

Expedition

Hands-on Workshop

Expedition: Migration and Security Assessment

<http://www.paloaltonetworks.com>

Table of Contents

Introduction	4
Activity 0 – Initial Setup.....	5
Task 1 – Configure Machine Learning Module (HTTPS)	5
Task 2 – Review and fix Internal Checks (SSH).....	6
Dashboard.....	8
Activity 1 – PanOS Traffic Logs (where the Magic begins)	9
Task 1 – VM-Series. Configure Scheduled Log Export.....	9
Task 2 – Import a Device into Expedition	11
Task 3 – Process Log Files	12
Task 4 – Creating a Project.....	14
Activity 2 – Rule Enrichment	16
Task 1 – The Log Connector	16
Task 2 – Set Rules for Enrichment.....	18
Task 3 – Enrich the missing Zones.....	21
Task 4 – Enrich Source IP Address.....	22
Task 5 – Enrich App-ID	23
Task 6 – Export the Discovery to Excel	26
Activity 3 – Rule Suggestions by M. Learning.....	27
Task 1 – Set Rules for M. Learning	27
Task 2 – Review the learned Servers.....	30
Task 3 – Import Suggested Rules.....	31
Activity 4 – Best Practices Adoption	35
Task 1 – Run the Best Practices Assessment Tool (BPA)	35
Task 2 – Export Report to Excel.....	37
Task 3 – Apply remediation to the failed Checks.....	39
Task 4 – Reviewing the Security Policies Best Practices.....	42
Activity 5 – Importing Iron-Skillet.....	44
Task 1 – Import a new Iron-Skillet configuration.....	44
Task 2 – Move Custom Reports and Security Profiles to your Configuration	45
Task 3 – Apply the iron-skillet profiles to your Rules.....	47

Activity 6 – Export changes via API.....48

Introduction

What is Expedition?

Expedition is the fourth evolution of the Palo Alto Networks Migration Tool. The main purpose of this tool is to help to reduce the time and effort to migrate a configuration from one of the supported vendors to Palo Alto Networks.

By using the Migration Tool, we were able to convert a configuration from Checkpoint, Cisco or any other vendor to PanOS and gave you more time to improve the results. Migration Tool 3 added some functionality to allow our customers to enforce security policies based on App-ID and User-ID.

With Expedition we have gone one step further. Not only because we want to continue helping to facilitate the transition of a security policy from other vendors to PanOS but we want to ensure the outcome is the best as possible. This is why we added a **Machine Learning module** who can help you to generate new security policies based on real traffic logs and the introduction of the **Best Practices Assessment Tool** to check that the configuration complies with the Best Practices recommended by our security experts.

In 2019 we introduced support for project Iron-Skillet too. Iron-Skillet provides a day1 configuration for a PanOS device with some of the configuration best practices already configured. With this you can create a base configuration to be used in your migrations with almost everything configured without any effort and allowing you to customize some of the parameters like hostname or Management IP address before generate it.

Expeditions is the glue between many initiatives born from different internal projects here at Palo Alto Networks to be easier to consume them.

Activity 0 – Initial Setup

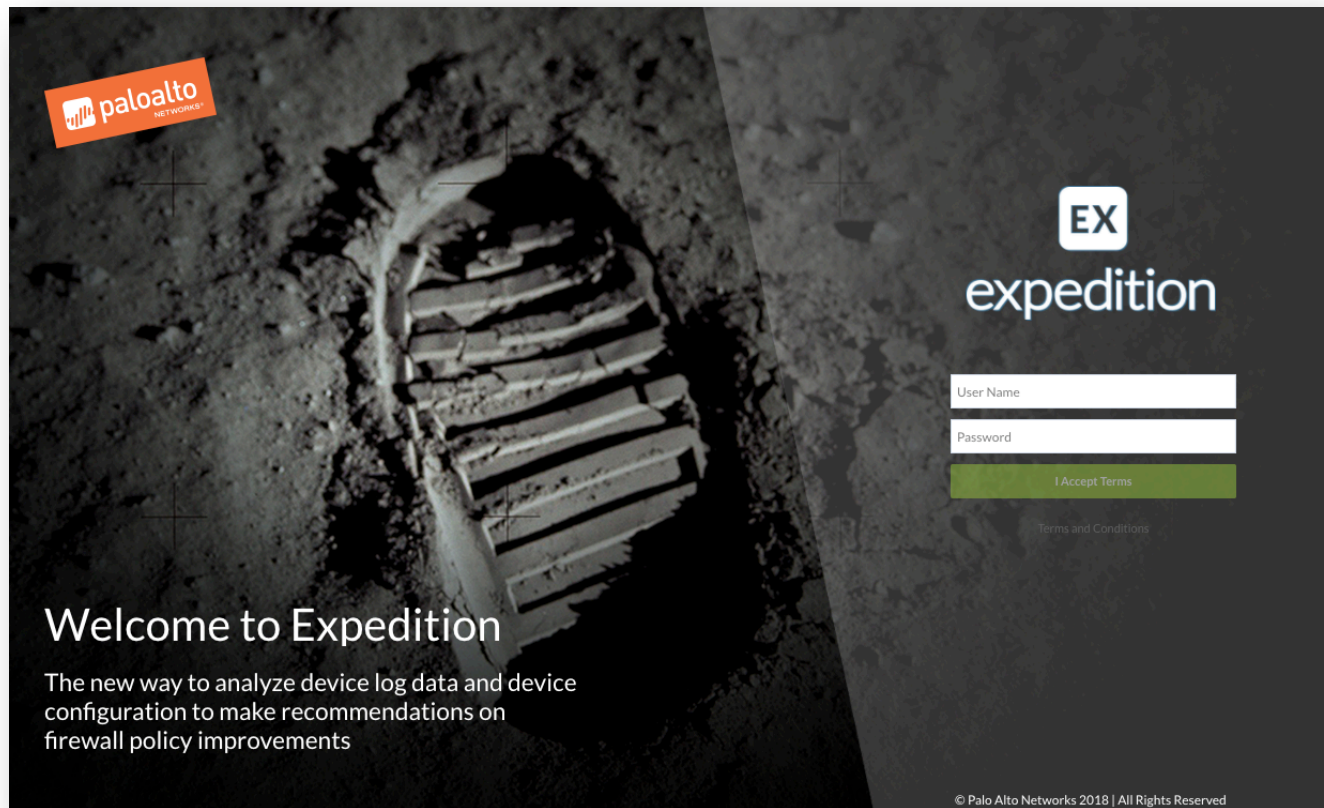
In this activity, you will:

- Configure and prepare Expedition to run for the first time and setup the Machine Learning module.
- Review and fix **any failed** health checks shown from the dashboard (Task 2).

Task 1 – Configure Machine Learning Module (HTTPS)

Step 1: First, make sure your laptop is installed with a modern browser that supports HTML 5.0. We recommend using the latest version of Chrome. **We recommend using the Private Browsing mode in your browser for this lab so any extensions do not interfere.**

Step 2: Log in to the Expedition GUI (*admin / paloalto*)

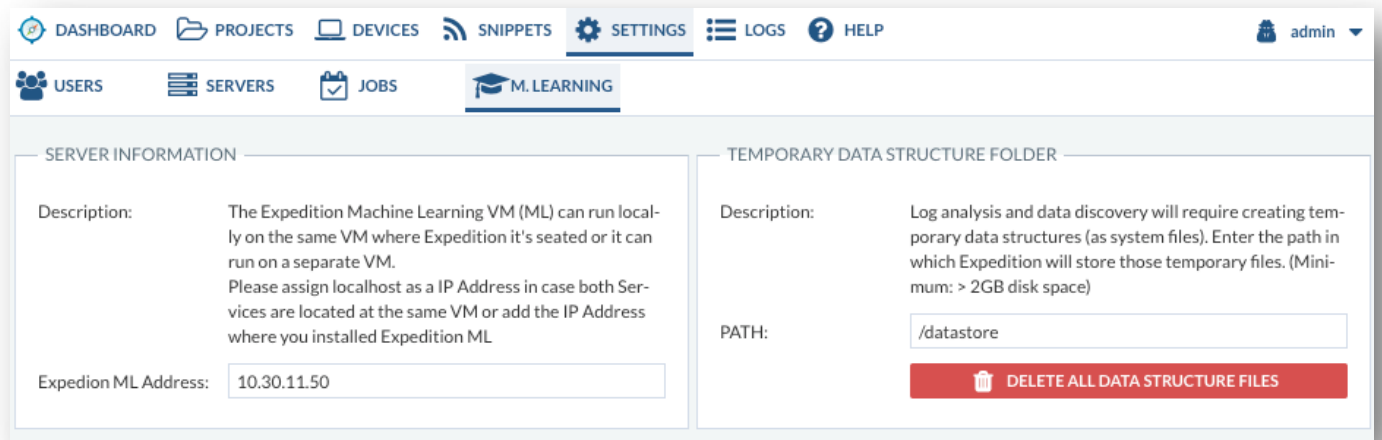


Step 3: Let's configure Expedition to be able to store and analyze logs.

- Select the tab called SETTINGS
- Select the sub-tab called M.LEARNING

Validate the Expedition ML Address IS NOT 127.0.0.1 and set the TEMPORARY DATA STRUCTURE FOLDER Path to:

/datastore



- Click SAVE from the bottom bar.

Note: Expedition can read CSV logs generated by PanOS devices but to analyze the data requires those files been stored on a format called PARQUET. PARQUET is a format utilized when a big amount of data needs to be processed and accessed in parallel to speed up the process.

[Task 2 – Review and any fix Internal Checks \(via SSH\) listed](#)

First thing we have to do is create the “datastore” folder in our Expedition instance:

Step 1: Using a SSH Client connect to your Expedition instance or use the Console link from the lab portal. Log in with these credentials **expedition / paloalto**

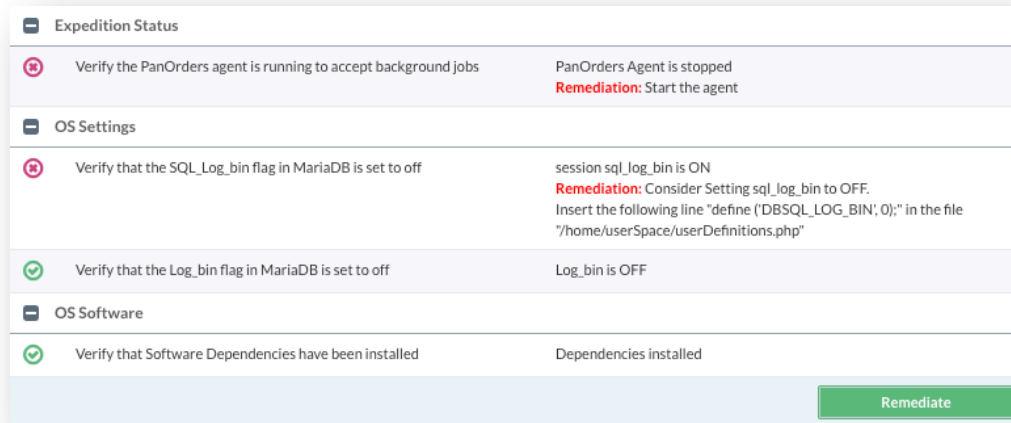
- Create the folder /datastore and allow the web server user write on that folder (Default Expedition web server user is www-data)

```
sudo mkdir /datastore
```

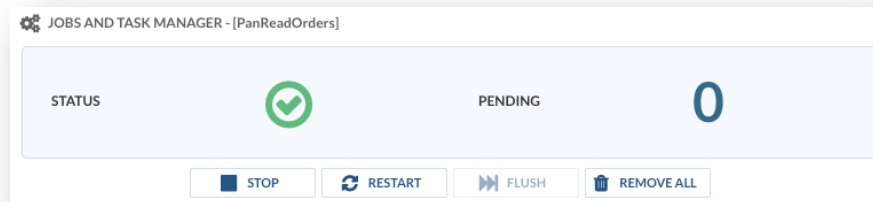
```
sudo chown -R www-data /datastore
```

Step 2: Going back to your browser select from your Expedition instance the DASHBOARD.

- Take a look to Expedition Internal Checks grid.



- Click on Remediate to allow Expedition try to fix some of them automatically
- Review the Task Manager now has been started and looks green.



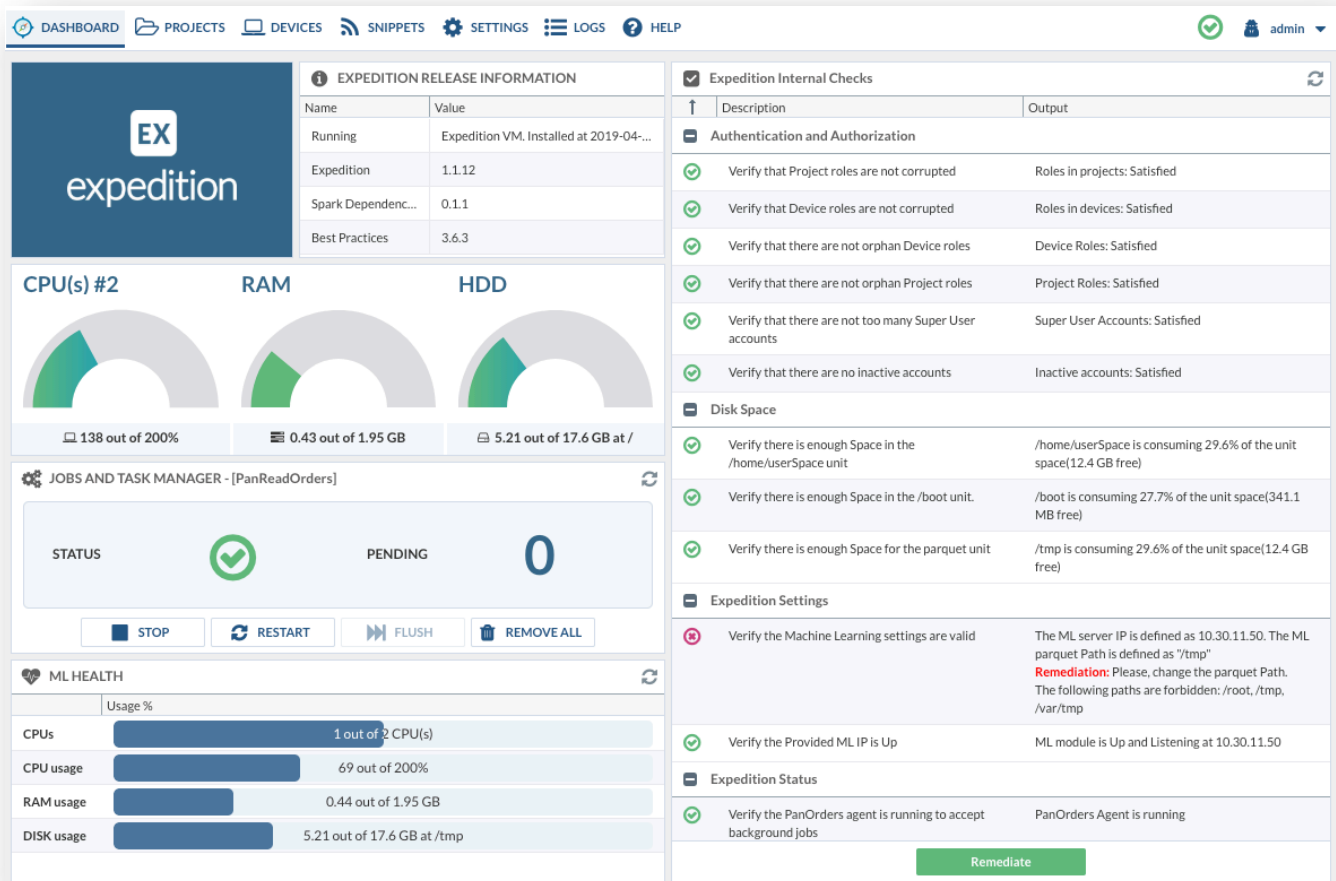
Step 3: Go back to your SSH/Console connection

- Following the recommendation from the Internal Checks for “OS settings” related to the SQL_Log_bin flag we have to modify one configuration file:
 - i) `sudo vi /home/userSpace/userDefinitions.php`
 - ii) Add this line at the bottom by moving the cursor to the end of the file and pressing “o”
`define ('DBSQL_LOG_BIN',0);`
 - iii) To save the changes and exit the editor press ESC and type “:wq”, press enter.
 - iv) Click on the Remediate button again.

End of Activity 1

Dashboard

Let's take a closer look to the DASHBOARD to understand all the important parts.



The Jobs and Task Manager: This process is in charge to start any task we want to run and check if the job is still alive from the backend, if we want to retrieve the running configuration from a device or we want to push the API calls generated after a transformation to one or more devices the Task manager will be responsible of that, so keep it UP and Running otherwise the task will be queued until you start it.

Expedition was conceived to run everything in a single VM or split in two. One piece will run the GUI and basic database and another piece with more resources (CPU and RAM) will run the Data analytics and Machine Learning. For this reason, in the case we were using two different VMs we can monitor the CPU, RAM and DISK of each instance, ML HEALTH will show the status of the Analytics and the gauge charts shows the status of the VM who is running the GUI and the database. In this exercise, all the charts will show the same information because we are using a single instance to run both tasks.

Activity 1 – PanOS Traffic Logs (where the Magic begins)

The Palo Alto Networks traffic logs are the most powerful data records generated by a network security device, they come with such level of details about who was the user, what was the application used, when it happened. That makes our logs key to evaluate risks and propose new rules based on a multitude of indicators. This is why Expedition needs the logs generated by our Technology to provide better security suggestions.

Expedition is capable of ingesting CSV files generated directly from our firewalls but on environments with a huge number of logs is preferred to use a syslog server and then, every day, rotate the log and import into Expedition. Expedition comes with a syslog-NG to run that task as well, but is preferred to run on a separate VM because the syslog has to write a lot to the disk and that can cause Expedition to run slowly.

In this activity you will:

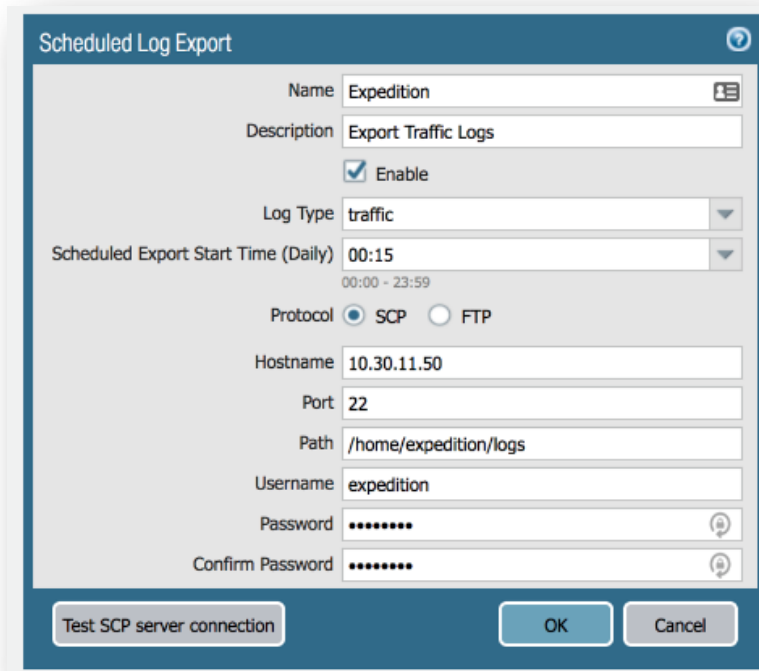
- Configure your VM-Series Firewall to export traffic logs every day to your Expedition VM
- Configure Expedition to import the VM-Series Firewall config and bind with the exported logs
- Create your first Project, attach the VM-Series Firewall to it and import the configuration

Task 1 – VM-Series. Configure Scheduled Log Export

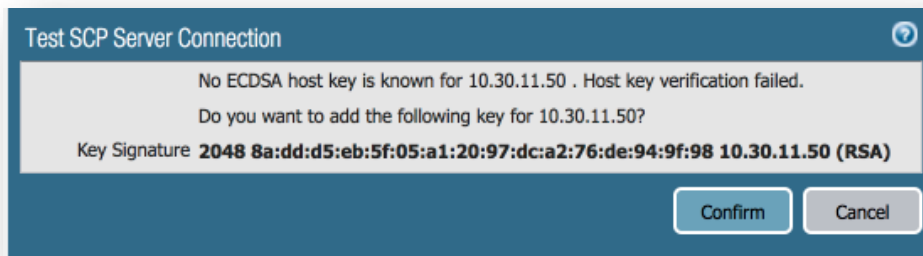
This task will show you how to configure your Next-Generation Firewall to export daily the logs to Expedition by using SCP (using a secure channel). With this process you don't need to worry about doing any addition task to get the logs out from your PanOS device.

Step 1: Log in to your NGFW GUI (*admin / admin*)

Step 2: Go to Device, and select from the left panel “Scheduled Log Export”, click on Add button and fill the fields with the information in the screenshot:



Step 3: Click on Test SCP Server connection to retrieve the SSH keys, click on Confirm



This step has already been done but would be needed for a new Expedition setup.

Step 4: Click again on Test SCP Server connection to validate we can write on that folder

- /home/expedition/logs

Note: With this our VM-Series Firewall will start sending logs every day at midnight to Expedition, for this Lab we have already uploaded some log files to that folder and we don't need to wait to start working on this laboratory.

Click OK.

Step 5: Go to Dashboard of your NGFW and take note from the Serial number located under General Information

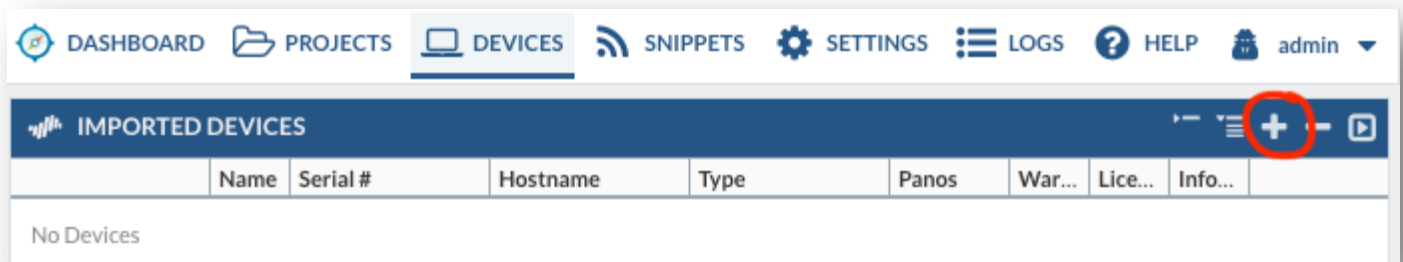
- Serial Number _____

Task 2 – Import a Device into Expedition

Expedition allow us to connect to a PanOS device using API keys. When it connects to the device and retrieve the configuration it keeps that configuration encrypted on the hard drive. That said if you make changes in the PanOS device and you want to update the configuration we had stored in Expedition you have to repeat the process to retrieve the running or candidate config again.

Step 1: Connect to your Expedition instance via HTTPS. Navigate to the DEVICES option. This view shows all defined Palo Alto Networks devices.

Step 2: Click on the plus button to add a new Device



Step 3: Fill the fields with the following information and click on Save

Field	Value
Device Name	VMSeriesFW
Hostname/IP	10.30.11.1
Serial	The serial captured on Task 1 – Step 5
Model	vm-series

Step 4: Edit the Device by double-click on it or clicking on the Edit icon located near the row's end.

Let's add the credentials in order to generate the API calls to interact with our firewall.

- On Authentication API Keys, click on the "+" to fill the Username and Password. Use the credentials **admin / Ignite19**. Click Add.

Add a new Key and assign a Role

Auth. type: Username and Password

Role: admin Apply all Roles

Username: admin Password:

Step 5: Go to the CONTENTS TAB to download the configuration of the firewall

- Click on Retrieve Contents and select Running Configuration
- Click on Save after the process ends.

Name	Serial #	Hostname	Type	Panos	Warnings	Licenses	Information
VMSeriesFW	xxxxxxxxxxxxx...	10.30.11.1	vm-series	9.0.1	No Warnings	<ul style="list-style-type: none"> WildFire License 2020-04-12 00:00:00 PA-VM 1969-12-31 00:00:00 PAN-DB URL Filtering 2020-04-12 00:00:00 AutoFocus Device License 2018-04-05 00:00:00 Threat Prevention 2020-04-12 00:00:00 GlobalProtect Gateway 2020-04-12 00:00:00 GlobalProtect Portal 1969-12-31 00:00:00 	<ul style="list-style-type: none"> Updated At: 2019-04-23 04:38:53 App Version: 8138-5378 (2019-03-28 21:49:54) Threat Version: 8138-5378 (2019-03-28 21:49:54)


Step 6: Edit the VMSeriesFW again. Go to M.LEARNING TAB located at the end of the Device Edit Window.

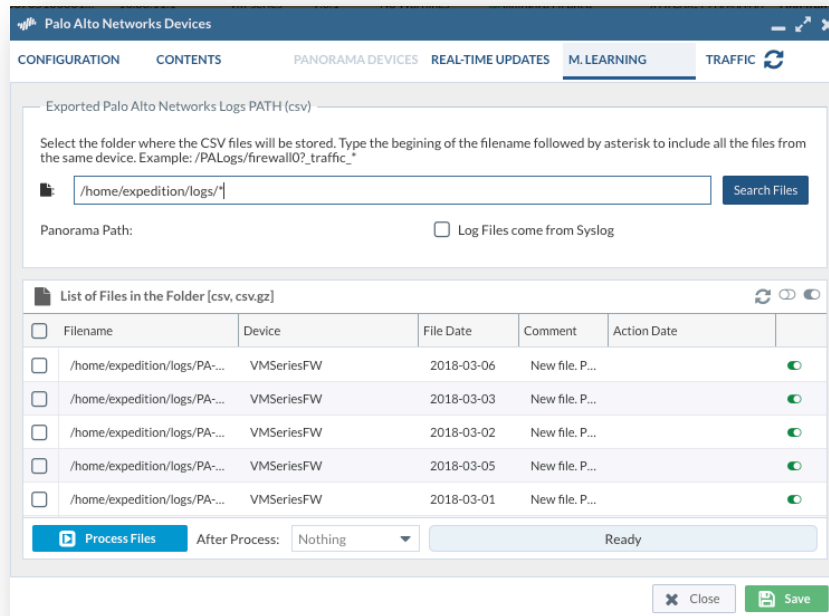
- Configure the PATH where the logs will be stored: /home/expedition/logs/*
- Click On SAVE.

Task 3 – Process Log Files

Step 1: Reopen the Device and come back to the M.LEARNING TAB

- (1) 6 Files will be shown.
- (2) The green switch indicates the file can be processed.

- (3) Files can be excluded from the process by selecting them and clicking on  the Ignore button.

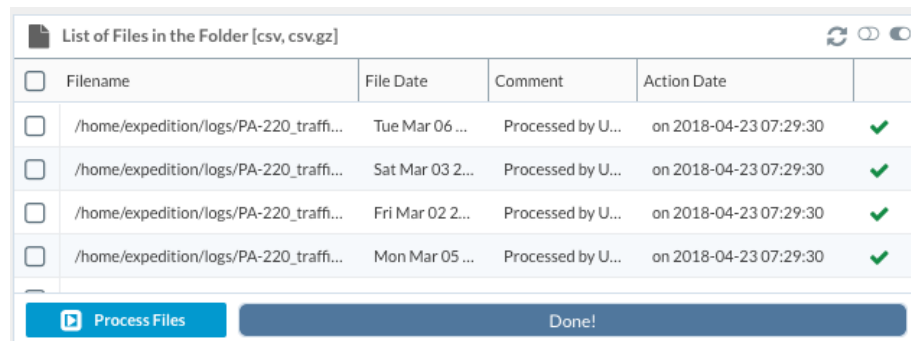


Step 2: Click on Process Files.

Note: This process can take up to 5 minutes. Notice the green check at the end when the file has been processed correctly.

This process can be tracked from the cli as well, just enter via cli to Expedition and run as root.

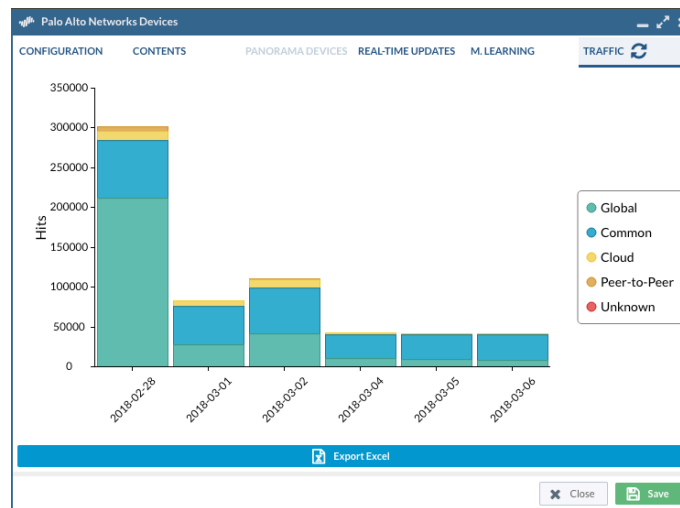
```
# tail -f /tmp/error_logCoCo
```



This process will convert the CSV logs into a new file called PARQUET and will be stored in the folder we created at the beginning of the lab “/datastore”. This process will reduce the amount of disk we need for the data analysis. Example: A log file with 100MB, if we compress to zip it will be reduced to

10MB, after ingesting the data and store as PARQUET format the same data will only occupy 1MB approx.

If you click on the tab called “TRAFFIC” **two times** it will show the number of hits by application type seen by day. This information can be exported as Excel file for further analysis since it will include all the apps seen by Rule. This is useful to understand if the log files imported has logs generated for a specific rule name.



Click Save when the process is completed.

Task 4 – Creating a Project

Step 1: Navigate from the Expedition GUI to the tab called PROJECTS and click on the plus icon located at the end of the header called LIBRARY to create a new one.

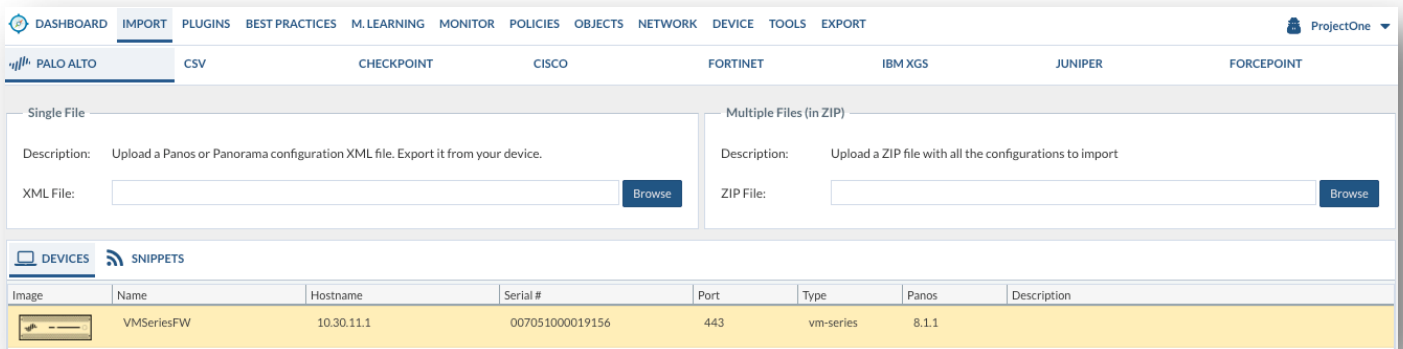
Step 2: Fill the fields with the following information

Field	Value
Name	ProjectOne
Source	Select the firewall VMSeriesVM

Note: With these steps we have created the project and attached the Firewall to it. We can modify these settings by clicking on “settings” on the selected Project.

Step 3: Double click on the Project called *ProjectOne* to get access on it.

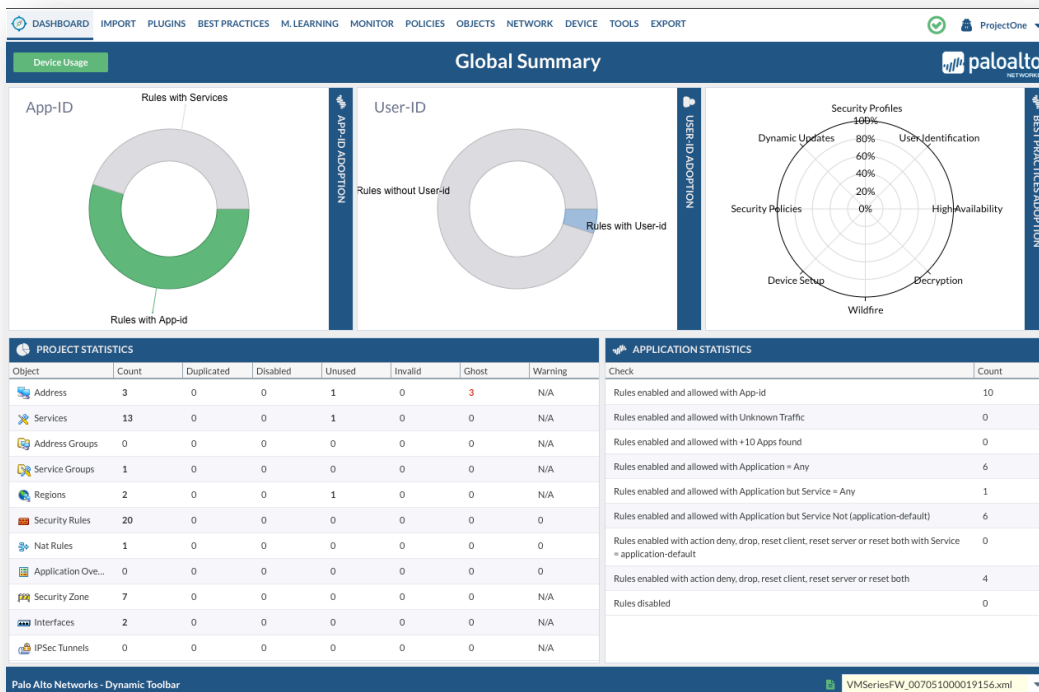
Step 4: From the new View select the option IMPORT and do a double click on the Device called VMSeriesFW in order to import the configuration



Step 5: Expedition will show you a Summary about the objects and rules imported.

App-ID and User-ID charts show the percentage of rules found using them and the third chart is related to the Best Practices Assessment Tool, this chart will not have any data until we run the analysis.

On the bottom bar there are one or two combo boxes, one is related to the configuration we are working on and the other in case of any will show the vsys/DG where we are focusing at the moment.



End of Activity 1

Activity 2 – Rule Enrichment

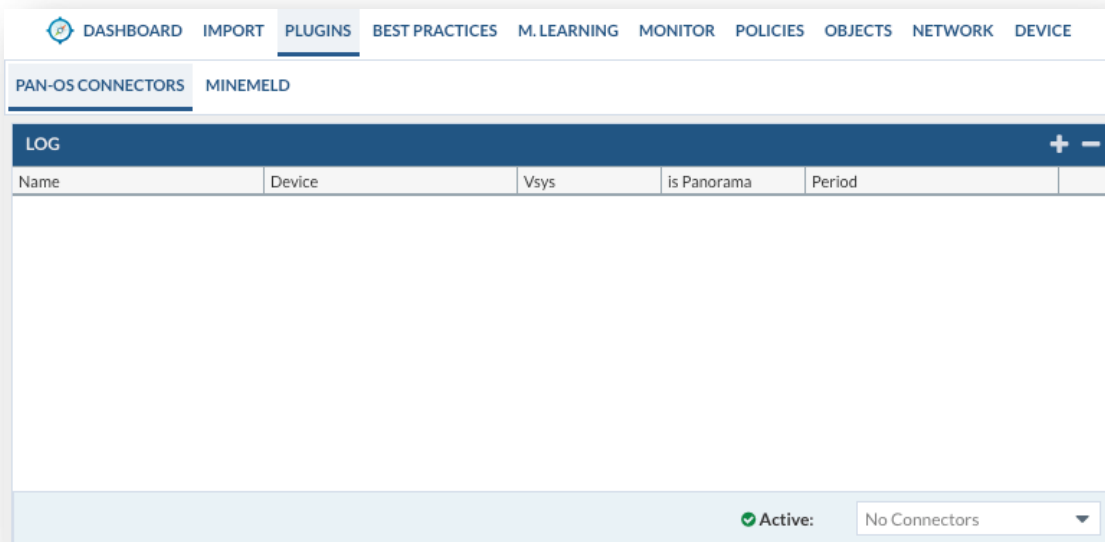
One of our missions here is guide you to improve your security posture and reduce the surface of attack. How can we help there? By providing you with the information you need to enrich your security policies in a way that can be easily consumed.

In this activity you will:

- Create a Log Connector. This is used to tell Expedition which Firewall we want to read the logs imported from.
- Run the Rule Enrichment functionality to learn all the missing parameters from our security policies and update them to reduce the Attack Surface starting with the security Zones.

Task 1 – The Log Connector

A Log Connector is a way to filter the information from all the logs we have stored in the PARQUET format to focus only in the data produced by a specific vsys from a firewall or from a group of firewalls included in a Panorama Device Group. When we create a Log Connector we are focusing only in some data and focusing on a period of time.



Step 1: From inside the Project navigate to PLUGINS tab

Step 2: Under PAN-OS CONNECTORS click on the plus button of the LOG grid.

Step 3: Fill the fields with this information

Field	Value
Connector Name	Provide a name – e.g. 'Last-30-Days'
Device	Select your firewall
Virtual System	vsys1
Period	Custom
Start Date	Add the start date
End Date	Add the end date
Note: The oldest log record is dependent on the logs available from the traffic logs uploaded to expedition.	

Step 4: Click on **Save**. This will automatically create the Log connector and make it active.

The screenshot shows a configuration window titled "LOG CONNECTOR (XML-API)". It contains the following fields and values:

- Connector Name: Vmfwlast3months
- Palo Alto Networks LOGS are stored in...
 - Select Device: VMSeriesFW
 - Virtual System: vsys1
- Period of TIME to Analyze
 - Period: custom
 - Start Date: 2018/01/01
 - Start Time: 00:00:00
 - End Date: 2018/04/30
 - End Time: 23:59:59

At the bottom, there are "Cancel" and "Save" buttons.

Note: You can see the active log Connector from the bar below the grid. It's mandatory to have one Active in order to use Rule Enrichment.

Name	Device	Vsys	Is Panorama	Period	
Vmfwlast3months	VMSeriesFW	vsys1	No	Start:2018-01-01 00:00:00 End:2018-04-30 23:59:59	

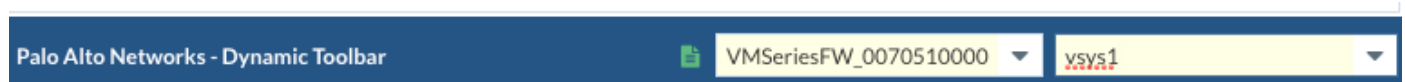
Active: Vmfwlast3months

Task 2 – Set Rules for Enrichment

We want to add Zones to some Rules. The goal of this task will be select the rules we want to enrich and let Expedition to tell us which Zones our firewall found for those rules and bring the **Zone From** and **Zone To** to our Security Policies.

Step 1: Navigate to the POLICIES tab

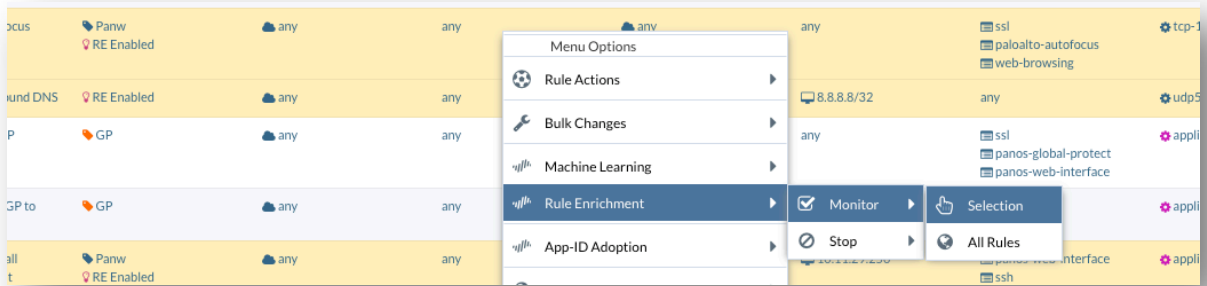
Step 2: Change from the Bottom bar the vsys to vsys1. This will enable the Security Policies view



Step 3: Select the following Rule Names, use the Ctrl + click to do it:

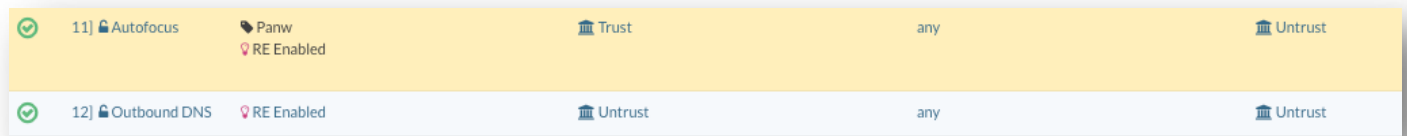
- Remote Access FW
- Autofocus
- Outbound Dns
- Firewall Management
- VPN Didac

Step 4: With the Rules selected right click over one and select Rule Enrichment -> Monitor (Selection)

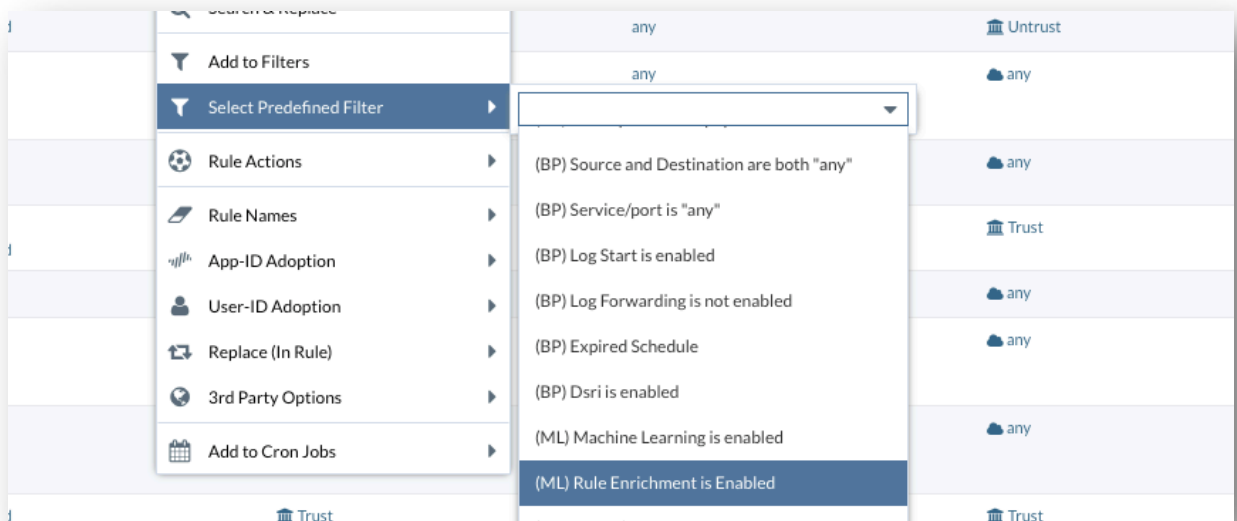


This will tag all the Selected Rules to be analyzed by the Rule Enrichment functionality

Note that a new TAG called RE Enabled has been added.



Step 5: Let's use the right-click from one of the rules to apply a predefined filter to show only the Rules with the Rule Enrichment Tag



Step 6: Located on the bottom bar, click on the green button called “Discovery” and select Rule Enrichment

Step 7: A new window will show up.

Step 8: Click on the Analyze Data blue button to start the analysis. (it can take up to 2 minutes).

This process will check for all the rules tagged with RE Enabled (Rule Enrichment) tag and start the analysis in the backend. Rule Enrichment will group all the data seen by rule and show it grouped.

Step 9: Advanced – You can follow the progress from the GUI or CLI

- For CLI: `tail -f /tmp/error_SecRulesEnrich`
- From GUI: After click on Analyze a URL will show up in the middle of the progress bar. If you click on that URL you will see the progress from another html page.

The screenshot displays the 'RULE ENRICHMENT' interface. It features a table titled 'Enrichment Data by Rule Name' with columns for Rule Name, Sources, Users, Destinations, Applications, and Services. The table lists several rules, including 'Autofo...', 'Outbo...', 'Firewa...', 'VPN D...', and 'Remot...'. The 'Remot...' rule shows a detailed list of source IP addresses and their corresponding countries. To the right of the table is an 'OPTIONS' panel with an 'ANALYZE' section containing instructions and a 'Time Frame Override' section with 'Start Date' and 'End Date' fields. At the bottom of the panel is a blue 'Analyze Data' button and an 'IMPORT INTO PROJECT' button. A status bar at the bottom of the window indicates 'Completed'.

Rule Name	Sources Z...	Sources	Sources ...	Users	Destinati...	Destinati...	Destinati...	Applicati...	Services
Autofo...	Trust	10.11...	Barcel...	any	50.18...	United...	Untrust	paloalt...	applica...
Outbo...	Untrust	192.16...	192.16...	any	8.8.8.8	United...	Untrust	dns	applica...
Firewa...	Trust	10.11...	Barcel...	any	10.11...	Barcel...	Trust	ssh	applica...
VPN D...	Trust VPN-D...	10.11... 192.16...	Barcel... Didac...	any	10.11... 192.16... 192.16...	Barcel... Didac...	Trust VPN-D...	ssl synolo...	applica...
Remot...	Untrust	38.142... 46.161... 50.116... 54.146... 66.175... 71.6.2... 74.82... 74.82... 80.82... 138.24... 139.16... 139.16... 139.16... 141.21... 163.17... More [...]	France Germa... Japan Russia... Seyche... Sweden United...	any	192.16... 192.16...	192.16... 192.16...	Untrust	ssl	applica...

Task 3 – Enrich the missing Zones

Let's import the Zones to our security policies.

Step 1: From the Discovery Window click on “IMPORT INTO PROJECT”

Step 2: Select “All Rules”

Step 3: Enable **Zone From** to import all the Source Zones found

Step 4: Enable **Zone To** to import all the Destination Zones found

Step 5: Check you are Updating the Existing Rule (Replace Rule) and the Source, VSYS and Template matches yours like in the screenshot.

(1) VMSeriesFW_007051000019156.xml

(2) vsys1

(3) template1

Enrichment Data by Rule Name

Rule Name	Sources Z...	Sources	Sources ...	Users	Destinati...	Destinati...	Destinati...	Applicati...	Services
Autofo...	Trust	10.11...	Barcel...	any	50.18...	United...	Untrust	paloalt...	applica...
Outbo...	Untrust	192.16...	192.16...	any	8.8.8.8	United...	Untrust	dns	applica...
Firewa...	Trust	10.11...	Barcel...	any	10.11...	Barcel...	Trust	ssh	applica...
VPN D...	Trust VPN-D...	10.11... 192.16...	Barcel... Didac...	any	10.11... 192.16... 192.16...	Barcel... Didac...	Trust VPN-D...	ssl synolo...	applica...
Remot...	Untrust	38.142... 46.161... 50.116... 54.146... 66.175... 71.6.2... 74.82... 74.82... 80.82... 138.24... 139.16... 139.16... 139.16... 141.21... 163.17... More [...]	France Germa... Japan Russia... Seyche... Sweden United...	any	192.16...	192.16...	Untrust	ssl	applica...

OPTIONS

ANALYZE +

IMPORT INTO PROJECT -

Apply To: Selection All Rules

Zone FROM Zone TO

Application Service

Users

Source: Destination:

IPs IPs

Create if objects doesn't exist.

Update to:

SOURCE:

VSYS/DG:

TEMPLATE:

Click on Analyze Data

Step 6: Click on the green button **Import** and wait for the task to finish and close the Window.

Step 7: Close the Window.

Step 8: Remove the filters by clicking on Clear All



Note: With this activity you learned how to fulfill the missing parameters on your security rules like Zones but It can be applied to Users / Applications / Services and Sources and Destinations IP address/Regions.

Try always to see if there is a chance to remove all the “any” from your Rules.

Task 4 – Enrich Source IP Address

Let’s continue working with this Security Policies and reuse the analysis we did to reduce the attack surface on the rule named Outbound DNS by adding the Source IP addresses seen.

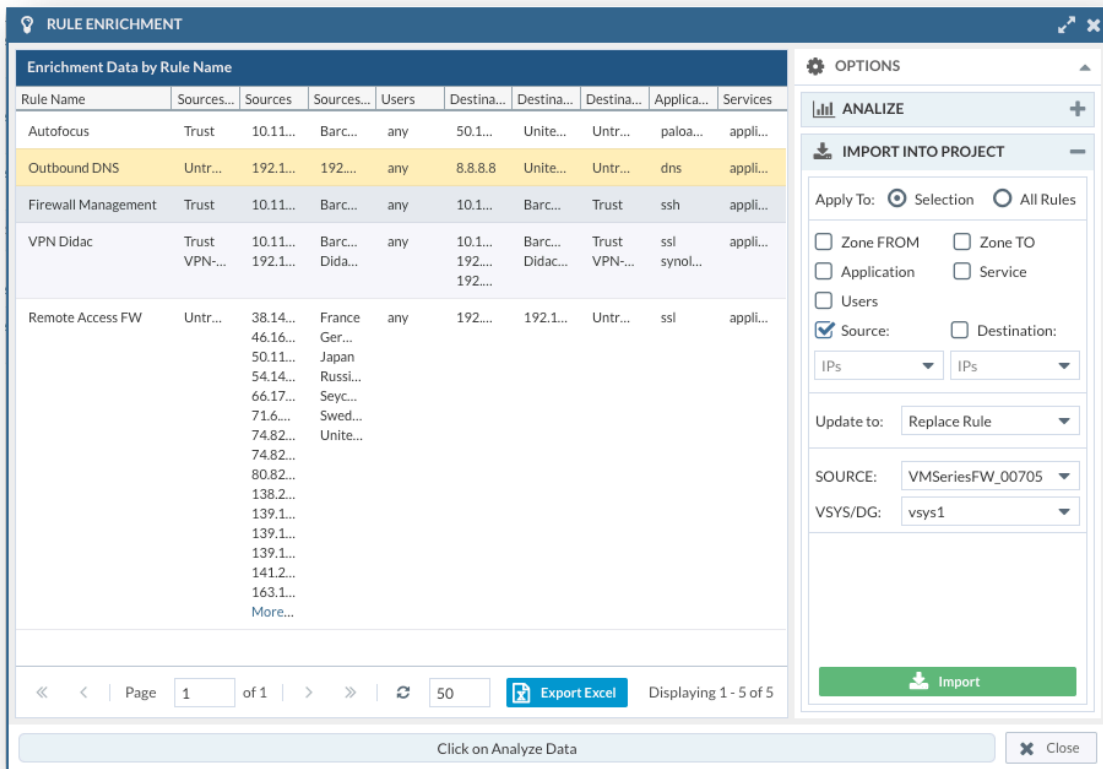
Step 1: From the POLICIES TAB click on the **Discovery** button and select Rule Enrichment.

Step 2: Select the Rule named Outbound DNS

Step 3: Click on the IMPORT INTO PROJECT panel

Step 4: Follow these instructions

- Apply to: Selection
- Check Source
- Under the Source keep IPs to import only the ip address instead the Regions to the Rule
- Update to: Replace Rule
- Validate the combo SOURCE is VMSeriesFW_007051000019156.xml
- Validate the combo VSYS/DG is vsys1
- Click on **Import** button



Step 5: Close the Window and review the policy

Step 6: Review the Security Rule called Outbound DNS

21	CL-uA- Outbound DNS	RE Enabled	Untrust	192.168.1.254	Untrust	8.8.8.8/32	any	udp53
12	Outbound DNS	RE Enabled	any	any	any	8.8.8.8/32	any	udp53

Check the original rule has been disabled to keep for review a new rule has been created with the changes introduced by the Rule Enrichment. Notice now the rule name is CL (cloned) uA (No Users, Yes Application) Original Rule Name. This is used by Expedition to know what type of rule we have created and in case we run again the Rule Enrichment consider if the change to make requires to split the rule because now we discovered users and we want that on a separate rule so the rule will be called CL (cloned) UA (Yes User, Yes Application) Original Rule Name.

Task 5 – Enrich App-ID

Let's continue working with this Security Policies and reuse the analysis we did to reduce the attack surface on the rule named Outbound DNS by adding the App-ID seen.

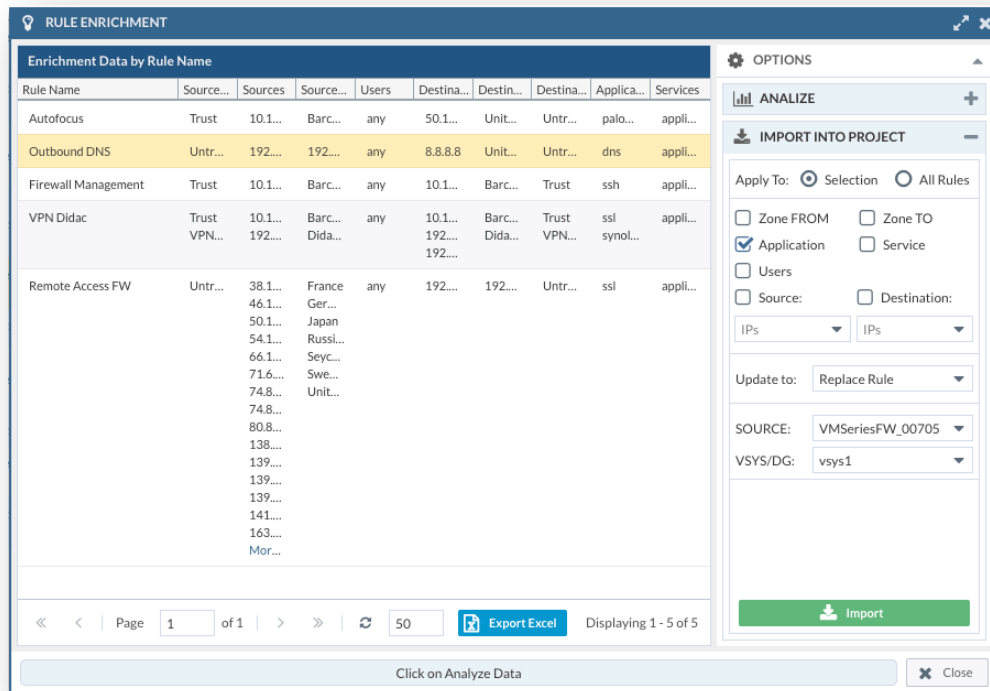
Step 1: From the POLICIES TAB click on the **Discovery** button and select Rule Enrichment.

Select the Rule named Outbound DNS

Step 2: Click on the IMPORT INTO PROJECT panel

Step 3: Follow these instructions

- Apply to: Selection
- Check Application
- Update to: Replace Rule
- Validate the combo SOURCE is VMSeriesFW_007051000019156.xml
- Validate the combo VSYS/DG is vsys1
- Click on **Import** button



Step 4: Close the Window and review the policy

Step 5: Review the Security Rule called CL-uA-Outbound DNS

21	CL-uA- Outbound DNS	RE Enabled	Untrust	192.168.1.254	Untrust	8.8.8.8/32	dns	udp53
12	Outbound DNS	RE Enabled	any	any	any	8.8.8.8/32	any	udp53

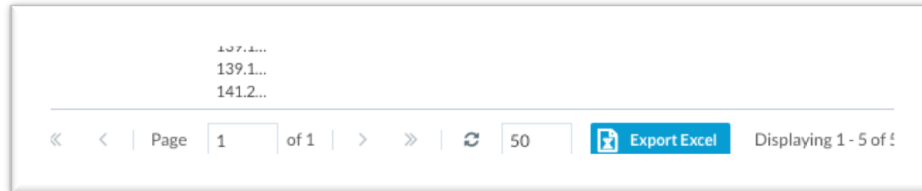
End of Activity 2

Task 6 – Export the Discovery to Excel

We can export the analysis to Excel to be analyzed offline. To export the analysis:

Step 1: From the Discovery Window, select the RULE ENRICHMENT TAB

Step 2: Click on Export Excel button from the bottom bar close the pagination buttons.



Step 3: Open with Excel or similar

	A	B	C	D	E	F	G	H	I	J
1	NAME	SOURCES	SOURCES	SOURCES	USERS	DESTINATIONS	DESTINATIONS	DESTINATIONS	APPLICATIONS	SERVICES
2	Autofocus	Trust	10.11.29.104	Barcelona		50.18.55.117	United States	Untrust	paloalto-autofocus	application-default
3	Outbound DNS	Untrust	192.168.1.254	192.168.192.168.255.255		8.8.8.8	United States	Untrust	dns	application-default
4	Firewall Management	Trust	10.11.29.4	Barcelona		10.11.29.250	Barcelona	Trust	ssh	application-default
5	Outbound	Trust	10.11.29.9,10.11.29.22	Barcelona	brw002556264e66, chromecest	8.8.8.8,10.100.11-10.100.11.1.12,216.58.210.174	10.0.0.0-10.255.255.11	Untrust	ping	any,
	Outbound	Trust	10.11.29.	Barcelona		2.16.72.5	10.0.0.0-	Untrust	adobe-	applicatio

End of Activity 2

Activity 3 – Rule Suggestions by M. Learning

In this activity you will:

- Run the Machine Learning Analysis to get Security Policies Suggestions to reduce the Attack surface
- Export the Changes back to the firewall by using API Integration

It's important to understand the differences between Machine Learning and Rule Enrichment.

When we use Rule Enrichment Expedition will group all the data by Rule Name and it will create a rule with all the traffic seen with Users, another one with the traffic seen without users, another one with the traffic where the applications were found through their default-port and another one with the traffic where the applications were found on a port different the default port.

That means with Rule Enrichment we will get a maximum of 4 rules by each rule we are analyzing.

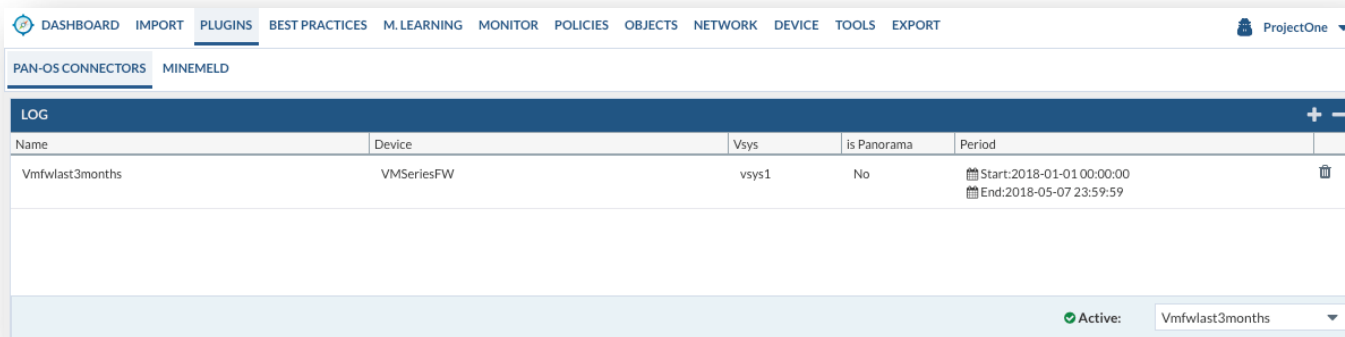
In case to use Machine Learning, what Expedition will do is to create as much rules as consumptions models we were able to identify from the traffic analyzed. That means we can get tons of rules from any rule selected for the analysis.

Machine Learning must be used when a security policy can lead us to have like a new ruleset basically because the rule itself was too wide open, like when we are on a Green Field and we have mostly one rule that allows all the traffic from **Trust** to **Untrust**, there we want to know who the Servers are and who is consuming what from the network.

To demonstrate this, we will show how a simple Rule that allows all the traffic between some Zones will be transformed in many new Rules more specific to reduce the attack surface and create a new security ruleset.

Task 1 – Set Rules for M. Learning

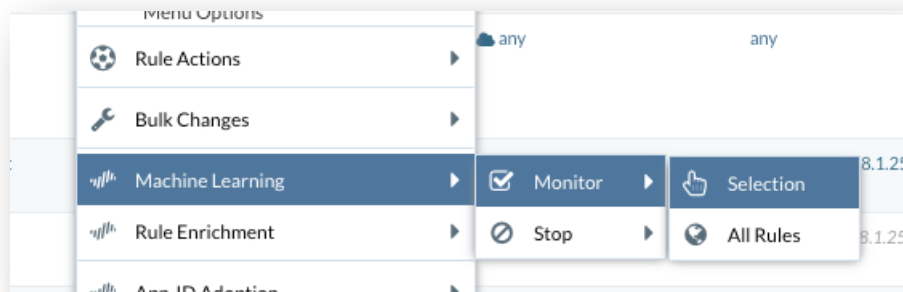
Step 1: Check we have a Log connector created and Active. Navigate to PLUGINS TAB.



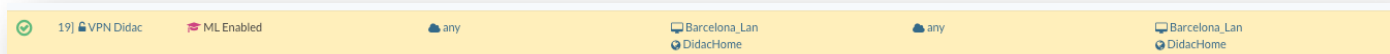
Step 2: Navigate to the POLICIES Tab.

Step 3: Select the Rule Name **19) VPN Didac** (*this rule is actually disabled because the Rule Enrichment process*)

Step 4: Right-click and select Machine Learning -> Monitor to enable the rule for being analyzed.



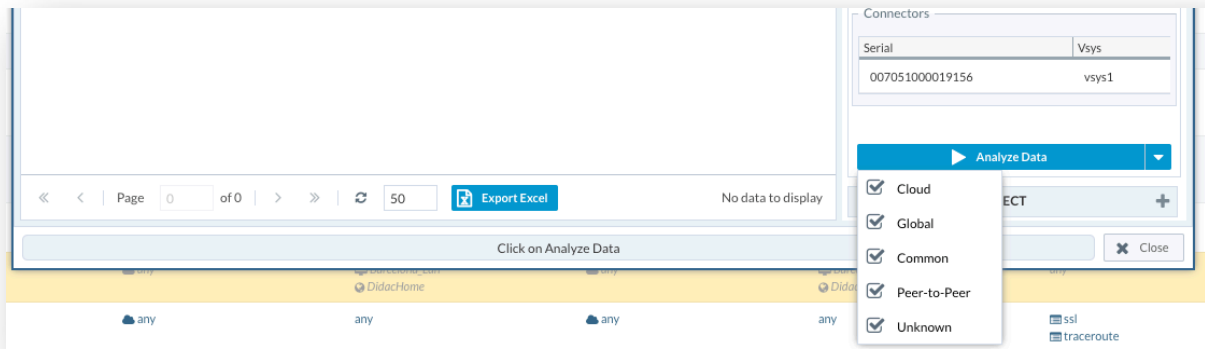
Step 5: Check the Rule now is tagged with ML Enabled



Step 6: Click on the green button **Discovery** and select Machine Learning

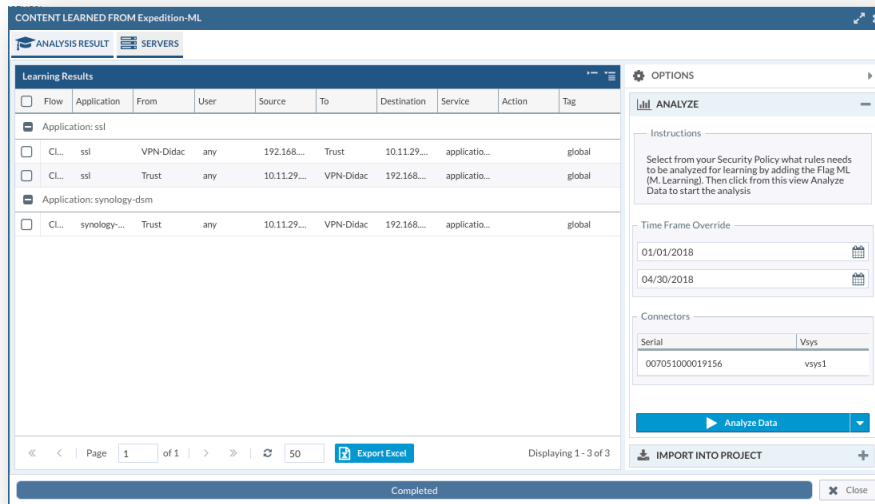
Step 7: The first TAB is called ANALISYS RESULT has on the right panel a button named **Analyze Data**.

The button can be extended by clicking on the arrow.



- a) Cloud: Means Expedition will consider some applications as Cloud, when found in the traffic the destination ip addresses will be considered as “any” since they can dynamically change and doesn’t make sense to keep the ones the network resolved in the moment we captured the traffic.
- b) Common: Are considered common applications those that are present in all the networks and generates a huge volume of logs. Ex: ping, dns, ldap. In some cases, you won’t want to waste resources to analyze logs related to those applications to speed up the analysis for other applications. In case Expedition finds traffic regarding those applications will be considered as source “any” and destination “any”. Ex: ping Rule suggested ANY – ANY – ping – ALLOW
- c) Peer-to-Peer: All the applications classified as peer to peer by Palo Alto Networks.
- d) Global: All the other applications. Expedition will analyze sources, destinations, users, service ports to suggest Rules based on how they are consumed.
- e) Unknown: It will analyze the unknown applications separately. (unknown-tcp, unknown-udp, unknown-p2p).

Step 8: Click on Analyze Data to start the analysis. Wait until a URL will be shown in the progress bar. In this exercise you cannot click there because Expedition It’s behind a NAT and the URL its internal.



This is the result of the analysis for a single rule. This is all the Rules suggested based on how the applications have been consumed. In this case there are no users.

The Flow has been calculated after figure it out who are the servers on the networks.

Tag tells you the container for the APP. In this case all were Global.

Task 2 – Review the learned Servers

Step 1: Click on the SERVERS TAB

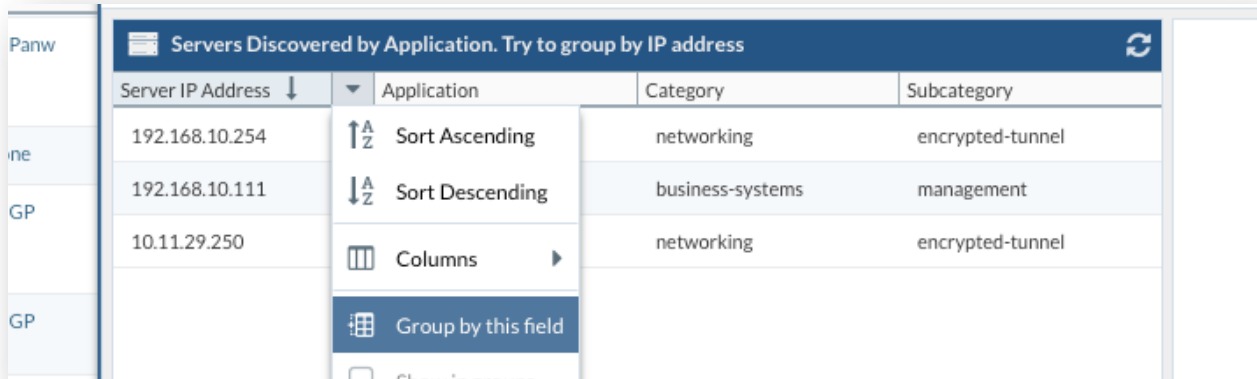
Server IP Address	Application	Category	Subcategory
10.11.29.250	ssl	networking	encrypted-tunnel
192.168.10.254	ssl	networking	encrypted-tunnel
192.168.10.111	synology-dsm	business-systems	management

This is the list of the servers we found from the logs after analyze who is who in the network. This is important to Expedition to understand the flow of the communications. Expedition supports asymmetric traffic environments.

This list of servers can be exported for an offline review by clicking on the Export Excel

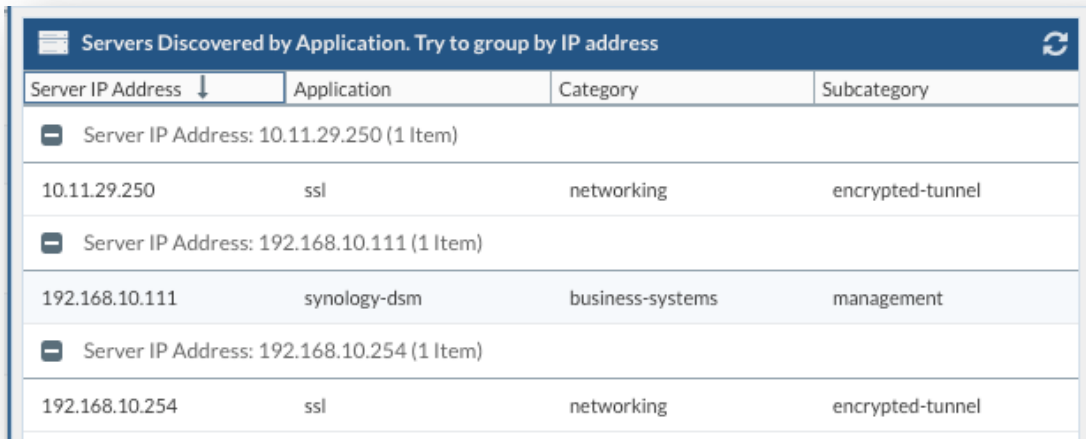
Step 2: Group the Applications seen by Server

- Point your mouse over the column “Server IP Address” and click on the arrow and click on the “Group by this field” In this example nothing will change but in real life environments will give you the applications served by each server we used.



The screenshot shows a table titled "Servers Discovered by Application. Try to group by IP address". The table has four columns: "Server IP Address", "Application", "Category", and "Subcategory". A context menu is open over the "Server IP Address" column, showing options: "Sort Ascending", "Sort Descending", "Columns", and "Group by this field". The table data is as follows:

Server IP Address	Application	Category	Subcategory
192.168.10.254		networking	encrypted-tunnel
192.168.10.111		business-systems	management
10.11.29.250		networking	encrypted-tunnel



The screenshot shows the same table after being grouped by "Server IP Address". The table is now grouped into three sections, each with a minus sign icon and a header: "Server IP Address: 10.11.29.250 (1 Item)", "Server IP Address: 192.168.10.111 (1 Item)", and "Server IP Address: 192.168.10.254 (1 Item)". The data rows are as follows:

Server IP Address	Application	Category	Subcategory
Server IP Address: 10.11.29.250 (1 Item)			
10.11.29.250	ssl	networking	encrypted-tunnel
Server IP Address: 192.168.10.111 (1 Item)			
192.168.10.111	synology-dsm	business-systems	management
Server IP Address: 192.168.10.254 (1 Item)			
192.168.10.254	ssl	networking	encrypted-tunnel

Task 3 – Import Suggested Rules

Step 1: Select ANALISYS RESULT TAB.

Step 2: Select all the Rules

Step 3: Click on the right panel called IMPORT INTO PROJECT

Step 4: Validate the following options are checked:

- Apply to: **Selection**
- Objects: **All Checked**
- Transform: **Unchecked**
- SOURCE: **VMSeriesFW_007051000019156.xml**
- VSYS/DG: **vsys1**

Step 5: Click on **Import**.

CONTENT LEARNED FROM Expedition-ML

ANALYSIS RESULT RULE ENRICHMENT SERVERS

Learning Results

Flow	Application	From	User	Source	To	Destina...	Service	Tag
Application: ssl								
Client_to_Server	ssl	Trust	any	10.11...	VPN-...	192.1...	application-default	global
Client_to_Server	ssl	VPN-Didac	any	192.1...	Trust	10.11...	application-default	global
Application: synology-dsm								
Client_to_Server	synology-dsm	Trust	any	10.11...	VPN-...	192.1...	application-default	global

OPTIONS

ANALYZE

IMPORT INTO PROJECT

Apply To: Selection All Rules

Objects: Address Applications Zones Services Users Security Rules

Transform: Objects as Shared

SOURCE: VMSeriesFW_0070

VSYS/DG: vsys1

Import

Page 1 of 1 50 Export Excel Displaying 1 - 3 of 3

Step 6: Close the Discovery window

Step 7: Scroll down on the Security Policy and select the new 3 rules created

tracertoute

26) EX 26	global Client_to_Server	VPN-Didac	192.168.10.4	Trust	10.11.29.250	ssl	application-default
27) EX 27	global Client_to_Server	Trust	10.11.29.25	VPN-Didac	192.168.10.254	ssl	application-default
28) EX 28	global Client_to_Server	Trust	10.11.29.25	VPN-Didac	192.168.10.111	synology-dsm	application-default

Page 1 of 1 50 Multi Edit Move Discovery Ready 1 - 28 of 28

Palo Alto Networks - Dynamic Toolbars VMSeriesFW_007051000019156.xml vsys1

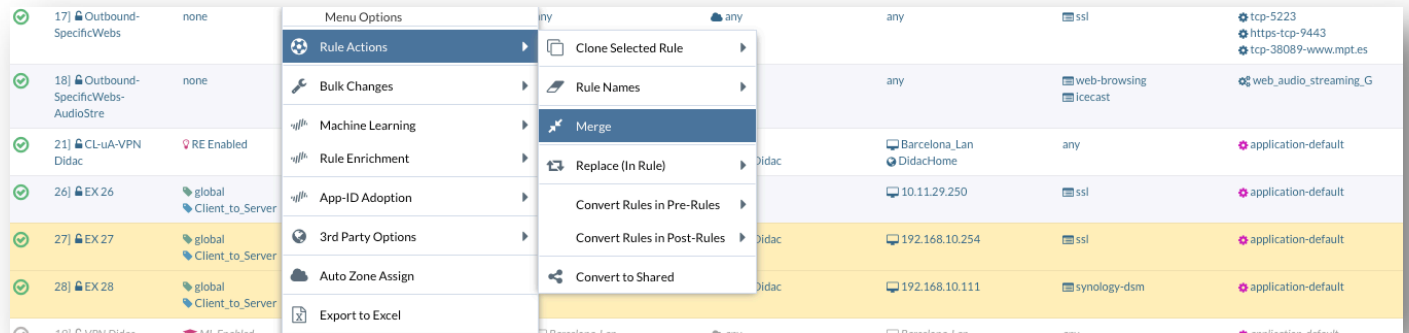
Step 8: Click on the **Move** blue button

Step 9: Move the selected rules to BEFORE VPN Didac



Step 10: Click on **Move**.

Step 11: Let's Merge 2 of the rules we just generated (EX27 and EX28) by just one by selecting them and then right-click and select Rule Actions -> Merge



Step 12: Check the merged rule. The rule contains all the information merged and the rule is tagged as merged for validation.



End of Activity 3

Activity 4 – Best Practices Adoption

Palo Alto Networks has been working on having a collection of Best Practices to help our customers use the most of our functionality in the best way as possible. In 2017, Palo Alto Networks created a tool called *Best Practices Assessment Tool* to evaluate PanOS configurations and provide feedback to guide on how to improve those configurations.

Expedition has gone one step beyond and has integrated the Best Practices Assessment Tool and implemented some remediations inside to be automatically configured to be in compliant of the Assessment Tool.

In this activity you will:

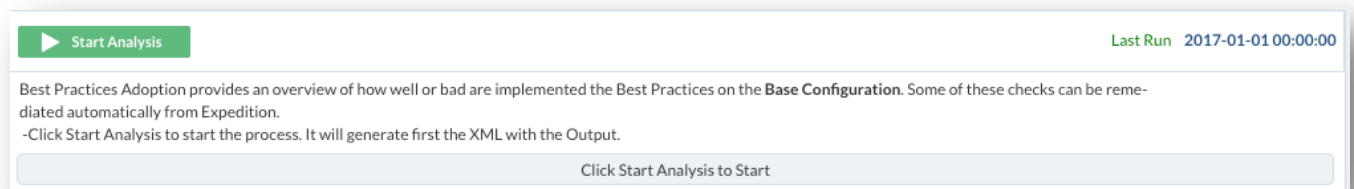
- Analyze your Firewall configuration against the Best Practices Assessment Tool from within Expedition
- Enforce remediation automatically to increase the security on the Platform
- Export the Changes back to the firewall by using API Integration

Task 1 – Run the Best Practices Assessment Tool (BPA)

Step 1: Navigate from within the Project to the BEST PRACTICES tab

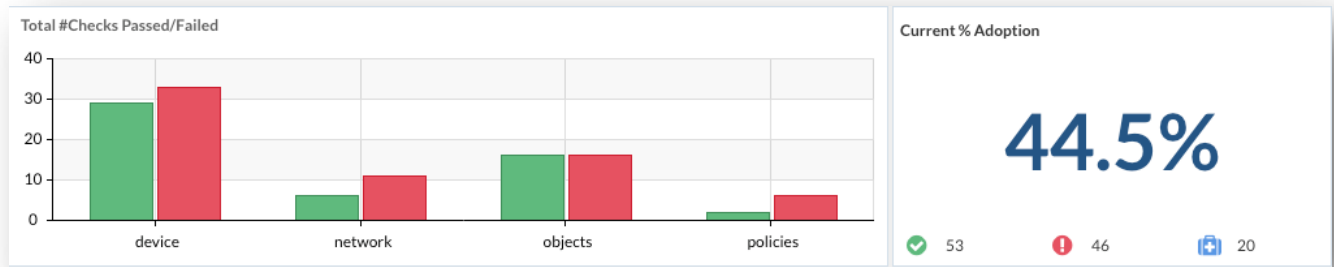
Step 2: Click on the Start Analysis green button

Note: The BPAT will only work if we have one Base Configuration loaded in the Project. Remember the base Configuration it's a Palo Alto Networks configuration and can be set as Base Configuration from the EXPORT tab.



Step 3: After the process ends you can read the last Run date to confirm that was just executed

Let's understand the charts:

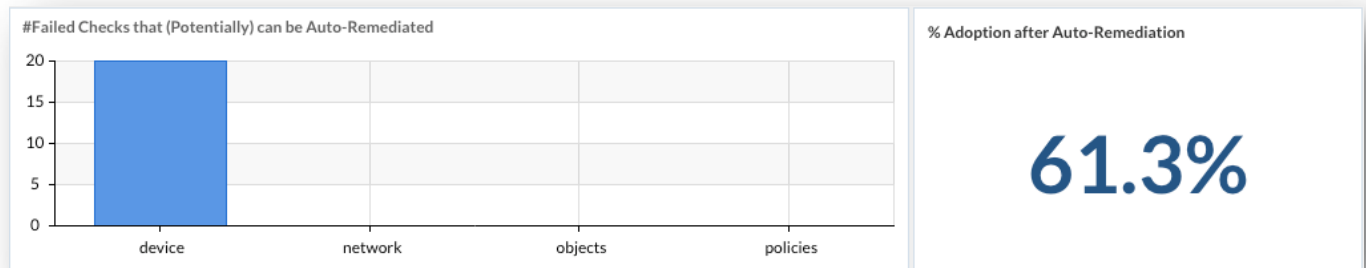


The first charts are telling you the amount of best practices passed vs the failed ones by TOPIC. Take as Topic Device for instance, that means all the checks we evaluated under the DEVICE Tab from a PANOS device.

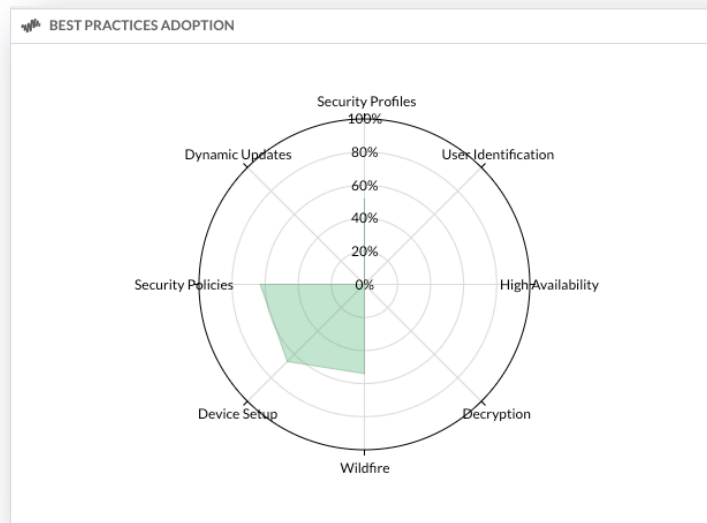
The next percentage is showing that, the percentage of the checks Passed, in this example 44,5% of the total checks has been passed.

Take a look to the blue bag, that blue bar tells us there are 20 checks that Expedition can remediate automatically. On summary we passed 53 checks and failed 46.

Next chart is showing us the amount of checks that Expedition can remediate by Topic, in our case all the checks that can be remediated are under the Device Topic only and the percentage is telling us if we remediate them we will increase the best practice adoption to 61,3% instead the 44,5% we have if we don't remediate them.



The Radar chart just shows us how we are doing the adoption by topic, our goal is always try to cover the whole Radar chart with green (100% passed) but not all the environments are equal, in case we don't need SSL Decrypt or HA those will stay in 0 so we will never reach 100% of the checks passed but it will be ok because we don't need them.



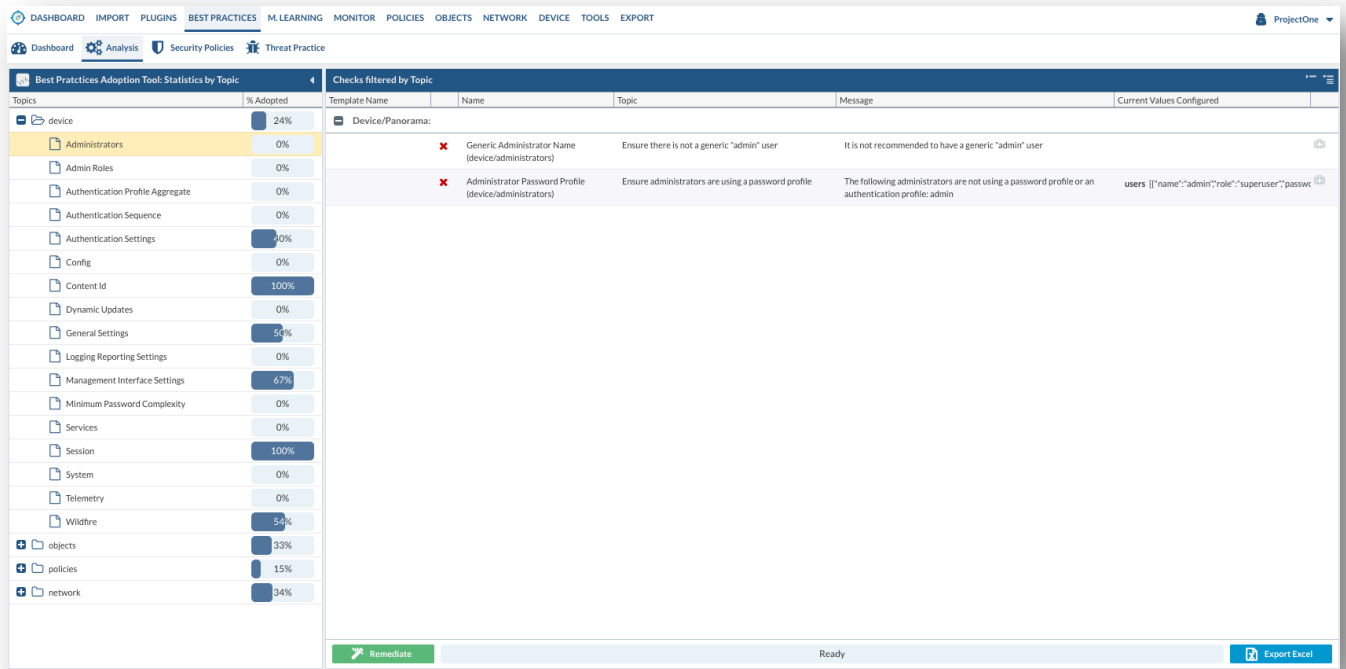
In this case we have a lot of room for improvement, starting with properly configure the Dynamic Updates for instance.

Task 2 – Export Report to Excel

Step 1: From within the Project and keeping selected the Best Practices Tab let's select the next one called Analysis.

Step 2: Open from the Tree located at the left the Device option and then select Administrators

This will show us two panels; the left panel shows the different topics (Device, Objects, Policies, Network and Panorama in case the configuration comes from Panorama) and the right panel who will show us the checks associated to the selected topic. The left panel will act as filter for the right's panel.



Let's Export all the Checks to an Excel file.

Step 3: Click on the Export Excel blue button located at the bottom right of the current view.

Step 4: Open it if you have Excel and review it.

RESULT	CHECK NAME	TOPIC	MESSAGE	RATIONALE
Administrators				
FAILED	Generic Administrator Name	Ensure there is not a generic "admin" user	It is not recommended to have a generic "admin" user	As we know that the default username is "admin" on our platform and we should never make it easy for an attacker with known usernames to get access or login to the system. The credentials for username and password both should be unique to the company to make it hard for any attacker to guess for credentials to gain access. Hence we should make sure there is no username with "admin"
FAILED	Administrator Password Profile	Ensure administrators are using a password profile	The following administrators are not using a password profile or an authentication profile: admin, dgil, adevega, mt_admin, xhoms, mt_viewer, mt_user	Password profile helps by setting a fixed period for the password to be active and expires after that period. This ensures no password is used forever and has to create a new password after the set period so saved credentials or stolen credentials cannot make any benefit from gaining access to the firewall by any user.
INFO	Local Admins	None	It is best practice to have no more than two administrators with local accounts.	When configuring Administrator accounts on the firewall make sure the Admin login accounts are configured as external authentication. External Authentication make sure an external authentication server handles such requests for all the requests originating in the company from different vendor products. It helps in single means of external authentication across the network devices and helps in setting more features as needed. Also

You can use this Excel file to track your changes and review them before plan how to remediate all you can.

Task 3 – Apply remediation to the failed Checks

Step 1: Navigate now to the Authentication Settings option, check the gray bag icon at the right of the view, if it's dark gray indicates that check can be automatically remediate.

Checks filtered by Topic						
Template Name	Name	Topic	Message	Current Values Configured		
Device/Panorama:						
✓	Authentication Profile (device/setup/management/authen...	Ensure an Authentication Profile is configured	Passing because Administrators are configured with a non-local authentication profile	authentication_profile	None	
✗	Certificate Profile (device/setup/management/authen...	Ensure a Certificate Profile is configured	It is recommended to configure a certification profile.	certificate_profile	None	
✓	Failed Attempts (device/setup/management/authen...	Ensure Failed Attempts is set to a value lower than or equal to 3	Test passed successfully !	failed_attempts	0	
✗	Idle Timeout (device/setup/management/authen...	Ensure Idle Timeout is set to a value lower than or equal to 10	It is recommended for idle timeout to be set to a value lower than or equal to 10.	idle_timeout	60	
✗	Lockout Time (device/setup/management/authen...	Ensure Lockout Time is set to a value lower than or equal to 15	It is recommended for lockout time to be set to a value greater than or equal to 15.	lockout_time	0	

In this case the last 3 checks can be remediated by the recommended values.

Step 2: Select Checks Idle Timeout and Lockout Time

Checks filtered by Topic						
Template Name	Name	Topic	Message	Current Values Configured		
Device/Panorama:						
✗	Authentication Profile (device/setup/management/authen...	Ensure an Authentication Profile is configured	It is recommended to use external authentication.	authentication_profile	None	
✗	Certificate Profile (device/setup/management/authen...	Ensure a Certificate Profile is configured	It is recommended to configure a certification profile.	certificate_profile	None	
✓	Failed Attempts (device/setup/management/authen...	Ensure Failed Attempts is set to a value lower than or equal to 3	Test passed successfully !	failed_attempts	0	
✗	Idle Timeout (device/setup/management/authen...	Ensure Idle Timeout is set to a value lower than or equal to 10	It is recommended for idle timeout to be set to a value lower than or equal to 10.	idle_timeout	60	
✗	Lockout Time (device/setup/management/authen...	Ensure Lockout Time is set to a value lower than or equal to 15	It is recommended for lockout time to be set to a value greater than or equal to 15.	lockout_time	0	

Remediate
Ready
Export Excel

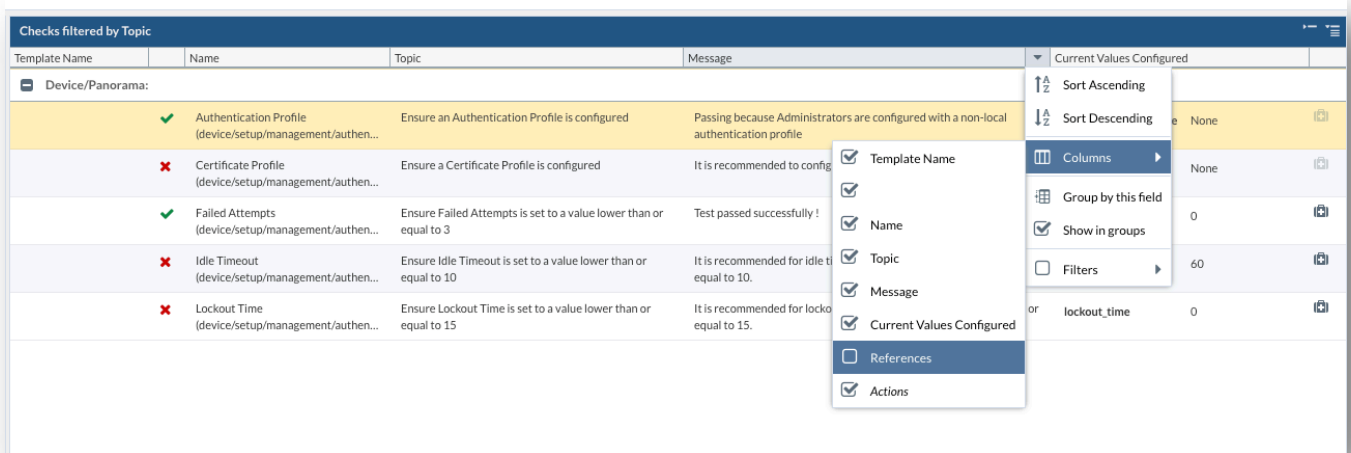
Step 3: Click on Remediate

Step 4: Validate the Checks now look in green

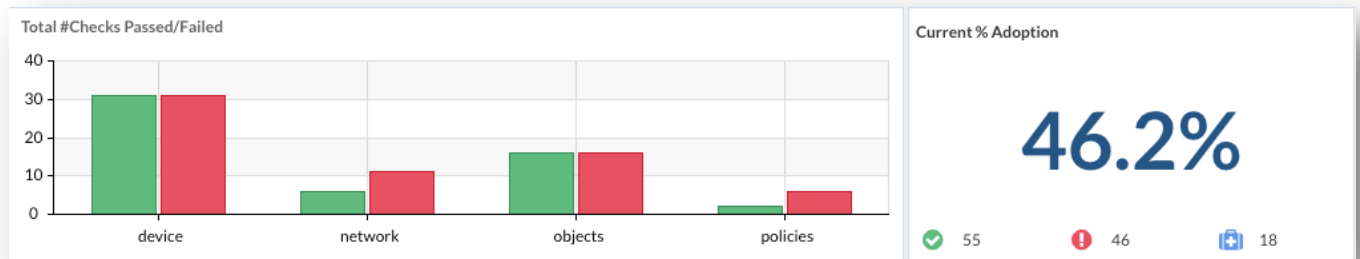
✓	Idle Timeout (device/setup/management/authen...	Ensure Idle Timeout is set to a value lower than or equal to 10	It is recommended for idle timeout to be set to a value lower than or equal to 10.	idle_timeout	60	
✓	Lockout Time (device/setup/management/authen...	Ensure Lockout Time is set to a value lower than or equal to 15	It is recommended for lockout time to be set to a value greater than or equal to 15.	lockout_time	0	

We can add more information related to the Check it self and the recommendation by showing a hidden column called references, in case there are any they will be web references that can be clicked to follow the link

Step 5: Point your mouse to one of the columns and when the arrow shows up click on Columns -> Reference



Step 6: Go back to the Dashboard and recheck the percentage of the Passed Checks

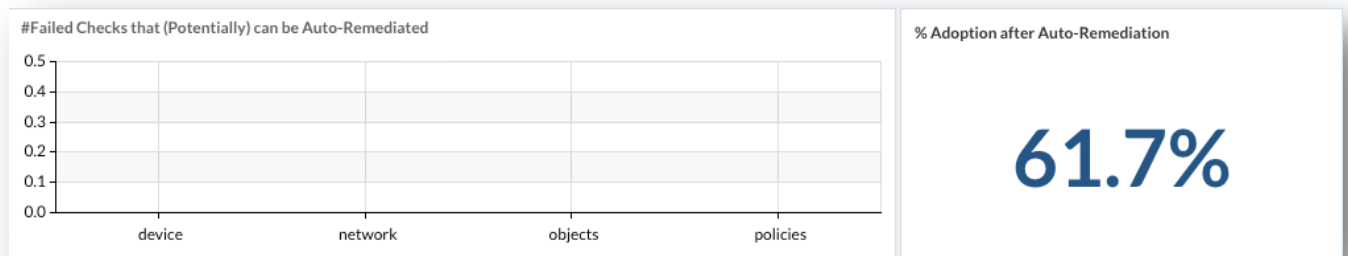
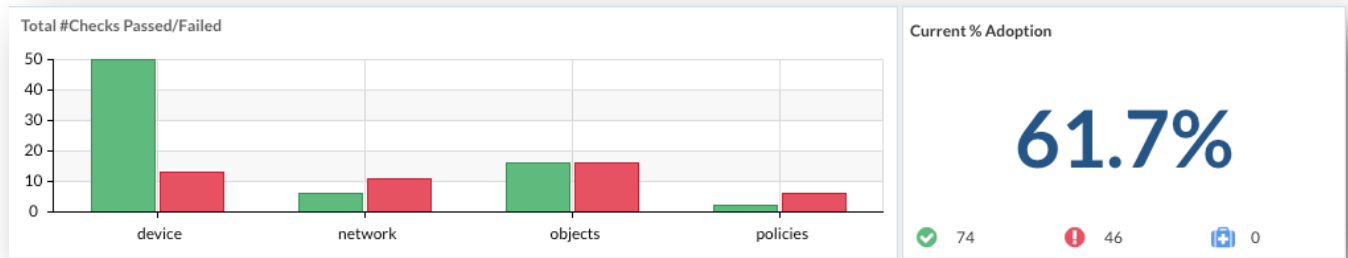


If we want to apply Remediation to the entire Devices Topic:

Step 7: From the Analysis tab click on the device option and select all the checks

Step 8: Click on Remediate, that will remediate all the checks available under device.

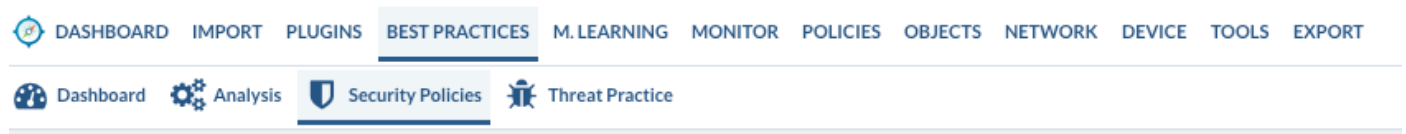
Step 9: Go back to the Dashboard to check all the remediation was applied



So now both are equal. All the other checks can be fixed by hand now from Expedition or from your PanOS device.

Task 4 – Reviewing the Security Policies Best Practices

Step 1: Navigate to the next Tab named Security Policies



This view shows some checks against the security policies configuration best practices, you can see how your security policies has been implemented. Goal is to follow the best practices at the time to manage the Security rules like ensure all the rules have Description, or you are not abusing of the LOG START that can create tons of logs.

Step 2: Expand the Rule under vsys1 to view all the checks

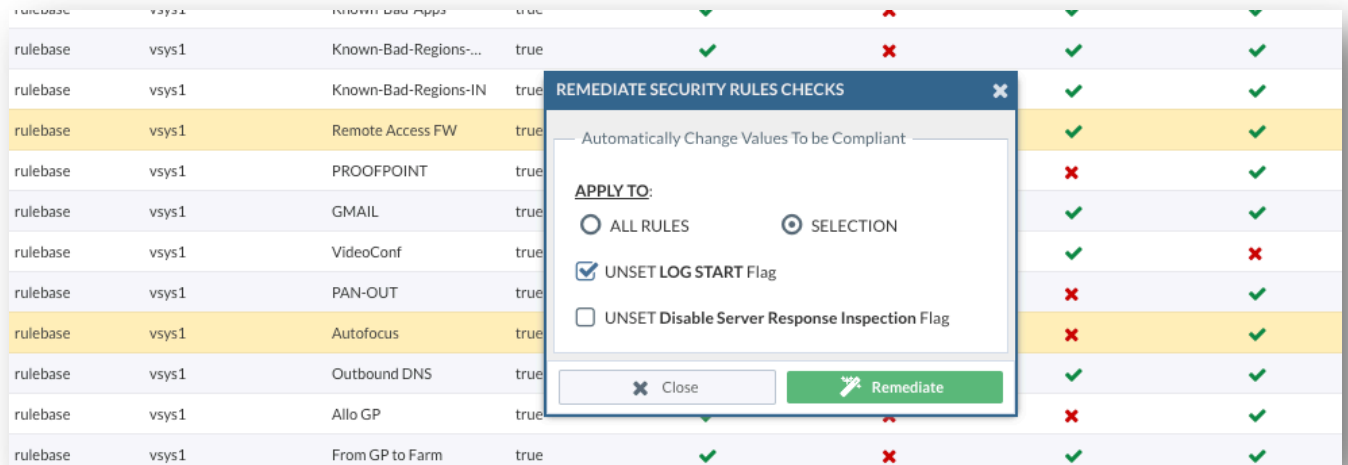
Step 3: Point your mouse in the icon for pass / failed to see the check description

ys	Rule Name	Rule Enabled	Tags Used	Description Populated	Source Destination Any	Serv
/sys: vsys1						
sys1	LAB USELESS RULE	true	✗	✗	✗	✓
sys1	Block Malware	true	✗	Ensure tags are used on Security rule	✓	✓
sys1	Known-Bad-Apps	true	✓	✗	✓	✓
sys1	Known-Bad-Regions-...	true	✓	✗	✓	✓
sys1	Known-Bad-Regions-IN	true	✓	✗	✓	✓

Step 4: Let's Review the Rules to find the ones where the Log Start was enabled so the check will be seen as Failed, because we recommend to don't abuse of the Log Start.

Step 5: Select the Rules where the check Log Start failed and click on the Remediate button

Step 6: A new window will be shown. Select SELECTION and check UNSET LOG START Flag

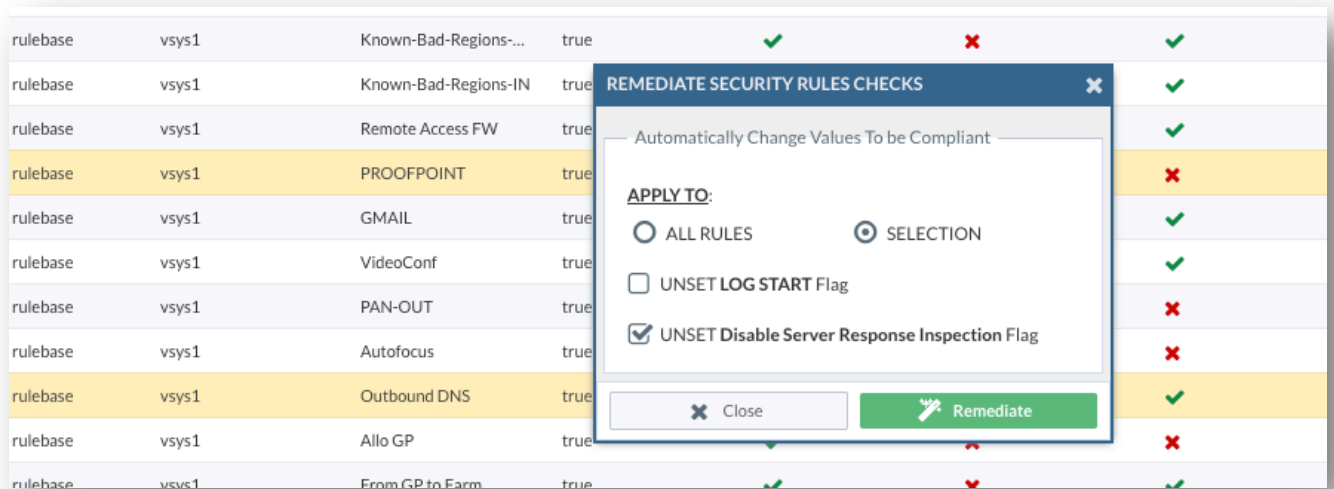


Step 7: Click on Remediate

Step 8: Let's now review the Rules where the Flag DSRI failed, that is related to the function Disable Server Response Inspection.

Step 9: Select the Rules affected by that flag and click on Remediate

Step 10: Click on SELECTION and check UNSET Disable Server Response Inspection flag



Step 11: Click on Remediate

End of Activity 4

Activity 5 – Importing Iron-Skillet

What is Iron-Skillet? The purpose of the Iron-Skillet project is to provide day-one best practice configuration templates that can be loaded into a Palo Alto Networks Next-Generation Firewall or Panorama management platform.

Iron-skillet can be used from Expedition to create base configuration files to import on top the policies and objects migrated from other vendors or to grab some pieces like best practices security profiles and import them in your current Palo Alto Networks configuration.

In this exercise we will create an Iron-Skillet configuration and we will import the security profiles to our current project and apply them to all our rules with the Bulk change capability.

Task 1 – Import a new Iron-Skillet configuration

Step 1: From within the current Project go to the IMPORT tab. Select Palo Alto TAB and click on IRON-SKILLET TAB

The screenshot shows the Expedition web interface. At the top, there is a navigation bar with tabs: DASHBOARD, IMPORT, PLUGINS, BEST PRACTICES, M. LEARNING, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, TOOLS, EXPORT. Below this is a sub-navigation bar with tabs: PALO ALTO, CSV, CHECKPOINT, CISCO, FORTINET, IBM XGS, JUNIPER, FORCEPOINT. The main content area is divided into two sections. The left section is titled 'Single File' and has a description: 'Upload a Panos or Panorama configuration XML file. Export it from your device.' It contains an 'XML File:' input field and a 'Browse' button. The right section is titled 'Multiple Files (in ZIP)' and has a description: 'Upload a ZIP file with all the configurations to import.' It contains a 'ZIP File:' input field and a 'Browse' button. Below these sections is a section titled 'IRON-SKILLET' with an 'Information' sub-section. The information text reads: 'Project Iron-skillet https://iron-skillet.readthedocs.io/en/panos_v8.0 provides an easy way to generate configurations day0 to automatically create all the best practices profiles, logging and reporting. By using the vars you can customise the output and use it in Expedition as a Base Configuration for your projects. Import your own variable values by using COPY and PASTE by clicking on LOAD FROM CLIPBOARD or assign them manually.' At the bottom of the Iron-Skillet section, there is a form with a dropdown menu for 'Configuration Type' set to 'NG-Firewall', a dropdown menu for 'PanOS © Version' set to '9.0', and a 'LOAD FROM CLIPBOARD' button.

Step 2: From Configuration Type keep NG-Firewall

Step 3: From PanOS Version select 9.0

Step 4: Click on GENERATE CONFIG AND IMPORT

This will generate a full PanOS firewall configuration based on version 9.0 and holding a ton of the best practices already configured. In this case we want to focus in the Security Profiles iron-skillet provides and a list of custom reports ready to be consumed. Let's import them into your project.

Task 2 – Move Custom Reports and Security Profiles to your Configuration

First check the configuration selected is panos_9.xml and the virtual system is vsys1 from the bottom bar

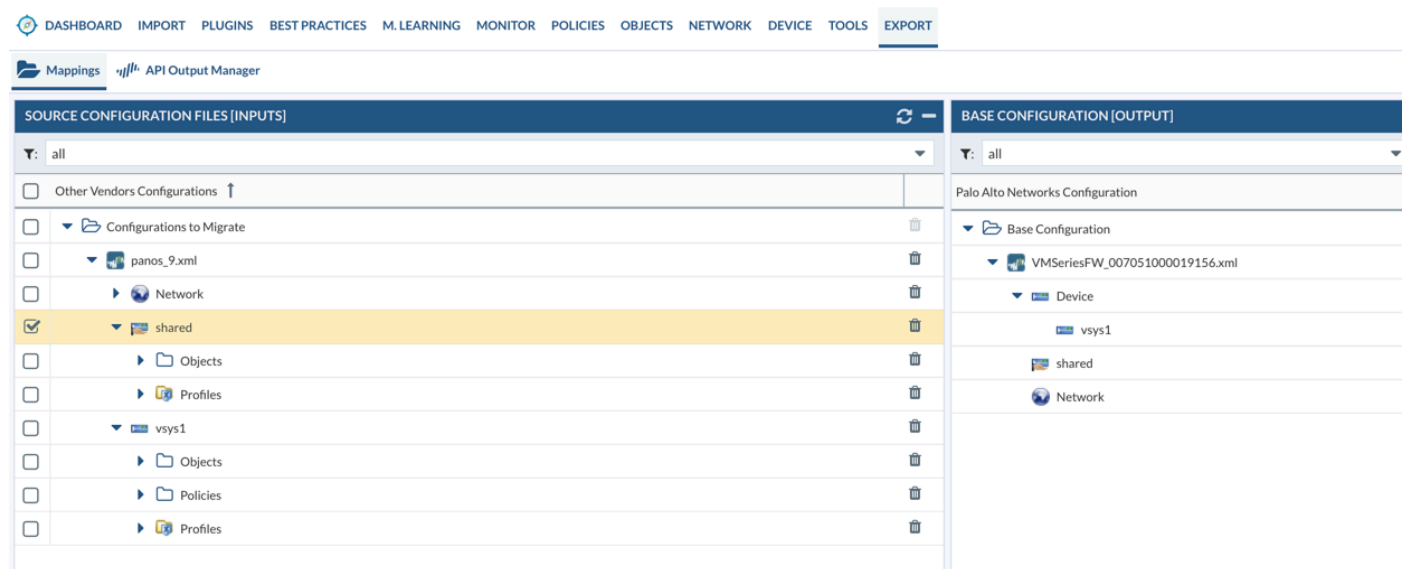


Step 1: Click on the Objects TAB and then select Contents TAB

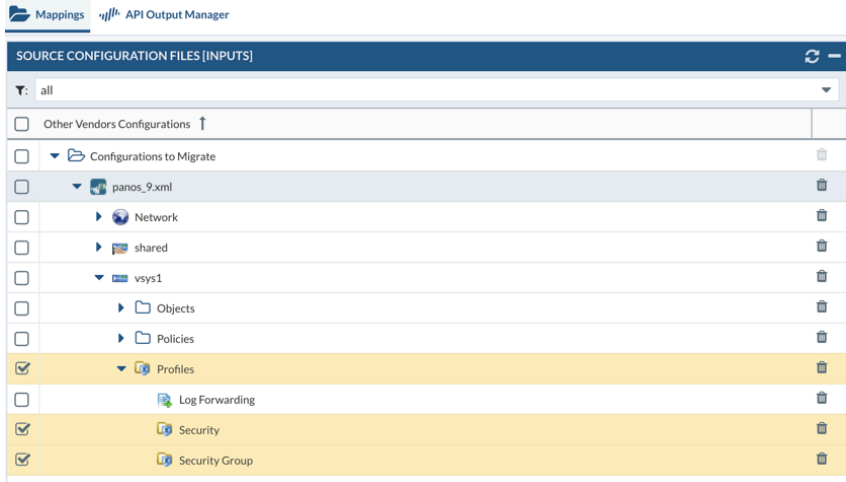
Step 2: Review the profiles to see there are some like Inbound-AV, Inbound-AS, etc

Step 3: Review the Custom Reports by navigating to MONITOR -> Reports

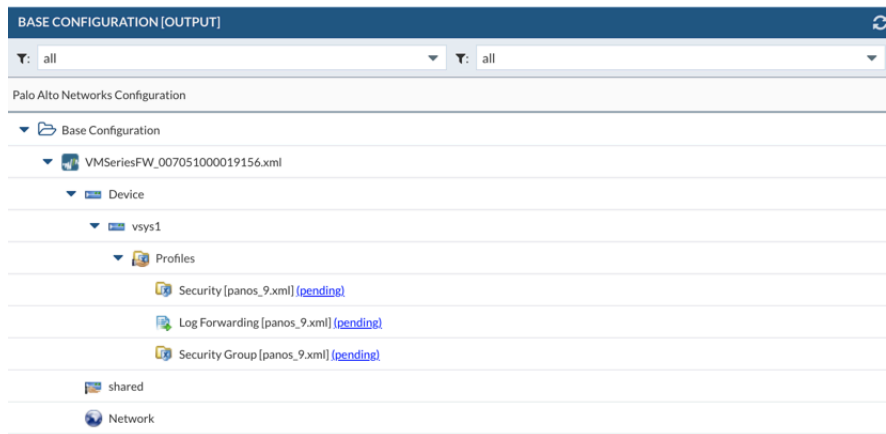
Step 4: Go to EXPORT TAB and open the 2 trees to see the panos_9 and the Base Configuration files



Step 5: From the Left Panel select on vsys1 the Profiles object and inside it the Security and Security Group

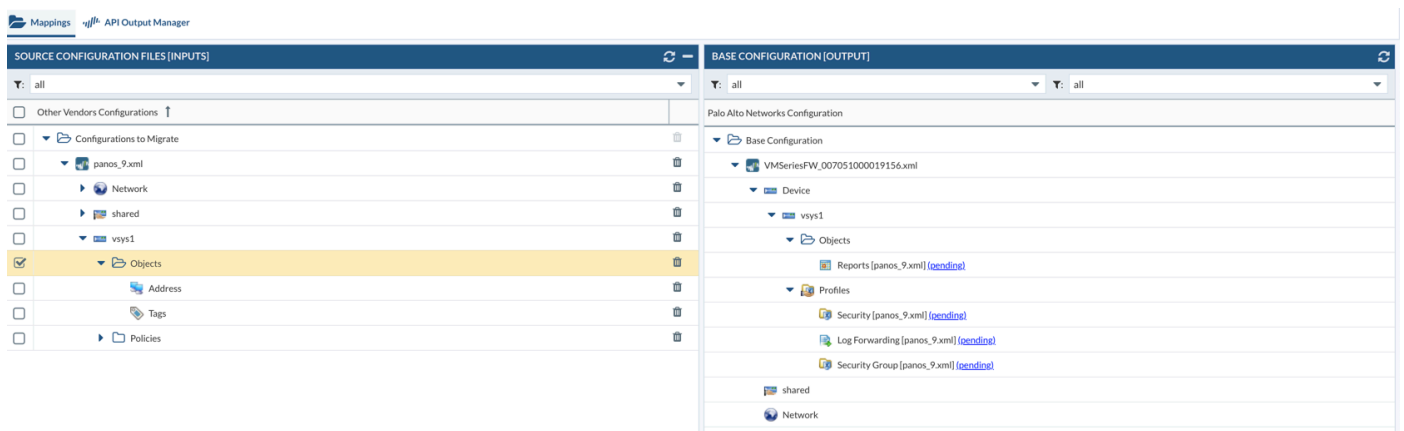


Step 6: Drag and drop to the right panel inside the vsys1



Step 7: Repeat the same with Reports under vsys1 from the left panel to the right

Step 8: Click on MERGE to make the change permanent.



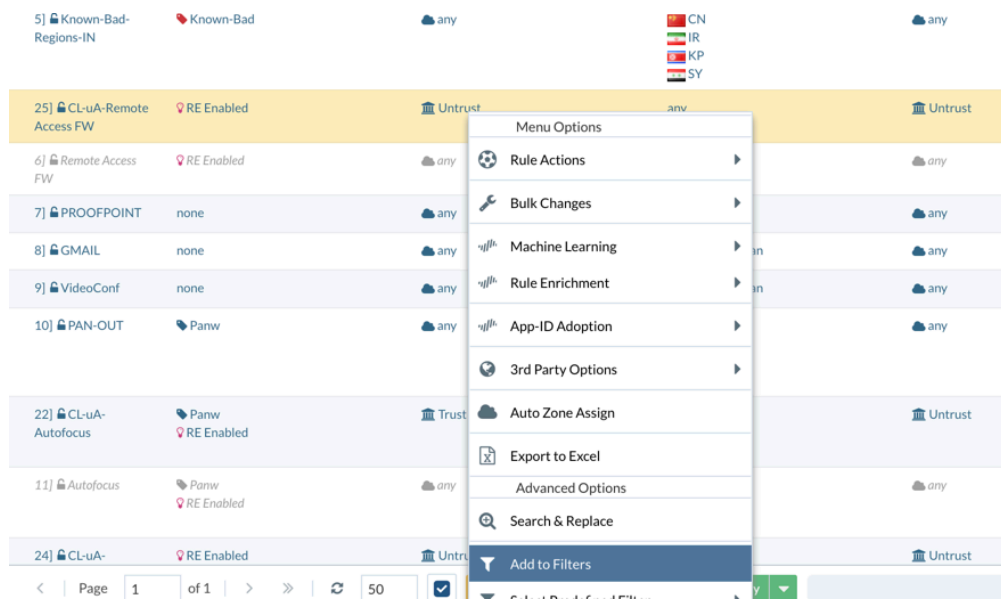
Task 3 – Apply the iron-sillet profiles to your Rules

Change the configuration to your Base configuration and select vsys1

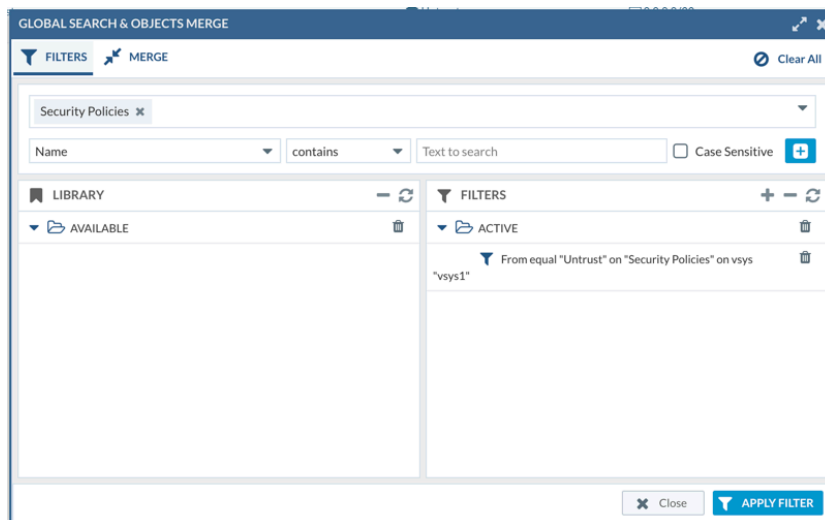


Step 1: Go to POLICIES

Step 2: Point your mouse in the rule where a source zone is Untrust like id 25 and with right-click select Add to filters.

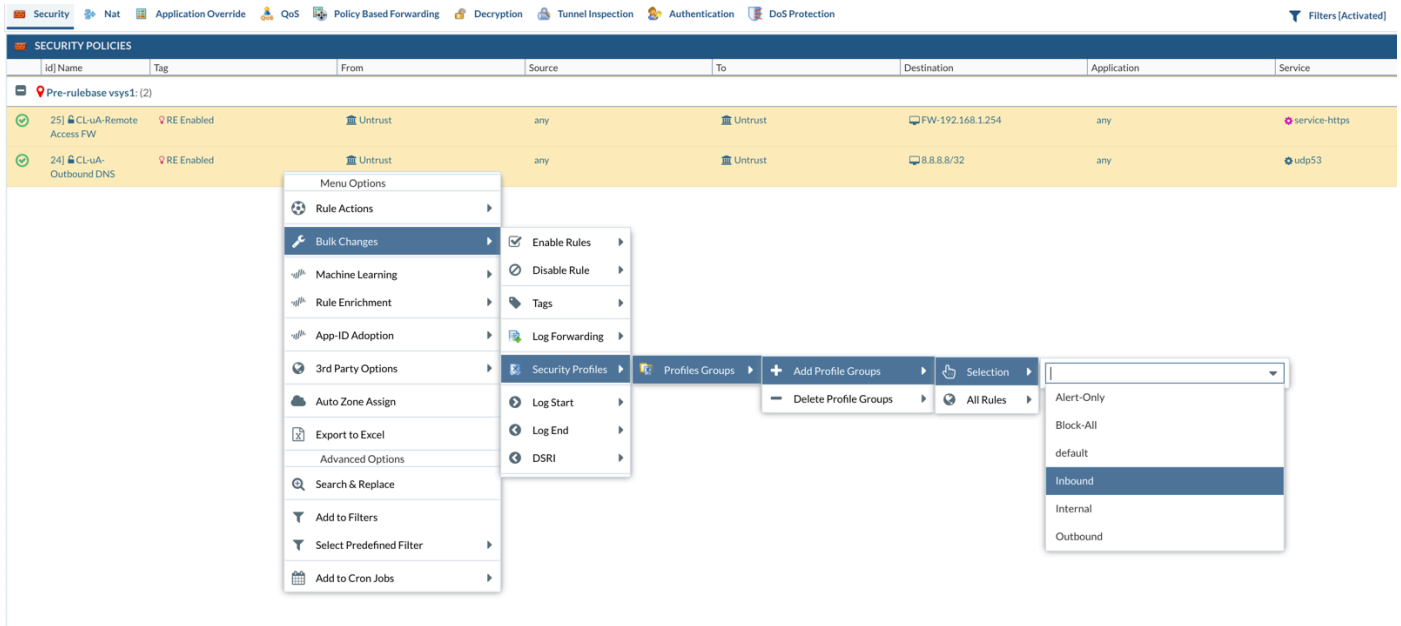


Step 3: A new window will show up with the filter click on Apply. That will show the rules where the Untrust zone is the From Zone.



Step 4: Select the rules shown.

Step 5: Apply bulk change with right-click to add the profile group INBOUND to those rules

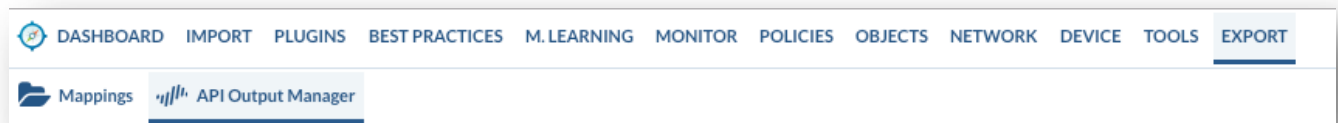


Step 6: Edit one of the rules to validate the Profile group has been attached.

End of Activity 5

Activity 6 – Export changes via API

Step 1: Navigate to EXPORT tab and click on API Output Manager

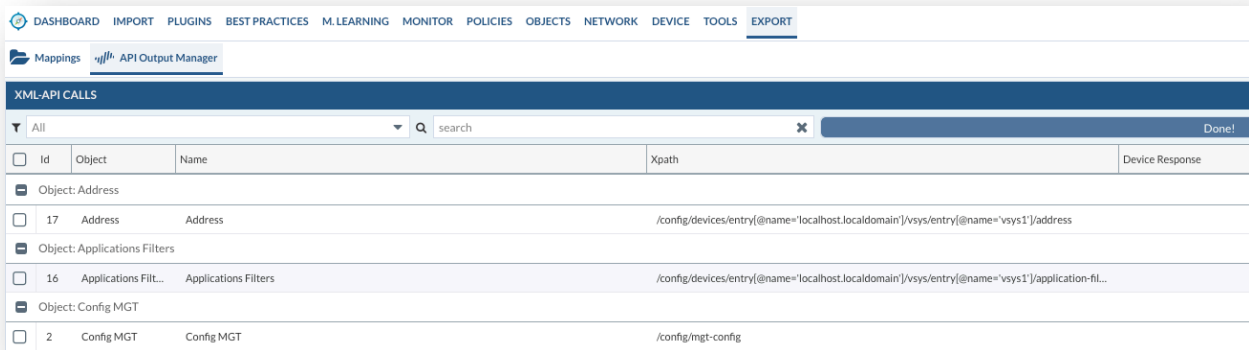


Step 2: Check the Atomic option is selected from the bottom bar

- Atomic Calls are API calls that contains in a single call the whole list of elements, example one API call will have all the address objects for a specific vsys
- SubAtomic: A single API call will contain a single object, so that means for the case of the address if you have 100 address you will get 100 API calls.

Step 3: Click on [Step 1] Generate API Requests

This will try to generate the XML output using your Base configuration plus the changes we made from the GUI, after that the API calls will be shown on the view



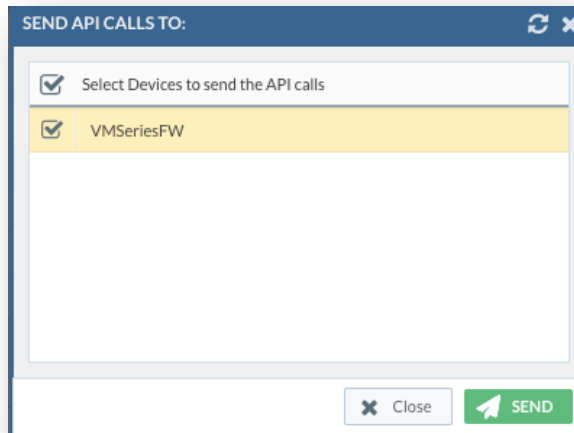
The Id tells you the order in case you want to be selective at the time to push the API calls back to your firewall, remember if we have address Groups we need to send first the Address because they can be members of the groups. So, the order on how you send the API calls matters. Expedition with the ID will in case you select some API calls it will send in the right order automatically.

If you don't select any API call but you press the [Step 2] Send API Request ALL the API calls will be sent in the right order.

Step 4: Don't select any Rule and click on the [Step 2] Send API Requests

Step 5: A new window will be shown, then you can select the devices where to push the API calls, in our Case only the VMSeriesFw will be shown

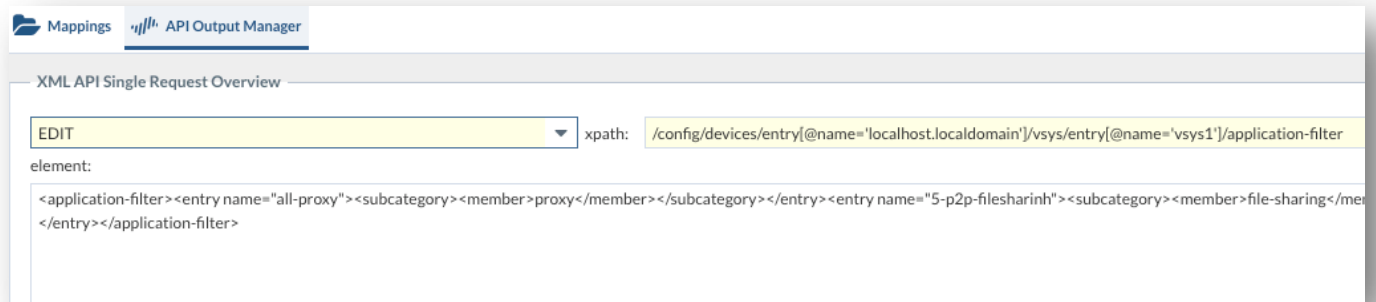
Step 6: Select the VMSeriesFW and click on SEND



Step 7: Review if all the API calls were successfully exported by reading the Device Response column.

XML-API CALLS					No pending Jobs	
Id	Object	Name	Xpath	Device	Response	
Object: Address						
17	Address	Address	/confg/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address	VMSeriesFW	command succeeded	
Object: Applications Filters						
16	Applications Filter	Applications Filters	/confg/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/application-filter	VMSeriesFW	command succeeded	
Object: Config MGT						
2	Config MGT	Config MGT	/confg/mgt-config	VMSeriesFW	command succeeded	
Object: DeviceConfig						
1	deviceconfig	DeviceConfig	/confg/devices/entry[@name='localhost.localdomain']/deviceconfig	VMSeriesFW	command succeeded	
Object: IKE Crypto Profiles						
7	IKE Crypto Profile	IKE Crypto Profiles	/confg/devices/entry[@name='localhost.localdomain']/network/ike/crypto-profiles/ike-crypto-profile	VMSeriesFW	command succeeded	
Object: IPSEC Crypto Profiles						
8	IPSEC Crypto Profile	IPSEC Crypto Profiles	/confg/devices/entry[@name='localhost.localdomain']/network/ike/crypto-profiles/ipsec-crypto-profile	VMSeriesFW	command succeeded	
Object: Interfaces Ethernet						
3	Interfaces Ethernet	Interfaces Ethernet Device	/confg/devices/entry[@name='localhost.localdomain']/network/interface/ethernet	VMSeriesFW	command succeeded	
Object: Management Profiles						
6	Management Profile	Management Profiles	/confg/devices/entry[@name='localhost.localdomain']/network/profiles/interface-management-profile	VMSeriesFW	command succeeded	
Object: Monitor Profiles						
5	Monitor Profiles	Monitor Profiles	/confg/devices/entry[@name='localhost.localdomain']/network/profiles/monitor-profile	VMSeriesFW	command succeeded	

Step 8: You can see the content of the API calls by double clicking on each one



Note: An API call is made by the Mode (EDIT, SET, DELETE, etc), the XPATH where to place the object and the element that contains the XML schema.

End of Activity 6