OpenWrt BarrierBreaker 14.07 with hostapd Quick Integration Guide

for PacketFence version 7.4.0

OpenWrt BarrierBreaker 14.07 with hostapd Quick Integration Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018

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 OpenWrt BarrierBreaker 14.07 with Hostapd.

Introduction

This guide will provide an example for the configuration of an open SSID (not encrypted) and a secured SSID (802.1X). You will need to install wpad and hostapd. These two SSIDs will do RADIUS authentication against PacketFence.

Assumptions

- You have a configured PacketFence environment with working test equipment
- The management IP of PacketFence will be 192.168.1.10 and has s3cr3t as its RADIUS shared secret
- You have an access point with OpenWrt BarrierBreaker 14.07 installed

Quick installation

Step 1: Packages installation

You can install the packages from the web interface of OpenWrt.

Go to **System → Software**

First update the repos by clicking the button Update lists if it's not up to date.

Then you will have to install the packages of Hostapd and wpad.

Go to the tab *Available packages* and then search for the package hostapd into the *Filter:* field.

Click Install the hostapd package, the actual version is 2014-06-03.1-1.

Do the same process for the wpad package version 2014-06-03.1-1.

Note

You will need the packages hostapd-commun and wpad-mini if they are not installed by default.

Step 2: Dynamic VLAN Configuration

Connect using SSH to the AP and create the file : /etc/config/hostapd.vlan

```
*          wlan0.#
```

Step 3: Hostapd configuration

You will need to modify the hostapd script that comes with the package that we previously installed.

Connect using SSH to the AP and run these commands:

```
cd /lib/netifd/
mv hostapd.sh hostapd.sh.old
opkg install curl
curl --insecure  https://github.com/inverse-inc/packetfence/tree/devel/addons/
hostapd/hostapd-14.07.sh >  hostapd.sh
wifi
```

Step 4: Configure the SSIDs

To configure the PF-Open SSID, we will use UCI:

```
uci add_list wireless.@wifi-iface[0]="wifi-iface"
uci add_list wireless.@wifi-iface[0].device="radio0"
uci add_list wireless.@wifi-iface[0].mode="ap"
uci add_list wireless.@wifi-iface[0].ssid="PF-Open"
uci add_list wireless.@wifi-iface[0].network="lan"
uci add_list wireless.@wifi-iface[0].encryption="none"
uci add_list wireless.@wifi-iface[0].auth_server="192.168.1.10"
uci add_list wireless.@wifi-iface[0].auth_port="1812"
uci add_list wireless.@wifi-iface[0].auth_secret="s3cr3t"
uci add_list wireless.@wifi-iface[0].acct_server="192.168.1.10"
uci add_list wireless.@wifi-iface[0].acct_port="1813"
uci add_list wireless.@wifi-iface[0].acct_secret="s3cr3t"
uci add_list wireless.@wifi-iface[0].dynamic_vlan="2"
uci add_list wireless.@wifi-iface[0].vlan_file="/etc/config/hostapd.vlan"
uci add_list wireless.@wifi-iface[0].vlan_tagged_interface="eth0"
uci add_list wireless.@wifi-iface[0].dae_secret="s3cr3t"
uci add_list wireless.@wifi-iface[0].dae_client="192.168.1.10"
uci add_list wireless.@wifi-iface[0].dae_port="3799"
uci add_list wireless.@wifi-iface[0].macfilter="2"
uci add_list wireless.@wifi-iface[0].nasid="ubiquiti"
uci commit
```

Configure the PF-Secure SSID:

```
uci add_list wireless.@wifi-iface[0]="wifi-iface"
uci add_list wireless.@wifi-iface[0].device="radio0"
uci add_list wireless.@wifi-iface[0].mode="ap"
uci add_list wireless.@wifi-iface[0].ssid="PF-Secure"
uci add_list wireless.@wifi-iface[0].network="lan"
uci add_list wireless.@wifi-iface[0].encryption="wpa2"
uci add_list wireless.@wifi-iface[0].auth_server="192.168.1.10"
uci add_list wireless.@wifi-iface[0].auth_port="1812"
uci add_list wireless.@wifi-iface[0].auth_secret="s3cr3t"
uci add_list wireless.@wifi-iface[0].acct_server="192.168.1.10"
uci add_list wireless.@wifi-iface[0].acct_port="1813"
uci add_list wireless.@wifi-iface[0].acct_secret="s3cr3t"
uci add_list wireless.@wifi-iface[0].dynamic_vlan="2"
uci add_list wireless.@wifi-iface[0].vlan_file="/etc/config/hostapd.vlan"
uci add_list wireless.@wifi-iface[0].vlan_tagged_interface="eth0"
uci add_list wireless.@wifi-iface[0].dae_secret="s3cr3t"
uci add_list wireless.@wifi-iface[0].dae_client="192.168.1.10"
uci add_list wireless.@wifi-iface[0].dae_port="3799"
uci add_list wireless.@wifi-iface[0].macfilter="2"
uci add_list wireless.@wifi-iface[0].nasid="ubiquiti"
uci commit
```

In order to apply this configuration, when you are connected using SSH on the AP, run the command *wifi*. It will reload the configuration and broadcast the SSID.

Note

It's known that you can't put 2 SSIDs with the same dae server at the same time. The deauthentication will not work on the second SSID.

Step 5: PacketFence configuration

Log in to the PacketFence administration web page and go under **Configuration → Policies and Access Control → Switches → Add switch**.

Definition:

- **IP Address/MAC Address/Range (CIDR)**: IP of your access point
- **Type**: Hostapd
- **Mode**: production
- **Deauthentication Method**: RADIUS
- **Dynamic Uplinks**: Checked

Roles:

- **Role by VLAN ID**: Checked
- **Registration**: Your registration VLAN ID
- **Isolation**: Your isolation VLAN ID

RADIUS:

- **Secret Passphrase**: s3cr3t

Save this configuration by clicking the *Save* button.

Step 6: Troubleshoot

Here few things you can do/check to see if you configuration is working.

To check the wireless configuration: uci show wireless or cat /etc/config/wireless

To check if your configuration is correctly set into the Hostapd configuration file: cat /var/run/his