Overview

Legacy firewall rules are created around the Network (IPs) and Transport (Ports) layers of the Open Systems Interconnection (OSI) model. During a phased migration, legacy firewall rules are often converted to Palo Alto with like functionality to reduce downtime and ensure successful migration. Though one of the key strengths of Palo Alto firewalls is the ability to apply security rules at the Application layer (layer 7) via App-ID. Applications and application functions are identified by Palo Alto firewalls via multiple techniques, including application signatures (App-ID), decryption (if needed), protocol decoding, and heuristics.

The Scenario

You've successfully migrated to a Palo Alto firewall as part of your phased deployment. As part of the second phase of the migration you will leverage Palo Alto's Migration Tool to streamline rule cleanup and conversion to application rules. After the firewall has been inline for at least two weeks you should have enough log information to begin the conversion process.

Tools of the Trade

You will need to download Palo Alto's migration tool as well install VirtualBox or VMWare Workstation Player to run the migration tool.

- ✓ Palo Alto's Migration Tool
- ✓ VirtualBox
  or
- ✓ VMware Workstation Player

Target Device

Palo Alto Firewall(s)

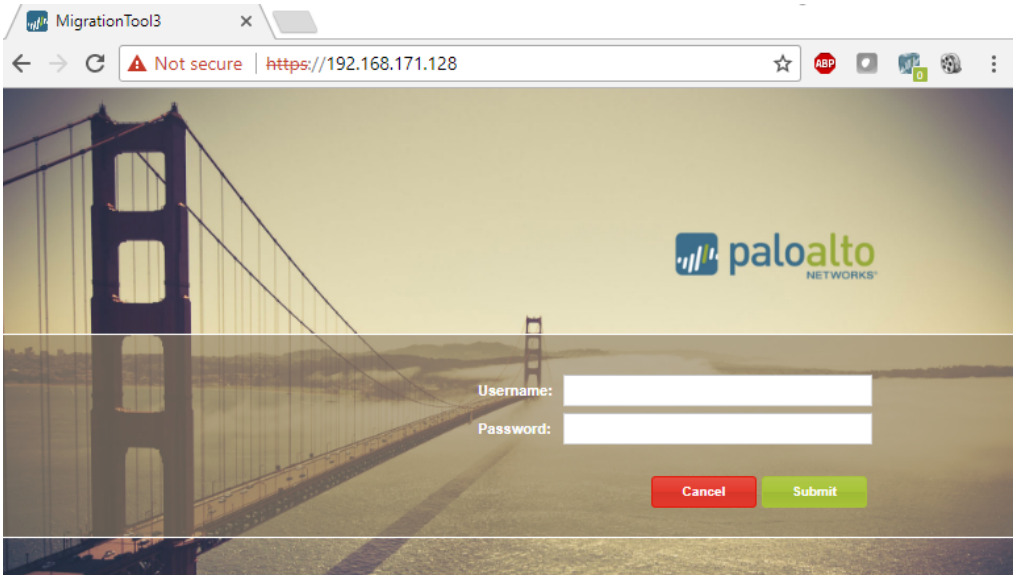
Getting Started

Once you have the migration tool running on your VM software of choice login, update, and connect your firewall.

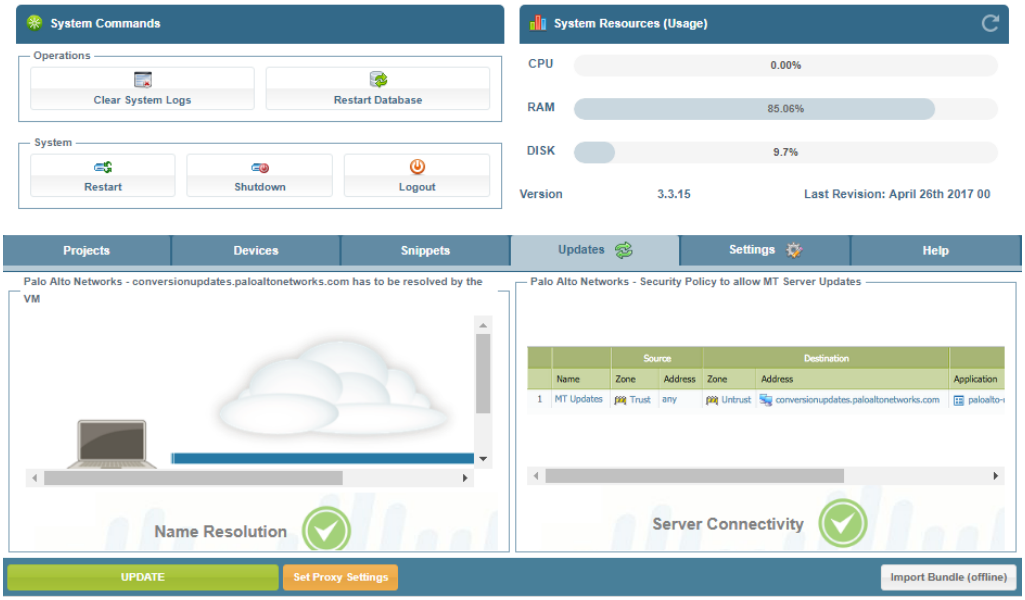
Migration Tool

1. Logging into the Migration Tool and Connect to your firewall

   The default credentials are:
   username: **admin**
   password: **paloalto**



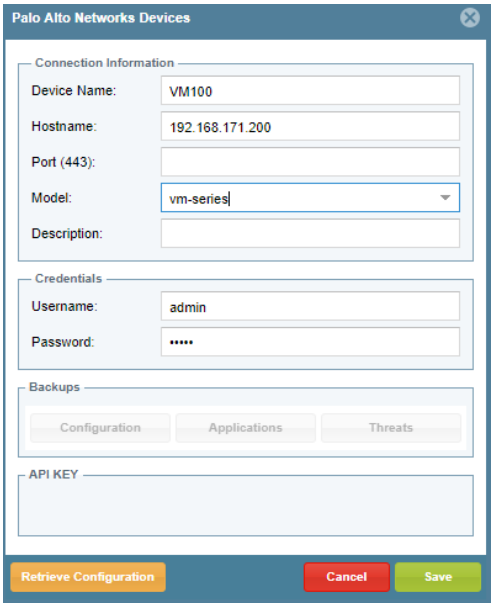
2. Check for the latest update to the migration tool by selecting the **'Updates'** tab and clicking the **'Update'** button in the lower left of the GUI.

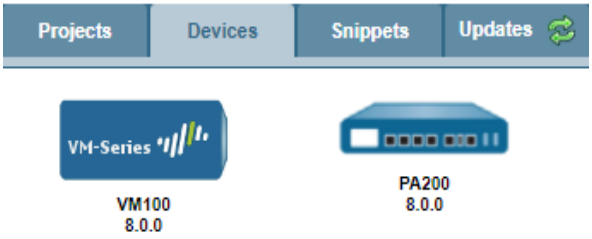


Add the Firewall

1. Connect to your firewall by clicking on the **'Devices'** Tab
2. Click **'Add'** and populate the device information and click **'Save'**.

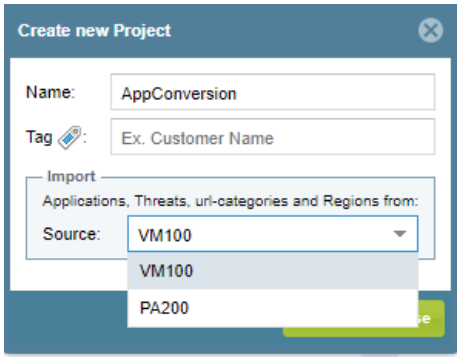
If credentials to the firewall and connectivity are successfully you will now see **'Device Added Successfully'** and the device in the list of firewalls.

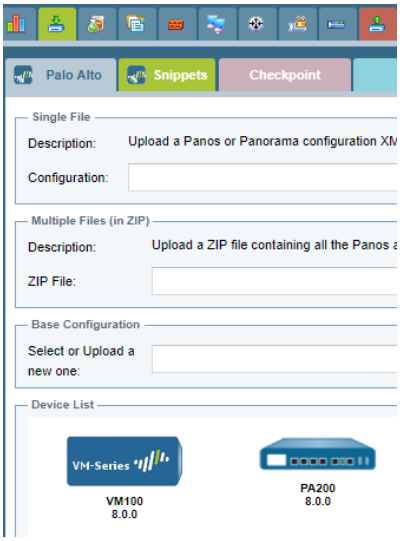




Create a Project

1. Click the **'Projects'** Tab, in the lower left corner click the **'Add New Project'**
2. Select the firewall you recently added from the source drop down to import its Applications, Threats, URL Categories, and Regions for use. *Note: Ensure your firewall has the latest App and Threat content.*
3. Once inside the project double-click the firewall to retrieve the configuration



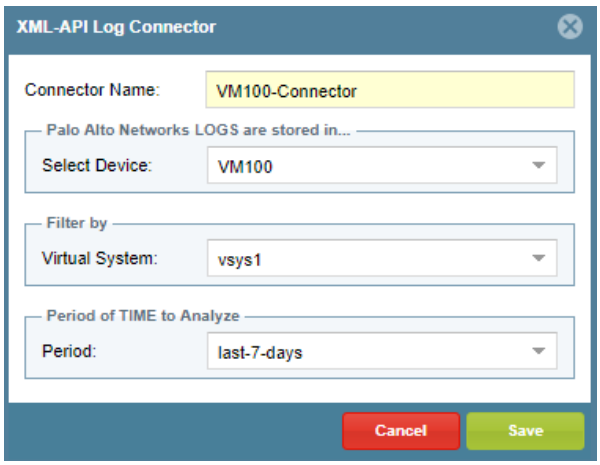


Add a Log Connector

The Migration Tool will use the Log Connector to retrieve your firewall's log repository to correlate traffic logs with current service rules for application matching. It is best practice to have at least two weeks of logs but this can vary based on the model of firewall and traffic.

1. Click on the chemistry beakers icon:

2. In the LOG connector Profile, click the **'Add Connector'** button and populate the XML-API Log Connector data. For our lab we are going back 7 days but this can vary depending on your device and its storage capacity.
3. Click **'Save'**
4. You will now see your connector under the Log Connector Profile.



Clone Rules and Match App-ID

Create a Snapshot before you start in the event you'd like to revert back in your progress.

1. Click on the **'Save'** icon (), at the bottom of the migration tool
2. Click **'save name configuration snapshot'**, name it (ex: 'version1').

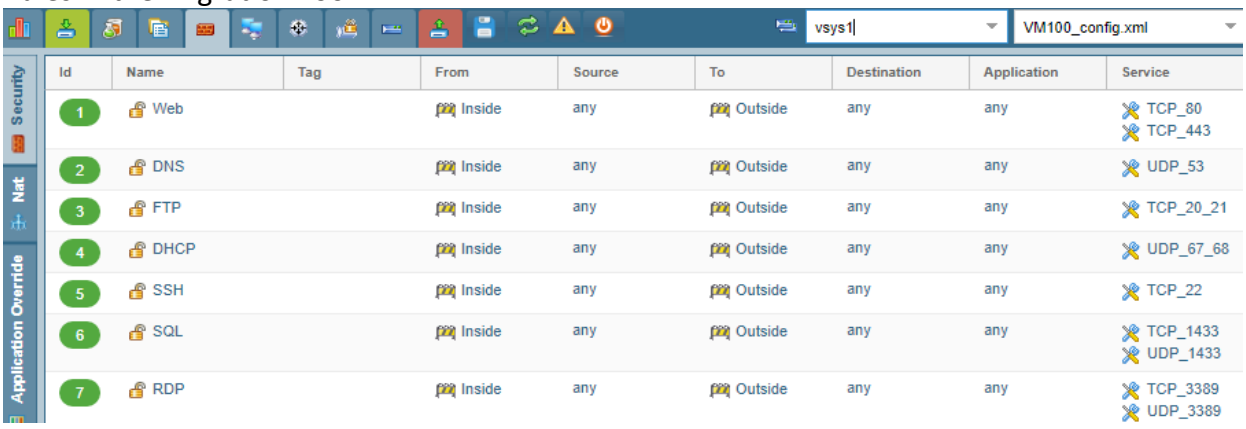
Note: In the event during your conversion you'd need to revert back. Click the same icon and choice **'load name configuration snapshot' and** select the named version you'd like to revert to.

As a best practice to reduce disruptions to production traffic, and for quick reference we will be cloning the existing legacy rules before utilizing the migration application feature. In the event the newly created application rule does not hit the top rule you'll still have the original below it. For reference, below is a screenshot of our rules on our test firewall and how they'll appear in the migration tool.

Rules on the Firewall

				Source				Destination						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
1	Web	none	universal	Inside	any	any	any	Outside	any	any	TCP_80 TCP_44	Allow		
2	DNS	none	universal	Inside	any	any	any	Outside	any	any	UDP_53	Allow		
3	FTP	none	universal	Inside	any	any	any	Outside	any	any	TCP_20_21	Allow		
4	DHCP	none	universal	Inside	any	any	any	Outside	any	any	UDP_67_68	Allow		
5	SSH	none	universal	Inside	any	any	any	Outside	any	any	TCP_22	Allow		
6	SQL	none	universal	Inside	any	any	any	Outside	any	any	TCP_1433 UDP_1433	Allow		
7	RDP	none	universal	Inside	any	any	any	Outside	any	any	TCP_3389 UDP_3389	Allow		
8	intrazon...	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
9	interzon...	none	interzone	any	any	any	any	any	any	any	any	Deny	none	

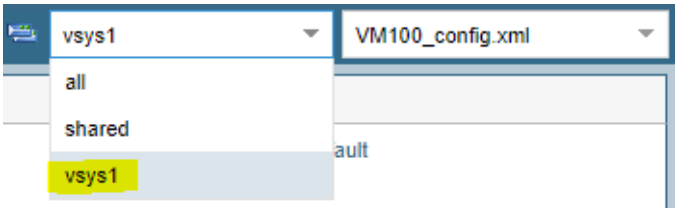
Rules in the Migration Tool



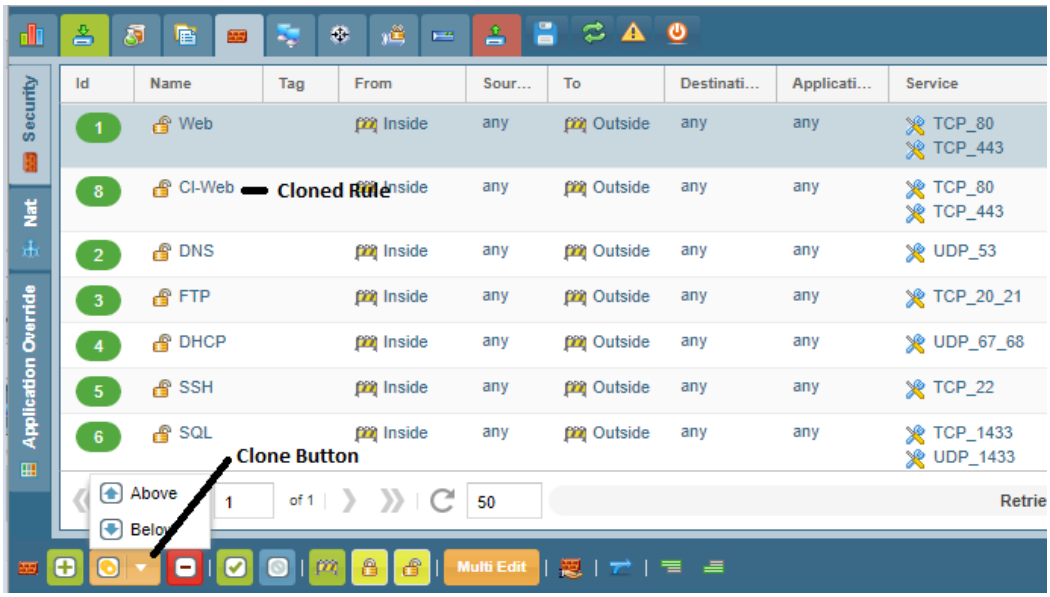
Id	Name	Tag	From	Source	To	Destination	Application	Service
1	Web		Inside	any	Outside	any	any	TCP_80 TCP_443
2	DNS		Inside	any	Outside	any	any	UDP_53
3	FTP		Inside	any	Outside	any	any	TCP_20_21
4	DHCP		Inside	any	Outside	any	any	UDP_67_68
5	SSH		Inside	any	Outside	any	any	TCP_22
6	SQL		Inside	any	Outside	any	any	TCP_1433 UDP_1433
7	RDP		Inside	any	Outside	any	any	TCP_3389 UDP_3389

Clone Rules

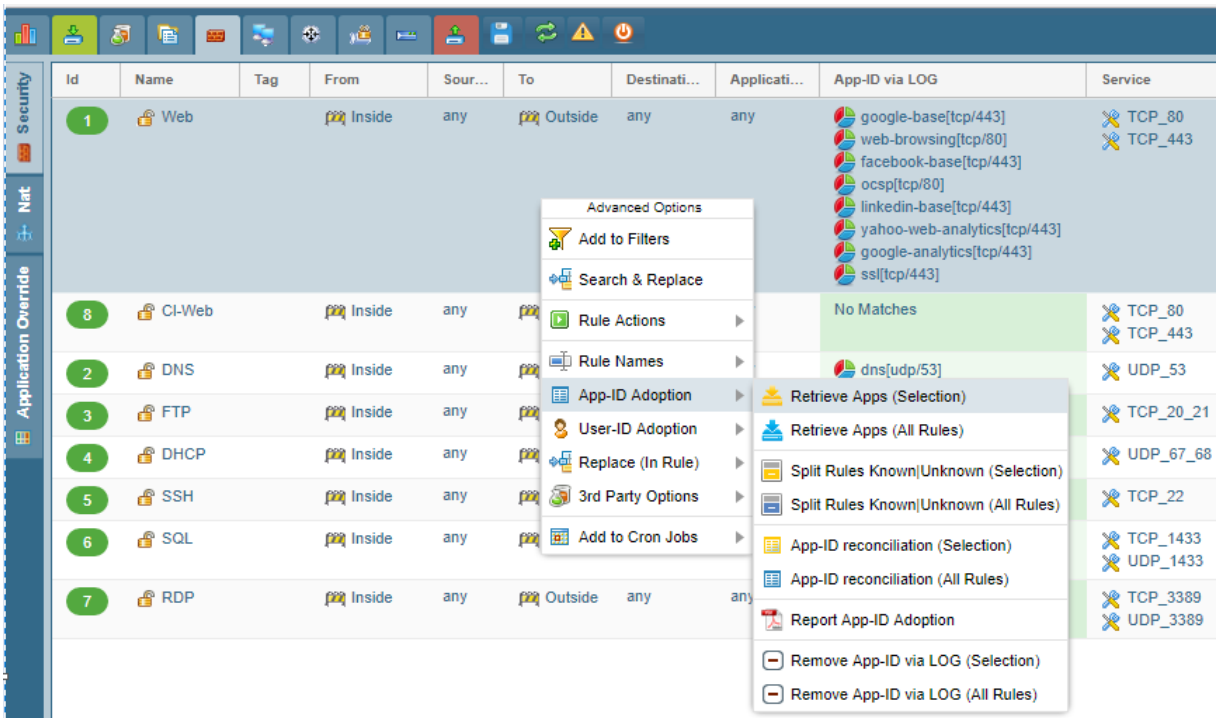
1. From the **'Manage Policy'** tab ( ) ensure you select the vsys (vsys1 in our example) you are working on in the upper right drop down.



2. Select the rule and use the lower left **'orange button'** drop down to clone the rule below the rule you will be modifying. The new cloned rule will have a 'CL' abbreviation in front of it.



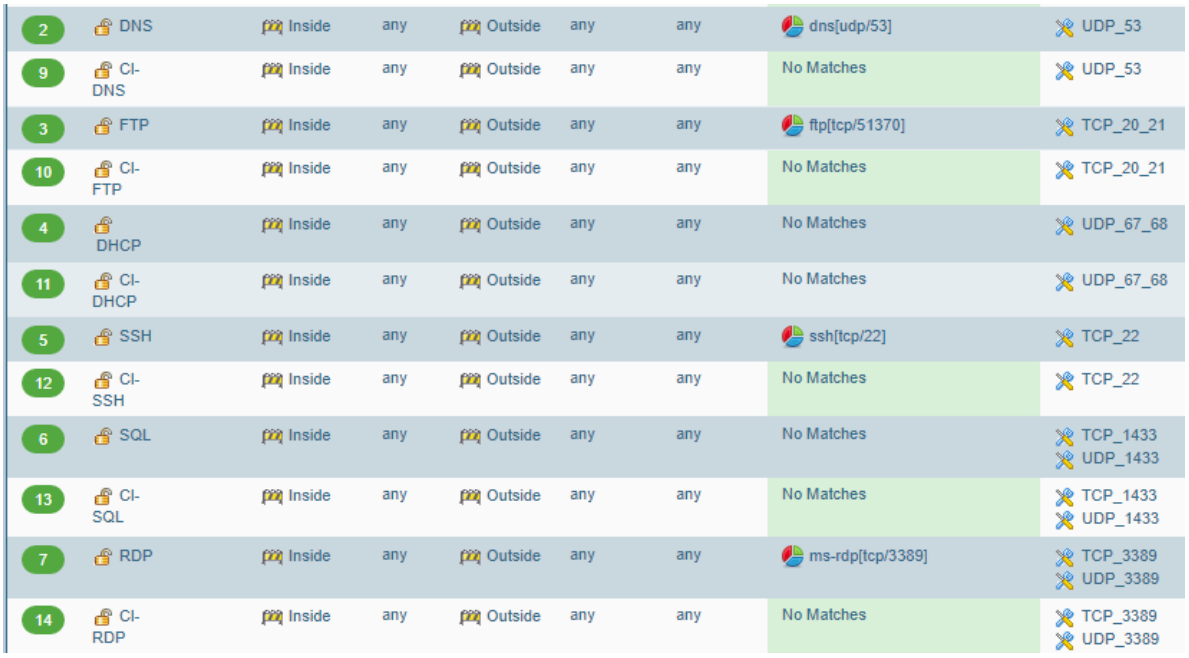
3. Right click the original rule (in the example 'Web'), select **'App-ID Adoption'>'Retrieve Apps (Selection)**. The result for our rule indicate that applications web-browsing, ssl, and ocsp. Additionally, more specific applications based on destination site identifying google, facebook, linkedin, and yahoo can replace the current service based rule.



Rule with syslog applications associated and the cloned rule below it.

Note: Though you can retrieve all Rules matches at once. It is recommend to start with one rule to get familiar with the process. The time to retrieve the logs may vary given the model of firewall you are working with.

4. Repeat this process for each rule. To expedite the process, select multiple rules**, 'clone below'**, and **'match application-ID'**. It is best to keep to 10-20 rules at a time in other to keep accurate track of what is being migrated.



2	DNS	Inside	any	Outside	any	any	dns[udp/53]	UDP_53
9	CI-DNS	Inside	any	Outside	any	any	No Matches	UDP_53
3	FTP	Inside	any	Outside	any	any	ftp[tcp/51370]	TCP_20_21
10	CI-FTP	Inside	any	Outside	any	any	No Matches	TCP_20_21
4	DHCP	Inside	any	Outside	any	any	No Matches	UDP_67_68
11	CI-DHCP	Inside	any	Outside	any	any	No Matches	UDP_67_68
5	SSH	Inside	any	Outside	any	any	ssh[tcp/22]	TCP_22
12	CI-SSH	Inside	any	Outside	any	any	No Matches	TCP_22
6	SQL	Inside	any	Outside	any	any	No Matches	TCP_1433 UDP_1433
13	CI-SQL	Inside	any	Outside	any	any	No Matches	TCP_1433 UDP_1433
7	RDP	Inside	any	Outside	any	any	ms-rdp[tcp/3389]	TCP_3389 UDP_3389
14	CI-RDP	Inside	any	Outside	any	any	No Matches	TCP_3389 UDP_3389

Non-Standard Ports

Notice in the above screenshot that ftp is running on tcp/51370 so in order for that rule to work we'd need to ensure that the service is set to 'Any' as to 'Application-Default' since the default would only allow ftp via tcp/21.

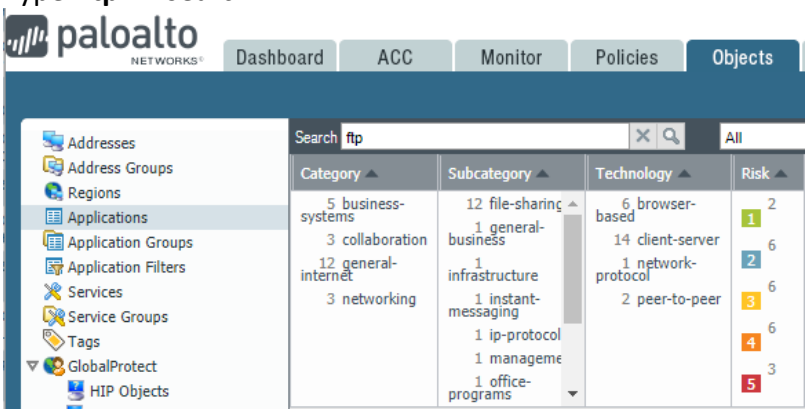
If the application identified is using the standard port for the application the migration tool identified from the syslogs it will change the service to 'Application-Default', if not it will change the service to 'Any'.

Any - This simply means all ports: 1-65535, TCP or UDP. The selected applications are allowed or denied on any protocol or port.

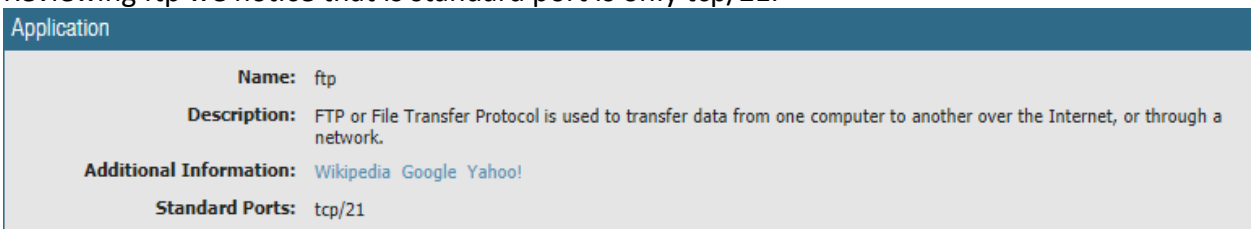
Application-Default - Choosing this means that the selected applications are allowed or denied only on their default ports defined by Palo Alto Networks. This option is recommended for allow policies because it prevents applications from running on unusual ports and protocols, which if not intentional, can be a sign of undesired application behavior and usage.

You can review what default port(s) Palo Alto assigns to an application from the firewall or Applipedia

1. Under the **'Object'>'Applications'** section.
2. Type **'ftp'** in search.



3. Reviewing ftp we notice that is standard port is only tcp/21.



Use the firewall and Palo Alto's Applipedia as reference for applications you are creating application rules for to verify expected rule enforcement behavior and to make accommodations if your environment runs an application on a non-standard port.

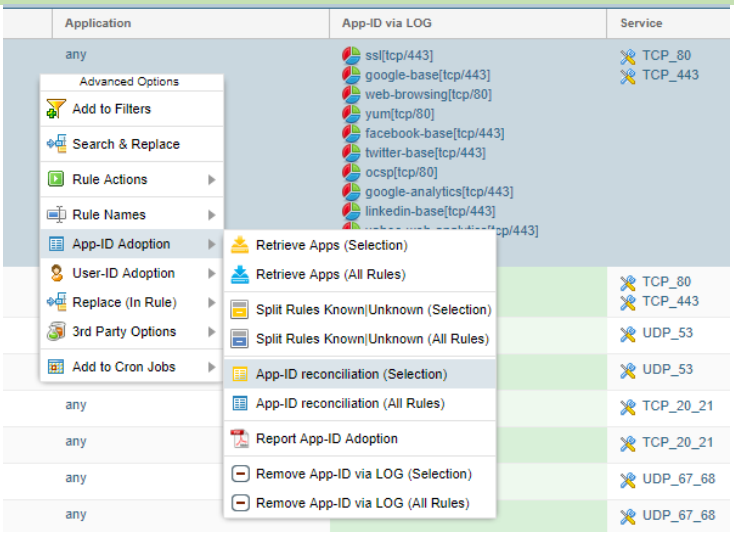
Palo Alto customers receive new content via Dynamic Updates which contains updates to App-ID from vendors that may have updated their application since release. Palo Alto firewall uses these updates to better identify and enforce application rules. Palo Alto sends notifications to it's customers before they deploy a new Application and Threat Content Release indicating what will change in each new version release for review. It is best practice to ensure you are using the latest application and threat versions.

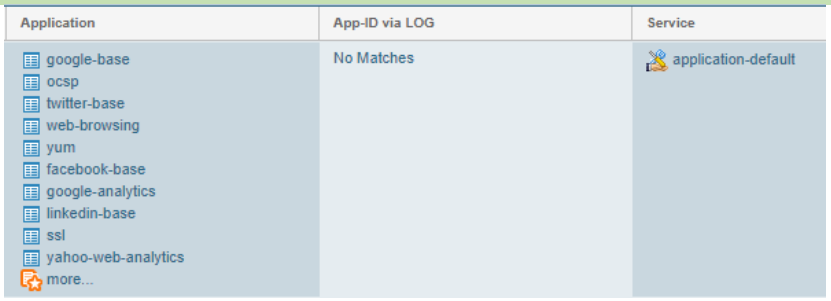
Reconcile Applications from Logs

Once you've had a chance to review the applications the migration tool has identified from the log connector you'll want to reconcile the application from the log. This process adds the identified application to the rule and modifies the service to 'application-default' or 'any' based on port(s) used.

1. Right click the rule to modify and selected **'App-ID reconciliation (Selection)'**. Though you can do all rules the better approach is to start with 10-20 rules at a time to keep track of changes occurring to your ruleset.

Rule Before Reconciliation	Rule After Reconciliation – Notice the App and Service Changes





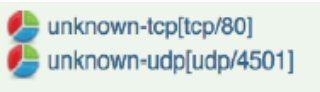
2. Once reconciliation is complete verify the rule(s) and service(s).

Application Anomalies

There may be times Palo Alto identifies an application as unknown which will then need to have a custom application or application override made for the traffic. Though creating customs applications is out of scope of this lab the follow guidance could assist during your migration.

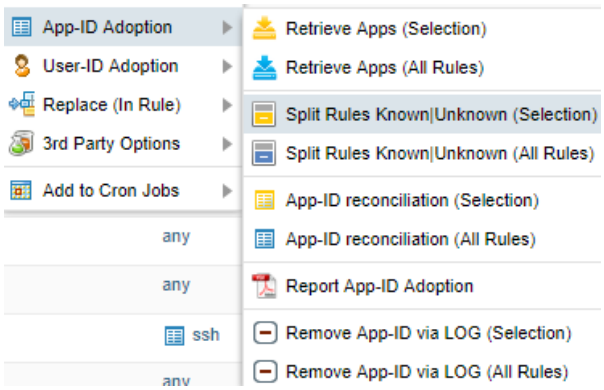
Unknown Applications

When the migration tool identifies an application as unknown, example:



The follow actions should be followed:

1. Attempt to identify the traffic and create a custom app for the traffic. Creating Custom Applications
2. If making a custom application isn't possible migrate the split unknown app rule.
   - Right click rule
   - **'App-ID Adoption'>'Split Rules Known/Unknown(Selection)**
   - Place the rule after order the application migrated rule but before the clone rule.



No Matches for Applications

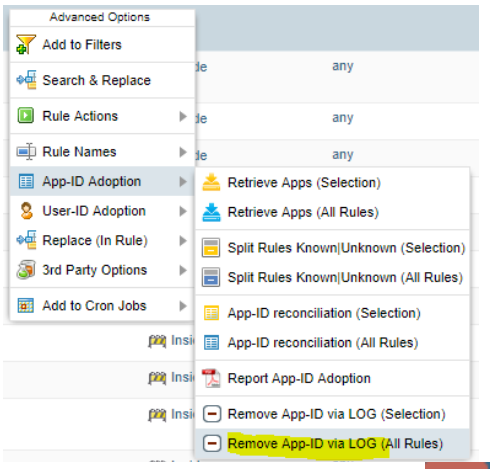
When the migration tool returns 'No Match' for a rule consider the follow:

1. That the rule is not being hit. Rule hits can quickly be seen by using the 'Highlight Unused Rules' check box on the firewall.
2. Run a report again on the firewall itself to make sure that rule has no hits.
3. Consider disabling the rule as a first step then remove the rule.

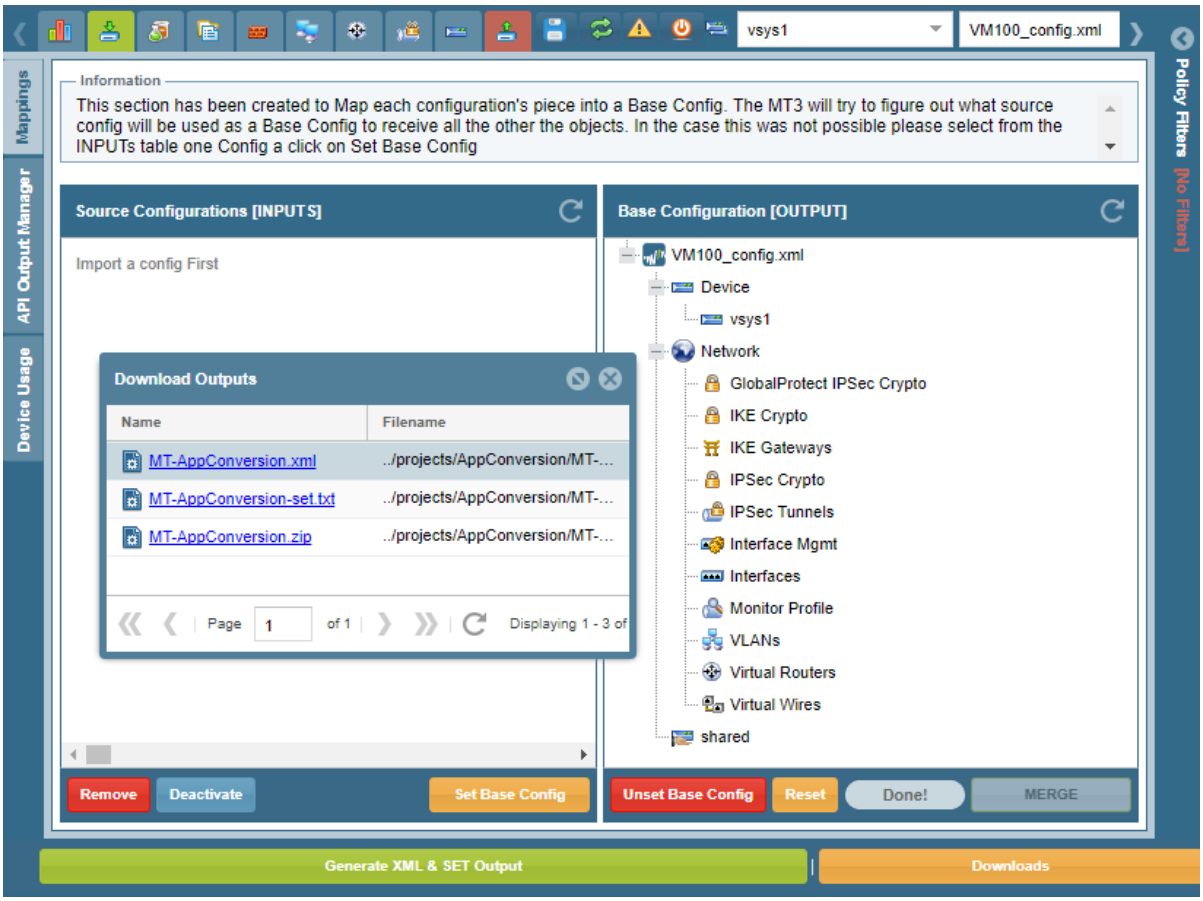
Uploading the App Config

Once you've worked through all rules it is time to upload the new configuration to the firewall.

1. Remove App-ID via syslog by right clicking rule**>App-ID Adoption>'Remove App-ID via Log'**



2. Click on the output icon ( ) in the migration tool.
3. Click the **'Generate XML & SET Output'** button at the bottom left which will bring up the modified config for use in the window **'Download Outputs'.**



4. Click and Download the XML file (MT-AppConversion.xml in our example)

Import it into the firewall

1. **Device>Setup>Operations>'Import named configuration snapshot'**
2. Load the configuration into the firewall. **Device>Setup>Operations> 'Load named configuration snapshot'**
3. Clean / Remove the clone rules "Deny" or "Drop" that you no longer need
4. Re-organize any Unknown Rules that you created after the APP-ID rules you've created but before the Clone Rule.
5. Review and verify your final configuration prior to commit.

Before App-ID Adoption

	Name	Tags	Type	Source				Destination		Application	Service	Action	Profile	Options
				Zone	Address	User	HIP Profile	Zone	Address					
1	Web	none	universal	Inside	any	any	any	Outside	any	any	TCP_80 TCP_44	Allow		
2	DNS	none	universal	Inside	any	any	any	Outside	any	any	UDP_53	Allow		
3	FTP	none	universal	Inside	any	any	any	Outside	any	any	TCP_20_21	Allow		
4	DHCP	none	universal	Inside	any	any	any	Outside	any	any	UDP_67_68	Allow		
5	SSH	none	universal	Inside	any	any	any	Outside	any	any	TCP_22	Allow		
6	SQL	none	universal	Inside	any	any	any	Outside	any	any	TCP_1433 UDP_1433	Allow		
7	RDP	none	universal	Inside	any	any	any	Outside	any	any	TCP_3389 UDP_3389	Allow		
8	intrazon...	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
9	interzon...	none	interzone	any	any	any	any	any	any	any	any	Deny	none	

After with cleanup and App-ID Adoption

	Name	Tags	Type	Source				Destination		Application	Service	Action	Profile	Options
				Zone	Address	User	HIP Profile	Zone	Address					
1	Web	Appid Adoption	universal	Inside	any	any	any	Outside	any	facebook-base google-analytics google-base linkedin-base ocsp ssl twitter-base more...	application-default	Allow		
2	DNS	Appid Adoption	universal	Inside	any	any	any	Outside	any	dns	application-default	Allow		
3	FTP	Appid Adoption	universal	Inside	any	any	any	Outside	any	ftp	application-default	Allow		
4	SSH	Appid Adoption	universal	Inside	any	any	any	Outside	any	ssh	application-default	Allow		
5	AppidRDP	Appid Adoption	universal	Inside	any	any	any	Outside	any	ms-rdp	application-default	Allow		
6	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
7	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	

Conclusion

Once all rules have been migrated from legacy rules to application rules you will want to assure that traffic passing through the firewall will not be able to evade your security policy. Review the Best Practice for Securing Your Network from Layer 4 and Layer 7 Evasion admin guide and verify additional DNS Proxy Object, Evasion Signatures, File Blocking and Zone Protection profiles are configured to ensure application policy is always enforced.

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 newly released 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, PSE-P, Sr. Network Security Engineer

Last Modified: Jan 3, 2018

Resource Links

Palo Alto's Migration Tool
https://live.paloaltonetworks.com/t5/Migration-Tool-Articles/Download-the-Migration-Tool/ta-p/56582

VirtualBox
https://www.virtualbox.org/wiki/Downloads

VMware Workstation Player
https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0

Creating Custom Applications:
https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Custom-applications-and-app-override/ta-p/71635

Palo Alto Networks Best Practice
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/best-practices-for-securing-your-network-from-layer-4-and-layer-7-evasions