



PacketFence Developer's Guide

for version 2.2.1

PacketFence Developer's Guide

Olivier Bilodeau

Dominik Gehl

Version 2.2.1 - June 2011

Copyright © 2008-2011 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 logo for Inverse, consisting of the word "inverse" in a light blue, lowercase, sans-serif font, rotated 180 degrees counter-clockwise.

Revision History		
Revision 2.4	2011-03-31	OBU
Updated wireless hardware support instructions and checklist. Added clarifications to the MAC Auth and 802.1X support development.		
Revision 2.3	2011-02-10	OBU
Template improvements		
Revision 2.2	2011-02-02	OBU
Reworked new switch support into a more general new network devices support. New content: Wireless Access-Points and Controllers, Switch support for MAC Auth and 802.1X, a new "add a network device to PacketFence" checklist and new exception handling techniques.		
Revision 2.1	2011-02-01	OBU
New content: a chapter on contributing, one on code conventions and one on developer recipes (run devel env., debug grammar).		
Revision 2.0	2011-01-31	OBU
Port to Docbook.		
Revision 1.0	2008-12-13	DGL
First OpenDocument version.		

Table of Contents

About this Guide	1
Code conventions	2
Code style	2
Customizing PacketFence	4
Registration Pages	4
Translations	4
Content	4
Workflow	5
Remediation Pages	5
Adding custom fields to the database	5
Adding a field to the database only	5
Adding a field and giving PacketFence read-only access	5
Adding a field and giving PacketFence read-write access	6
VLAN assignment	6
Modifying how pfsetvlan calculates the VLAN for a node	7
SNMP	8
Introduction	8
Obtaining switch and port information	8
Switch Type	8
Switchport indexes and descriptions	8
Switchport types	8
Switchport status	8
Obtaining VLAN information on Cisco switches	9
Access VLAN on a switchport	9
Supporting new network hardware	10
Switch	10
Link change capabilities	10
MAC notification capabilities	10
Port security capabilities	11
MAC Authentication	11
802.1X	11
Wireless Access-Points or Controllers	12
Minimum hardware requirements	12
Template module	12
Required methods	13
Override methods	13
The "adding a new network device module in PacketFence" checklist	13
Developer recipes	14
Running development version	14
Bleeding edge	14
Not so bleeding edge	14
Debugging PacketFence grammar	14
New Exception handling techniques under testing	14
Contributing	16
Creating patches	16
Additional Information	17
Commercial Support and Contact Information	18
GNU Free Documentation License	19

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 instructions are based on version 2.2.1 of PacketFence.

The latest version of this guide is available online at

<http://www.packetfence.org/download/guides.html>.

Code conventions

Code style

Caution

This is 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 manually wrap longer lines
- No tab characters
- Use constants instead of hardcoded strings or numbers (use `constant` or `Readonly` modules)
- in object-oriented modules we use CamelCase notation (ex: `$radiusRequest->getVoIpAttributes();`)
- in procedural modules we use perl usual notation (ex: `$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";
}
```

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

```
$node_statements->{'node_add_sql'} = get_db_handle()->prepare(qq[
  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 (
    ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?
  )
]);
```

Customizing PacketFence

Registration Pages

Translations

The language of the user registration pages is selected through the `general.locale` configuration parameter.

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.

Currently, PacketFence has language files for Dutch, English, French, Italian and Spanish. The PO files are stored in `/usr/local/pf/conf/locale`.

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
```

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

Content

Since version 1.7 of PacketFence, the registration pages use Template Toolkit (<http://template-toolkit.org/>).

All the template files are located in `/usr/local/pf/html/user/content/templates`. The first template you might want to customize are surely the registration templates `/usr/local/pf/html/user/content/templates/register.html` and `/usr/local/pf/html/user/content/templates/register_1.html`. You can freely edit the HTML code in this file (and all other template files). However, if you want to customize the pages beyond the HTML template

(for example by adding new variables to it), you'll need to look into the `/usr/local/pf/lib/pf/web.pm` Perl module. This module contains one function per template file. So if you want to modify the registration page, you'll have to modify the `generate_registration_page` function.

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`
2. requested CGI script in `/usr/local/pf/cgi-bin` is executed
3. CGI script calls a `generate_<type>` function which is defined in `/usr/local/pf/lib/pf/web.pm`
4. the `generate_<type>` function uses Template Toolkit and the templates in `/usr/local/pf/html/user/content/templates` in order to render the page

Remediation Pages

The remediation page shown to the user during isolation is specified through the `url` parameter of the given violation in `/usr/local/pf/conf/violations.conf`. In its default configuration, PacketFence uses PHP templates located in the directory `/usr/local/pf/html/user/content/violations/`.

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` and the Web Admin GUI, 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`.

Last, but not least, you'll have to modify the file `/usr/local/pf/conf/ui.conf`. In this file, you can also give a nice looking name to your field for showing up in the Web Admin GUI.

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.

The last step is to make PacketFence's grammar aware of the new field. Modify `/usr/local/pf/lib/pf/pfcmd/pfcmd.pm` and then re-generate the precompiled grammar (which is used by the pfcmd CLI) with:

```
cd /usr/local/pf

/usr/bin/perl -w -e '
    use strict; use warnings; use diagnostics;
    use Parse::RecDescent; use lib "/usr/local/pf/lib";
    use pf::pfcmd::pfcmd;
    Parse::RecDescent->Precompile($grammar, "pfcmd_pregrammar");
'

mv pfcmd_pregrammar.pm /usr/local/pf/lib/pf/pfcmd/pfcmd_pregrammar.pm
```

VLAN assignment

Caution

This information in the following section is obsolete.

The `pfsetvlan` daemon assigns by default a MAC to the VLAN which is saved in the VLAN field in its database entry. This VLAN field is, again by default, filled during registration with the `normalVlan` configuration setting, defined in `/usr/local/pf/conf/switches.conf`.

So, there are two different ways to change the VLAN a given node ends up in: by modifying the content which is saved in the VLAN field during registration and by modifying how `pfsetvlan` uses this information.

Modifying the VLAN assignment during registration

You can change the default behavior by modifying the following lines in `/usr/local/pf/cgi-bin/register.cgi`

```
#determine default VLAN if VLAN isolation is enabled
#and the vlan has not been set yet
if (isenabled($Config{'network'}{'vlan'})) {
    if (! defined($info{'vlan'})) {
        my %ConfigVlan;
        tie %ConfigVlan, 'Config::IniFiles',
            (-file = '/usr/local/pf/conf/switches.conf');
        $info{'vlan'} = $ConfigVlan{'default'}{'normalVlan'};
    }
}
```

Modifying how pfsetvlan calculates the VLAN for a node

pfsetvlan uses the `getNormalVlan` function defined in `pf::vlan::custom` to determine a node's VLAN. Here's the default function:

```
sub getNormalVlan {
    # $switch is the switch object (pf::SNMP)
    # $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 ($this, $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
```

Obtaining VLAN information on Cisco switches

Access VLAN on a switchport

```
snmpwalk -c public -m CISCO-VLAN-MEMBERSHIP-MIB -M \  
/usr/local/share/snmp/mibs:/usr/share/snmp/mibs \  
-v 2c 192.168.1.10 vmVlan
```

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::SNMP` 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::SNMP` and defines at least the following functions:

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

The `parseTrap` function will need to return a hash with keys `trapType` and `trapIfIndex`. The associated values must be up or down for `trapType` and the traps `ifIndex` for `trapIfIndex`.

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 be able to return a third value for the `trapType` key: `mac`. In this case, the hash also needs to contain `trapOperation`, `trapVlan` and `trapMac` keys.

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 be able to return `secureMacAddrViolation` for the `trapType` key.

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 it's real world physical equivalent. For example in Cisco requests are in the 50xxx while physical ports 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 : : SNMP` will bounce the port if there is no Voice over IP 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`

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 it's real world physical equivalent. For example in Cisco requests are in the 50xxx while physical ports 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::SNMP` uses the `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; }
```

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 based on RADIUS attributes
- SNMP deassociation/deauthentication traps
- a CLI, SNMP, RADIUS¹ or WebServices command to deassociate/deauthenticate a client

Most of these features work out of the box for enterprise grade Access Points or Controllers. Where the situation starts to vary is for deauthentication support.

SSH or Telnet is an error prone interface and requires preparation for the SSH access or is insecure for Telnet.

SNMP is implemented when available but not all vendor support it.

RADIUS is an upcoming deauthentication mechanism in PacketFence. It's the support for RFC 3576 Change of Authorization (CoA) or Disconnect-Messages (DM aka PoD). Once implemented it will be the preferred deauthentication technique.

Template module

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

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

Required methods

You need to implement at least:

- `getVersion()` - fetch firmware version
- `parseTrap()` - parses the SNMP Traps sent by the hardware. For wireless hardware an empty method like the one in `pf::SNMP::WirelessModuleTemplate` is ok.
- `deauthenticateMac()` - performs deauthentication
- `supportsWirelessMacAuth()`, `supportsWirelessDot1x()` - based on what the hardware supports

Override methods

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

- `extractSsid()` - extract SSID from RADIUS Request

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
- Add it to `pf/html/admin/configuration/switches_add.php` and `switches_edit.php`
- 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`

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.

Care should be taken not to commit local configuration files changes and files not in the repository.

Not so bleeding edge

Using the development **yum** repository and upgrade packetfence often is a good way to proceed. Check our [snapshots download page](#) for instructions.

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

Debugging PacketFence grammar

PacketFence uses a parser to validate user input. This parser is referred to as the grammar. When you see errors like

```
Command not understood. (pfcmd grammar test failed at line 217.)
```

it means that you faced a problem in the command you are trying to send or in the grammar itself.

The parsing of a command is a tricky process. First the command is interpreted in the `pf::pfcmd` module using traditional regular expressions. Then some of the commands will trigger the parser `pf::pfcmd::pfcmd_pregrammar` which is a precompiled module that is generated from `pf::pfcmd::pfcmd` when packetfence is built.

To help troubleshoot a failing command, you can enable tracing on the parser by removing the comment from the following line in `pfcmd:#our $RD_TRACE = 1;`

New Exception handling techniques under testing

Little attention was given to error-handling in PacketFence's early design. This is understandable as it wasn't probably the most bang-for-the-buck thing to do. However we must now live with a large codebase that explodes at runtime or that doesn't differentiate an erroneous condition from a null or 0 value. Refactoring to improve error-handling will be gradual but new code should follow these tips:

1. use `Try::Tiny`
2. wrap stuff in `try {...} catch {...};` (and optionally a `finally {...};`)
3. in the code use `die(...);` to throw an exception and make the error message meaningful
4. in the catch block, use `$logger->logcarp(string . $@)` if I want output to the CLI, otherwise, choose wisely

This catches a lot of errors (including runtime crashers) and allows us to recover from these conditions so its pretty cool!

So far, it is mandatory to wrap the Web Services enabled network devices modules' code since `SOAP::Lite` will die on you if host is unreachable for example (actually it's `LWP::UserAgent` who will).

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: <http://www.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

If you plan on doing a lot of code, use monotone and track our current development branch. Develop the feature in small chunks and stay in touch with us. This way it'll be merged quickly in our codebase. No big code dumps after finishing your feature please.

Creating patches

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

```
diff -u oldfile newfile
```

or from a checkout of the PacketFence source code from monotone:

```
mtn diff
```

If required a public branch can be created for contributors on our [public source code repository](#).

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.