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.

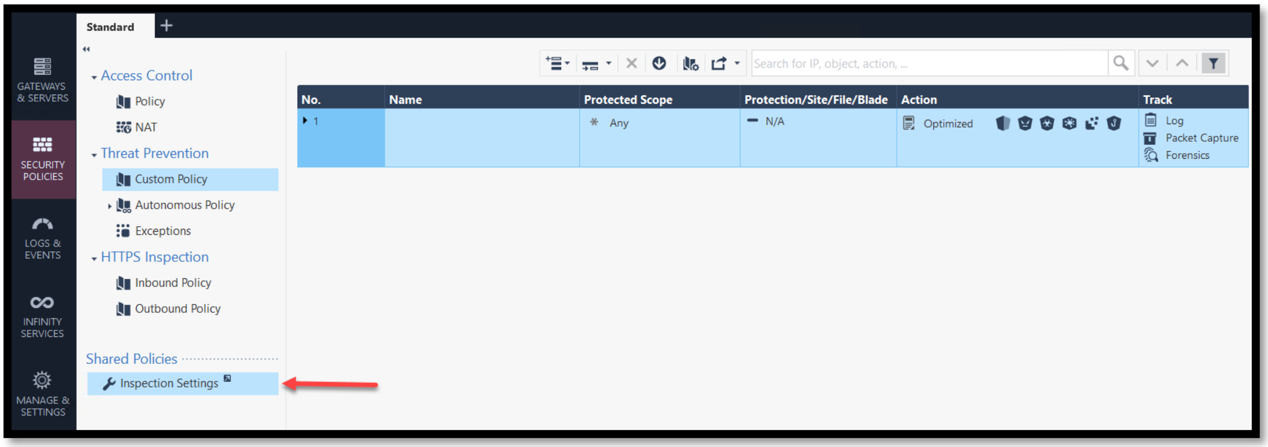
Exercise 1: Inspection Settings basics

The Security Management Server comes with two preconfigured inspection profiles:

- Default Inspection
- Recommended Inspection

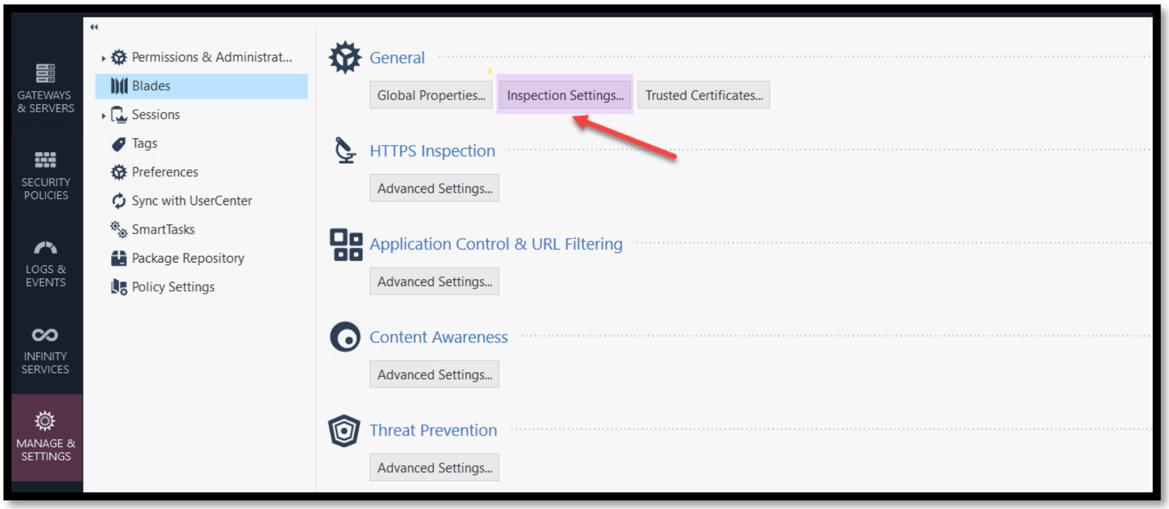
The Default Inspection profile is enabled by default. You can change the settings and assign the “Recommended Inspection” profile to the Security Gateway, or to create and assign a custom profile.

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

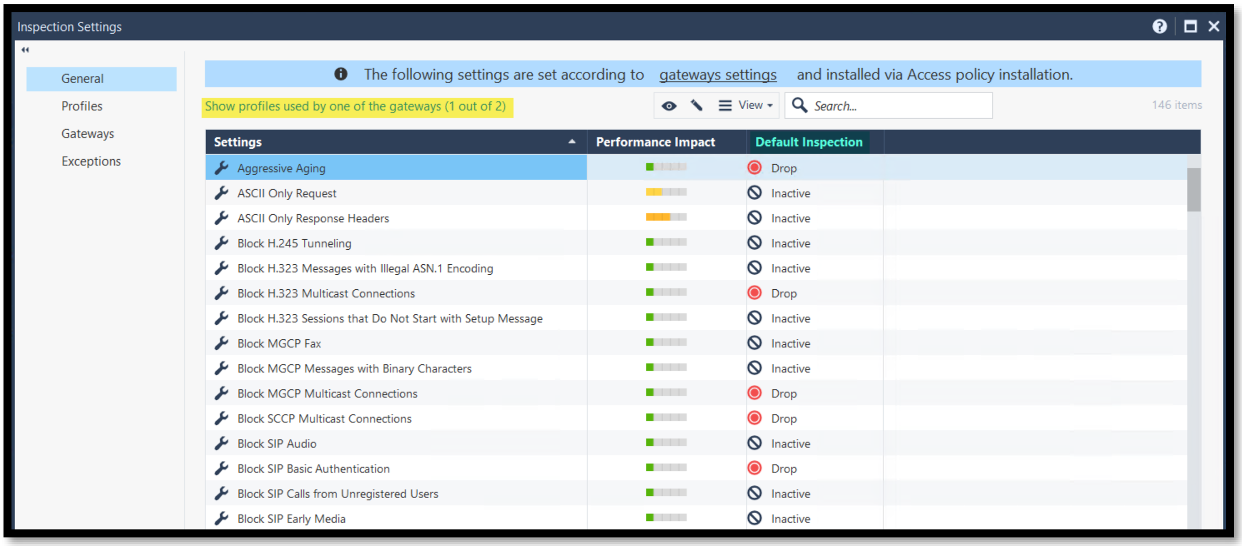


No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track
1		Any	N/A	Optimized	Log Packet Capture Forensics

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



2. 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.



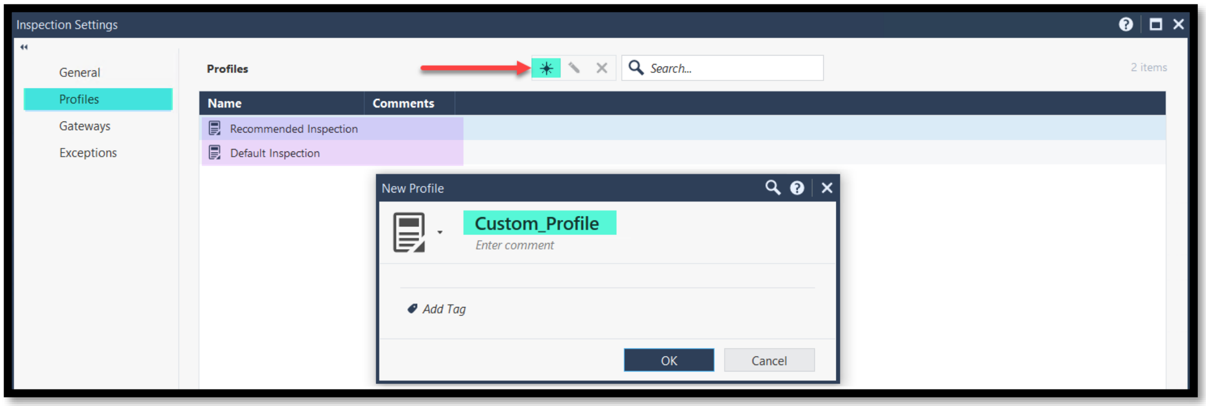
The following settings are set according to gateways settings and installed via Access policy installation.

Show profiles used by one of the gateways (1 out of 2)

Settings	Performance Impact	Default Inspection
Aggressive Aging	🟩	Drop
ASCII Only Request	🟨	Inactive
ASCII Only Response Headers	🟧	Inactive
Block H.245 Tunneling	🟩	Inactive
Block H.323 Messages with Illegal ASN.1 Encoding	🟩	Inactive
Block H.323 Multicast Connections	🟩	Drop
Block H.323 Sessions that Do Not Start with Setup Message	🟩	Inactive
Block MGCP Fax	🟩	Inactive
Block MGCP Messages with Binary Characters	🟩	Inactive
Block MGCP Multicast Connections	🟩	Drop
Block SCCP Multicast Connections	🟩	Drop
Block SIP Audio	🟩	Inactive
Block SIP Basic Authentication	🟩	Drop
Block SIP Calls from Unregistered Users	🟩	Inactive
Block SIP Early Media	🟩	Inactive

3. 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.



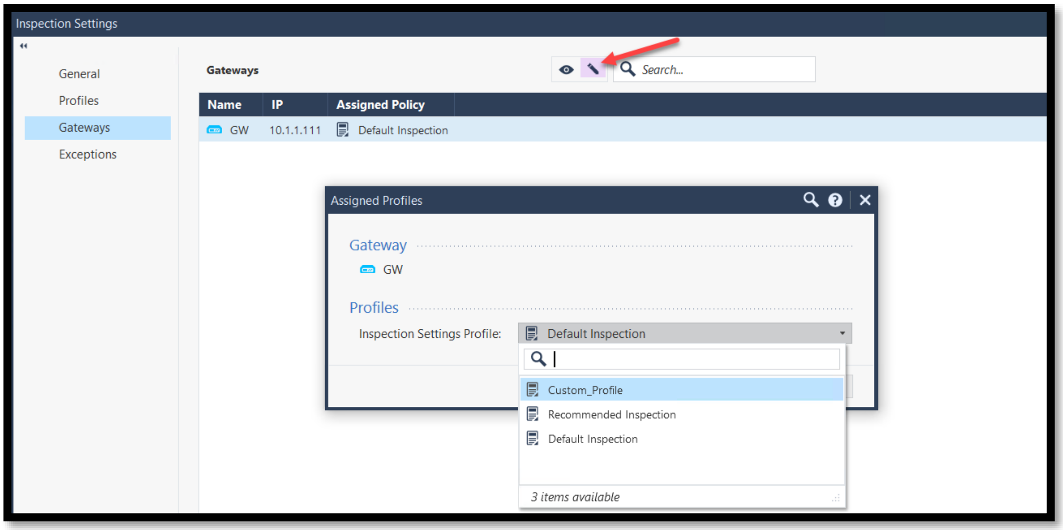
Name	Comments
Recommended Inspection	
Default Inspection	

Custom_Profile

Enter comment

Add Tag

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.



Name	IP	Assigned Policy
GW	10.1.1.111	Default Inspection

Gateway

GW

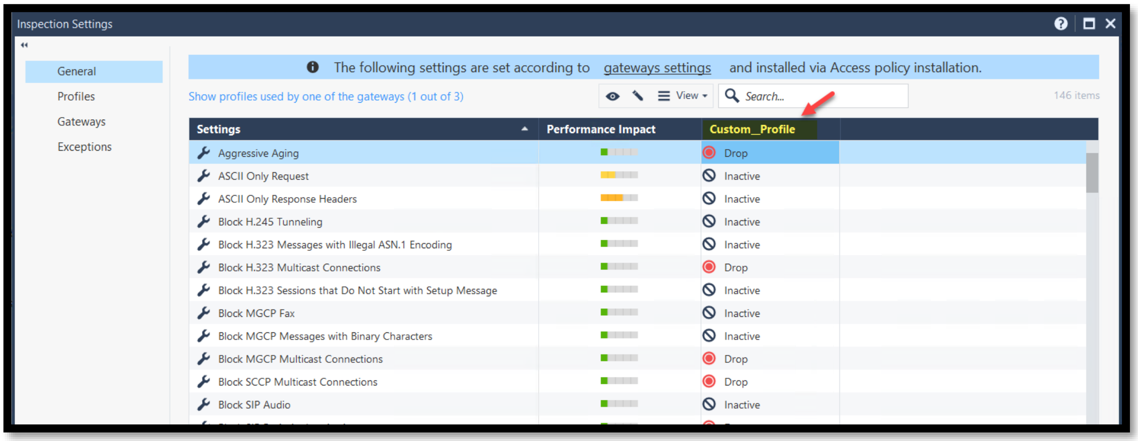
Profiles

Inspection Settings Profile: Default Inspection

Custom_Profile
Recommended Inspection
Default Inspection

3 items available

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



The following settings are set according to gateways settings and installed via Access policy installation.

Show profiles used by one of the gateways (1 out of 3)

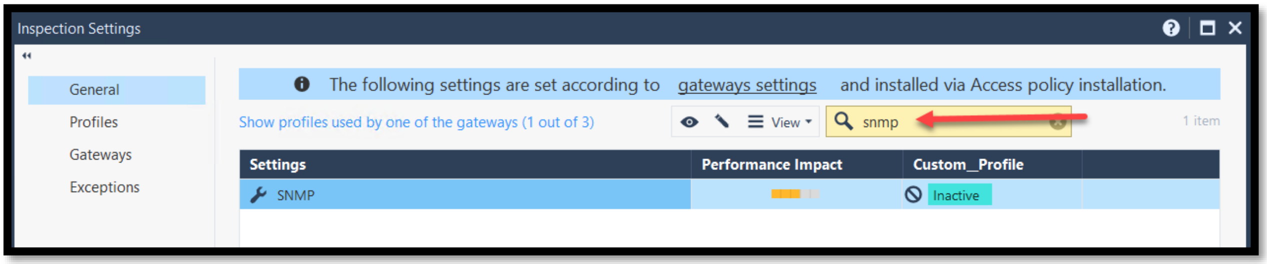
Settings	Performance Impact	Custom_Profile
Aggressive Aging	▮▯▯▯▯	Drop
ASCII Only Request	▮▮▯▯▯	Inactive
ASCII Only Response Headers	▮▮▮▯▯	Inactive
Block H.245 Tunneling	▮▯▯▯▯	Inactive
Block H.323 Messages with Illegal ASN.1 Encoding	▮▯▯▯▯	Inactive
Block H.323 Multicast Connections	▮▯▯▯▯	Drop
Block H.323 Sessions that Do Not Start with Setup Message	▮▯▯▯▯	Inactive
Block MGCP Fax	▮▯▯▯▯	Inactive
Block MGCP Messages with Binary Characters	▮▯▯▯▯	Inactive
Block MGCP Multicast Connections	▮▯▯▯▯	Drop
Block SCCP Multicast Connections	▮▯▯▯▯	Drop
Block SIP Audio	▮▯▯▯▯	Inactive

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.

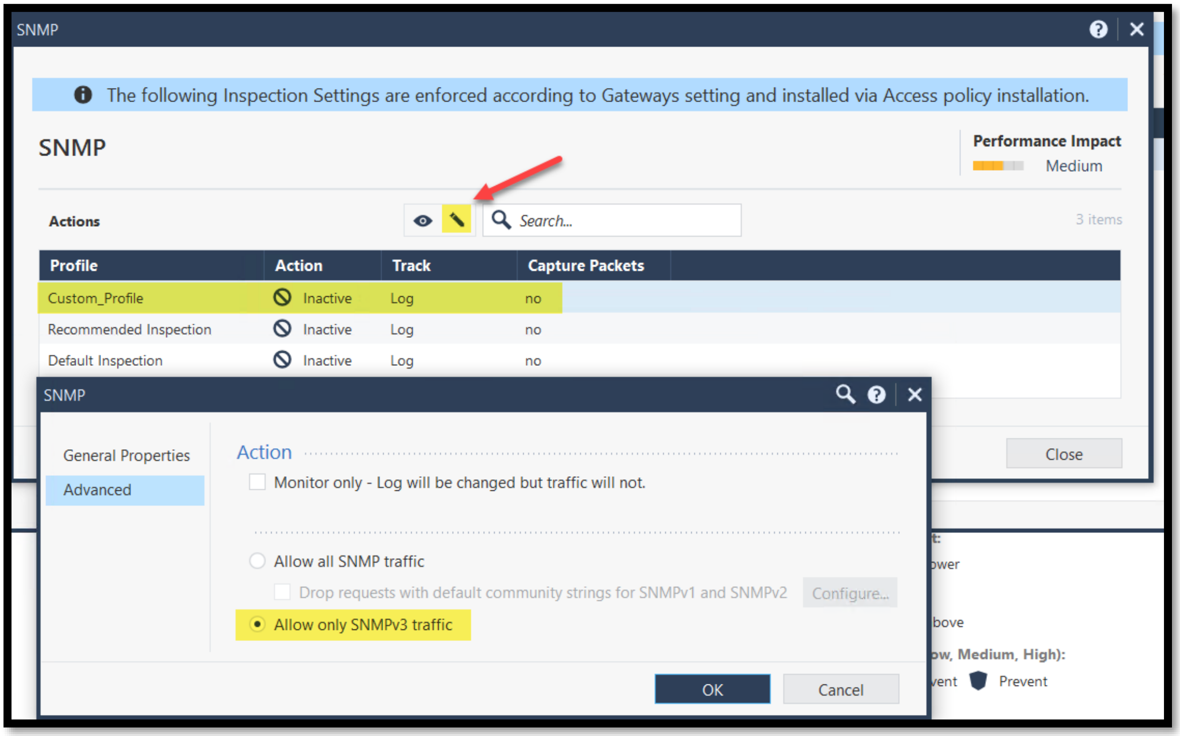


The following settings are set according to gateways settings and installed via Access policy installation.

Search: snmp

Settings	Performance Impact	Custom_Profile
SNMP		Inactive

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



The following Inspection Settings are enforced according to Gateways setting and installed via Access policy installation.

SNMP

Performance Impact: Medium

Profile	Action	Track	Capture Packets
Custom_Profile	Inactive	Log	no
Recommended Inspection	Inactive	Log	no
Default Inspection	Inactive	Log	no

Action

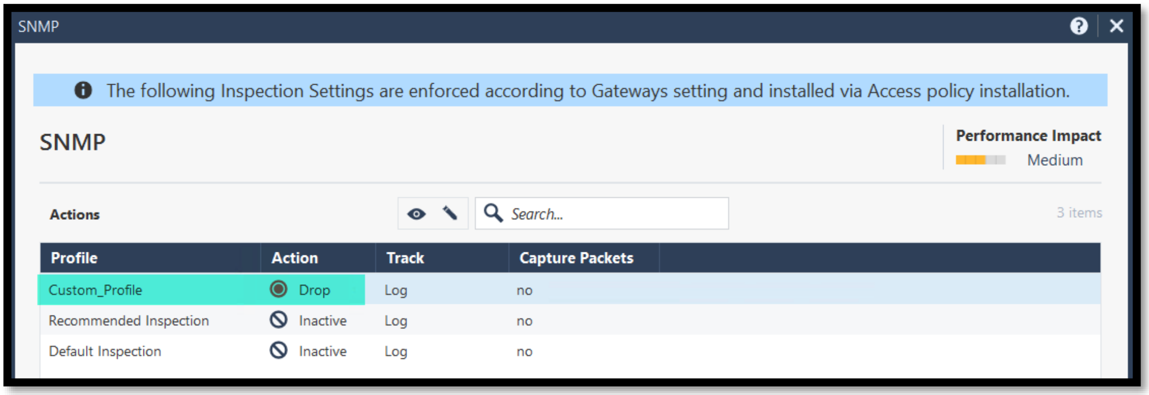
□ Monitor only - Log will be changed but traffic will not.

○ Allow all SNMP traffic

□ Drop requests with default community strings for SNMPv1 and SNMPv2

● Allow only SNMPv3 traffic

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



SNMP

The following Inspection Settings are enforced according to Gateways setting and installed via Access policy installation.

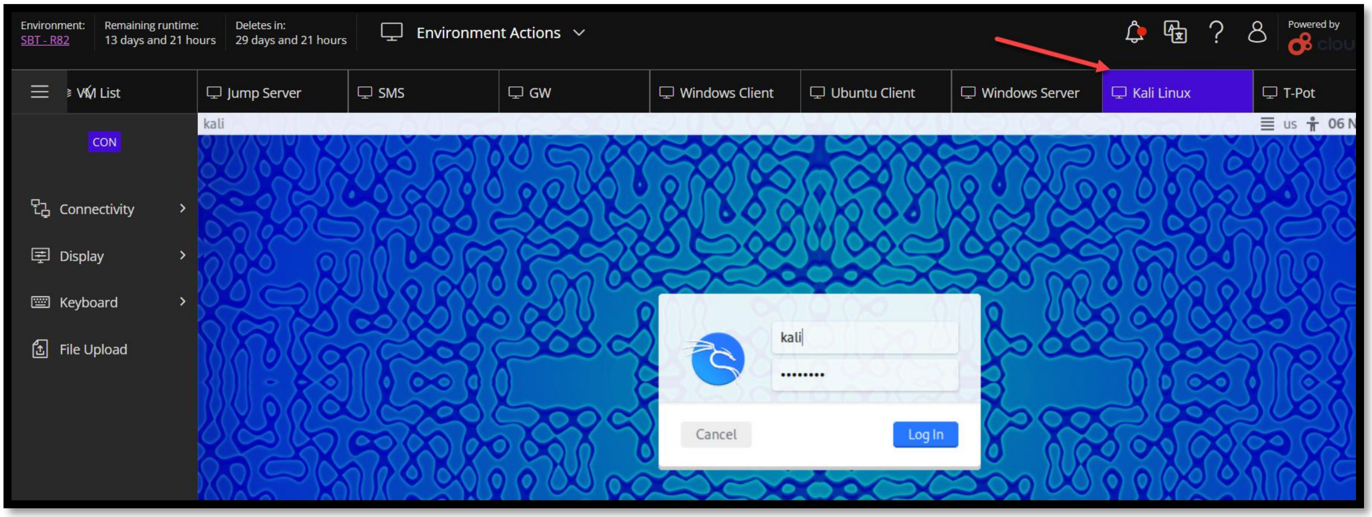
SNMP

Performance Impact: Medium

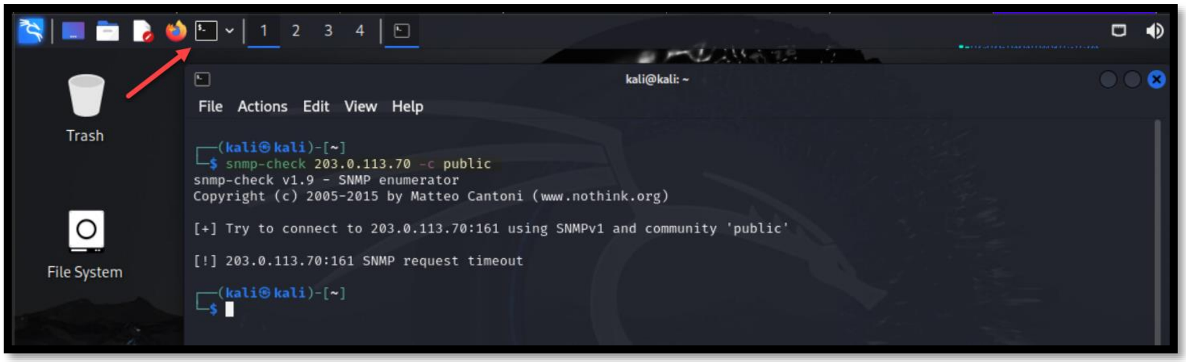
Actions — Search... — 3 items

Profile	Action	Track	Capture Packets
Custom_Profile	Drop	Log	no
Recommended Inspection	Inactive	Log	no
Default Inspection	Inactive	Log	no

3. Install the Access Policy.
4. In the training environment, navigate to the Kali Linux host and login with kali/Cpwins!1.

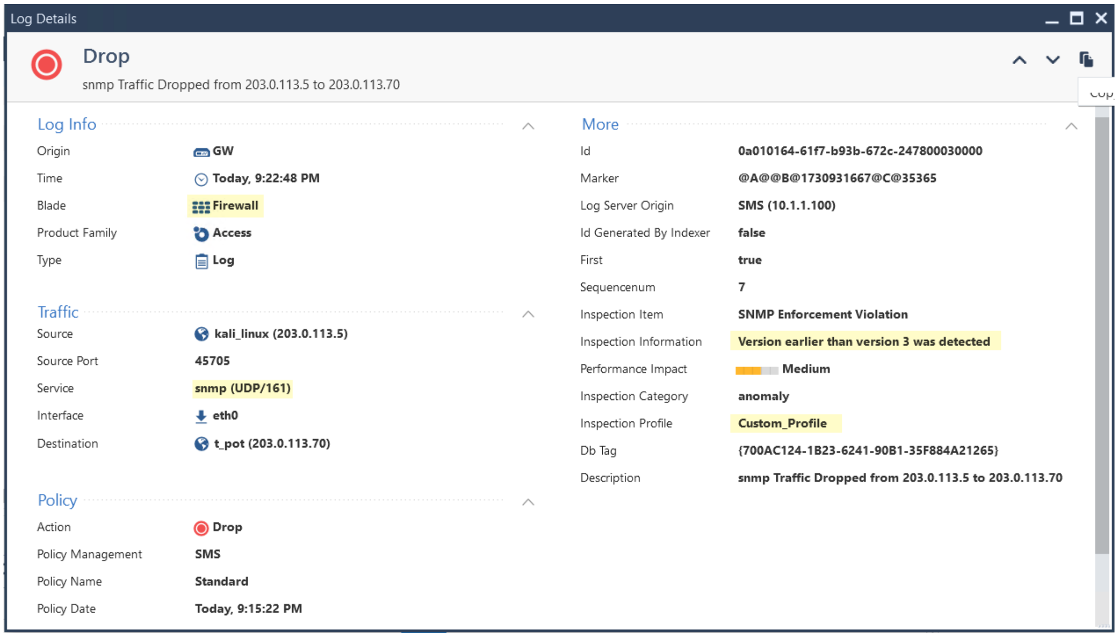


6. Open a terminal and run the command (snmp-check 203.0.113.70 -c public)



```
┌──(kali㉿kali)-[~]
└─$ snmp-check 203.0.113.70 -c public
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 203.0.113.70:161 using SNMPv1 and community 'public'

[!] 203.0.113.70:161 SNMP request timeout

┌──(kali㉿kali)-[~]
└─$ 
```

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



Log Details

Drop
snmp Traffic Dropped from 203.0.113.5 to 203.0.113.70

Log Info

Origin	GW
Time	Today, 9:22:48 PM
Blade	Firewall
Product Family	Access
Type	Log

Traffic

Source	kali_linux (203.0.113.5)
Source Port	45705
Service	snmp (UDP/161)
Interface	eth0
Destination	t_pot (203.0.113.70)

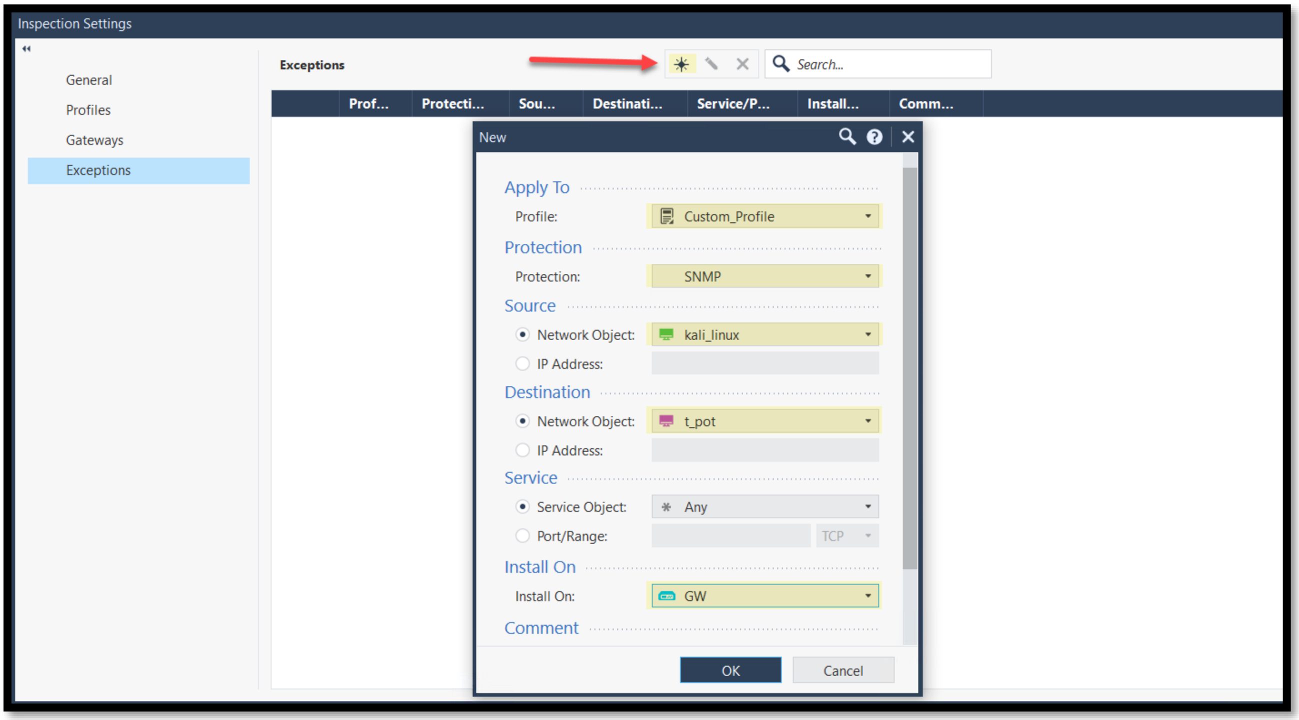
Policy

Action	Drop
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 9:15:22 PM

More

Id	0a010164-61f7-b93b-672c-247800030000
Marker	@A@@B@1730931667@C@35365
Log Server Origin	SMS (10.1.1.100)
Id Generated By Indexer	false
First	true
Sequencenum	7
Inspection Item	SNMP Enforcement Violation
Inspection Information	Version earlier than version 3 was detected
Performance Impact	Medium
Inspection Category	anomaly
Inspection Profile	Custom_Profile
Db Tag	{700AC124-1B23-6241-90B1-35F884A21265}
Description	snmp Traffic Dropped from 203.0.113.5 to 203.0.113.70

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.



New

Apply To
Profile: Custom_Profile

Protection
Protection: SNMP

Source
● Network Object: kali_linux
○ IP Address:

Destination
● Network Object: t_pot
○ IP Address:

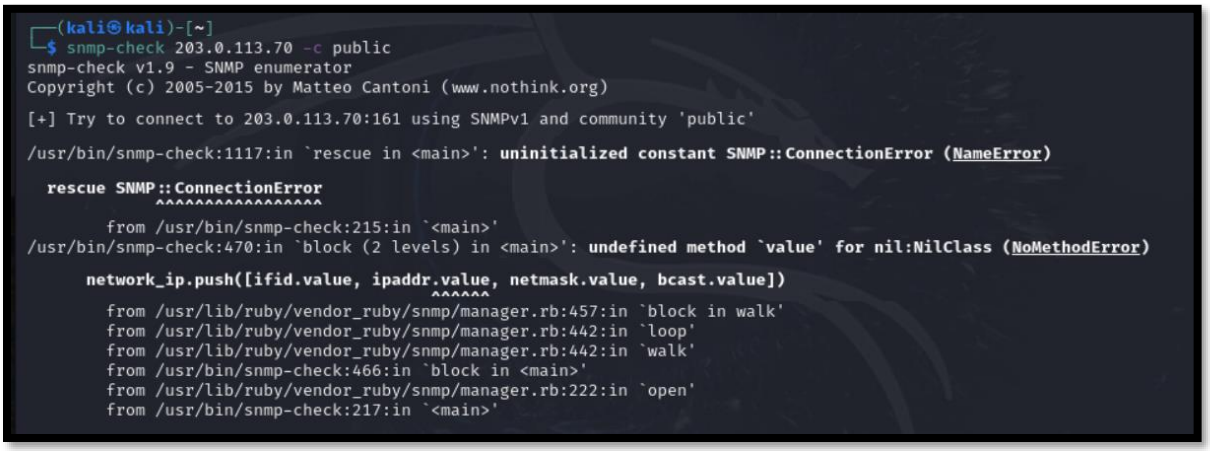
Service
● Service Object: Any
○ Port/Range: TCP

Install On
Install On: GW

Comment

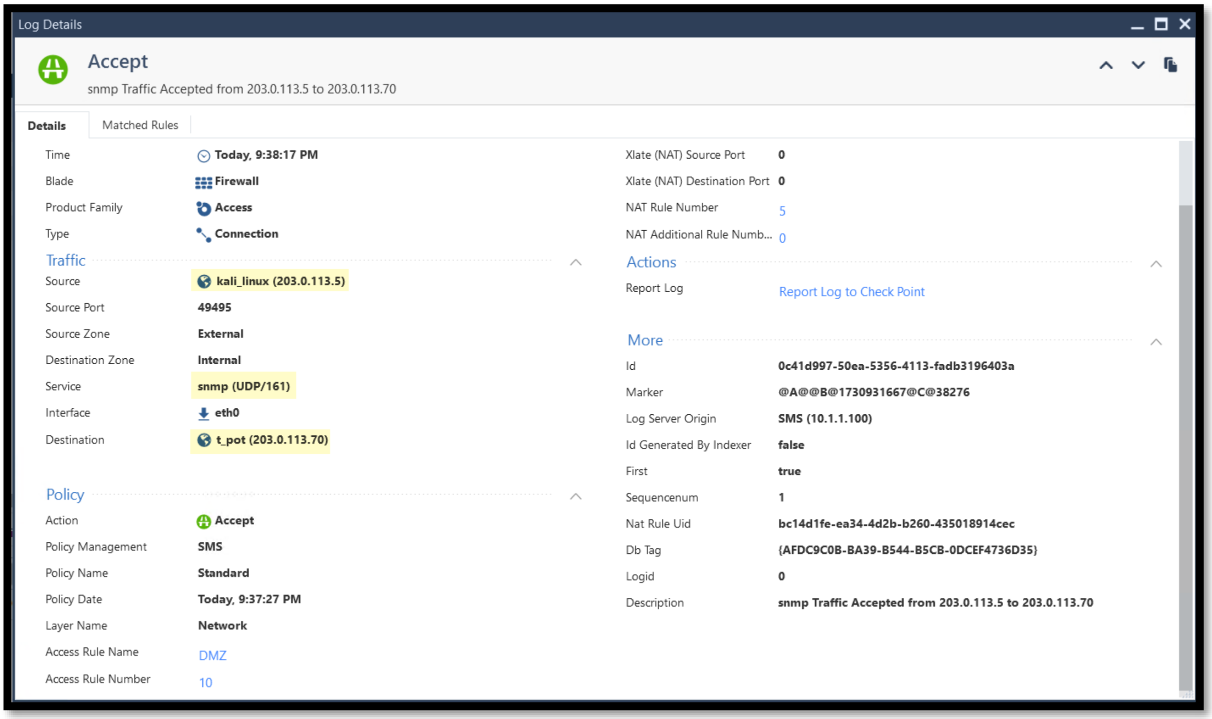
OK Cancel

9. Install the Access Policy.
10. Test the same command again. Notice that the command is returning some results.



```
┌──(kali㉿kali)-[~]
└─$ snmp-check 203.0.113.70 -c public
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 203.0.113.70:161 using SNMPv1 and community 'public'

/usr/bin/snmp-check:1117:in `rescue in <main>': uninitialized constant SNMP::ConnectionError (NameError)

  rescue SNMP::ConnectionError
             ^^^^^^^^^^^^^^^^^

        from /usr/bin/snmp-check:215:in `<main>'
/usr/bin/snmp-check:470:in `block (2 levels) in <main>': undefined method `value' for nil:NilClass (NoMethodError)

      network_ip.push([ifid.value, ipaddr.value, netmask.value, bcast.value])
                                         ^^^^^^
        from /usr/lib/ruby/vendor_ruby/snmp/manager.rb:457:in `block in walk'
        from /usr/lib/ruby/vendor_ruby/snmp/manager.rb:442:in `loop'
        from /usr/lib/ruby/vendor_ruby/snmp/manager.rb:442:in `walk'
        from /usr/bin/snmp-check:466:in `block in <main>'
        from /usr/lib/ruby/vendor_ruby/snmp/manager.rb:222:in `open'
        from /usr/bin/snmp-check:217:in `<main>'
```

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.



Log Details

Accept

snmp Traffic Accepted from 203.0.113.5 to 203.0.113.70

Details | Matched Rules

Time	Today, 9:38:17 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	kali_linux (203.0.113.5)
Source Port	49495
Source Zone	External
Destination Zone	Internal
Service	snmp (UDP/161)
Interface	eth0
Destination	t_pot (203.0.113.70)

Policy

Action	Accept
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 9:37:27 PM
Layer Name	Network
Access Rule Name	DMZ
Access Rule Number	10

Xlate (NAT) Source Port	0
Xlate (NAT) Destination Port	0
NAT Rule Number	5
NAT Additional Rule Numb...	0

Actions

Report Log	Report Log to Check Point

More

Id	0c41d997-50ea-5356-4113-fadb3196403a
Marker	@A@@B@1730931667@C@38276
Log Server Origin	SMS (10.1.1.100)
Id Generated By Indexer	false
First	true
Sequencenum	1
Nat Rule Uid	bc14d1fe-ea34-4d2b-b260-435018914cec
Db Tag	{AFDC9C0B-BA39-B544-B5CB-0DCEF4736D35}
Logid	0
Description	snmp Traffic Accepted from 203.0.113.5 to 203.0.113.70