



Brocade Quick Installation Guide

for PacketFence version 7.4.0

Brocade Quick Installation Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018

Copyright © 2013 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 Deployment	3
Step 1: Pre-load	3
Step 2: Configure Network and PacketFence	4
Step 3: Configure the Brocade equipment	8
Step 4: Configuration of Windows 7 client for DemoSecure	11
Step 5: Test and Demonstrate	11

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 Brocade equipment.

The instructions are based on version 7.4.0 of the PacketFence Live Image.

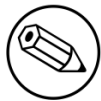
Assumptions

- You will need a USB key with a capacity of at least 4GB;
- You will need a laptop or a PC from which the PacketFence Live USB key will run from;
- You will deploy a VLAN enforcement environment according to the customer specifications;
- Your customer will provide the network equipment (switch, cabled, etc) to interconnect this PoC setup;
- Brocade Wireless Controller is using WINGS 5.2 software.

Quick Deployment

Step 1: Pre-load

This step is only necessary in the case you don't already have a pre-loaded PacketFence USB key. If you already have one, proceed to step 2, otherwise, follow these quick and simple instructions to pre-load a new USB key with PacketFence.



Note

The following process will remove everything from the USB key so if you currently have stuff on it, make sure to do backups!

Download the PacketFence USB key image

Make sure you have the latest version of the PacketFence USB key image.

Download the application to write the image to the USB key

To write the PacketFence image on a USB key, you'll need to use a third-party application that will provide you with a graphical interface to do so.

Go to <https://launchpad.net/win32-image-writer/0.6/0.6/+download/win32diskimager-binary.zip>. That will download the necessary application. Once downloaded, extract the zip file.

Write the PacketFence image to the USB key

First, make sure your USB key is plugged into the PC then open up the folder where you extracted the application and double-click the Win32DiskImager.exe file. Once done, simply choose the PacketFence USB image file (unzipped .img file), choose the device on which you want to write and click Write.

Step 2: Configure Network and PacketFence

The next step is the network setup and the PacketFence configuration. The following step is usually performed when you arrive at a customer site. Sometimes, you will know the network settings in advance, sometimes not. If you want to save time, you should ask/tell the client what is needed in order to have the demonstration running smoothly. That way, you will be able to preconfigure the PacketFence environment prior arrival.

Preliminary Questions

Here is a quick list of questions to ask to a customer in order to easily configure a PacketFence environment:

1. What is the VLAN ID and subnet to be used for a registration VLAN? (ie. VLAN ID 2, Subnet 192.168.2.0/24)
2. What is the VLAN ID and subnet to be used for an isolation VLAN? (ie. VLAN ID 3, Subnet 192.168.3.0/24)
3. What is the VLAN ID of the production VLAN? (ie. VLAN ID 10)
4. A list of production DHCP server(s) (for rogue DHCP detection)

Steps for the customer

Some steps needs to be taken by the customer for having the network ready. Here is a list of what we think should be ready for a demo:

- 1 TRUNK port to connect the demonstration PC which will run the PacketFence environment. The native VLAN should be a management VLAN that will be used for communication between the equipment and the environment
- 1 TRUNK port to connect the controller
- 1 TRUNK port to connect the AP

Configuring your PacketFence environment

Simply plug the previously created USB key in one of the demonstration PC USB port. You will have to make sure the PC will boot from the USB key (it is usually a pre-boot option or a setting in the BIOS).

Before booting, make sure the network cable coming from the TRUNK port for the demonstration PC is correctly plugged in the switch and the PC and that the link is up.

Once powered, the PC will boot from the USB key and will automatically get to a graphical user interface with an opened web browser prompting for PacketFence configuration. The configuration

process is a five steps process at the end of which, the USB key will be a persistent working PacketFence environment.

Step 1: Enforcement

The first and most important step of the configuration process. This is where you'll choose the enforcement technique; either VLAN (out-of-band), INLINE (in-band) or both of them.

The choice(s) made on this step will influence the next step where you'll need to configure the different networks.

Each enforcement mode has its own required interface types that you'll have to configure on step 2.

For our customer scenario, we'll choose VLAN enforcement.

Step 2: Networks

This step will ask you to statically configure your network interfaces (note that DHCP interfaces configuration is not supported yet).

Depending on the choice(s) made on step 1, you'll have to configure the required types of interface. The web interface will list all currently installed network interfaces on the system. An IP and a netmask will be visible if the network interface is configured (either by DHCP or already manually configured). You can edit those ones, create/delete VLANs on physical interfaces and enable/disable an interface. Note that these changes are effective on the moment you make them. Persistence will be written only for ENABLED interfaces.

In all time, you'll need to set a Management interface.

Required interface types for inline enforcement:

```
Management
Inline
```

Required interface types for VLAN enforcement:

```
Management
Registration
Isolation
```

Note that you can only set ONE (1) management interface. This one will work for both in the case you choose both modes.

In our customer scenario, we will create two new vlans on the wired interface (will be eth0 most of the time). To do so, click the Add VLAN button besides the wired interface for each of the needed vlan:

Here's a sample configuration for both of them:

Registration

```
Virtual LAN ID: 2
IP Address: 192.168.2.1
Netmask: 255.255.255.0
```


Isolation

```
Virtual LAN ID: 3
IP Address: 192.168.3.1
Netmask: 255.255.255.0
```

Don't forget to also edit the physical interface with the correct management network information by clicking the Edit button next to it.

According to our customer scenario, we'll associate the correct type the each interfaces.

```
eth0: Management
eth0 VLAN 2: Registration
eth0 VLAN 3: Isolation
```

Make sure that those three (3) interfaces are in an Enabled state for the persistence to occur.

We also need to set the Default Gateway which will generally be the gateway of the management network.

Once everything's set, click Continue to proceed with the next step.

Step 3: Database Configuration

This step will configure the MySQL server needed by PacketFence. Database and schema will be created as well as the necessary user for operations. Root account will also be secured if necessary (set a password and disallow remote login).

Since Debian based MySQL installations are not "secured", we'll need to go through it. That step is fairly simple to accomplish and is a one time deal.

In the root account credentials section, enter root as Username and click Test. You'll be prompted for a new root password. Choose a password for the MySQL root user and click Save. You can now enter your newly created password in the root account credentials section and click Test.

Next section of this step is the PacketFence user account on the MySQL server. Simply leave the default pf username here and choose of a password. This one will automatically be set in the PacketFence configuration where you'll be able to retrieve it in any case. Once the password entered twice, click Create user.

Third section will create the database and load the correct schema on it. Simply leave the default and click Create tables and indexes.

You should have Success beside these three section, click Continue.

Step 4: PacketFence Configuration

This step will configure the general options of your PacketFence installation. Theses are needed configurations that will most of the time fits customer specifications.

Almost all of the required information here are self-explanatory. The only one that could be confusing is the DHCP Servers section. In this one, enter a comma-delimited list of all the DHCP

Server on the customer network so when PacketFence will see DHCP traffic originating from these IPs, no rogue-dhcp alerts will be triggered.

Click Continue once all the field are completed.

Step 5: Administration

This is the step where we create the administrative user to access the PacketFence Administration Web Interface.

Simply provide the desired username and password, then click Create user.

Step 6: Services - Confirmation

The last but not the least. Here, we start the PacketFence server according to the configurations made in the previous steps. If everything goes as expected, you'll be prompted by a window inviting you to continue to the web administration interface.

You'll be able to login to the PacketFence web administration interface with the credentials created in Step 4.

Services status will help you monitor if everything goes as expected. If not, you'll see which service is in trouble and the log output will help you determine the problem that occurs.

Configuring the Brocade equipment in PacketFence

Now that you have a fully functional PacketFence installation, you'll need to add the Brocade switch and wireless controller to the PacketFence switches database for correct integration.

To do so, login to the PacketFence web administration interface if it is not already done. Click on the Configuration tab and select the switches section under Policies and Access Control.

We'll use the clone function to add a new network device to the PacketFence database. With the mouse pointer, go over the default switch and you'll see a set of icons appearing at the left of it. Click on the second one (a paper sheet with a plus sign).

The Adding new switch window will appear, in which, you'll enter the correct information for the integration. Use theses values to populate each of the fields; leave the others as is:

```
IP: This will be the IP of the Brocade switch on the customer management network
Type: Brocade
Mode: Production
Vlans: 2,3,10
Normal VLAN: 10
Registration VLAN: 2
Isolation VLAN: 3
SNMP Version: 2c
SNMP Read Community: brocadeRead
SNMP Write Community: brocadeWrite
RADIUS Secret: aSecurePassword
```

Click Add switch

The newly added switch should show up in the list. Reproduce the last steps to add the Brocade Wireless controller. This time, use the type "Brocade::RFS" instead.

PacketFence configuration is now done. You may now reboot the demonstration PC (leave the USB key in). Once rebooted, the web browser should open in the PacketFence web administration interface.

Step 3: Configure the Brocade equipment

This section will discuss about the configuration of your Brocade equipment in order to use it with our configured PacketFence environment.

Brocade RFS Wireless Controller

First thing to do is to connect the controller and the AP. Like we saw in Step 2, we should have 1 TRUNK port for the controller and 1 TRUNK port for the AP. Connect them appropriately.

Provision the controller

By default, the controller will come no management IP (or set to DHCP). You may need to connect to it using a console cable, and change its management IP accordingly. You should ensure also that your controller is using WiNGS 5.2 as the OS.



Note

Please refer to the Brocade RFS System Reference Guide available at http://www.brocade.com/downloads/documents/product_manuals/Mobility/Mobility_05200_SRG.pdf.

Create AAA Policy

First, we need to build the AAA Policy. Under Configuration > Wireless > AAA Policy, click on the Add button at the bottom right. Configure the RADIUS profile like the following:

Host: Choose IP Address in the drop down, and put the RADIUS server address (Demonstration Management IP)
 Insert the RADIUS secret passphrase you configured at Step 2
 Select "Through Wireless Controller" request mode

Since we are using RADIUS Dynamic Authorization, we need to enable the RADIUS accounting. Under the RADIUS accounting tab, click the Add button at the bottom right, and insert the proper values.

Configure the Open SSID

Under Configuration > Wireless > Wireless LANs, click on the Add button at the bottom right. Under Basic Configuration:

```
Profile Name: Give a convenient Name (ie. DemoOpen)
SSID: Input DemoOpen in the field
WLAN Status: Set to enable
VLAN assignment technique: Select Single VLAN
Allow RADIUS Override: Select
```

Under Security Configuration:

```
Authentication Type: Select MAC
AAA Policy: Select the Policy you just created in the previous step
Encryption: Select Open
```

Under Advanced Configuration:

```
RADIUS Dynamic Authorization: Select
```

Configure the Secure SSID

Under Configuration > Wireless > Wireless LANs, click on the Add button at the bottom right.
Under Basic Configuration:

```
Profile Name: Give a convenient Name (ie. DemoSecure)
SSID: Input DemoSecure in the field
WLAN Status: Set to enable
VLAN assignment technique: Select Single VLAN
Allow RADIUS Override: Select
```

Under Security Configuration:

```
Authentication Type: Select EAP
AAA Policy: Select the Policy you just created in the previous step
Encryption: Select WPA/WPA2-TKIP
Fast Roaming: Unselect everything
```

Under Advanced Configuration:

```
RADIUS Dynamic Authorization: Select
```

WLAN Mapping

You have multiple options here. Either, you create a general AP profile, and you assign it to your Aps, or you modify the AP device configuration to map the WLAN to the radio interfaces.

For the purpose of this document, we will modify the general profile. Under Profiles > default-apXXX (where XXX is your AP model), in Interface > Radios, edit the existing radios settings. Go to the WLAN Mapping tab, select the two SSIDs and click on the << button.

VLANs

You need to ensure that the uplink interface of the controller is configured as a trunk, and that all the necessary VLANs are created on the device. This is configured under Device > rfsXXXX-MAC

(where XXXX is your controller series, and MAC is the latest 3 octets of its mac address). Edit the device configuration, and go to Interface > Ethernet Ports. Ensure that the up1 interface is set as trunk, with all the allowed VLANs. Next, create the VLAN under Interface > Virtual Interfaces. You will need to create the VLAN Interface for VLAN 2 and 3.

Configure SNMP

Last step, we need to configure the SNMP to add a valid read community string. This is done in the Configuration > Management section. Edit the management policy for the SNMP section. Use the SNMP read community you defined at Step 2.

Brocade Wired Switch

Now that we have the wireless part done, let's configure the Brocade switch to perform 802.1X. Connect to the switch using SSH or using a console port. Escalate in Enable privileged mode.

Global config

Input "configure terminal", and type :

```
aaa authentication dot1x default radius
radius-server host PF_MANAGEMENT auth-port 1812 acct-port 1813 default
radius-server key aSecretPassword
```

Replace PF_MANAGEMENT with the Demonstration PC management IP, and the sSecretPassword with the RADIUS secret configured at Step 2.

MAC Authentication

Now we need to enable MAC Authentication globally. In "configure terminal", type :

```
mac-authentication enable
mac-authentication mac-vlan-dyn-activation
```

When done, we need to activate it on the switchport level. For example, let's do it for port 10. In "configure terminal", type :

```
int ethe 1/1/10
mac-authentication enable
mac-authentication enable-dynamic-vlan
end
```

802.1X

If we want to have 802.1X and MAC Authentication enabled on the same port, you need to enable 802.1X globally first. In "configure terminal", type :

```
dot1x-enable
re-authentication
enable ethe 1/1/10
```

Finally, you need to enable it at the switchport level. Again, we will use port 10. In configure terminal, type :

```
int ethe 1/1/10
dot1x port-control auto
```

Step 4: Configuration of Windows 7 client for DemoSecure

In Control Panel\Network and Internet\Manage Wireless Networks, click on Add. Click Manually create a network profile

```
Network name: DemoSecure
Security type WPA2-Enterprise
Encryption AES
```

Next, change connection settings. On Security tab, click Settings, uncheck Validate server certificate. On the same tab click Configure and uncheck Automatically use my Windows logon name and password. Return on the Security tab and click on Advanced settings. On 802.1X settings, click on Specify authentication mode and select User authentication. On 802.11 settings uncheck Enable Pairwise Master Key (PMK) caching. Validate all the modifications and click on close.

Step 5: Test and Demonstrate

Congratulations, you have everything setup and ready! If your setup is properly configured, you should be able to :

- reach (ping) the controller from the PacketFence environment
- see the DemoOpen, and DemoSecure SSIDs
- login the PacketFence administrative UI (https://management_IP:1443)
- connects a client device on the DemoOpen SSID using demouser/demouser credentials on the captive-portal
- connects a client device on the DemoSecure SSID using demouser/demouser credentials in the Windows network login dialog