Overview

In order to prevent successful cyberattacks, many organizations collect indicators of compromise (IOCs) from various threat intelligence providers with the intent of creating new controls for their security devices. Unfortunately, legacy approaches to aggregation and enforcement are highly manual in nature, often creating complex workflows and extending the time needed to identify and validate which IOCs should be blocked.

Now security organizations can leverage MineMeld, an open-source application that streamlines the aggregation, enforcement and sharing of threat intelligence. This lab will walk you through the deployment and initial configuration of Mine Meld as a dynamic data feed into your Palo Alto Networks firewall.

Objective

The purpose of this lab is to familiarize you with Palo Alto's MineMeld product and to demonstrate how to aggregate multiple threat feeds to utilize the threat intelligence on a Palo Alto firewall. By the end of the lab we will have a MineMeld instance configure, know how to configure threat feeds, and populate our Palo Alto firewall with IoC and SaaS service information.

Tools of the Trade

You will need to download Palo Alto's MineMeld OVA as well install VirtualBox or VMWare Workstation Player to run an instance of MineMeld for this lab.

✓ VirtualBox
or
✓ VMware Workstation Player
And
✓ Minemeld OVA

Target Device

Palo Alto Firewall(s) with PANOS 7.1.x or greater

MineMeld VM

Getting Started

Though there are multiple ways to install MineMeld for the purpose of this lab we will be using the OVA image that has MineMeld preconfigured.

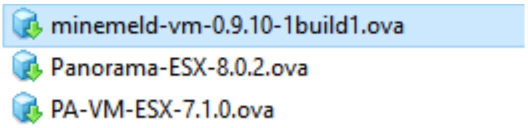
1. To set up a lab installation, Download MineMeld OVA from the following link:

https://s3-eu-west-1.amazonaws.com/minemeld-dist/0_9/minemeld-vm-0.9.10-1build1.ova

The OVA is an original Ubuntu 14.04 image with a preconfigured MineMeld instance.

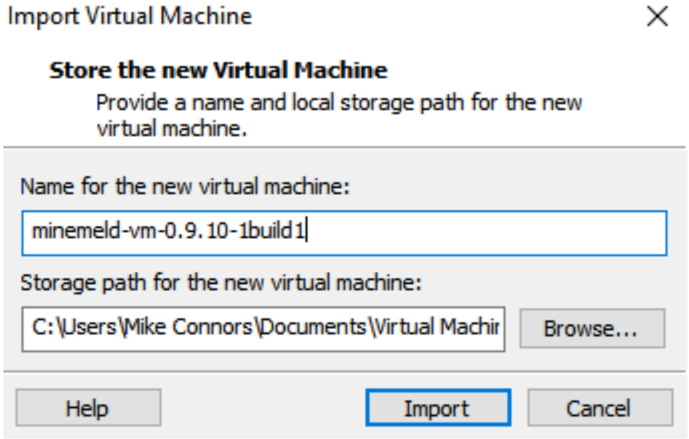
Importing the OVA

1. In VMWare - Select File > open.. and brose to the location where the OVA was downloaded.



minemeld-vm-0.9.10-1build1.ova
Panorama-ESX-8.0.2.ova
PA-VM-ESX-7.1.0.ova

2. Name the VM and select the path where you wish to install the instance.



Import Virtual Machine

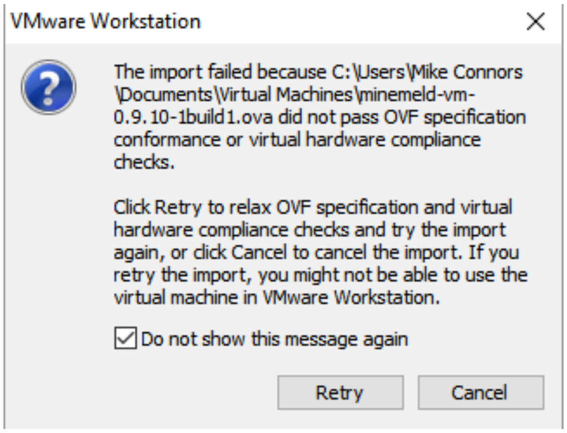
Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine: minemeld-vm-0.9.10-1build1

Storage path for the new virtual machine: C:\Users\Mike Connors\Documents\Virtual Machir

NOTE. If VMWare throws an error about the OVF format just press 'Retry'



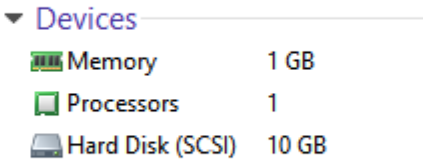
VMware Workstation

The import failed because C:\Users\Mike Connors \Documents\Virtual Machines\minemeld-vm-0.9.10-1build1.ova did not pass OVF specification conformance or virtual hardware compliance checks.

Click Retry to relax OVF specification and virtual hardware compliance checks and try the import again, or click Cancel to cancel the import. If you retry the import, you might not be able to use the virtual machine in VMware Workstation.

☑ Do not show this message again

The VM will be provisioned with minimal resources. For the purpose of this lab the default setting is adequate.



Devices

Memory	1 GB
Processors	1
Hard Disk (SCSI)	10 GB

Accessing MineMeld VM shell

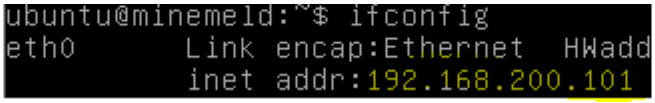
1. Start the VM, Once the system is booted the Default credentials for shell access are:

   Username: **ubuntu**
   Password: **rsplizardspock**

2. Upon boot the MineMeld image will check for the latest version (as of this writing 9.44 is current release) if there is outbound connectivity. It is good practice to verify that you are running the latest instance. To update MineMeld once booted issue:

   >sudo minemeld-auto-update

3. Obtain the IP of the instance and are ready to log into MineMeld. Issuing 'ifconfig' at the cli and taking note of the IP.



```
ubuntu@minemeld:~$ ifconfig
eth0      Link encap:Ethernet  HWadd
          inet addr:192.168.200.101
```

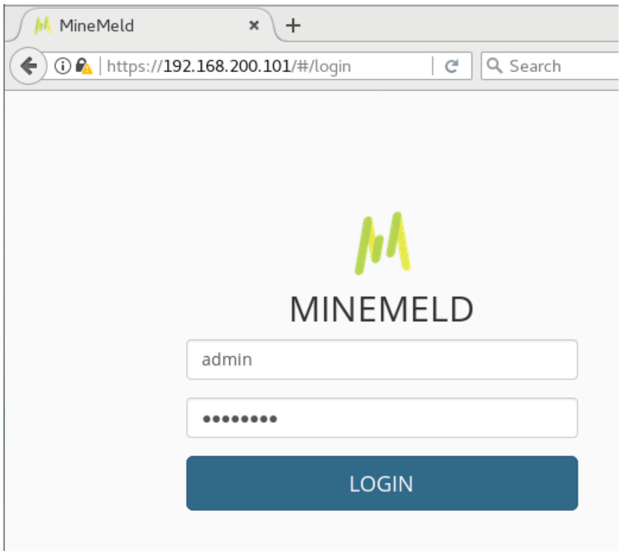
For this lab we are using 192.168.200.101

Accessing MineMeld WebUI

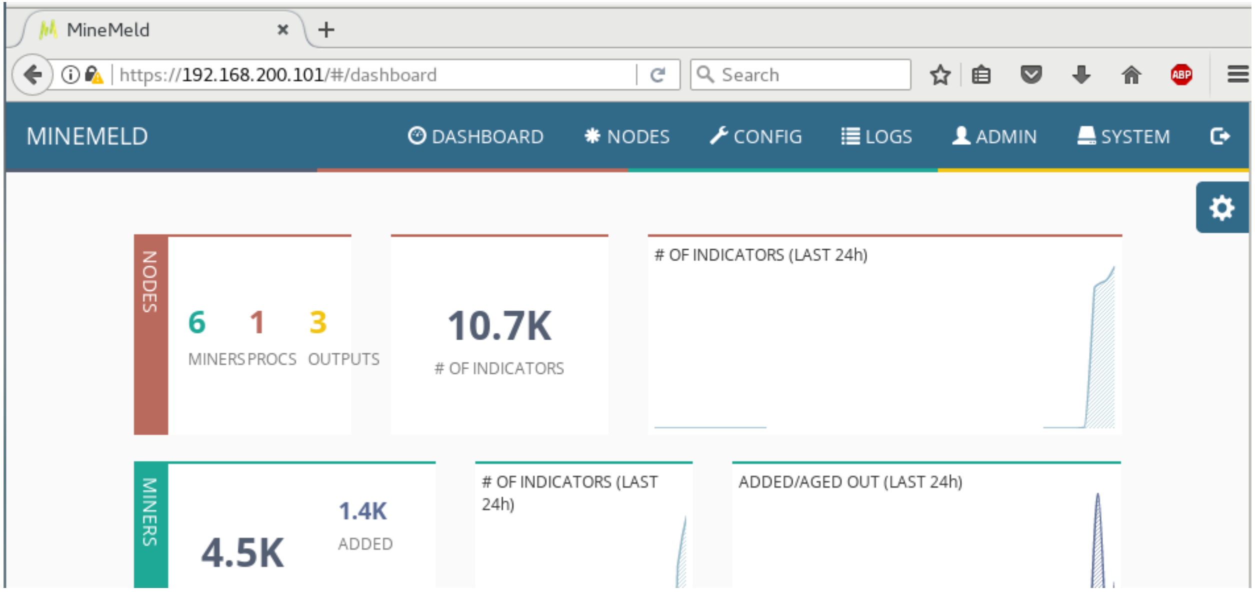
1. Open a webbrowser and enter https://<your-MineMeld-ip-address>. For this lab https://192.168.200.101

2. Default credentials for WebUI access are are:

Username: **admin**
Password: **minemeld**



After successful login to MineMeld you'll see the Dashboard



MineMeld Concepts

It is important to familiarize yourself with some of the basic concepts that MineMeld uses. The core concepts to understand are Nodes, Miners, Process, and Outputs.

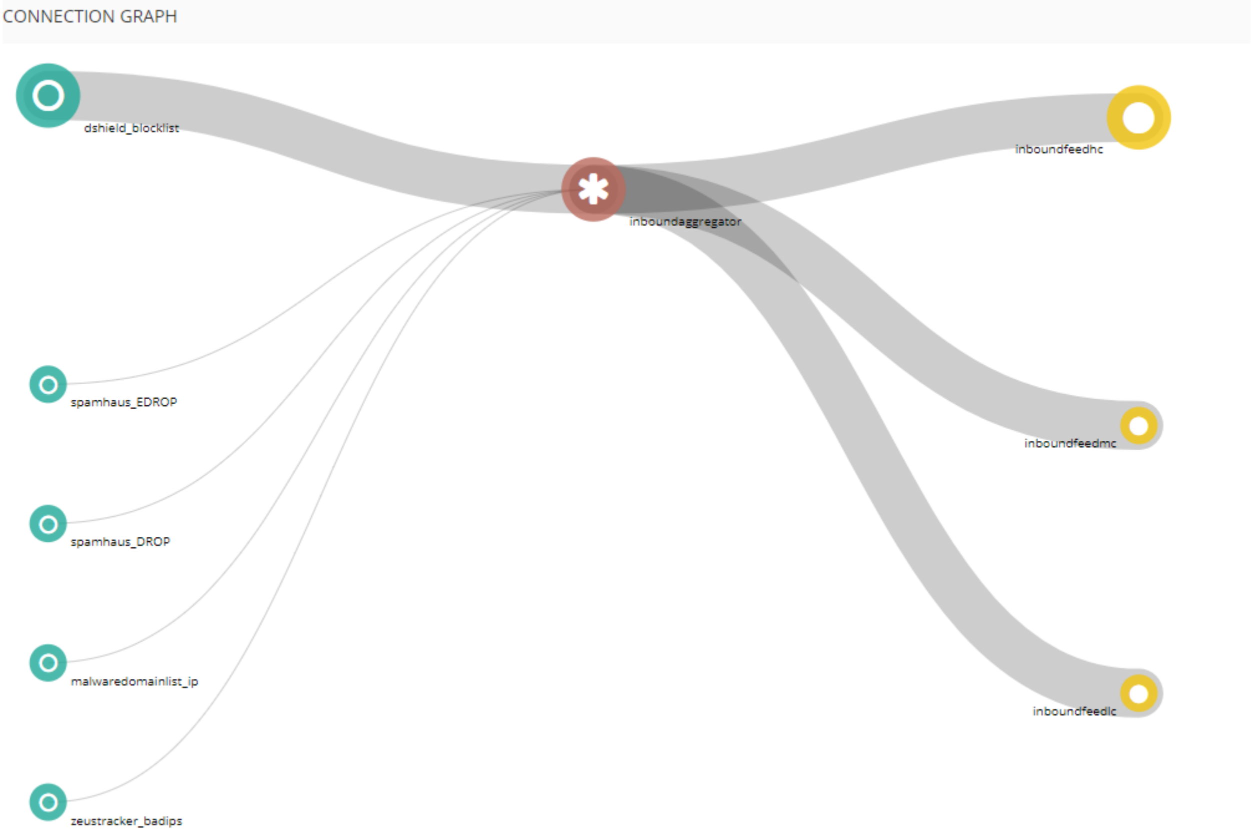
A node is defined as having:

- Name - A unique node name.
- Inputs - A list of nodes the node should receive messages from.
- Output - A boolean value that enables/disables messages to downstream nodes.
- Class - Defines which kind of processing is applied to indicators. Defines what is actually done by the node
- Config - Configuration of the node class.

Example of types of nodes and their function

Node Icon	Description
◎	Miner Node - responsible for periodically retrieving indicators from different feeds and removing indicators
✱	Process Node- aggregates indicators received from miners and sends downstream the aggregated indicators.
○	Output Node - receive indicators from the processor nodes and transform them into a format that could be directly consumed by Palo Alto Firewall(s)

In the following graph, the process node inboundaggregator has spamhaus_DROP, spamhaus_EDROP and dshield_blocklist as miner input nodes. If a node has no input nodes it is considered a Miner. In the following graph spamhaus_DROP, spamhaus_EDROP and dshield_blocklist have no input nodes because they are Miners.



Miners and are responsible for periodically retrieving indicators from different feeds and pushing them downstream to the connected nodes using update messages. Miners are also responsible for aging out indicators: when indicators disappear from the original feed or when an indicator is considered dead, the corresponding Miner instructs the downstream nodes of removing the indicator via a withdraw message.

From the above graph the central red node is a Processor node. In this specific configuration, the processor node is an IPv4 aggregator node and aggregates IPv4 indicators received from the 5 Miners and sends downstream the aggregated indicators.

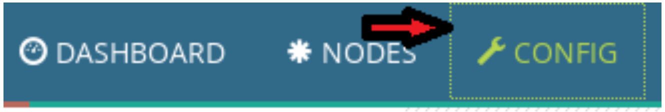
The 3 yellow nodes on the right are Output nodes. These nodes receive indicators from the processor nodes and transform them into a format that could be directly consumed by Palo Alto firewalls. In the default config the 3 output nodes translate the indicators received from the aggregator node into a format that can be consumed using the PAN-OS External Dynamic List (EDL) feature. All 3 output nodes in this graph receive the same set of indicators from the aggregator node, but each of them stores a different subset of these indicators based on the configured input filters. inboundfeedhc accepts only indicators with confidence level > 75, inboundfeedmc only indicators with confidence level < 75 and > 50, inboundfeedlc indicators with confidence level < 50. These subsets of indicators are stored into 3 different EDLs that can be used in different ways inside the PAN-OS configuration.

Configure a Node set for Use on Firewall

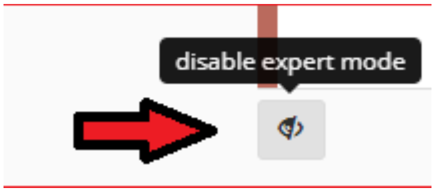
For this lab we will be using the default output nodes inboundfeedhc and inboundfeedmc, adding *zeustracker.badips* and *malwaredomainlist.ip* miners to the aggregation process inboundaggregator. Remember that inboundfeedhc accepts only indicators with confidence level > 75, inboundfeedmc only indicators with confidence level < 75 and > 50.

To Add the Miners:

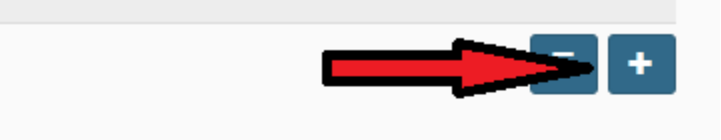
1. In MineMeld, Click config



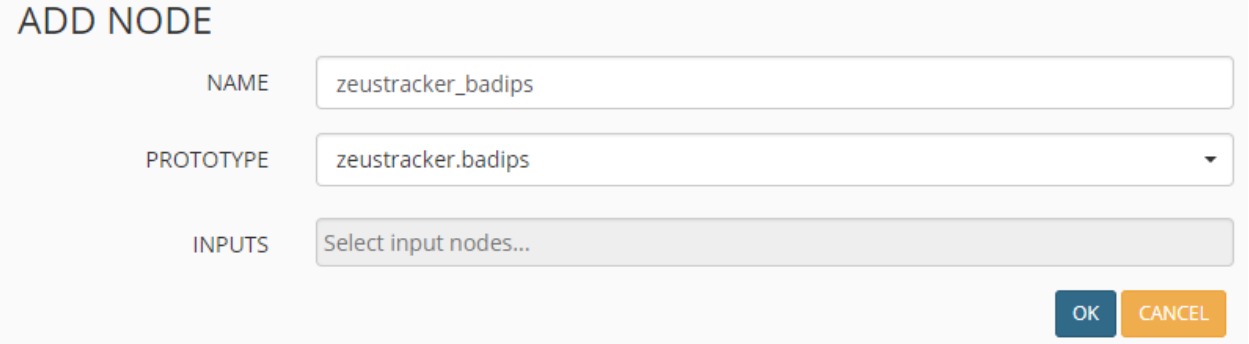
Note: Verify you are in 'expert mode'. The eye in the bottom lower left corner should have a strike through it.



2. Click on the + icon in the lower right corner



3. Add 'zeustracker.badips' which has a confidence level 100 so will be aggregated into the high confidence output (inboundfeedhc)
   - Name: zeustracker_badips
   - Prototype: zeustracker.badips
   - Inputs: inboundaggregator



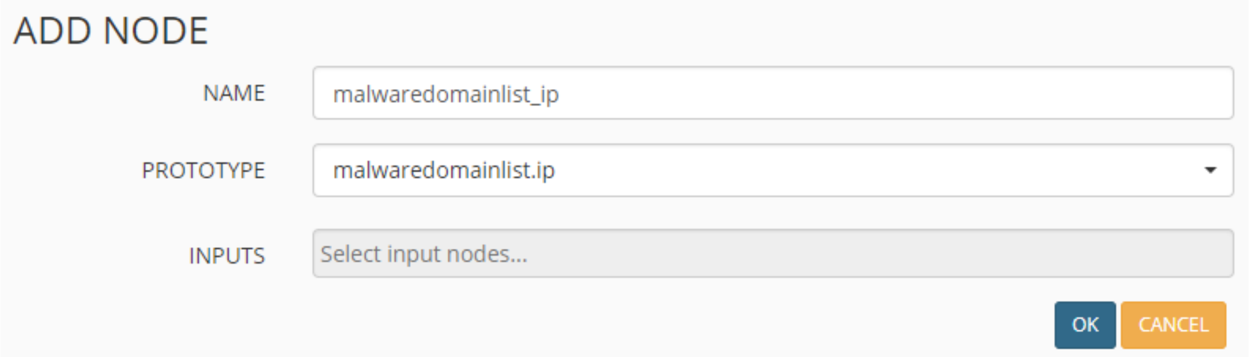
ADD NODE

NAME: zeustracker_badips

PROTOTYPE: zeustracker.badips

INPUTS: Select input nodes...

4. Add 'malwaredomainlist.ip' it has a confidence level 50 so will be aggregated into the MC EDL
   - Name: malwaredomainlist_ip
   - Prototype: malwaredomainlist.ip
   - Inputs: inboundaggregator



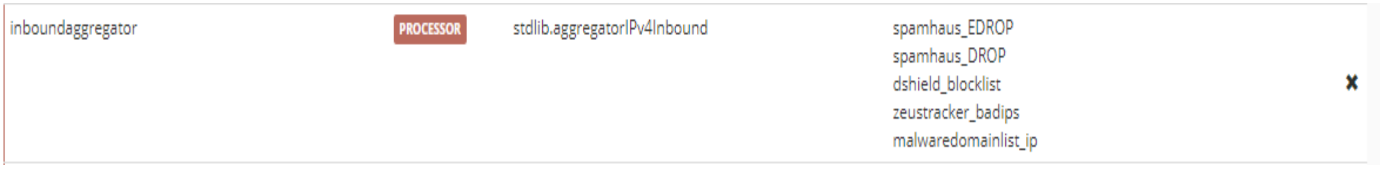
ADD NODE

NAME: malwaredomainlist_ip

PROTOTYPE: malwaredomainlist.ip

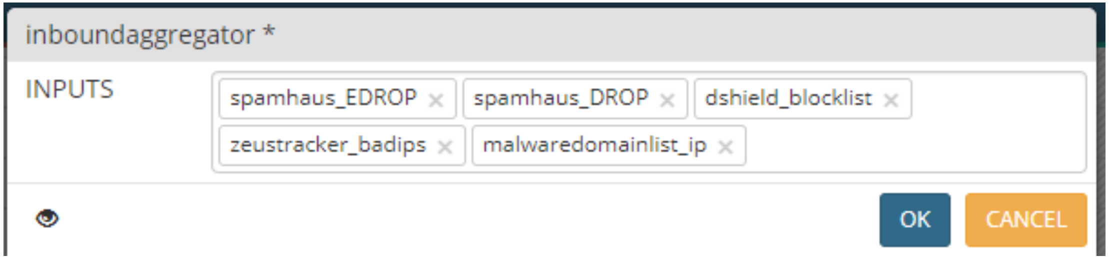
INPUTS: Select input nodes...

5. Verify that both 'malwaredomainlist_ip' and 'zeustracker_badips' are in the inboundaggregator node.
   a. Config>locate inboundaggregator processor and you'll see the additional miners you created



inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	spamhaus_EDROP spamhaus_DROP dshield_blocklist zeustracker_badips malwaredomainlist_ip	✘

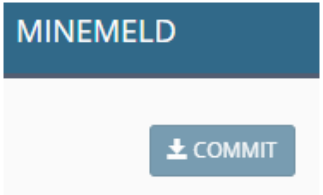
b. Clicking on 'inboundaggregator' allows you to associate additional miners if you wish with the aggregator.



inboundaggregator *

INPUTS: spamhaus_EDROP ×, spamhaus_DROP ×, dshield_blocklist ×, zeustracker_badips ×, malwaredomainlist_ip ×

6. Click 'Commit' in the upper right

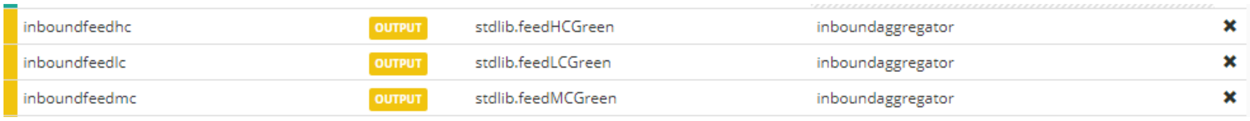


7. The inboundaggregator will now populate the output node which will filter the IoC based on confidence.

Add the needed EDLs to the firewall

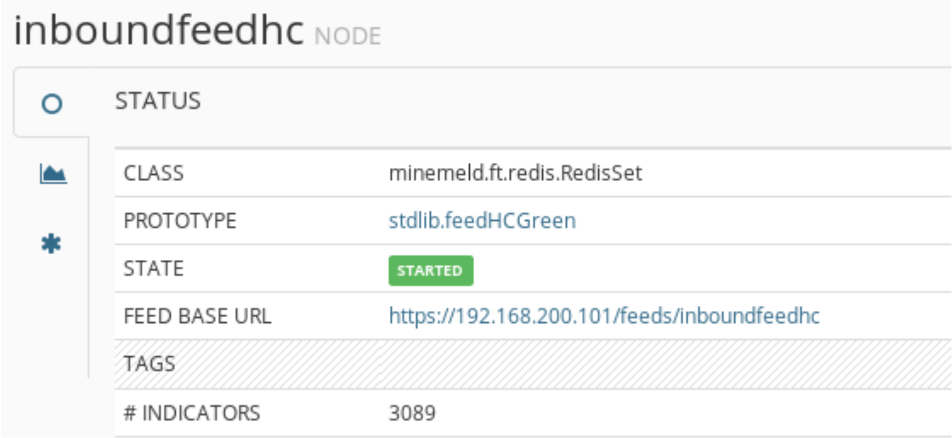
In order to use the IoC data on the firewall we need to add EDLs objects to the firewall. In MineMeld:

1. Click Config
2. Browse to inboundfeedhc and inboundfeedmc



inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundaggregator	✖
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	✖
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	✖

3. Click on each and take note of the 'FEED BASE URL' as we will use this on the firewall to retrieve the IoC list.

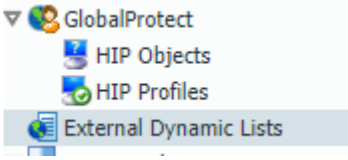


inboundfeedhc NODE

STATUS

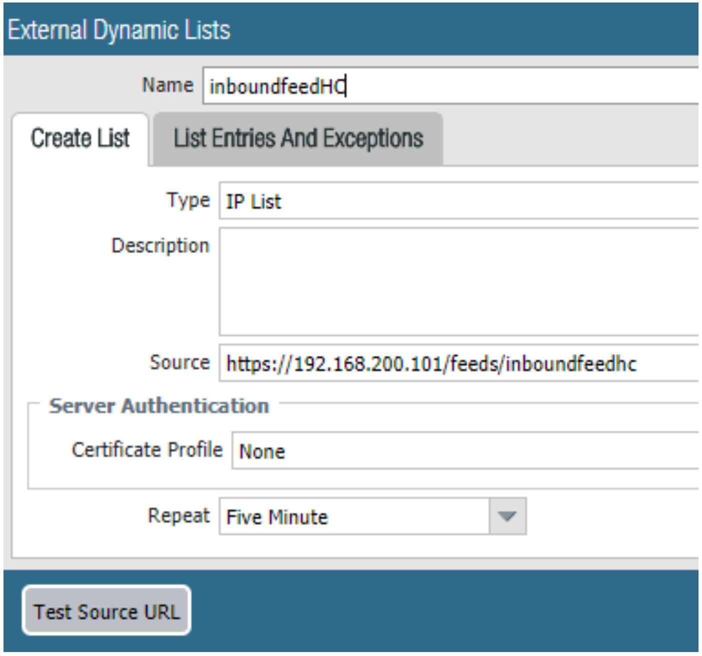
CLASS	minemeld.ft.redis.RedisSet
PROTOTYPE	stdlib.feedHCGreen
STATE	STARTED
FEED BASE URL	https://192.168.200.101/feeds/inboundfeedhc
TAGS	
# INDICATORS	3089

4. Login into your Firewall
5. Browse to Objects>External Dynamic List



6. Click 'Add'
7. Create an EDL for both inboundfeedhc and inboundfeedmc
   - Name: inboundfeedhc
   - Type: IP List
   - Source: <paste the FEED BASE URL from MineMeld>
   - Repeat: Five Minute
8. Test Source URL
9. Repeat for inboundfeedmc

Example of EDL for inboundfeedhc



Name: inboundfeedHC

Type: IP List

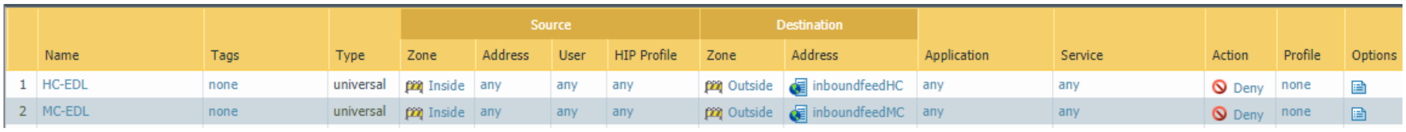
Description:

Source: https://192.168.200.101/feeds/inboundfeedhc

Certificate Profile: None

Repeat: Five Minute

After creating both EDLs we can use them in firewall policy. Since both of these EDLs are of IoCs configure policy to deny traffic. The example below we are denying Inside to Outside to these EDL IPs.



				Source				Destination						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
1	HC-EDL	none	universal	Inside	any	any	any	Outside	inboundfeedHC	any	any	Deny	none	
2	MC-EDL	none	universal	Inside	any	any	any	Outside	inboundfeedMC	any	any	Deny	none	

Tips for using EDLs

If you'd like to View the List of Entries in an External Dynamic List

1. Log in to the CLI on the firewall.
2. Enter the following command to view the list of entries that the firewall has retrieved from the web server:
    a. request system external-list show name <name>

example:

```
admin@PA-VM> request system external-list show type ip name inboundfeedHC
vsys1/inboundfeedHC:
    Next update at      : Fri May  4 11:00:26 2018
    Source              : https://192.168.200.101/feeds/inboundfeedhc
    Referenced          : Yes
    Valid               : Yes
    Auth-Valid          : Yes
    Total valid entries   : 4504
    Total invalid entries : 0
    Valid ips:
        113.201.51.0-113.201.51.255
        118.26.116.0-118.26.119.255
…
```

In the event you'd like to force a refresh of the List of Entries in an External Dynamic List

1. Log in to the CLI on the firewall.
2. Enter the following command to view the list of entries that the firewall has retrieved from the web server:
    a. request system external-list show name <name>

example:

```
admin@PA-VM> request system external-list refresh type ip name
 inboundfeedHC    inboundfeedHC
 inboundfeedMC    inboundfeedMC
 <name>           <name>
admin@PA-VM> request system external-list refresh type ip name   inboundfeedHC
```

Hardware limitations

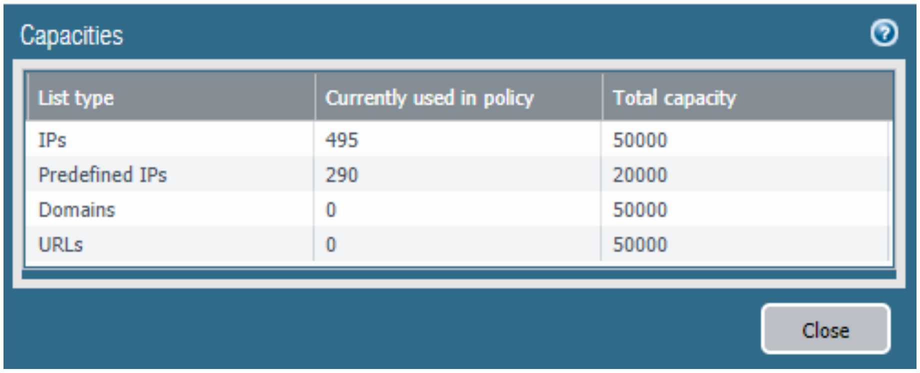
Check the number of external dynamic list entries used in policy to make sure you don't go over the firewall limit.

In PAN-OS 8.0, you can reference a total of 30 external dynamic lists with unique sources across all security policy rules. In addition, external dynamic list entries (IP addresses, domain, and

URLs) now only count toward the maximum number supported by the firewall if they belong to lists referenced in Security policy rules you enforce on the firewall.

1. Select ObjectsExternal Dynamic List.
2. Click List Capacities in the bottom bar

Compare how many IP addresses, domains, and URLs are currently used in policy against the total number of entries that the firewall supports for each list type. Since these values vary from firewall to firewall, the List Capacities window is not available on Panorama. Predefined IPs displays the number of IP addresses in the most recent Palo Alto Networks Malicious IP Address Feeds saved to your firewall, even if they are not used in policy.



List type	Currently used in policy	Total capacity
IPs	495	50000
Predefined IPs	290	20000
Domains	0	50000
URLs	0	50000

Other Useful Feeds

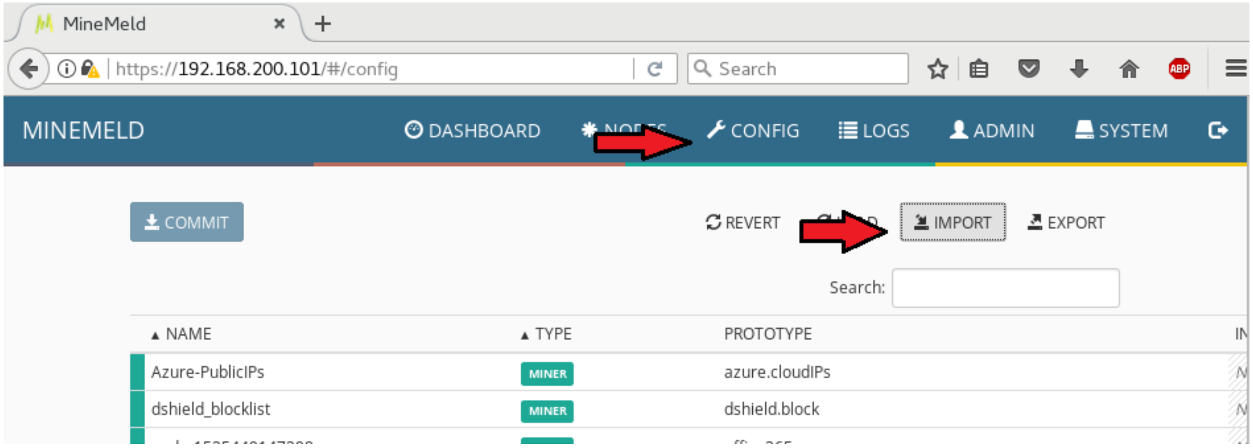
In addition to IoC you can use MineMeld for certain SaaS application. Due to the dynamic IP nature of cloud-based applications, keeping updated on IP/URL changes and incorporate them into firewall policy can be a daunting task. Fortunately, with MineMeld you can add feeds from SaaS vendors that provide the information. In this example we will be adding Office365 miners and feeds to our MineMeld instance.

Obtain & Import Configuration

MineMeld already come with Prototypes for each of the O365 services but you would normally need to create a miner for each of these from those Prototypes, along with 3 processors and 3 outputs (one each for IPv4 addresses, IPv6 addresses and URLs respectfully). To save you the hassle Palo Alto created a configuration you can import, simply download it from https://paloaltonetworks.app.box.com/s/4ubmkgrq72a8mdd24j733ddqdgbkyvv4

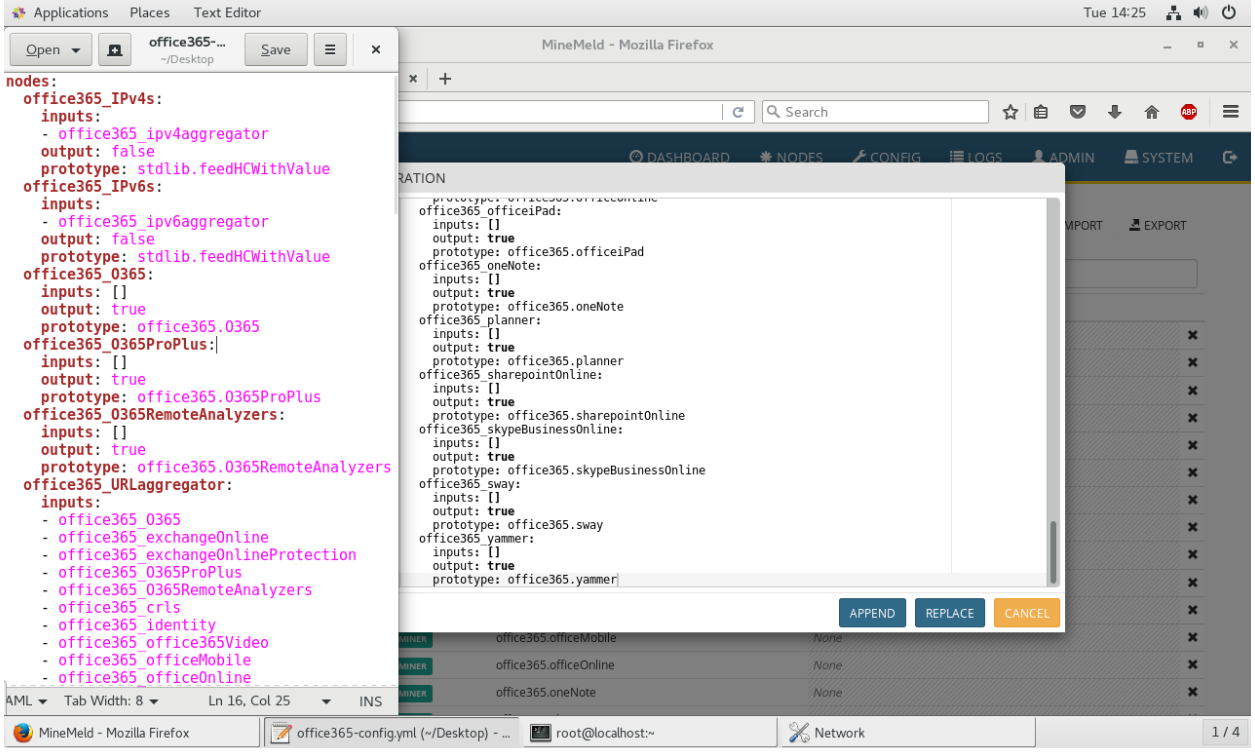
NOTE: for a minimal config collecting all the IPv4s, IPv6 and URLs of all the O365 products download this instead:
https://paloaltonetworks.box.com/s/gndwe5rzheg1ekwplxb4m3mrpcf5k41f

1. Log into MineMeld and Click configure
2. Export your current config as a backup
3. Then click Import



▲ NAME	▲ TYPE	PROTOTYPE
Azure-PublicIPs	MINER	azure.cloudIPs
dshield_blocklist	MINER	dshield.block

4. open the “office365-config.yml” file you download in a text editor
5. Paste the contents into the ‘import candidate configuration window
6. Assure you click ‘Append’ (Click replace will overwrite your whole node config)



```
nodes:
  office365_IPv4s:
    inputs:
    - office365_ipv4aggregator
    output: false
    prototype: stdlib.feedHCWithValue
  office365_IPv6s:
    inputs:
    - office365_ipv6aggregator
    output: false
    prototype: stdlib.feedHCWithValue
  office365_O365:
    inputs: []
    output: true
    prototype: office365.O365
  office365_O365ProPlus:
    inputs: []
    output: true
    prototype: office365.O365ProPlus
  office365_O365RemoteAnalyzers:
    inputs: []
    output: true
    prototype: office365.O365RemoteAnalyzers
  office365_URLaggregator:
    inputs:
    - office365_O365
    - office365_exchangeOnline
    - office365_exchangeOnlineProtection
    - office365_O365ProPlus
    - office365_O365RemoteAnalyzers
    - office365_crls
    - office365_identity
    - office365_office365Video
    - office365_officeMobile
    - office365_officeOnline
```

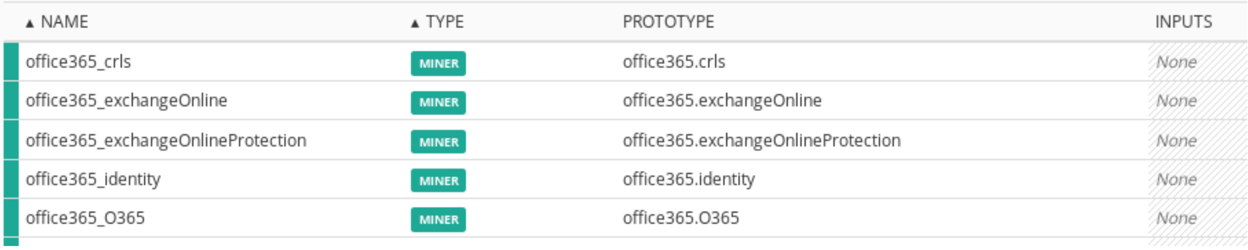
```
office365_officeiPad:
  inputs: []
  output: true
  prototype: office365.officeiPad
office365_oneNote:
  inputs: []
  output: true
  prototype: office365.oneNote
office365_planner:
  inputs: []
  output: true
  prototype: office365.planner
office365_sharepointOnline:
  inputs: []
  output: true
  prototype: office365.sharepointOnline
office365_skypeBusinessOnline:
  inputs: []
  output: true
  prototype: office365.skypeBusinessOnline
office365_sway:
  inputs: []
  output: true
  prototype: office365.sway
office365_yammer:
  inputs: []
  output: true
  prototype: office365.yammer
```

MINER	office365.officeMobile	None
MINER	office365.officeOnline	None
MINER	office365.oneNote	None

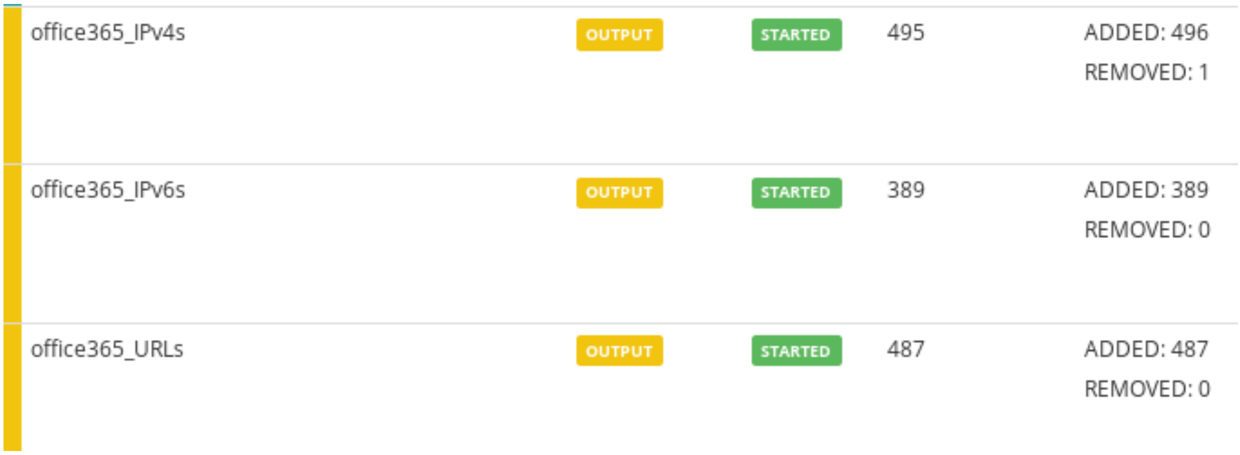
7. Click Commit

You should now have the miners, process, and output for office365 under Config section from the ribbon.

Figure shows examples of the newly imported miners and protocols.

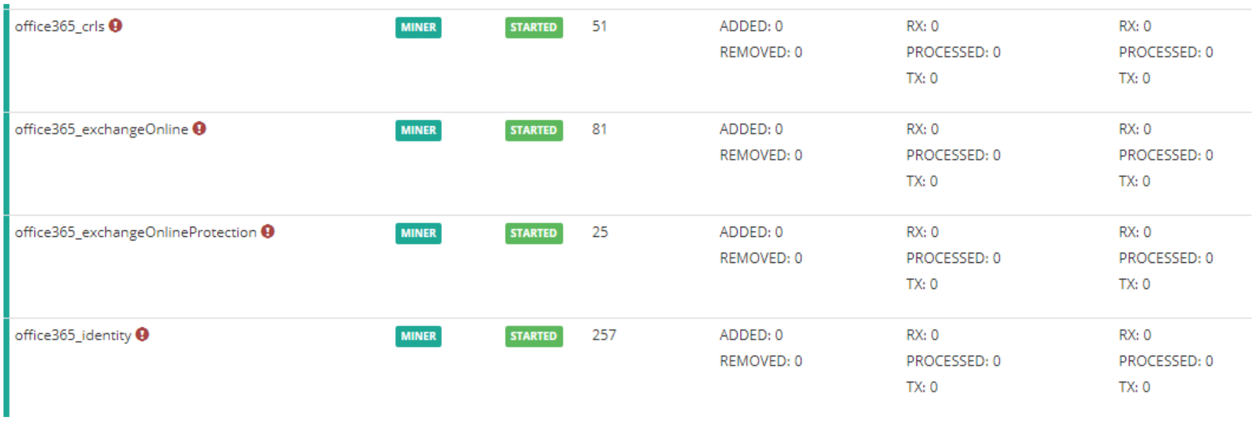


▲ NAME	▲ TYPE	PROTOTYPE	INPUTS
office365_crls	MINER	office365.crls	None
office365_exchangeOnline	MINER	office365.exchangeOnline	None
office365_exchangeOnlineProtection	MINER	office365.exchangeOnlineProtection	None
office365_identity	MINER	office365.identity	None
office365_O365	MINER	office365.O365	None



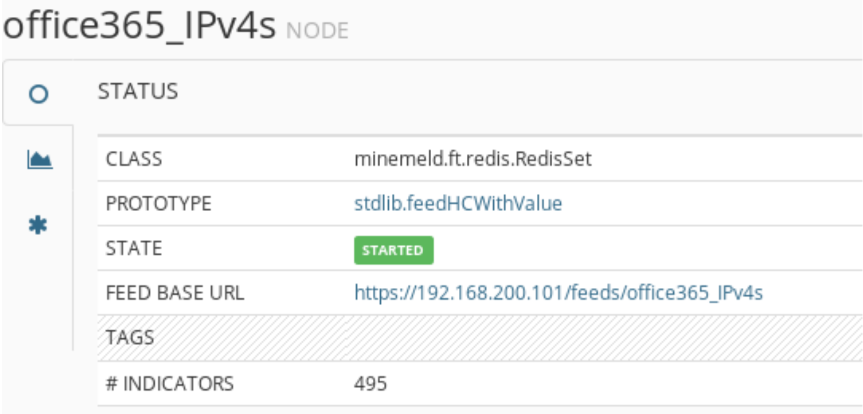
office365_IPv4s	OUTPUT	STARTED	495	ADDED: 496 REMOVED: 1
office365_IPv6s	OUTPUT	STARTED	389	ADDED: 389 REMOVED: 0
office365_URLs	OUTPUT	STARTED	487	ADDED: 487 REMOVED: 0

After giving the MineMeld engine a few minutes to restart, click “Config” in the banner at the top of the interface and then, click any of the nodes in the list.



office365_crls ❗	MINER	STARTED	51	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
office365_exchangeOnline ❗	MINER	STARTED	81	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
office365_exchangeOnlineProtection ❗	MINER	STARTED	25	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
office365_identity ❗	MINER	STARTED	257	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0

Similar to before, take note of the FEED BASE URL from the output mine (In this case ‘office365_IPv4s) so we can add the EDL to the firewall.

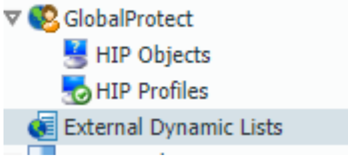


office365_IPv4s NODE

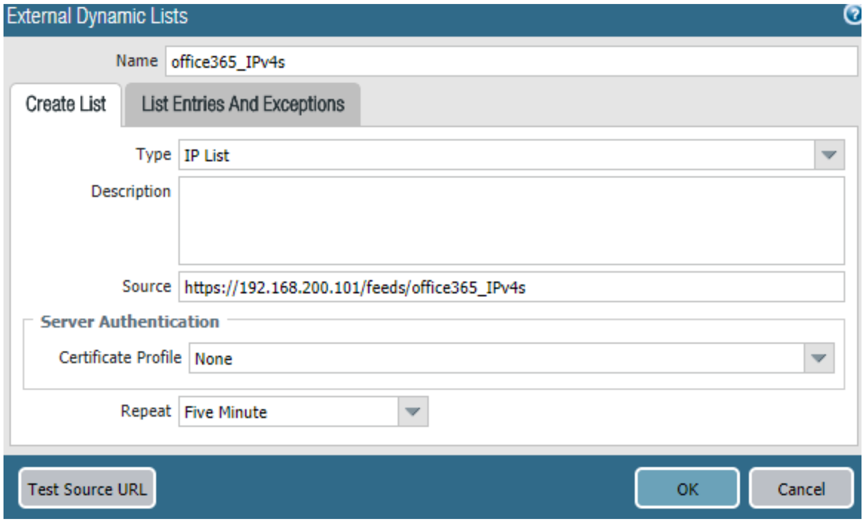
STATUS

CLASS	minemeld.ft.redis.RedisSet
PROTOTYPE	stdlib.feedHCWithValue
STATE	STARTED
FEED BASE URL	https://192.168.200.101/feeds/office365_IPv4s
TAGS	
# INDICATORS	495

1. Login into your Firewall
2. Browse to Objects>External Dynamic List



3. Click ‘Add’
4. Create an EDL for office365_IPv4s
    - Name: office365_IPv4s
    - Type: IP List
    - Source: <paste the FEED BASE URL from MineMeld>
    - Repeat: Five Minute
5. Test Source URL



External Dynamic Lists

Name: office365_IPv4s

Type: IP List

Description:

Source: https://192.168.200.101/feeds/office365_IPv4s

Server Authentication

Certificate Profile: None

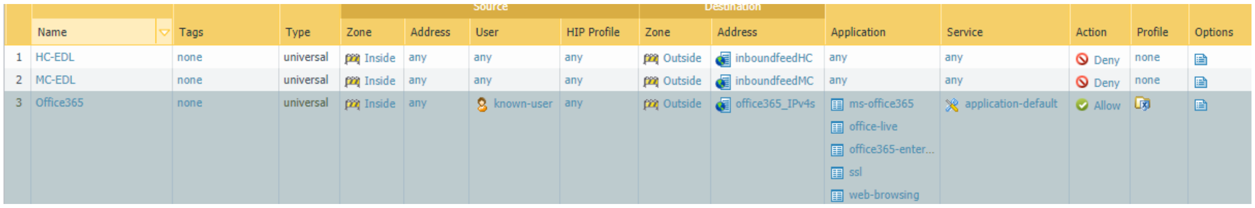
Repeat: Five Minute

3. Log in to the CLI on the firewall.
4. Enter the following command to view the list of entries that the firewall has retrieved from the web server:
    a. request system external-list show name <name>

```
admin@PA-VM> request system external-list show type ip name office365_IPv4s
vsys1/office365_IPv4s:
        Next update at        : Fri May  4 19:00:04 2018
        Source              : https://192.168.200.101/feeds/office365_IPv4s
        Referenced          : Yes
        Valid               : Yes
        Auth-Valid          : Yes
        Total valid entries   : 495
        Total invalid entries : 0
        Valid ips:
                111.221.112.0-111.221.119.255
                13.107.128.0-13.107.131.255
. . .
```

Create Security Policies

Now that we have EDLs we will modify/create our security policies. In the example below, we are allowing our Office 365 apps for all known users in the Inside zone. The destination zone has been set to Outside zone but with the IPv4 lists as destination addresses.



				Source				Destination					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
1	HC-EDL	none	universal	Inside	any	any	any	Outside	inboundfeedHC	any	any	Deny	none	
2	MC-EDL	none	universal	Inside	any	any	any	Outside	inboundfeedMC	any	any	Deny	none	
3	Office365	none	universal	Inside	any	known-user	any	Outside	office365_IPv4s	ms-office365 office-live office365-enter... ssl web-browsing	application-default	Allow		

App-IDs that you may find detected during use of Office 365 (depending on the clients and product sets being used)

activesync
mapi-over-http
ms-exchange
ms-office365
ms-onedrive
rpc-over-http
soap
ssl
stun

web-browsing
webdav
ms-office365
office-live
office-on-demand
outlook-web-online
ms-lync-online
ms-lync-online-apps-sharing
sharepoint-online
ms-lync-online-file-transfer

The Next Steps

If you want to test this on your own and do not have access to a lab environment to do so, you have a couple options:

a. Contact your Sun Management Account Rep to get pricing on a lab bundle. The PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

If you are unsure who your Account Rep is or do not have one yet, you can reach out to **sales@sunmanagement.net** for assistance.

b. Reach out through the free Fuel Users Group (www.fuelusersgroup.org) which at the time this lab is being written is offering limited free access to a virtual lab environment, which they refer to as their "Virtual Test Lab," in which you can practice the steps outlined above. (Note: The Fuel Users Group may alter or discontinue offering their "Virtual Test Lab" at any time)

c. For access to live Palo Alto Networks boxes for lab practice purposes please go to: **https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab**. This is a no charge service provided by Palo Alto Networks.

If you feel Sun Management brings value to you and your organization with these labs, please keep us in mind for other network and network security related requirements. We are here to help you. Thank you for your business.

Please direct any questions/comments/feedback on this lab exercise to: ***education@sunmanagement.net***

Lab Author: *Mike Connors CISSP, PCNSE, PCNSC, PSE-P*

Sr. Network Security Engineer

Last Modified: May 4, 2018

Resource Links

https://live.paloaltonetworks.com/t5/MineMeld-Articles/What-is-in-a-MineMeld-node/ta-p/72046

https://live.paloaltonetworks.com/t5/MineMeld-Articles/How-to-Safely-Enable-access-to-Office-365-using-MineMeld/ta-p/120280

https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/external-dynamic-list-enhancements

https://live.paloaltonetworks.com/t5/MineMeld-Articles/Connecting-PAN-OS-to-MineMeld-using-External-Dynamic-Lists/ta-p/190414

https://live.paloaltonetworks.com/t5/MineMeld-Articles/How-to-Safely-Enable-access-to-Office-365-using-MineMeld/ta-p/120280