



FortiGate firewall Quick Integration Guide

for PacketFence version 7.3.0

FortiGate firewall Quick Integration Guide

by Inverse Inc.

Version 7.3.0 - Sept 2017

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: <http://scripts.sil.org/OFL>

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

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

9279VnJ

Table of Contents

About this Guide	1
Assumptions	2
Quick installation	3
Step 1: Configuration of the RSSO Agent	3
Step 2: Configure the endpoint attribute	3
Step 3: Activate the Accounting Listening	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 **FortiGate** firewall.

Assumptions

- You have a configured PacketFence environment with working test equipment;
- You have a FortiGate firewall.

Quick installation

Step 1: Configuration of the RSSO Agent

Go to your FortiGate administration webpage in **User & Device** → **User** → **User Groups** → **Create New**.

- **Name:** RSSO_group
- **Type:** RADIUS Single Sign-On (RSSO)
- **RADIUS Attribute Value:** RSSO_Student (use the rolename of PacketFence, it's case sensitive)



You can also see that in the webpage at **User & Device** → **Monitor** → **Firewall**

Step 2: Configure the endpoint attribute

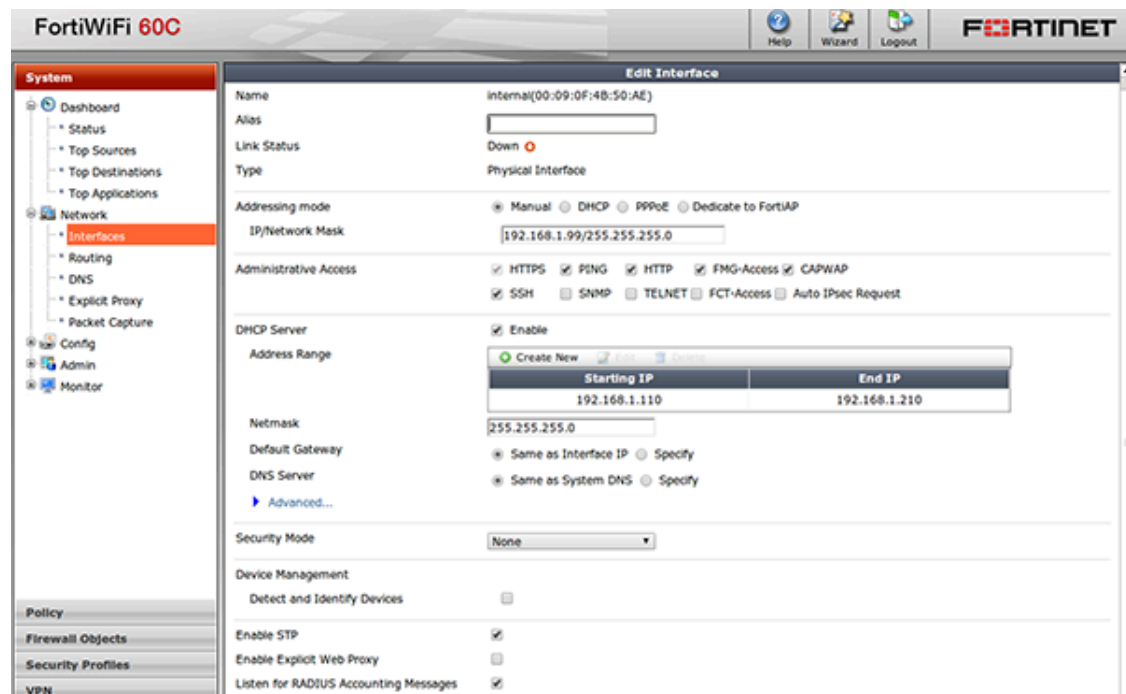
The default endpoint attribute is the Calling-Station-Id so the MAC address shows up under User Name, we can change that in CLI:

```
config user radius
edit RSSO_agent
set rso-endpoint-attribute User-Name
end
```

Step 3: Activate the Accounting Listening

Go to **System** → **Network** → **Interfaces**.

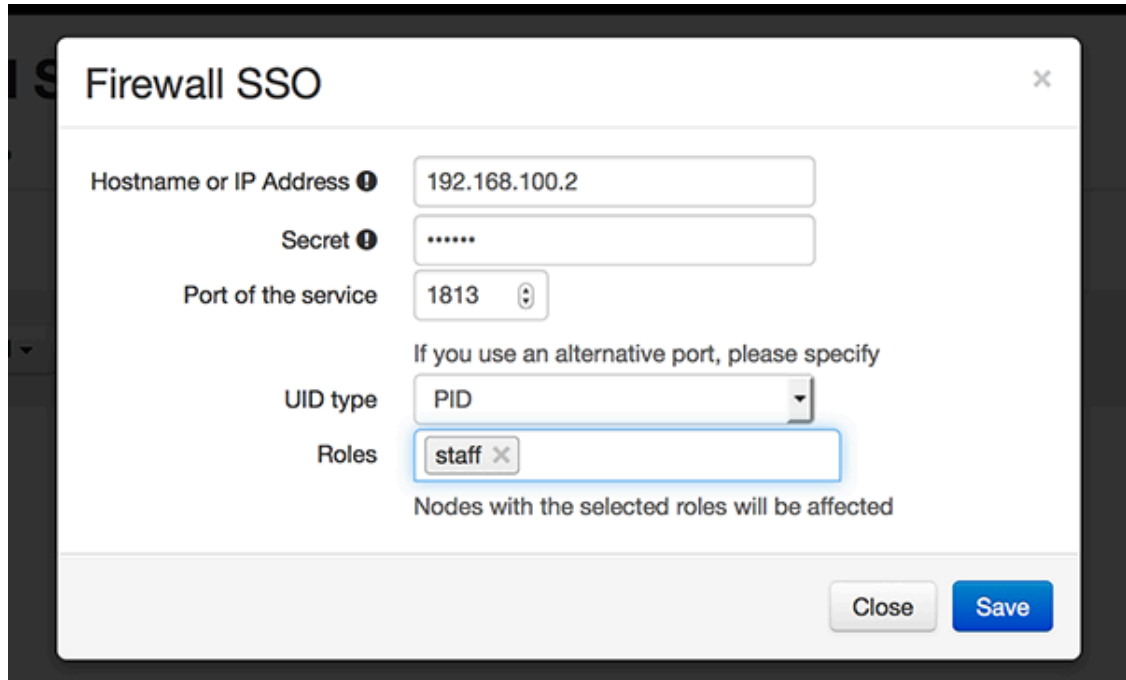
Select the interface that will communicate with PacketFence and check *Listen for RADIUS Accounting Messages* then confirm.



Step 4: SSO Configuration in PacketFence

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

- **Hostname or IP Address:** IP of your firewall
- **Secret or Key:** secret (radius shared secret)
- **Port:** 1813
- **Roles:** add the roles that you want to do SSO



The screenshot shows a 'Firewall SSO' configuration window. It contains the following fields and options:

- Hostname or IP Address**: 192.168.100.2
- Secret**: masked with six dots
- Port of the service**: 1813
- UID type**: PID (selected from a dropdown menu)
- Roles**: staff (selected from a list, with a blue highlight and a close button 'x')

Below the 'Roles' field, it says: 'Nodes with the selected roles will be affected'.

At the bottom right, there are two buttons: 'Close' and 'Save'.

Step 5: Verification

If you want to see if it's working, you can log into the firewall over SSH and run these following commands:

```
di debug enable
di debug application radiusd -1
```