

# **Tenable for Palo Alto Networks**

### Introduction

This document describes how to deploy Tenable SecurityCenter<sup>®</sup> and Nessus<sup>®</sup> for integration with Palo Alto Networks next-generation firewalls (NGFW). Please email any comments and suggestions to <u>support@tenable.com</u>.

Monitoring the security settings of your Palo Alto Networks firewalls is critical for maintaining your network's security posture. Unless your vulnerability management (VM) platform is equipped with configuration assessment checks specifically designed for Palo Alto firewalls, your network may be exposed to unnecessary risk.

Additionally, better VM platforms offer continuous listening through passive vulnerability monitoring to help bridge the vulnerability intelligence gap in between periodic active scans and audits. However, placing passive monitors on every network segment throughout a global enterprise can be impractical. Although more organizations are turning to SIEMs (security information and event management) to uncover hidden threats, most SIEMs take months to deploy and are costly to acquire and maintain.

Benefits of integrating Tenable SecurityCenter with Palo Alto Networks include:

- Maintain compliance with industry best practices for firewall hardening
- Achieve real-time, 100% asset discovery by detecting new hosts connected to network segments not monitored by Tenable Passive Vulnerability Scanner<sup>®</sup> (PVS<sup>™</sup>)
- Discover system vulnerabilities and security misconfigurations of mobile devices and virtual machines not present during the last periodic full-network scan
- Maintain compliance with government and industry regulations that mandate log aggregation, such as PCI, HIPAA, FISMA, and more
- Uncover advanced cyberthreats by correlating Palo Alto firewall log data against log data from other network and security devices

### **Integration Overview**

SecurityCenter and Nessus offer a series of plugins specifically designed to audit Palo Alto Networks physical and virtual NGFWs to identify security misconfigurations and ensure best-practice hardening guidelines are followed. To perform the audit, SecurityCenter (via Nessus) initiates a credentialed scan of the Palo Alto NGFW, authenticating credentials through the Palo Alto XML API. Once completed, detailed findings of the Palo Alto audit can be reviewed within SecurityCenter scan results, dashboards, and reports.

In addition to configuration audits, Tenable can also import real-time log data from Palo Alto NGFWs into its Log Correlation Engine<sup>®</sup> (LCE<sup>®</sup>) to help identify assets on networks not monitored by Tenable PVS. Once hosts are identified they can be

automatically assigned to dynamic asset lists and audited with Nessus to detect any possible vulnerabilities or misconfigurations.

Tenable LCE also allows the log data gathered from Palo Alto NGFWs to be accessed and correlated against other network and security data sources to help uncover hidden cyberthreats and maintain compliance with government and industry regulations.



Nessus Manager version 6.x, Tenable.io, and SecurityCenter and SecurityCenter Continuous View version 4.8 and higher support Palo Alto Networks integration. Nessus, Tenable.io, and SecurityCenter solutions work with Palo Alto Networks PAN-OS versions 4.x through 7.x.

## Integrating with Palo Alto Networks

### Palo Alto NGFW Configuration Audit

Integrating SecurityCenter and Palo Alto to perform audit checks requires configuration in both SecurityCenter and PAN-OS.

Within PAN-OS, the following configuration tasks are required:

- Create a service account for SecurityCenter
- Grant SecurityCenter access to the PAN-OS management interface
- Configure SNMP to be allowed by local security policies

For detailed instruction on configuring PAN-OS for integration please refer to the Palo Alto PAN-OS Administrator's Guide.

Once the configuration steps for PAN-OS are complete, log in to SecurityCenter, click "Scans", and select "Audit Files".

Security	Center	Das	shboard 🔻	Analysis 🗸	Scans - Report	ing 🗸
Executi		21/			Active Scans	
LXECUII	verD	Agent Scans				
					Scan Results	
Executive 7 D	ay - Current	√ulnerability 1	ype Matrix		Policies	utive 7
	Total	Active	Passive	Compliance	Audit Files	
Critical	0	0	0	N/A	Credentials	·itical
High	0	0	0	0	Blackout Windows	ligh
Medium	0	0	0	0	Diackout Windows	dium

Click "+Add" and select "Palo Alto Networks PAN-OS" from the list of available audit file templates.

SecurityCenter	Dashboard <del>-</del>	Analysis <del>▼</del> Scans <del>▼</del>	Reporting - Assets	Workflow    Users
Add Audit File				
Templates				
Adtran NetVanta	BlueCoat ProxySG	Brocade FabricOS	Check Point GAiA	Cisco IOS
Extreme ExtremeXOS	FireEye	FortiGate FortiOS	HP ProCurve	Huawei VRP
NetApp Data ONTAP	Palo Alto Networks PAN-OS	RHEV	SonicWALL SonicOS	Unix
Windows File Contents				
Custom				
Advanced Create a custom audit file.				

In the "General" section, enter a name for the audit file and a description (optional).

SecurityCenter	Dashboard <del>-</del>	Analysis 🗸	Scans 🕶	Reporting <del>-</del>	Assets	Workflow <del>-</del>	Users <del>-</del>
Edit Palo Alto Au	ıdit File						
	General						
	Name*	Tenable_Palo	_Alto_Best P	ractices_Audit			
	Description	The Tenable/P Practices Aud	Palo Alto PAN it File	-OS Best			
				li			
			_				

Configure each option within the "Compliance Checks" section. Each option will be pre-populated by default. The info contains default values set in the audit database. The information will need to be customized for each environment.

Once the "Compliance Checks" configuration is complete, click "Submit".

FW config timestamp*	2013/10/09 14:59:07/04	
Primary DNS server*	8.8.8.8	
Primary NTP server*	0.pool.ntp.org	
SW update server*	updates.paloaltonetworks.com	
Secondary DNS server*	8.8.4.4	
Secondary NTP server*	1.pool.ntp.org	
Time zone*	US/Central	
Time zone*	US/Central	

The table below contains a description of each "Compliance Checks" option:

#### Table 1: Compliance Checks Options

Option	Description
FW config timestamp	Firewall configuration timestamp of the Palo Alto Networks device
Primary DNS server	Primary DNS server (Domain Name Server) of the Palo Alto Networks device
Primary NTP server	Primary NTP (Network Time Protocol) server of the Palo Alto Networks device
SW update server	The content update URL for Palo Alto Networks devices. The recommended setting is "updates.paloaltonetworks.com".
Secondary DNS server	Secondary DNS server (Domain Name Server) of the Palo Alto Networks device
Secondary NTP server	Secondary NTP (Network Time Protocol) server of the Palo Alto Networks device
Time zone	Time zone of the Palo Alto Networks device

#### Click "Credentials" and click "+Add".

Active Scans Agent Scans Scan Results Policies Audit Files Credentials Blackout Windows   Name • Type Group   Tenable_Palo_Alto_Best Practices_Audit Palo Alto 1.15 Full Access	SecurityCenter	Dashboard <del>-</del>	Analysis <del>-</del>	Scans 🗸	Reporting <del>-</del>	Assets	Workflow <del>-</del>	Users 🗸
Active Scans       Agent Scans       Scan Results       Policies       Audit Files       Credentials       Blackout Windows         Name •       Type       Group         Tenable_Palo_Alto_Best Practices_Audit       Palo Alto 1.15       Full Access	Audit Files							
Name     Type     Group       Tenable_Palo_Alto_Best Practices_Audit     Palo Alto 1.15     Full Access	Active Scans Agent Scans	Scan Results	Policies	Audit Files	Credentials	Black	out Windows	
Tenable_Palo_Alto_Best Practices_Audit     Palo Alto 1.15     Full Access	Name 🔺				Туре		Group	
	Tenable_Palo_Alto_Best Practices	_Audit			Palo Alto 1.15		Full A	ccess

In the "General" section, enter a name for the SNMP credentials and a description (optional). Under the "Credential" section, click the drop-down and select "**SNMP**". In the "Community" box, enter the SNMP community string. Click "**Submit**".

SecurityCenter	Dashboard <del>-</del>	Analysis <del>-</del>	Scans 🕶	Reporting <del>-</del>	Assets	Workflow <del>-</del>	Users <del>-</del>
Edit Credential							
	General						
	Name*	PAN-OS_SN	MP_Credenti	als			
	Description	PAN-OS SNI	MP Credentia	ls	]		
				,	4		
	Credentia	l					
	Туре	SNMP					
	Community*	public					
	Culumit Co	nool					
	Supmit						

To create the scan policy, click "Policies" and then click "+Add".

SecurityCer	iter	Dashboard <del>-</del>	Analysis <del>-</del>	Scans <del>-</del>	Reporting <del>-</del>	Assets	Workflow <del>-</del>	Users <del>-</del>
Credentials	i							
Active Scans A	gent Scans	Scan Results	Policies	Audit Files	Credentials	Black	out Windows	
Name				Туре	)	Group		
PAN-OS_SNMP_Crea	lentials			SNM	IP	Full Acc	ess	



In the "Setup" section, enter a name for the audit policy and a description (optional). The options under "Configuration" can be left as "Default" or set to "Custom". If the configuration options are set to "Custom", the "Advanced" and "Host Discovery" categories will be enabled in the left-hand menu. Leaving the options as "Default" will keep those items hidden.

SecurityCenter Dashboard - Ana	lysis ▼ Scans ▼	Reporting <del>-</del> Assets	Workflow - Users -
Add Policy > Policy Compliand	ce Auditing	3	
Setup	General		
Host Discovery	Name*	PAN-OS_Audit_Policy	
Report	Description	PAN-OS_Audit_Policy	
Advanced			le la
Authentication			
Compliance	Configura	tion	
	Advanced	Custom 👻	Choose your own advanced settings. Choose your own discovery settings.
	Discovery	Custom 👻	
_		Default Custom	
Submit Cancel			

Select the "Policy Compliance Auditing" template.

Navigate to the "Authentication" section, and click "**+Add Authentication Settings**". Under the "Authentication" section, click the drop-down next to "**Type**" and select "**Miscellaneous**". Click the second drop-down and select "**Palo Alto Networks PAN-OS**" and then click "**Select**".

SecurityCenter Dashboard Add Policy > Policy Complian	nalysis - Scans - Reporting - Assets Workflow - Users -
Setup Host Discovery Report Advanced	Authentication Type Miscellaneous  Palo Alto Networks PAN-OS  Select You may add 1 more
Authentication	SNMP
	UDP port*     161       Additional UDP port #1*     161       Additional UDP port #2*     161
	Additional UDP port #3* 161

SNMP ports default to port 161. Configure ports to correspond to SNMP port settings in PAN-OS.

In the "Authentication" section, enter the "**Username**" and "**Password**" to allow SecurityCenter to authenticate to PAN-OS. Specify the "**Port**" (default is 443) and enable or disable "**Verify SSL Certificate**" (enabled by default). Click the checkmark to finalize the settings.

SecurityCenter Dashboard - Add Policy > Policy Comp	Analysis - Scans - Reporting - Assets Workflow - Users -	
Setup	Authentication	
Host Discovery	Username* Palo_Alto_Username	
Report	Password*	
Advanced	Port* 443	
Authentication	Verify SSL Certificate	
Compliance		✓ ×

Navigate to the "Compliance" section and click "+Add Audit File". In the "Compliance" section, click the "Select a Type" dropdown and select "Palo Alto". Next, click the "Select an Audit File" drop-down and select the previously configured Palo Alto audit file. Click the checkmark to finalize the settings.

SecurityCenter <sup>®</sup> Dashboard + Add Policy > Policy Complia	Analysis - Scans - Reporting - Assets Workflow - Users - ance Auditing	
Setup	Compliance	
Host Discovery	Palo Alto 💌 Tenable_Palo_Alto_Best Practices_Audit 💌	✓ ×
Report		
Advanced		
Authentication		
Compliance		
Submit Cancel		

To create an audit scan of Palo Alto NGFWs, click on "Scans" and select "Active Scans". Click on "+Add".

In the "General" section, enter a scan name and description (optional). Click the "**Select a Policy**" drop-down and select the previously configured Palo Alto audit policy. In the "Schedule" section, the scan can be configured to run "On Demand" (default), or it can be configured to run on a custom schedule as required.

SecurityCenter	Dashboard 🕶	Analysis 🔻	Scans 🔻	Reporting -	Assets	Workflow 🔫	Users 🗸
Add Active Scan							
	General			General			
	Settings			Name*	PAN-OS_S	can	
	Targets			Description	PAN-OS_S	can	
	Credentials						
	Post Scan			Policy*	PAN-OS_A	udit_Policy 🔻	
				Schedule			
				Schedule Or	Demand 🖋		
	Submit C	ancel					

Navigate to the "Targets" section and click the "**Target Type**" drop-down. Select "**IP/DNS Name**" and enter the Palo Alto NGFW IP address or DNS name.

SecurityCenter	Dashboard 🗸 🛛 Analysis 🖣	Scans ▼ Reporting ▼ Assets Workflow ▼ Users ▼
Add Active Scan		
	General Settings	Target Type IP / DNS Name  IPs / DNS Names* 172.1.1
	Targets	
	Credentials Post Scan	
	Submit Cancel	

Navigate to "Credentials" and click "+ Add Credential". Click the drop-down and select "SNMP". Once SNMP is selected, a second drop-down box will appear. Click the box and select the previously configured SNMP credentials for PAN-OS. Click the checkmark to finalize the settings.

SecurityCenter	Dashboard 👻 Analysis	s Scans Reporting Assets Workflow Users	
Add Active Scan			
	General	Scan Credentials	
	Settings	SNMP V PAN-OS_SNMP_Creden Vou may add 4 more SNMP credentials.	
	Targets		
	Credentials		
	Post Scan		
	Submit Cancel		

### Importing Palo Alto NGFW Logs

Real-time log data from Palo Alto NGFWs can be imported into SecurityCenter (via LCE). Integration requires configuration changes within PAN-OS and within SecurityCenter, as well as the installation and configuration of Tenable NetFlow Monitor.

Within PAN-OS, the following configuration tasks are required:

- Configure Tenable Log Correlation Engine (LCE) as a syslog server
- Enable log forwarding to LCE
- Permit and Deny policy configuration
- Define NetFlow server IP address and port

For detailed instruction on configuring PAN-OS for integration please refer to the Palo Alto PAN-OS Administrator's Guide.

Once the PAN-OS configuration tasks are complete, download the Tenable NetFlow Monitor LCE client from the Tenable Support Portal.

Install the Tenable NetFlow Monitor LCE client. Please refer to the Log Correlation Engine 4.4 Client Guide for detailed installation instructions.

The Tenable NetFlow Monitor LCE client can be run directly on the LCE server. It must be configured to connect to either the localhost (127.0.0.1) or the IP address of the LCE server. Multiple LCE Client types (such as the LCE Log Agent and the Tenable NetFlow Monitor) can be run at the same time as well.

Log in to SecurityCenter using an admin account and navigate to "Resources" and select "LCE Clients".

SecurityCenter	Dashboard	Resources ▼ Repositories ▼
Overview		Nessus Scanners Scan Zones
System Status		Passive Vulnerability Scanners
Job Daemon Running	Start Stop	LCE Clients
Scanner Status		

Click the drop-down arrow to the right of the "**netflowclient**" and select "**Authorize**". If successful, a pop-up message stating it has been successfully authorized will appear.

saus Scances       Scan Zones       Passive Vulnenability Scannes       Log Correlation Engines       LCE Lines       CE Client P       Policy       Policy       State       Version       Last Upd-term         Name         Client P       OS       Type       Policy       State       Version       Last Upd-term       Imperturbation       Never       Imperturbation       Never       Imperturbation       Imperturbation       Never       Imperturbation       Imperturbation       Never       Imperturbation       Imperupation       Imperupation	CE Clients								
Name         Client IP         OS         Type         Policy         State         Version         Last Update           172 26 37.17         rhel         netfloxclient log         Alive         v4.2.0.0         Never         Image: Client log         Image: C	essus Scanners Scan Zones Passive Vulnerability Scanners	Log Correlation Engines	LCE CI	ents LCE Client P	Policies				< T
172.26.37.17 rhei nettiowcient defauit_rhei_nettiowcient.kp Aiwe v4.2.0 Never to view the second sec	Name	Client IP	OS	Туре	Policy	State	Version	Last Updated	
View Edit Authorize	Š	172.26.37.17	rhel	netflowclient	default_rhel_netflowclient.lcp	Alive	v4.2.0.0	Never	0.*
Edit Authorize								Vie	3W
Authorize								Ed	it
								Au	thorize

Click on the "**netflowclient**" to edit the LCE client and assign a policy. Click the "**Policy**" drop-down to select the desired policy. Click "**Submit**". If successful, a pop-up message stating "LCE Client Edited Successfully" will appear.

SecurityCenter	Dashboard	Resources 🕶	Repositories 🕶	Organizations	Users 🕶	Scanning 🕶	System <del>-</del>
Edit LCE Client							
		Name* Policy*	default_rhel_n	etflowclien 👻			
		Submit	Cancel				
					-		-

Once configured, log data from the Palo Alto NGFW will be imported into SecurityCenter to help achieve 100% asset discovery. The log data can also be correlated against other data sources to uncover any potential advanced threats and to help organizations meet compliance obligations.

## Dashboards and Reports

Information obtained through Palo Alto NGFW configuration audits and the collection of log data can be easily viewed and analyzed through SecurityCenter's pre-defined, customizable dashboards and reports.

Alto Networks PAN-OS Audit Results - Compliance	Summary			Palo Alto Networks F	AN-OS Audit Results - Audit Check Subnet Summar	ry .		
Check Count	Passed 23	Manual Check	Failed 6	26 26 26	Midun		E High	
System Ratio	82% 1 100%	0	18% 1 100%	22 23 18 16 14				
pdated: 3 minutes ago				13 16				
Nto Networks PAN-OS Audit Results - 90 Day Con	npliance Summary			2		172.350.004 Dev Repository		
				Last Updated: 3 minut	as ago			
				Palo Alto Networks F	AN-OS Audit Results - Top 50 Manual Audit Checks			
				Plugin ID	Name	Severity	Host Total	
dated: 3 minutes ago to Networks PAN-OS Audit Results - Audit Sumr	nary		■ Offical ■ Color ■ Color ■ Color ■ Color ■ Offical ■ Offical	Last Updated: 3 minut	16 BQO			
				Palo Alto Networks F	AN-OS Audit Results - Top 50 Failed Audit Checks			
				Palo Alto Networks P Plugin ID	AN-OS Audit Results - Top 50 Failed Audit Checks Name		Severity	Host Total
dated: 3 minutes ago				Palo Alto Networks P Plugin ID 1001832	AN-OS Audit Results - Top 50 Failed Audit Checks Name Palo Ato - Datect Config Change'		Severity High	Host Total
datest: 3 minutes ago				Palo Alto Networks F Plugin ID 1001832 1001831	AN-OS Audit Results - Top 50 Failed Audit Checks Name Paio Ato - Datect Config Change' Paio Ato Security Settings - 'secondary DNS serv	er has been configured'	Severity High	Host Total
denci 3 minutes ago				Palo Alto Networks F Plugin ID 1001832 1001831 1001830	AN-OS Audit Results - Top 50 Pailed Audit Checks Name Paio Ato - Detect Config Change' Paio Ato Securty Settings - 'secondary DNS server Paio Ato Securty Settings - 'primary DNS server	er has been configured" has been configured	Severity High High	Host Total 1 1
otano di minute logo				Palo Alto Networks R Plugin ID 1001832 1001830 1001805	ANI-OS Audit Results - Top 50 Failed Audit Checks Name Palo Ato - Detect Config Change' Palo Ato - Securty Settings - 'socindary DNS serv Palo Ato Securty Settings - 'sorinary DNS server Palo Ato Securty Settings - 'springer DNS server Palo Ato Subdate Settings - 'springer DNS server	er has been configured has been onfigured en configured	Severity Migh High High High	Host Total

Palo Alto Networks PAN-OS Audit Results Dashboard



Palo Alto Networks PAN-OS Audit Report Title Page

Table of Contents	
About This Report	1
Executive Summary	2
Audit Summary 3.2 - Failed Audits 3.3 - Manual Audits 3.4 - Passed Audits	4 6 7

Palo Alto Networks PAN-OS Audit Report Table of Contents

# About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.