



# Barracuda firewall Quick Integration Guide

for PacketFence version 5.0.0

---

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

Copyright © Łukasz Dziejdzic, <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 Barracuda in PacketFence ..... 3
  - Step 2: Verification ..... 4

# 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 **Barracuda firewall**.

# Assumptions

---

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

# Quick installation

---

## Step 1: Configuration of the Barracuda in PacketFence

---

Go to Configuration → Firewall SSO → Add Firewall → Barracuda.

- **Hostname or IP Address:** IP of your Barracuda
- **Firewall type:** Barracuda (Barracuda = SSH requests)
- **Password:** secret
- **Port:** 22
- **Roles:** add the roles that you want to do SSO

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

- Hostname or IP Address:** 192.168.100.3
- Username:** root
- Password:** masked with dots
- Port of the service:** 22
- Roles:** staff

Below the roles field, there is a note: 'If you use an alternative port, please specify'. At the bottom right, there are 'Close' and 'Save' buttons.

## Step 2: Verification

---

For our example, when the user registers on the portal it will be registered and the role staff will be assigned. The PacketFence server will send a request to the Barracuda database.

If you want to see if it's working, open an SSH access to your Barracuda and run this command following commands:

```
acpfctrl auth show
```

You will get that:

```
[root@baracudafw:~]# acpfctrl auth show
1 entries
172.20.20.152/0
origin=PacketFence
service=PacketFence
user=Jdoe
```