

PaloAlto firewall Quick Integration Guide

for PacketFence version 5.0.0

PaloAlto firewall Quick Integration Guide

by Inverse Inc.

Version 5.0.0 - Mar 2015 Copyright © 2014 Inverse inc.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

The fonts used in this guide are licensed under the SIL Open Font License, Version 1.1. This license is available with a FAQ at: <u>http://</u><u>scripts.sil.org/OFL</u>

Copyright © Łukasz Dziedzic, http://www.latofonts.com, with Reserved Font Name: "Lato".

Copyright © Raph Levien, <u>http://levien.com/</u>, with Reserved Font Name: "Inconsolata".

inverse

Table of Contents

About this Guide	1
Assumptions	2
Quick installation	3
Step 1: Create a SSO role	3
Step 2: Create the account in PAN-OS	3
Step 3: Get the XML Key	4
Step 4: SSO Configuration in PacketFence	4
Step 5: Verification	5

About this Guide

This guide has been created in order to help sales engineers, product managers, or network specialists demonstrate the PacketFence capabilities on-site with an existing or potential customer. It can also provide guidelines to setup a proof of concept for a potential PacketFence deployment using the PaloAlto firewall.

Assumptions

- You have a configured PacketFence environment with working test equipment
- You have a PaloAlto firewall with PanOS 6

Quick installation

Step 1: Create a SSO role

You will first need to create an SSO role on the web interface on the PaloAlto firewall.

Go to Device \rightarrow Admin Roles \rightarrow Add.

Create the role name SSO_Role, under the XML API tab, enable everything and validate it with OK.



Step 2: Create the account in PAN-OS

Now you have created the role, you will associate an user with it.

```
Go to Device \rightarrow Administrator \rightarrow Add.
```

- Name: xmluser
- Authentication Profile: None
- Password: xmluser
- Role: Role Based
- Profile: SSO_Role (Previously created)
- Password Profile: None

paloalto		Dashboard	ACC	Monitor	Policies	Objects	Network	Device			
🔯 Setup	S .										
Config Audit			Administrator							0	
Admin Roles		Name		Namo						_	ocked U
Password Profiles				Name	NICCLAR					_	
Administrators		admin	Authen	tication Profile	None					-	
WM Information Sources					Use only client	certificate authen	tication (Web)				
High Availability				Password							
V Certificate Management			6	Gree Descused	[
Certificates			Con	nrm Password	•••••						
🔂 Certificate Profile					Use Public Key	Authentication (S	SH)				
🔂 OCSP Responder				Role	O Dynamic 💿	Role Based					
Response Pages	1									-	
V Log Settings				Profile	SSO_Role					-	
System			Pa	ssword Profile	None					-	
Config								_			
Alarms									JK Cano	:el	
Manage Logs											
▼ 👩 Server Profiles											

Step 3: Get the XML Key

Go on this URL: https://@IP-of-PaloAlto/api/?type=keygen&user=xmluser&password=xmluser.

It should display:

```
<response status="success">
<result>
<key>
LUFRPT1jeFV6SHd1QnJHaU55dnYvRlFNSkJNeTR6Uzg9TDgzNV1j0=
</key>
</result>
</response>
```

Step 4: SSO Configuration in PacketFence

Now that we have the key, we will configure the PaloAlto firewall in PacketFence.

Go to Configuration \rightarrow Firewall SSO \rightarrow Add Firewall \rightarrow PaloAlto.

Hostname or IP Address: IP of your firewall

- Secret or Key: LUFRPT1jeFV6SHd1QnJHaU55dnYvRIFNSkJNeTR6Uzg9TDgzNVlj0= (use the key previously generated)
- Port of the service: 443
- Roles: add the roles that you want to do SSO with

I S	New Firewall SS	60 ×
Р	Hostname or IP Address ()	192.168.100.1
	Firewall Type	PaloAlto Firewall
I SSC	Secret or Key Ø	
	Port of the service	443 🔅
	Roles	If you use an alternative port, please specify staff × gaming ×
		Nodes with the selected roles will be affected
		Close
		Close Save

Step 5: Verification

Now we will check that PacketFence is sending information when a user register on the portal. If the process worked, you will see the entry in the PaloAlto database.

Use SSH on the PaloAlto firewall and run this command:

admin@PA-VM> sho	ow user	ip-user-mapping all					
IP MaxTimeout(s)	Vsys	From	User	IdleTimeout(s)			
 192.168.100.10 Never	vsys1	XMLAPI	domain\user1	Never			