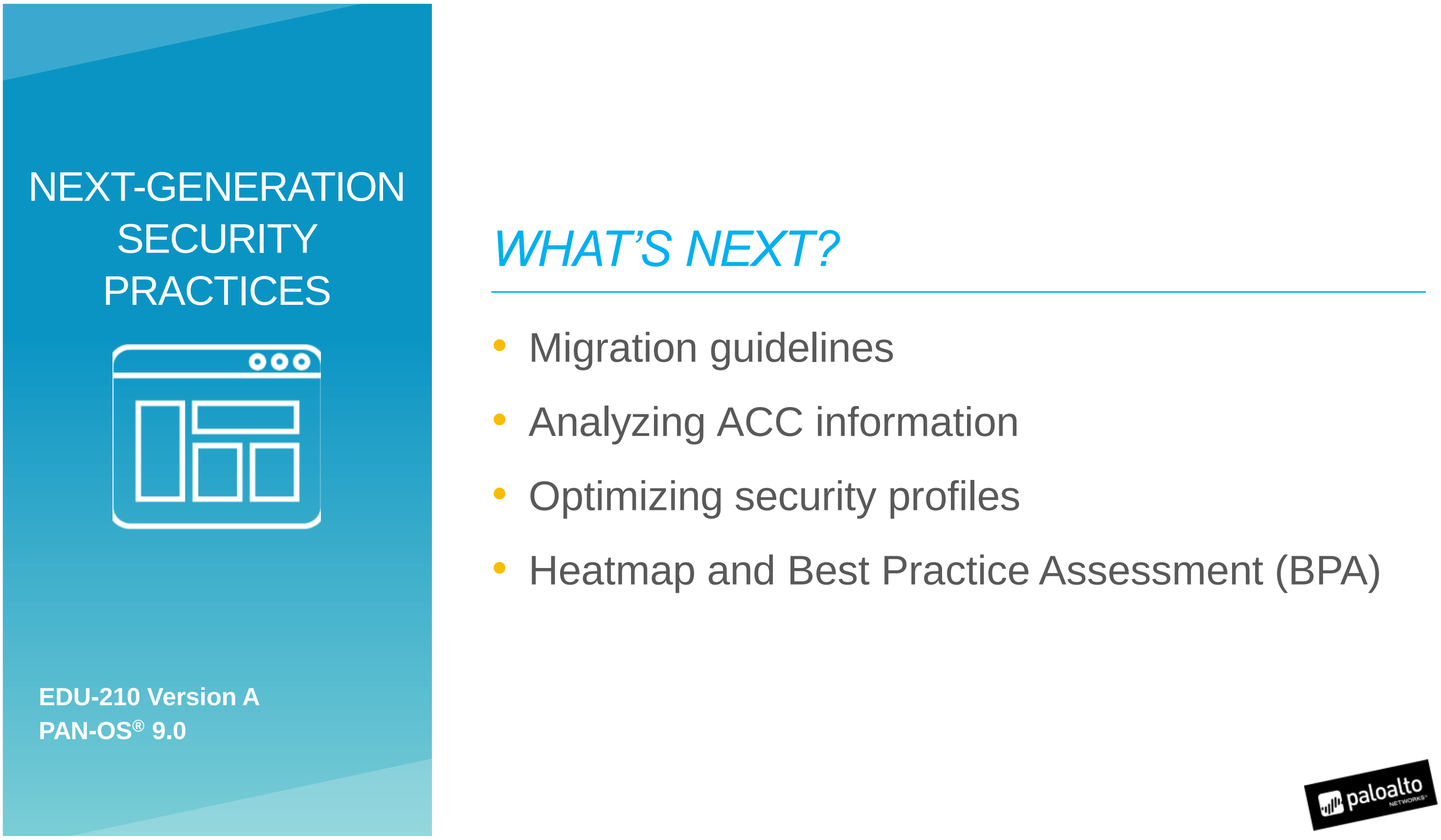
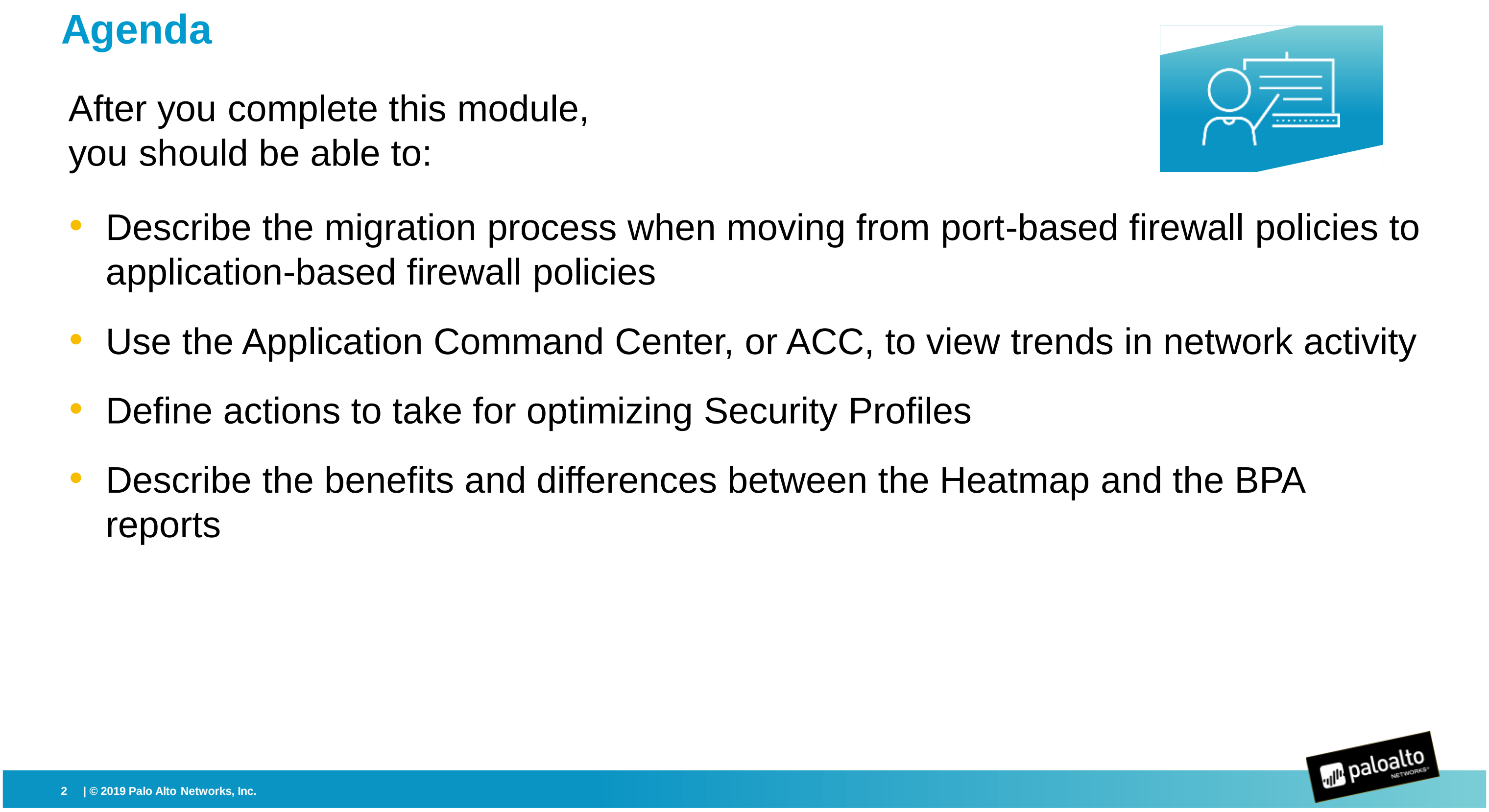


NEXT-GENERATION SECURITY PRACTICES

EDU-210 Version A
PAN-OS® 9.0

WHAT'S NEXT?

- Migration guidelines
- Analyzing ACC information
- Optimizing security profiles
- Heatmap and Best Practice Assessment (BPA)



Agenda

After you complete this module,
you should be able to:

- Describe the migration process when moving from port-based firewall policies to application-based firewall policies
- Use the Application Command Center, or ACC, to view trends in network activity
- Define actions to take for optimizing Security Profiles
- Describe the benefits and differences between the Heatmap and the BPA reports

After you complete this module, you should be able to:

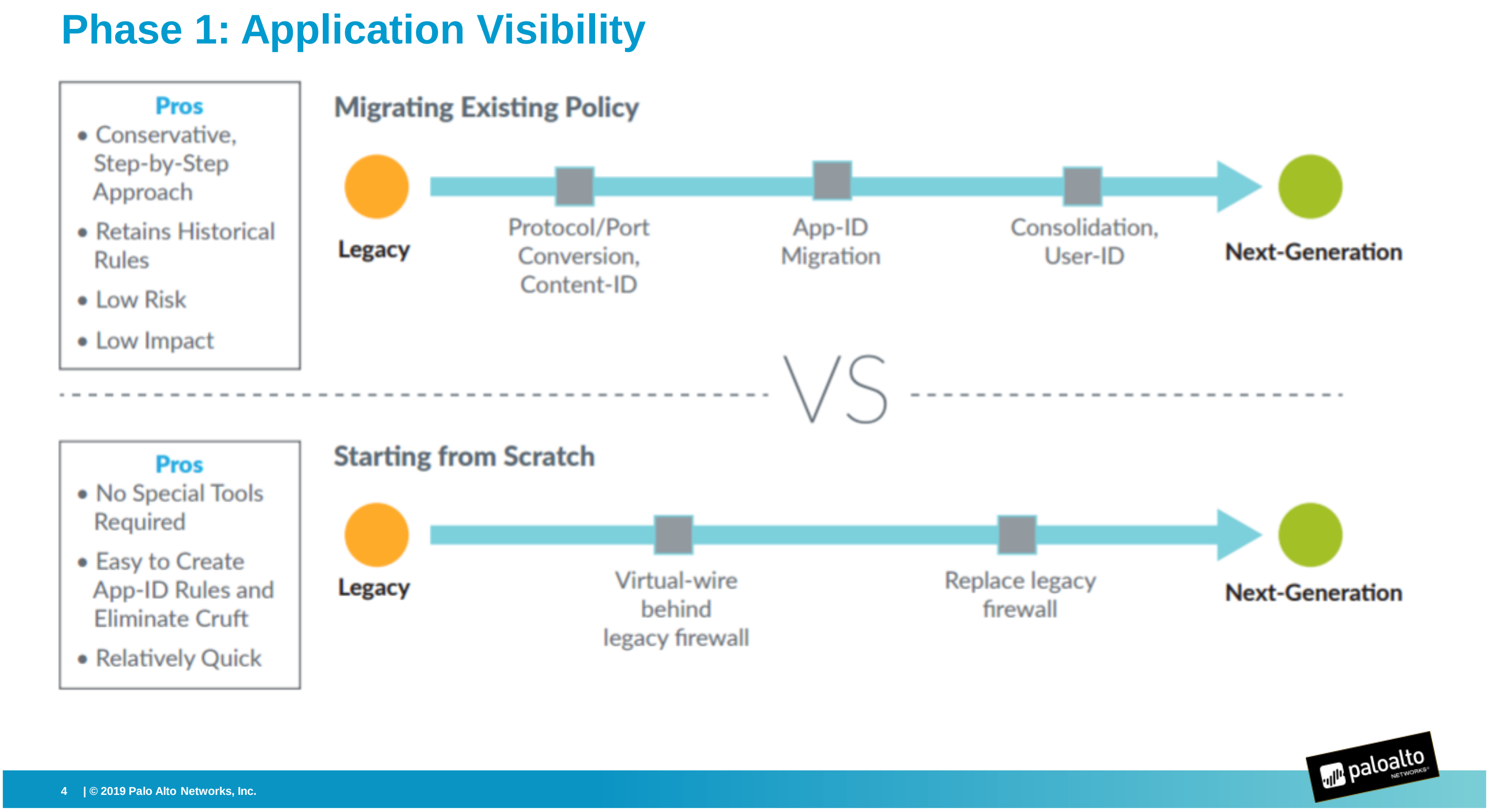
- Describe the migration process when moving from port-based firewall policies to application-based firewall policies
- Use the Application Command Center, or ACC, to view trends in network activity
- Define actions to take for optimizing Security Profiles
- Describe the benefits and differences between the Heatmap and the BPA reports

Migration guidelines

Analyzing ACC information

Optimizing security profiles

Heatmap and Best Practice Assessment (BPA)



Phase 1: Application Visibility

Pros

- Conservative, Step-by-Step Approach
- Retains Historical Rules
- Low Risk
- Low Impact

Migrating Existing Policy

Legacy → Protocol/Port Conversion, Content-ID → App-ID Migration → Consolidation, User-ID → Next-Generation

VS

Pros

- No Special Tools Required
- Easy to Create App-ID Rules and Eliminate Cruft
- Relatively Quick

Starting from Scratch

Legacy → Virtual-wire behind legacy firewall → Replace legacy firewall → Next-Generation

4 | © 2019 Palo Alto Networks, Inc.

The two basic approaches to deploying application-based policies with App-ID technology are as follows:

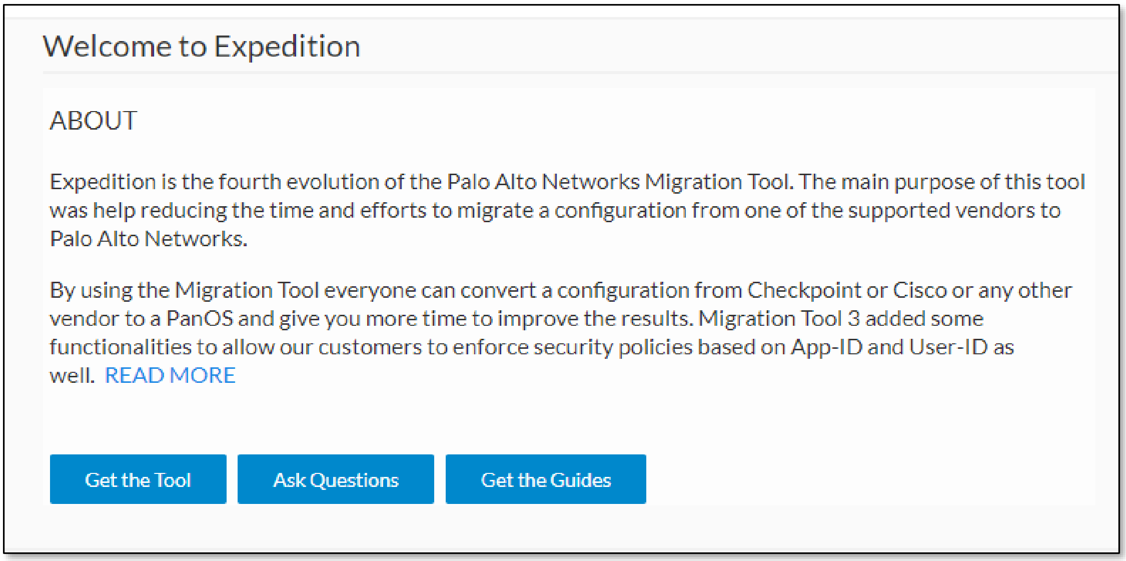
1. Migrate existing policies from your legacy, port-based firewall
2. Start from a clean configuration and create new policies, either in a previously unprotected network location or as a slow transition from a legacy, port-based firewall

Phase 1 is appropriate only during an initial deployment (about 30 days), and is meant to record logs of production traffic so that informed policy can be implemented for security.

This phase is intended to provide visibility. Features such as decryption and User-ID technology should be deployed at this time.

Expedition (Migration Tool)

- Migrate policy from a pre-existing firewall
- https://live.paloaltonetworks.com/t5/Migration-Tool/ct-p/migration_tool



Welcome to Expedition

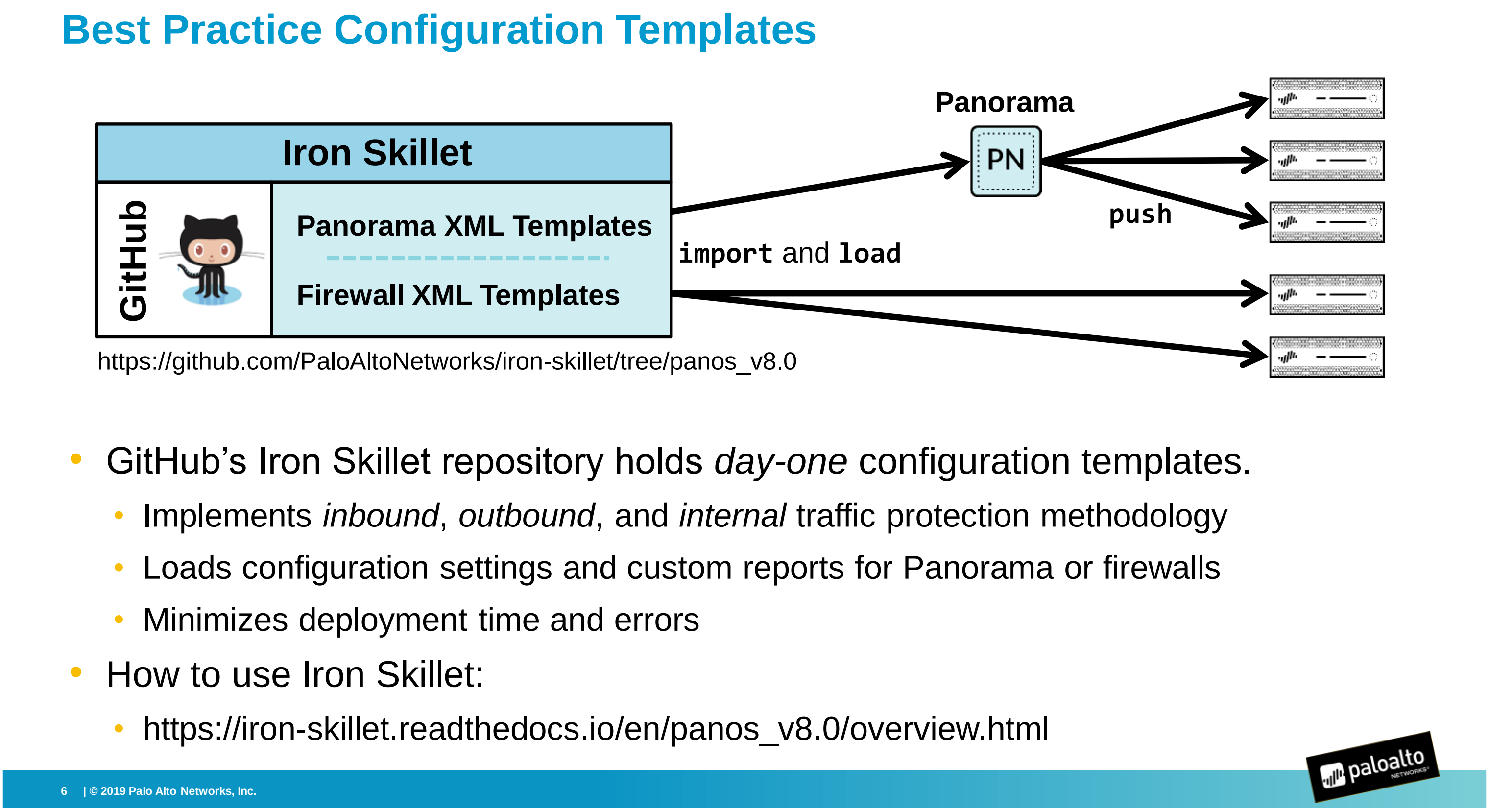
ABOUT

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

By using the Migration Tool everyone can convert a configuration from Checkpoint or Cisco or any other vendor to a PanOS and give you more time to improve the results. Migration Tool 3 added some functionalities to allow our customers to enforce security policies based on App-ID and User-ID as well. READ MORE

The main objective of the fourth generation Migration Tool, or Expedition, is to assist network security administrators, professional consultants, or anyone who is working on a migration project with rules optimization, security controls validation, or App-ID implementation. Expedition is intended to help reduce the time and effort to migrate configuration from one of the Supported vendors to Palo Alto Networks.

With the release of the Migration tool 3.0, functionality was added to allow you to enforce Security policies based on App-ID and User-ID. With the release of Expedition, Machine Learning has been introduced to help you generate Security policies based on log traffic and the Best Practices Assessment Tool, or BPA.



Best Practice Configuration Templates

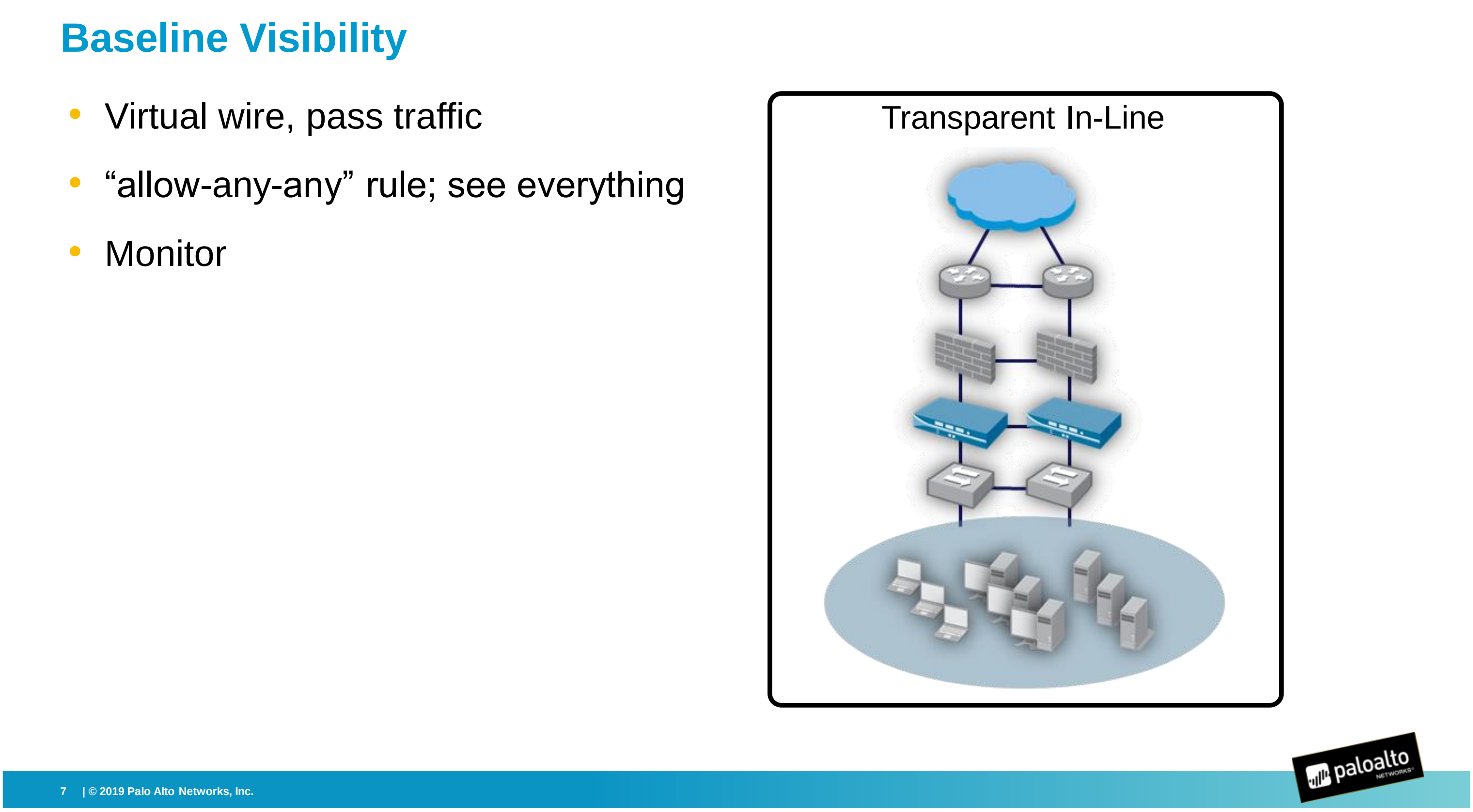
https://github.com/PaloAltoNetworks/iron-skillet/tree/panos_v8.0

- GitHub’s Iron Skillet repository holds *day-one* configuration templates.
  - Implements *inbound*, *outbound*, and *internal* traffic protection methodology
  - Loads configuration settings and custom reports for Panorama or firewalls
  - Minimizes deployment time and errors
- How to use Iron Skillet:
  - https://iron-skillet.readthedocs.io/en/panos_v8.0/overview.html

The Iron Skillet website provides a repository of firewall and Panorama *day-one* XML configuration templates that you can use to secure your networks in accordance with best practice recommendations. The *day-one* configuration blocks malware to keep your network safe while minimizing application downtime as a result of a too-strict configuration. A day-one configuration is considered to be a safe starting point for most deployments. As you learn more about the specific applications and user activities in your environment, you can add additional configuration settings appropriate for your network.

The Iron Skillet templates deploy best-practice protections for *inbound*, *outbound*, and *internal* traffic. For example, Iron Skillet templates create a set of inbound, outbound, and internal Security Profiles and Security Profile Groups similar to what you have just seen in this training module. However, Iron Skillet goes further and also creates a set of useful custom reports and various log and log forwarding settings. Using preconfigured XML configuration templates minimizes deployment time and errors. The templates provide a configuration that is use case agnostic.

The day-one XML configuration templates are not complete configuration templates. The emphasis is on key security elements such as dynamic updates, Security Profiles, Security rules, and logging that should be consistent across deployments. To insert a firewall into your network requires additional customizations including network interface addresses, zone names, routing, and other settings. Also not included are use-case specific items such as whitelist Security policy rules, User-ID settings, and Decryption policy rules that can be deployment and use case specific.

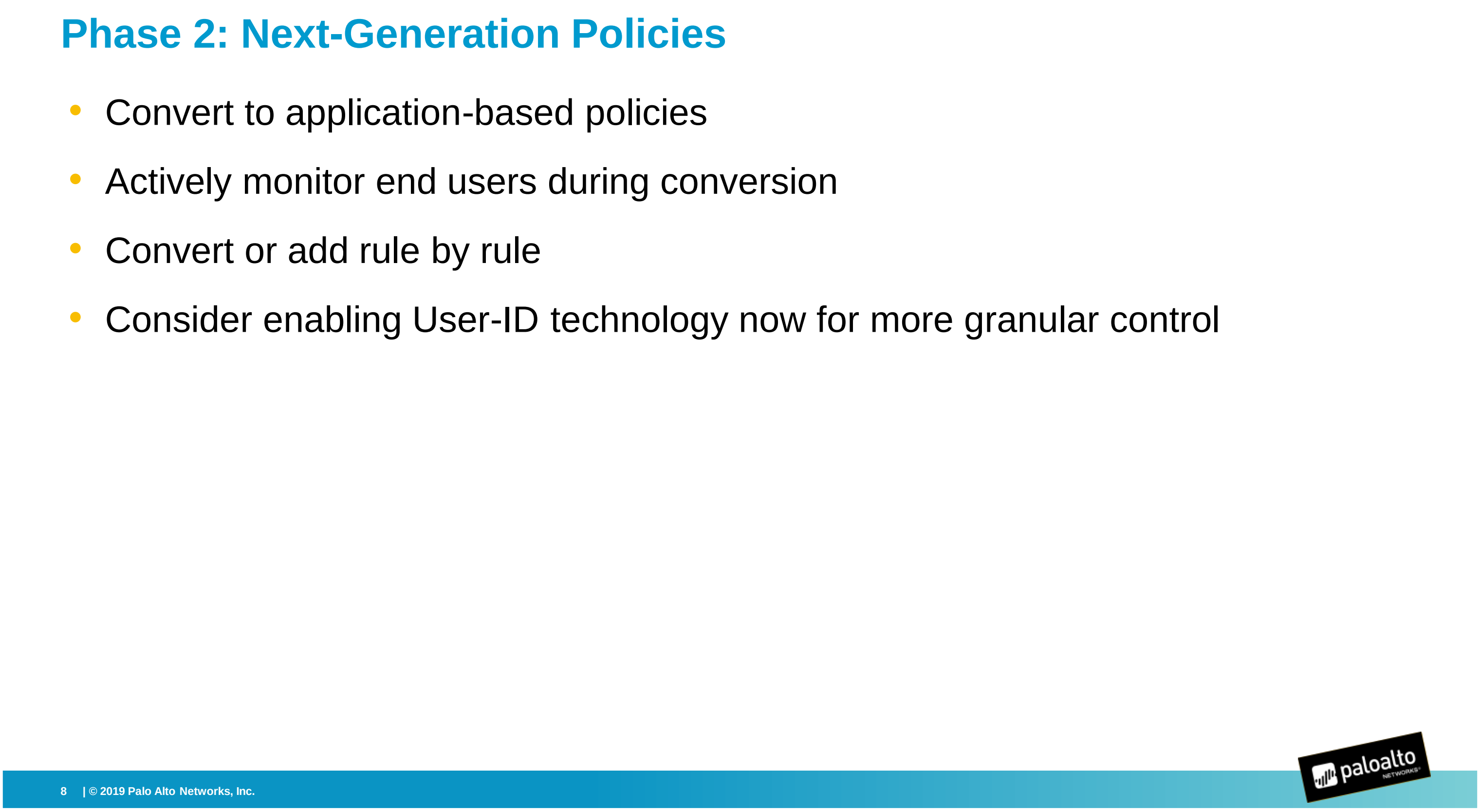


Baseline Visibility

- Virtual wire, pass traffic
- “allow-any-any” rule; see everything
- Monitor

You may want to create your own next-generation Security policy rules. However, before you can start creating effective application-based policies, you first must understand your organization’s traffic flow and/or log data.

The first step is to place your NGFW in Virtual Wire or Transparent mode behind, or in front of, your legacy firewall with an explicit “allow-any-any” rule. You will not be enforcing any policy, but you will have visibility into all traffic within the context of applications, which will give you a baseline for later building policies.



Phase 2: Next-Generation Policies

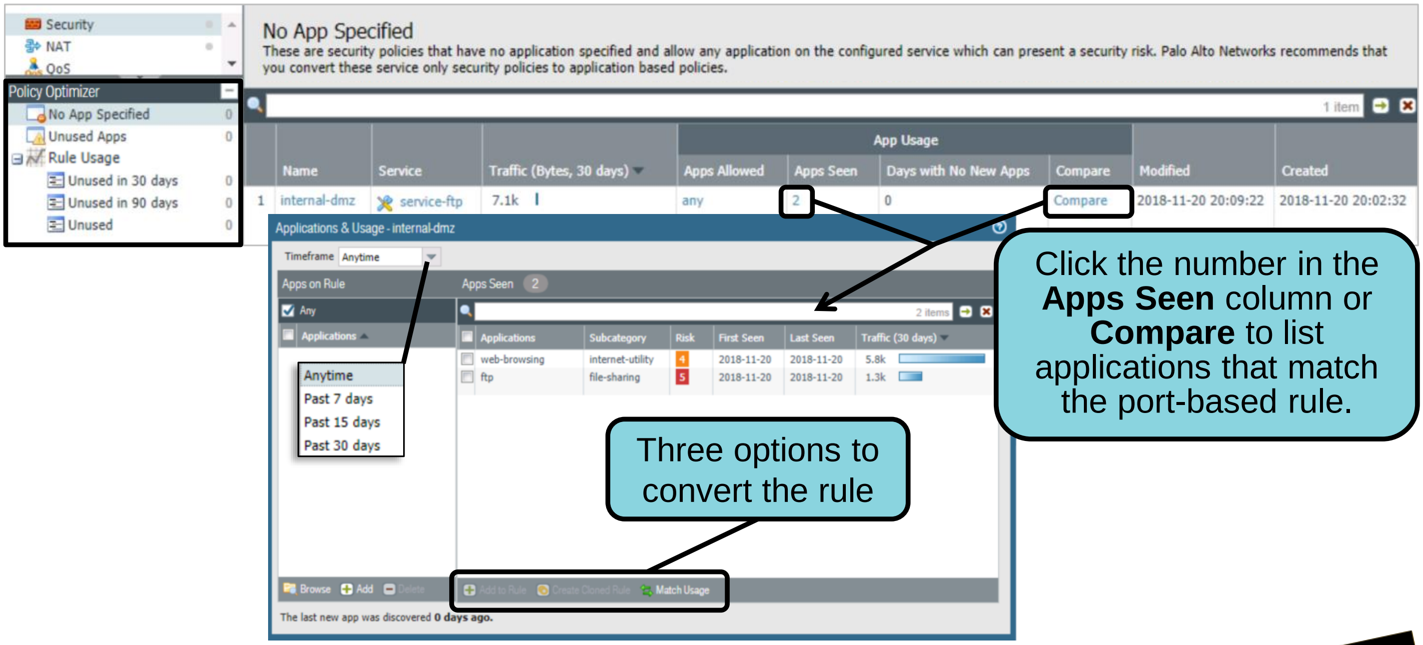
- Convert to application-based policies
- Actively monitor end users during conversion
- Convert or add rule by rule
- Consider enabling User-ID technology now for more granular control

8 | © 2019 Palo Alto Networks, Inc.

Safely enable applications by making sure that you have properly enabled all legitimate applications, and that you have identified and restricted applications that pose a danger to your network.

Policy Optimizer

Policies > Security > Policy Optimizer > No App Specified



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
1	internal-dmz	service-ftp	7.1k	any	2	0	Compare	2018-11-20 20:09:22	2018-11-20 20:02:32

Applications & Usage - internal-dmz

Timeframe Anytime

Apps on Rule

☑ Any

□ Applications

Apps Seen 2

□	Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
□	web-browsing	internet-utility	4	2018-11-20	2018-11-20	5.8k
□	ftp	file-sharing	5	2018-11-20	2018-11-20	1.3k

The last new app was discovered **0 days ago.**

Click the number in the **Apps Seen** column or **Compare** to list applications that match the port-based rule.

Three options to convert the rule

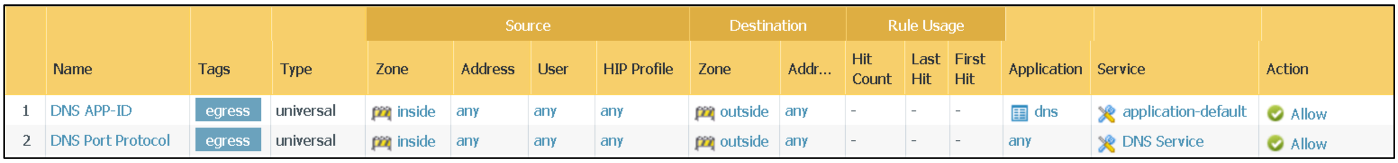
The Policy Optimizer provides a simple workflow to migrate your legacy Security policy rulebase to an App-ID-based rulebase, which improves your security by reducing the attack surface and making available information about applications so you can safely enable them. If you allow any application, you increase the attack surface because any application can use an open port. The Policy Optimizer identifies all applications seen on your legacy Security policy rules and provides you with an easy workflow for selecting the applications you want to allow on that rule. The Policy Optimizer enables you to add applications to port-based rules that convert those rules to an application-based whitelist rule or to clone an existing port-based rule and add the appropriate applications to your cloned rule.

The **Rule Usage** application information can help you prioritize which port-based rules to migrate to application-based rules first, identify rules to clean up, and analyze rule usage characteristics.

The **Unused Apps** displays application-based rules configured with applications that are not in use on the network. Identification and removal of unused applications from Security policy rules strengthens your security posture because your attack surface is reduced.

Rule Conversion: Port and Protocol to App-ID

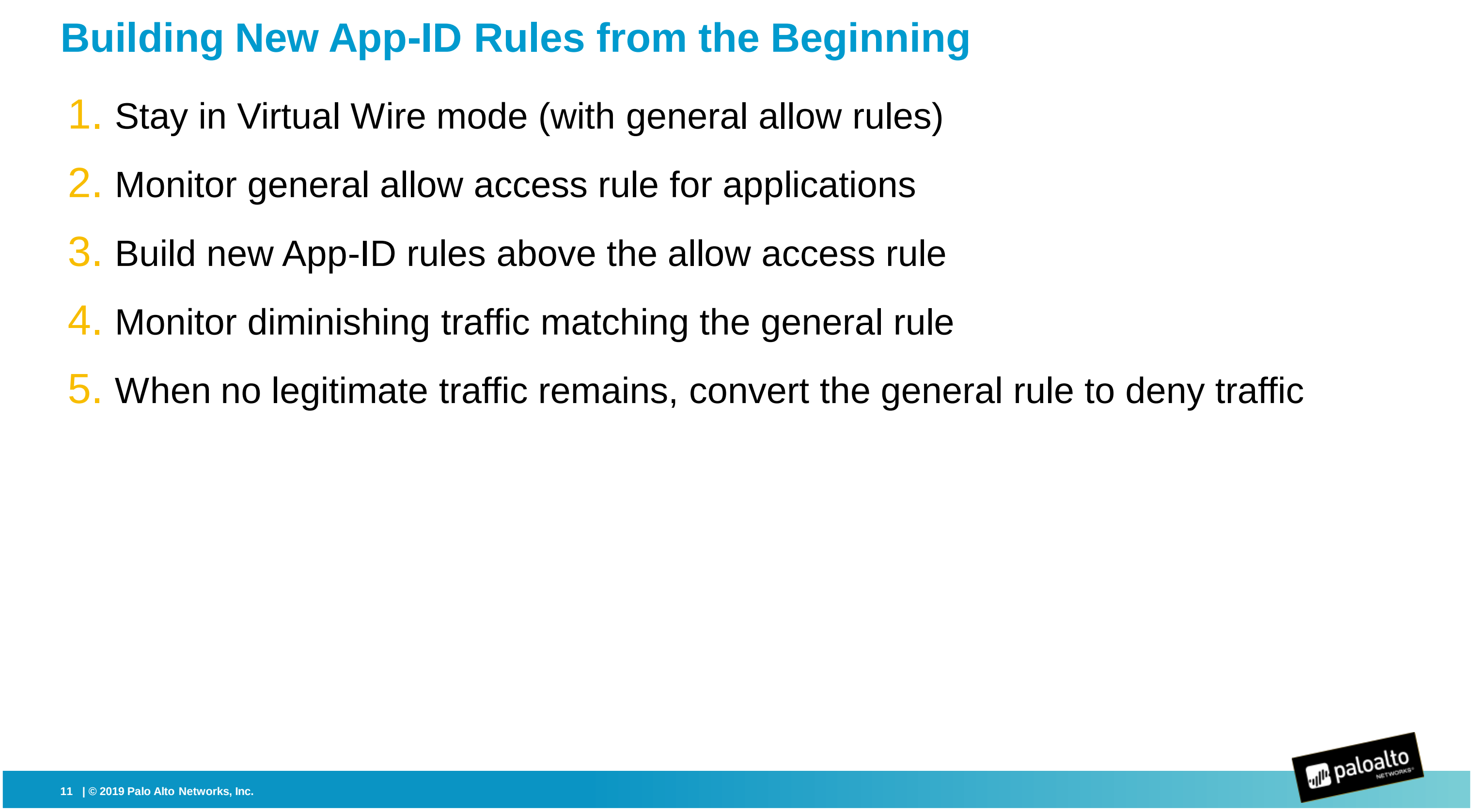
1. Monitor current rule for applications
2. Clone rule, adding App-ID
3. Move new rule above original rule
4. Monitor to confirm that no additional traffic matches the original rule
5. Remove original rule



				Source				Destination		Rule Usage					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Addr...	Hit Count	Last Hit	First Hit	Application	Service	Action
1	DNS APP-ID	egress	universal	inside	any	any	any	outside	any	-	-	-	dns	application-default	Allow
2	DNS Port Protocol	egress	universal	inside	any	any	any	outside	any	-	-	-	any	DNS Service	Allow

The best way to convert rules to be application-aware is to go rule by rule, look at which applications are being allowed or denied, clone the rule, and populate the App-ID field. Then you move the new rule above the original rule and let traffic run through it for another 30 to 90 days to verify that no traffic is still matching that original rule. You now can remove the original, port-based rule. The most important step in the process is removing port-based rules, so make sure that this removal is done for every rule that is converted.

After all port-based rules have been removed, your policy set primarily will be application-based, which allows or denies traffic at the application level, even if the application uses a nonstandard port. A few port-based likely remain where appropriate.



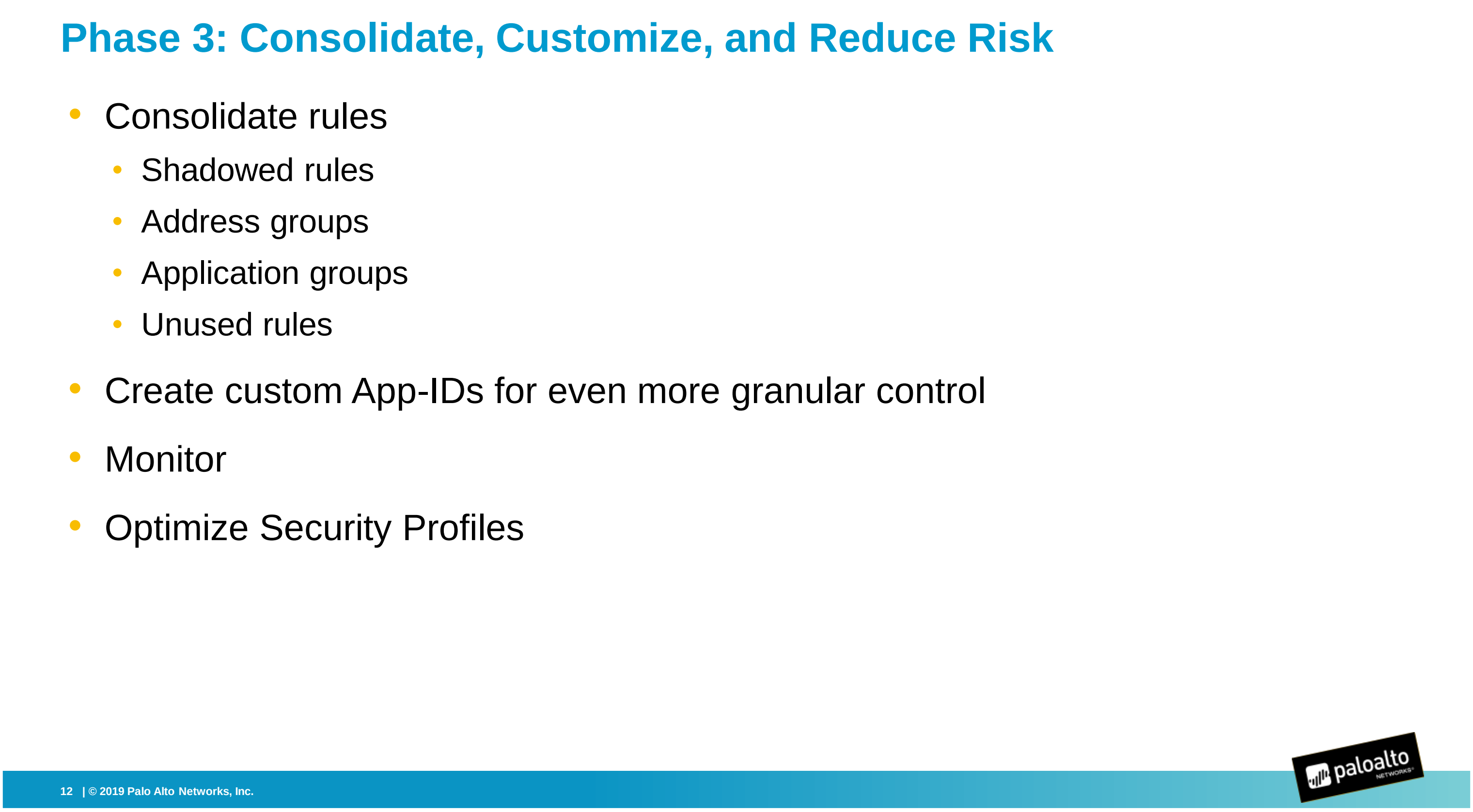
Building New App-ID Rules from the Beginning

1. Stay in Virtual Wire mode (with general allow rules)
2. Monitor general allow access rule for applications
3. Build new App-ID rules above the allow access rule
4. Monitor diminishing traffic matching the general rule
5. When no legitimate traffic remains, convert the general rule to deny traffic

11 | © 2019 Palo Alto Networks, Inc.

After you have collected traffic for 30 days and have a comprehensive representation of your traffic, you can begin to build application-based policy. Leave the virtual wire in place as you create your new policies. As you build out the ruleset, you will see less and less traffic that matches the “allow-any-any” rule you started with.

When no legitimate traffic matches the explicit “allow-any-any” rule, change the rule into a “deny-any-any” rule. You now are ready to completely replace the legacy firewall with your NGFW.



Phase 3: Consolidate, Customize, and Reduce Risk

- Consolidate rules
  - Shadowed rules
  - Address groups
  - Application groups
  - Unused rules
- Create custom App-IDs for even more granular control
- Monitor
- Optimize Security Profiles

Now that you have application-based policies in place, you may be able to consolidate the number of policies and further build out your ruleset by adding custom applications using the vast library of Palo Alto Networks application decoders.

Rule consolidation reduces management overhead by simplifying your view of what is allowed or blocked by your NGFW. Instead of having a single rule each for application, user, and threat prevention, for example, Palo Alto Networks allows you to combine these traffic parameters into a single policy, which often substantially reduces the number of rules that you must manage, thus making the task of keeping rulesets updated much easier.

For more information about creating Custom App-IDs, see https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html.

After your NGFW is deployed with consolidated, customized, next-generation Security policy rules, actively monitor your network traffic and look to optimize your Security Profiles.

Migration guidelines

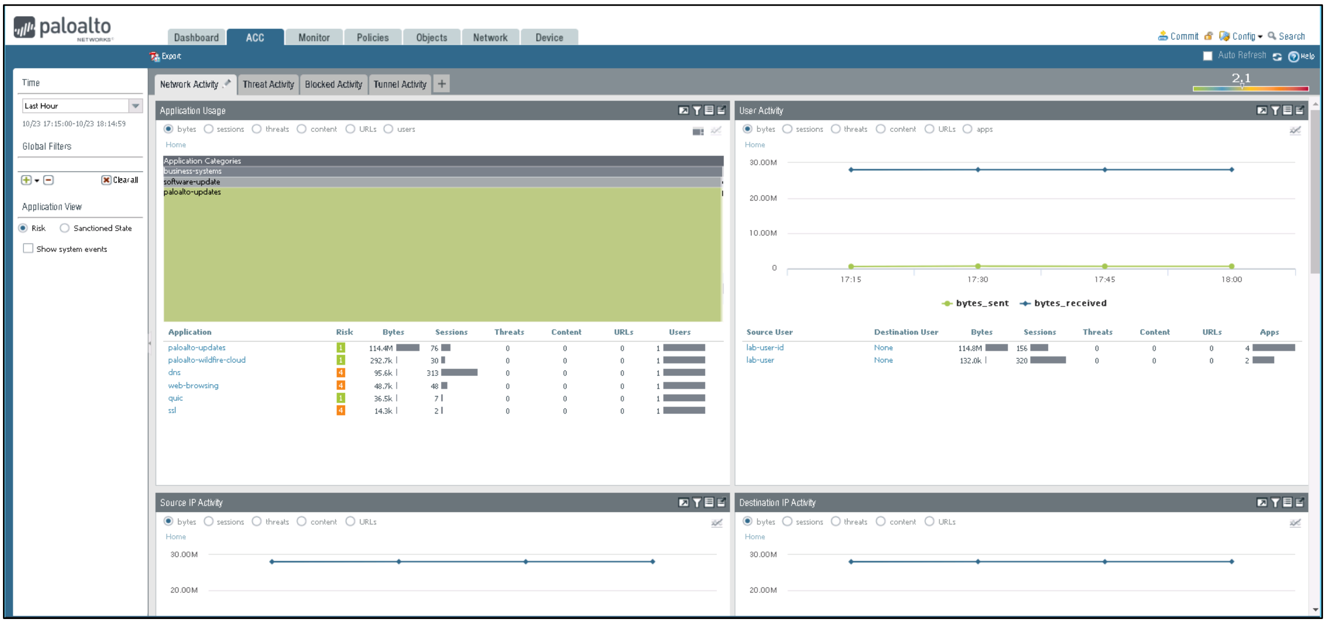
Analyzing ACC information

Optimizing security profiles

Heatmap and Best Practice Assessment (BPA)

Application Command Center (ACC)

- Best place to get a high-level view of network activity



Time: Last Hour

10/23 17:15:00-10/23 18:14:59

Application View: ● Risk ○ Sanctioned State

□ Show system events

Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
paloalto-updates	1	114.4M	76	0	0	0	1
paloalto-wildfire-cloud	1	292.7k	30	0	0	0	1
dns	4	95.6k	313	0	0	0	1
web-browsing	4	48.7k	48	0	0	0	1
quic	1	36.5k	7	0	0	0	1
ssl	4	14.3k	2	0	0	0	1

Source User	Destination User	Bytes	Sessions	Threats	Content	URLs	Apps
lab-user-id	None	114.8M	156	0	0	0	4
lab-user	None	132.0k	320	0	0	0	2

14 | © 2019 Palo Alto Networks, Inc.

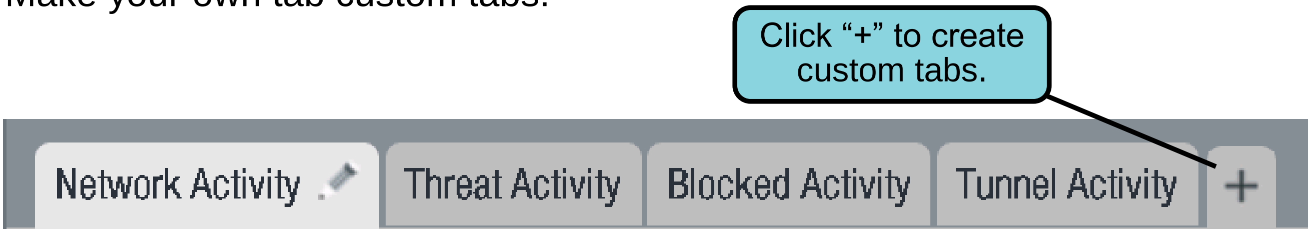
The ACC is an analytical tool that provides details about network activity that you can use to fine-tune your firewall configuration. The ACC uses the firewall logs for graphically depicting traffic trends on your network.

The graphical representation allows you to interact with the data and to visualize the relationships between events on the network, including network use patterns, traffic patterns, and suspicious activity and anomalies.

This visualization allows you to uncover anomalies or find ways to enhance your network security rules. For a personalized view of your network, you also can add a custom tab and include widgets that allow you to focus on the information that is most important to you.

Tabs

- Network Activity: An overview of traffic and user activity on your network
- Threat Activity: An overview of the top threats, such as vulnerabilities, spyware, and viruses
- Blocked Activity: Focuses on traffic that was prevented from coming into the network
- Make your own tab custom tabs:



Network Activity
This tab displays an overview of traffic and user activity on your network. It focuses on this information:

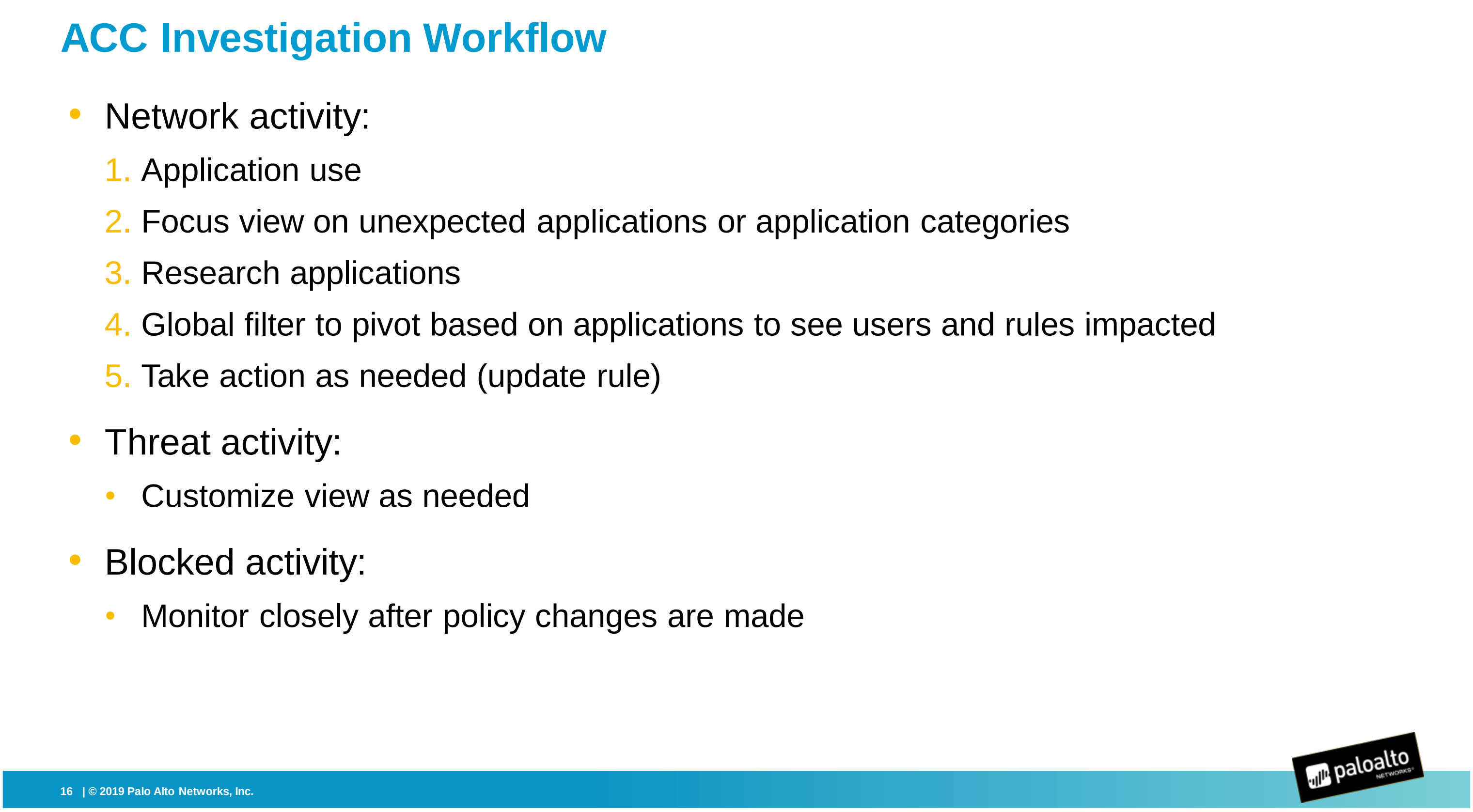
- Top applications in use
- Top users who generate traffic (with additional details into the bytes, content, threat, or URLs accessed by the user)
- Most used security rules against which traffic matches occur

You also can display network activity by source or destination zone, region, or IP address. You can view ingress or egress interfaces, and host information such as the operating systems of the devices most commonly used on the network.

Threat Activity
This tab displays an overview of the threats on the network. It focuses on the top threats: vulnerabilities, spyware, virus, hosts visiting malicious domains or URLs, top WildFire® submissions by file type and application, and applications that use nonstandard ports.

Blocked Activity
This tab focuses on traffic that was prevented from coming into the network. The widgets in this tab allow you to view activity denied by application name, username, threat name, and content (files and data), and the top security rules with a "deny" action that blocked traffic.

Tunnel Activity
This tab focuses on tunnel traffic that the firewall has inspected. Information includes tunnel usage based on tunnel ID, monitor tag, user, and tunnel protocol.



ACC Investigation Workflow

- Network activity:
  1. Application use
  2. Focus view on unexpected applications or application categories
  3. Research applications
  4. Global filter to pivot based on applications to see users and rules impacted
  5. Take action as needed (update rule)
- Threat activity:
  - Customize view as needed
- Blocked activity:
  - Monitor closely after policy changes are made

Use the ACC to review network data or trends to find which applications or users are generating the most traffic, and how many application are responsible for the threats seen on the network.

The ACC can help identify which application(s) and user(s) generated the traffic, determine whether the application was on the default port, and identify which policy rule(s) allowed the traffic into the network. If any threat did come through, the ACC also can determine whether the threat is spreading laterally on the network.

Use the conclusions from your investigation to craft goal-oriented policies that can secure users and your network.

Migration guidelines

Analyzing ACC information

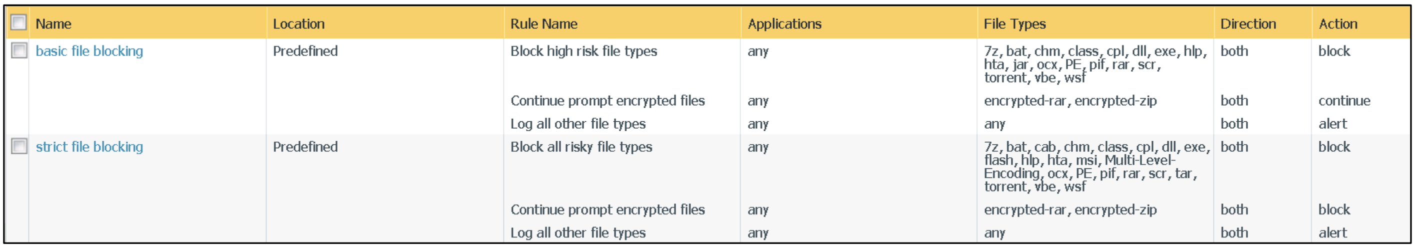
Optimizing security profiles

Heatmap and Best Practice Assessment (BPA)

File Blocking

- Start by cloning the default profiles and modify as necessary
- Block suspicious files that have no common use case
- Set allowed files to “continue” (prevents drive-by downloads)
- Set “alert” for everything else

Objects > Security Profiles > File Blocking



☐	Name	Location	Rule Name	Applications	File Types	Direction	Action
☐	basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
			Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
			Log all other file types	any	any	both	alert
☐	strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
			Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	block
			Log all other file types	any	any	both	alert

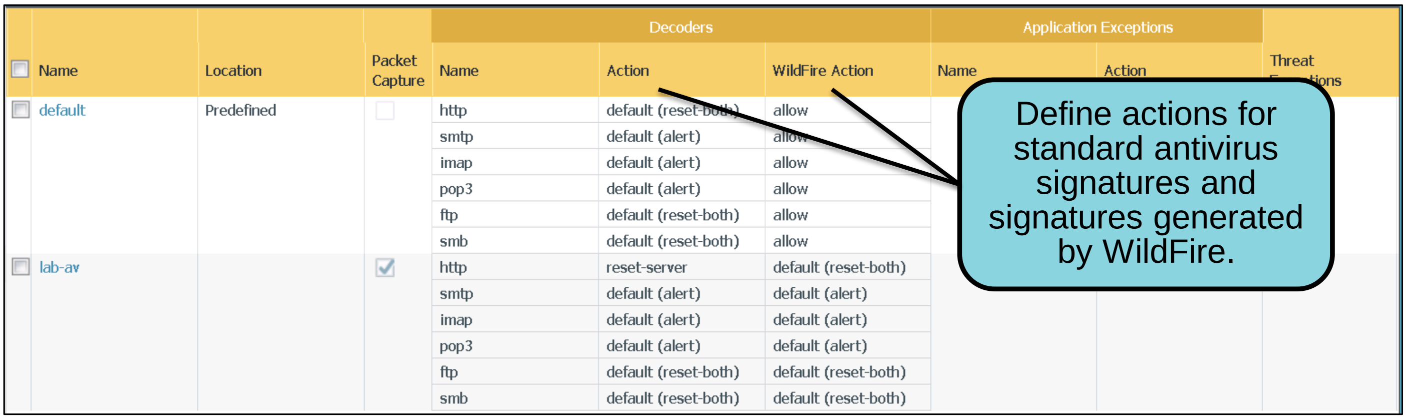
Clone a default File Blocking Profile or create a new profile that blocks files that are commonly included in malware attack campaigns or that have no real use case for upload or download. These files now include batch files, DLLs, Java class files, help files, Windows shortcuts (.lnk), and BitTorrent files. You can allow download or upload of personal executables (PEs) and archive files (.zip and .rar) but force users to click **continue** before they transfer a file to give them a chance to reconsider. Finally, alert on all other file types for visibility into which other file transfers are happening so that you can determine if you need to make policy changes.

Educate your users that they may be subject to a malicious download if they are prompted to continue with a file transfer they did not knowingly initiate.

Antivirus

- The default Antivirus Profile is the recommended behavior:

Objects > Security Profiles > Antivirus



				Decoders			Application Exceptions		
☐	Name	Location	Packet Capture	Name	Action	WildFire Action	Name	Action	Threat Exceptions
☐	default	Predefined	☐	http	default (reset-both)	allow			
				smtp	default (alert)	allow			
				imap	default (alert)	allow			
				pop3	default (alert)	allow			
				ftp	default (reset-both)	allow			
				smb	default (reset-both)	allow			
☐	lab-av		☑	http	reset-server	default (reset-both)			
				smtp	default (alert)	default (alert)			
				imap	default (alert)	default (alert)			
				pop3	default (alert)	default (alert)			
				ftp	default (reset-both)	default (reset-both)			
				smb	default (reset-both)	default (reset-both)			

Define actions for standard antivirus signatures and signatures generated by WildFire.

- Increase SMTP protection if no email security is in place

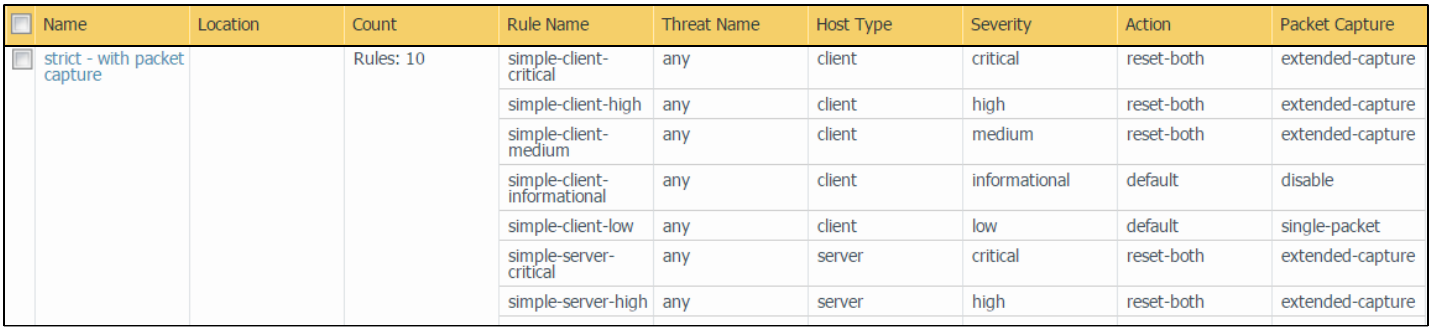
The recommended Antivirus Profile uses the “default” action when it detects traffic that matches either an antivirus signature or a signature generated by WildFire. The “default” action differs for each protocol and follows the most up-to-date recommendation from Palo Alto Networks for how to best prevent propagation of malware in each type of protocol.

By default, the firewall alerts on viruses found in SMTP traffic. However, if you do not have a dedicated antivirus gateway solution in place for your SMTP traffic, define a stricter action for this protocol to protect against infected email content. Use the “reset-both” action to return a 541 response to the sending SMTP server to prevent it from resending the blocked message.

Vulnerability Protection

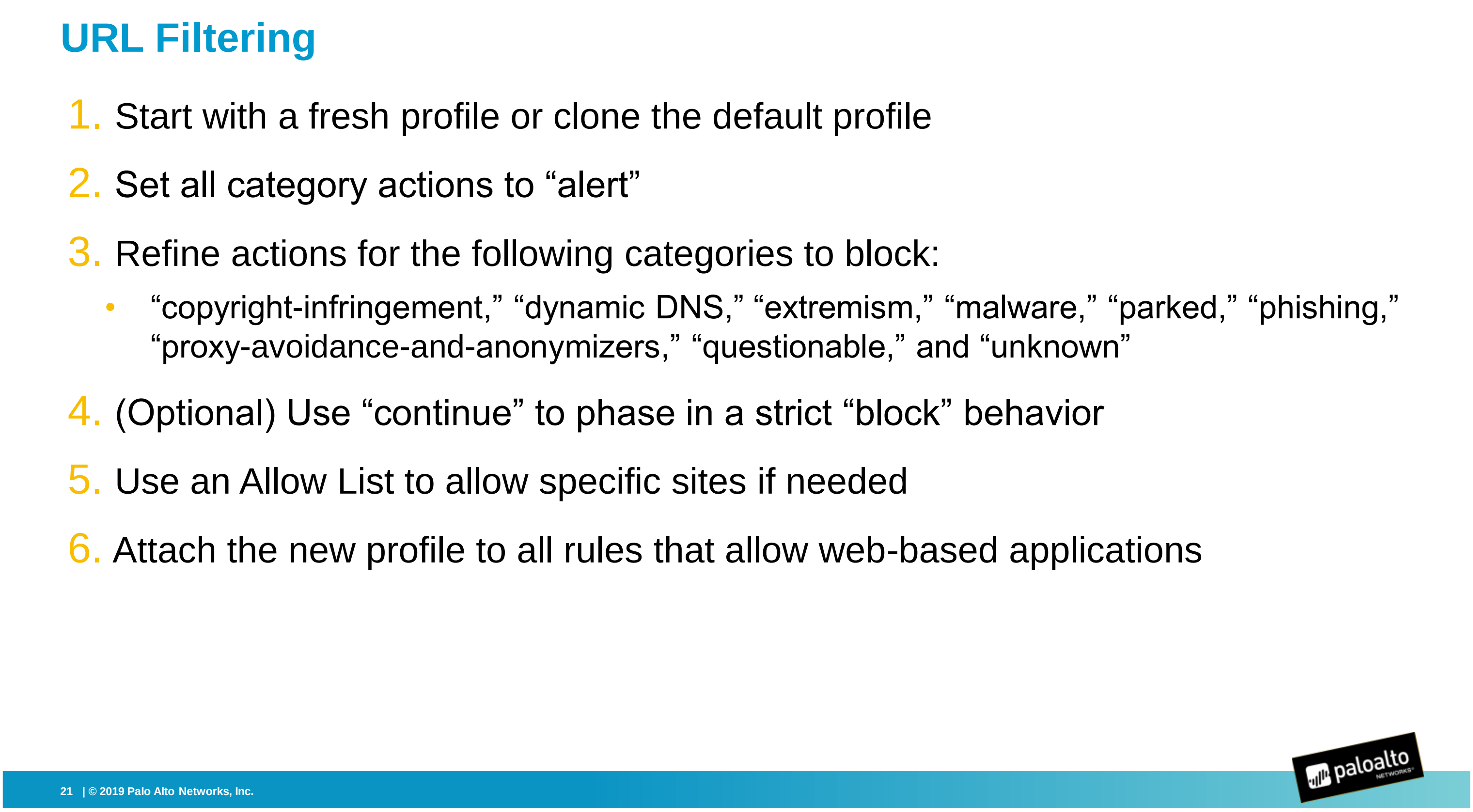
- Clone the predefined strict profile
- Enable packet capture

Objects > Security Profiles > Vulnerability Protection



□	Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
□	strict - with packet capture		Rules: 10	simple-client-critical	any	client	critical	reset-both	extended-capture
				simple-client-high	any	client	high	reset-both	extended-capture
				simple-client-medium	any	client	medium	reset-both	extended-capture
				simple-client-informational	any	client	informational	default	disable
				simple-client-low	any	client	low	default	single-packet
				simple-server-critical	any	server	critical	reset-both	extended-capture
				simple-server-high	any	server	high	reset-both	extended-capture

The recommended profile is a clone of the predefined strict profile, with packet capture settings enabled to help you identify the source of any potential attacks.



URL Filtering

1. Start with a fresh profile or clone the default profile
2. Set all category actions to “alert”
3. Refine actions for the following categories to block:
   - “copyright-infringement,” “dynamic DNS,” “extremism,” “malware,” “parked,” “phishing,” “proxy-avoidance-and-anonymizers,” “questionable,” and “unknown”
4. (Optional) Use “continue” to phase in a strict “block” behavior
5. Use an Allow List to allow specific sites if needed
6. Attach the new profile to all rules that allow web-based applications

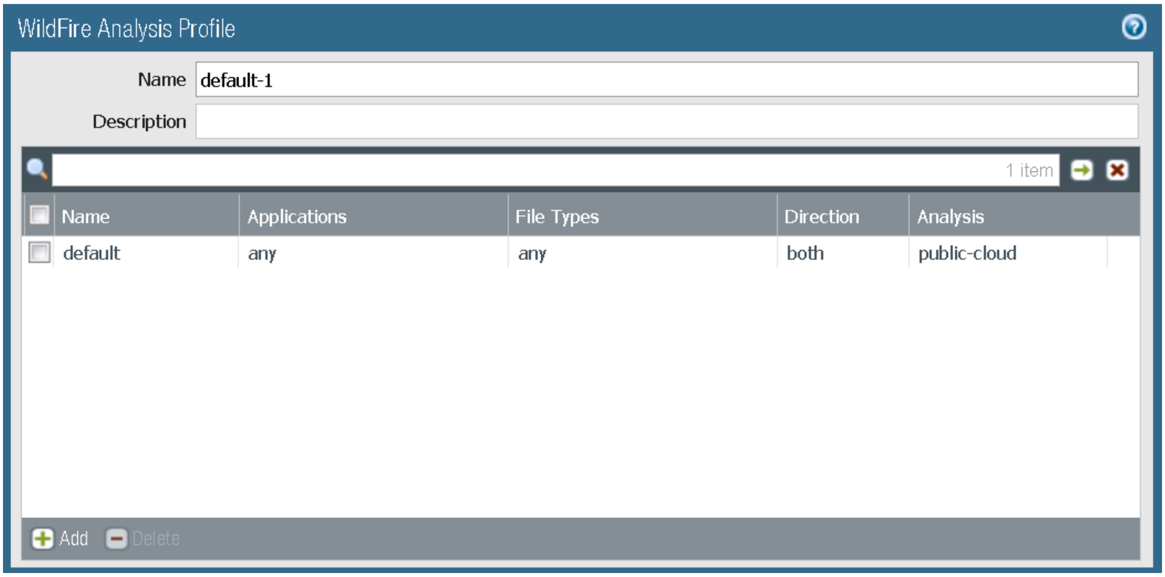
The recommended URL Filtering Profile sets all known dangerous URL categories to “block.” These categories are “copyright-infringement,” “dynamic DNS,” “extremism,” “malware,” “parked,” “phishing,” “proxy-avoidance-and-anonymizers,” “questionable,” and “unknown.” Failure to block these dangerous categories puts you at risk for exploit infiltration, malware download, command-and-control activity, and data exfiltration.

If you need to phase in a block policy, set categories to “continue” and create a custom response page to educate users about your acceptable use policies and alert them to the fact that they are visiting a site that may pose a threat. This process will enable you to properly block URL categories after an initial monitoring period.

WildFire Analysis

- Clone the default Profile and modify as necessary:

Objects > Security Profiles > WildFire Analysis



WildFire Analysis Profile

Name: default-1

Description:

1 item

□	Name	Applications	File Types	Direction	Analysis
□	default	any	any	both	public-cloud

The recommended WildFire Analysis Profile sends all files in both directions (upload and download) to WildFire for analysis. Specifically make sure that you are sending all PE files (if you are not blocking them per the file blocking recommendation), Adobe Flash and Reader files (PDF, SWF), Android files (.APK), Java files (Java, .CLASS), and Microsoft Office files (PowerPoint, Excel, Word, RTF).

Migration guidelines

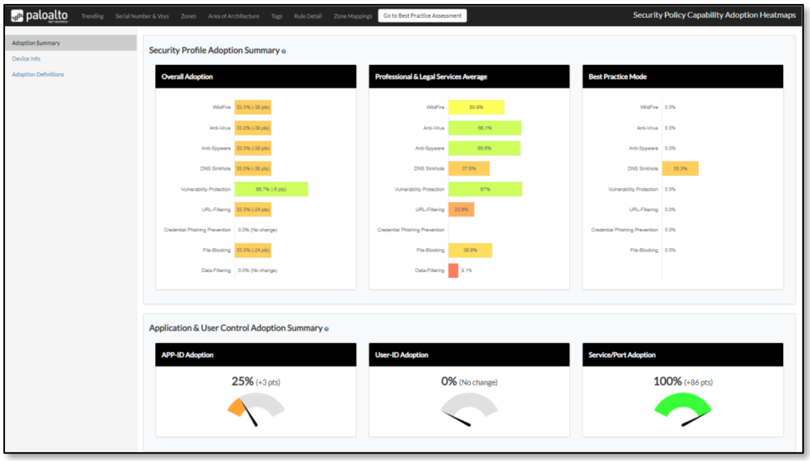
Analyzing ACC information

Optimizing security profiles

Heatmap and Best Practice Assessment (BPA)

Heatmap and Best Practice Assessment Tool

- Online tools compare your firewall configuration with industry standards.
- Online tool available through the customer support portal
- Provide reports to show what currently meets recommended best practices
- Provide recommendations to bring the firewall up to recommended best practices



Security Policy Capability Adoption Heatmaps

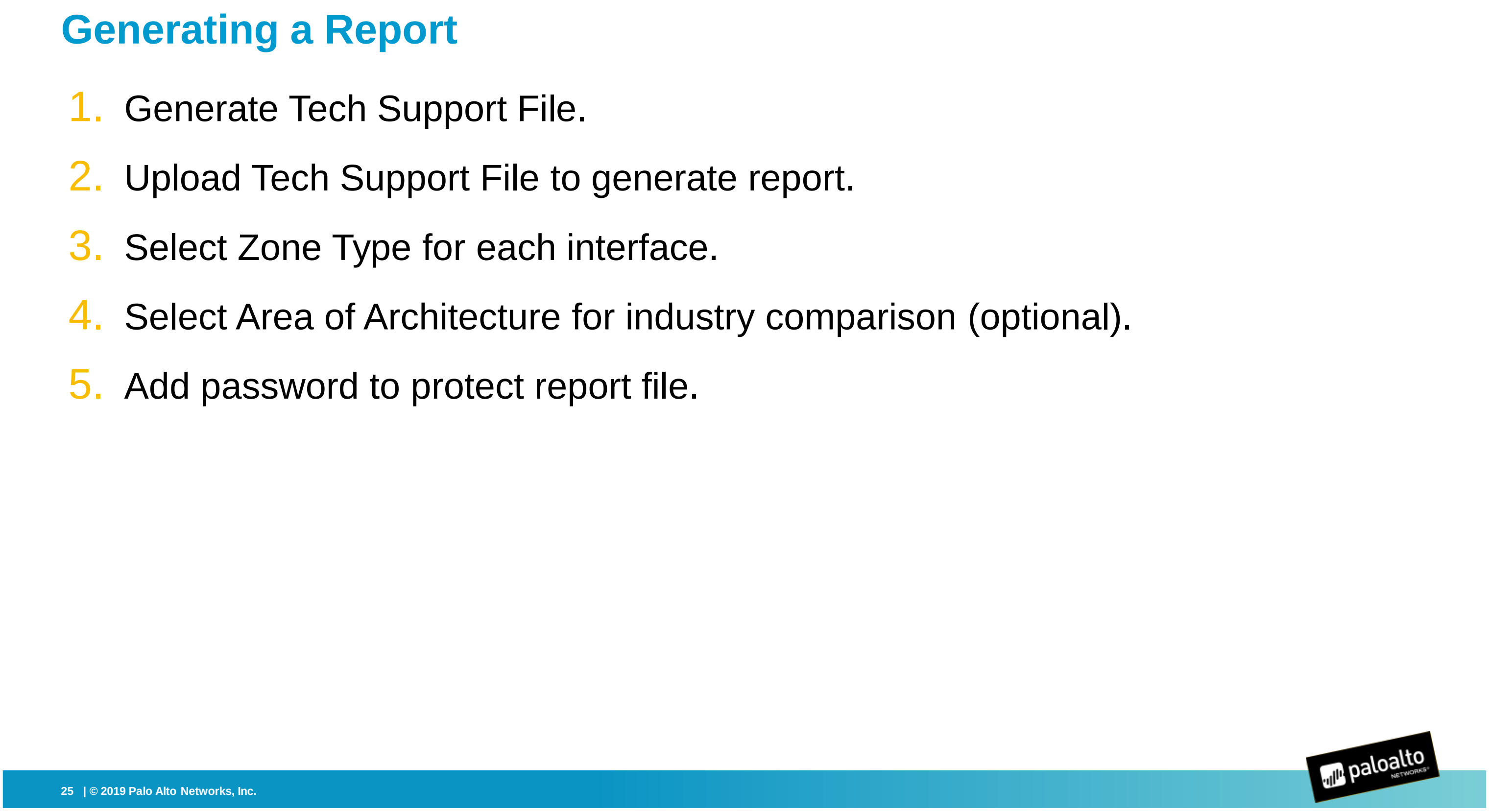
Security Profile Adoption Summary

	Overall Adoption	Professional & Legal Services Average	Best Practice Mode
WildFire	33.3% (-38 pts)	50.9%	0.0%
Anti-Virus	33.3% (-38 pts)	66.1%	0.0%
Anti-Spyware	33.3% (-38 pts)	65.6%	0.0%
DNS Sinkhole	33.3% (-38 pts)	37.6%	33.3%
Vulnerability Protection	66.7% (-5 pts)	67%	0.0%
URL-Filtering	33.3% (-24 pts)	23.6%	0.0%
Credential Phishing Prevention	0.0% (No change)		0.0%
File-Blocking	33.3% (-24 pts)	39.9%	0.0%
Data-Filtering	0.0% (No change)	9.1%	

Application & User Control Adoption Summary

APP-ID Adoption	User-ID Adoption	Service/Port Adoption
25% (+3 pts)	0% (No change)	100% (+86 pts)

Security Policy Capability Adoption Heatmap, or Heatmap, and Best Practice Assessment, or BPA, are tools that compare your firewall's current configuration with those of other companies within the same or similar industry and provide recommended best practices for a Palo Alto Networks firewall. The Heatmap and BPA reports help you to validate that your current configuration is configured as you intended. Each report provides multiple views to help you better understand where some of your security gaps might be and recommendations about how to fill those gaps. Heatmap and BPA are available through the Customer Support Portal.



Generating a Report

1. Generate Tech Support File.
2. Upload Tech Support File to generate report.
3. Select Zone Type for each interface.
4. Select Area of Architecture for industry comparison (optional).
5. Add password to protect report file.

A Heatmap and/or BPA report require you to generate a Tech Support File directly from your firewall or through Panorama. To generate a Tech Support File on the firewall, navigate to **Device** > **Support** > **Tech Support File** and click the **Generate Tech Support File** link. After the Tech Support File has been generated, click the **Download Tech Support File** link and save the file locally for uploading to the Heatmap and the BPA online tools.

The **Zone Type** mapping enables you to define which zone type each zone is part of. Your choices are **Internal**, **Internal Strict**, or **External**. The default value is set to **Internal**.

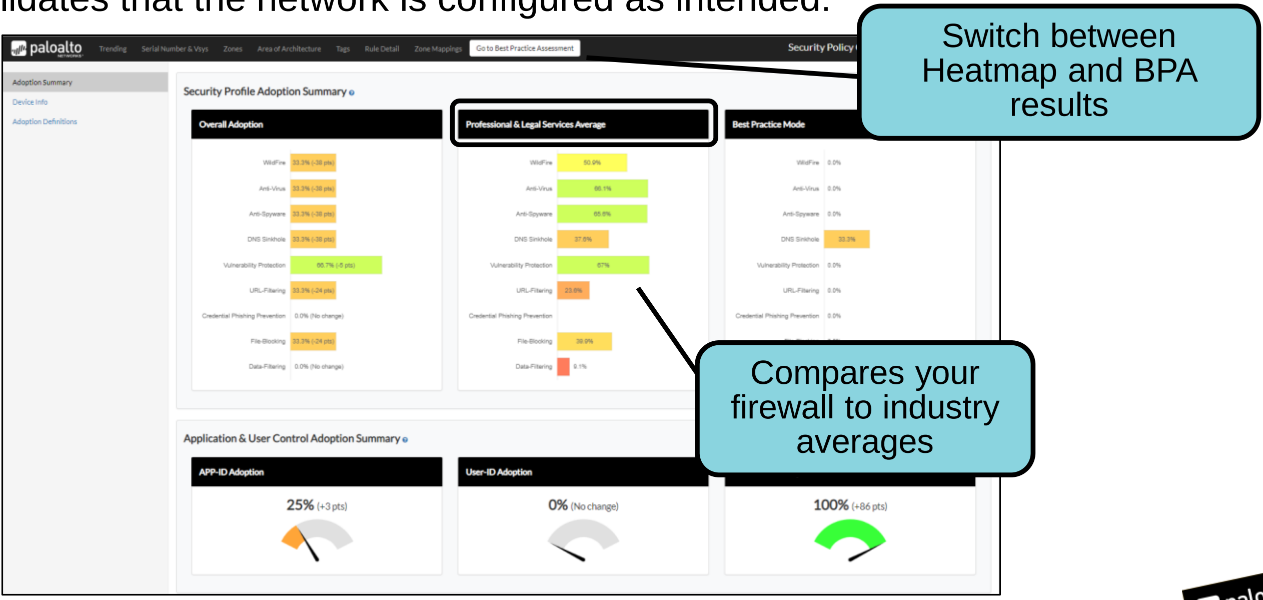
The **Area of Architecture** mapping enables you to map each zone to how that zone is being accessed. Your choices are **Perimeter Internet**, **Internal Core**, **Remote Office**, **Data Center North South**, **Data Center East West**, **Cloud, Guest/BYOD**, **3rd Party/Vendors**, and **Remote Users/VPN**. The default value is set to **Perimeter Internet**.

The **Area of Architecture** enables you to compare your firewall configuration to a specific industry type, such as Healthcare. This step is optional and can be disabled.

The last task to perform is to specify an email address where your report will be sent and add an additional layer of security to your report by password-protecting your report file.

Heatmap Report

- Measures percentage of “allow” rules to identify where capabilities are used
- Validates that the network is configured as intended:



Security Profile Adoption Summary

Overall Adoption	
WildFire	33.3% (-38 pts)
Anti-Virus	33.3% (-38 pts)
Anti-Spyware	33.3% (-38 pts)
DNS Sinkhole	33.3% (-38 pts)
Vulnerability Protection	66.7% (-5 pts)
URL-Filtering	33.3% (-24 pts)
Credential Phishing Prevention	0.0% (No change)
File-Blocking	33.3% (-24 pts)
Data-Filtering	0.0% (No change)

Professional & Legal Services Average	
WildFire	50.9%
Anti-Virus	66.1%
Anti-Spyware	65.6%
DNS Sinkhole	37.6%
Vulnerability Protection	67%
URL-Filtering	23.6%
Credential Phishing Prevention	
File-Blocking	39.9%
Data-Filtering	9.1%

Best Practice Mode	
WildFire	0.0%
Anti-Virus	0.0%
Anti-Spyware	0.0%
DNS Sinkhole	33.3%
Vulnerability Protection	0.0%
URL-Filtering	0.0%
Credential Phishing Prevention	0.0%

Application & User Control Adoption Summary

APP-ID Adoption	User-ID Adoption	
25% (+3 pts)	0% (No change)	100% (+86 pts)

Switch between Heatmap and BPA results

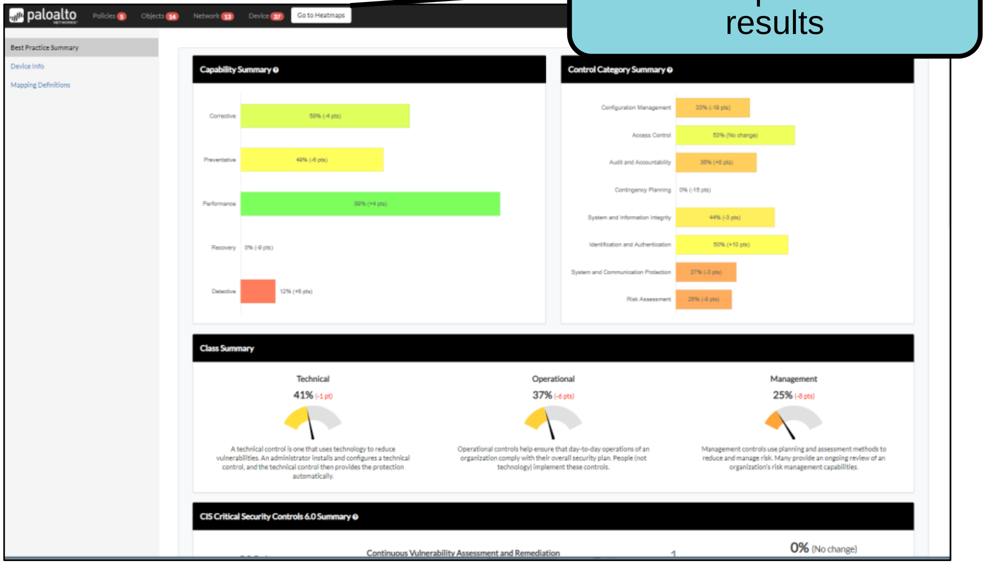
Compares your firewall to industry averages

The Heatmap report is designed to show you which percentage of your enabled prevention profiles have been adopted per rule to help you identify gaps that may be in your configuration. The Heatmap tool analyzes your configuration and measures how your current firewall settings compare to those from other companies within the same or similar industry.

Use the **Go to BPA** button on the top right of the menu bar to access the BPA report.

BPA Report

- Compares your firewall with recommended best practices
- Results show either pass or fail:


paloalto NETWORKS
Policies 5
Objects 14
Network 13
Device 37
Go to Heatmaps
Best Practice Summary
Device Info
Mapping Definitions
Capability Summary
Corrective 58% (-4 pts)
Preventative 49% (-6 pts)
Performance 80% (+4 pts)
Recovery 0% (-9 pts)
Detective 12% (+6 pts)
Control Category Summary
Configuration Management 33% (-19 pts)
Access Control 53% (No change)
Audit and Accountability 36% (+8 pts)
Contingency Planning 0% (-15 pts)
System and Information Integrity 44% (-3 pts)
Identification and Authentication 50% (+10 pts)
System and Communication Protection 27% (-3 pts)
Risk Assessment 25% (-8 pts)
Class Summary
Technical 41% (-1 pt)
Operational 37% (-6 pts)
Management 25% (-8 pts)
CIS Critical Security Controls 6.0 Summary
Continuous Vulnerability Assessment and Remediation
1
0% (No change)

A technical control is one that uses technology to reduce vulnerabilities. An administrator installs and configures a technical control, and the technical control then provides the protection automatically.

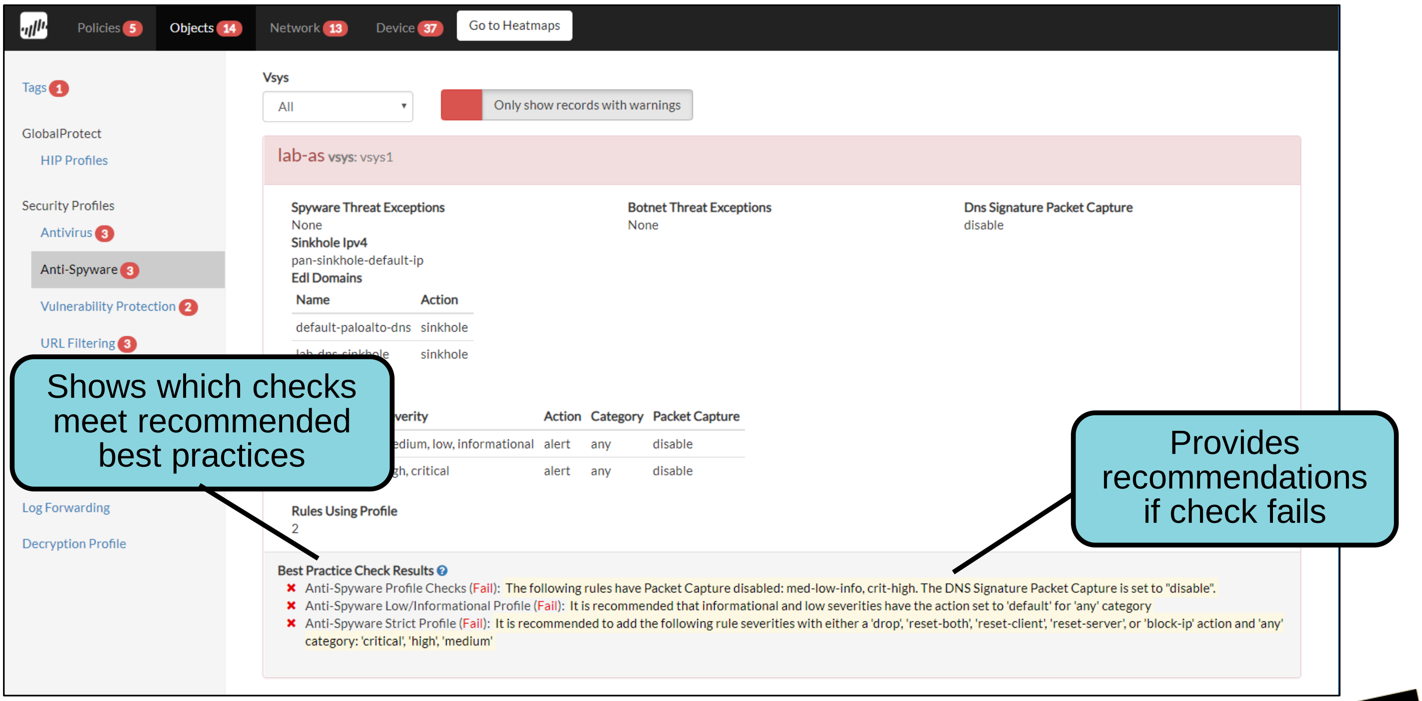
Operational controls help ensure that day-to-day operations of an organization comply with their overall security plan. People (not technology) implement these controls.

Management controls use planning and assessment methods to reduce and manage risk. Many provide an ongoing review of an organization's risk management capabilities.

Switch between Heatmap and BPA results

Best practices are the recommended configuration settings for your firewall that helps you combat attacks. The BPA report shows how your current configuration compares to Palo Alto Networks recommendations, and the results show either a pass or fail. A pass means that the current configuration parameters meet the recommended best practices. Recommendations show you how you can reconfigure your firewall to meet the best practices.

Best Practices Check Results



Policies 5 | Objects 14 | Network 13 | Device 37 | Go to Heatmaps

Tags 1

GlobalProtect
HIP Profiles

Security Profiles
Antivirus 3
Anti-Spyware 3
Vulnerability Protection 2
URL Filtering 3

Log Forwarding

Decryption Profile

Vsys: All ▾ | Only show records with warnings

lab-as vsys: vsys1

Spyware Threat Exceptions
None
Sinkhole Ipv4
pan-sinkhole-default-ip
Edl Domains

Name	Action
default-paloalto-dns	sinkhole
lab-dns-sinkhole	sinkhole

Botnet Threat Exceptions
None

Dns Signature Packet Capture
disable

verity	Action	Category	Packet Capture
edium, low, informational	alert	any	disable
gh, critical	alert	any	disable

Rules Using Profile
2

Best Practice Check Results

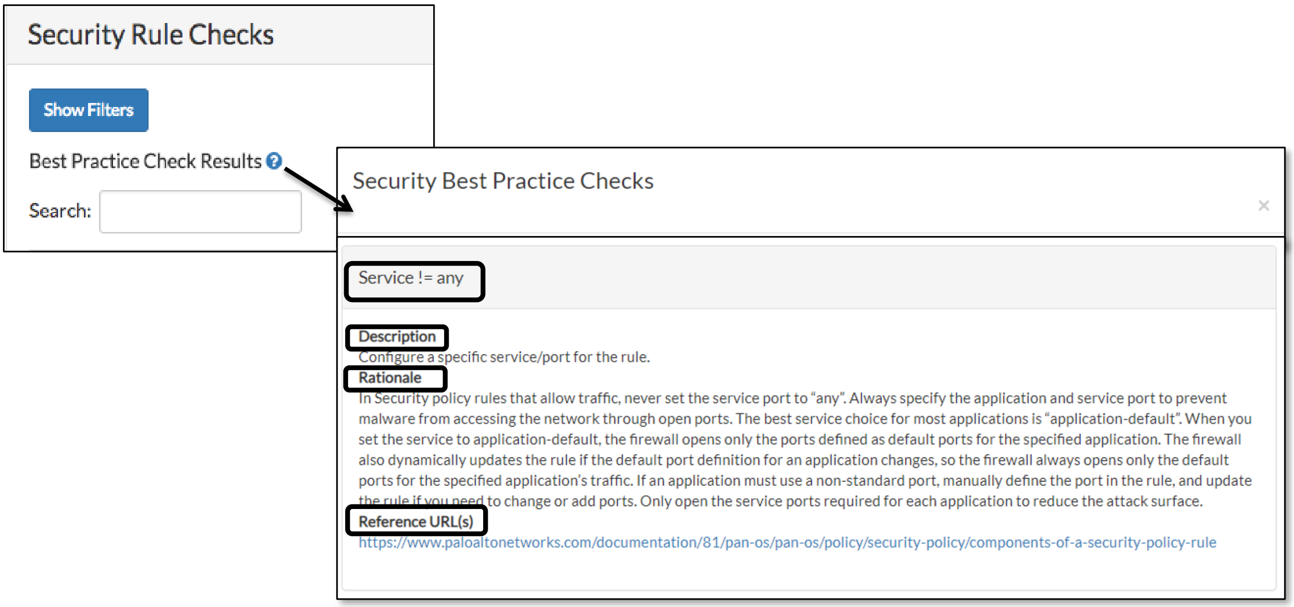
- ✗ Anti-Spyware Profile Checks (Fail): The following rules have Packet Capture disabled: med-low-info, crit-high. The DNS Signature Packet Capture is set to "disable".
- ✗ Anti-Spyware Low/Informational Profile (Fail): It is recommended that informational and low severities have the action set to 'default' for 'any' category
- ✗ Anti-Spyware Strict Profile (Fail): It is recommended to add the following rule severities with either a 'drop', 'reset-both', 'reset-client', 'reset-server', or 'block-ip' action and 'any' category: 'critical', 'high', 'medium'

Shows which checks meet recommended best practices

Provides recommendations if check fails

Numbers in red in the report indicate an area that has failed a best practice check.

BPA Check Criteria



Security Rule Checks

Best Practice Check Results

Search:

Security Best Practice Checks

Service != any

Description

Configure a specific service/port for the rule.

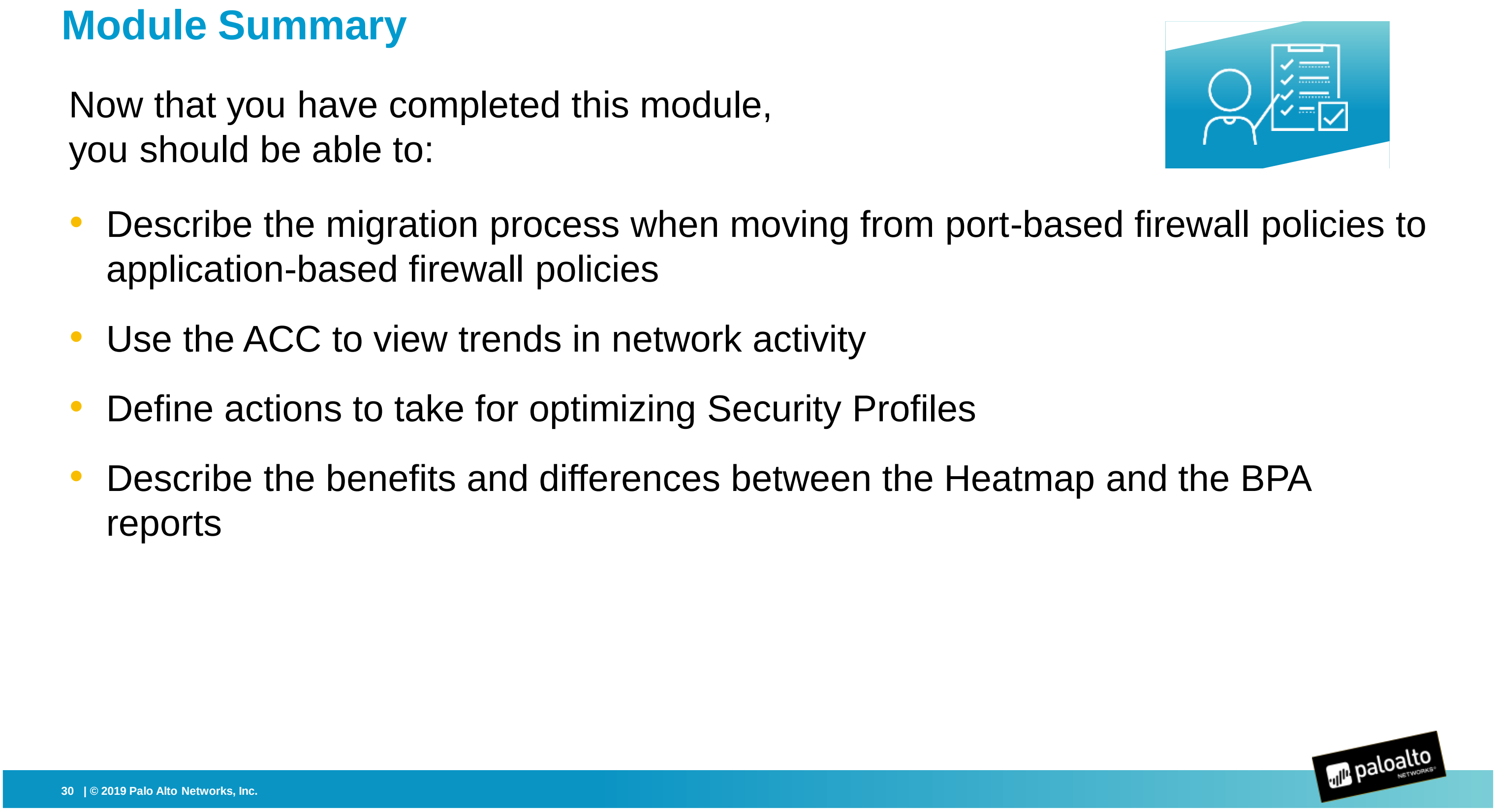
Rationale

In Security policy rules that allow traffic, never set the service port to "any". Always specify the application and service port to prevent malware from accessing the network through open ports. The best service choice for most applications is "application-default". When you set the service to application-default, the firewall opens only the ports defined as default ports for the specified application. The firewall also dynamically updates the rule if the default port definition for an application changes, so the firewall always opens only the default ports for the specified application's traffic. If an application must use a non-standard port, manually define the port in the rule, and update the rule if you need to change or add ports. Only open the service ports required for each application to reduce the attack surface.

Reference URL(s)

https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/policy/security-policy/components-of-a-security-policy-rule

The BPA report also provides details about which information is shown in your report. After you select the **?** icon, you can see what was tested, the rationale behind the recommendations, and a link to provide additional resources or to provide a how-to document to help with implementation.



Module Summary

Now that you have completed this module,
you should be able to:

- Describe the migration process when moving from port-based firewall policies to application-based firewall policies
- Use the ACC to view trends in network activity
- Define actions to take for optimizing Security Profiles
- Describe the benefits and differences between the Heatmap and the BPA reports

30 | © 2019 Palo Alto Networks, Inc.

Now that you have completed the module, you should be able to:

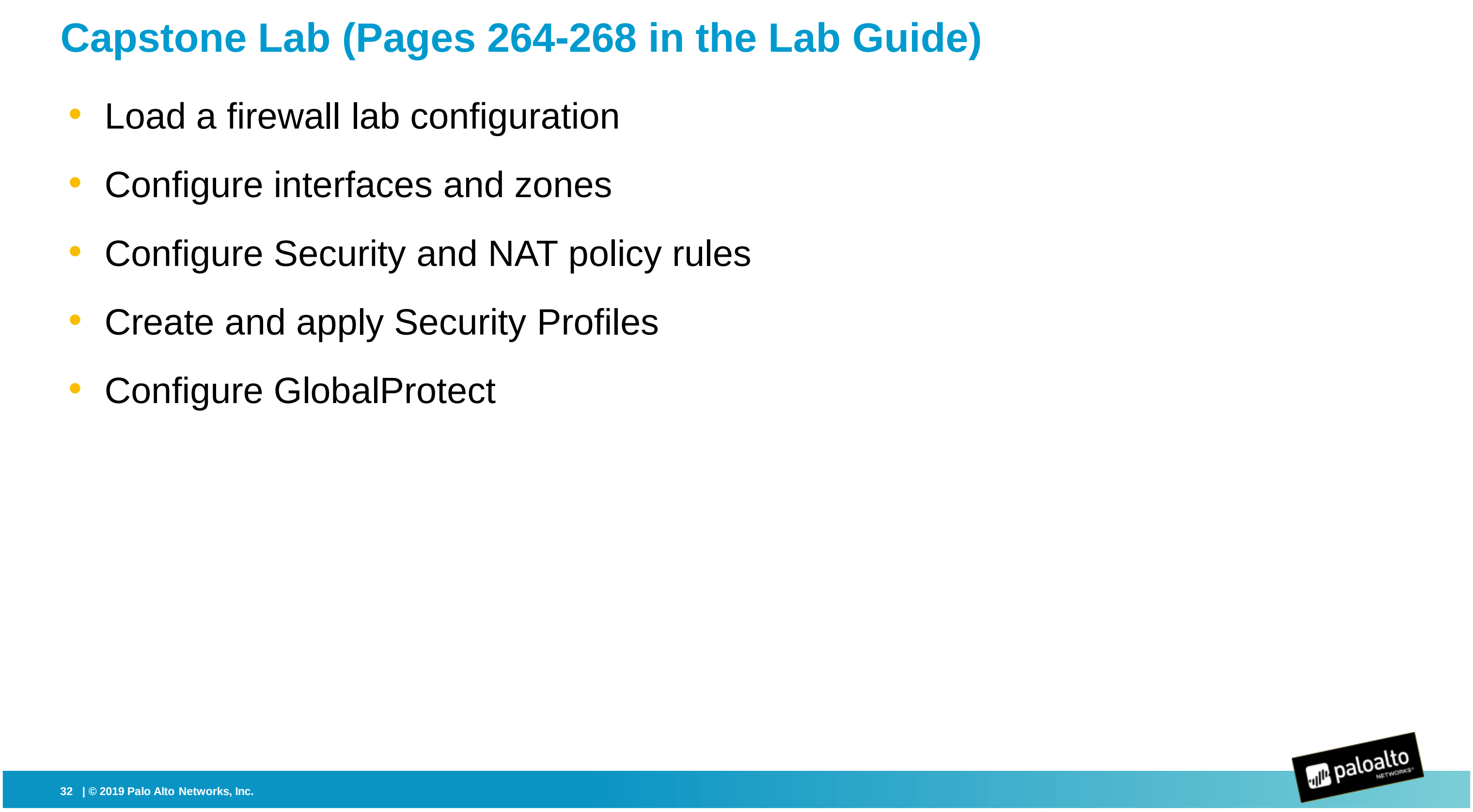
- Describe the migration process when moving from port-based firewall policies to application-based firewall policies
- Use the Application Command Center, or ACC, to view trends in network activity
- Define actions to take for optimizing Security Profiles
- Describe the benefits and differences between the Heatmap and the BPA reports

Questions?

31 | © 2019 Palo Alto Networks, Inc.

Review Questions

1. Which phase is *not* one of the three phases used in a migration from port-based firewall policies to application-based firewall policies?
   a. Application Visibility
   b. Baseline Visibility
   c. Consolidate, Customize, and Reduce Risk
   d. Next-Generation Policies
2. Which tab in the ACC provides an overview of traffic and user activity on your network?
   a. Tunnel Activity
   b. Blocked Activity
   c. Network Activity
   d. Threat Activity
3. You should set all category actions to which level when you create a new URL Filtering Profile?
   a. alert
   b. block
   c. continue
   d. allow
4. True or false? Heatmap and BPA are online tool available only to partners and employees.
   a. true
   b. false
5. To create a Heatmap and BPA report, which type of file would you need to create and download from the firewall?
   a. Stats Dump File
   b. Config File saved in XML format
   c. Config File saved in CSV format
   d. Tech Support File



Capstone Lab (Pages 264-268 in the Lab Guide)

- Load a firewall lab configuration
- Configure interfaces and zones
- Configure Security and NAT policy rules
- Create and apply Security Profiles
- Configure GlobalProtect

PROTECTION. DELIVERED.

Answers to Review Questions

1. b
2. c
3. a
4. a (true)
5. d

This page intentionally left blank