Expedition New Functionalities

11th November 2019

OVERVIEW

The Expedition Team has been working very hard to bring this new functionalities to our community. Under the spirit of continuously improve and enhance Expedition capabilities we added two new functions to help our customers to speed up App-ID adoption function and get a better visibility on the panos devices state.

GOALS

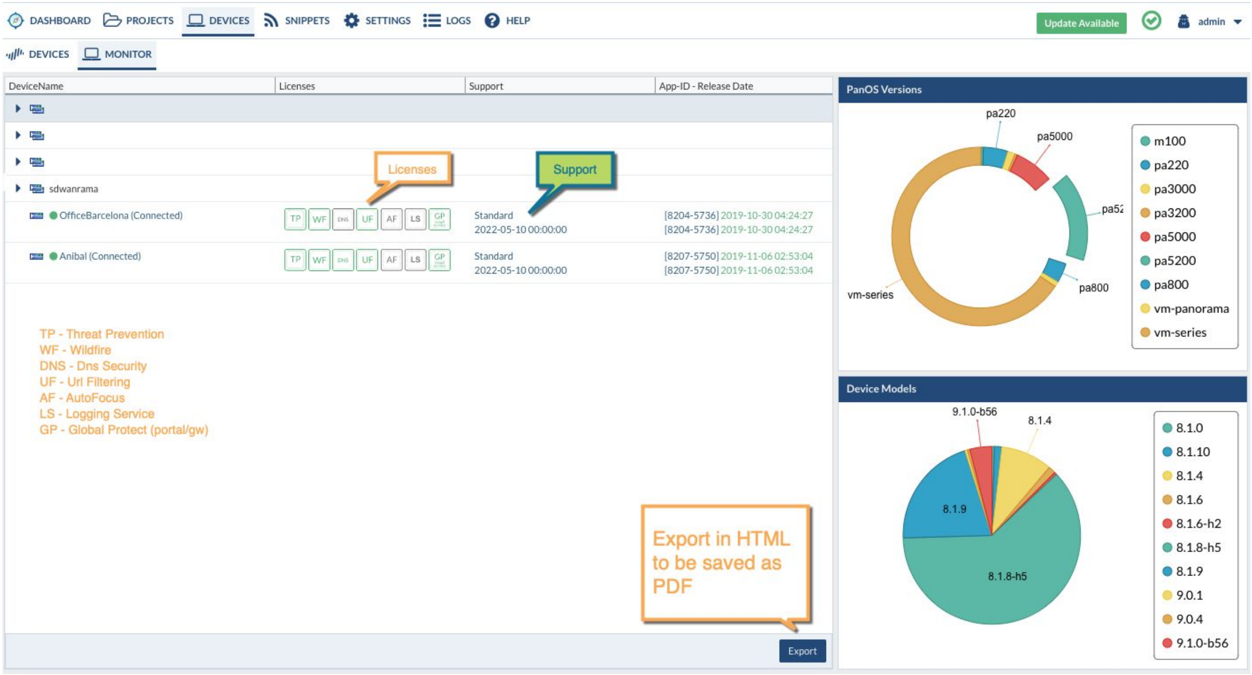
1. Log Connectors are used to generate filters who will be applied to API calls to generate reports based on applications seen in the logs for the selected security policies. If you have multiple device-groups in Panorama you have to switch in the log connector every time the device group you want to analyse. This task can be painful.
2. When you are managing Panorama with tons of firewalls you need visibility about, Panos versions deployed, licenses and check if Support is still valid or even check if the Apps and Threats are up to date or they are obsolete…

New Devices Monitor Tab

Where is located?

Once you login in Expedition you have to go to DEVICES, then after you add a Panorama/Firewall to Expedition and after retrieving the configuration click on MONITOR

Expedition New Functionalities



DeviceName	Licenses	Support	App-ID - Release Date
sdwanrama			
● OfficeBarcelona (Connected)	TP WF DNS UF AF LS GP	Standard 2022-05-10 00:00:00	[8204-5736] 2019-10-30 04:24:27 [8204-5736] 2019-10-30 04:24:27
● Anibal (Connected)	TP WF DNS UF AF LS GP	Standard 2022-05-10 00:00:00	[8207-5750] 2019-11-06 02:53:04 [8207-5750] 2019-11-06 02:53:04

TP - Threat Prevention
WF - Wildfire
DNS - Dns Security
UF - Url Filtering
AF - AutoFocus
LS - Logging Service
GP - Global Protect (portal/gw)

Export in HTML to be saved as PDF

What it does?

when we add a device in Expedition and we retrieve the configuration after adding the credentials or API key, Expedition downloads not just the configuration but runs a “show system info”, “request license info” and “request support check” on each device to generate this Dashboard.

The Dashboard shows the licenses are enabled and still valid, the ones expired and uses color from green to say is valid and red to say is expired.

The Dashboard shows the App-ID, Threat and AV content update and when was the last time it was installed. If more than 30 days it will show up in red too.

The Dashboard shows you the different versions of PanOS deployed across all the devices we have in Expedition and their hardware or virtualized platform too.

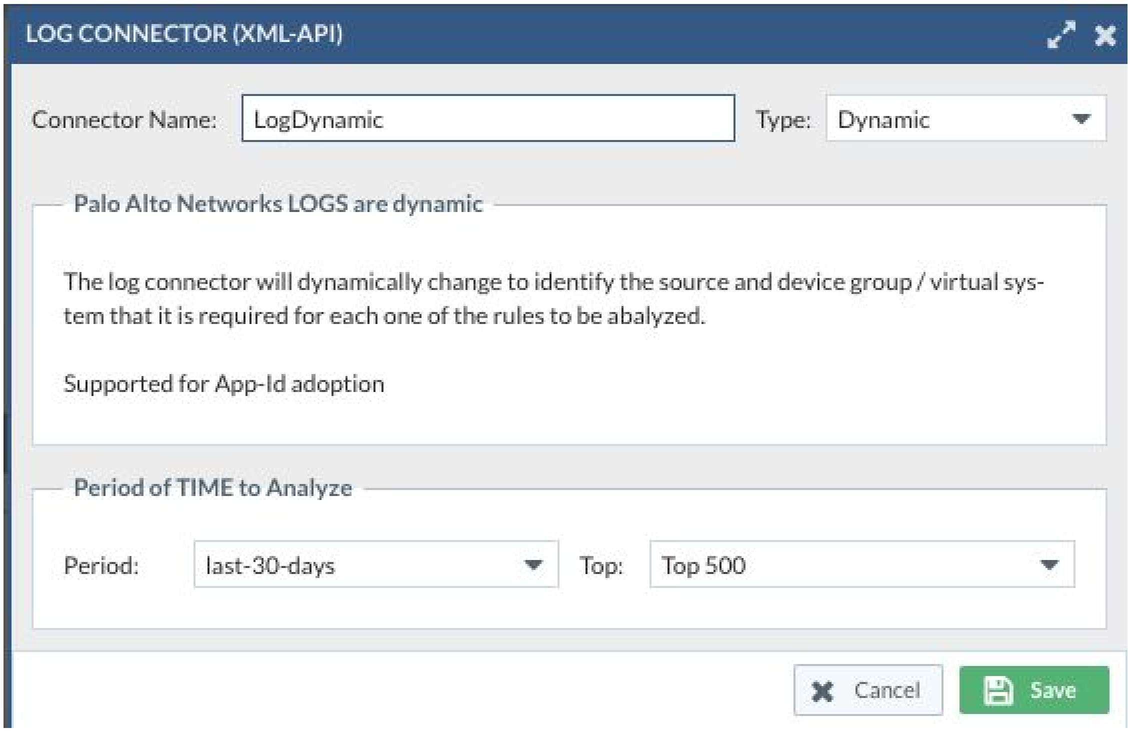
All this information can be exported to another page that will open an HTML web that can be used to print to PDF for instance.

Expedition New Functionalities

App-ID Adoption and DYNAMIC Log Connectors

Where is located?

Once you have created a project and imported your Panos device in it for run App-ID Adoption functions you have to go to PLUGINS. Click on the plus button to create a new Log Connector and select type Dynamic



LOG CONNECTOR (XML-API)

Connector Name: LogDynamic

Type: Dynamic

Palo Alto Networks LOGS are dynamic

The log connector will dynamically change to identify the source and device group / virtual system that it is required for each one of the rules to be abalyzed.

Supported for App-Id adoption

Period of TIME to Analyze

Period: last-30-days

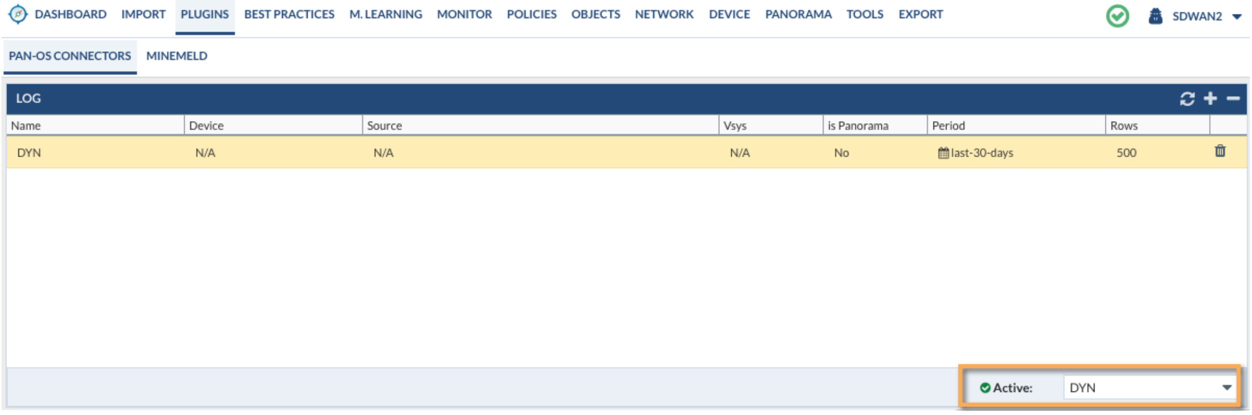
Top: Top 500

The only parameters we need to fill is the Period of time to analyse and the number of rows we want to retrieve. In this case we will generate reports for the last 30 days and we expect a max of 500 applications per rule.

What it does?

After we create the Dynamic Log Connector we have to apply it to the Project by selecting from the combo-box in the log connector's grid

Expedition New Functionalities



Name	Device	Source	Vsys	is Panorama	Period	Rows
DYN	N/A	N/A	N/A	No	last-30-days	500

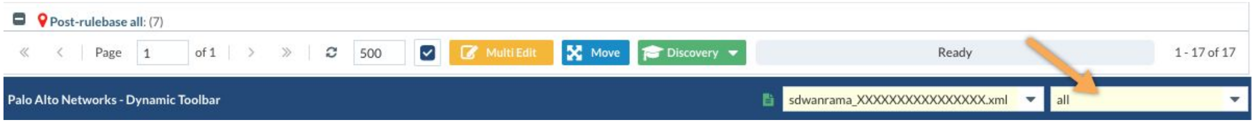
Active: DYN

What this will enable us to go to the Security Policies, select them all even if they are in different device-groups or virtual-systems and retrieve the Applications without having to go to the connector and change every time the Devicegroup/vsys because Expedition will calculate that from the backend by understanding each rule where is located and what is the right filter to generate. This Dynamic Log Connector will use all the serials associated to each Device-group when a rule is located in. If you want to be more selective and limit the analysis to only some serials inside the device-group you will have to use the Static Log Connector instead.

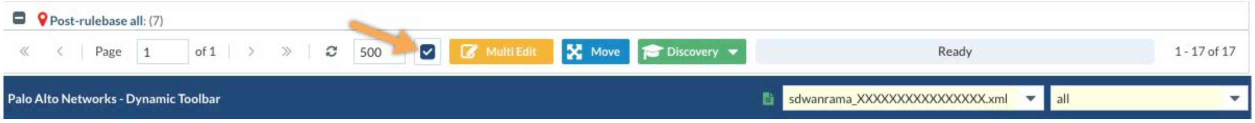
Let’s use it !

just to recap:

1) Create the Dynamic Log Connector
2) Apply it to the Project
3) Go to Security Policies and select the device-group/vsys “all”

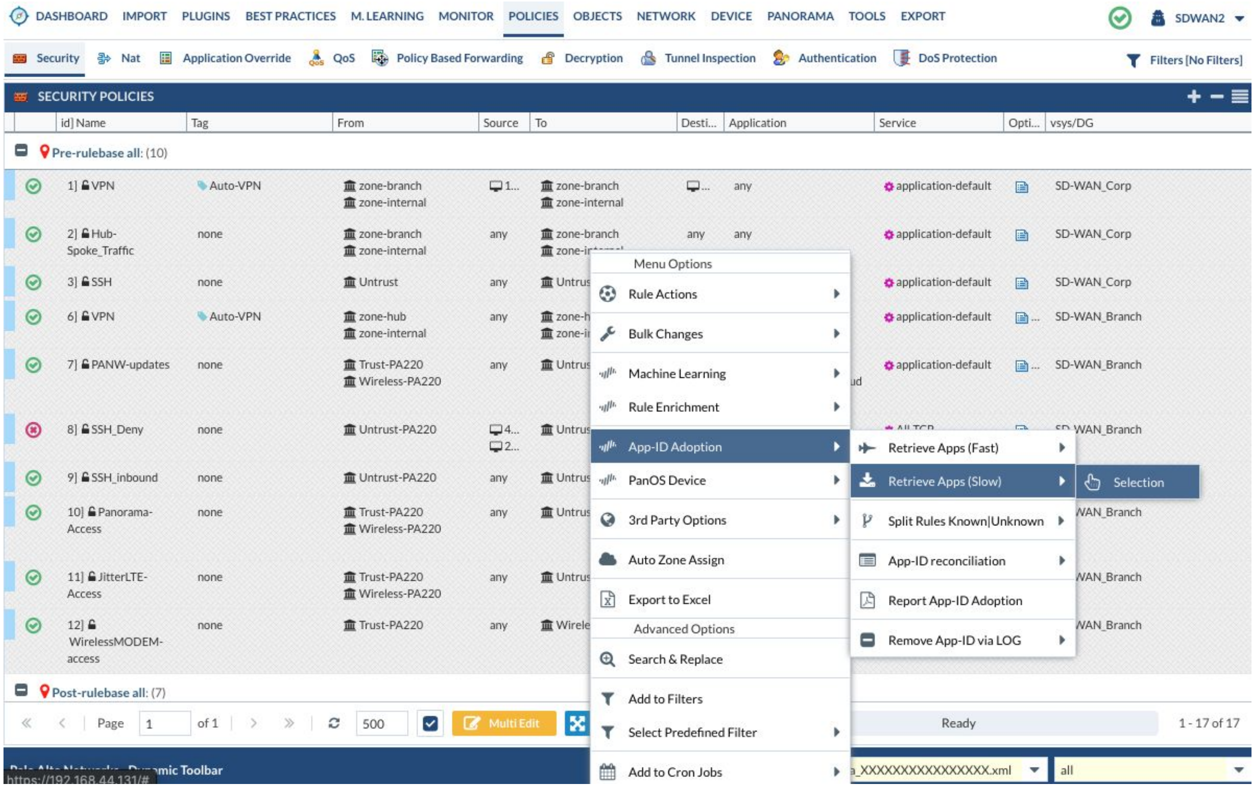


4) Click on the checkbox to Select ALL rules



Expedition New Functionalities

5) right-click on one of the rules and select App-ID Adoption -> Retrieve Apps (slow) -> Selection



Pre-rulebase all: (10)

id] Name	Tag	From	Source	To	Desti...	Application	Service	Opti...	vsys/DG
1] VPN	Auto-VPN	zone-branch zone-internal	1...	zone-branch zone-internal	...	any	application-default		SD-WAN_Corp
2] Hub-Spoke_Traffic	none	zone-branch zone-internal	any	zone-branch zone-i	any	any	application-default		SD-WAN_Corp
3] SSH	none	Untrust	any	Untrus			application-default		SD-WAN_Corp
6] VPN	Auto-VPN	zone-hub zone-internal	any	zone-h zone-i			application-default	...	SD-WAN_Branch
7] PANW-updates	none	Trust-PA220 Wireless-PA220	any	Untrus		ud	application-default	...	SD-WAN_Branch
8] SSH_Deny	none	Untrust-PA220	4... 2...	Untrus			All TCP		SD-WAN_Branch
9] SSH_inbound	none	Untrust-PA220	any	Untrus					
10] Panorama-Access	none	Trust-PA220 Wireless-PA220	any	Untrus					WAN_Branch
11] JitterLTE-Access	none	Trust-PA220 Wireless-PA220	any	Untrus					WAN_Branch
12] WirelessMODEM-access	none	Trust-PA220	any	Wirele					WAN_Branch

Post-rulebase all: (7)

Page 1 of 1 · 500

a_XXXXXXXXXXXXXXXX.xml · all

What is the difference between Retrieve Apps (Fast) and (Slow) modes?

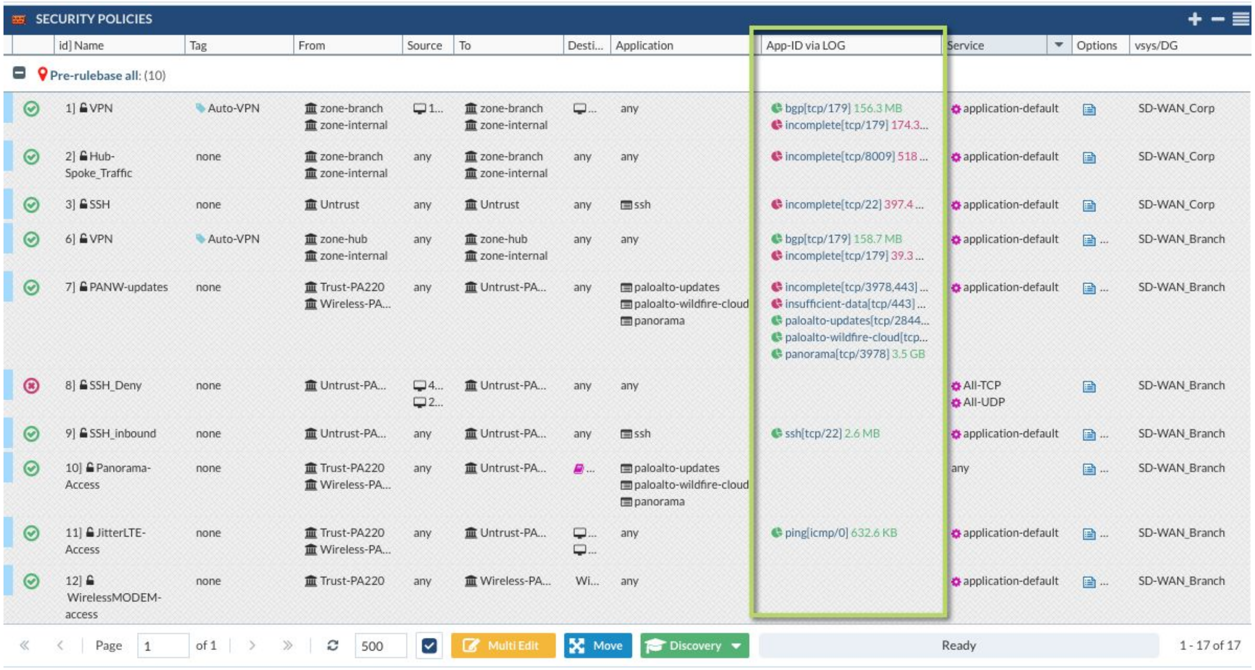
The main difference is the database we are tackling to generate the reports, in the case of the Fast we are going to ask to the summary database, this database is faster to answer because the information stored there is less rich, so when we use Fast we will not see the ports, protocol, bytes and packets used by application but the generation of the report will be very fast and stress less your PanOS device.

In case of generating the (Slow) report the data retrieved will be richer, so we will get the port, protocol, bytes and packets seen for each rule analysed. This report will take longer for the device to process since this information is based on each log and needs to be retrieved and grouped first.

What is the Outcome?

After the analysis ends you will see a new column named app-id via log showing the apps retrieved by Expedition.

Expedition New Functionalities



SECURITY POLICIES

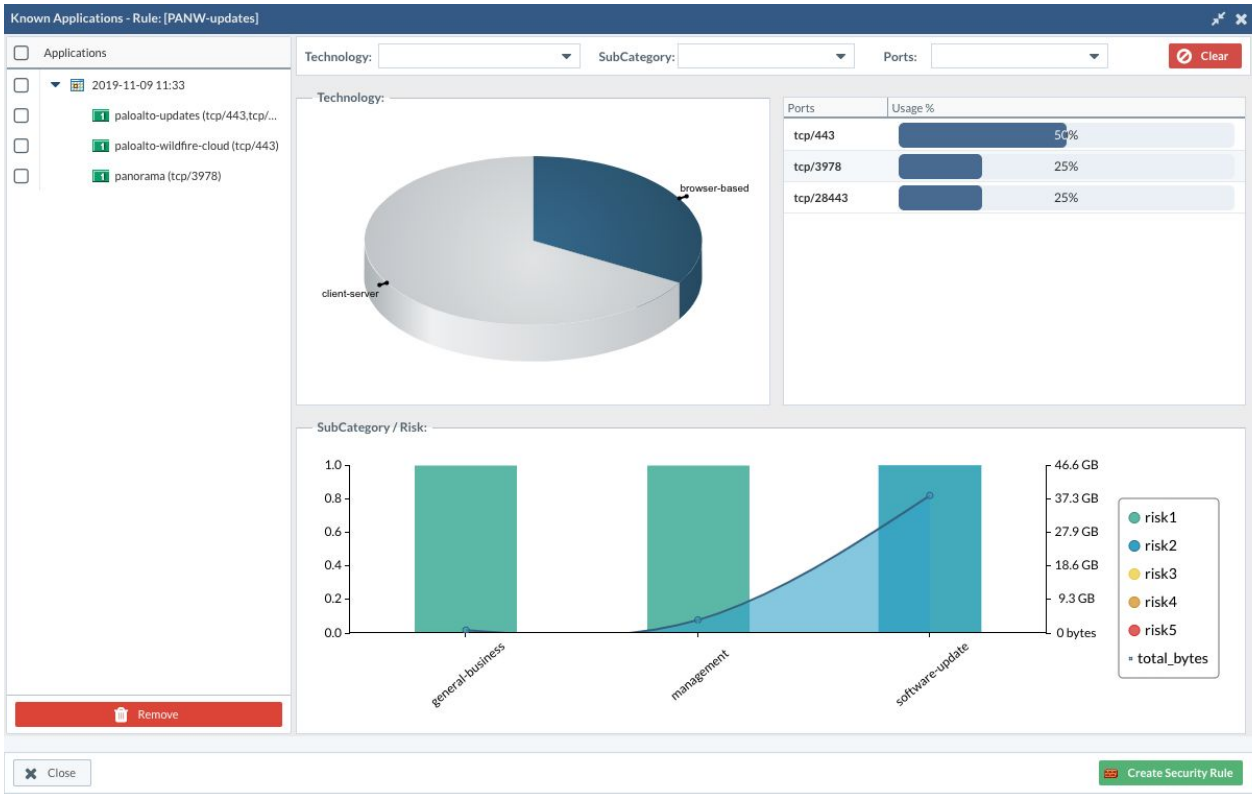
Pre-rulebase all: (10)

	id] Name	Tag	From	Source	To	Desti...	Application	App-ID via LOG	Service	Options	vsys/DG
✓	1] VPN	Auto-VPN	zone-branch zone-internal	1...	zone-branch zone-internal	...	any	bgp[tcp/179] 156.3 MB incomplete[tcp/179] 174.3...	application-default	🗎	SD-WAN_Corp
✓	2] Hub-Spoke_Traffic	none	zone-branch zone-internal	any	zone-branch zone-internal	any	any	incomplete[tcp/8009] 518 ...	application-default	🗎	SD-WAN_Corp
✓	3] SSH	none	Untrust	any	Untrust	any	ssh	incomplete[tcp/22] 397.4 ...	application-default	🗎	SD-WAN_Corp
✓	6] VPN	Auto-VPN	zone-hub zone-internal	any	zone-hub zone-internal	any	any	bgp[tcp/179] 158.7 MB incomplete[tcp/179] 39.3 ...	application-default	🗎 ...	SD-WAN_Branch
✓	7] PANW-updates	none	Trust-PA220 Wireless-PA...	any	Untrust-PA...	any	paloalto-updates paloalto-wildfire-cloud panorama	incomplete[tcp/3978,443] ... insufficient-data[tcp/443] ... paloalto-updates[tcp/2844... paloalto-wildfire-cloud[tcp... panorama[tcp/3978] 3.5 GB	application-default	🗎 ...	SD-WAN_Branch
✗	8] SSH_Deny	none	Untrust-PA...	4... 2...	Untrust-PA...	any	any		All-TCP All-UDP	🗎	SD-WAN_Branch
✓	9] SSH_inbound	none	Untrust-PA...	any	Untrust-PA...	any	ssh	ssh[tcp/22] 2.6 MB	application-default	🗎 ...	SD-WAN_Branch
✓	10] Panorama-Access	none	Trust-PA220 Wireless-PA...	any	Untrust-PA...	...	paloalto-updates paloalto-wildfire-cloud panorama		any	🗎 ...	SD-WAN_Branch
✓	11] JitterLTE-Access	none	Trust-PA220 Wireless-PA...	any	Untrust-PA...	... ...	any	ping[icmp/0] 632.6 KB	application-default	🗎 ...	SD-WAN_Branch
✓	12] WirelessMODEM-access	none	Trust-PA220	any	Wireless-PA...	Wi...	any		application-default	🗎 ...	SD-WAN_Branch

As you can see Expedition will tell you the applications found for each rule, marking in red if we seen incompletes, insufficient-data and unknowns and all the other apps in green.

If we want to focus on a specific rule just click in the new applications shown to go and do further analysis to decide if we want to import all the apps or we have to break the current rule in many others. Please follow the best practices to run App-ID adoption.

Expedition New Functionalities



- ☐ Applications
- ☐ 2019-11-09 11:33
  - ☐ paloalto-updates (tcp/443,tcp/...
  - ☐ paloalto-wildfire-cloud (tcp/443)
  - ☐ panorama (tcp/3978)

Ports	Usage %
tcp/443	50%
tcp/3978	25%
tcp/28443	25%

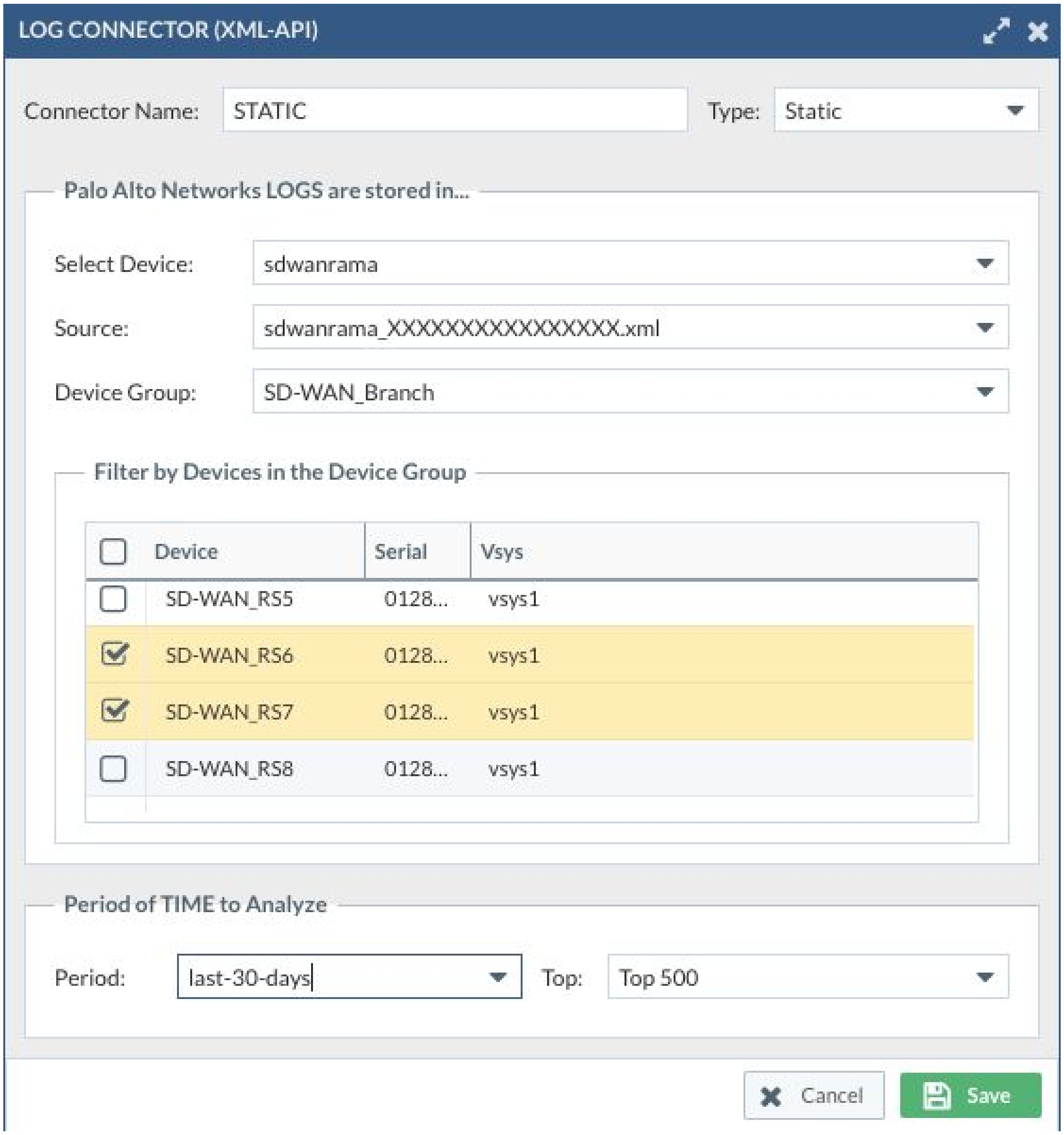
App-ID Adoption and STATIC Log Connectors

What is the difference with Dynamic?

Main difference is granularity. When a Dynamic Log Connector is configured Expedition calculates the configuration and the device-group/virtual-system based on each rule, which means in case of panorama and a device-group all the serials attached to it (or underneath in the DG hierarchie) will be used in the query to filter out the traffic from those serials to the security rule under analysis.

When Static is used you can select the configuration, the device where to ask and select only from which serials we want to filter. In case we want to always use all the serials associated to a device-group then is recommended to use Dynamic.

Expedition New Functionalities



LOG CONNECTOR (XML-API)

Connector Name: STATIC

Type: Static

Palo Alto Networks LOGS are stored in...

Select Device: sdwanrama

Source: sdwanrama_XXXXXXXXXXXXXXXX.xml

Device Group: SD-WAN_Branch

Filter by Devices in the Device Group

□	Device	Serial	Vsys
□	SD-WAN_RS5	0128...	vsys1
☑	SD-WAN_RS6	0128...	vsys1
☑	SD-WAN_RS7	0128...	vsys1
□	SD-WAN_RS8	0128...	vsys1

Period of TIME to Analyze

Period: last-30-days

Top: Top 500

Hope this functionality helps you to speed up the time to embrace App-ID and gives you another view in how healthy are your Devices or what licenses you should consider to enable in the future.