

Inspection Settings

Introduction

Using the Inspection Settings, You can configure inspection settings for the security Gateway:

- Deep packet inspection settings.
- Protocol parsing inspection settings.
- VoIP packet inspection settings.

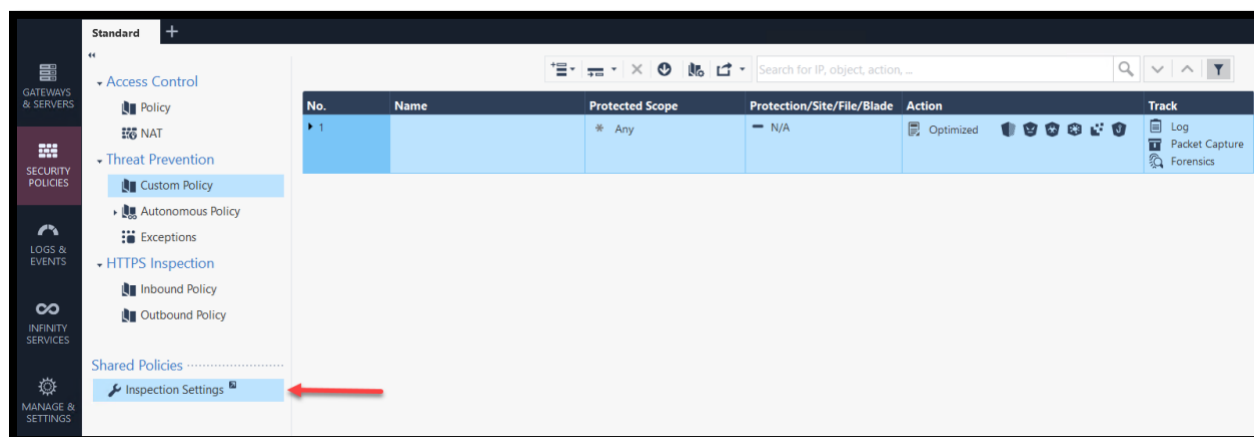
Exercise 1: Inspection Settings basics

The Security Management Server comes with two preconfigured inspection profiles:

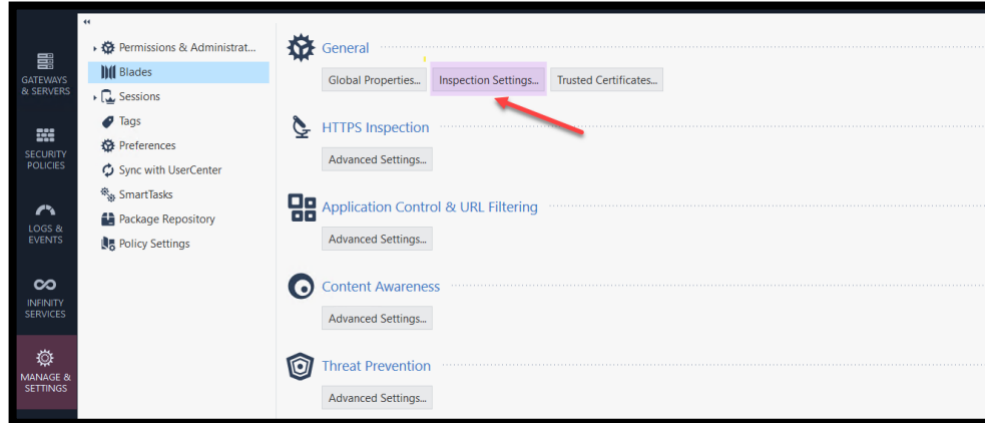
- Default Inspection
- Recommended Inspection

The Default Inspection profile is enabled by default. You can change the settings and assign the “Recommended Inspection” profile to the Security Gateway, or to create and assign a custom profile.

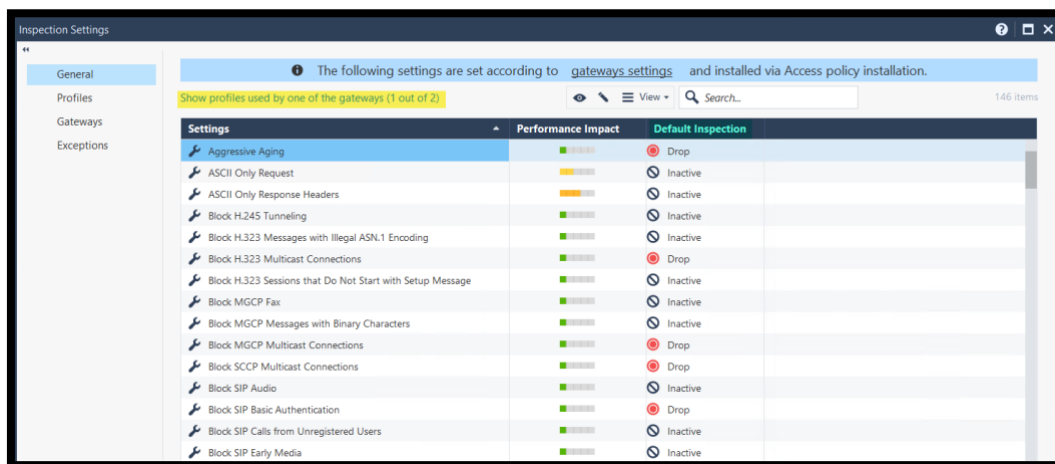
1. Open the Inspection Settings under **Security Policies** -> **Inspection Settings**.



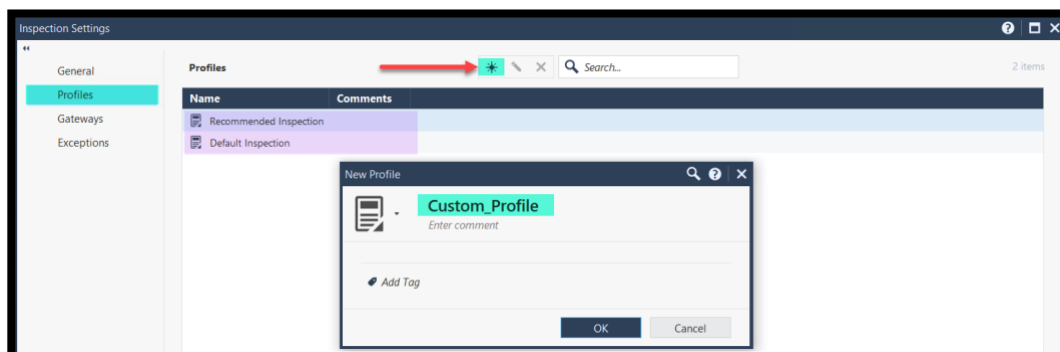
Note: It is also accessible via Manage & settings -> Blades -> General



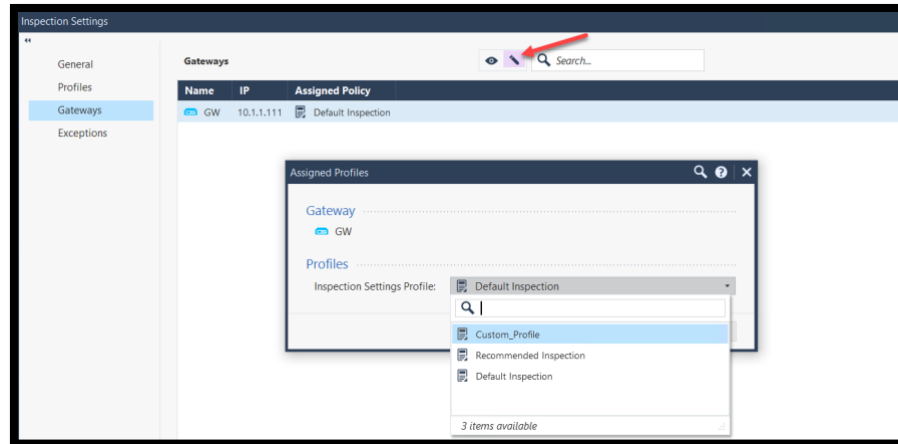
- Under the General view, notice that the Default Inspection profile settings are listed. Notice that only the profile assigned to the GW is visible by default.



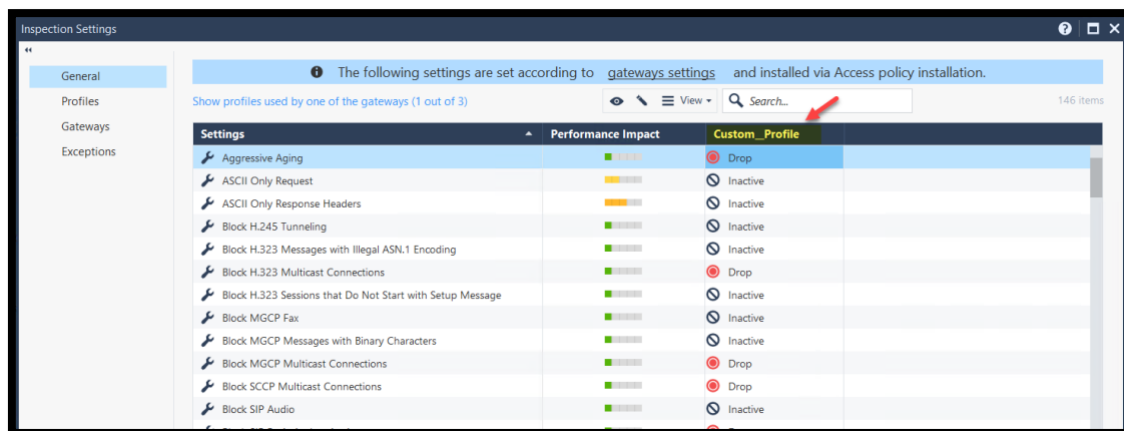
- Under **Profiles**, create a new profile and give it a proper name.
 - Note that the profiles and all the settings in this lab are not related to the IPS blade. These settings are configured and Installed via the Access Policy.



4. Move down to the Gateways view and click edit to change the default profile assignment settings and select the new profile we just created.



5. Move up to the “General” view and notice that only the assigned profile is displayed

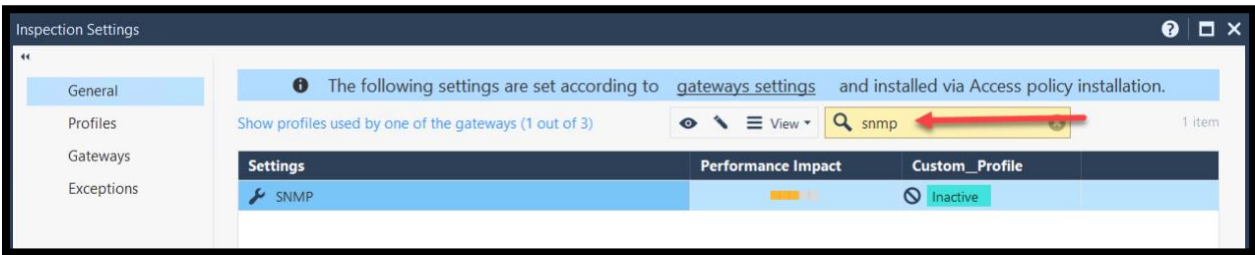


Exercise 2: Customizing the Inspection Settings

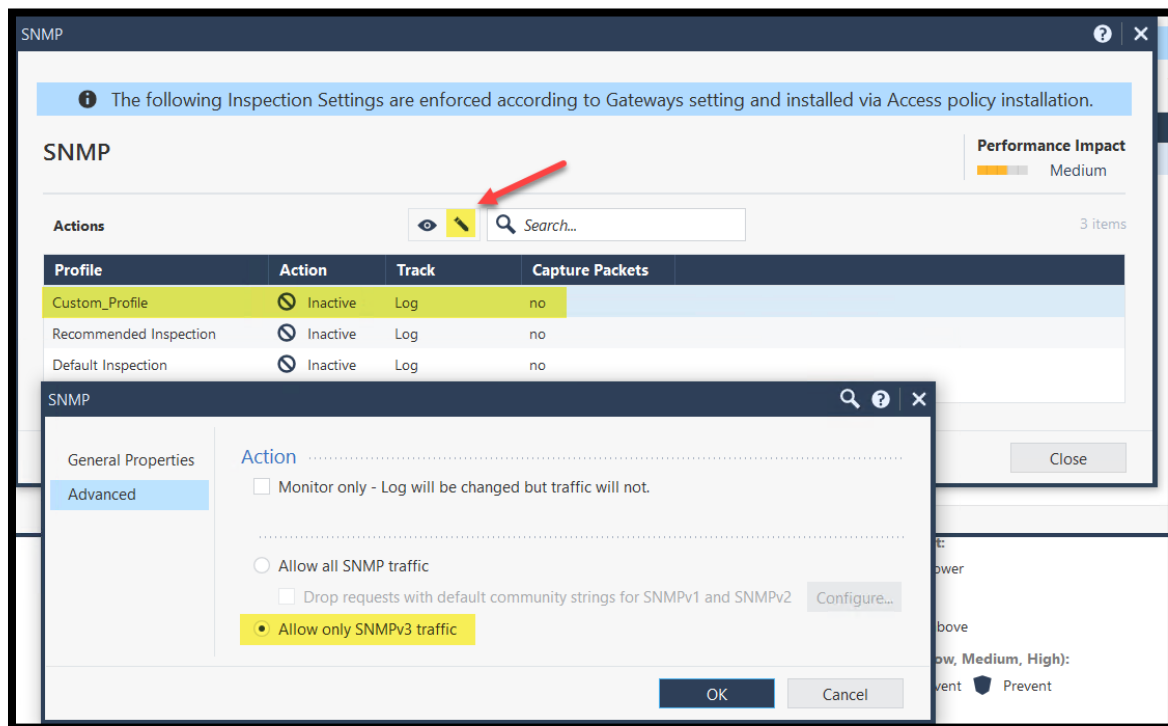
In the previous exercise, we created a custom profile. The new profile is a clone of the Default Profile.

In this exercise, we will customize the settings and test the enforcement of the protocol specifications of the SNMP protocol.

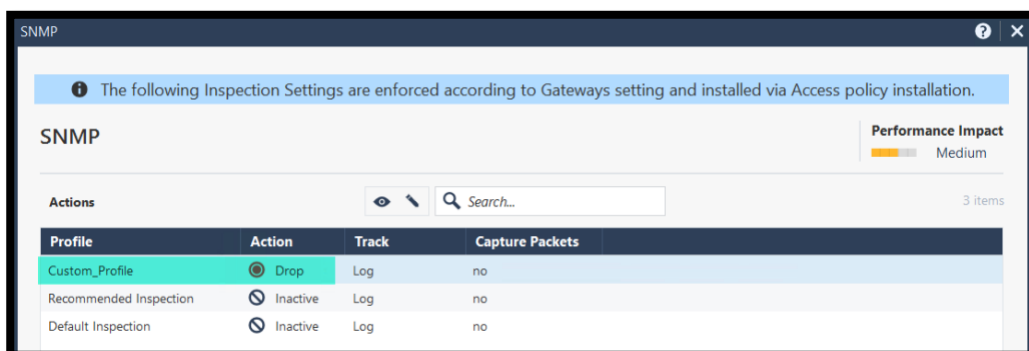
1. While in the Inspection Settings General View, search for the **SNMP** protocol settings and click **Edit** to customize the protocol settings.



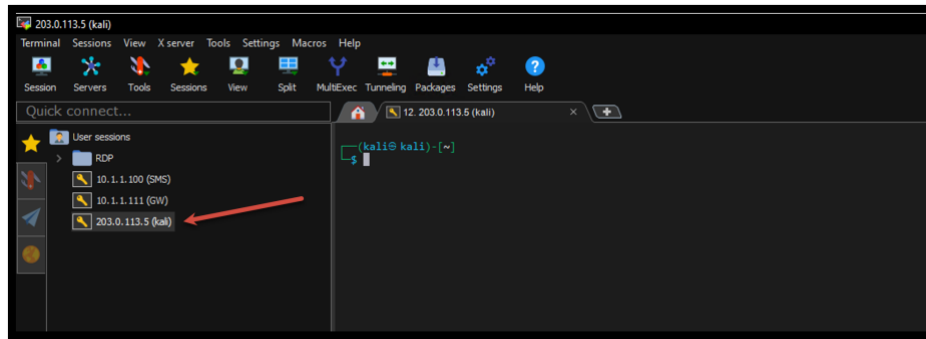
2. Select the **Custom Profile** and Click **Edit**. Then Allow only **SNMPv3** traffic under the Advanced settings window.



Note: The protection action will change to “Drop” when this option is selected.



3. Install the Access Control Policy.
4. Use the saved SSH session to login to the Kali Linux host and login **kali/Cpwins!1**.

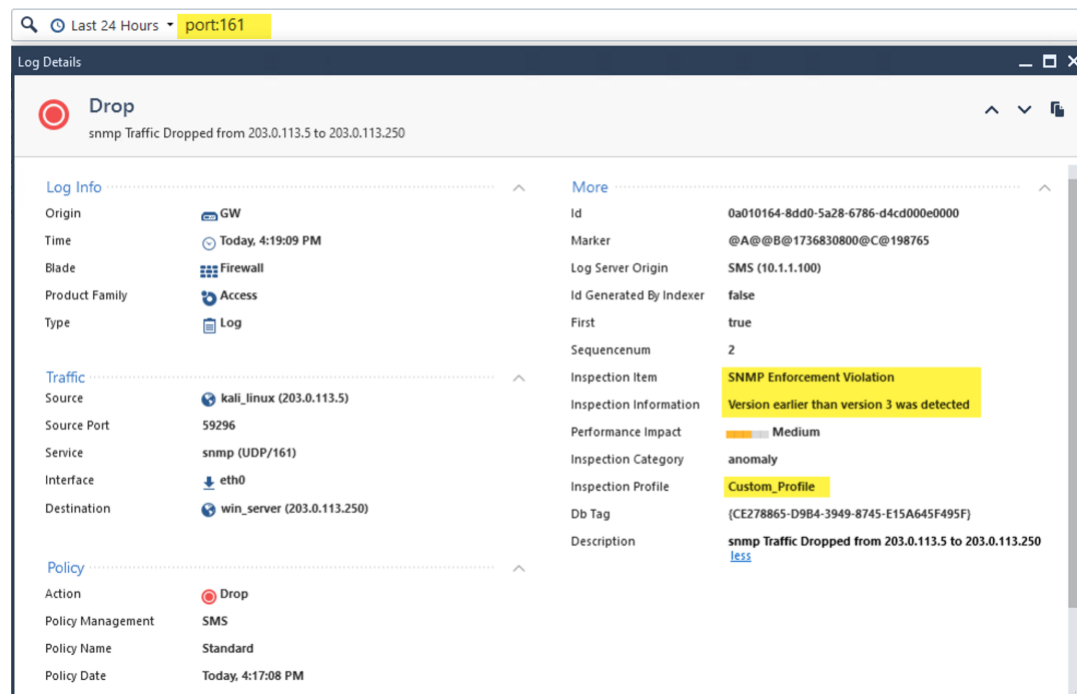


6. Open a terminal and run the command **snmp-check 203.0.113.250 -c public**

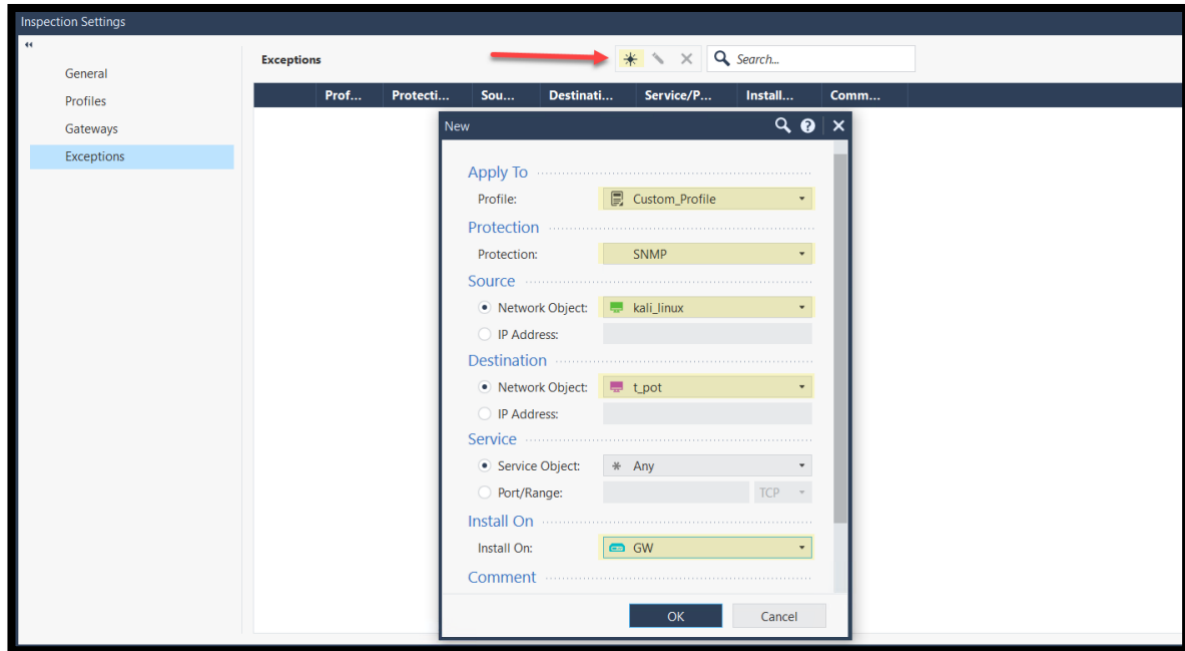
```
(kali@kali)-[~]
$ snmp-check 203.0.113.250 -c public
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 203.0.113.250:161 using SNMPv1 and community 'public'
[!] 203.0.113.250:161 SNMP request timeout
```

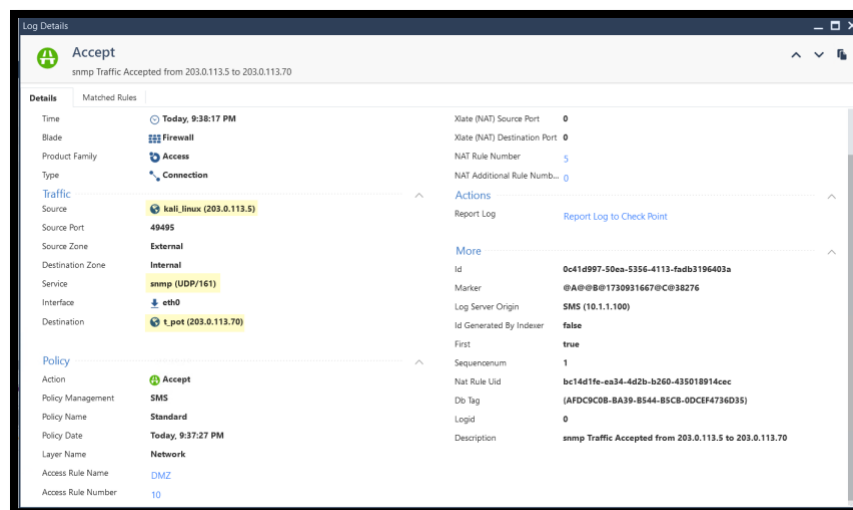
7. Review the logs; filter for traffic for **port:161** or type SNMP.



8. Open the inspection settings view and add a new exception. Make it specific to the Kali as a source. We do not want the changes we made to apply to this host.



9. Install the Access Policy.
10. Test the same command again to generate a new log.
11. Review the security logs and notice that the traffic is accepted by the access Rulebase and there are no logs related to inspection settings.



End of Lab 4