CoovaChilli Quick Integration Guide

for PacketFence version 7.4.0

CoovaChilli Quick Integration Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018

Table of Contents

Chapter 1

About this Guide

This guide has been created in order to help setting up a consumer grade access point running CoovaChilli integration with PacketFence to use UAM capabilities along with PacketFence feature set. It can also help sales engineers, product managers, or network specialists demonstrate the PacketFence capabilities on-site with an existing or potential customer, or, provide guidelines to setup a proof of concept for a potential PacketFence deployment using CoovaChilli capable products.

The instructions are based on version 7.4.0 of the PacketFence Zero Effort NAC (ZEN) image.

Chapter 2

Assumptions

- You have a CoovaChilli capable access point running LEDE/OpenWRT, on which CoovaChilli is installed (CoovaChilli installation is not covered in this guide);
- You have a virtual "host" on which it is possible to load the latest PacketFence ZEN image;
- Network interconnection between the virtual "host" running the latest PacketFence ZEN image, the CoovaChilli capable access point, and Internet is functional;
- A PacketFence WebAuth enforcement setup will be deployed;

Quick Deployment

Step 0: Get PacketFence Zero Effort NAC (ZEN) latest image

This step is only required in the case you do not already have a working PacketFence installation. If it’s the case, you might want to go ahead and proceed with step 1 (or maybe 2) and further.

In the scope of ease the process, we recommend using latest PacketFence ZEN image available to download on the PacketFence website. You can find it at https://packetfence.org/download.html#/zen under the *Virtual Appliance (OVF)* section.

Having the ZEN image on hand, load it onto the virtual host and fire it up. You should be able to access it using *https://IP_ADDRESS:1443* which will bring the PacketFence configurator

Step 1: Basic PacketFence and network installation / configuration

This step again, is only required in the case you do not already have a working (and configured) PacketFence installation. If it’s the case, you might want to go ahead and proceed with step 2.

Network interconnectivity

For the scope of this guide, the following network setup will be configured. Please note that a more complex configuration can easily be used but will not be covered in this guide.

- 1 switch port configured as access onto a "management" VLAN to connect the CoovaChilli capable access point
- 1 switch port configured as access onto that same "management" VLAN mapped to the PacketFence ZEN virtual machine
- Internet access through that same "management" VLAN

The final design should allow PacketFence to communicate with the CoovaChilli capable access point, the opposite, and a full access to the Internet for both using that "management" VLAN.

PacketFence basic configuration

Assuming you are able to reach the configurator running from the ZEN image, follow theses quick guidelines to go through the configurator and have a PacketFence installation working in WebAuth enforcement mode.

Step 1: Enforcement

The choice made on this step will influence the next steps 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 the purpose of this guide, we will choose *WebAuth 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. Persistence will be written only for *enabled* interfaces.

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

Note that you can only set ONE (1) management interface but a same management interface can serve multiple purposes.

For the purpose of this guide, we will use only one interface which we will configure as the "management" one and on which we will add a *portal* additional daemon.

To do so, simply click the network interface name you want to assign and in the edit modal window, make the following changes then click "Save":

- Type: Management
- Additional listening daemon(s): portal

You might want to make sure the "Default Gateway" is properly set. This is generally the gateway of the management network.

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).

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 created 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 retrieve 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*.

Step 4: PacketFence Configuration

This step will configure the general options of your PacketFence installation.

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 traffic originating from these IPs, no rogue-dhcp alerts will be triggered. It can safely be ignored for the purpose of this guide.

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 5.

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.

Step 2: Access Point and CoovaChilli Configuration

Now that we have a functional PacketFence installation, we will go ahead and start by configuring the access point and CoovaChilli running on it. We will then use some of the configuration parameters to finish PacketFence integration in step 3.

This guide assume that CoovaChilli is installed on the access point. If it's not, we suggest you search relevant information on the Internet to install CoovaChilli as there are too many network equipment vendors that support CoovaChilli to accurately document this step here.

The guide also assumes that you have an SSID configured on the access point. Assumption is also made that the network interface / bridge is configured and assigned for the given SSID.

You should also make sure to have a default route properly configured on the access point (so that it can access the Internet) and that DNS resolution is working.

Also note that changes on the OpenWRT access point are done using SSH shell access.

Please note that any interface name reference might be different from one equipment vendor to an other.

Configure chilli

chilli configuration might differ from one equipment vendor to an other one. Just make sure to follow these configuration guidelines and you should be all-set.

- chilli configuration file can be found under

```
/etc/config/chilli
```

- Edit the following parameters to integrate with PacketFence

```
option disabled 1        This should be commented out so that chilli is marked
 as enabled
option dns1              Set this to a working DNS server (this will be used by
 hotspot clients)
option dns2              Set this to a working DNS server (this will be used by
 hotspot clients)
option ipup              /etc/chilli/up.sh (Depending on the package, the script
 path might need to be adjusted)
option ipdown            /etc/chilli/down.sh (Depending on the package, the
 script path might need to be adjusted)
option radiusserver1     PacketFence management IP
option radiusserver2     PacketFence management IP
option radiussecret      The RADIUS secret that will be used between chilli and
 PacketFence
option radiusnasid       Access-point IP address
option dhcpif            The network interface / bridge assigned to the SSID
 (Hotspot clients network)
option uamserver         http://PACKETFENCE_MANAGEMENT_IP/CoovaChilli
option ssid              SSID name
option nasip             Access-point IP address
option coaport           3799
```

A startup script might be required depending on the equipment vendor. Again, a quick documentation search on the Internet might be the best solution to find the best one

Once set up, you might want to activate chilli at boot (by using the startup script) and finally, reboot the AP.

Step 3: PacketFence configuration for CoovaChilli integration

Having a working PacketFence installation and a configured LEDE / OpenWRT access point running CoovaChilli, the last step is PacketFence configuration for CoovaChilli integration.

To do so, login to the PacketFence web administration interface if it is not already done.

Switch configuration

Click on the *Configuration* tab and select the *Switches* menu option under the *NETWORK* section on the left hand side.

On the bottom of the page, click the *Add switch to group* button then select the *default* to bring up the *New Switch* configuration modal window.

Definition tab

- **IP**: Access-point IP address
- **Type**: CoovaChilli
- **Mode**: Production
- **External Portal Enforcement**: Checked

RADIUS tab

- **Secret Passphrase**: The RADIUS secret configured in the previous step

Click *Save*

Portal configuration

It is required to disable HTTPS redirection by clicking the *Configuration* tab and then the *Captive portal* menu option on the left hand side. Make sure *Secure redirect* is unchecked.