Overview

Sun Management is a Palo Alto Networks Partner, Palo Alto Networks Certified Services Partner, and Palo Alto Networks Authorized Training Center. Our Engineers have designed and installed over $100M in Palo Alto Firewall Security since 2009. As a Palo Alto Networks Authorized Training Center we have trained over 2000 students on effective utilization of the Palo Alto Networks Firewall. As such, we aim to provide continuous access to on going training for out existing clients, potential clients and any other individual interested in further develop of their engineering skills with Palo Alto Networks Firewalls.

Legacy firewall rules control traffic using the port and protocol, in addition to source and destinations but provide no visibility into the Layer 7 applications that are crossing the firewall. During a phased migration, legacy firewall rules are often converted to Palo Alto Firewalls 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. This increased level of granular visibility will reduce the burden on your SOC (Security Operations Center), decrease your attack surface, and generate better results around Penetration Testing. Success implementation of App-ID rules will provide increased PCI and/or GDRP compliance.

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 Policy Optimizer to safely migrate from port-based rules to app-based rules. This second phase can be started as soon as two weeks after the firewall is in use.

The Tools of the Trade

Policy Optimizer a feature of PAN-OS, first introduced in version 9.0 and since then refined in successive releases. Policy Optimizer provides a simple workflow to migrate your legacy port-based Security policy rulebase to an App-ID based rulebase, which improves your security. Security is improved by reducing the attack surface and gaining visibility into applications. Policy Optimizer identifies port-based rules so you can convert them to application-based allow rules or add applications from a port-based rule to an existing application-based rule without compromising application availability.

Target Device

Palo Alto Firewall

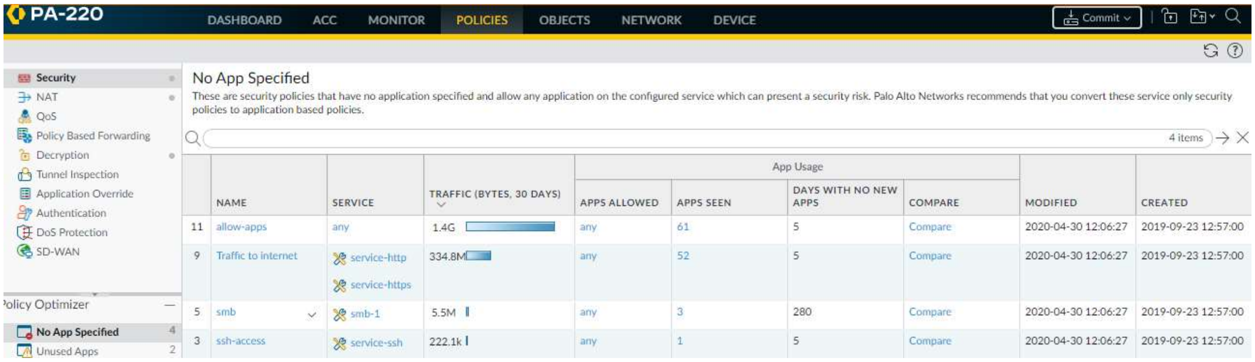
GETTING STARTED

Once you have your firewall in place and have run with port-based rules for a few weeks or more, you are ready to get started.

MIGRATION WORKFLOW

Step 1: Identify port-based rules.

Port-based rules have no configured applications. On the firewall, go to **Policies > Security > Policy Optimizer > No App Specified** to display all port-based rules.



No App Specified

These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks recommends that you convert these service only security policies to application based policies.

				App Usage					
	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE	MODIFIED	CREATED
11	allow-apps	any	1.4G	any	61	5	Compare	2020-04-30 12:06:27	2019-09-23 12:57:00
9	Traffic to internet	service-http service-https	334.8M	any	52	5	Compare	2020-04-30 12:06:27	2019-09-23 12:57:00
5	smb	smb-1	5.5M	any	3	280	Compare	2020-04-30 12:06:27	2019-09-23 12:57:00
3	ssh-access	service-ssh	222.1k	any	1	5	Compare	2020-04-30 12:06:27	2019-09-23 12:57:00

Step 2: Choose what rules to convert to App-Based first.

Once you are in **Policies > Security > Policy Optimizer > No App Specified** you can sort rules in different ways to help prioritize what rules to convert first. There a number of ways depending on your goals and risk tolerance.

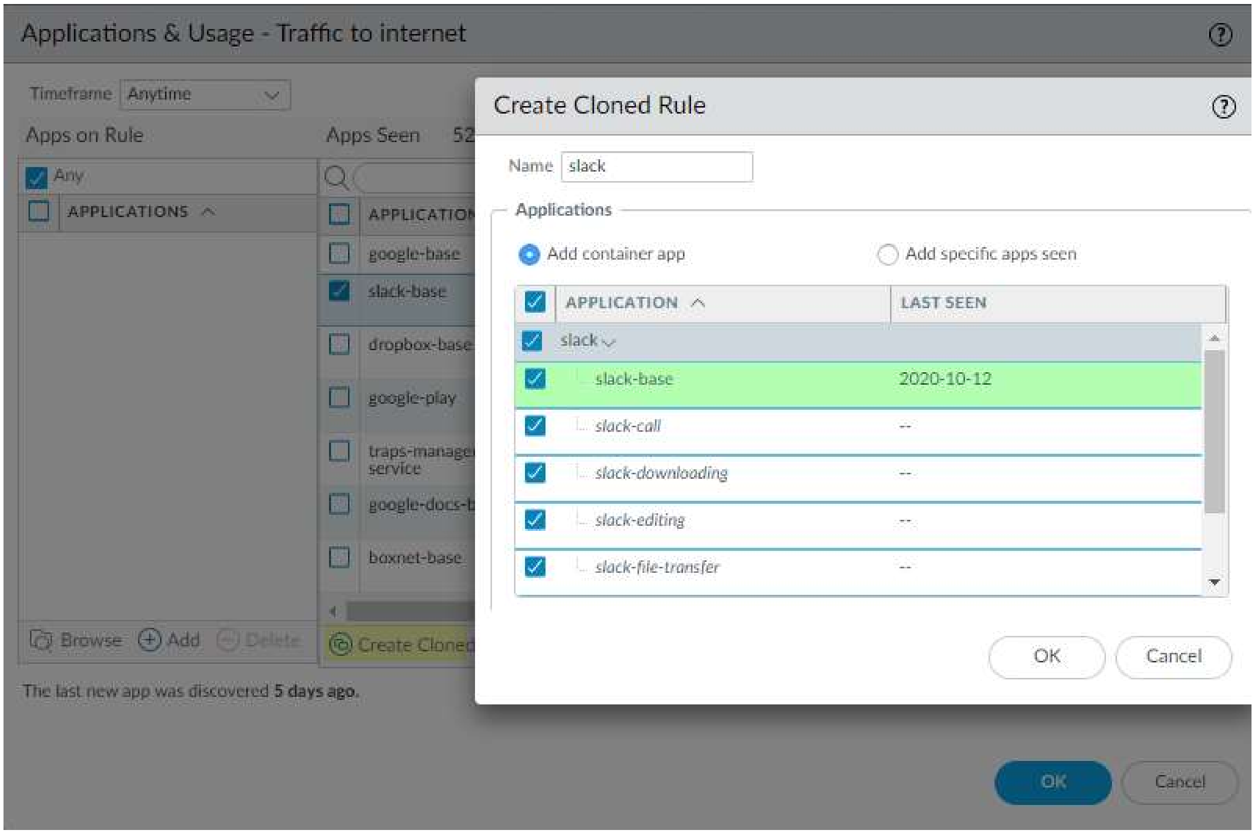
- **Traffic (Bytes, 30 days)** (click to sort) – will show rules that have the most traffic at top.
- **Apps Seen** (click to sort) – will show rules with large number of apps going across the port-based rule. Rules with large numbers of apps may require multiple app-based rules to properly scope the applications, users, and sources/destinations for the new app-based rule.
- **Days with No New Apps** (click to sort) – will show rules that are “stable”, that is, they have not seen new apps in a while. Rules that are more stable could be considered safer to migrate since you are less likely to block legitimate traffic by accident.
- **Hit Count** – shows rules with the most matches over the selected time frame.

Recommendations:
Low risk tolerance: find a rule or two that is relatively stable (high number of days with No New Apps) and that also has a small amount of traffic. Convert those first to see how the process works and because this is safer to start with.

Security first posture: find the rules that have the most traffic or most applications crossing them. Convert those first to accelerate adoption of app-based rules in the fastest possible manner, increasing the security posture of the organization without undue regard for application availability.

Step 3: Once you choose the rules to convert, review the **Apps Seen**.

Once you determine the rule you want to start with, click on the Apps Seen for that rule. Look through the list and confirm whether or not these are sanctioned apps. For all that are deemed sanctioned apps, select them and then use the “Create Cloned Rule”. Cloning is the safest way to migrate rules. Cloning also preserves the original port-based rule and places it below the application-based rule. In our example we are cloning to a new rule named slack. In the example, we selected “Add container app” which exposes the container named slack, with applications under the container. On our port-based rule, the firewall observed the application called slack-base and in addition to that observed app, we have decided to add other related apps from the same container, which are shown in italics (slack-call, slack-downloading, slack-editing, slack-filetransfer, …)



Applications & Usage - Traffic to internet

Timeframe: Anytime

Apps on Rule

☑ Any

□ APPLICATIONS

Apps Seen 52

	APPLICATION
□	google-base
☑	slack-base
□	dropbox-base
□	google-play
□	traps-management-service
□	google-docs-b
□	boxnet-base

The last new app was discovered **5 days ago.**

Create Cloned Rule

Name: slack

Applications

● Add container app ○ Add specific apps seen

	APPLICATION	LAST SEEN
☑	slack	
☑	slack-base	2020-10-12
☑	*slack-call*	--
☑	*slack-downloading*	--
☑	*slack-editing*	--
☑	*slack-file-transfer*	--

Those in italics were not seen by the firewall, but if they are sanctioned for use in your organization, adding them now will prevent the rule from “breaking” the app in the future. If you want to further future-proof your rule, you can leave the container app enabled (slack in the example). This will then automatically add to your rule any new apps added to the container in the future. This could happen in our example if Palo Alto Networks released an Apps and Threats update with a new sub-app called *slack-foobar*. If you prefer to limit the rule to what you have explicitly selected then do not leave the container selected.

There are no application dependencies in our example, but if there were app dependencies you would want to leave them selected so the application would function correctly, this includes the common app-dependencies for SSL and web-browsing. (If you know that the app-dependencies are resolved by a different rule then you do not need to add them here.)

Click OK to add the new app-based rule above the port based rule. Open the rule and set it to use the service application-default. This means that traffic will only be allowed for those applications on the default port(s) as defined by Palo Alto Networks in the appli-pedia.

If the port-based rule is stable, once you have migrated all sanctioned apps to app-based rule(s) you can select the port based rule and disable it.

Commit your changes.

Step 4: Repeat as needed

Repeat this process as needed for additional port-based rules.

Recommendations:

- When you disable a port based rule, use a new tag "disabled <date>", or a comment in the rule description "disabled <date>", so that you can later search for those rules and delete them after 90 days. This can also be useful if you inadvertently block some legitimate traffic and need to turn those port based rule(s) back on shortly after disabling them.

- Risk averse organizations can leave the port based rules enabled, clear that rule's hit counters, and revisit them after one week to see if any new applications have been seen. After which if no new apps were observed then disable the rule.

- Think about any recurring quarterly or annual process that may use different applications and be ready to accommodate that as needed.

Application Anomalies

There may be times Palo Alto identifies an application as unknown which will then need to have a custom application made for the traffic. Though creating custom applications is not covered in detail in this lab, the following guidance could assist during your migration.

Unknown Applications

When the Policy Optimizer identifies an application as unknown, you have some options:

1. For commercial software, ask Palo Alto Networks to add it to the appli-pedia which means they will write the signature.
2. For custom apps (not commercially available), create a custom application to match the traffic. This requires packet captures and traffic analysis on your part.
3. Block the application if it is not sanctioned by your organization.
4. Create an app-based rule to allow the unknown traffic (such as "unknown-tcp") and scope it tightly by user group, source and destination addresses.

Conclusion

Policy Optimizer is a powerful tool that provides workflows to move from port-based to app-based policies. In this lab you have learned a safe and automated way to use Policy Optimizer to accomplish the goal of moving from port-based to app-based policies. Using app-based policies improves the security posture of your organization. Once all rules have been migrated from legacy rules to application rules, you will want to make sure you have configured Security Profiles to inspect and protect the traffic.

Policy Optimizer has other functionality around cleaning up your rulebase by identifying unused and overprovisioned rules, which is outside the scope of this write-up, but is something that would be good to consider when you are done cleaning up the port-based rules.

To go a step further, you will want to assure that traffic passing through the firewall will not be able to evade your security policies. 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 policies are always enforced.

Next Steps

If you want to implement this in your environment and would be more comfortable having someone with experience help you in the process, contact your Sun Management account rep to schedule one of our certified Palo Alto Networks engineers to assist with your policy cleanup.

If you want to test this on your own and do not have access to a lab environment to do so, contact your Sun Management account rep to get pricing on a lab bundle. The PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

Sun Management

Sun Management is a Value Added Reseller (VAR) focusing on Network and Internetwork Security Requirements. We work primarily in the Mid Atlantic area: Maryland (MD), Virginia (VA), District of Columbia (DC), West Virginia (WV), Delaware (DE) and Pennsylvania (PA). Our credentials include Palo Alto Networks Services Provider, Palo Alto Networks Certified Training Partner, and Palo Alto Networks Certified Managed Security Service Provider (MSSP) using CORTEX XSOAR in a multi-tenant environment.

We address requirements concerning Network Detection and Response (NDR); internal and external TLS and SSL requirements for complete data visibility; End Point Detection and Response (EDR); Gramm Leach Bliley Act, HIPPA, Sarbanes Oaxley and PCI DSS; penetration testing and firewall optimization; and Data Protection by tracking all Data Flows within the network, across applications, between users/servers and in the cloud. Contact us at (888) 773-9422 to setup a POC or if you just want more information.

Resource Links

Palo Alto Network's Policy Optimizer
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/security-policy-rule-optimization.html

Creating Custom Applications:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRoCAK

Palo Alto Networks Best Practices
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/set-up-antivirus-anti-spyware-and-vulnerability-protection.html

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/best-practices-for-securing-your-network-from-layer-4-and-layer-7-evasions.html