Intrusion Prevention System (IPS)

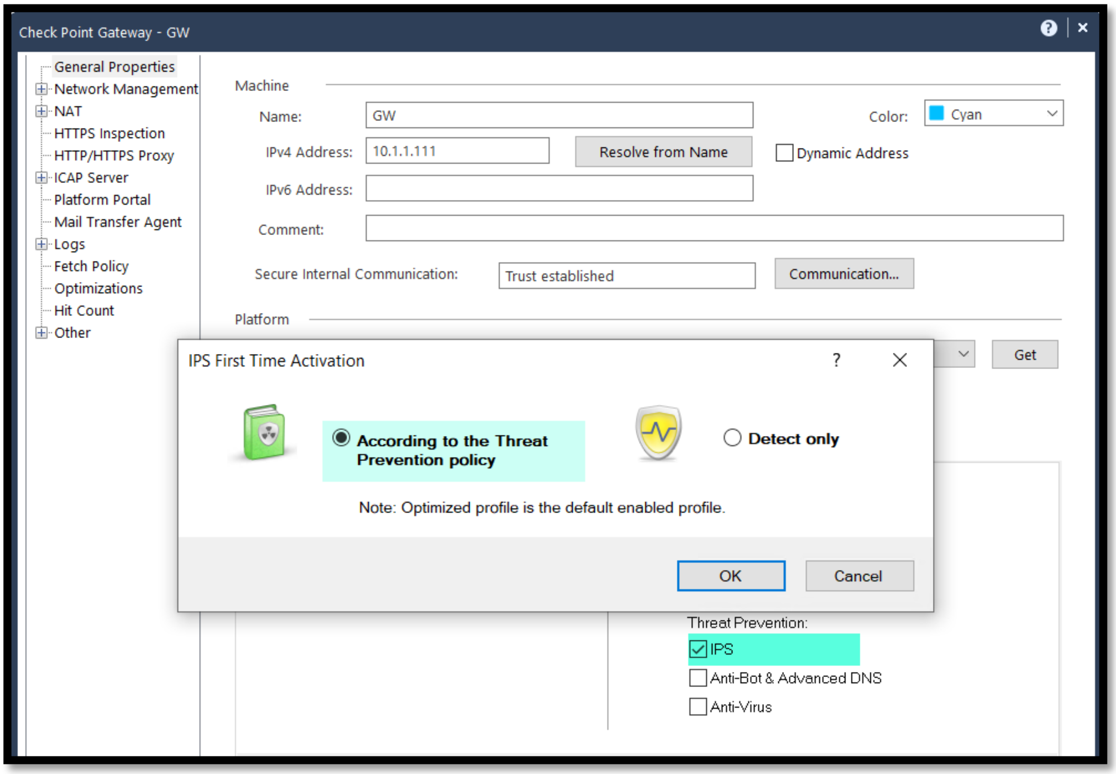
Introduction

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.



Machine

Name: GW

Color: Cyan

IPv4 Address: 10.1.1.111

☐ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

IPS First Time Activation

● According to the Threat Prevention policy

○ Detect only

Note: Optimized profile is the default enabled profile.

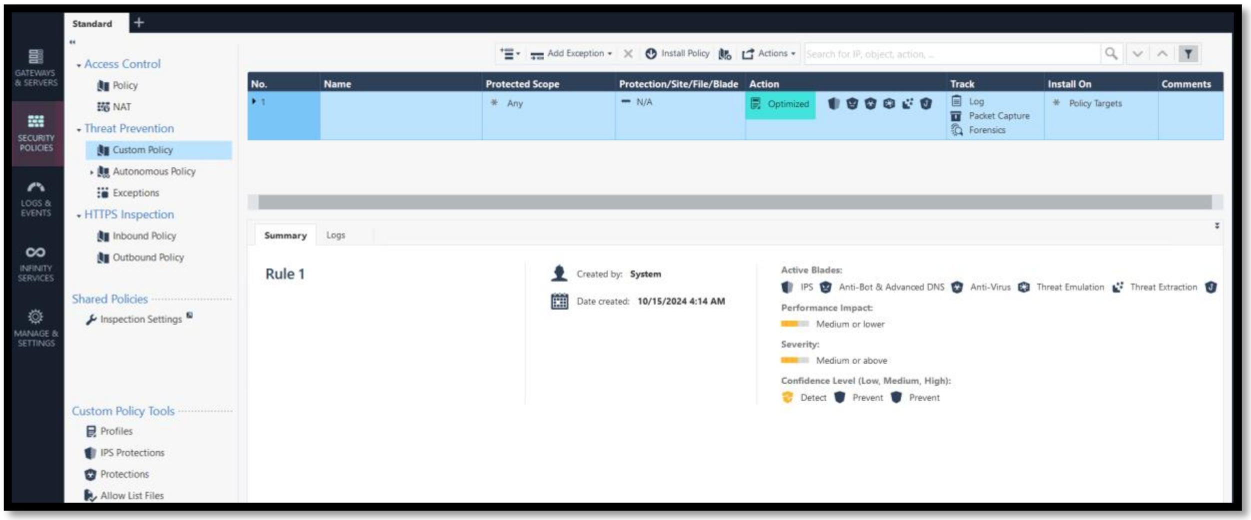
Threat Prevention:

☑ IPS

☐ Anti-Bot & Advanced DNS

☐ Anti-Virus

2. Under the Custom **Threat Prevention** Policy. Notice that the **Optimized** profile is assigned by default. It is customized 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	

Rule 1

Created by: **System**
Date created: **10/15/2024 4:14 AM**

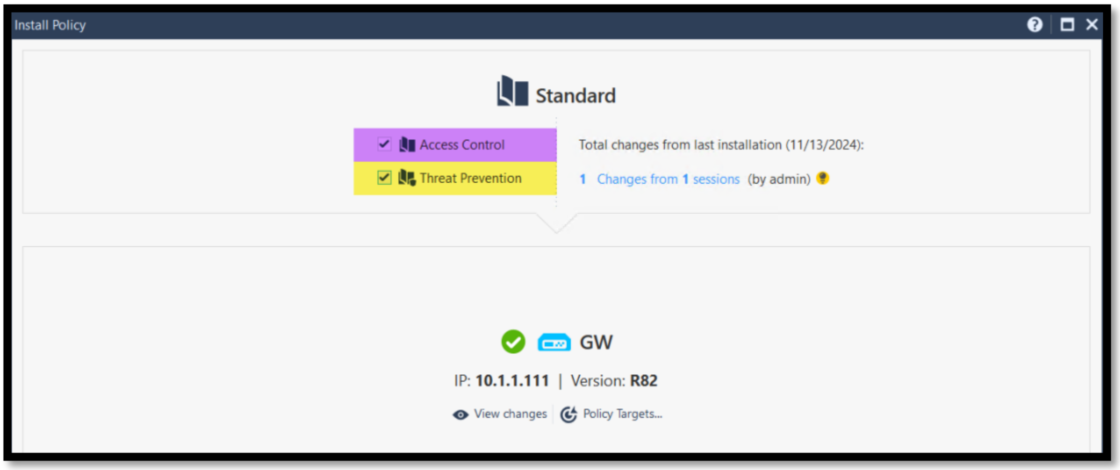
Active Blades:
IPS Anti-Bot & Advanced DNS Anti-Virus Threat Emulation Threat Extraction

Performance Impact:
Medium or lower

Severity:
Medium or above

Confidence Level (Low, Medium, High):
Detect Prevent Prevent

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



Standard

☑ Access Control
☑ Threat Prevention

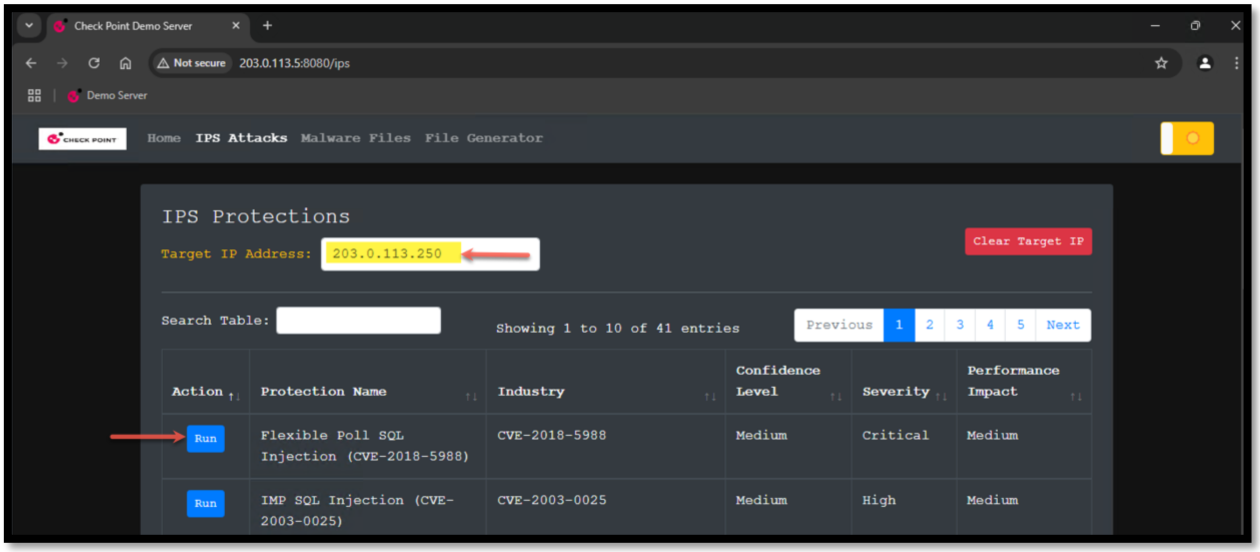
Total changes from last installation (11/13/2024):
1 Changes from 1 sessions (by admin)

GW
IP: **10.1.1.111** | Version: **R82**

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.



IPS Protections

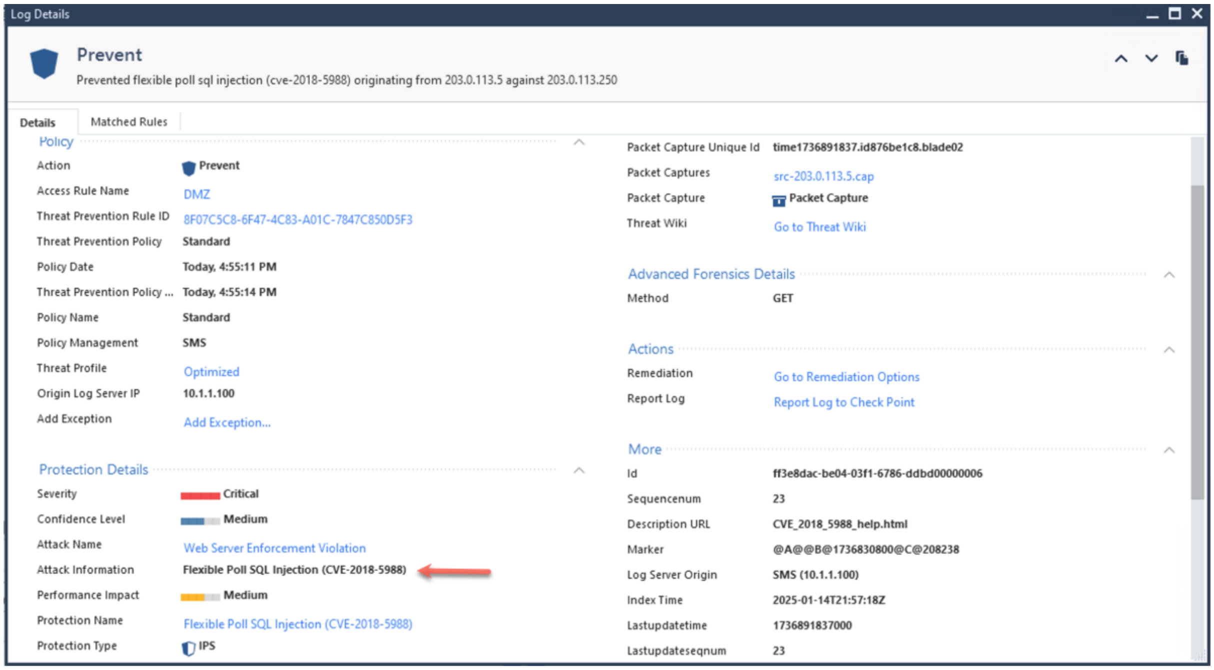
Target IP Address: 203.0.113.250

Search Table:

Showing 1 to 10 of 41 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.



Prevent

Prevented flexible poll sql injection (cve-2018-5988) originating from 203.0.113.5 against 203.0.113.250

Policy

Action	Prevent
Access Rule Name	DMZ
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-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...

Protection Details

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

Packet Capture Unique Id	time1736891837.id876be1c8.blade02
Packet Captures	src-203.0.113.5.cap
Packet Capture	Packet Capture
Threat Wiki	Go to Threat Wiki

Advanced Forensics Details

Method	GET

Actions

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

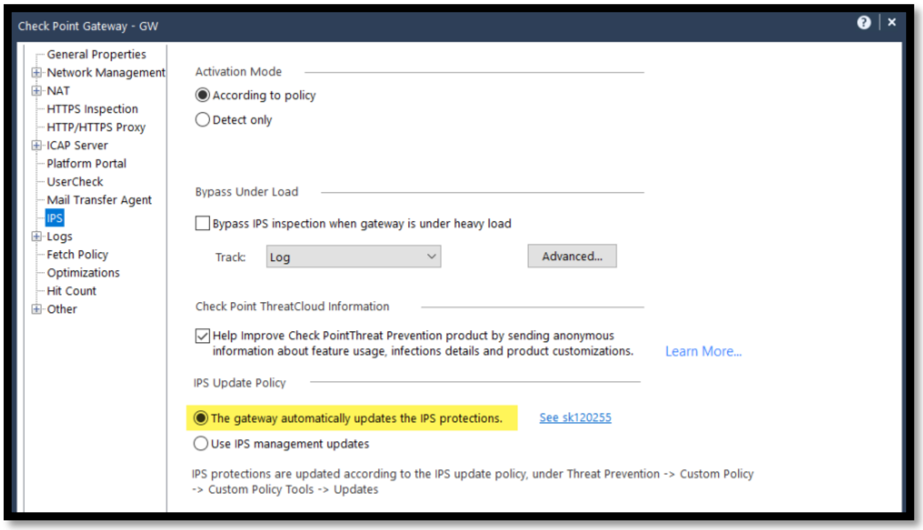
More

Id	ff3e8dac-be04-03f1-6786-ddbd00000006
Sequencenum	23
Description URL	CVE_2018_5988_help.html
Marker	@A@@B@1736830800@C@208238
Log Server Origin	SMS (10.1.1.100)
Index Time	2025-01-14T21:57:18Z
Lastupdatetime	1736891837000
Lastupdateseqnum	23

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.



Activation Mode
● According to policy
○ Detect only

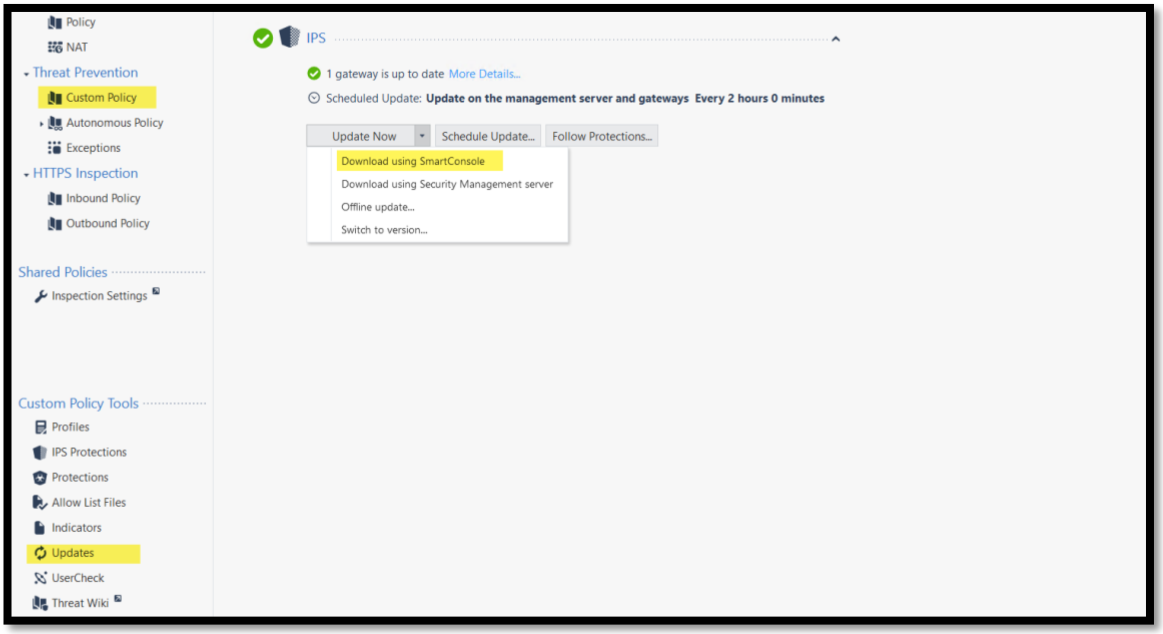
Bypass Under Load
□ Bypass IPS inspection when gateway is under heavy load
Track: Log

Check Point ThreatCloud Information
☑ Help Improve Check PointThreat Prevention product by sending anonymous information about feature usage, infections details and product customizations.

IPS Update Policy
● The gateway automatically updates the IPS protections.
○ Use IPS management updates

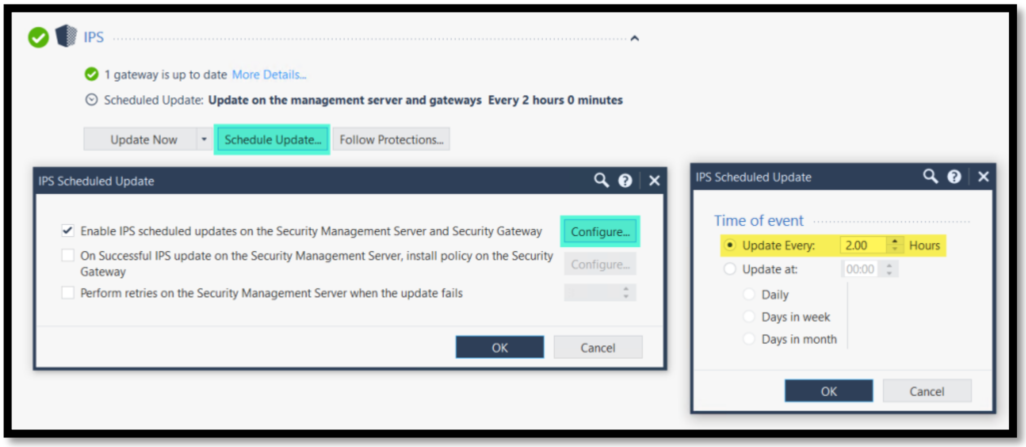
IPS protections are updated according to the IPS update policy, under Threat Prevention -> Custom Policy -> Custom Policy Tools -> Updates

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



1 gateway is up to date More Details...
Scheduled Update: **Update on the management server and gateways Every 2 hours 0 minutes**

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



IPS

1 gateway is up to date More Details...

Scheduled Update: **Update on the management server and gateways Every 2 hours 0 minutes**

☑ Enable IPS scheduled updates on the Security Management Server and Security Gateway

☐ On Successful IPS update on the Security Management Server, install policy on the Security Gateway

☐ Perform retries on the Security Management Server when the update fails

Time of event

● Update Every: 2.00 Hours

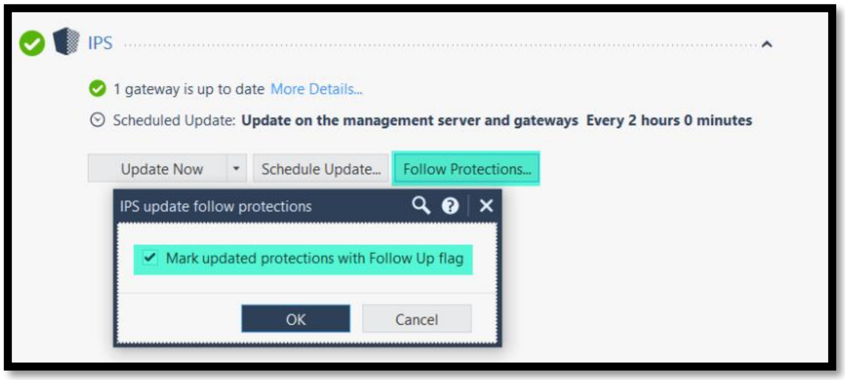
○ Update at: 00:00

○ Daily

○ Days in week

○ Days in month

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



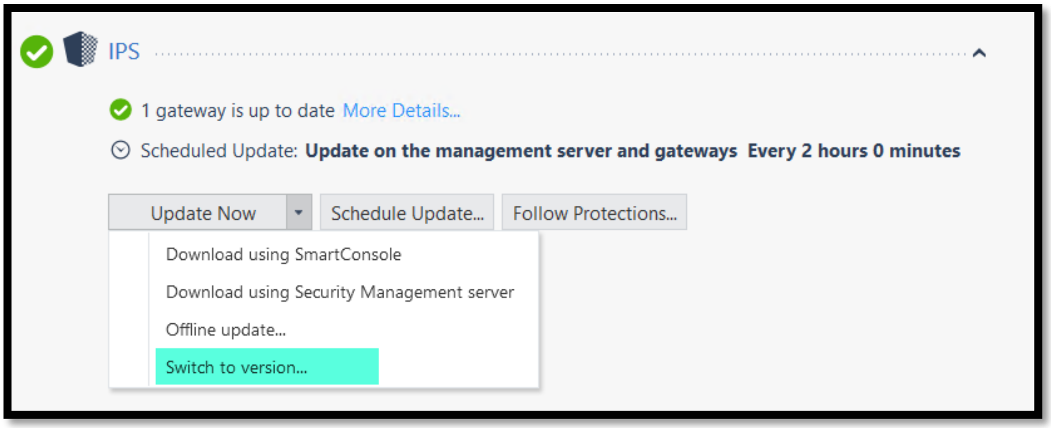
IPS

1 gateway is up to date More Details...

Scheduled Update: **Update on the management server and gateways Every 2 hours 0 minutes**

☑ Mark updated protections with Follow Up flag

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

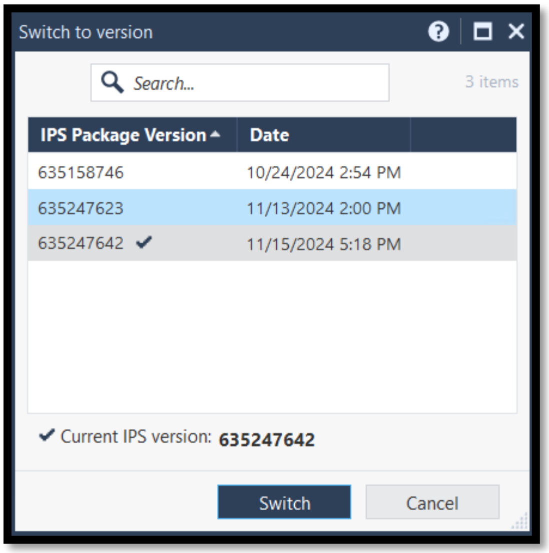


IPS

1 gateway is up to date More Details...

Scheduled Update: **Update on the management server and gateways Every 2 hours 0 minutes**

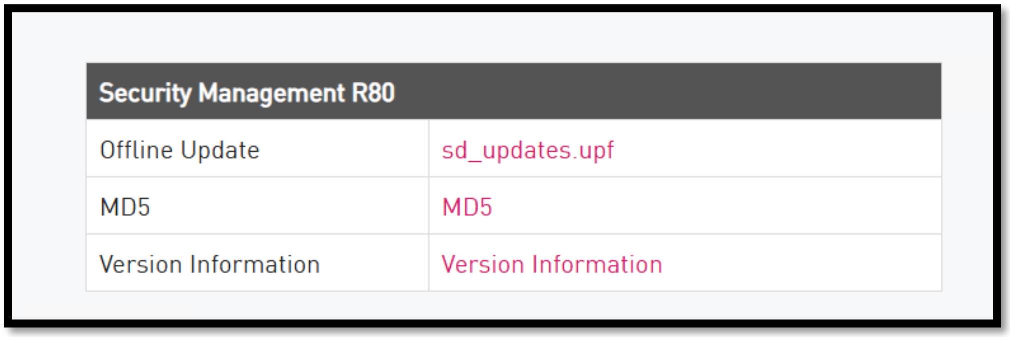
6. From the list of versions, select the version to revert to and click Switch.



IPS Package Version ▲	Date
635158746	10/24/2024 2:54 PM
635247623	11/13/2024 2:00 PM
635247642 ✓	11/15/2024 5:18 PM

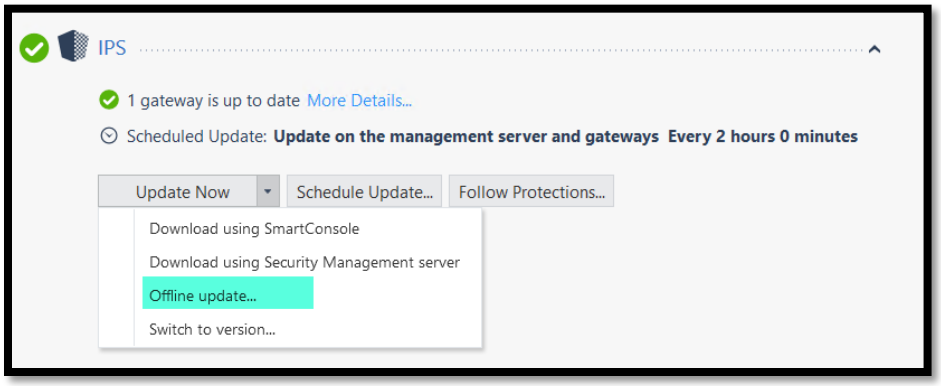
✓ Current IPS version: **635247642**

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

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



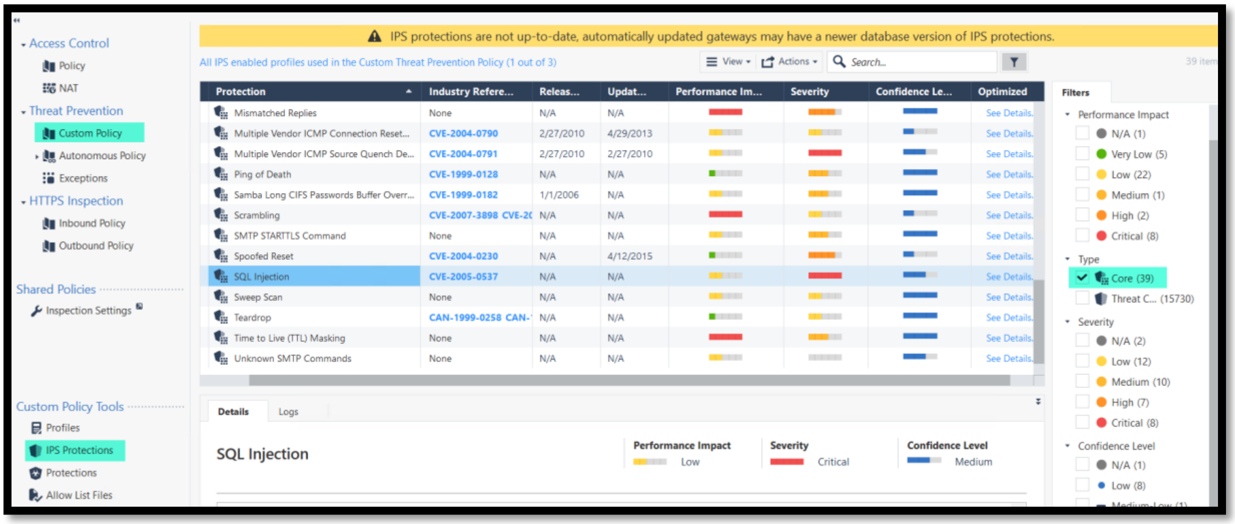
1 gateway is up to date More Details...

Scheduled Update: **Update on the management server and gateways Every 2 hours 0 minutes**

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.



⚠ IPS protections are not up-to-date, automatically updated gateways may have a newer database version of IPS protections.

All IPS enabled profiles used in the Custom Threat Prevention Policy (1 out of 3)

39 item

Protection	Industry Refere...	Releas...	Updat...	Performance Im...	Severity	Confidence Le...	Optimized
Mismatched Replies	None	N/A	N/A				See Details.
Multiple Vendor ICMP Connection Reset...	CVE-2004-0790	2/27/2010	4/29/2013				See Details.
Multiple Vendor ICMP Source Quench De...	CVE-2004-0791	2/27/2010	2/27/2010				See Details.
Ping of Death	CVE-1999-0128	N/A	N/A				See Details.
Samba Long CIFS Passwords Buffer Overr...	CVE-1999-0182	1/1/2006	N/A				See Details.
Scrambling	CVE-2007-3898 CVE-2(	N/A	N/A				See Details.
SMTP STARTTLS Command	None	N/A	N/A				See Details.
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.

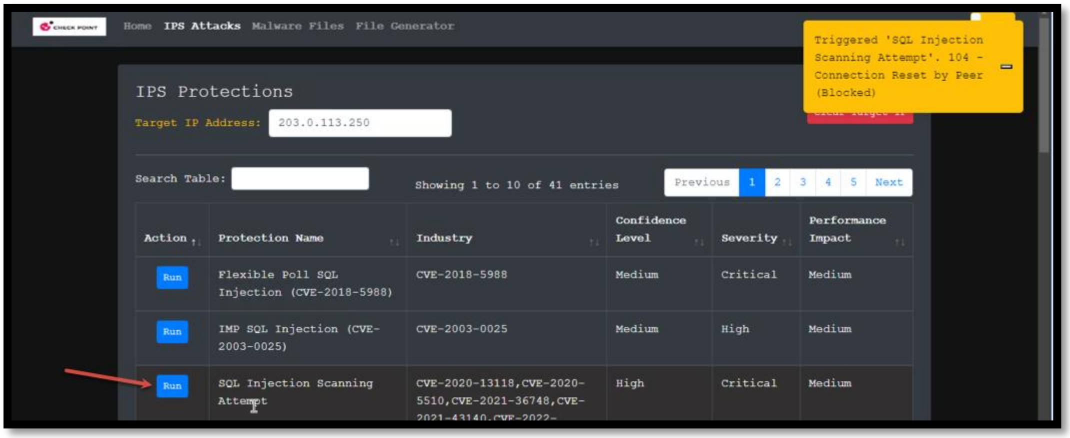
SQL Injection

Performance Impact: Low
Severity: Critical
Confidence Level: Medium

Filters

- Performance Impact
  - □ N/A (1)
  - □ Very Low (5)
  - □ Low (22)
  - □ Medium (1)
  - □ High (2)
  - □ Critical (8)
- Type
  - ☑ Core (39)
  - □ Threat C... (15730)
- Severity
  - □ N/A (2)
  - □ Low (12)
  - □ Medium (10)
  - □ High (7)
  - □ Critical (8)
- Confidence Level
  - □ N/A (1)
  - □ Low (8)
  - □ Medium-Low (1)

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



Triggered 'SQL Injection Scanning Attempt'. 104 - Connection Reset by Peer (Blocked)

IPS Protections

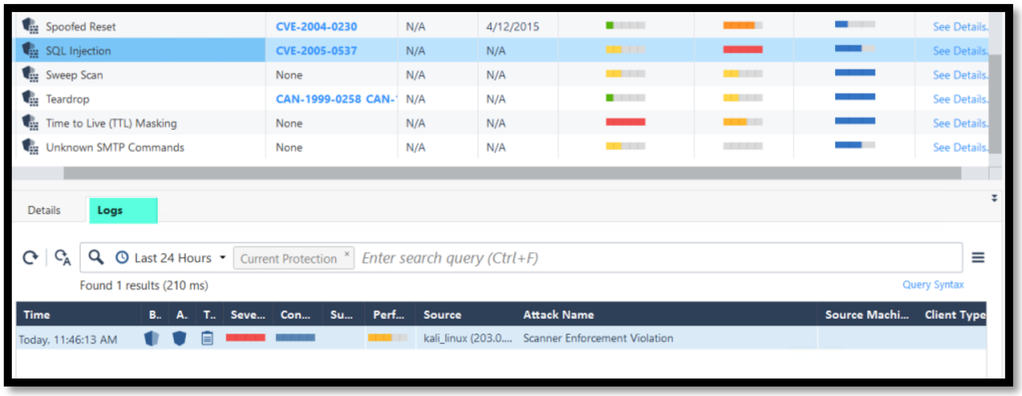
Target IP Address: 203.0.113.250

Search Table:

Showing 1 to 10 of 41 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
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.

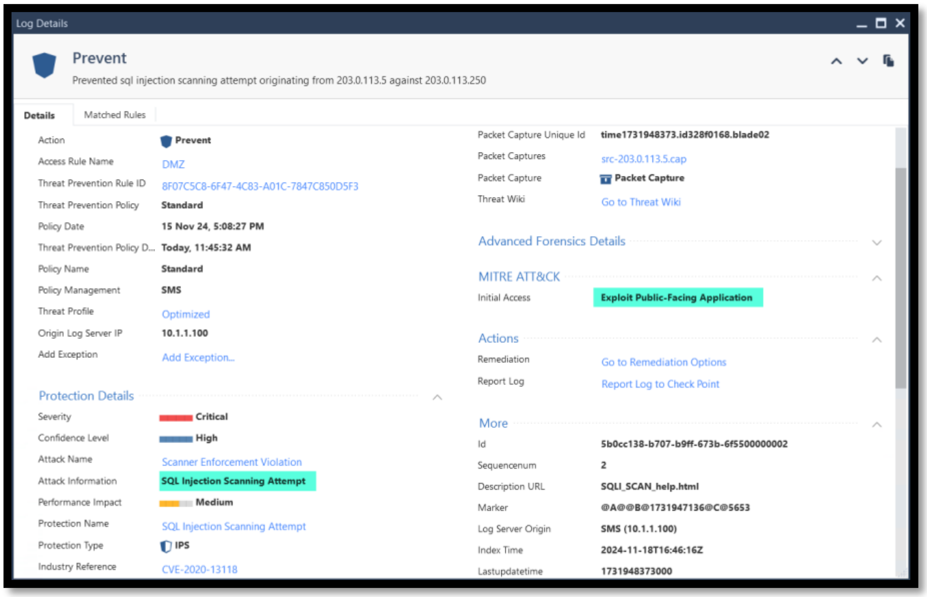


Spoofed Reset	CVE-2004-0230	N/A	4/12/2015	See Details.
SQL Injection	CVE-2005-0537	N/A	N/A	See Details.
Sweep Scan	None	N/A	N/A	See Details.
Teardrop	CAN-1999-0258 CAN-`	N/A	N/A	See Details.
Time to Live (TTL) Masking	None	N/A	N/A	See Details.
Unknown SMTP Commands	None	N/A	N/A	See Details.

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		

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



Prevent

Prevented sql injection scanning attempt originating from 203.0.113.5 against 203.0.113.250

Action	Prevent
Access Rule Name	DMZ
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-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

Packet Capture Unique Id	time1731948373.id328f0168.blade02
Packet Captures	src-203.0.113.5.cap
Packet Capture	Packet Capture
Threat Wiki	Go to Threat Wiki

Advanced Forensics Details

MITRE ATT&CK

Initial Access	Exploit Public-Facing Application

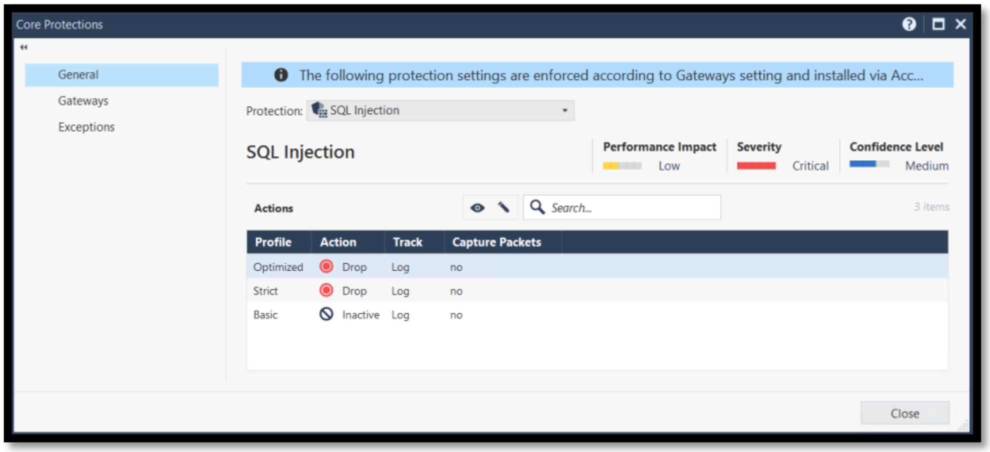
Actions

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

More

Id	5b0cc138-b707-b9ff-673b-6f5500000002
Sequencenum	2
Description URL	SQLI_SCAN_help.html
Marker	@A@@B@1731947136@C@5653
Log Server Origin	SMS (10.1.1.100)
Index Time	2024-11-18T16:46:16Z
Lastupdatedatetime	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 following protection settings are enforced according to Gateways setting and installed via Acc...

Protection: SQL Injection

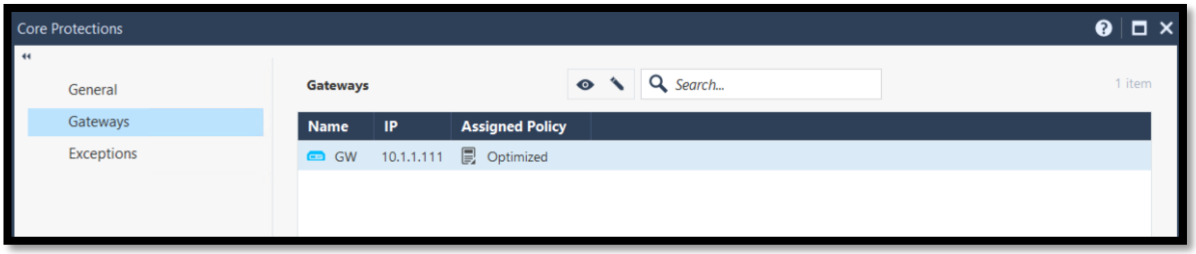
SQL Injection

Performance Impact	Severity	Confidence Level
Low	Critical	Medium

Actions

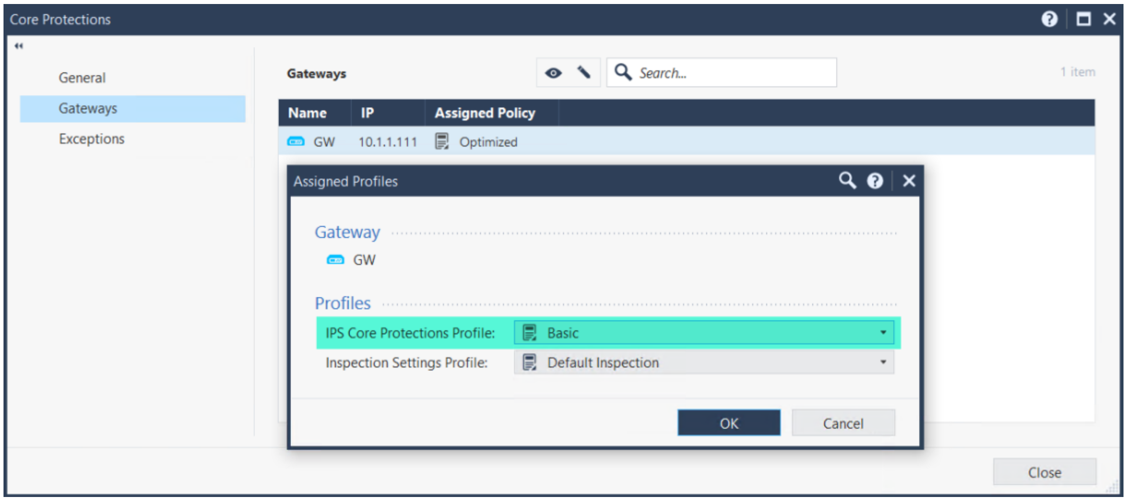
Profile	Action	Track	Capture Packets
Optimized	Drop	Log	no
Strict	Drop	Log	no
Basic	Inactive	Log	no

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.



Name	IP	Assigned Policy
GW	10.1.1.111	Optimized

7. Edit the selection and select the Basic profile

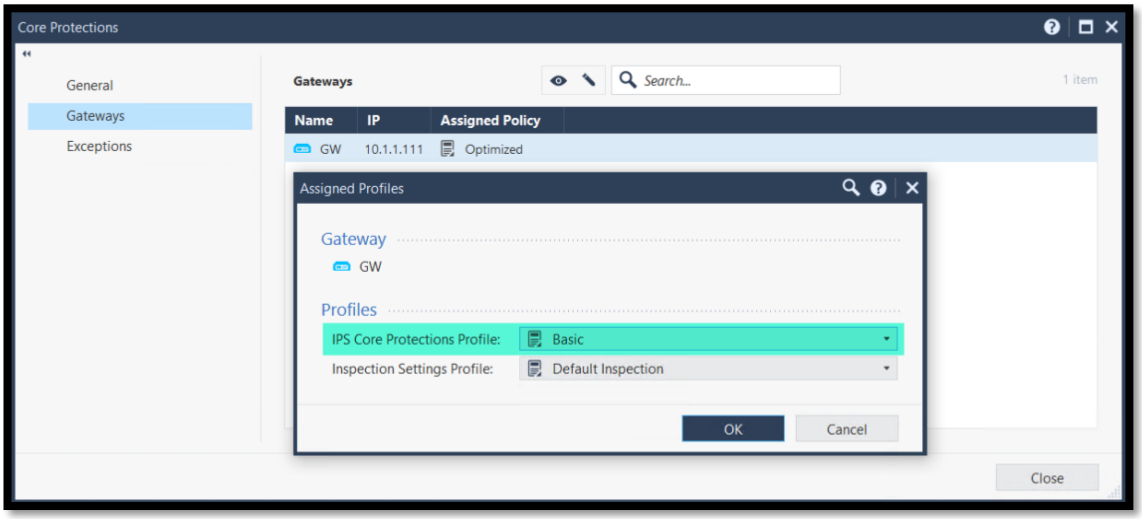


Name	IP	Assigned Policy
GW	10.1.1.111	Optimized

IPS Core Protections Profile: Basic

Inspection Settings Profile: Default Inspection

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

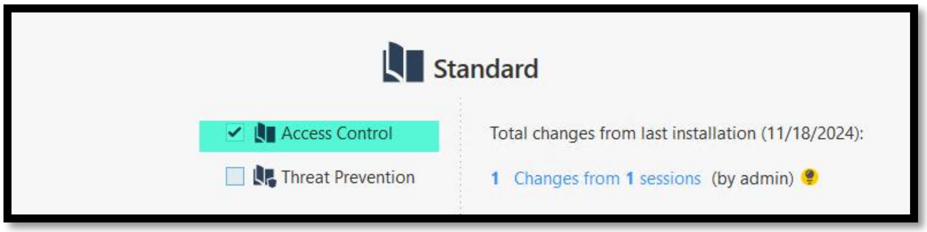


Name	IP	Assigned Policy
GW	10.1.1.111	Optimized

IPS Core Protections Profile: Basic

Inspection Settings Profile: Default Inspection

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



Standard

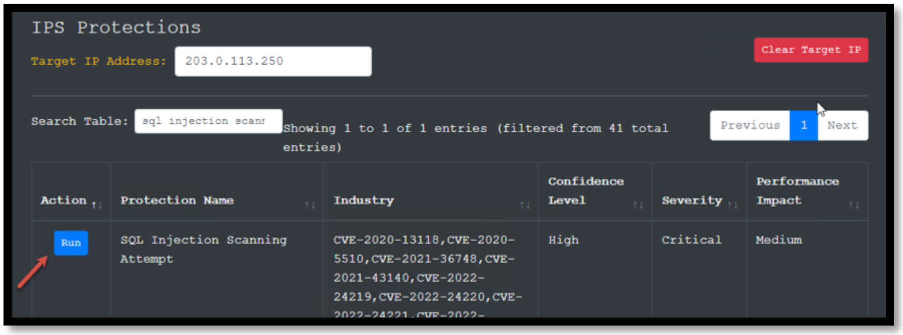
☑ Access Control

□ Threat Prevention

Total changes from last installation (11/18/2024):

1 Changes from 1 sessions (by admin)

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 scanr

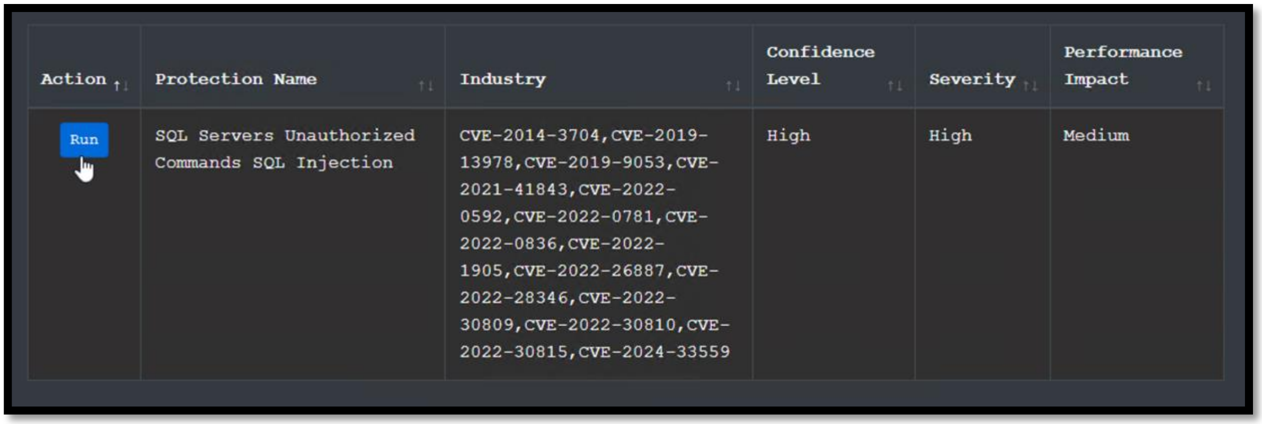
Showing 1 to 1 of 1 entries (filtered from 41 total entries)

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.

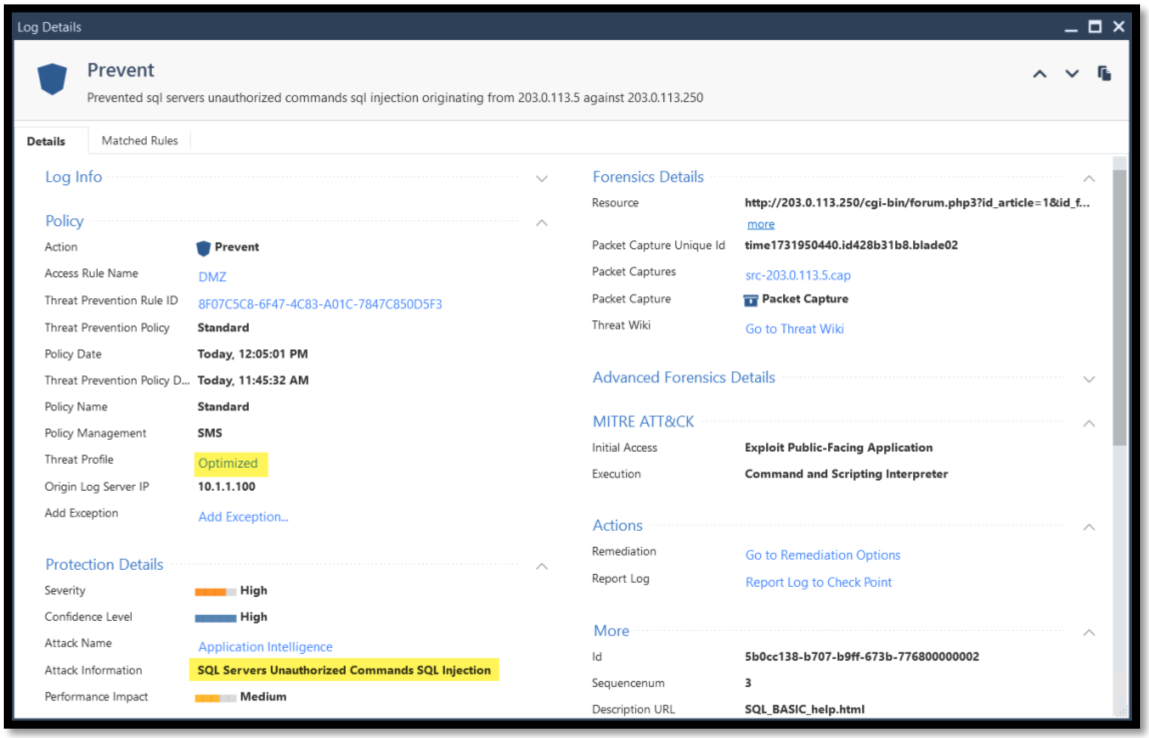
12. Run a different attack, this time trigger the protection **SQL Servers Unauthorized Commands SQL Injection**.



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.



Log Details

Prevent
Prevented sql servers unauthorized commands sql injection originating from 203.0.113.5 against 203.0.113.250

Log Info

Policy

Action	Prevent
Access Rule Name	DMZ
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-A01C-7847C850D5F3
Threat Prevention Policy	Standard
Policy Date	Today, 12:05:01 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	High
Confidence Level	High
Attack Name	Application Intelligence
Attack Information	SQL Servers Unauthorized Commands SQL Injection
Performance Impact	Medium

Forensics Details

Resource	http://203.0.113.250/cgi-bin/forum.php3?id_article=1&id_f... more
Packet Capture Unique Id	time1731950440.id428b31b8.blade02
Packet Captures	src-203.0.113.5.cap
Packet Capture	Packet Capture
Threat Wiki	Go to Threat Wiki

Advanced Forensics Details

MITRE ATT&CK

Initial Access	Exploit Public-Facing Application
Execution	Command and Scripting Interpreter

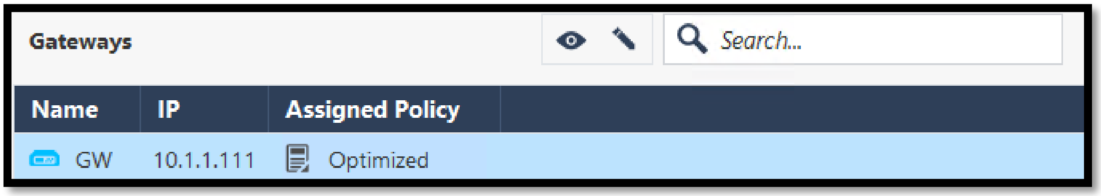
Actions

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

More

Id	5b0cc138-b707-b9ff-673b-776800000002
Sequencenum	3
Description URL	SQL_BASIC_help.html

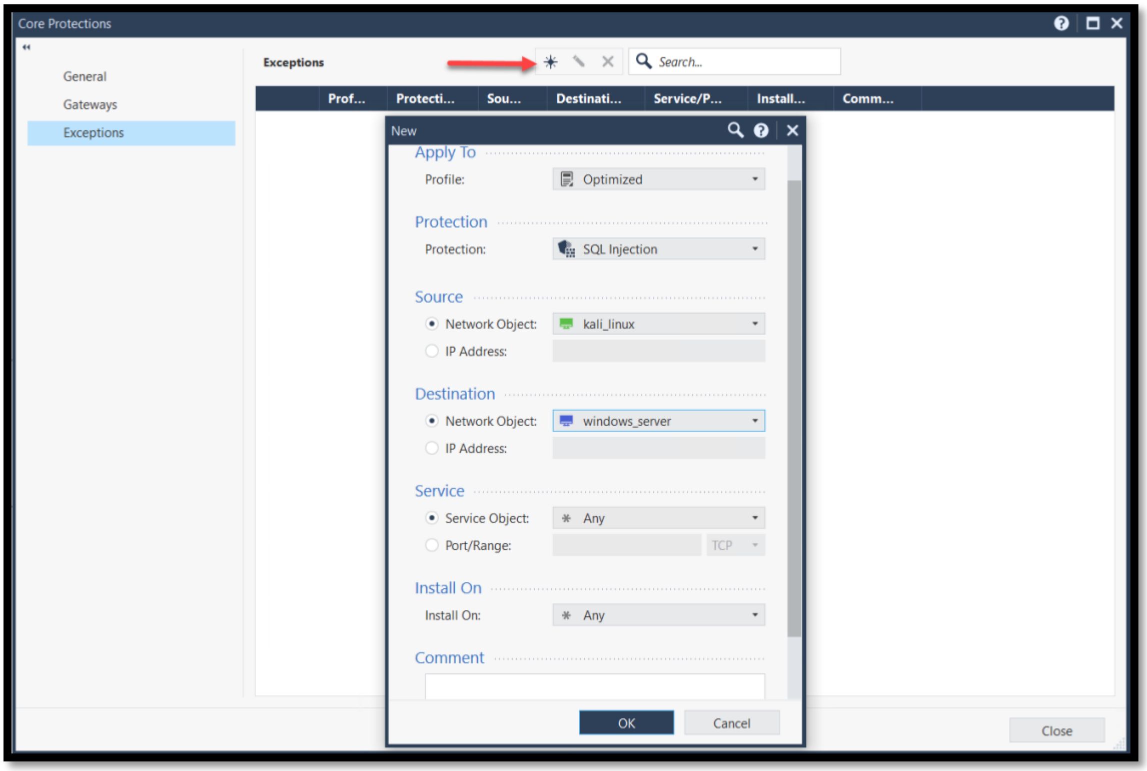
14. Edit the SQL protection settings and assign the **Optimized Profile**.



Gateways

Name	IP	Assigned Policy
GW	10.1.1.111	Optimized

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


Core Protections
General
Gateways
Exceptions
Search...
Prof... | Protecti... | Sou... | Destinati... | Service/P... | Install... | Comm...
New
OK
Cancel
Close

Apply To

Profile: Optimized

Protection

Protection: SQL Injection

Source

● Network Object: kali_linux

○ IP Address:

Destination

● Network Object: windows_server

○ IP Address:

Service

● Service Object: Any

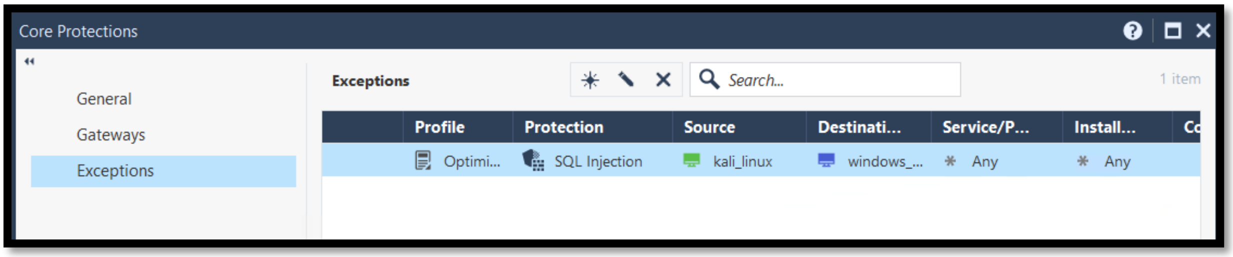
○ Port/Range: TCP

Install On

Install On: Any

Comment

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



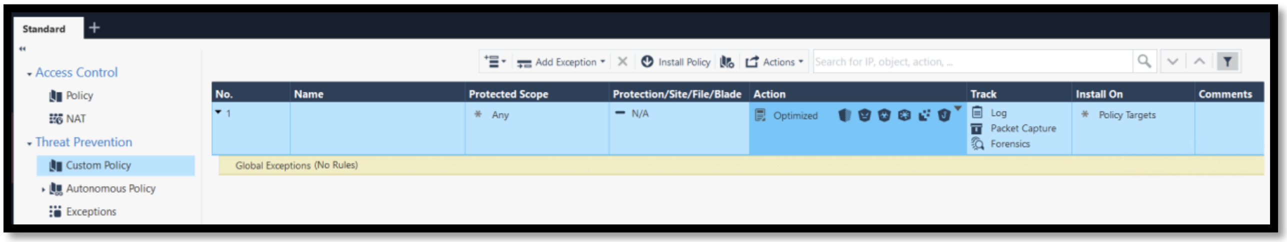
Profile	Protection	Source	Destinati...	Service/P...	Install...	Co
Optimi...	SQL Injection	kali_linux	windows_...	Any	Any	

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.

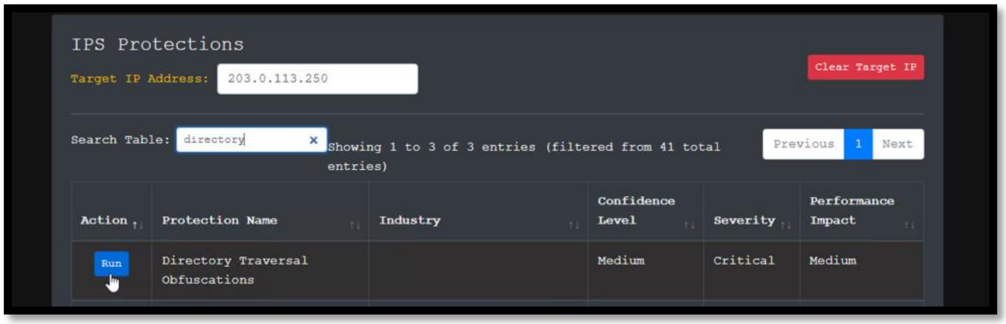
1. Review the default rule In the Threat Prevention Custom policy. Notice that the optimized profile is assigned by default.



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

Global Exceptions (No Rules)

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



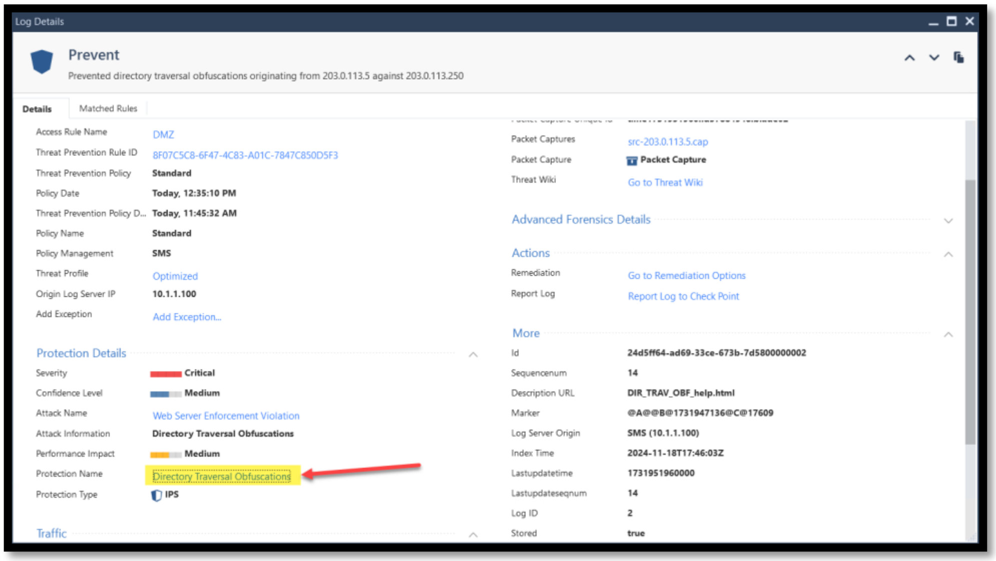
Target IP Address: 203.0.113.250

Search Table: directory

Showing 1 to 3 of 3 entries (filtered from 41 total entries)

Action	Protection Name	Industry	Confidence Level	Severity	Performance Impact
Run	Directory Traversal Obfuscations		Medium	Critical	Medium

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



Prevent

Prevented directory traversal obfuscations originating from 203.0.113.5 against 203.0.113.250

Access Rule Name	DMZ
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-A01C-7847C850D5F3
Threat Prevention Policy	Standard
Policy Date	Today, 12:35:10 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	Medium
Attack Name	Web Server Enforcement Violation
Attack Information	Directory Traversal Obfuscations
Performance Impact	Medium
Protection Name	Directory Traversal Obfuscations
Protection Type	IPS

Traffic

Packet Captures	src-203.0.113.5.cap
Packet Capture	Packet Capture
Threat Wiki	Go to Threat Wiki

Advanced Forensics Details

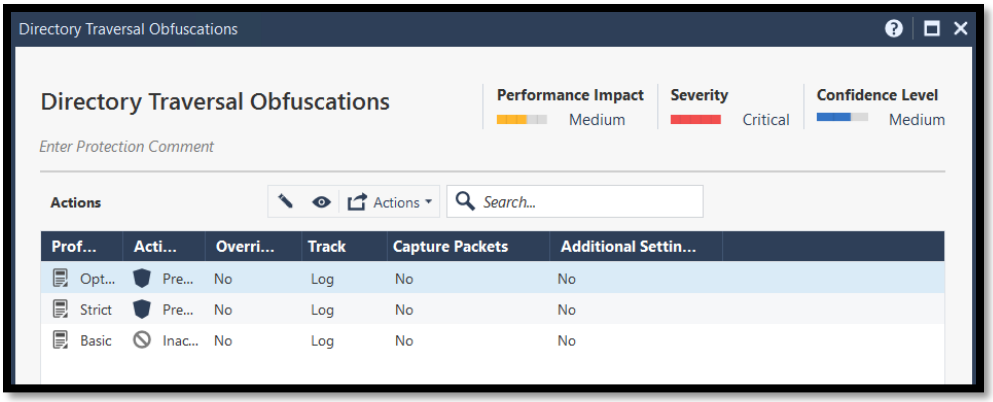
Actions

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

More

Id	24d5ff64-ad69-33ce-673b-7d5800000002
Sequencenum	14
Description URL	DIR_TRAV_OBF_help.html
Marker	@A@@B@1731947136@C@17609
Log Server Origin	SMS (10.1.1.100)
Index Time	2024-11-18T17:46:03Z
Lastupdatetime	1731951960000
Lastupdateseqnum	14
Log ID	2
Stored	true

4. 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.

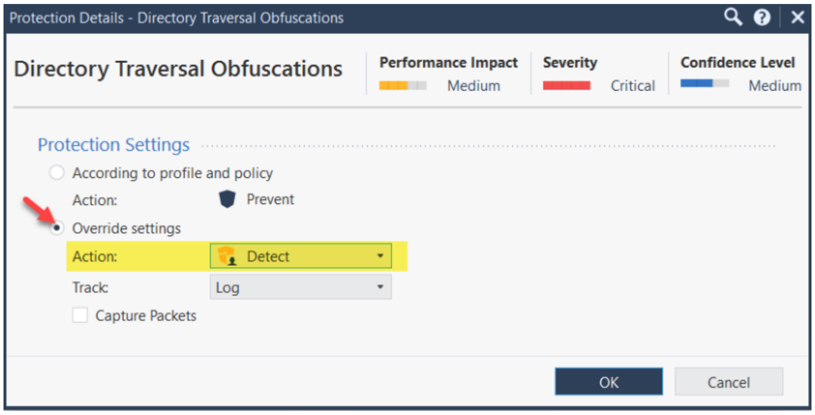


Directory Traversal Obfuscations

Performance Impact: Medium | Severity: Critical | Confidence Level: Medium

Prof...	Acti...	Overri...	Track	Capture Packets	Additional Settin...
Opt...	Pre...	No	Log	No	No
Strict	Pre...	No	Log	No	No
Basic	Inac...	No	Log	No	No

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



Directory Traversal Obfuscations

Performance Impact: Medium | Severity: Critical | Confidence Level: Medium

Protection Settings

○ According to profile and policy

Action: Prevent

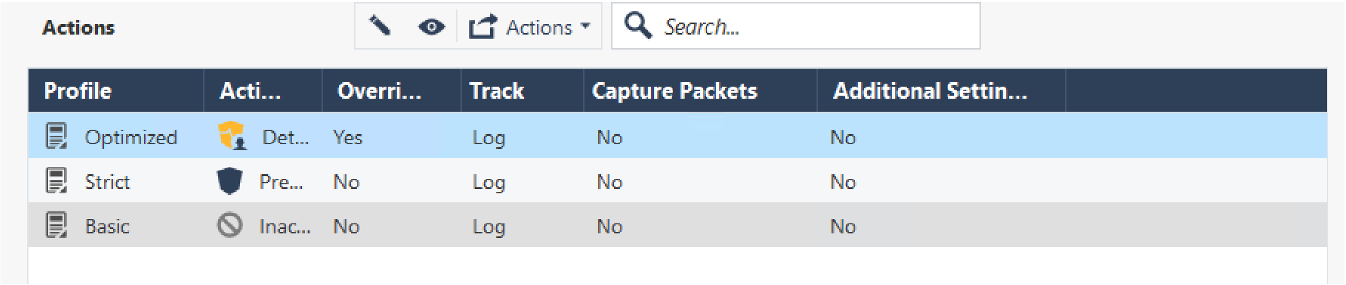
● Override settings

Action: Detect

Track: Log

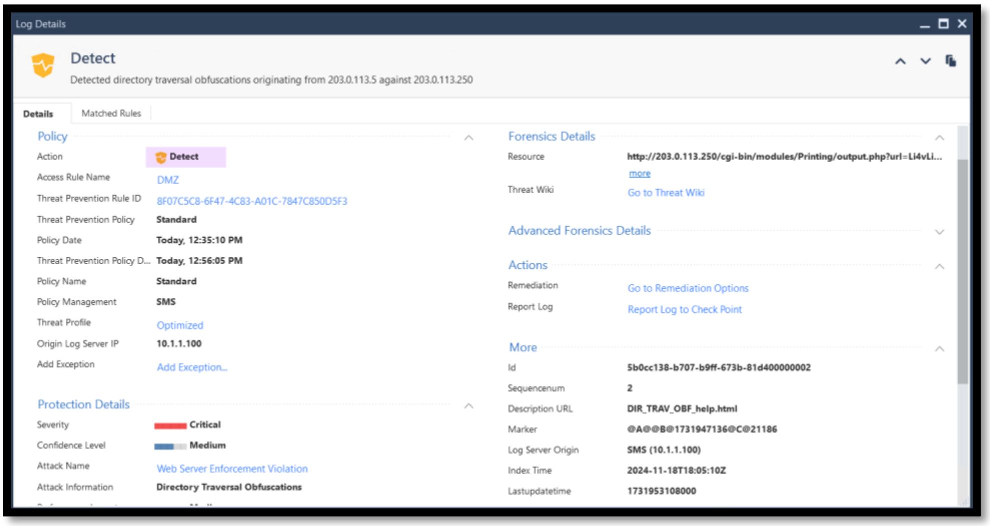
□ Capture Packets

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



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

7. 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.



Log Details

Detect

Detected directory traversal obfuscations originating from 203.0.113.5 against 203.0.113.250

Details | Matched Rules

Policy

Action	**Detect**
Access Rule Name	DMZ
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-A01C-7847C850D5F3
Threat Prevention Policy	**Standard**
Policy Date	**Today, 12:35:10 PM**
Threat Prevention Policy D...	**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=Li4vLi...** more
Threat Wiki	Go to Threat Wiki

Advanced Forensics Details

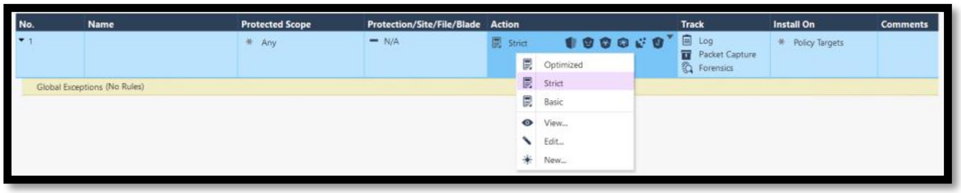
Actions

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**
Lastupdatedatetime	**1731953108000**

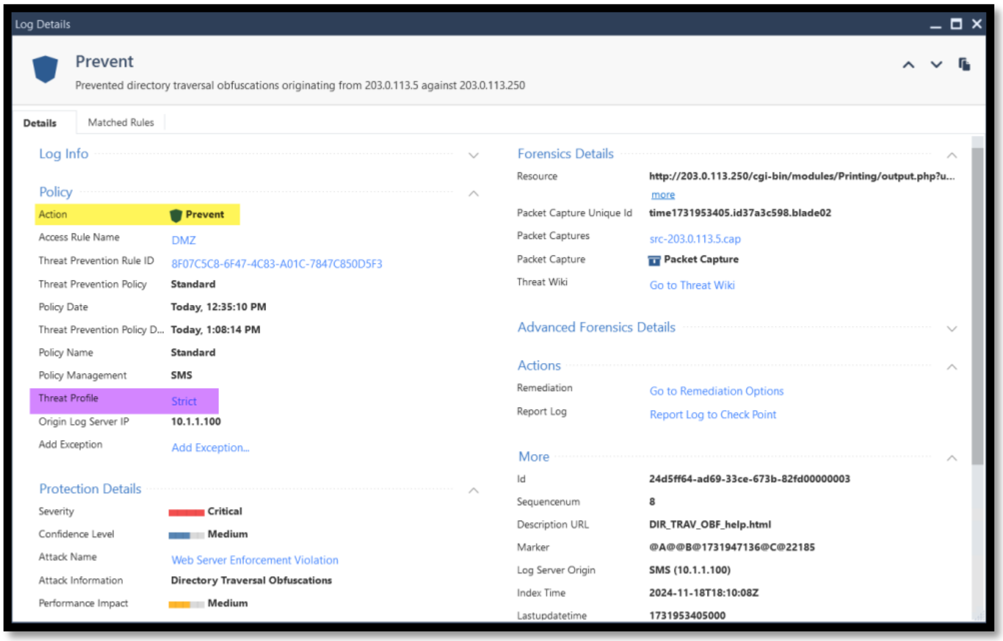
8. Change the profile assigned to the default rule, select the Strict profile and install the Threat Prevention Policy.



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)

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



Log Details

Prevent

Prevented directory traversal obfuscations originating from 203.0.113.5 against 203.0.113.250

Details | Matched Rules

Log Info

Policy

Action	**Prevent**
Access Rule Name	DMZ
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-A01C-7847C850D5F3
Threat Prevention Policy	**Standard**
Policy Date	**Today, 12:35:10 PM**
Threat Prevention Policy D...	**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?u...** more
Packet Capture Unique Id	**time1731953405.id37a3c598.blade02**
Packet Captures	src-203.0.113.5.cap
Packet Capture	**Packet Capture**
Threat Wiki	Go to Threat Wiki

Advanced Forensics Details

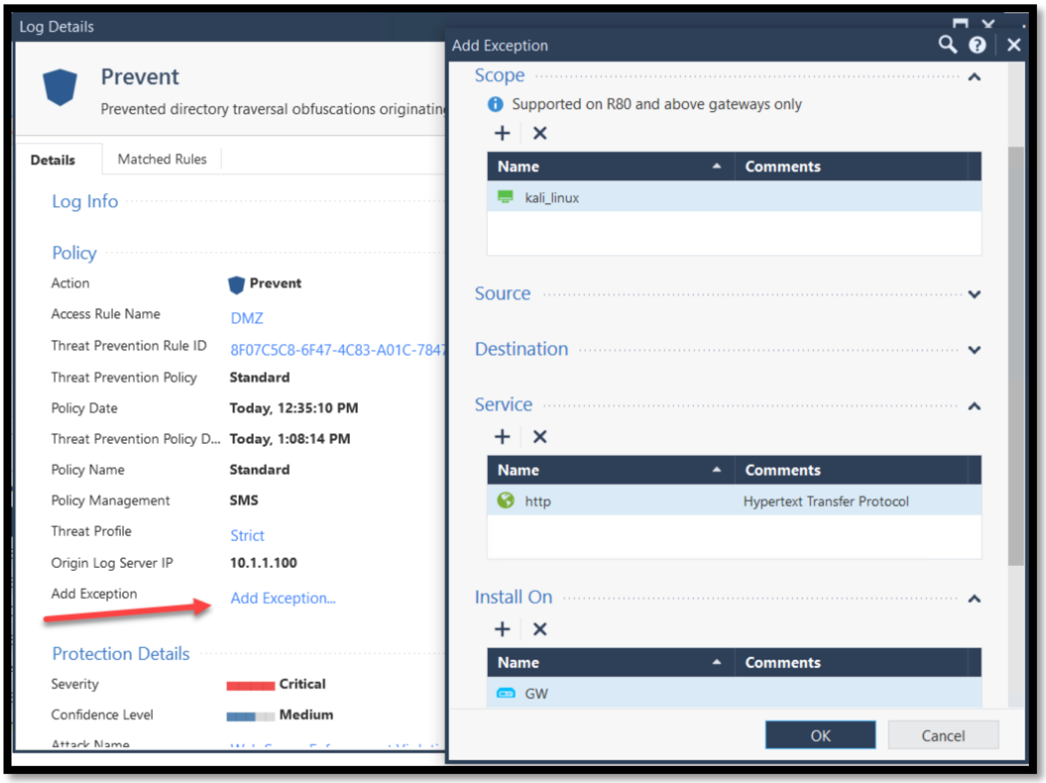
Actions

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

More

Id	**24d5ff64-ad69-33ce-673b-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	**2024-11-18T18:10:08Z**
Lastupdatedatetime	**1731953405000**

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



Log Details

Prevent

Prevented directory traversal obfuscations originatin

Details | Matched Rules

Log Info

Policy

Action	Prevent
Access Rule Name	DMZ
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-A01C-7847
Threat Prevention Policy	Standard
Policy Date	Today, 12:35:10 PM
Threat Prevention Policy D...	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	

Add Exception

Scope

Supported on R80 and above gateways only

Name	Comments
kali_linux	

Source

Destination

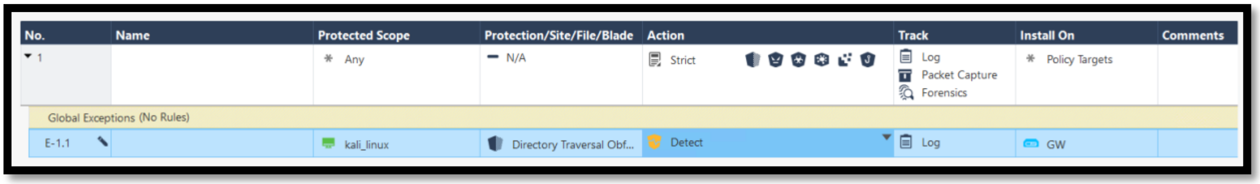
Service

Name	Comments
http	Hypertext Transfer Protocol

Install On

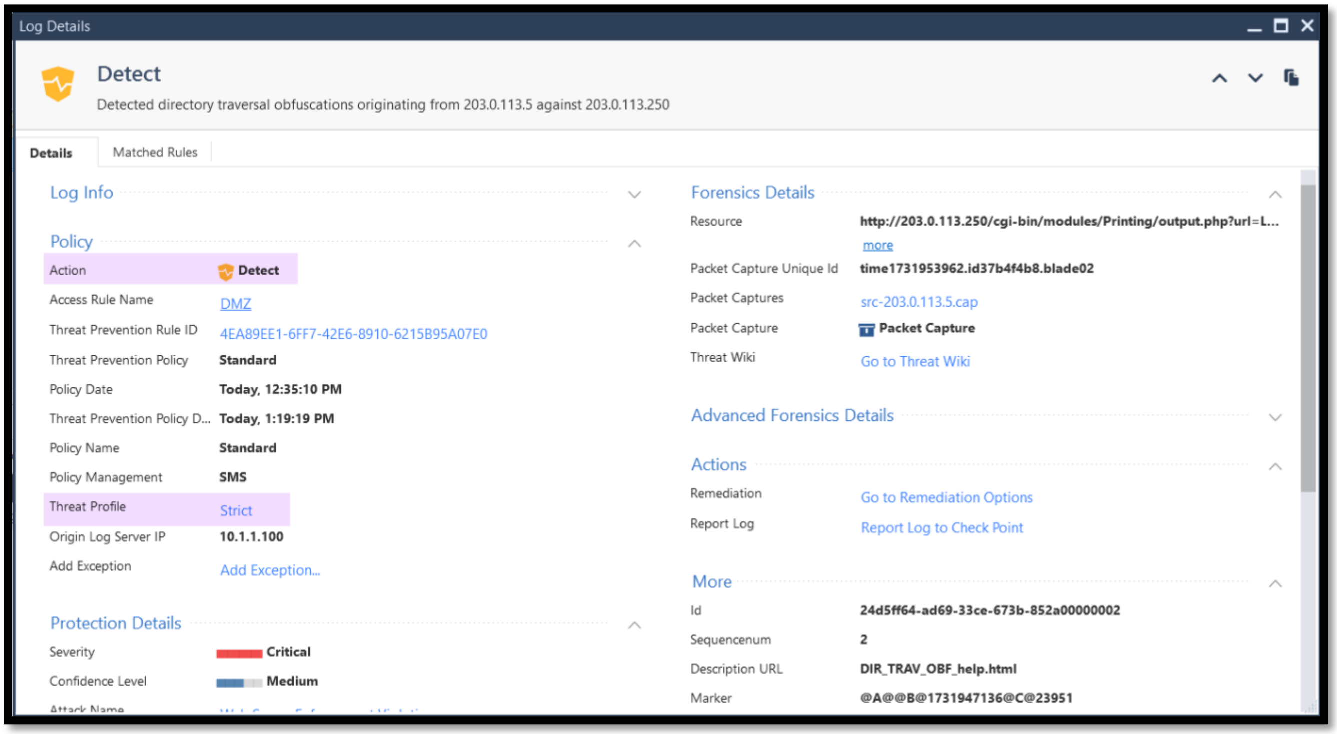
Name	Comments
GW	

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.



Detect

Detected directory traversal obfuscations originating from 203.0.113.5 against 203.0.113.250

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
Attack Name	

Forensics Details

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

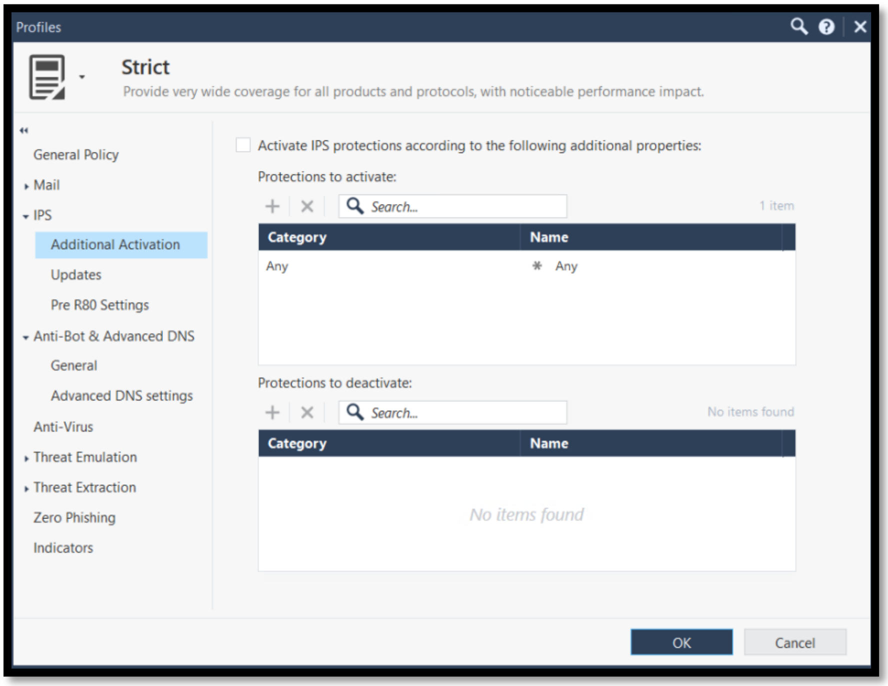
Actions

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.



Strict

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

□ Activate IPS protections according to the following additional properties:

Protections to activate:

Category	Name
Any	✱ Any

Protections to deactivate:

Category	Name

No items found

End of Lab 5