PacketFence ZEN Administration Guide

for version 4.0.0

PacketFence ZEN Administration Guide

by Inverse Inc.

Version 4.0.0 - April 2013

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 4.0.0 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, Fusion 3.x and Workstation 7.x with 1024MB RAM dedicated to the virtual machine. It might work using other VMWare products. You need a CPU that support long mode. In other words, you need to have a 64-bit capable CPU on your host.

We build two separate virtual machine, one to run on ESXi 4.0 (OVF format) and one to run on VMWare Fusion/Workstation (VMX/VMDK format).

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, isolation, MAC detection, registration, and a guest VLAN for wireless 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 4 is the MAC detection VLAN (empty VLAN: no DHCP, no routing, no nothing)
- VLAN 5 is the guest VLAN
- VLAN 10 is the “regular” VLAN
- VLAN 200 is the “inline” 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
4	Mac Detection			
5	Guests	192.168.5.0/24	192.168.5.10	192.168.5.10
10	Normal	192.168.1.0/24	192.168.1.1	192.168.1.10
200	Inline	192.168.200.0/24	192.168.200.10	192.168.200.10

DHCP/DNS

- We use a DHCP server on the PacketFence ZEN box which will take care of IP address distribution in VLANs 2,3,5,10, and 200

- We use a DNS server on the PacketFence ZEN box which will take care of domain resolution in VLANs 2 and 3

Installation

Import the virtual machine

PacketFence ZEN 4.0.0 comes in a pre-built virtual disk (OVF), or a pre-configured vmx file. You can import the vmx file in many VMWare desktop products and it will automatically create your VM. However, if you are using an ESX type hypervisor, you need to import the OVF 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 4095), and assign the profile to the PacketFence ZEN VM vEthernet.

Import to VMWare Player/Workstation for Linux

Newer version of VMWare Player handles the VLAN trunking a lot better. Having that said, we can use a single interface on the VM. So, you need to ensure that your VM host is plugged into a physical trunk port with VLAN 1,2,3,5,10 and 200 as the allowed VLAN.

Important

Please refer to the Annexe 1 if you have troubles using Workstation with only one trunked interface. We tested most with VMWare Player for Linux. We cannot support VMWare Fusion anymore, there are some issues when we need to do routing through Mac OS X VLAN interfaces.

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 plugged 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. http://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.

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 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 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 etho 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 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).

Since the MySQL installation is pre-built with the username "root" and the password "p@ck3tfence", you can simply enter these 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 retrive 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 trafic originating from these IPs, no rogue-dhcp alerts will be triggered. Don't forget to add your newly created local VLAN interface!

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.

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. In standard inline enforcement setup, you should not have to modify anything to make things work.

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 guests and production 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.

FreeRADIUS

PacketFence ZEN 4.0.0 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 MAC Detection, 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)
- Plug your host's etho to the trunk port
- put one port of the switch in the Registration VLAN

- put another port in the Isolation VLAN
- put another port in the MAC Detection VLAN
- plug a device with a static IP (configured with appropriate subnet) in the Registration VLAN
- plug a device with a static IP (configured with appropriate subnet) in the Isolation VLAN
- plug a device with a DHCP IP in the MAC Detection VLAN
- make sure the device in VLAN 2 can communicate with PacketFence through (and only through) etho.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) etho.3
- make sure the device in VLAN 3 can not communicate with any device in any other VLAN
- make sure the device in VLAN 4 can not communicate with any device in any other VLAN

Test

Register a device in inline enforcement

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

- Plug an unregistered device into the switch
- Make sure PacketFence provides an IP address to the user. Look into the following log file: /var/log/messages

On the computer:

- Open a web browser
- Try to connect to a site
- 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 changes the firewall (iptables) rules so that the user is authorized through. Look into PacketFence log file: /usr/local/pf/logs/packetfence.log
- The computer has access to the network and the internet.

Register a device in VLAN enforcement

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

- Plug an unregistered device into the switch
- Make sure PacketFence receives the appropriate trap from the switch. Look into the PacketFence log file: /usr/local/pf/logs/packetfence.log

- Make sure PacketFence handle the trap 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 site
- 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
- The computer has access to the network and the internet.

PacketFence Web Admin Interface

PacketFence provides a web admin interface. Go to https://DHCP_RECEIVED_IP:1443

- User: admin
- Password: p\@ck3tf3nc3

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/support.html for details.

GNU Free Documentation License

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

Appendix A. Legacy configuration for VMWare Workstation

- /etc/sysconfig/network-scripts/ifcfg-etho.2

```
DEVICE=eth0.2
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.2.2
NETMASK=255.255.255.0
VLAN=yes
```

- /etc/sysconfig/network-scripts/ifcfg-etho.3

```
DEVICE=eth0.3
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.3.2
NETMASK=255.255.255.0
VLAN=yes
```

- /etc/sysconfig/network-scripts/ifcfg-etho.5

```
DEVICE=eth0.5
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.5.2
NETMASK=255.255.255.0
VLAN=yes
```

- /etc/sysconfig/network-scripts/ifcfg-etho.10

```
DEVICE=eth0.10
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.2
NETMASK=255.255.255.0
VLAN=yes
```

- /etc/sysconfig/network-scripts/ifcfg-etho.200

```
DEVICE=eth0.200
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.200.2
NETMASK=255.255.255.0
VLAN=yes
```

Execute the VMware configuration utility (under Linux: vmware-config.pl) and define eth0, eth0.2, eth0.3, eth0.5, eth0.10, and eth0.200 as bridged networks.

Create five virtual network cards. They should be linked to /dev/vmnet0, /dev/vmnet1, /dev/vmnet2, /dev/vmnet3, /dev/vmnet4 and /dev/vmnet5. This way, the PacketFence ZEN virtual appliance will obtain six separate NICs which are able to communicate in VLANs 1, 2, 3, 5, 10 and 200.

Note

You may need to reconfigure the IP addresses on the VM interfaces. Refer to the previous IP and Subnet table to help you re-configure the interfaces.