

FortiGate firewall Quick Integration Guide

for PacketFence version 7.4.0

FortiGate firewall Quick Integration Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018 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: 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 \rightarrow User \rightarrow User Groups \rightarrow 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)

FortiWiFi 60C	3-	
System Policy Firewall Objects Security Profiles	Name Type RADIUS Attribute Value	Edit User Group SSS0_SSt05mt Firewall © Fortinet Single Sign-On (FSS0) © Guest @ RADIUS Single Sign-On (RSS0) RSSOStudent
User & Device		OK Cancel

You can also see that in the webpage at User & Device \rightarrow Monitor \rightarrow 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 RSS0_agent
set rsso-endpoint-attribute User-Name
end
```

Step 3: Activate the Accounting Listening

Go to System \rightarrow Network \rightarrow Interfaces.

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

FortiWiFi 60C	Jan L	
System		Edit Interface
B Dathboard	Name	internal(00:09:0F:48:50:AE)
- Status	Allas	
* Top Sources	Link Status	Down O
* Top Destinations	Туре	Physical Interface
* Top Applications	Addressing mode	Manual DHCP PPPoE Dedicate to FortiAP
* Si Network	IP/Network Mask	192.168.1.99/255.255.255.0
- * Routing - * DNS - * Explicit Praxy	Administrative Access	HTTPS PENG HTTP FMG-Access CAPWAP SSH SNMP TELNET FCT-Access Auto IPsec Request
Packet Capture Gonfig	DHCP Server	Ø Enable
🛞 🌄 Admin	Address Kange	O Create New 🧟 Edit. 🖀 Osiste
🖲 🐺 Monitor		102 168 1 110 102 168 1 210
	Netmask	
	Default Gateway	235.255.255.0
	DAS Secur	Same as Interface IP Specify
	Advanced	a Same as System DNS Specify
	Security Mode	None
	Device Management	
Belley	Detect and Identify Devices	8
Policy	Foahie STP	2
Firewall Objects	Foable Evolutit Web Provy	~
Security Profiles	Listen for BADIUS Accounting Messages	2
VPN		w/

Step 4: SSO Configuration in PacketFence

Go to Configuration \rightarrow Integration \rightarrow Firewall SSO \rightarrow Add Firewall \rightarrow 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

S	Firewall SSO	×
	Hostname or IP Address 4 Secret 4 Port of the service	192.168.100.2 1813 🔅
1 4 1	UID type Roles	If you use an alternative port, please specify PID
		Close 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