Intrusion Prevention System (IPS)

Expected Time: 45 Minutes

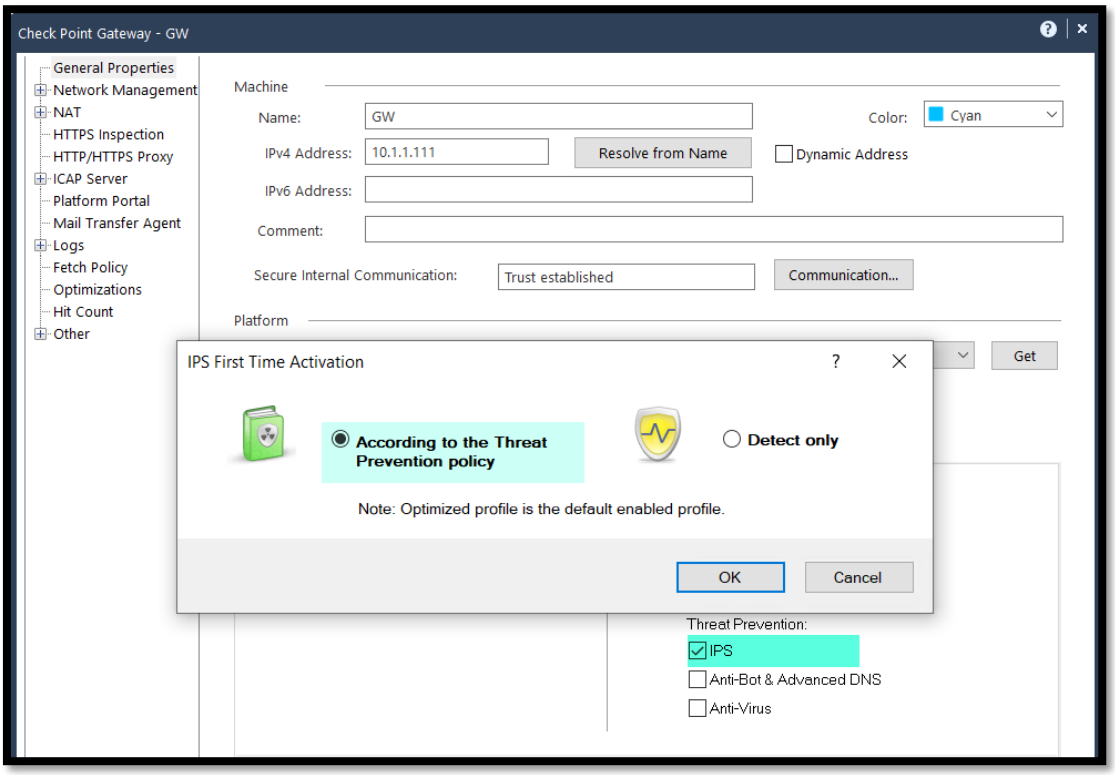
Introduction

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.

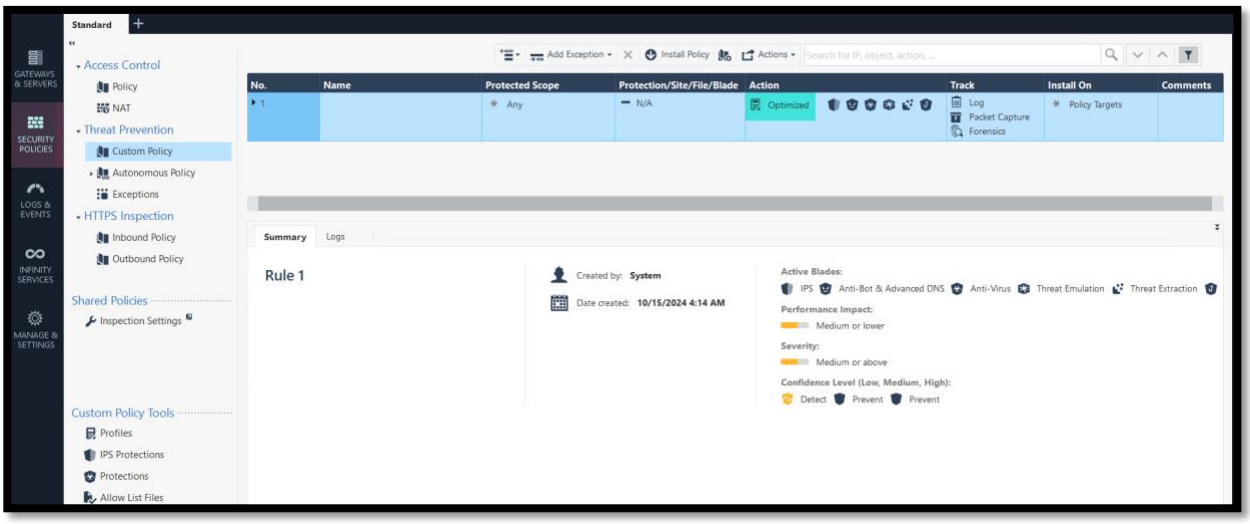
Exercise 1: Onboarding

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.

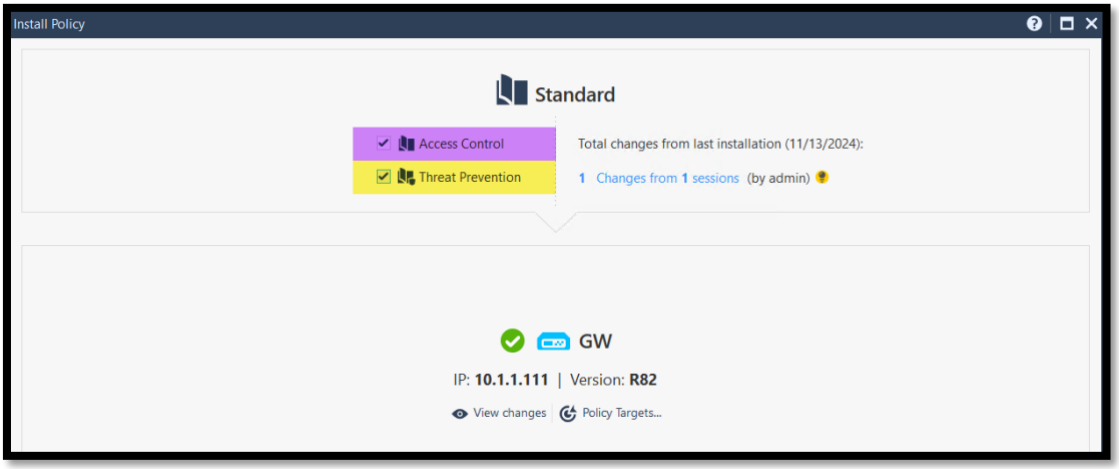
1. Edit the **GW** object and enable the **IPS** blade According to the Threat Prevention Policy.



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.



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

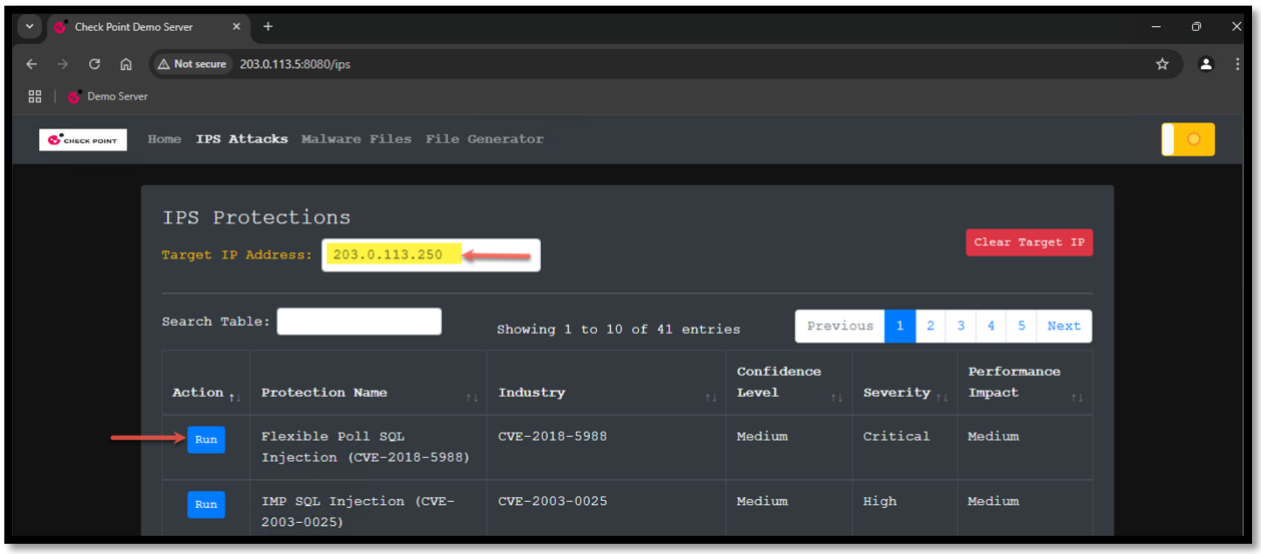


4. From **win_client**, Open the browser and browse to the Demo Server at http://203.0.113.5:8080

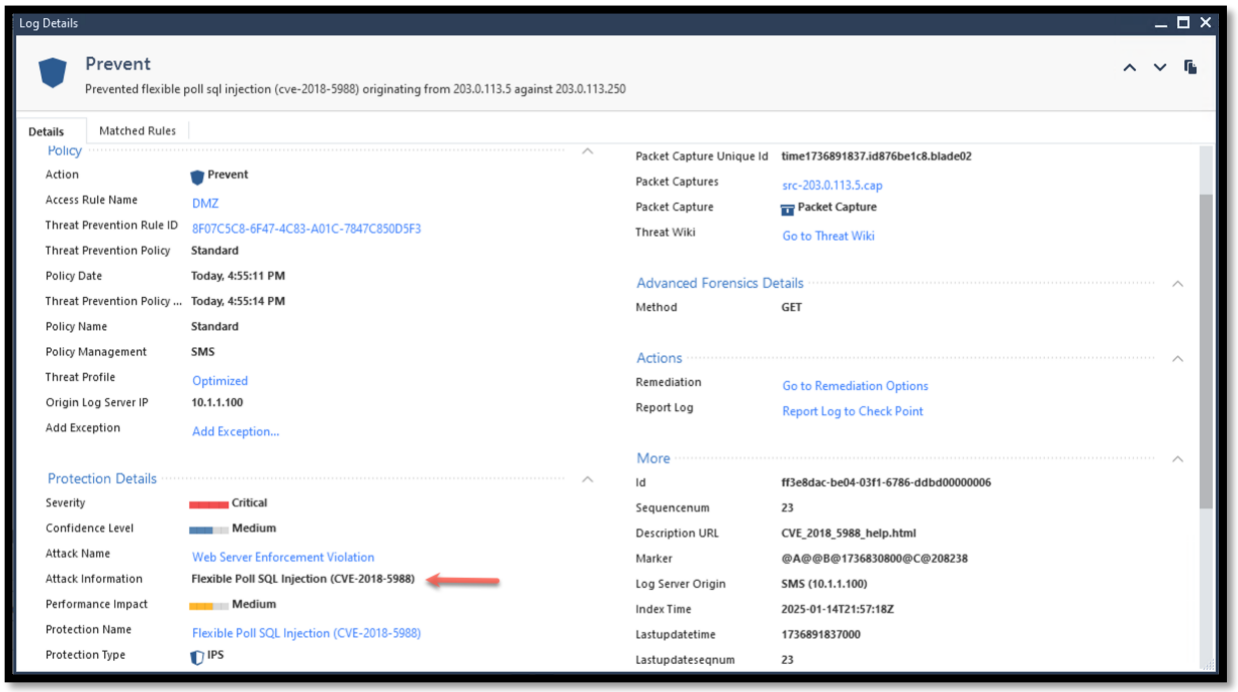
Notes:

- 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.



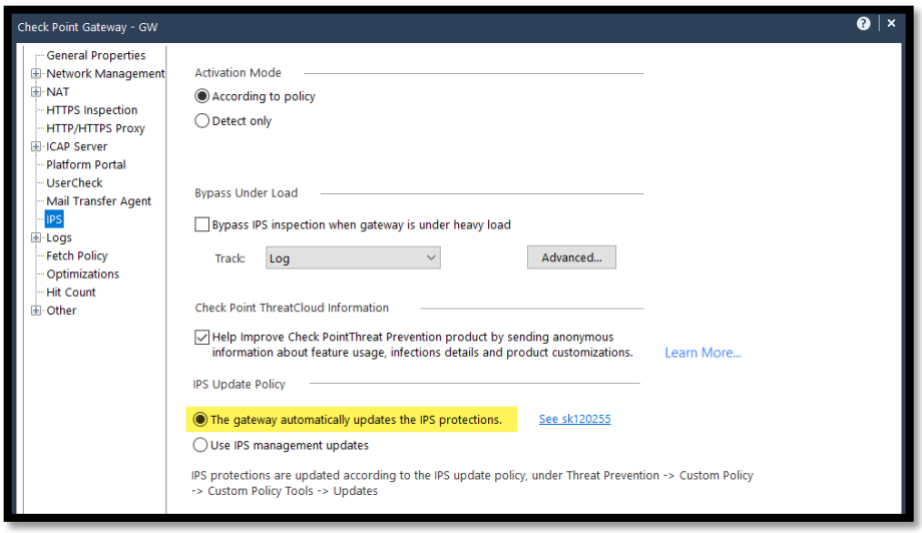
6. Filter the logs in SmartConsole to show logs from **IPS** only. Notice that the attack we triggered generated a log and the **Packet Capture** is attached to the log.



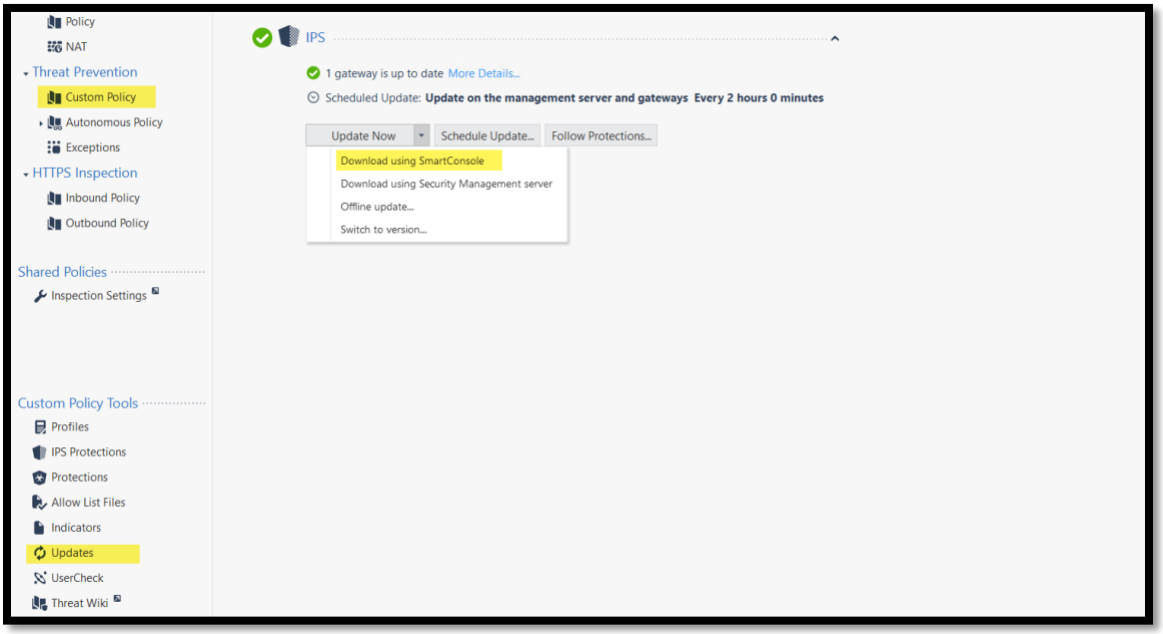
Exercise 2: Updates

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.

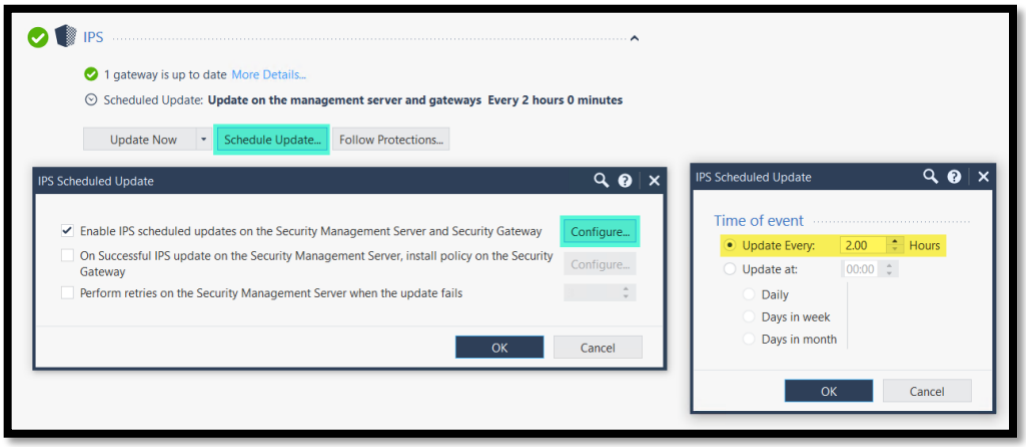
1. Open the **GW** object and review the **IPS Update Policy** settings for the GW. Notice that by default, the GW will try to update the IPS protections automatically. Read SK120225 for more details.



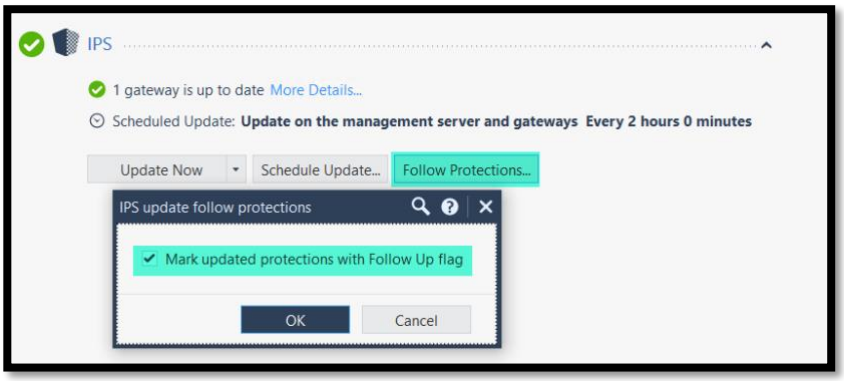
2. While in the Custom Threat Prevention Policy View, click updates and review the available methods to update IPS. Update using SmartConsole.



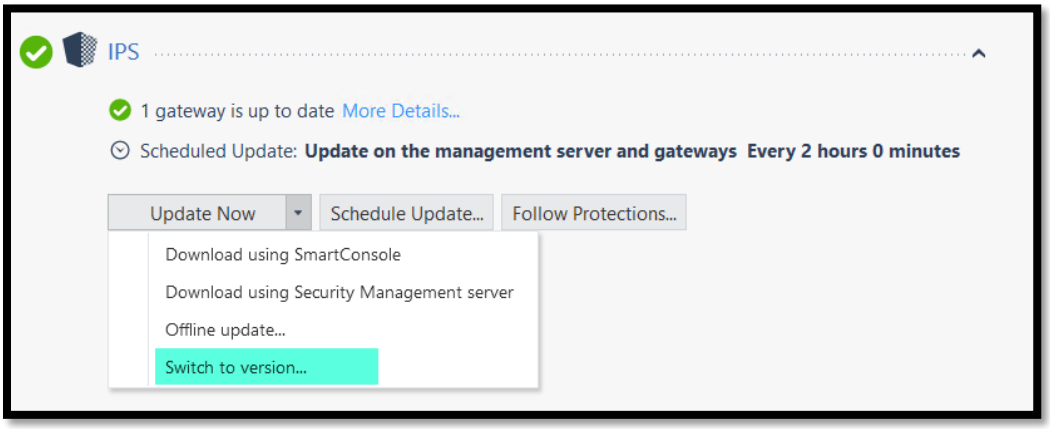
3. Review the scheduled updates. By default, the security management and security gateways check for updated every 2 hours.



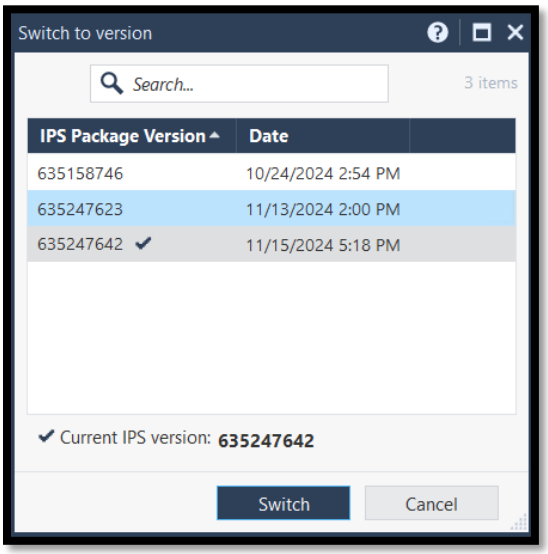
4. To be able to tell which protection were updated, they are marked by default. Review the settings under “Follow Protections”.



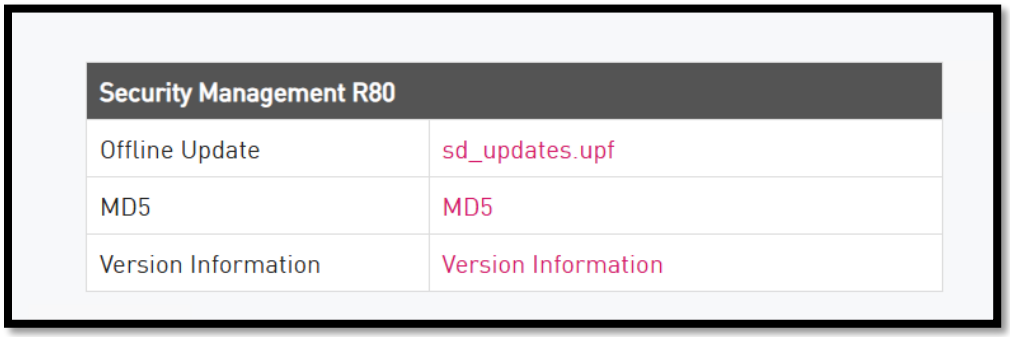
5. In case you updated IPS and for any reason you would like to revert to one of the older versions, navigate to the list of updated under: **Update Now** -> Switch to version



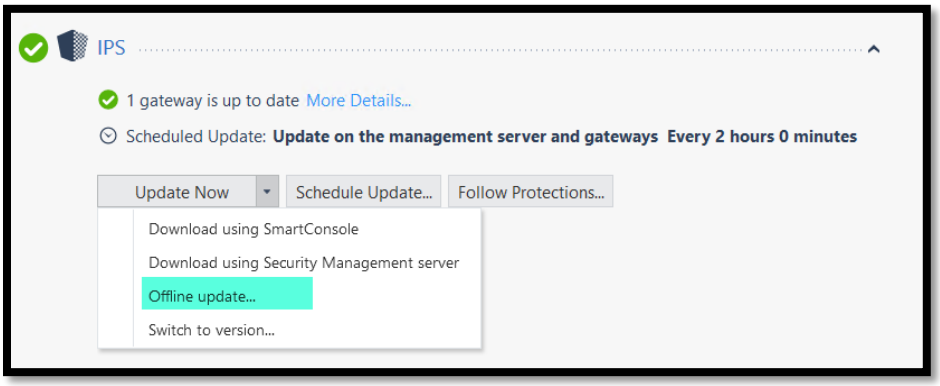
6. From the list of versions, select the version to revert to and click Switch.



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



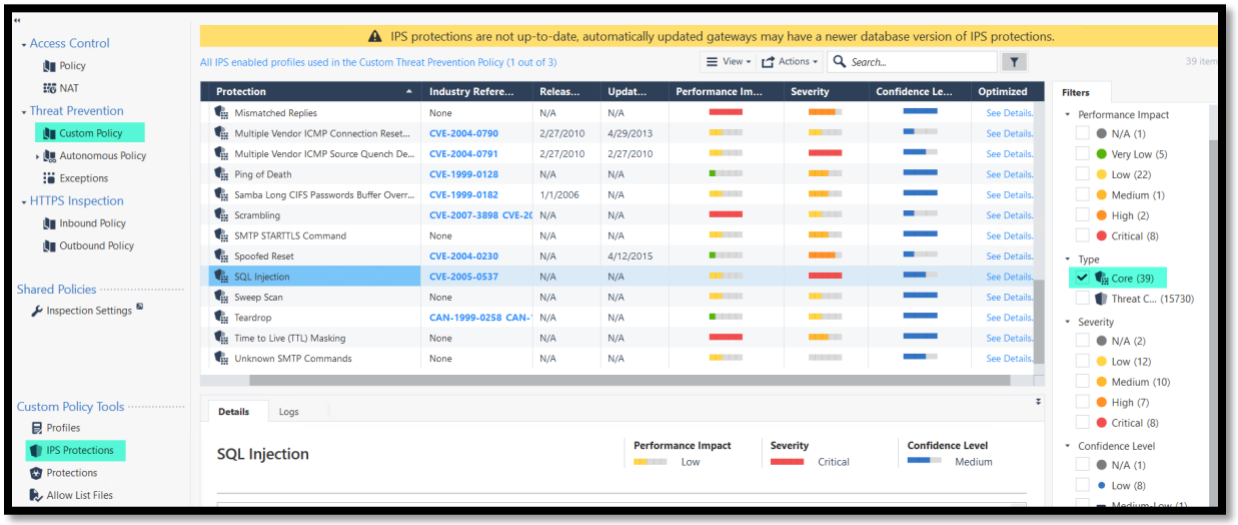
8. When Offline Updates is selected from the drop-down menu, you will be asked to point to the update file location.



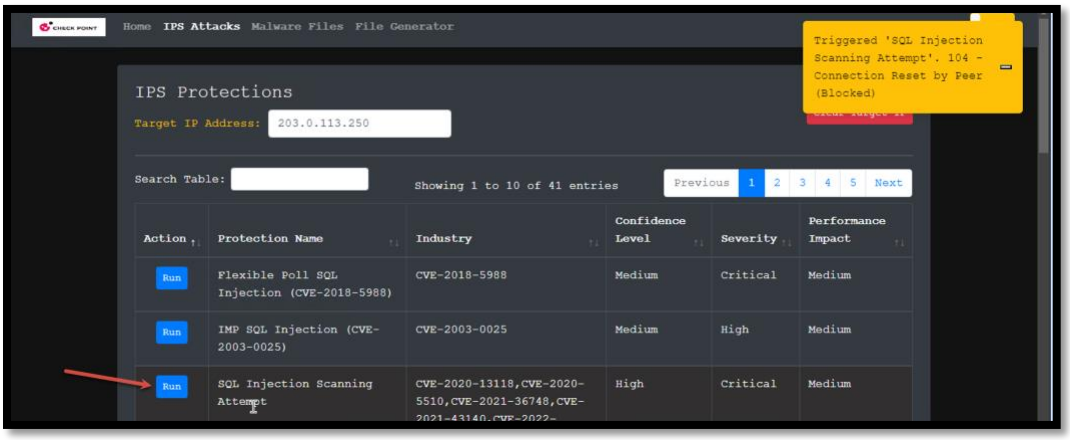
Exercise 3: Core Protections

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.

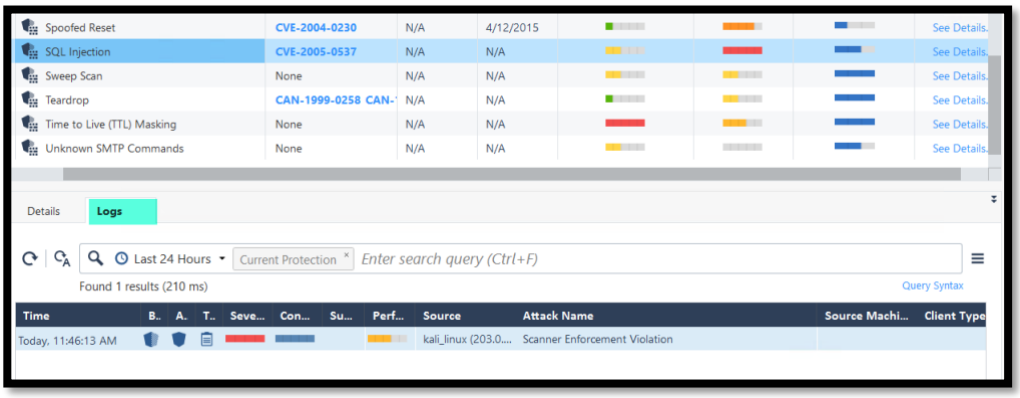
1. Open the **IPS Protections** tab and filter the protections to show **Core** protections only. Notice that the icon for the core protections differ from the **Threat Cloud** protections.



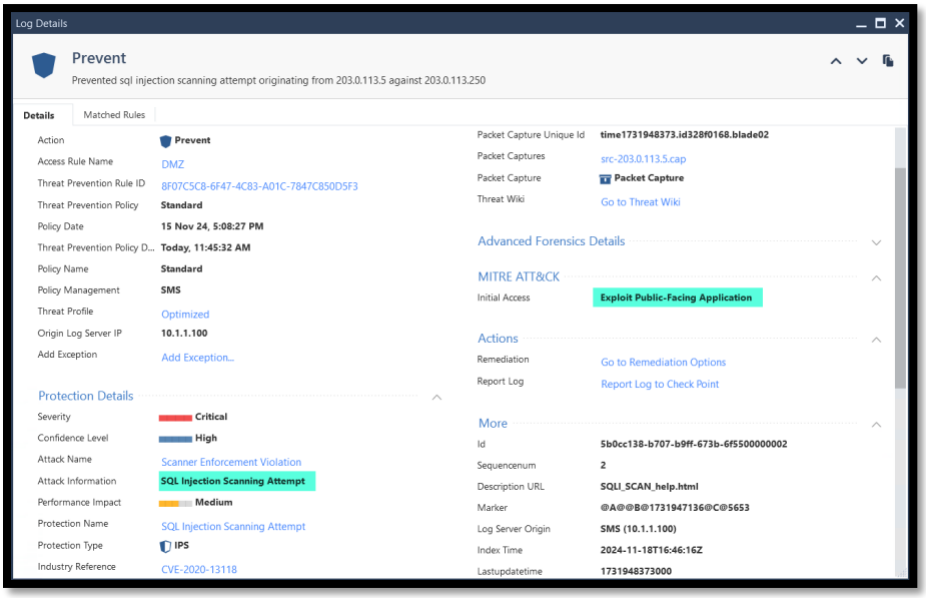
2. From the Demo Server, trigger one of the SQL attacks. For example, trigger the protection SQL Injection scanning attempt.



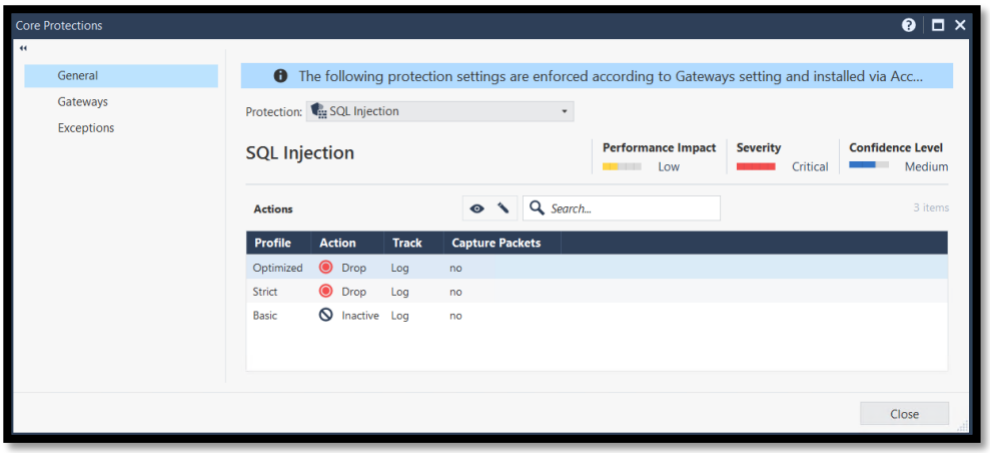
3. Look for the SQL protection in the Core protections list and select the log tab to see logs related to this protection.



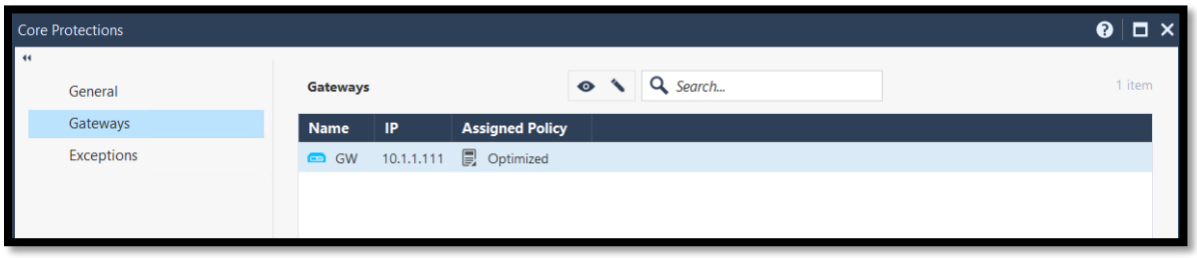
4. Review the log and the field of each section.



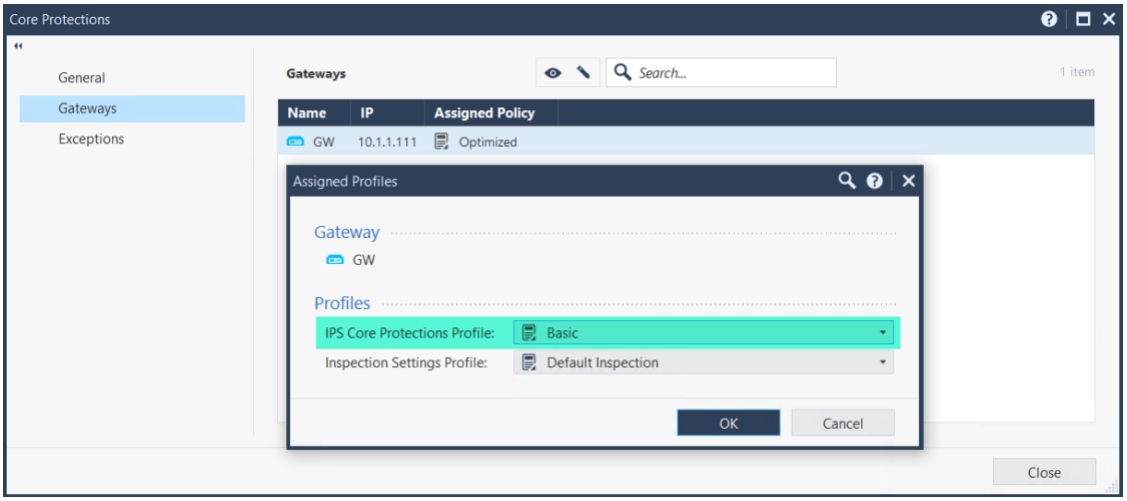
5. Open the SQL Protection and review the default action per profile. Notice that the SQL Injection Core Protection is disabled by default in the Basic profile.



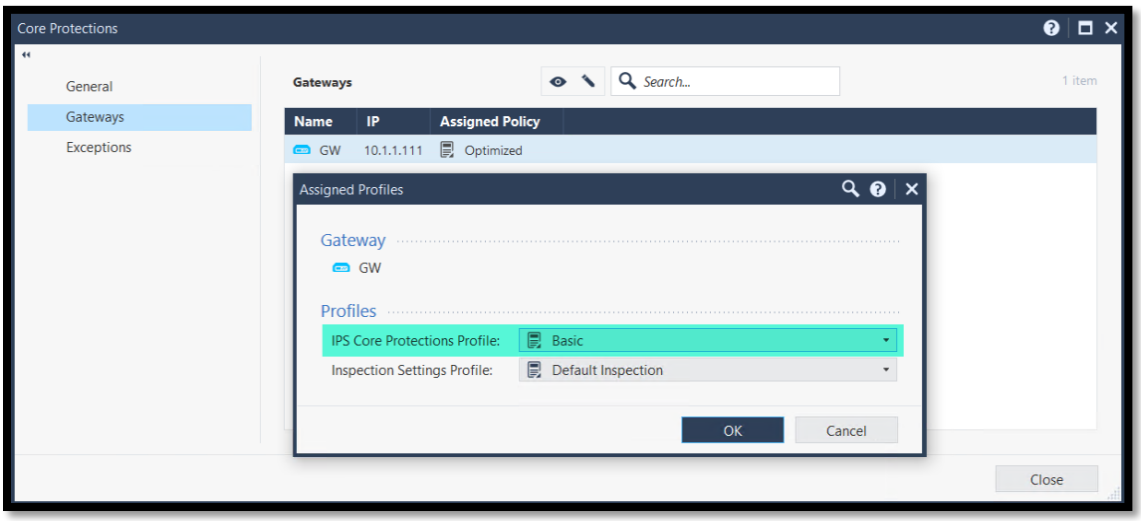
6. Move to the Gateways tab and review the default profile settings. Notice that this profile assignment is independent of the profile assigned in the rule base.



7. Edit the selection and select the Basic profile

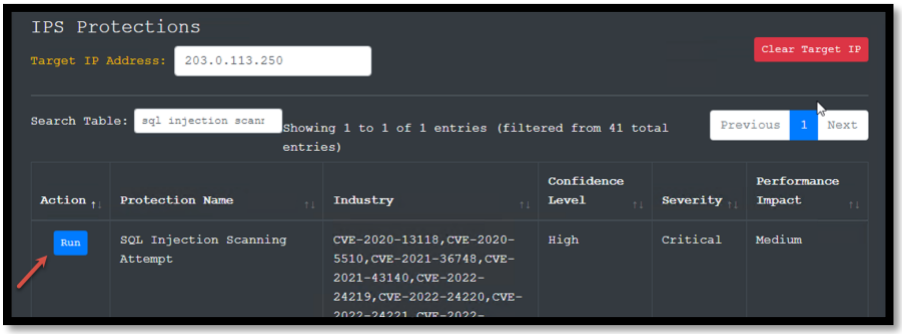


8. Edit the profile selection and select the Basic Profile.



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)



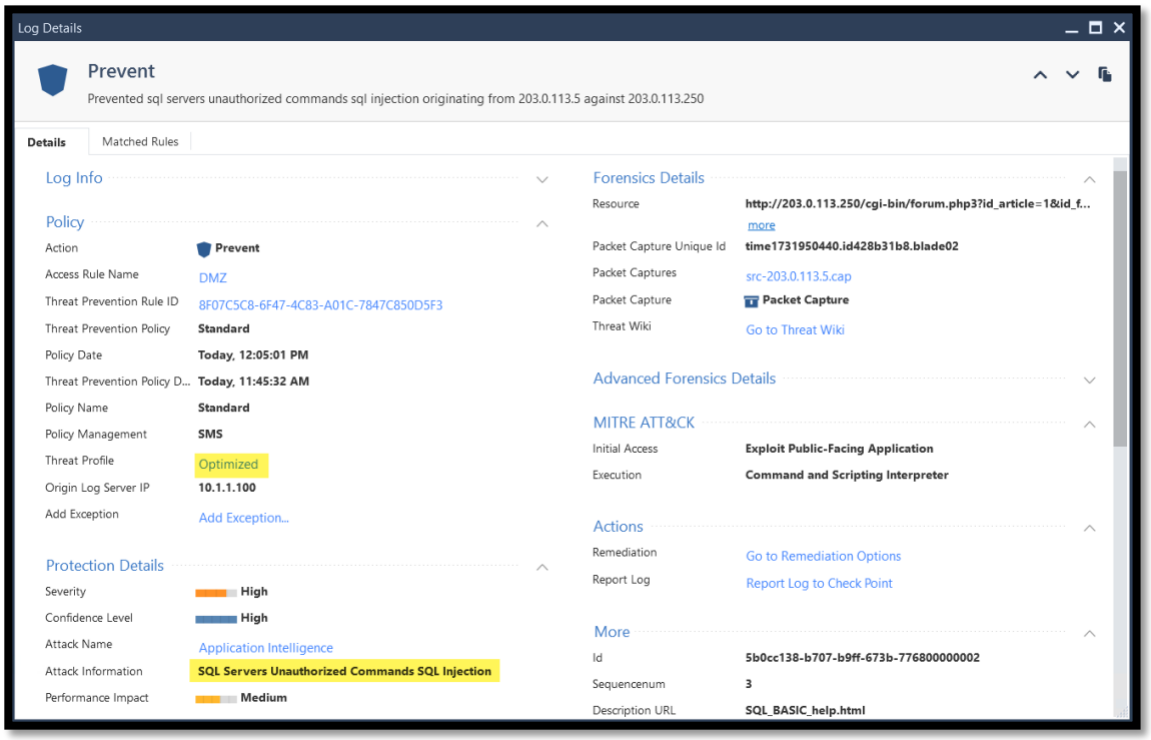
11. Review the logs and notice that no new protection logs were generated as expected.

- 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.

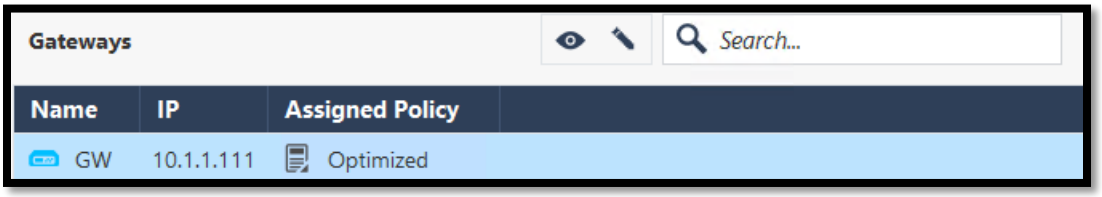
12. Run a different attack, this time trigger the protection **SQL Servers Unauthorized Commands SQL Injection**.

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

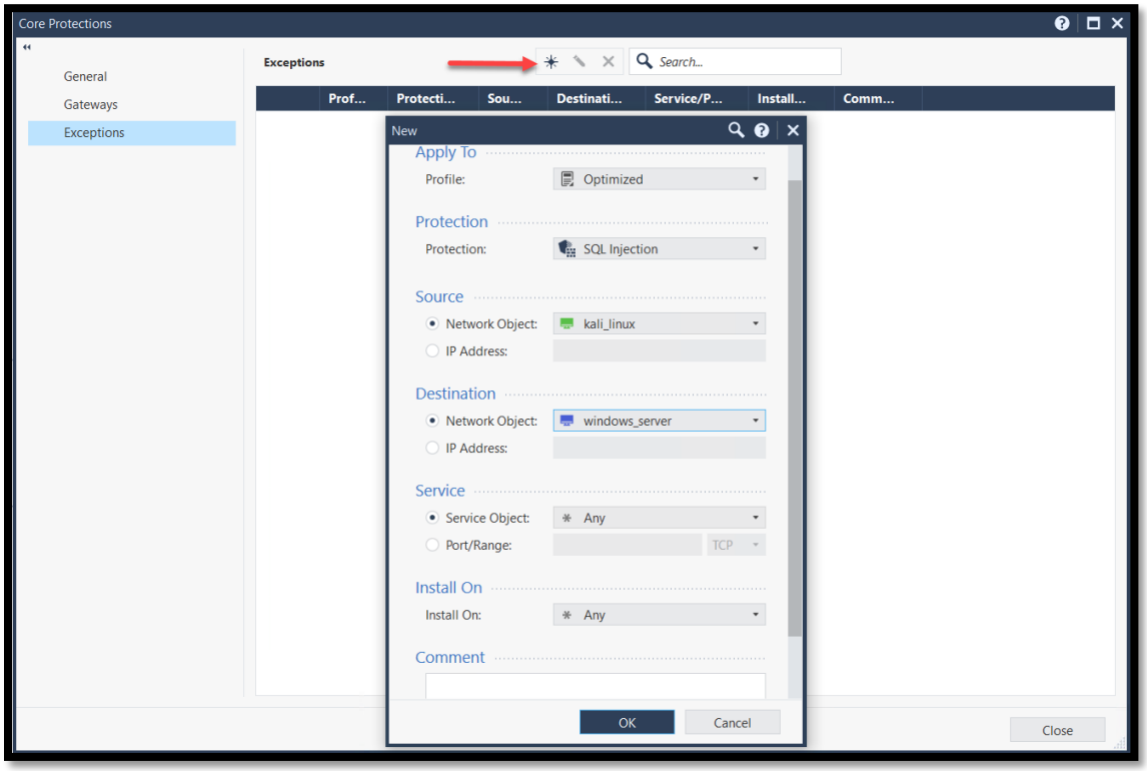
    - Check Point provide multiple protections that work in parallel to protect your environment.
    - Notice that this protection is managed via the Optimized profile assigned in the rule base and not the Basic profile we assigned to core protections.



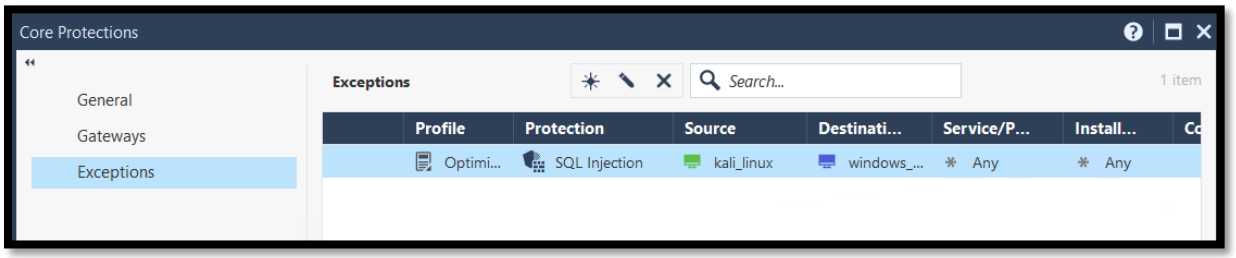
14. Edit the SQL protection settings and assign the **Optimized Profile**.



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

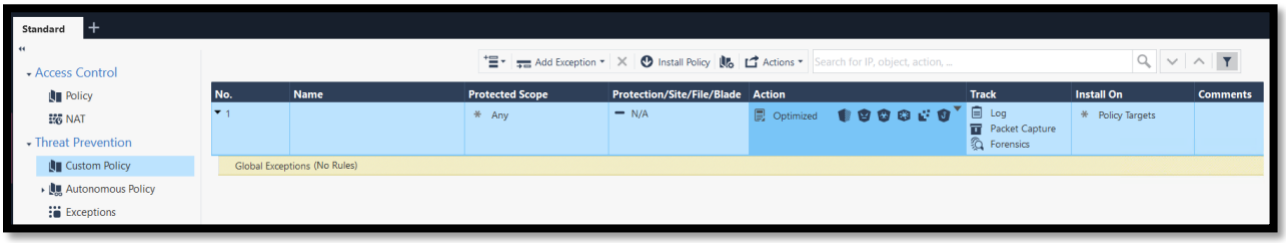


17. Run a new test using the same protection trigger from the demo server.
    - Notice that the protection is no longer triggered since we added an exception.
    - Making exception is a preferred method in most cases. Add an exception specific to a host or network.
    - Like the behavior above, other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

Exercise 4: Threat Cloud Protections

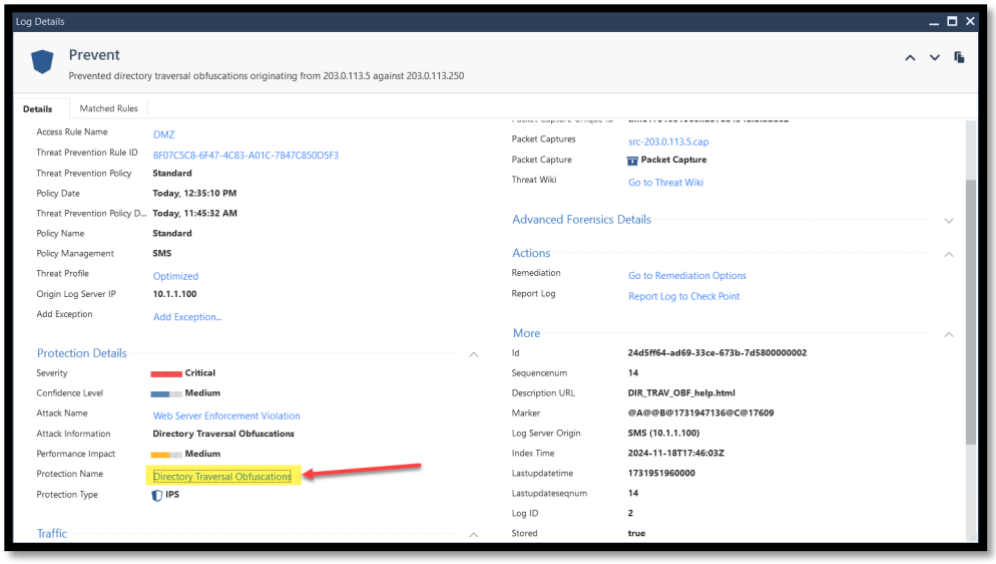
Threat Cloud Protections are updated regularly by the Check Point research team. Those protections are dynamic with new protections added regularly.

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

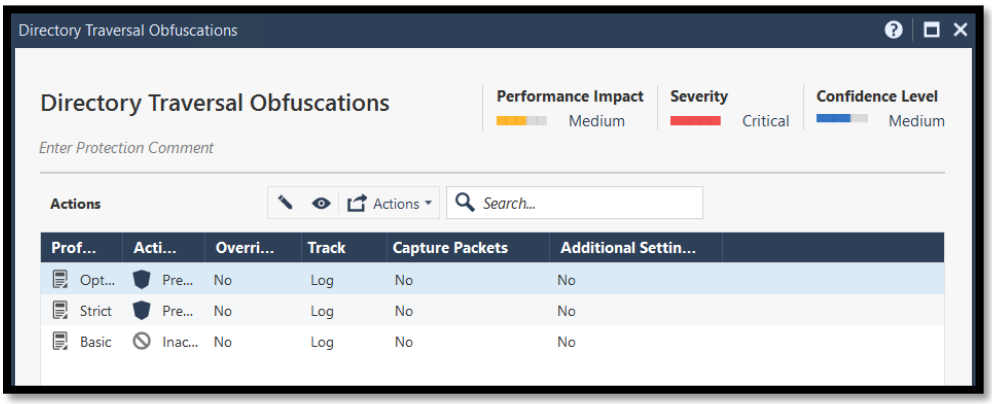


13. From the demo server, trigger the protection **Directory Traversal Obfuscation**

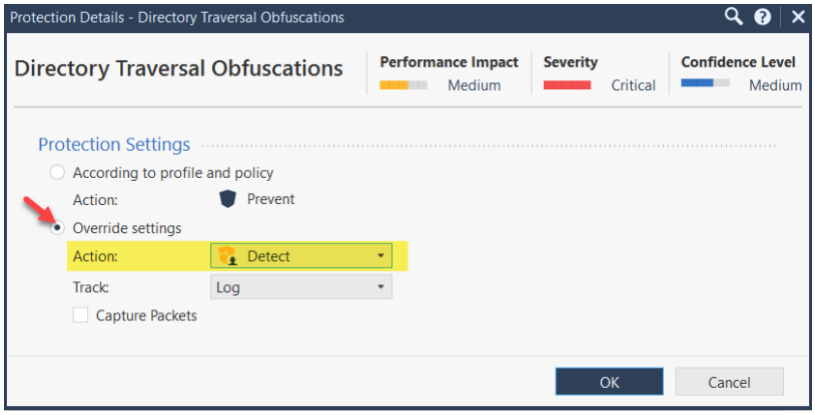
14. Review the log and pay attention to the profile.



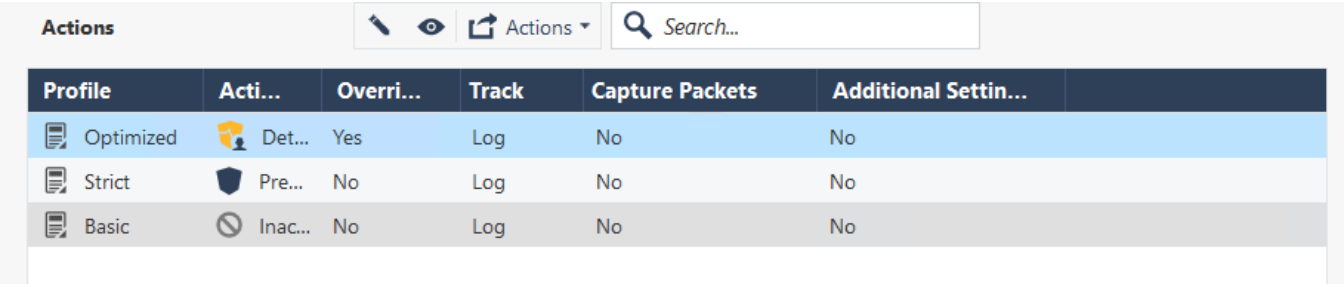
15. Click on the highlighted protection name link. This will open the corresponding protection window. Notice that this protection is set to prevent mode by default for the Strict and Optimized profiles.



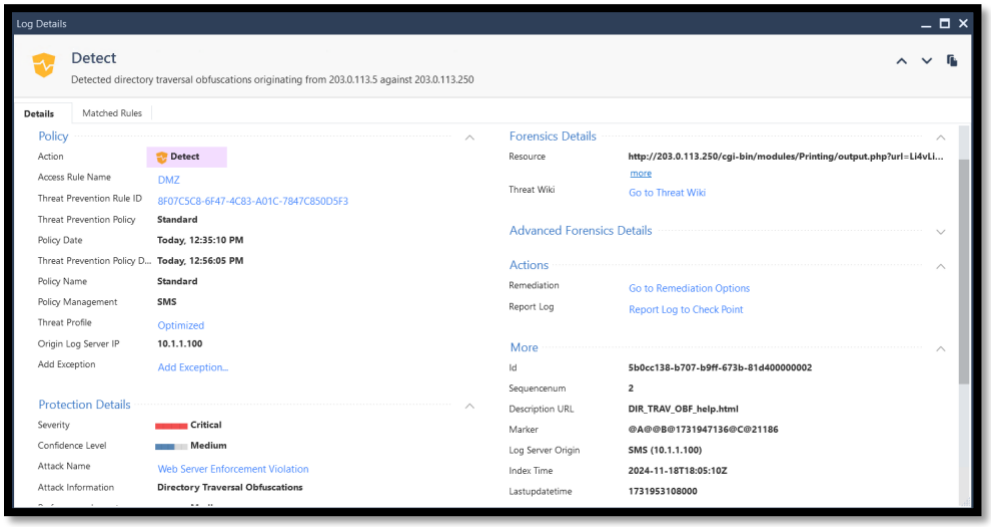
16. While Optimized is selected, edit the settings and change the behavior to detect instead of Prevent.



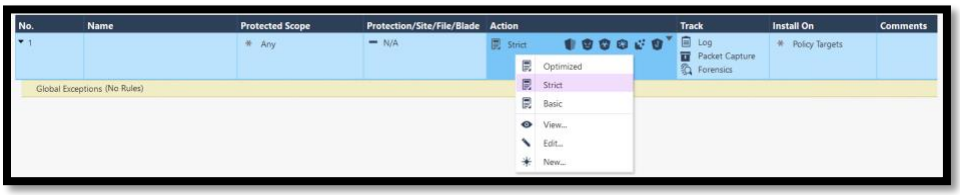
17. Confirm the changes and Install the Threat Prevention Policy.



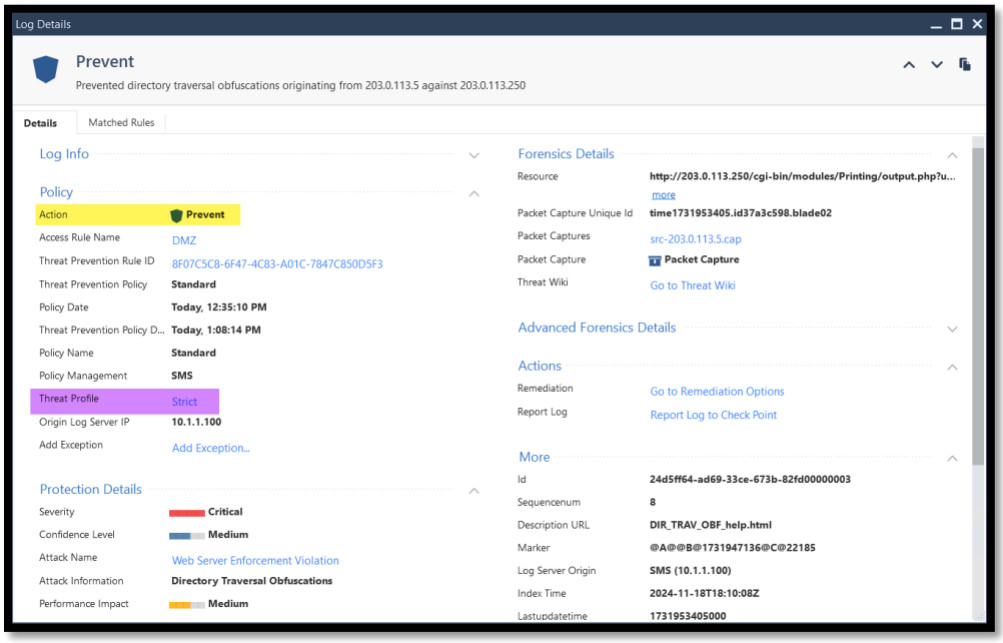
18. Trigger the same protection again and review the logs. You should see a detect log. Note that this is only made for the optimized profile. However, this applies to all hosts and networks.



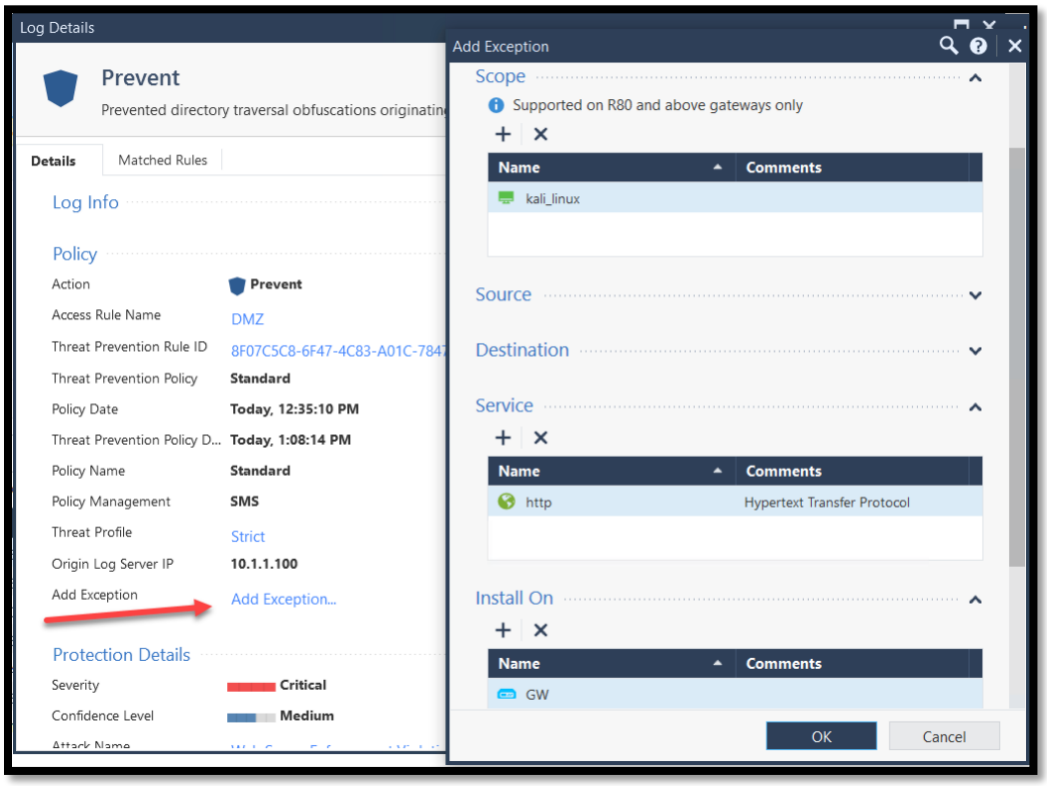
19. Change the profile assigned to the default rule, select the Strict profile and install the Threat Prevention Policy.



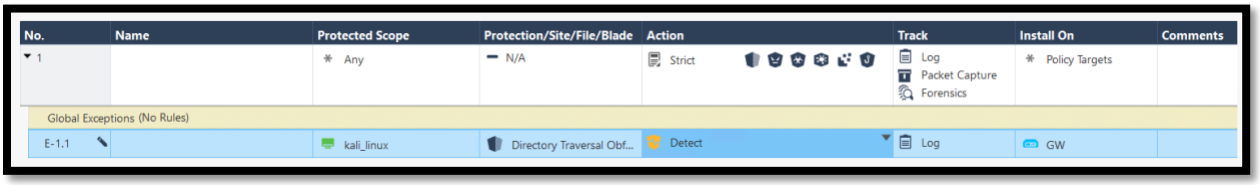
20. Trigger the same protection again. Review the logs and notice that the traffic is now prevented by the Strict profile.



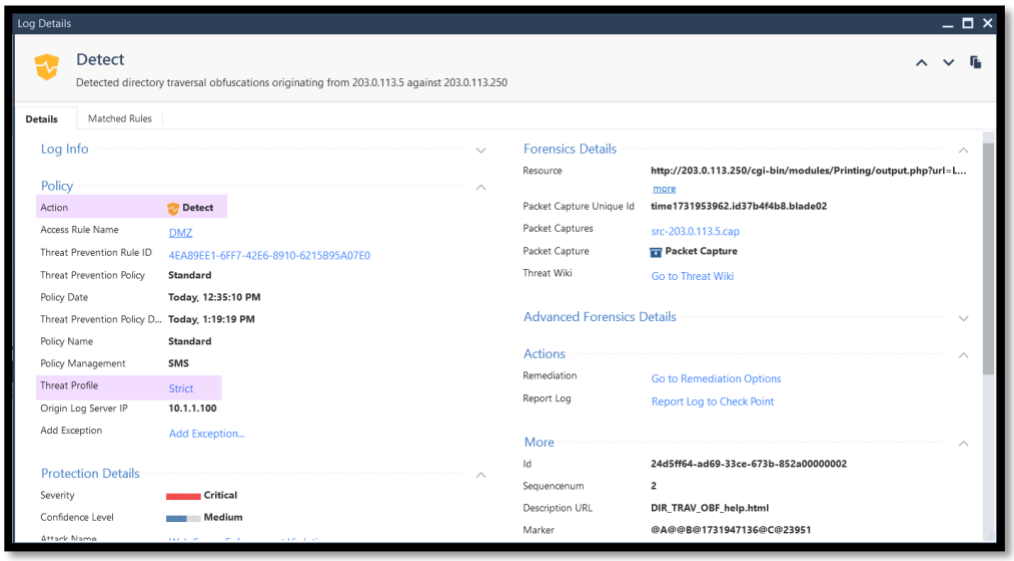
21. Use the Add Exception feature from the log to add an exception to the rule base.



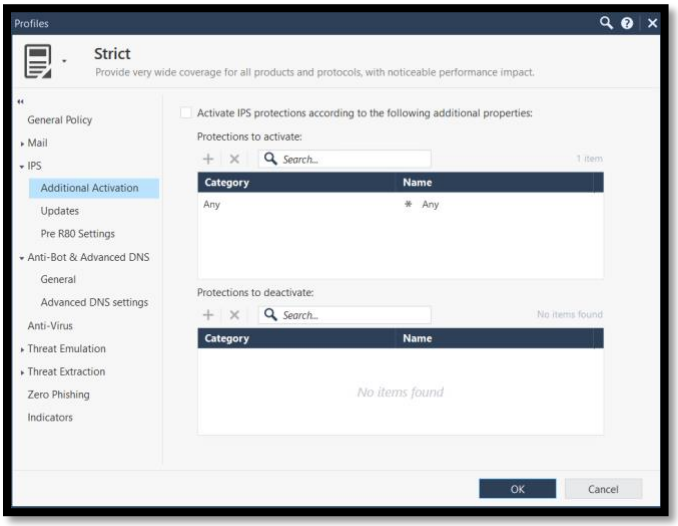
22. Notice that the exception was added to deactivate the protection for a specific source. Change the action to detect and install the Threat Prevention Policy.



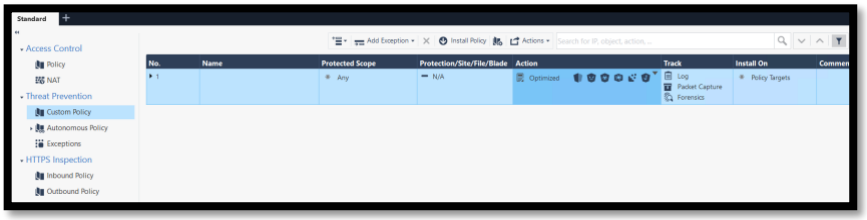
23. Review the detect log and notice that we now have an exception for a specific host.



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

