PacketFence Out-of-Band Deployment Quick Guide using ZEN

for PacketFence version 5.3.1

PacketFence Out-of-Band Deployment Quick Guide using ZEN

by Inverse Inc.

Version 5.3.1 - July 2015

Table of Contents

About this Guide

This guide will walk you through the installation and configuration of the PacketFence ZEN solution. It covers VLAN isolation setup.

The instructions are based on version 5.3.1 of PacketFence.

The latest version of this guide is available online at http://www.packetfence.org/documentation/guides.html

Other sources of information

We suggest that you also have a look in the PacketFence Administration Guide, and in the PacketFence Network Devices Configuration Guide. Both are available online at http://www.packetfence.org/documentation/guides.html

Getting Started

Virtual Machine

This setup has been tested using VMWare ESXi 4.0 & 5.0 with 8GB RAM dedicated to the virtual machine. It might work using other virtualization products. You need a 64-bit capable CPU on your host.*

VLAN Enforcement

In order to build a VLAN isolation setup you need :

- a supported switch (please consult the list of supported switch vendors and types in the *Network Devices Configuration Guide* including information on uplinks
- a regular, registration and isolation VLAN for visitors (VLAN numbers and subnets)
- a switch port for the PacketFence (PacketFence) ZEN box which needs to be configured as a dot1q trunk (several VLANs on the port) with VLAN 1 as the native (untagged) VLAN.

Assumptions

Throughout this configuration example we use the following assumptions for our network infrastructure:

Network Setup

- VLAN 1 is the management VLAN
- VLAN 2 is the registration VLAN (unregistered devices will be put in this VLAN)
- VLAN 3 is the isolation VLAN (isolated devices will be put in this VLAN)
- VLAN 10 is the "regular" VLAN

Please refer to the following table for IP and Subnet information :

VLAN ID	VLAN Name	Subnet	Gateway	PacketFence Address
1	Management	DHCP		DHCP
2	Registration	192.168.2.0/24	192.168.2.10	192.168.2.10
3	Isolation	192.168.3.0/24	192.168.3.10	192.168.3.10
10	Normal	192.168.1.0/24	192.168.1.1	

DHCP/DNS

- PacketFence provides its own DHCP services. It will take care of IP address distribution in VLANs 2 and 3. PacketFence will not provide DHCP services on VLAN 10 - this is the responsibility of your own infrastructure.
- PacketFence provides its own DNS service. It will take care of naming resolution in VLANs 2 and 3. PacketFence will not provide DNS services on VLAN 10 - this is the responsibility of your own infrastructure.

Installation

Import the virtual machine

PacketFence ZEN 5.3.1 comes in a pre-built virtual disk (OVA). If you are using an ESX-type hypervisor, you need to import the OVA using vSphere Client (or vCenter). We are not supporting any Xen-based hypervisors yet.

Import to ESX

Make sure that there is only one virtual network card created, and also make sure that your vEthernet is connected to a virtual switch (vSwitch). You will need to create a “TRUNK” profile to allow all VLAN tags (usually VLAN all (4095)), and assign the profile to the PacketFence ZEN VM vEthernet.

Virtual Machine passwords

Management (SSH/Console) and MySQL

- Login: root
- Password: p@ck3tf3nc3

Captive Portal / 802.1X Registration User

- Login: demouser
- Password: demouser

Configuration

Configuring your PacketFence environment

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

Once powered, open a browser and point it to the configuration URL as stated by the VM login prompt (ie. https://PF_IP:1443/configurator). The configuration process is a five steps process at the end of which, the VM 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.

In this guide we will show you how to configure the VLAN (out-of-band) mode. If you want to configure the INLINE (in-band) mode please refer to PacketFence Inline Deployment Quick Guide using ZEN

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 theses changes are effective on the moment you make them. Persistance will be written only for ENABLED interfaces.

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

Required interface types for VLAN enforcement:

```
Management
Registration
Isolation
```

Note that you can only set ONE (1) management interface.

In our example, 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
```

Note

Ignore the High-Availability options for now. If you are interested in a PacketFence cluster, please refer to the PacketFence Clustering Guide

Don't forget to also edit the physical interface with the correct management network information by clicking on the network interface name (eth0).

According to our example, 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 persistance 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).

Start the MySQLd service if it is not started. Click the MySQL Start button at the top of the web page *Warning! MySQL server does not seems to be running. You should start it to avoid any problems. Start MySQL*.

Then you will need to create the root password for MySQL database. Click on the Test button and write a complex password (recommended) twice and save. When you are done creating the

password, put the new root password and click on Test to validate it. You should see *Success! Successfully connected to the database mysql with user root*

Next section will create the database and load the correct schema on it. Simply leave the default database name and click Create databases and tables.

The last 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 retrive it in any case. Once the password entered twice, click Create user.

If you got a *Success!* message for this all three sections, 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 trafic originating from these IPs, no rogue-dhcp alerts will be triggered. Packetfence will use the domain and the hostname to generate the url to redirect devices on the captive portal. If you have a http certificate use the same hostname and domain name to validate the SSL connection on the captive portal.

In the last section, Local Database Passwords, you will have to chose the password encryption for local accounts (guest automatically generated and manualy created account)

Click Continue once all the fields 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 Modify the password.

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 DHCP OMAPI (optional)

In order to speed up the IP address lease lookup, you can configure the DHCP OMAPI so that queries for IP and MAC associations are made faster.

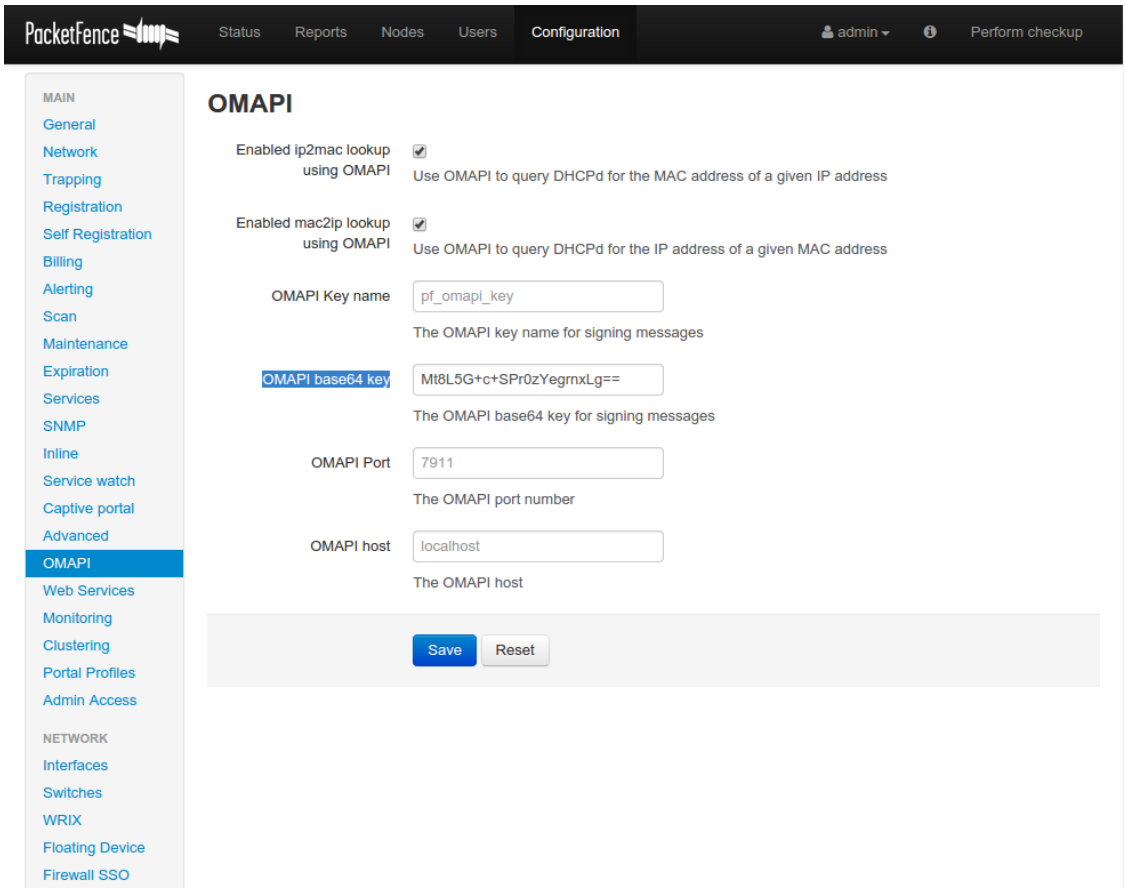
First, execute the following command in an SSH session.

```
# dd if=/dev/urandom bs=16 count=1 2>/dev/null | openssl enc -e -base64
```

This should produce an output similar to this :

```
m4NMkOKc9IxfWk8cL2fP4g==
```

Now paste the output in the Administration interface under *Configuration/OMAPI/OMAPI base64 key* and save.



Now restart the dhcpd service using the following command in an SSH session.

```
# /usr/local/pf/bin/pfcmd service dhcpd restart
```

PacketFence configuration files

If you want to customize the configuration files, we suggest that you take a look into the PacketFence Administration Guide prior doing so.

The main configuration files are :

- `conf/pf.conf` : Configuration for the PacketFence services
- `conf/networks.conf` : Definition of the registration and isolation networks to build DNS and DHCP configurations. In our case, we included the registration and isolation networks.
- `conf/switches.conf` : Definition of our VLANs and network devices

Network Devices

Please refer to the Network Devices Configuration Guide in order to properly configure your devices.

Now that you have a fully functionnal PacketFence installation, we will provide a example of Cisco Catalyst 2960 integrated with Packetfence using mac-authentication.

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 under Network section.

To add a new switch (the Catalyst 2960) to the PacketFence database, click on the Add switch at the bottom.

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:

Definition:

```
IP: This will be the IP of the Catalyst 2960 switch on the management network
Description: Cisco Catalyst 2960
Type: Cisco::Catalyst_2960
Mode: Production
Deauthentication: RADIUS
Dynamic Uplinks: Checked
```

Roles:

```
Role by VLAN ID: checked
registration VLAN: 2
isolation VLAN: 3
default: 10
```

Radius:

```
Secret Passphrase: useStrongerSecret
```

Snmp:

```
SNMP Version: 2c
SNMP Read Community: ciscoRead
SNMP Write Community: ciscoWrite
```

Click Save to add the switch

The newly added switch should shows up in the list.

Configure the Cisco Catalyst 2960

This step will discuss about the configuration of your Cisco 2960 switch in order to use it with our configured PacketFence environment. We will assume you do everything using the switch CLI.

Enable 802.1X

As a first configuration step, you need to enable 802.1X globally on the switch. To do so, use the following:

```
dot1x system-auth-control
```

Configure AAA

The next step is to configure AAA so it will use your newly created PacketFence server. Make sure you replace the PF_MANAGEMENT_IP variable with your actual PacketFence management IP in the following commands:

```
aaa new-model
aaa group server radius packetfence
 server PF_MANAGEMENT_IP auth-port 1812 acct-port 1813
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence
radius-server host PF_MANAGEMENT_IP auth-port 1812 acct-port 1813 timeout 2 key
 useStrongerSecret
radius-server vsa send authentication
```

Note

Make sure to have a local account on the switch.

Configure switchports for MAB

Once AAA is ready, we can configure some or all switchports to perform Mac-Authentication Bypass (MAB) (w/o voice support):

```
switchport mode access
authentication host-mode single-host
authentication order mab dot1x
authentication priority mab dot1x
authentication port-control auto
authentication periodic
authentication timer restart 10800
authentication timer reauthenticate 10800
mab
no snmp trap link-status
dot1x pae authenticator
dot1x timeout quiet-period 2
dot1x timeout tx-period 3
```

If you want to test some ports with a VoIP phone (ex: Voice VLAN 100), add the following lines to your interface configuration:

```
switchport voice vlan 100
authentication host-mode multi-domain
```

Configure SNMP

Finally, for some operations (like VoIP), PacketFence still need to have SNMP access to the switch. Make sure you configure the two SNMP communities like:

```
snmp-server community ciscoRead ro
snmp-server community ciscoWrite rw
```

Note

You can refer to the Cisco Catalyst documentation for more options. The latest documentation is available here: http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/15.0_1_se/configuration/guide/sw8021x.html

Configure the Change of Authorization (CoA)

aaa server radius dynamic-author client PF_MANAGEMENT_IP server-key useStrongerSecret port 3799

Save the config!

When done, don't forget to save your configs using `write mem`!

Test and Demonstrate

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

- reach (ping) the switch from the PacketFence environment
- login the PacketFence administrative UI (https://management_IP:1443)
- connects a client device on a mac-authentication switchport using demouser/demouser credentials, and show a registration.

FreeRADIUS

PacketFence ZEN 5.3.1 comes with a pre-configured FreeRADIUS to do Wired and Wireless 802.1X with EAP as well as MAC Authentication. We created a local user for the 802.1X authentication.

The main configuration files are :

- `/usr/local/pf/conf/radiusd.conf` : Template for the configuration for the RADIUS service
- `/usr/local/pf/conf/eap.conf` : Template for the configuration for 802.1X using EAP
- `/usr/local/pf/conf/sql.conf` : Template for the RADIUS accounting and RADIUS clients configuration in PacketFence.
- `/usr/local/pf/raddb/users` : Definition of our local 802.1X user
- `/usr/local/pf/raddb/sites-enabled/packetfence` : Definition of the default virtual to configure the modules used in the different phase of the AAA (authenticate-authorization-accounting)
- `/usr/local/pf/raddb/sites-enabled/packetfence-tunnel` : Definition of a local virtual host mainly for tunnelled EAP processing. This is an extension of the default virtual host.
- `/usr/local/pf/raddb/packetfence.pm` : PacketFence's FreeRADIUS module. Talks with PacketFence server.

VLAN Access

- make sure to configure the Registration, Isolation, and Normal VLANs on the switch
- configure one switch port as a trunk port (dot1q) with access to all four VLANs. The native VLAN should be the management VLAN (1)
- connect your host's eth0 to the trunk port
- put one port of the switch in the Registration VLAN
- put another port in the Isolation VLAN
- assign a device with a static IP (configured with appropriate subnet) in the Registration VLAN

- assign a device with a static IP (configured with appropriate subnet) in the Isolation VLAN
- make sure the device in VLAN 2 can communicate with PacketFence through (and only through) eth0.2
- make sure the device in VLAN 2 can not communicate with any device in any other VLAN
- make sure the device in VLAN 3 can communicate with PacketFence through (and only through) eth0.3
- make sure the device in VLAN 3 can not communicate with any device in any other VLAN

Test

Register a device in VLAN enforcement

You can now test the registration process. In order to do so:

- connect an unregistered device into the switch
- make sure PacketFence receives the radius authentication request from the switch. Look into the PacketFence log file: /usr/local/pf/logs/packetfence.log
- make sure PacketFence handle radius request and sets the switch port into the registration VLAN (VLAN 2). Look again into PacketFence log file: /usr/local/pf/logs/packetfence.log

On the computer:

- open a web browser
- try to connect to a HTTP site (Not HTTPS, eg. http://www.google.com)
- make sure that whatever site you want to connect to, you have only access to the registration page.

Register the computer using:

- user: demouser
- password: demouser

Once a computer has been registered, make sure:

- PacketFence puts the switch port into the regular VLAN (VLAN 10)
- The computer has access to the network and the internet.

Additional Information

For more information, please consult the mailing archives or post your questions to it. For details, see:

- packetfence-announce@lists.sourceforge.net: Public announcements (new releases, security warnings etc.) regarding PacketFence
- packetfence-devel@lists.sourceforge.net: Discussion of PacketFence development
- packetfence-users@lists.sourceforge.net: User and usage discussions

Commercial Support and Contact Information

For any questions or comments, do not hesitate to contact us by writing an email to: support@inverse.ca.

Inverse (http://inverse.ca) offers professional services around PacketFence to help organizations deploy the solution, customize, migrate versions or from another system, performance tuning or aligning with best practices.

Hourly rates or support packages are offered to best suit your needs.

Please visit http://inverse.ca/ for details.

GNU Free Documentation License

Please refer to http://www.gnu.org/licenses/fdl-1.2.txt for the full license.