PaloAlto firewall Quick Integration Guide

for PacketFence version 7.4.0

PaloAlto firewall Quick Integration Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018

Table of Contents

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

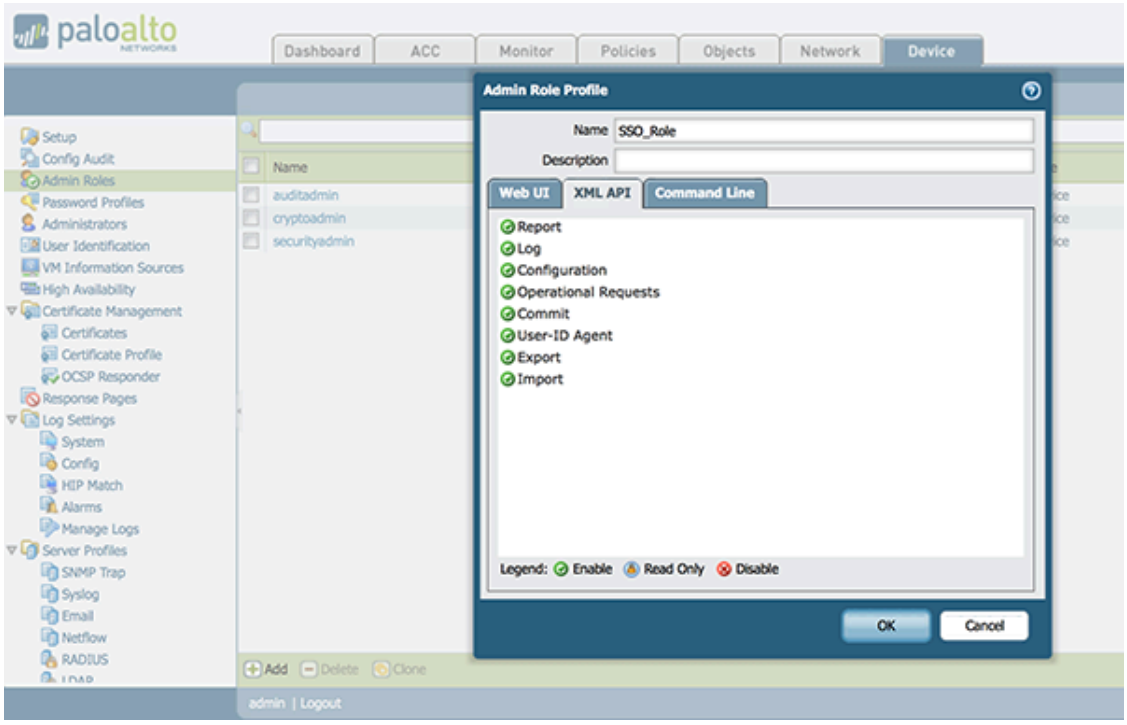
Installation using XMLAPI

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 → Admin Roles → Add**.

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

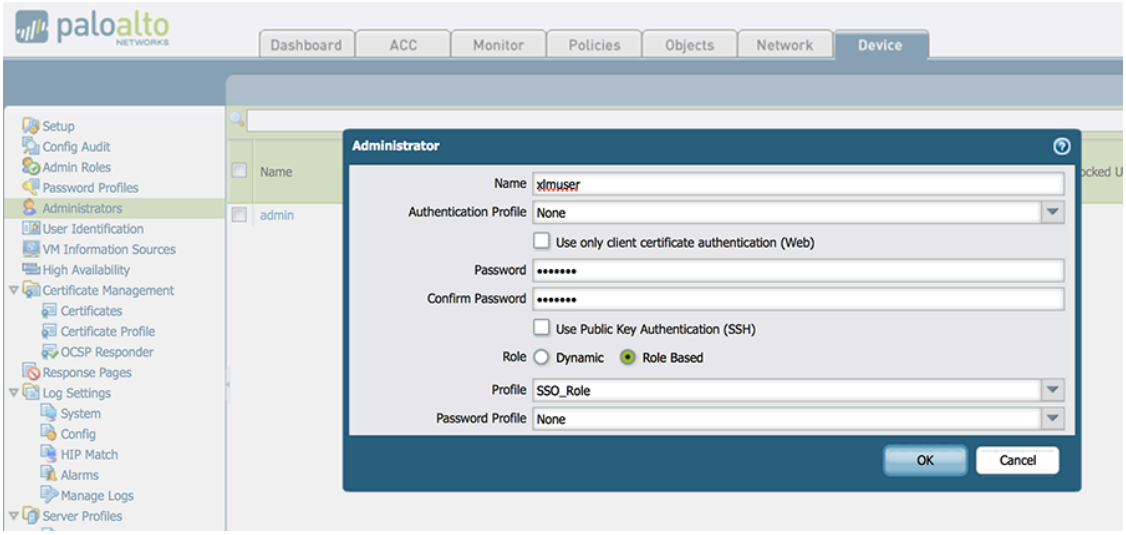


Step 2: Create the account in PAN-OS

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

Go to **Device → Administrator → Add**.

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



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>
LUFRPT1jeFV6SHd1QnJHaU55dnYvRlFNSkJNeTR6Uzg9TDgzNVlj0=
</key>
</result>
</response>
```

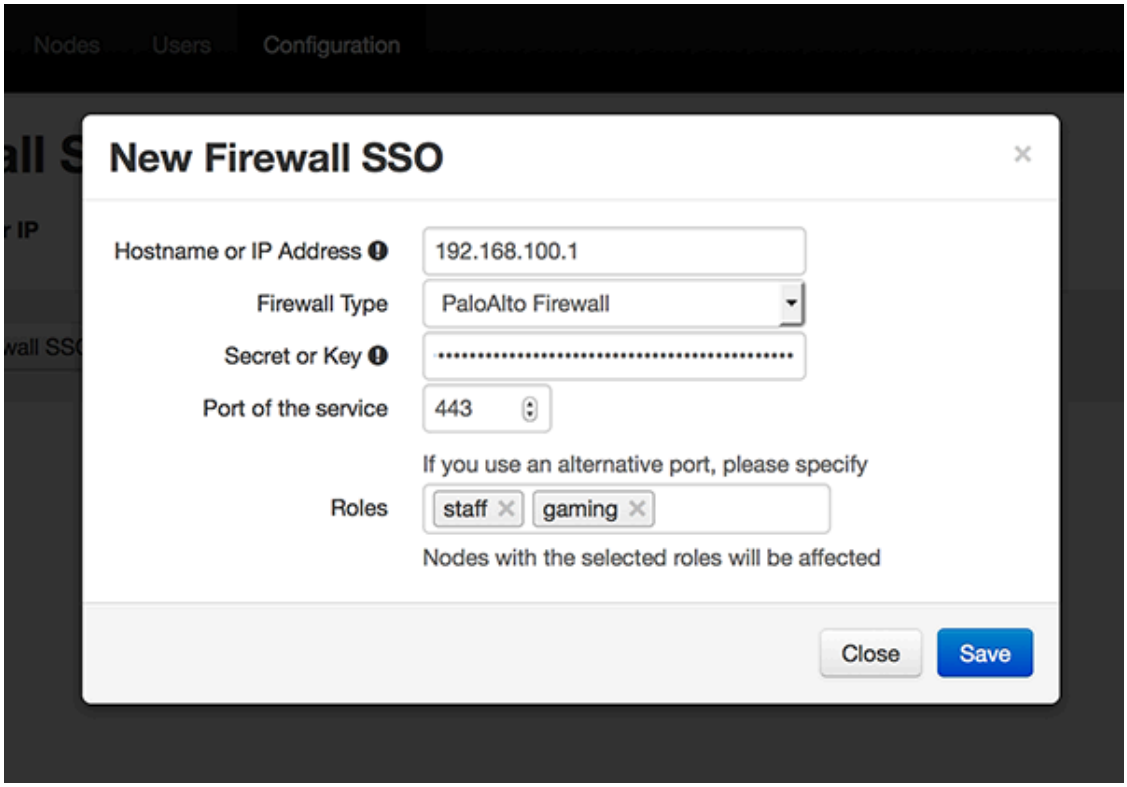
Step 4: SSO Configuration in PacketFence

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

Go to **Configuration → Integration → Firewall SSO → Add Firewall → PaloAlto**.

- **Hostname or IP Address**: IP of your firewall

- **Transport**: HTTP
- **Secret or Key**: LUFRPT1jeFV6SHd1QnJHaU55dnYvRlFNSkJNeTR6Uzg9TDgzNVlj0= (use the key previously generated)
- **Port of the service**: 443
- **Roles**: add the roles that you want to do SSO with



Step 5: Verification

Now we will check that PacketFence is sending information when a user registers 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> show user ip-user-mapping all

IP              Vsys   From    User                              IdleTimeout(s)
 MaxTimeout(s)
--------------- ------ ------- -------------------------------- --------------
 -------------
192.168.100.10  vsys1  XMLAPI  domain\user1                      Never
 Never
```

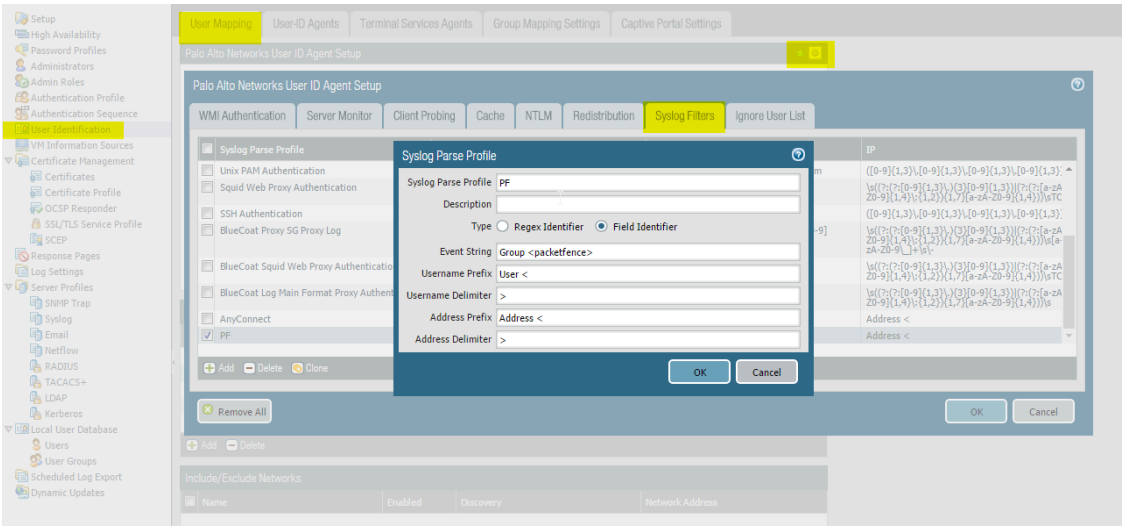
Installation using syslog

Note

This installation mode is not suggested unless you use the SSO for informational purposes (no enforcement). PacketFence will use easily spoofable UDP packets to communicate with the Palo Alto firewall. If you require encryption and origin validation of the SSO messages, please use the XML API.

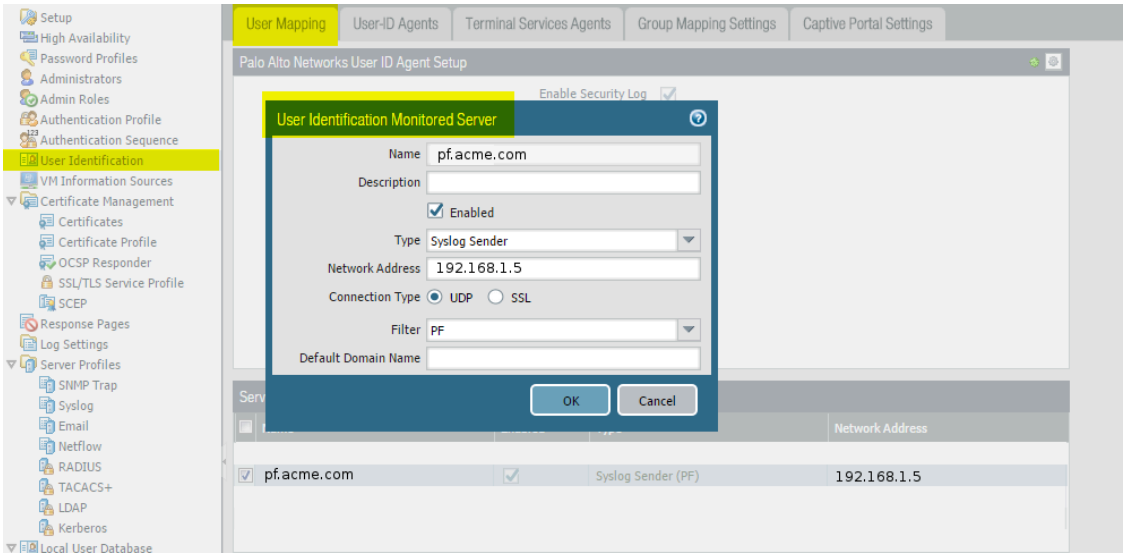
Step 1: Create a filter

You will first need to create a filter to parse the SSO line that PacketFence will send. This can be done in *User Identification→User Mapping*



Step 2: Assign the filter to a *Monitored Server*

Next, configure the filter to be used in a syslog receiver on the Palo Alto. In order to do so, go in *User Identification→User Mapping* and configure a syslog sender.



Step 4: SSO Configuration in PacketFence

Next you need to configure the firewall in PacketFence.

Go to **Configuration → Integration → Firewall SSO → Add Firewall → PaloAlto**.

- **Hostname or IP Address**: IP of your firewall
- **Transport**: Syslog
- **Secret or Key**: Ignore this parameter
- **Port of the service**: Ignore this parameter
- **Roles**: add the roles that you want to do SSO with

Step 5: Verification

Now we will check that PacketFence is sending information when a user registers 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> show user ip-user-mapping all

IP              Vsys   From    User                            IdleTimeout(s)
 MaxTimeout(s)
--------------- ------ ------- ------------------------------- --------------
 -------------
192.168.100.10  vsys1  syslog  domain\user1                    Never
 Never
```

Note

If the process is not working and you get the following error `Usage: Socket::inet_ntoa(ip_address_sv)`, check that the hostname of your PacketFence server can be resolved correctly on the server itself. If its not, make sure you adjust your hosts file or your DNS server.