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

Table of Contents

Chapter 1

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.

Chapter 2

Assumptions

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

Chapter 3

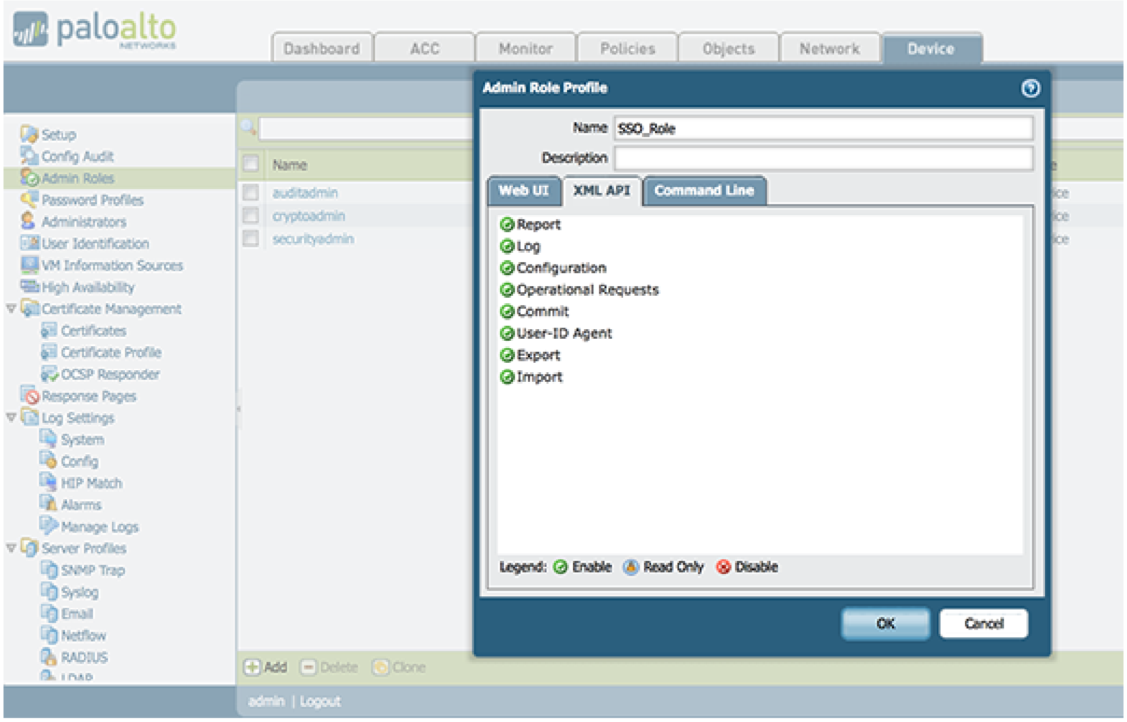
Quick installation

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** → **Admin Roles** → **Add**.

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



Admin Role Profile

Name: SSO_Role

Description:

XML API

- ✓ Report
- ✓ Log
- ✓ Configuration
- ✓ Operational Requests
- ✓ Commit
- ✓ User-ID Agent
- ✓ Export
- ✓ Import

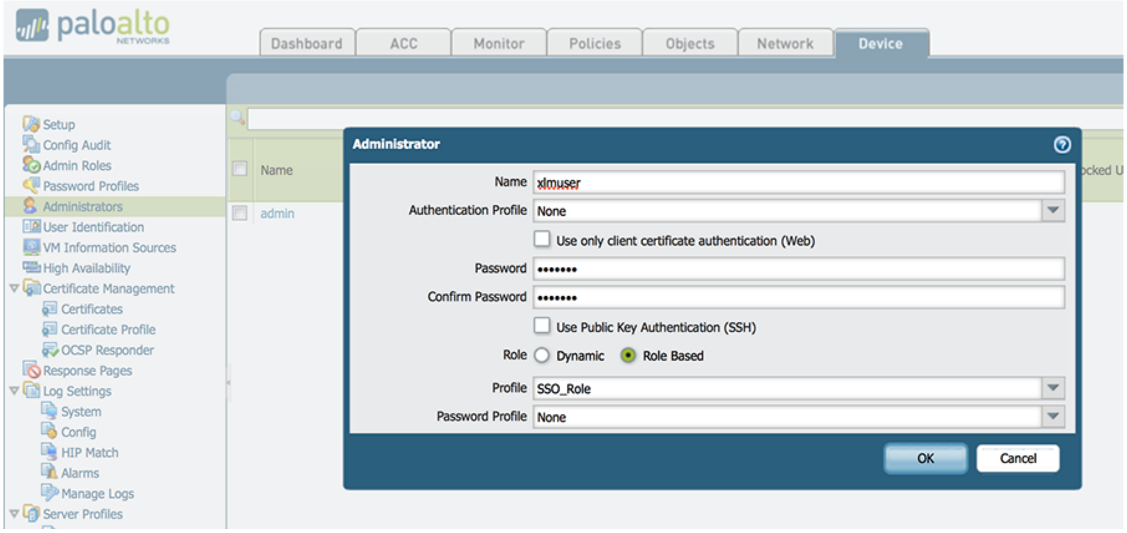
Legend: ✓ Enable ● Read Only ⊗ Disable

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



Administrator

Name: xlmuser

Authentication Profile: None

☐ Use only client certificate authentication (Web)

Password: •••••••

Confirm Password: •••••••

☐ Use Public Key Authentication (SSH)

Role: ○ Dynamic ● Role Based

Profile: SSO_Role

Password Profile: None

OK Cancel

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>
```

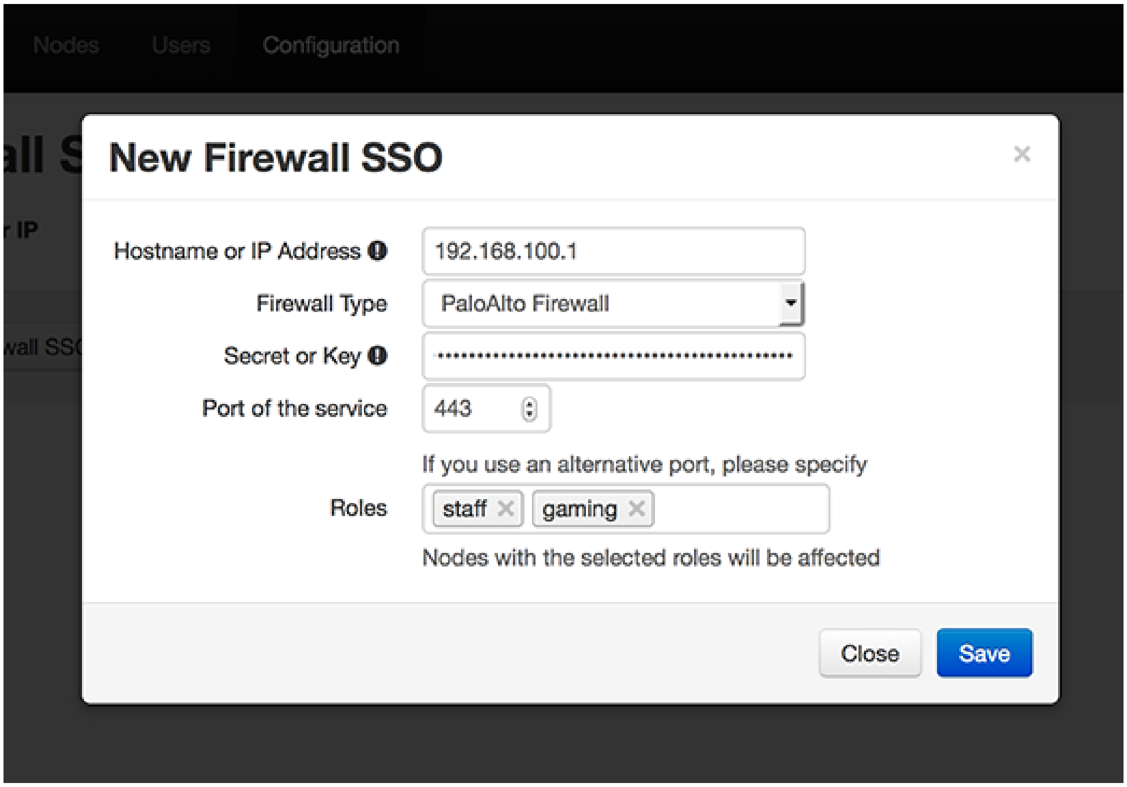
Step 4: SSO Configuration in PacketFence

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

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

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

- **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



New Firewall SSO

Hostname or IP Address: 192.168.100.1

Firewall Type: PaloAlto Firewall

Secret or Key: ••

Port of the service: 443

If you use an alternative port, please specify

Roles: staff × gaming ×

Nodes with the selected roles will be affected

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> show user ip-user-mapping all

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