Peter Elmer, February 2019

Support for Custom Intelligence Feeds

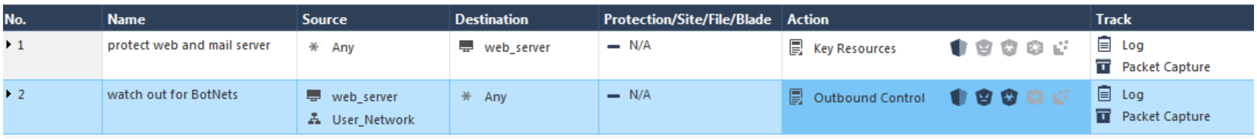
Many government customers and some vertical markets require the gateway importing 'Indicators of Compromise' from intelligence sources relevant for this market. These indicators are available in the form of feeds providing information in the form of csv or STIX (Structured Threat Indication eXpression) format.

Check Point Security Gateways can consume these intelligence feeds in the Antivirus and Anti-Bot Blade following the instructions given in sk132193. The solution is qualified for all R80.20 releases (GA and any JHF) and for a gateway running R80.10 and JHF 121. Note that only the JHF 121 is supported. In case you require the function to be ported to a different R80.10 JHF please contact Solution Center.

The following notes have been taken testing the function using a feed found at MISP (Open Standards Threat Intelligence Platform) https://www.misp-project.org/features.html. In the test access to a Zeus node is successfully blocked.

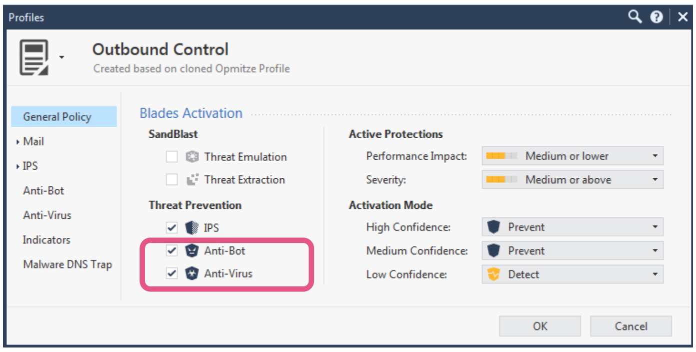
Threat Prevention rule base

Using source / destination logic is making the policy easier to be read.



No.	Name	Source	Destination	Protection/Site/File/Blade	Action	Track
1	protect web and mail server	Any	web_server	N/A	Key Resources	Log Packet Capture
2	watch out for BotNets	web_server User_Network	Any	N/A	Outbound Control	Log Packet Capture

Make sure the Antivirus and Anti-Bot Blades are being active in the threat prevention profile and the 'use indicators' flag is set.



Outbound Control
Created based on cloned Opmitze Profile

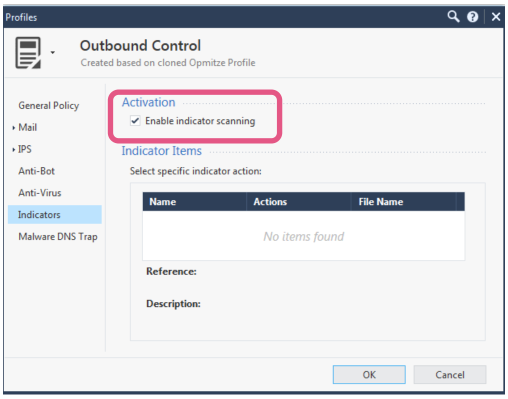
Blades Activation

SandBlast
- □ Threat Emulation
- □ Threat Extraction

Threat Prevention
- ☑ IPS
- ☑ Anti-Bot
- ☑ Anti-Virus

Active Protections
- Performance Impact: Medium or lower
- Severity: Medium or above

Activation Mode
- High Confidence: Prevent
- Medium Confidence: Prevent
- Low Confidence: Detect



Outbound Control
Created based on cloned Opmitze Profile

Activation
- ☑ Enable indicator scanning

Indicator Items

Select specific indicator action:

Name	Actions	File Name
No items found		

Reference:

Description:

Configure the ‘Custom Intelligence Feed’

The configuration of the feed(s) is controlled using CLI commands. You can add and remove feeds and define the download interval defining the schedule to fetch updated content from the feed.

This default schedule interval for downloading and updating the feeds is defined to the value of 300 seconds. Note that there might be feeds blocking the download at such a short intervals and you may need to increase the interval. For example the TOR nodes list at MISP allows a minimum interval of 30 minutes.

Configure the feeds update interval

Check the current defined interval

```
[Expert@r8020gw:0]# ioc_feeds show_interval
Feeds will be fetched every 300 seconds
[Expert@r8020gw:0]#
```

Define an interval of 1800 seconds

```
[Expert@r8020gw:0]# ioc_feeds set_interval 1800
Setting interval to 1800
```

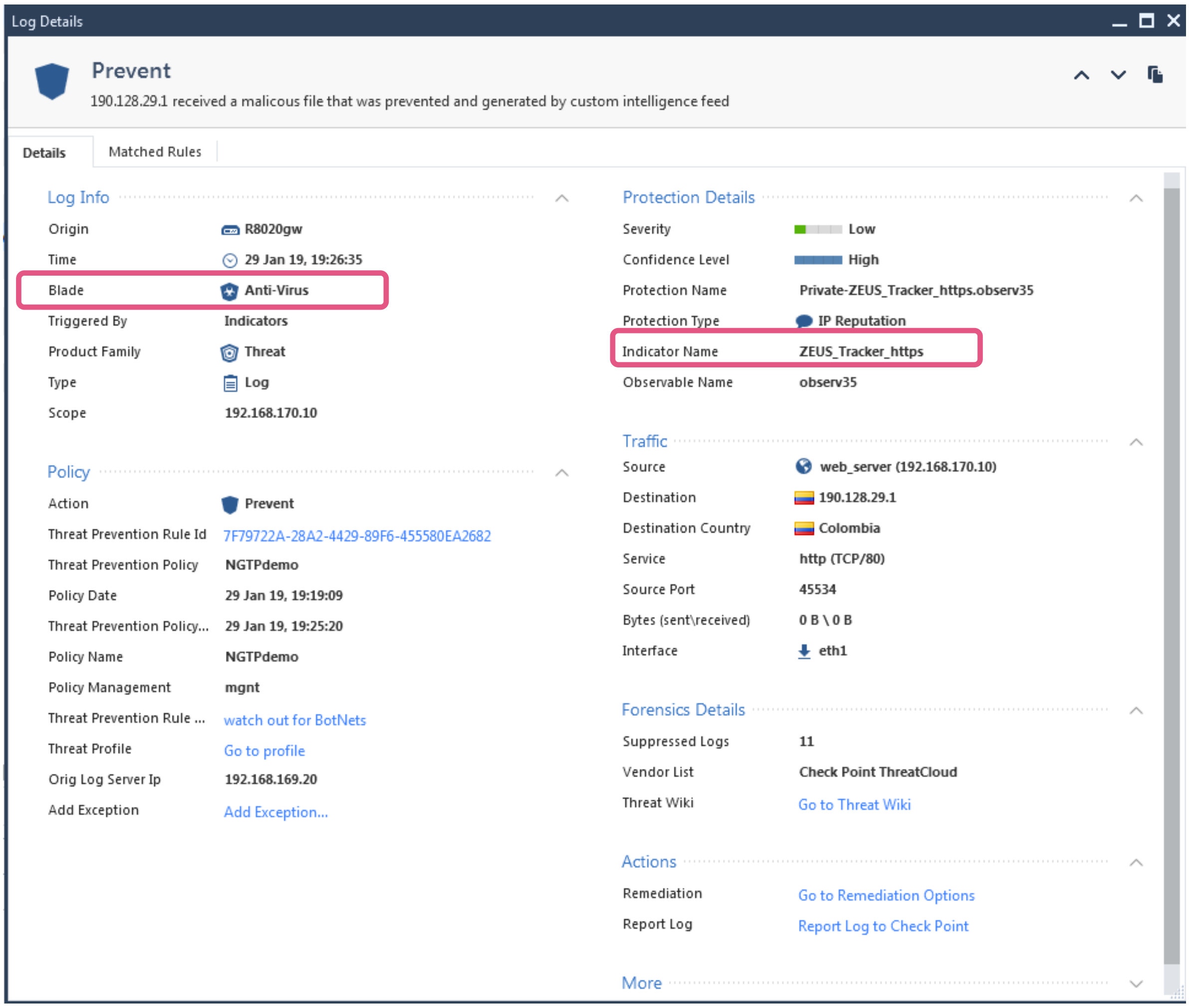
Adding a feed to the system

The following example is adding the list of Zeus nodes to the system

```
[Expert@r8020gw:0]# ioc_feeds add --feed_name ZEUS_Tracker --transport https --
resource "https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist" --format
[value:1,type:ip] --comment [#]

Default value for active is: true
Default value for feed_action is: prevent

Feed Name: ZEUS_Tracker
Feed is Active
File will be fetched via HTTPS
Resource: https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist
Action: Prevent

[============================================================] 100.0% ...Getting file
from the server
The server security certificate is not trusted by your machine.
SHA256
Fingerprint=6D:88:53:54:C6:39:AB:13:1D:76:6A:4E:AA:00:24:F8:40:F0:45:26:A7:D8:EF:3F:7B
:3E:1A:1E:5B:21:BD:5C

Fetching active feeds
Convert your csv format to Check Point's supported csv format. Supported fields:
[name,value,type,confidence,severity,product,comment]
All content coming after  ['#']  will be ignored

[Name, Value, Type]
observ1,101.200.81.187,ip,,,,
observ2,103.19.89.118,ip,,,,
observ3,103.230.84.239,ip,,,,
observ4,103.4.52.150,ip,,,,
observ5,103.7.59.135,ip,,,,
observ6,104.247.219.41,ip,,,,
observ7,109.127.8.242,ip,,,,
observ8,109.229.210.250,ip,,,,
observ9,109.229.36.65,ip,,,,
observ10,113.29.230.24,ip,,,,
observ11,120.31.134.133,ip,,,,
Successfully converted
Convert your csv format to Check Point's supported csv format. Supported fields:
[name,value,type,confidence,severity,product,comment]

[Name, Value, Type]

Successfully converted
Signatures loaded successfully

Update summary
##############
feed: ZEUS_Tracker. Status: Succeed
##############
Activating Scheduler

[Expert@r8020gw:0]#
```

Verify information provided by the feed is consumed by the gateway

You can access one of the known Zeus IP Addresses and then check the log messages.



Prevent

190.128.29.1 received a malicous file that was prevented and generated by custom intelligence feed

Log Info

Origin	R8020gw
Time	29 Jan 19, 19:26:35
Blade	Anti-Virus
Triggered By	Indicators
Product Family	Threat
Type	Log
Scope	192.168.170.10

Policy

Action	Prevent
Threat Prevention Rule Id	7F79722A-28A2-4429-89F6-455580EA2682
Threat Prevention Policy	NGTPdemo
Policy Date	29 Jan 19, 19:19:09
Threat Prevention Policy...	29 Jan 19, 19:25:20
Policy Name	NGTPdemo
Policy Management	mgnt
Threat Prevention Rule ...	watch out for BotNets
Threat Profile	Go to profile
Orig Log Server Ip	192.168.169.20
Add Exception	Add Exception...

Protection Details

Severity	Low
Confidence Level	High
Protection Name	Private-ZEUS_Tracker_https.observ35
Protection Type	IP Reputation
Indicator Name	ZEUS_Tracker_https
Observable Name	observ35

Traffic

Source	web_server (192.168.170.10)
Destination	190.128.29.1
Destination Country	Colombia
Service	http (TCP/80)
Source Port	45534
Bytes (sent\received)	0 B \ 0 B
Interface	eth1

Forensics Details

Suppressed Logs	11
Vendor List	Check Point ThreatCloud
Threat Wiki	Go to Threat Wiki

Actions

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