PacketFence ZEN – version 2.0.1

Installation Guide

Version 2.0.1 – December 2010

Contents

Chapter 1 **About this Guide** **3**
Other sources of information 3

Chapter 2 **System Requirements** **4**
Virtual Machine 4
VLAN Isolation 4

Chapter 3 **Assumptions** **5**
Network Setup 5
DHCP/DNS 5
Network Devices 6
Wireless use case 6

Chapter 4 **Installation** **7**
Import the virtual machine 7
Virtual Machine passwords 10

Chapter 5 **Configuration** **11**
Introduction 11
PacketFence Configurator 11
PacketFence configuration files 13
Network Devices 14
Production DHCP 14
FreeRADIUS 14
VLAN Access 14
IPTABLES 15
SNORT 16

Chapter 6 **Test** **17**
Register a device 17
PacketFence Web Admin Interface 17

Chapter 7 **Additional Information** **18**

Chapter 8 **Commercial Support and Contact Information** **19**

Chapter 9 **GNU Free Documentation License** **20**

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 2.0.1 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

System Requirements

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 64bit 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 Isolation

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

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

VLAN ID	VLAN Name	Subnet	Gateway	PacketFence Address
1	Management	10.0.10.0/24		10.0.10.1
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	192.168.1.10	192.168.1.10

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 and 10
- ❑ We use a DNS server on the PacketFence ZEN box which will take care of domain resolution in VLANs 2 and 3

Network Devices

Switch

- ❑ IP: 10.0.10.2
- ❑ Type: Catalyst 2960
- ❑ Uplink: f0/24
- ❑ 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: f0/0
- ❑ Telnet username : Cisco, password: Cisco
- ❑ Public (MAC Auth.) SSID = InverseGuest
- ❑ Secure (WPA2) SSID = InverseSecure
- ❑ Radius Secret (802.1X/MAC Auth.) = s3cr3t

Wireless use case

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 2.0.1 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 Fusion/Workstation

Because of a limitation in the way those products handle the VLAN tagging on the bridged interface, we need to do a little bit more efforts to make it work. In fact, the VMDK version is having 5 vEthernet cards, one for each VLAN it controls. You need to make sure that the following matchup is properly configured between the vEthernet and the host's VLAN interfaces :

- ❑ eth0 (VLAN1) --> eth0 on your host
- ❑ eth1 (VLAN2) --> eth0.2 on your host
- ❑ eth2 (VLAN3) --> eth0.3 on your host
- ❑ eth3 (VLAN5) --> eth0.5 on your host
- ❑ eth4 (VLAN10) --> eth0.10 on your host

For VMWare Workstation

Configure your Host with one NIC in each VLAN. For example under Linux:

- ❑ /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2

ONBOOT=yes

BOOTPROTO=static
```

```
IPADDR=192.168.2.2

NETMASK=255.255.255.0

VLAN=yes
```

- /etc/sysconfig/network-scripts/ifcfg-eth0.3

```
DEVICE=eth0.3

ONBOOT=yes

BOOTPROTO=static

IPADDR=192.168.3.2

NETMASK=255.255.255.0

VLAN=yes
```

- /etc/sysconfig/network-scripts/ifcfg-eth0.5

```
DEVICE=eth0.5

ONBOOT=yes

BOOTPROTO=static

IPADDR=192.168.5.2

NETMASK=255.255.255.0

VLAN=yes
```

- /etc/sysconfig/network-scripts/ifcfg-eth0.10

```
DEVICE=eth0.10

ONBOOT=yes

BOOTPROTO=static

IPADDR=192.168.1.2

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 and eth0.10 as bridged networks.

Create five virtual network cards. They should be linked to /dev/vmnet0, /dev/vmnet2, /dev/vmnet3,/dev/vmnet5, and /dev/vmnet10. This way, the PacketFence ZEN virtual appliance will obtain three separate NICs which are able to communicate in VLANs 1, 2, 3, 5, and 10.

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.

```
DEVICE=ethX

BOOTPROTO=static

ONBOOT=yes

HWADDR=[VETH_MAC_ADDRESS]

IPADDR=[IP ADDRESS]

NETMASK=255.255.255.0
```

For VMWare Fusion 3.x

In MAC OSX, we can also create VLAN interfaces. This is done in the System Preferences -> Network -> Settings (Icon) --> Manage Virtual Interfaces. Use vlanX as the name, where X is the VLAN ID.

Create one VLAN interface for each of the managed VLANs, which means 4 VLAN interfaces since we assume that the management VLAN is native. Then in the VM settings, match the virtual interface with the proper MAC OSX VLAN interface per the following :

- ❑ eth0 (VLAN1) --> Ethernet on your host
- ❑ eth1 (VLAN2) --> vlan2 on your host
- ❑ eth2 (VLAN3) --> vlan3 on your host
- ❑ eth3 (VLAN5) --> vlan5 on your host
- ❑ eth4 (VLAN10) --> vlan10 on your host

At this point, you should be able to start the virtual machine and connect to it.

Virtual Machine passwords

Management (SSH/Console) and MySQL

login: root

pwd: p@ck3tf3nc3

PacketFence Administrative UI

login: admin

pwd: p@ck3tf3nc3

Captive Portal / 802.1X Registration User

login: demouser

pwd: 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 2.0.1 Administration Guide.

NOTE: 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. Here is an example:

```
root@localhost pf]# cd /usr/local/pf/ && ./configurator.pl
Checking existing configuration...
No existing configuration found
Would you like to use a template configuration or custom [t|c] t
Which template would you like:
                        1) ARP mode in Testing
                        2) ARP mode with Registration
                        3) ARP mode with Detection (snort)
                        4) ARP mode with Registration and Detection
(snort)
                        5) ARP mode with Registration, Detection
(snort) & Scanning (nessus)
                        6) ARP mode with Session-based
Authentication
                        7) VLAN isolation mode with Registration
                        8) VLAN isolation mode with Registration and
Detection (snort)
                        9) VLAN isolation mode ready for PacketFence
ZEN
 [1|2|3|4|5|6|7|8|9] 9
  Setting option network.mode to template value vlan
  Setting option network.dhcpdetector to template value enabled
  Setting option trapping.testing to template value disabled
```

```
  Setting option trapping.registration to template value enabled
  Setting option trapping.detection to template value disabled
  Setting option registration.auth to template value local
  Setting option database.user to template value pf
  Setting option database.host to template value localhost
  Setting option database.pass to template value pfz3n
  Setting option database.db to template value pf
  Setting option database.port to template value 3306
  Setting option vlan.dhcpd to template value enabled
  Setting option vlan.named to template value enabled
Loading Template: Warning PacketFence is going LIVE - WEAPONS HOT

** NOTE: The configuration can be a bit tedious.  If you get bored,
you can always just edit /usr/local/pf/conf/pf.conf directly **

GENERAL CONFIGURATION
DNS Domain Name (current: , default: example.com [?]): pfzen.local
pfzen.local - ok? [y|n] y
Host Name (without DNS domain name) (current: , default: abc [?]):
pf-zen
pf-zen - ok? [y|n] y
DNS Servers including PacketFence (comma delimited) (current:
192.168.1.1, default: 127.0.0.1 [?]):
192.168.1.1,192.168.2.10,192.168.3.10
192.168.1.1,192.168.2.10,192.168.3.10 - ok? [y|n] y
DHCP Servers including PacketFence (comma delimited) (default:
127.0.0.1 [?]): 192.168.1.10,192.168.2.10,192.168.3.10,192.168.5.10
192.168.1.10,192.168.2.10,192.168.3.10,192.168.5.10 - ok? [y|n] y
Your isolation mode is vlan. If you are interested in SNMP trap
statistics please create the following crontab entry

*/5 * * * * /usr/local/pf/bin/pfcmd traplog update
What is my management interface? (default: <NONE>) [eth0|eth0.5|
eth0.3|eth0.2|eth0.10|?]: eth0.10
eth0.10 - ok? [y|n] y
What is its IP address? (current: 192.168.1.10, default: <NONE>
[?]):
192.168.1.10 - ok? [y|n] y
What is its mask? (current: 255.255.255.0, default: <NONE> [?]):
255.255.255.0 - ok? [y|n] y
What is my gateway? (current: 192.168.1.1, default: <NONE> [?]):
192.168.1.1
192.168.1.1 - ok? [y|n] y

DHCP AND DNS CONFIGURATION FOR REGISTRATION NETWORK

What is the REGISTRATION network prefix (ex: 192.168.1.0)? (default:
<NONE> [?]): 192.168.2.0
192.168.2.0 - ok? [y|n] y
What is the REGISTRATION network mask (ex: 255.255.255.0)? (default:
<NONE> [?]):
<NONE> - ok? [y|n] n
What is the REGISTRATION network mask (ex: 255.255.255.0)? (default:
<NONE> [?]): 255.255.255.0
255.255.255.0 - ok? [y|n] y
```

```
What is the IP address of PacketFence in the REGISTRATION network?
(default: <NONE> [?]): 192.168.2.10
192.168.2.10 - ok? [y|n] y
What is the REGISTRATION network DHCP scope starting address?
(default: <NONE> [?]): 192.168.2.11
192.168.2.11 - ok? [y|n] y
What is the REGISTRATION network DHCP scope ending address?
(default: <NONE> [?]): 192.168.2.254
192.168.2.254 - ok? [y|n] y


TRAPPING CONFIGURATION

ALERTING CONFIGURATION
Where would you like notifications of traps, rogue DHCP servers, and
other sundry goods sent? (default: pf@localhost [?]):
pf@localhost - ok? [y|n] y
What should I use as my SMTP relay server? (default: localhost [?]):
localhost - ok? [y|n] y

DATABASE CONFIGURATION
Where is my database server? (default: localhost [?]):
localhost - ok? [y|n] y
What port is is listening on? (default: 3306 [?]):
3306 - ok? [y|n] y
What database should I use? (default: pf [?]):
pf - ok? [y|n] y
What account should I use? (default: pf [?]):
pf - ok? [y|n] y
What password should I use? (current: pfz3n, default: packet [?]):
pfz3n - ok? [y|n] y
Please review conf/pf.conf and conf/networks.conf to correct any
errors or change pathing to daemons
```

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 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 2.0.1 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/default : Definition of the default virtual to configure the modules used in the different phase of the AAA (authenticate-authorization-accounting)
- ❑ /etc/raddb/sites-enabled/inner-tunnel : Definition of a local virtual host mainly for tunnelled EAP processing. This is an extension of the default virtual host.

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 eth0 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) 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
- ❑ make sure the device in VLAN 4 can not communicate with any device in any other VLAN

IPTABLES

You need to open the following ports in IPTABLES:

- ❑ 162 (SNMP) and 1443 (Web Admin Interface) on eth0
- ❑ 53 (DNS), 80 (HTTP), 443 (HTTPS) on eth0.2 and eth0.3

Here are the /etc/sysconfig/iptables lines for our setup:

```
-A RH-Firewall-1-INPUT -p udp -m udp --dport 53 -s 192.168.2.0/24 -d
192.168.2.10 -i eth0.2 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 53 -s 192.168.3.0/24 -d
192.168.3.10 -i eth0.3 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 80 -s 192.168.2.0/24 -d
192.168.2.10 -i eth0.2 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 80 -s 192.168.3.0/24 -d
192.168.3.10 -i eth0.3 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 162 -d 10.0.10.1 -i
eth0 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 1812 -d 10.0.10.1 -i
eth0 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 1813 -d 10.0.10.1 -i
eth0 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 443 -s 192.168.2.0/24
-d 192.168.2.10 -i eth0.2 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 443 -s 192.168.3.0/24
-d 192.168.3.10 -i eth0.3 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 1443 -d 192.168.1.10 -i
eth0.10 -j ACCEPT
```

SNORT

SNORT is configured to listen and monitor the production (eth0.10) interface. However, no violations other than the default ones have been configured. This is done in the conf/violations.conf file.

Test

Register a device

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
- ❑ pwd: 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://192.168.1.10:1443

- ❑ uid: admin
- ❑ pwd: 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.