PacketFence ZEN Administration Guide

for version 3.2.0

PacketFence ZEN Administration Guide

Olivier Bilodeau
François Gaudreault
Regis Balzard

Version 3.2.0 - February 2012

Revision History

Revision 2.0	2012-02-22	FG
Port from ODT to Asciidoc		
Revision 1.0	2009-01-29	RB
First OpenDocument version.		

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 3.2.0 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).

Inline Enforcement

Inline enforcement is enabled by default. Every device is supported, and the only thing you need to do is to drop the VM in the proper VLAN (Management and Inline VLAN) and bridge your devices to this inline VLAN. In other words, the eth0 of the VM is intended to be the management interface, and the eth0.200 interface (eth5 in the desktop version) is intended to be the inline interface. Hook them to the right place.

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.

Note

This mode is not enabled by default in the new ZEN version. To enable this mode, follow the indications in pf.conf, networks.conf, and start the proper ethernet interfaces on the VM, they are configured with “ONBOOT=no”.

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

Network Devices (VLAN enforcement)

Switch

- IP: 10.0.10.2
- Type: Catalyst 2960
- Uplink: fo/24
- SNMP Read Community = public
- SNMP Write Community = private
- Radius Secret (802.1X/MAC Auth.) = s3cr3t

Access Point

- IP: 10.0.10.3
- Type: Aironet 1242
- Uplink: fo/0
- Telnet username : Cisco, password: Cisco
- Public (MAC Auth.) SSID = InverseGuest
- Secure (WPA2) SSID = InverseSecure
- Radius Secret (802.1X/MAC Auth.) = s3cr3t

Wireless use case (VLAN enforcement)

For our setup, we are considering the following use case for the public SSID wireless users :

- Unregistered users will end in the registration VLAN, and hit the captive portal
- When registered, the user will be placed in the guest VLAN (VLAN 5)

For our setup, we are considering the following use case for the secure SSID wireless users :

- Unregistered users that provides valid 802.1X credentials will be automatically registered, and won't hit the captive portal.

- When registered, the user will be placed in the regular VLAN (VLAN 10)

Installation

Import the virtual machine

PacketFence ZEN 3.1.0 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

Administrative UI

- URL: https://dhcp_ip:1443
- Login: admin
- Password: p@ck3tf3nc3

Captive Portal / 802.1X Registration User

- Login: demouser
- Password: demouser

Configuration

Introduction

Since the PacketFence ZEN virtual machine comes as a pre-configured machine ready to serve, this section will explains how things are configured, and not how to configure them. For more information about custom configurations, please refer to the PacketFence 3.1.0 Administration Guide.

Tip

The following section may expose some of the ESX VM version configurations.

PacketFence Configurator

PacketFence provides a configurator that sets a minimum of options for you depending on the type of setup you want. You just have to choose the appropriate template and answer the questions. In our case, for the setup covered in this document, this portion was done. But, if you want to change subnets or other configuration parameters feel free to run the configurator again.

PacketFence configuration files

If you want to customize the provisioned 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.

Production DHCP

By default, we disabled the DHCP for the regular VLAN (VLAN 10). However, the network definitions are commented in conf/networks.conf. Simply remove the pound signs, and restart the packetfence service if you need it to be enabled.

FreeRADIUS

PacketFence ZEN 3.1.0 comes with a pre-configured FreeRADIUS to do Wired and Wireless 802.1X with EAP as well as MAC Authentication. The fictive Cisco 2960 and the Aironet 1242 are already configured as RADIUS clients, and we created a local user for the 802.1X authentication.

The main configuration files are :

- /etc/raddb/radiusd.conf : Configuration for the RADIUS service
- /etc/raddb/eap.conf : Configuration for 802.1X using EAP
- /etc/raddb/clients : Definition of our RADIUS clients
- /etc/raddb/users: Definition of our local 802.1X user
- /etc/raddb/sites-enabled/packetfence : Definition of the default virtual to configure the modules used in the different phase of the AAA (authenticate-authorization-accounting)
- /etc/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.
- /etc/raddb/packetfence.pm : PacketFence's FreeRADIUS module. Talks with PacketFence server.
- /etc/raddb/sql.conf : Relates to the RADIUS accounting and RADIUS clients configuration in PacketFence.

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

SNORT

SNORT is configured to listen and monitor the inline (etho.200) interface. However, no violations other than the default ones have been configured. This is done in the conf/violations.conf file or under Configuration › Violations in the Web Administration.

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 etho, etho.2, etho.3, etho.5, etho.10, and etho.200 as bridged networks.

Create five virtual network cards. They should be linked to /dev/vmneto, /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.