Cisco Quick Installation Guide

for PacketFence version 5.0.0

Cisco Quick Installation Guide

by Inverse Inc.

Version 5.0.0 - Mar 2015

Table of Contents

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 Cisco Catalyst equipment.

The instructions are based on version 5.0.0 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;
- A Cisco Catalyst 2960 switch loaded with the latest IOS 15.0 available.

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 to the customer network (for Production Access)

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 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 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 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 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 setted 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 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.

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 a Cisco Catalyst 2960 in PacketFence

Now that you have a fully functionnal PacketFence installation, you'll need to add the Cisco Catalyst 2960 to the PacketFence switches database for correct intergration.

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.

We'll use the clone function to add a new switch (the Catalyst 2960) 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 Catalyst 2960 switch on the customer management
 network
Type: Cisco::Catalyst_2960
Mode: Production
Vlans: 2,3,10
Normal VLAN: 10
Registration VLAN: 2
Isolation VLAN: 3
SNMP Version: 2c
SNMP Read Community: ciscoRead
SNMP Write Community: ciscoWrite
RADIUS Secret: aSecurePassword
```

Click Add switch

The newly added switch should shows up in the list.

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

Step 3: Configure the Cisco Catalyst 2960

This section 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
```

Configure switchports for 802.1X

Once AAA is ready, we can configure some or all switchports to perform 802.1X. The following configuration will make your switchports to do 802.1X with MAB failback (w/o voice support):

```
switchport mode access
authentication host-mode single-host
authentication order dot1x mab
authentication priority dot1x mab
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, add the following lines to your interface configuration:

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

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 SNMP

Finally, for some operations, 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
```

Save the config!

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

Step 4: Configuration of Windows 7 client for wired 802.1X

For demonstration purpose, you need a Windows 7 laptop capable of doing 802.1X. This section will explain you how to configure the laptop' supplicant. You need administrator rights to do the following steps.

1. Click on Start, then in the search field, write services.msc, then hit enter.
2. In the Services dialog box, click the Standard tab, right click on "Wired AutoConfig", and then click Start.
3. Open Network Connections by clicking the Start button , clicking Control Panel, clicking Network and Internet, clicking Network and Sharing Center, and then clicking Manage network connections.
4. Right-click the connection that you want to enable 802.1X authentication for, and then click Properties. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
5. Click the Authentication tab, and then select the Enable IEEE 802.1X authentication check box.
6. Select PEAP as the authentication method, and click Settings. Uncheck Validate server certificate.
7. On the same tab click Configure and uncheck Automatically use my Windows logon name and password.
8. Return on the Security tab and click on Advanced settings. On 802.1X settings, click on Specify authentication mode and select User authentication.
9. 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 switch from the PacketFence environment
- login the PacketFence administrative UI (https://management_IP:1443)
- connects a client device on an 802.1X switchport using demouser/demouser credentials, and show a registration.