



Developer's Guide

for PacketFence version 9.2.0

Developer's Guide

by Inverse Inc.

Version 9.2.0 - November 2019

Copyright © 2019 Inverse inc.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

The fonts used in this guide are licensed under the SIL Open Font License, Version 1.1. This license is available with a FAQ at: <http://scripts.sil.org/OFL>

Copyright © Łukasz Dziejdzic, <http://www.latofonts.com>, with Reserved Font Name: "Lato".

Copyright © Raph Levien, <http://levien.com/>, with Reserved Font Name: "Inconsolata".

A decorative graphic consisting of a series of light blue, stylized characters that resemble a mix of Latin and Cyrillic letters, including 'e', 'z', 'r', 'e', 'v', 'n', 'j'. The characters are rendered in a clean, sans-serif font style.

Table of Contents

About this Guide	1
Other sources of information	1
Documentation	2
AsciiDoc documentation	3
Documentation Conventions	3
Checklist to create a new guide	6
Golang environment	7
PacketFence Golang libraries	7
Code conventions	10
Code style	10
HTTP JSON API	12
How to use the API	12
Customizing PacketFence	14
Captive Portal	14
Adding custom fields to the database	16
VLAN assignment	17
SNMP	18
Introduction	18
Obtaining switch and port information	18
Supporting new network hardware	20
Switch	20
Wireless Access-Points or Controllers	24
The "adding a new network device module in PacketFence" checklist	25
Creating a new Switch via a Template	26
Required Parameters	26
RADIUS scope Parameters	26
Comments	26
Defining RADIUS Attributes	27
RADIUS Vendor Attributes for CoA	27
Dynamic RADIUS Attribute Value Syntax	27
PacketFence builds	34
Packer	34
Anatomy of Packer template	34
How to build Docker images ?	35
Troubleshooting	35
Developer recipes	36
Running development version	36
Contributing	38
Creating patches	38
Translations	39
Admin GUI	39
Additional Information	41
Commercial Support and Contact Information	42
GNU Free Documentation License	43

About this Guide

This guide will help you modifying PacketFence to your particular needs. It also contains information on how to add support for new switches.

The latest version of this guide is available at <https://packetfence.org/documentation/>.

Other sources of information

Network Devices Configuration Guide	Covers switch, controllers and access points configuration.
Administration Guide	Covers PacketFence installation, configuration and administration.
NEWS	Covers noteworthy features, improvements and bug fixes by release.
UPGRADE	Covers compatibility related changes, manual instructions and general notes about upgrading.
ChangeLog	Covers all changes to the source code.

These files are included in the package and release tarballs.

Documentation

The in-depth or more technical documentation is always as close to the code as possible. Always look at the **POD** doc¹. To do so, the preferred way is using the **perldoc** command as follows:

```
perldoc lib/pfconfig/cached.pm
```

¹Perl's Plain Old Documentation: <http://perldoc.perl.org/perlpod.html>

AsciiDoc documentation

Documentation Conventions

Source: [AsciiDoc Mark-up Quick Reference for Red Hat Documentation](#)




Note

Some markup examples used in this overview are based on new AsciiDoctor features and they are not a part of the standard set of elements. Please, use the `:experimental:` tag in the header of your document to enable this functionality.

Element	Mark-up	Example rendered output
Application name	No special markup	The foo application.
Code blocks	<pre>[source,golang] ---- package main import "fmt" func main() { fmt.Println("Hello World !") } ----</pre>	<pre>package main import "fmt" func main() { fmt.Println("Hello World !") }</pre>
Code - inline	<code>`print("Hello, World!")`</code>	<code>`print("Hello, World!")`</code>
Command block	<pre>---- \$ echo "Hello, World!" > hello.txt ----</pre>	<pre>\$ echo "Hello, World!" > hello.txt</pre>
Command - inline	Use the <code>[command]</code> <code>`oc get`</code> command to get a list of services.	Use the <code>[command]</code> <code>oc get</code> command to get a list of services.
Emphasis for a term	Use <code>_this_</code> approach.	Use <i>this</i> approach.

Filenames or directory paths	<p>Edit the [filename]`pf.conf` file as required and save your changes.</p> <p>The [filename]`networks.conf` configuration file is located in the [filename]`/usr/local/pf/` directory.</p>	<p>Edit the [filename]`pf.conf` file as required and save your changes.</p> <p>The [filename]`networks.conf` configuration file is located in the [filename]`/usr/local/pf/` directory.</p>
GUI Text	The web browser displays *404* for an unreachable URL.	The web browser displays 404 for an unreachable URL.
GUI Button (experimental feature, AsciiDoctor only)	Click btn:[Save As] to save the file under a different name.	Click btn:[Save As] to save the file under a different name.
GUI Menu (experimental feature, AsciiDoctor only)	Navigate to menu:File[Import>Import csv] to import a csv file.	Navigate to menu:File[Import>Import csv] to import a csv file.
GUI button and menu (non-experimental)	Navigate to <code>_Configuration -> Policies and Access Control_</code>	Navigate to <i>Configuration → Policies and Access Control</i>
Inline Image	<code>image::image.png[width=25px]</code>	<code>image::image.png[width=25px]</code>
Block Image	<code>.Tux image::image.png[width=100px]</code>	<code>.Tux image::image.png[width=100px]</code>
Inline operations and user input	<p>The `GET` operation can be used to do something.</p> <p>Answer by typing `Yes` or `No` when prompted.</p>	<p>The GET operation can be used to do something.</p> <p>Answer by typing Yes or No when prompted.</p>
Keyboard shortcuts (experimental feature, AsciiDoctor only)	<code>kbd:[Ctrl+Alt+Del]</code>	<code>kbd:[Ctrl+Alt+Del]</code>
Link (external)	<code>link:http://www.packetfence.org[PacketFence]</code>	<code>link:http://www.packetfence.org[PacketFence]</code>

<p>Lists</p>  <p>Note</p> <p>Do not put steps in bold.</p>	<pre>.Ordered list . First item . Second item . Third item .Unordered list * This * That * The other .Definition or labeled list Term A:: description Term B:: description .Checklist * [] first step ** [] first task ** [] second task * [] second step * [] third step</pre>	<p>Ordered list</p> <ol style="list-style-type: none"> 1. First item 2. Second item 3. Third item <p>Unordered list</p> <ul style="list-style-type: none"> ▪ This ▪ That ▪ The other <p>Definition or labeled list</p> <p>Term A description</p> <p>Term B description</p> <p>Checklist</p> <ul style="list-style-type: none"> ▪ [] first step <ul style="list-style-type: none"> ▪ [] first task ▪ [] second task ▪ [] second step ▪ [] third step
<p>Literal value</p>	<pre>The function returns `true`.</pre>	<p>The function returns true.</p>
<p>Package</p>	<pre>Install the [package]`packetfence` package.</pre>	<p>Install the [package]packetfence package.</p>
<p>Product name</p>	<p>No special markup. Use {nbsp} in the company and product names. Example: Inverse{nbsp}Inc.</p>	<p>Inverse Inc.</p>
<p>Reference to Packet-Fence guides</p>	<pre>See the PacketFence link:guide- url[_Installation Guide_] for more information.</pre>	<p>See the PacketFence Installation Guide for more information.</p>

System or software variable to be replaced by the user	Use the following command to roll back a deployment, specifying the deployment name: <code>`oc rollback _deployment_`</code> .	Use the following command to roll back a deployment, specifying the deployment name: <code>oc rollback _deployment_</code> .
System or software configuration parameter or environment variable	Use the <code>`_IP_ADDRESS_`</code> environment variable for the server IP address.	Use the <code>_IP_ADDRESS_</code> environment variable for the server IP address.
System item, daemon, or service	<p>Include the <code>`pf::Switch`</code> library.</p> <p>Stop the <code>`pfqueue`</code> daemon.</p> <p>Start the <code>`iptables`</code> service.</p>	<p>Include the <code>pf::Switch</code> library.</p> <p>Stop the <code>pfqueue</code> daemon.</p> <p>Start the <code>packetfence-iptables</code> service.</p>

Shell commands in code blocks

To ease copy-paste of shell commands:

- Remove useless characters in code blocks like `#` or `$`
- Split long lines with `\`

Checklist to create a new guide

- create `PacketFence_GUIDENAME.asciidoc` based on PacketFence [Template Guide](#)
- create `PacketFence_GUIDENAME-docinfo.xml` with only `copyright` tag
- update `all` target in Makefile
- update packaging (if necessary)
- update website listing to add a new guide

Golang environment

PacketFence Golang libraries

Basic setup

This is a guide on how to setup/use the PacketFence Golang libraries.

In order to bootstrap your environment:

```
cd /usr/local/pf/go
make go-env
```

If you work directly on sources, you can run:

```
cd go
GO_REPO=${PWD} make go-env
```

This will install Golang version use to build PacketFence Golang binaries and check if all modules defined in [filename]go.mod are available.

You should then source your .bashrc to get the new environment variables:

```
source ~/.bashrc
```

You can get a complete overview of your Golang environment with [command]go env command.

Pulling the dependencies

Dependencies use go modules and will be fetched automatically during build time.

You will also need [package]ipset-devel and [package]pkgconfig libraries which can be installed using the following command:

CentOS.

```
yum install ipset-devel pkgconfig
```

Debian.

```
apt install libipset-dev pkg-config
```

Building the code

All code should be built into a Caddy middleware which we'll then use in a [filename]Caddyfile to create our recipes. Only reason for not using Caddy would be that the binaries doesn't interact using HTTP (which Caddy can handle at some point). For now, we'll focus only on services using HTTP until we're comfortable with Caddy.

A local version of Caddy is in [filename]caddy/caddy. This is a vendored version of Caddy which includes the plugins and middlewares for PacketFence.

In order to build the Caddy HTTP service (`pfhttpd`):

```
make pfhttpd
```

Do the same to build `pfdns`, `pfdhcp`, `pfdetect` and `pfstats`:

```
make all
make copy
```

Creating a service

Once you've built `pfhttpd`, you can use a [filename]Caddyfile to load your middleware and bind it on a specific port:

```
localhost:1234 {
  logger {
    requesthistory 100
    level DEBUG
  }
  statsd {
    proto udp
    prefix pfsso
  }
  pfsso
}
```

This file should be put in [filename]/usr/local/pf/conf/caddy-services/pfexample.conf

Note how you can control the logger configuration from the [filename]Caddyfile. If your middleware (in this example `pfsso`) uses or calls the logger, you **must** declare it in your [filename]Caddyfile.

If your middleware uses `statsd`, you don't have to configure `statsd` in your [filename]Caddyfile which will result in the packets just not being sent (a dummy `statsd` client will be created).

You can start `pfhttpd` with your [filename]Caddyfile using the following command:

```
/usr/local/pf/sbin/pfhttpd -conf /usr/local/pf/conf/caddy-services/pfexample.conf
```

Once you have ascertained that the service is working correctly, you need to create an instance of `pf::services::manager` for it. You will also need to create a unitfile for it in `[filename]conf/systemd` like the following:

```
[Unit]
Description=PacketFence Example Service
Wants=packetfence-base.target packetfence-config.service packetfence-iptables.service
After=packetfence-base.target packetfence-config.service packetfence-iptables.service
Before=packetfence-pfexample.service

[Service]
PIDFile=/usr/local/pf/var/run/pfexample.pid
ExecStart=/usr/local/pf/sbin/pfhttpd -conf /usr/local/pf/conf/caddy-services/pfexample.conf
Restart=on-failure
Slice=packetfence.slice

[Install]
WantedBy=packetfence.target
```

Make sure that the packaging is also updated to copy those files in the `[filename]/usr/lib/systemd/system` directory.

Running the tests

Like the perl unit tests, the Golang tests rely on the presence of the test `pfconfig` process to execute properly.

In order to start the test `pfconfig` process:

```
cd /usr/local/pf/t && ./pfconfig-test
```

You can proceed to execute all or some of the Golang unit tests:

```
cd /usr/local/pf/go
go test ./...

cd /usr/local/pf/go/firewallsso/lib
go test
```

In order to run all the tests easily you can also do:

```
cd /usr/local/pf/go
make test
```

Code conventions

Code style



Caution

Work in progress.

We are slowly migrating away from an automated `perltidy` code style. The reason we are not doing another pass of tidy is that it messes up code history and makes maintainer's job more complicated than it should be. Every new change uses the new guidelines so over time the old code style will slowly disappear.

- Lines of 120 character width maximum
- No tab characters
- Stay consistent with surrounding white spaces
- Document each subroutine in POD format (`perldoc perlpod`)
- Use constants instead of hard coded strings or numbers (use `constant` or `Readonly` modules)
- in object-oriented modules we use CamelCase ¹ notation (ex: `$radiusRequest->getVoIpAttributes();`)
- in procedural modules we use Perl's usual notation (ex: `$node_info{'pid'} = $current_request{'pid'};`)
- regular expressions should be documented (with the `/x` modifier)

```

if ($phone_number =~ /
    ^\(?([2-9]\d{2})\)? # captures first 3 digits allows parens
    (?-|\.|\\s)?      # separator -, ., space or nothing
    (\d{3})           # captures 3 digits
    (?-|\.|\\s)?      # separator -, ., space or nothing
    (\d{4})$         # captures last 4 digits
    /x) {
    return "$1$2$3";
}

```

¹<http://en.wikipedia.org/wiki/CamelCase>

- SQL should be capitalized, properly indented and always use named fields (no *)

```
$node_statements->{'node_add_sql'} = get_db_handle()->prepare(<<'SQL');
    INSERT INTO node (
        mac, pid, category_id, status, voip, bypass_vlan,
        detect_date, regdate, unregdate, lastskip,
        user_agent, computername, dhcp_fingerprint,
        last_arp, last_dhcp,
        notes,
    ) VALUES (
        ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?
    )
SQL
```

HTTP JSON API

PacketFence provides an HTTP JSON API which exposes most of its functionality.

The full API specification for:

- the latest stable release is available from: <https://packetfence.org/doc/api/>
- the latest devel release is available from: <https://packetfence.org/doc/api-devel/>

The API is exposed on 127.0.0.1 (localhost) as well as the management interface of the server for remote calls. Users access the API on TCP port 9999 over a secure connection (HTTPS).

Authentication can be done using either the webservices credentials or any credentials that are valid on the web admin interface.

How to use the API

On a PacketFence server

The [command] `pfperl-api` command located in [filename] `/usr/local/pf/sbin/` directory can be use directly from a PacketFence server to query the API without having to specify an authentication token and extra-parameters.

Example to get your general configuration:

```
/usr/local/pf/sbin/pfperl-api get /api/v1/config/base/general \  
| python -m json.tool
```

Example to create a node:

```
/usr/local/pf/sbin/pfperl-api get -M POST /api/v1/nodes/ \  
-c '{"mac":"22:33:44:55:66:77","pid":"host/MYCOMPUTER"}' \  
| python -m json.tool
```

On a different computer



Note

The API specification mentioned above provides ready-to-use curl commands through the "Try it out" button.

First, get an authentication token with the webservices credentials or an admin account:

```
curl -X POST "https://PF_MANAGEMENT_IP:9999/api/v1/login" \  
-H "accept: application/json" \  
-H "Content-Type: application/json" \  
-d "{\"username\":\"admin\", \"password\":\"admin\"}" \  
--insecure | \  
python -m json.tool
```

You will get following response :

```
{  
  "token": "MY_TOKEN"  
}
```

Then use this token to query the API. The following example fetches the general configuration:

```
curl -X GET "https://PF_MANAGEMENT_IP:9999/api/v1/config/base/general" \  
-H "accept: application/json" \  
-H "Authorization: MY_TOKEN" \  
--insecure | \  
python -m json.tool
```

Although the API should mostly stay the same, backward compatibility is not 100% guaranteed for the moment until the v1 API reaches full maturity.

Customizing PacketFence

Captive Portal

Presentation

XHTML Templates

Captive portal content use [Template Toolkit](#) templates. The default template files are located in `/usr/local/pf/html/captive-portal/templates`. You can freely edit the HTML code in these files.

Each template relies on `layout.html` for the common top and bottom portions of the page.

Internationalized AUP

In the event that you need an Acceptable Usage Policy that should be translated in different languages in the captive portal, you can create specially named templates that will be used for different languages.

For example, if the browser locale is `es_ES`, creating a template named `aup_text.es.html` will display this AUP when it detects this locale. Same goes for a browser with locale `en_US`, where creating a template named `aup_text.en.html` will be used for English browsers.

The template `aup_text.html` is used as the final fallback for all locales.

Note that you cannot use the full locale in the template name (i.e. `aup_text.en_US.html`) as only the two letter prefix should be used.

CSS

The default stylesheet is the result of processing some [Sass](#) files structured around the solid [inuitcss](#) architectural foundation.

- `/usr/local/pf/html/common/Gruntfile.js` – the task runner configuration file
- `/usr/local/pf/html/common/package.js` – the npm dependencies required to process the Sass files
- `/usr/local/pf/html/common/scss/` – the directory containing the Sass source files
- `/usr/local/pf/html/common/styles.css` – the generated stylesheet

In order to prepare your environment to process the Sass files, you need to install [grunt](#) (the task runner) and additional [nodejs](#) modules, including the various inuitcss components:

```
sudo npm install -g grunt-cli
cd /usr/local/pf/html/common
npm install
```

Once all modules are downloaded, you can customize the Sass files and generate a new stylesheet:

```
grunt dist
```

To change the color palette of the captive portal, modify the file `scss/_settings.colors.scss`.

Workflow

When a HTTP request is received by the Apache web server, the following workflow happens:

1. URL is compared against the redirection instructions in `/usr/local/pf/conf/httpd.conf.d/captive-portal-cleanurls.conf`
2. Requested CGI script in `/usr/local/pf/html/captive-portal/` is executed
3. CGI script calls a `generate_<type>` which is defined in `/usr/local/pf/lib/pf/web.pm`
4. The `generate_<type>` function populate the proper template in `/usr/local/pf/html/captive-portal/templates` in order to render the page

Remediation Pages

The remediation page shown to the user during isolation are specified through the URL parameter of the given security event in `/usr/local/pf/conf/security_events.conf`. In its default configuration, PacketFence uses Template Toolkit to render text provided in the directory `/usr/local/pf/html/captive-portal/templates/security_events` and obeys to everything mentioned in the [Presentation](#) section.

Translations

The language of the user registration pages is selected through the `general.locale` configuration parameter. Translatable strings are handled differently for the Remediation pages and the rest of the captive portal:

- Remediation pages

Strings defined in the security event pages (in `/usr/local/pf/html/captive-portal/templates/security_events`) will be looked up in the translation files in `/usr/local/pf/conf/locale/..` and if a translation is available the translated string will be the one visible on the captive portal.

Also, if you create a security event template with the name of your locale in `/usr/local/pf/html/captive-portal/templates/security_events` in the format: `<template_name>.<locale_name>.html`. It will be loaded instead of the default `<template_name>.html` and so you can put strings and HTML directly in your target language without the hassle of escaping everything properly as you would need to do with `gettext`.

For example, if `malware.es_ES.html` exists and you are using the `es_ES` (Spanish) locale then it will be loaded instead of `malware.html` on a security event set to load the `malware` template.

- Rest of the captive portal

In the templates, if a string is in a `i18n()` call it will be translated. Also `pf::web` takes care of performing some of the other translations.

Adding custom fields to the database

You can, if needed, add additional fields to the PacketFence database. Keep in mind though that this might lead to more work when you upgrade to the next PacketFence version. Depending on the degree of integration of these fields with PacketFence, you'll have to execute one or more of the following steps

Adding a field to the database only

In this case, the field is part of one of the main PacketFence tables, but PacketFence is unaware of it. PacketFence won't consult the field and won't be able to modify it. A possible usage scenario would be a 3rd party application which maintains this field.

Since PacketFence doesn't have to know about the field, all you have to do is execute your `SQL ALTER TABLE` query and you are done.

Adding a field and giving PacketFence read-only access

In this case, PacketFence can show the contents of the table using both `pfcmd` but won't be able to modify the contents of the field.

Start by modifying the database table using an `SQL ALTER TABLE` query.

Then, modify the Perl module having the same name as the table you have added the field to, i.e. If you added the field to the node table, then edit `/usr/local/pf/lib/pf/node.pm`. You'll have to modify the `SQL SELECT` queries at the beginning of the file to include your new field and, possibly the functions using these queries. If your new field should be used in reports, the dashboard or graphs, you'll also have to modify the queries in `/usr/local/pf/lib/pf/pfcmd/graph.pm`, `/usr/local/pf/lib/pf/pfcmd/report.pm` and `/usr/local/pf/lib/pf/pfcmd/dashboard.pm`.

Adding a field and giving PacketFence read-write access

Start by creating the read-only field as described above.

Then, modify the 'SQL UPDATE' and `INSERT` queries in the database tables' Perl module, as well as the associated functions.

VLAN assignment

PacketFence uses the `getRegisteredRole` function defined in `pf::role::custom` to determine a node's VLAN. Here's the default function:

```
sub getRegisteredRole {
    # $switch is the switch object (pf::Switch)
    # $ifIndex is the ifIndex of the computer connected to
    # $mac is the mac connected
    # $node_info is the node info hashref (result of pf::node's node_view on $mac)
    # $conn_type is set to the connection type expressed as the constant in
    pf::config
    # $user_name is set to the RADIUS User-Name attribute (802.1X Username or MAC
    address under MAC Authentication)
    # $ssid is the name of the SSID (Be careful: will be empty string if radius
    non-wireless and undef if not radius)
    my ($self, $switch, $ifIndex, $mac, $node_info, $connection_type, $user_name,
    $ssid) = @_;

    my $logger = Log::Log4perl->get_logger();

    return $switch->getVlanByName('normalVlan');
}
```

As you can see, the function receives several parameters (such as the switch and full node details) which allow you to return the VLAN in a way that matches exactly your needs!

SNMP

Introduction

Good places to start reading about SNMP are <http://en.wikipedia.org/wiki/SNMP> and <http://www.net-snmp.org/>.

When working with SNMP, you'll sooner or later (in fact more sooner than later) be confronted with having to translate between OIDs and variable names. When the OIDs are part of the Cisco MIBs, you can use the following tool to do the translation: <http://tools.cisco.com/Support/SNMP/public.jsp>. Otherwise, you'll have to use `snmptranslate` for example and setup your own collection of MIBs, provided (hopefully) by the manufacturer of your network equipment.

Obtaining switch and port information

Below are some example of how to obtain simple switch and port information using SNMP. We'll assume that your switch understands SNMP v2, has the read community `public` defined and is reachable at `192.168.1.10`.

Switch Type

```
snmpwalk -v 2c -c public 192.168.1.10 sysDescr
```

Switchport indexes and descriptions

```
snmpwalk -v 2c -c public 192.168.1.10 ifDescr
```

Switchport types

```
snmpwalk -v 2c -c public 192.168.1.10 ifType
```

Switchport status

```
snmpwalk -v 2c -c public 192.168.1.10 ifAdminStatus  
snmpwalk -v 2c -c public 192.168.1.10 ifOperStatus
```

Supporting new network hardware

PacketFence is designed to ease the addition of support for new network hardware referred to as Network Devices. All supported network devices are represented through Perl objects with an extensive use of inheritance. Adding support for a new product comes down to extending the `pf::Switch` class (in `/usr/local/pf/lib/pf`).

The starting point to adding support for a new network device should be the vendor's documentation! First of all, you'll have to figure out the exact capabilities of the switch and how these capabilities will fit into PacketFence. Is it a Switch, an Access-Point or a Wireless Controller?

Switch

Will you be able to use only link change traps? Does your switch allow you to use MAC notification traps? Port Security? MAC Authentication? 802.1X?

Link change capabilities

You need to define a new class which inherits from `pf::Switch` and defines at least the following functions:

- `getMacAddrVlan`
- `getVersion`
- `getVlan`
- `getVlans`
- `isDefinedVlan`
- `parseTrap`
- `_getMacAtIfIndex`
- `_setVlan`

The `'parseTrap'` function will need to return an hash with keys `trapType` and `trapIfIndex`. The associated values must be `up` or `down` for `trapType` and the traps' `ifIndex` for `trapIfIndex`. See a similar switch's implementation for inspiration. Usually recent modules are better coded than older ones.

MAC notification capabilities

In addition to the functions mentioned for link change, you need to define the following function:

- `isLearntTrapsEnabled`

Also, your `parseTrap` function will need to return `trapOperation`, `trapVlan` and `trapMac` keys in addition to `trapType` equals `mac`. See a similar switch's implementation for inspiration. Usually recent modules are better coded than older ones.

Port security capabilities

In addition to the functions mentioned for link change, you need to define the following functions:

- `isPortSecurityEnabled`
- `authorizeMAC`

In this case, the `parseTrap` function needs to return `secureMacAddrViolation` for the `trapType` key. See a similar switch's implementation for inspiration. Usually recent modules are better coded than older ones.

MAC Authentication



Note

Work in progress

NAS-Port translation

Often the `ifIndex` provided by the switch in a RADIUS `Access-Request` is not the same as its real world physical equivalent. For example in Cisco requests are in the 50xxx while physical `ifIndex` are 10xxx. In order for PacketFence to properly shut the port or request re-authentication a translation between the two is required. To do so provide an implementation of the following interface:

- `NasPortToIfIndex`

MAC Authentication re-evaluation

MAC Authentication re-evaluation is necessary in order to provoke a VLAN change in the PacketFence system. This happens for instance when a node is isolated based on an IDS event or when the user successfully authenticates through the captive portal. The default implementation in `pf::Switch` will bounce the port if there is no Voice over IP (VoIP) devices connected to the port. Otherwise it will do nothing and send an email. If your device has specific needs (for example it doesn't support RADIUS Dynamic VLAN Assignments) override:

- `handleReAssignVlanTrapForWiredMacAuth`

Please note that the default implementation works 99% of the time. If you are unsure whether to override, it means you don't need to override.

Once the MAC Authentication works, add the Wired MAC Auth capability to the switch's code with:

```
sub supportsWiredMacAuth { return $TRUE; }
```


802.1X



Note

Work in progress

NAS-Port translation

Often the `ifIndex` provided by the switch in a RADIUS `Access-Request` is not the same as its real world physical equivalent. For example in Cisco requests are in the 50xxx while physical `ifIndex` are 10xxx. In order for PacketFence to properly shut the port or request re-authentication a translation between the two is required. To do so provide an implementation of the following interface:

- `NasPortToIfIndex`

So far the implementation has been the same for MAC Authentication and 802.1X.

Force 802.1X re-authentication

802.1X re-authentication is necessary in order to provoke a VLAN change in the PacketFence system. This happens for instance when a node is isolated based on an IDS event or when the user successfully authenticates through the captive portal. The default implementation in `pf::Switch` uses SNMP and the standard `IEEE8021-PAE-MIB` and is generally well supported. If the default implementation to force 802.1X re-authentication doesn't work override:

- `dot1xPortReauthenticate`

Proper 802.1X implementations will perform re-authentication while still allowing traffic to go through for supplicants under re-evaluation.

Once the `802.1X` works, add the Wired Dot1X capability to the switch's code with:

```
sub supportsWiredDot1x { return $TRUE; }
```

RADIUS Dynamic Authorization (RFC3576)



Note

RADIUS Dynamic Authorization implementation is not recommended on the wired side at this point.

RADIUS Dynamic Authorization also known as RADIUS Change of Authorization (CoA) or RADIUS Disconnect Messages is supported by PacketFence starting with version 3.1.

On wired network devices CoA can be used to change the security posture of a MAC and perform other functions like bounce a port. So far we only encountered support for CoA on the wired side on the Cisco hardware. For an implementation example check `_radiusBounceMac` in `pf::Switch::Cisco`.

Floating Network Devices Support

Floating Network Devices are described in the Administration Guide under "Floating Network Devices" in the "Optional Components" section. Refer to this documentation if you don't know what Floating Network Devices are.

In order to support Floating Network Devices on a switch, you need to implement the following methods:

- `setPortSecurityEnableByIfIndex($ifIndex, $enable)`
- `isTrunkPort($ifIndex)`
- `setModeTrunk($ifIndex, $enable)`
- `setTaggedVlans($ifIndex, $switch_locker_ref, @vlans)`
- `removeAllTaggedVlans($ifIndex, $switch_locker_ref)`

You might need to implement the following:

- `enablePortConfigAsTrunk($mac, $switch_port, $switch_locker, $taggedVlans)`

Provided by `pf::Switch` core as the glue between `setModeTrunk()`, `setTaggedVlans()` and `removeAllTaggedVlans()`. Override if necessary.

- `disablePortConfigAsTrunk($switch_port)`

Provided by `pf::Switch` core as the glue between `setModeTrunk()`, `setTaggedVlans()` and `removeAllTaggedVlans()`. Override if necessary.

- `enablePortSecurityByIfIndex($ifIndex)`

Provided by `pf::Switch` core as a slim accessor to `setPortSecurityEnableByIfIndex()`. Override if necessary.

- `disablePortSecurityByIfIndex($ifIndex)`

Provided by `pf::Switch` core as a slim accessor to `setPortSecurityEnableByIfIndex()`. Override if necessary.

- `enableIfLinkUpDownTraps($ifIndex)`

Provided by `pf::Switch` core as a slim accessor to `setIfLinkUpDownTrapEnable`. Override if necessary.

- `disableIfLinkUpDownTraps($ifIndex)`

Provided by `pf::Switch` core as a slim accessor to `setIfLinkUpDownTrapEnable`. Override if necessary.

Once all the required methods are implemented, enable the capability in the switch's code with:

```
sub supportsFloatingDevice { return $TRUE; }
```

Wireless Access-Points or Controllers

Minimum hardware requirements

PacketFence's minimum requirements regarding Wireless hardware is:

- definition of several SSID with several VLANs inside every SSID (minimum of 2 VLANs per SSID)
- RADIUS authentication (MAC Authentication / 802.1X)
- Dynamic VLAN assignment through RADIUS attributes
- a means to de-associate or de-authenticate a client through CLI (Telnet or SSH), SNMP, RADIUS Dyn-Auth¹ or WebServices

Most of these features are available on enterprise grade Access Points (AP) or Controllers. Where the situation starts to vary wildly is for deauthentication support.

De-authentication techniques

CLI (SSH or Telnet)

An error prone interface and requires preparation for the SSH access or is insecure for Telnet. Not recommended if you can avoid it.

SNMP

SNMP de-authentication works well when available. However Vendor support is not consistent and the OID to use are not standard.

RADIUS Dynamic Authorization (RFC3576)

RADIUS Dynamic Authorization also known as RADIUS Change of Authorization (CoA) or RADIUS Disconnect Messages is supported by PacketFence starting with version 3.1. When supported it is the preferred technique to perform de-authentication. It is standard and requires less configuration from the user.

An actual implementation can be found in `pf::Switch::Aruba`.

Template module

Start with a copy of the template module `pf/lib/pf/Switch/WirelessModuleTemplate.pm` and fill in appropriate documentation and code.

Required methods

You need to implement at least:

¹RADIUS Dynamic Authorization (RFC 3576) aka Change of Authorization (CoA) or Disconnect-Messages (DM aka PoD)

<code>getVersion()</code>	Fetches firmware version
<code>parseTrap()</code>	Parses the SNMP Traps sent by the hardware. For wireless hardware an empty method like the one in <code>pf::Switch::WirelessModuleTemplate</code> is ok.
<code>deauthenticateMac()</code>	Performs deauthentication
<code>supportsWirelessMacAuth()</code>	Return <code>\$TRUE</code> if MAC-Authentication is supported
<code>supportsWirelessDot1x()</code>	Return <code>\$TRUE</code> if 802.1X (aka WPA-Enterprise) is supported

Override methods

If default implementation of the following methods doesn't work you will need to override them:

`extractSsid()` Extract SSID from RADIUS Request

Special case: bridged versus tunneled modes and deauthentication

It is important to validate the Access-Point (AP) to Controller relationship when operating in bridged mode versus when operating in tunneled mode. For example, some hardware will send the RADIUS `Access-Request` from the AP when in bridged mode even though it is controlled by a controller. This behavior impacts deauthentication because it still needs to be performed on the controller. To support this behavior a `switches.conf` parameter was introduced: `controller_ip`.

When adding a new Wireless module try to validate the bridged versus tunneled behavior and modify `deauthenticateMac()` to honor `controller_ip` if required.

The "adding a new network device module in PacketFence" checklist

Here's a quick rundown of the several files you need to edit in order to add a new switch into PacketFence. There's a plan to reduce this amount of work in progress see [issue #1085](#).

- Tested model and firmware version should be documented in module's POD
- Any bugs and limitations should be documented in module's POD
- Make sure that all tests pass
- Add configuration documentation to the Network Devices Guide
- Add switch to the Network Devices Guide's switch chart
- Add switch to the chart in `README.network-devices`

Creating a new Switch via a Template

To create a new Switch Template you must create a template file in the `/usr/local/pf/lib/pf/Switch` directory. The file must have the following pattern `/usr/local/pf/lib/pf/Switch/<Vendor>/<Switch-Name>.def`

For example to create a template for the vendor "Cyberdyne" and switch "Switchinator 800". The file name is `/usr/local/pf/lib/pf/Switch/Cyberdyne/Switchinator800.def` The file name must only consist of alphanumeric characters and under scores and must begin with a letter.

The file consist of parameter names and their values.

Required Parameters

- `description` - The description of the switch.
- `radiusDisconnect` - The RADIUS disconnect methods to use. Must be one of the following values `coa|disconnect|coaOrDisconnect` .

RADIUS scope Parameters

- `acceptVlan` - Attributes for accept vlan scope
- `acceptRole` - Attributes for accept role scope.
- `reject` - Attributes for rejection scope.
- `disconnect` - Attributes for disconnect scope (required if `radiusDisconnect` is `disconnect` or `coaOrDisconnect`)
- `coa` - Attributes for CoA scope (required if `radiusDisconnect` is `coa` or `coaOrDisconnect`)

Comments

The line of a comment must begin with a `#` For example:

```
# This is a comment
```

Defining RADIUS Attributes.

```
scopeName = <<EOT
Attribute-Name1 = value1
Attribute-Name2 = value2
EOT
```

RADIUS Vendor Attributes for CoA

```
scopeName = <<EOT
VendorName:Attribute-Name1 = value1
VendorName:Attribute-Name2 = value2
EOT
```

Dynamic RADIUS Attribute Value Syntax

Some values depends on the context of the current request. So here is mini templating language to format values.

- Text replacement: \$name
-
- Functions: \${f1("",\$var, f2())}

Available variables for RADIUS scope

- acceptRole - (Same as acceptVlan)
- reject - (Same as acceptVlan)
- acceptVlan
 - autoreg
 - connection_sub_type

- connection_type
- eap_type
- fingerbank_info.device_name
- fingerbank_info.device_fq
- fingerbank_info.device_hierarchy_names
- fingerbank_info.device_hierarchy_ids
- fingerbank_info.score
- fingerbank_info.version
- fingerbank_info.mobile
- ifDesc
- ifIndex
- isPhone
- last_accounting.acctsessionid
- last_accounting.username
- mac
- nas_port_id
- nas_port_type
- node_info.autoreg
- node_info.status
- node_info.bypass_vlan
- node_info.bandwidth_balance
- node_info.regdate
- node_info.bypass_role
- node_info.device_class
- node_info.device_type
- node_info.device_version
- node_info.device_score
- node_info.pid

- node_info.category
- node_info.mac
- node_info.last_arp
- node_info.lastskip
- node_info.last_dhcp
- node_info.user_agent
- node_info.computername
- node_info.dhcp_fingerprint
- node_info.detect_date
- node_info.voip
- node_info.notes
- node_info.time_balance
- node_info.sessionid
- node_info.dhcp_vendor
- profile._access_registration_when_registered
- profile._always_use_redirecturl
- profile._autoregister
- profile._block_interval
- profile._description
- profile._dot1x_recompute_role_from_portal
- profile._dot1x_unset_on_unmatch
- profile._dpsk
- profile._locale
- profile._login_attempt_limit
- profile._logo
- profile._name
- profile._network_logoff
- profile._network_logoff_popup

- profile._redirecturl
- profile._reuse_dot1x_credentials
- profile._root_module
- profile._self_service
- profile._sms_pin_retry_limit
- profile._sms_request_limit
- profile._status
- profile._unreg_on_acct_stop
- profile._vlan_pool_technique
- radius_request.<Radius Attribute Name>
- realm
- session_id
- source_ip
- ssid
- stripped_user_name
- switch._ExternalPortalEnforcement
- switch._RoleMap
- switch._SNMPAuthPasswordRead
- switch._SNMPAuthPasswordTrap
- switch._SNMPAuthPasswordWrite
- switch._SNMPAuthProtocolRead
- switch._SNMPAuthProtocolTrap
- switch._SNMPAuthProtocolWrite
- switch._SNMPCommunityRead
- switch._SNMPCommunityTrap
- switch._SNMPCommunityWrite
- switch._SNMPEngineID
- switch._SNMPPrivPasswordRead

- switch._SNMPPrivPasswordWrite
- switch._SNMPPrivProtocolRead
- switch._SNMPPrivProtocolTrap
- switch._SNMPPrivProtocolWrite
- switch._SNMPUserNameRead
- switch._SNMPUserNameTrap
- switch._SNMPUserNameWrite
- switch._SNMPVersion
- switch._SNMPVersionTrap
- switch._TenantId
- switch._UrlMap
- switch._VlanMap
- switch._VoIPEnabled
- switch._cliEnablePwd
- switch._cliPwd
- switch._cliTransport
- switch._cliUser
- switch._coaPort
- switch._controllerIp
- switch._deauthMethod
- switch._disconnectPort
- switch._id
- switch._inlineTrigger
- switch._ip
- switch._macSearchesMaxNb
- switch._macSearchesSleepInterval
- switch._mode
- switch._roles

- switch._switchMac
- switch._uplink
- switch._useCoA
- switch._vlans
- switch._wsPwd
- switch._wsTransport
- switch._wsUser
- switch_ip
- switch_mac
- time
- user_name
- user_role
- vlan
- wasInline
- coa
 - last_accounting.acctsessionid
 - last_accounting.username
 - mac
 - role
- disconnect
 - disconnectIp
 - last_accounting.acctsessionid
 - last_accounting.username
 - mac

Available functions

- macToEUI48(\$mac) - format a mac to AA-BB-CC-DD-FF-EE format
- uc(\$string) - uppercases a string
- lc(\$string) - lowercases a string
- log(\$string) - log a message to the log

- substr(\$str, \$offset, \$len) - Extracts a substring from a string
- split(\$sep, \$str) - Split a string by a separator.
- join(\$sep, \$a, \$b, ..) - Join a list of string with a separator.

Full Working Example

```
description = The Switchinator 800
radiusDisconnect = disconnect

acceptVlan = <<EOT
Tunnel-Medium-Type = 6
Tunnel-Type = 13
Tunnel-Private-Group-ID = $vlan
EOT

acceptRole = <<EOT
Filter-Id = $role
EOT

reject = <<EOT
Reply-Message = Hasta la vista, baby.
EOT

disconnect = <<EOT
Calling-Station-Id= ${macToEUI48($mac)}
NAS-IP-Address = $disconnectIp
EOT

coa = <<EOT
Calling-Station-Id= ${macToEUI48($mac)}
NAS-IP-Address = $disconnectIp
Cisco:Cisco-AVPair = subscriber:command=bounce-host-port
EOT
```

PacketFence builds

Packer

To build PacketFence, we use [Packer](#) to create [Docker images](#) that are then used in a GitLab pipeline.

Anatomy of Packer template

PacketFence rely on [buildpkg Docker images](#) to run GitLab pipeline with [gitlab-buildpkg-tools](#). Packer template ([filename]pfbuid.json) use these images as base to build inverseinc Docker images.

Custom build dependencies

To start building PacketFence, we need to install specific things in images like:

- custom repositories and GPG keys to install RPM or DEB packages at build time
- install and configure upstream softwares necessary to build PacketFence if we can't use packages

We use Ansible and shell scripts to cover these steps. It's possible because Python is already installed in [buildpkg Docker images](#).

When GPG keys from upstream repos can't be download automatically from Internet, we store them in [filename]ci/packer/provisionners/upstream directory to upload them in Docker images.

Build dependencies in packages specs

Build dependencies need to be install in Docker images before starting build process. We rely on [package]gitlab-buildpkg-tools to automatically install those dependencies based on packages specifications file. Consequently, all build requires need to be define in packages specifications file.

Golang environment

We use Packer to set up a Golang environment in order to build Golang binaries in Docker images.

We also set environment variables in Docker images, using ENV directives, to simplify usage of [command]go commands.

Clean up

To make Docker images lightweight, we make a clean up at end of the process.

How to build Docker images ?

Docker images are built inside a GitLab pipeline. It can be run manually or detect changes on packages specifications files to start.

Prerequisites

Install following softwares:

- [Packer](#) (>=1.4.2)
- [Docker](#)
- Ansible

Makefile

Because we run build inside a GitLab pipeline, many environment variables can be set to change build behavior. A [filename]**Makefile** is provided to simplify creation a new Docker images based on environment variables.

Example usage of Makefile.

```
make -C ci/packer
GOVERSION=go1.9.3 DOCKER_TAG=$GOVERSION ACTIVE_BUILDS=pfbuild-stretch \
make -e -C ci/packer
```

Troubleshooting

You can troubleshoot issue in Packer builds by setting environment variable **\$PACKER_LOG** environment variable to 1.

Developer recipes

Running development version

Bleeding edge

For day to day development one can run a checkout of the current development branch in `/usr/local/pf/` and develop there within a working setup.

Install following softwares:

- [Vagrant](#) (`>= 1.9.3`)
- Virtualbox if you want to use Virtualbox as a provider for Vagrant
- libvirt, KVM/QEMU and `vagrant-libvirt` if you want to use libvirt as a provider for Vagrant

Following steps assume you use a CentOS machine but you can have same behavior under Debian.

Install Ansible, Mazer and PacketFence's source code:

```
sudo yum install -y epel-release
sudo yum install -y git python-pip
pip install --user ansible
pip install --user mazer
git clone https://github.com/inverse-inc/packetfence.git
```

Install PacketFence's collection and Ansible roles:

```
cd packetfence/addons/vagrant
mazer install --lockfile=collections_lockfile.yml
ansible-galaxy install -r requirements.yml
```

Start CentOS 7 virtual machine via Vagrant to set up development environment:

```
vagrant up pfcen7dev
```

Reboot virtual machine to disable SELinux:

```
vagrant reload pfcen7dev
```

At the end of this process, you will have latest PacketFence's source code, running in a CentOS 7 virtual machine, located in `[filename]/usr/local/pf` with all dependencies installed as RPM packages. You can directly develop from `[filename]/usr/local/pf`.

Web admin should be reachable through management IP address of `pfcen7dev` machine, configured in `[filename]addons/vagrant/inventory/hosts`.

Not so bleeding edge

If you prefer to use packages, you can install latest PacketFence packages from nightly builds.

Initial setup

Install [development prerequisites](#) and follow [initial setup](#) but in place of starting `pfcen7dev`, you can start:

- `pfcen7night`
- `pfdeb9night`

These machines will be auto-configured to install nightly builds from development repositories.

Day to day usage

To keep your machine up-to-date, you can run the following commands:

```
cd packetfence/addons/vagrant
vagrant provision --provision-with=config pfcen7night
vagrant provision --provision-with=config pfdeb9night
```

Make sure you read the `UPGRADE` document after every upgrades to avoid any surprises.

Running an Ansible playbook against Vagrant virtual machines

If you want to use Ansible directly against Vagrant virtual machines, you can use following commands:

```
cd packetfence/addons/vagrant
ansible-playbook site.yml --limit pfcen7night
```

It's possible because we use a static Ansible inventory. This inventory is also used by Vagrant to start virtual machines.

Contributing

Here are some golden rules of contributing to PacketFence:

- Be active on the [developer mailing list](#)

The place to be if you want to contribute to the PacketFence project is our developers mailing list: <https://lists.sourceforge.net/lists/listinfo/packetfence-devel>. Let us know your issues, what you are working on and how you want to solve your problems. The more you collaborate the greater the chances that your work will be incorporated in a timely fashion.

- Use the issue tracker: <https://packetfence.org/bugs/>

Good chances that the bug you want to fix or the feature you want to implement is already filed and that information in the ticket will help you.

- Please provide small, focused and manageable patches or pull-requests

If you plan on doing a lot of code, use **git** and track our current stable branch called **stable**. Develop the feature in small chunks and stay in touch with us. This way it'll be merged quickly in our code base. Ideally there would be no big code dumps after finishing a feature.

Creating patches



Note

Since we migrated to git / github, using these tools is recommended over sending patches by hand.

Patches should be sent in unified diff format. This can be obtained from the **diff** or **git** tools.

```
diff -u oldfile newfile
```

or from a checkout of the PacketFence source code from **git**:

```
git diff
```

Translations

The internationalization process uses `gettext`. If you are new to `gettext`, please consult <http://www.gnu.org/software/gettext/manual/gettext.html#Overview> for a quick introduction.

The PO files are stored in `/usr/local/pf/conf/locale`. List that directory to see the languages we currently have translations for.

Online using Transifex

We use the hosted service Transifex to translate PacketFence's PO files. It offers the possibility to translate all the strings online as well as providing a command-line tool to push your changes. It's very convenient.

To use Transifex, you must first sign up for a free account here: <https://www.transifex.net/plans/signup/free/>

- Once registered, [request a new team for your language](#)
- Once authorized, you'll be able to start/continue translating PacketFence in your language

If you need further help about using Transifex, you might want to have [a look here](#).

Using traditional method

If you want to add support for a new language, please follow these steps:

1. create a new language subdirectory in `/usr/local/pf/conf/locale`
2. change into your newly created directory
3. create a new subdirectory `LC_MESSAGES`
4. change into your newly created directory
5. copy the file `/usr/local/pf/conf/locale/en/LC_MESSAGES/packetfence.po` into your directory
6. translate the message strings in `packetfence.po`
7. create the MO file by executing:

```
/usr/bin/msgfmt packetfence.po
```

Submit your new translation to the PacketFence project by contacting us at packetfence-devel@lists.sourceforge.net.

Admin GUI

The Admin GUI can be customized via Controllers and templates.

Templates

You can add customize templates to the `/usr/local/pf/html/pfappserver/root-custom/` folder to override current templates.

However when doing this you must keep track of any changes to those templates across versions.

Stylesheets and JavaScript

The main stylesheet is the result of processing some [Sass](#) files structured around the excellent [Bootstrap](#) framework.

- `/usr/local/pf/html/pfappserver/root/static/Gruntfile.js` — the task runner configuration file
- `/usr/local/pf/html/pfappserver/root/static/package.js` — the npm dependencies required to process the Sass files and to package the JavaScript code
- `/usr/local/pf/html/pfappserver/root/static/bower.json` — the list of required components
- `/usr/local/pf/html/pfappserver/root/static/scss/` — the directory containing the Sass source files
- `/usr/local/pf/html/pfappserver/root/static/css/styles.css` — the generated stylesheet
- `/usr/local/pf/html/pfappserver/root/static/js/vendor/` — the directory containing the external JavaScript libraries

In order to prepare your environment, you need to install [grunt](#) (the task runner) and [bower](#) (the package manager):

```
sudo npm install -g grunt-cli
sudo npm install -g bower
cd /usr/local/pf/html/pfappserver/root/static/
npm install
bower install
```

Once all modules and components are downloaded, you can customize the Sass files or JavaScript files and generate a new version of the static files:

```
grunt dist
```

Controllers

You change the behavior of the controllers by modifying the controllers in the path.

`/usr/local/pf/html/pfappserver/lib/pfappserver/Controller/`

However when doing this you must keep track of any changes to those Controllers across versions.

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/> for details.

GNU Free Documentation License

Please refer to <http://www.gnu.org/licenses/fdl-1.2.txt> for the full license.