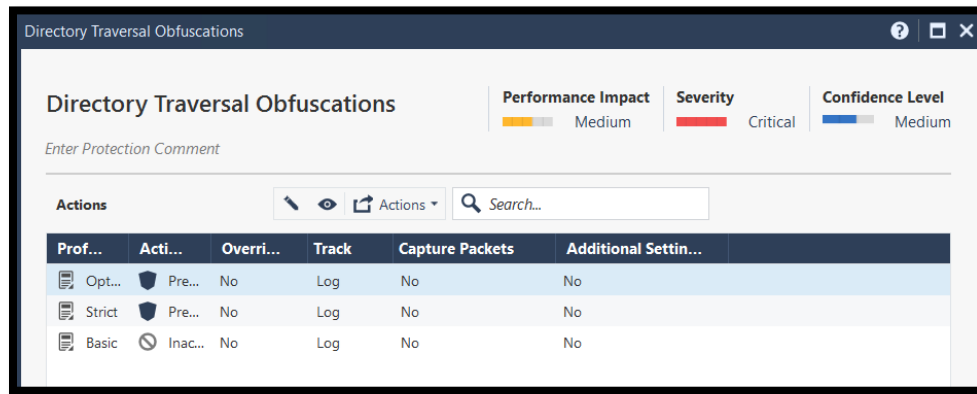
2. From the demo server, trigger the protection “Directory Traversal Obfuscation”

Attack	Protection Name	Industry	Level	Severity	Impact
Run	Apache Tomcat Server Malicious Request Information Disclosure	CVE-2002-2006,CVE-2002-2007,CVE-2002-2008	High	Medium	Medium
Run	Athena Web Registration Command Injection (CVE-2004-1782)	CVE-2004-1782	Medium	High	Medium
Run	AWStats Totals awstatstotal.php sort Parameter Code Execution	CVE-2008-3922	Medium	High	Medium
Run	Directory Traversal Obfuscations		Medium	Critical	Medium

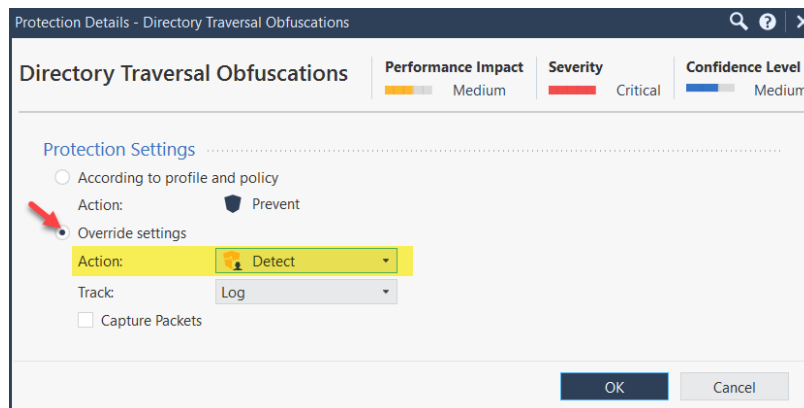
3. Review the log and pay attention to the profile.






- 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.



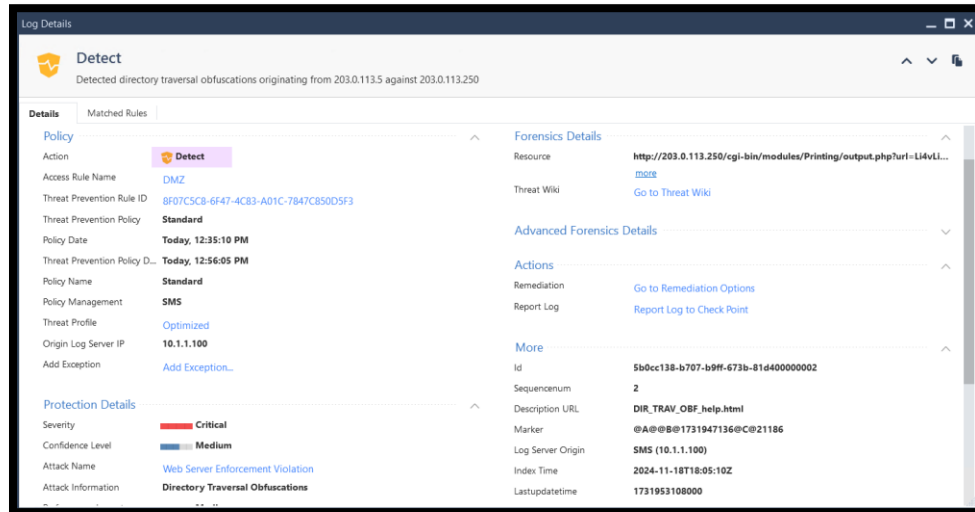
- While Optimized is selected, edit the settings and change the behavior to detect instead of Prevent.



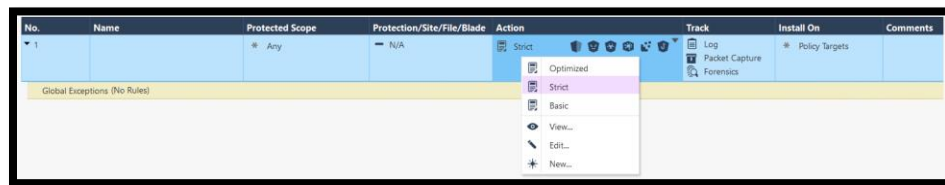
- Confirm the changes and Install the Threat Prevention Policy.

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	

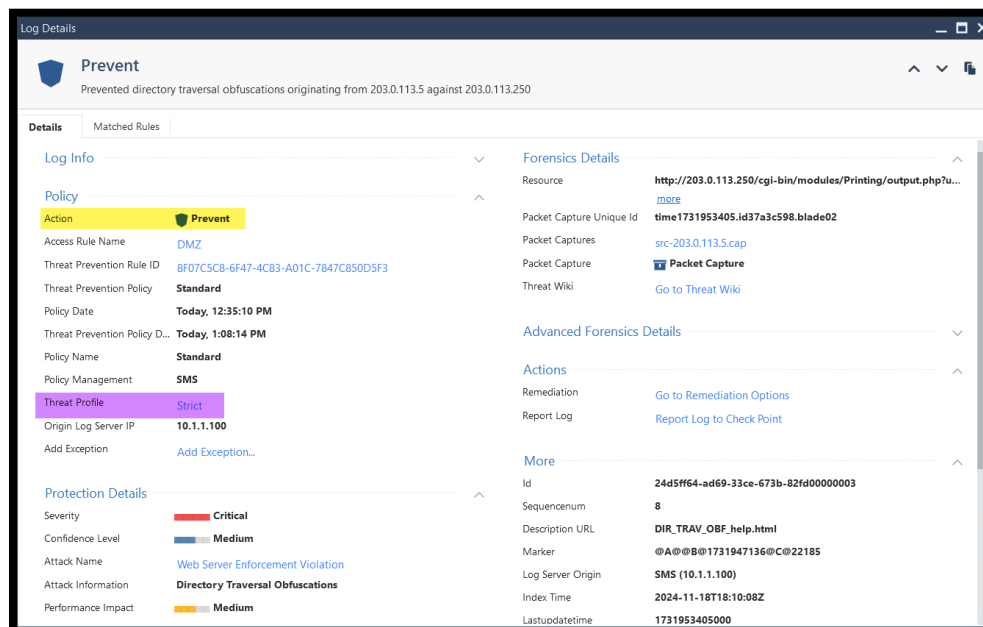
- Trigger the same protection again and review the logs. You should see a detect log. Note that this is only made for the optimized profile. However this applies to all hosts and networks.



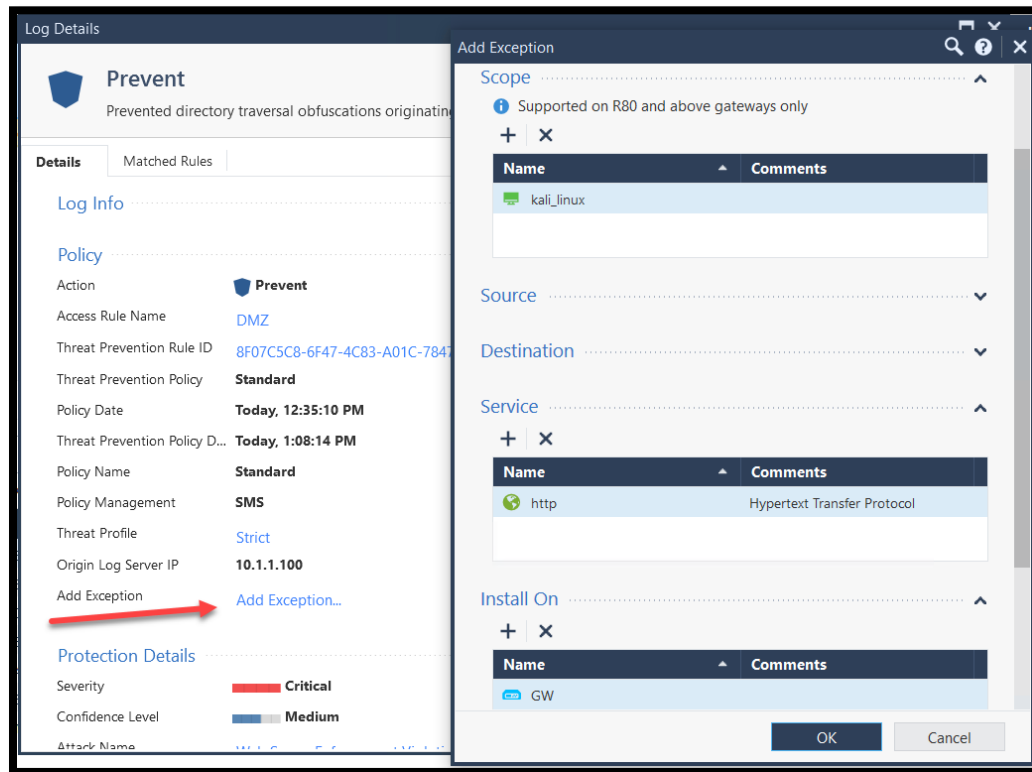
8. Change the profile assigned to the default rule, select the Strict profile and install the Threat Prevention Policy.



9. Trigger the same protection again. Review the logs and notice that the traffic is not prevented by the Strict profile.



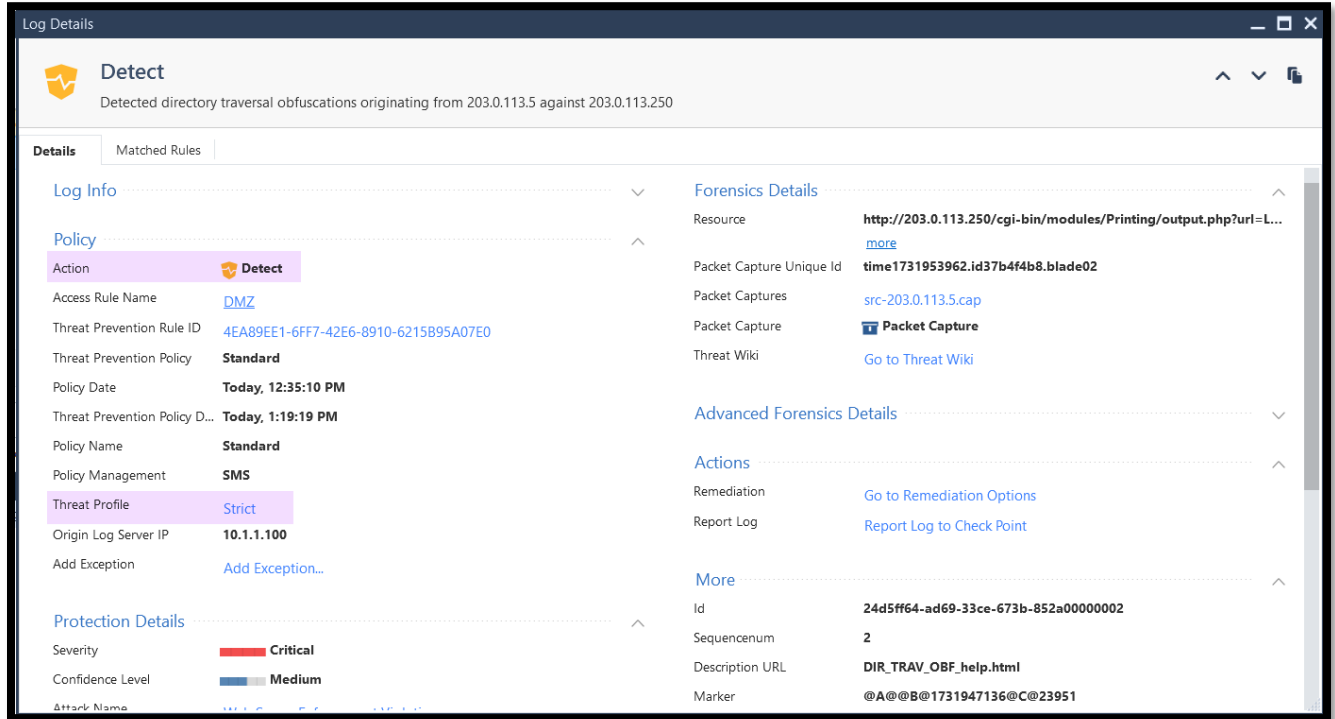
10. Use the Add Exception feature from the log to add an exception to the Rulebase



11. 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	

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



Log Details

Detect
Detected directory traversal obfuscations originating from 203.0.113.5 against 203.0.113.250

Details | Matched Rules

Log Info

Policy

Action: **Detect**

Access Rule Name: **DMZ**

Threat Prevention Rule ID: **4EA89EE1-6FF7-42E6-8910-6215B95A07E0**

Threat Prevention Policy: **Standard**

Policy Date: **Today, 12:35:10 PM**

Threat Prevention Policy D...: **Today, 1:19:19 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**

Forensics Details

Resource: <http://203.0.113.250/cgi-bin/modules/Printing/output.php?url=L...>

Packet Capture Unique Id: **time1731953962.id37b4f4b8.blade02**

Packet Captures: [src-203.0.113.5.cap](#)

Packet Capture: [Packet Capture](#)

Threat Wiki: [Go to Threat Wiki](#)

Advanced Forensics Details

Actions

Remediation: [Go to Remediation Options](#)

Report Log: [Report Log to Check Point](#)

More

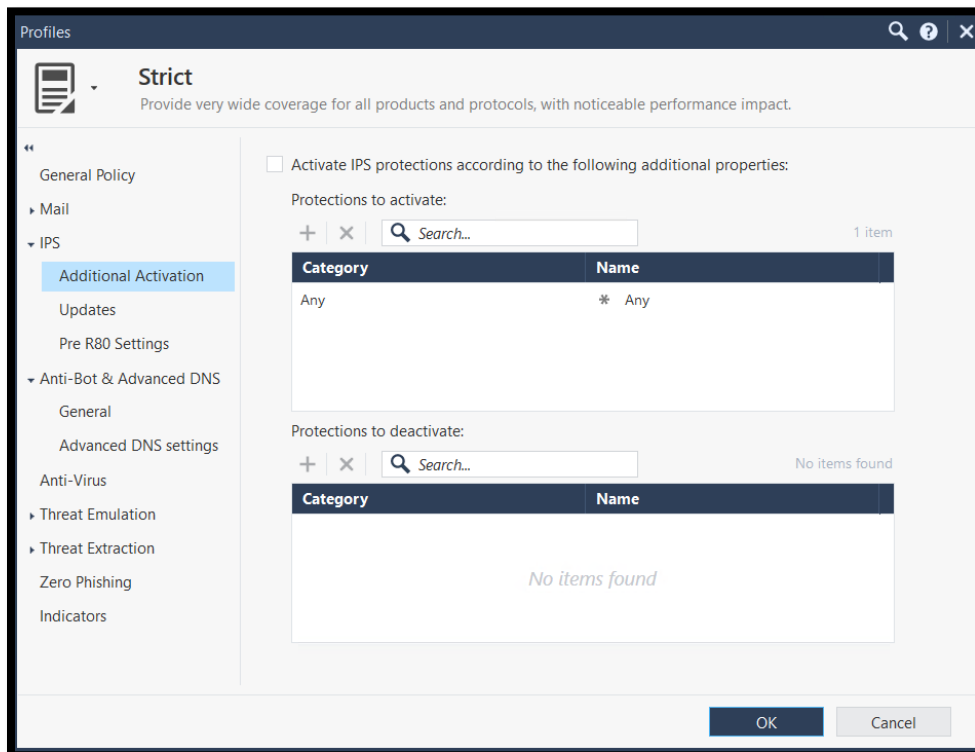
Id: **24d5ff64-ad69-33ce-673b-852a00000002**

Sequencenum: **2**

Description URL: **DIR_TRAV_OBF_help.html**

Marker: **@A@@B@1731947136@C@23951**

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



Profiles

Strict
Provide very wide coverage for all products and protocols, with noticeable performance impact.

General Policy

Mail

IPS

Additional Activation

Updates

Pre R80 Settings

Anti-Bot & Advanced DNS

General

Advanced DNS settings

Anti-Virus

Threat Emulation

Threat Extraction

Zero Phishing

Indicators

☐ Activate IPS protections according to the following additional properties:

Protections to activate:

+ × Search... 1 item

Category	Name
Any	* Any

Protections to deactivate:

+ × Search... No items found

Category	Name
No items found	

OK **Cancel**

End of Lab 5