# Introduction to PFSense

Matthew White and Nick Starke

# What is PFSense?

PFSense is an open source firewall software suite.

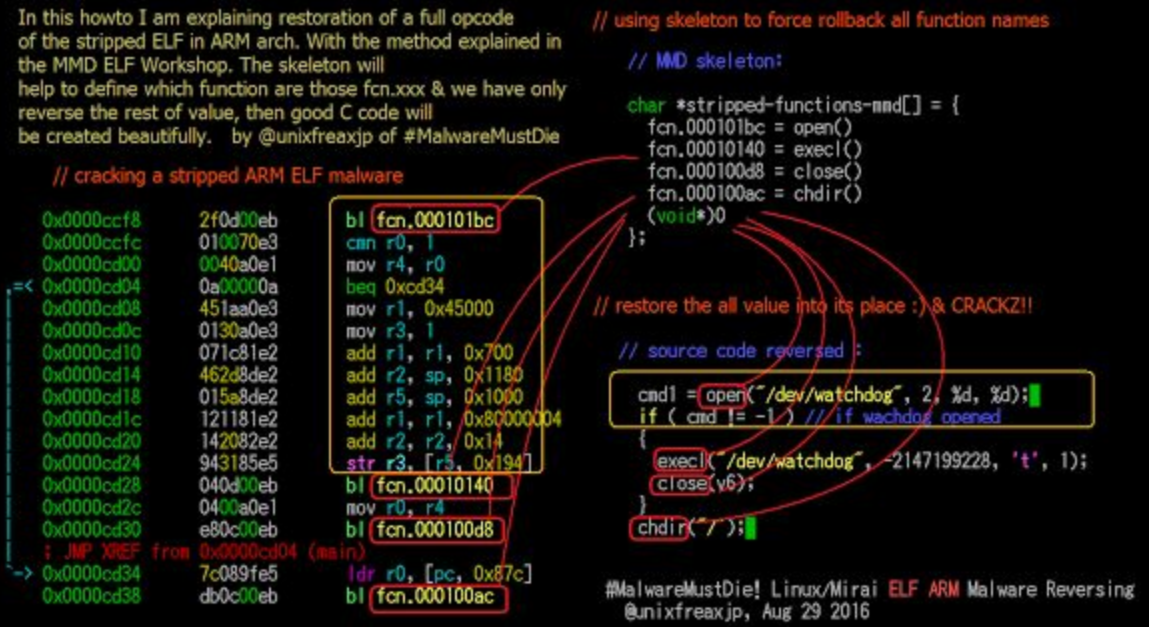
https://github.com/pfsense/pfsense

# What can it be used for?

DSL Modem, WAN/LAN Router, DHCP Client/Server, DNS Server, IPS, IDS, VPN

# What DSL Modem? Why do that?

1. Consumer modems have vulnerabilities that vendors just plain refuse to fix.
2. Botnets
3. Because it’s fun!



In this howto I am explaining restoration of a full opcode
of the stripped ELF in ARM arch. With the method explained in
the MMD ELF Workshop. The skeleton will
help to define which function are those fcn.xxx & we have only
reverse the rest of value, then good C code will
be created beautifully.   by @unixfreaxjp of #MalwareMustDie

```
// cracking a stripped ARM ELF malware

      0x0000ccf8    2f0d00eb    bl fcn.000101bc
      0x0000ccfc    010070e3    cmn r0, 1
      0x0000cd00    0040a0e1    mov r4, r0
  ,=< 0x0000cd04    0a00000a    beq 0xcd34
  |   0x0000cd08    451aa0e3    mov r1, 0x45000
  |   0x0000cd0c    0130a0e3    mov r3, 1
  |   0x0000cd10    071c81e2    add r1, r1, 0x700
  |   0x0000cd14    462d8de2    add r2, sp, 0x1180
  |   0x0000cd18    015a8de2    add r5, sp, 0x1000
  |   0x0000cd1c    121181e2    add r1, r1, 0x80000004
  |   0x0000cd20    142082e2    add r2, r2, 0x14
  |   0x0000cd24    943185e5    str r3, [r5, 0x194]
  |   0x0000cd28    040d00eb    bl fcn.00010140
  |   0x0000cd2c    0400a0e1    mov r0, r4
  |   0x0000cd30    e80c00eb    bl fcn.000100d8
  |   ; JMP XREF from 0x0000cd04 (main)
  `-> 0x0000cd34    7c089fe5    ldr r0, [pc, 0x87c]
      0x0000cd38    db0c00eb    bl fcn.000100ac
```

```
// using skeleton to force rollback all function names

  // MMD skeleton:

  char *stripped-functions-mmd[] = {
    fcn.000101bc = open()
    fcn.00010140 = execl()
    fcn.000100d8 = close()
    fcn.000100ac = chdir()
    (void*)0
  };

// restore the all value into its place :) & CRACKZ!!

  // source code reversed :

    cmd1 = open("/dev/watchdog", 2, %d, %d);
    if ( cmd != -1 ) // if wachdog opened
    {
      execl("/dev/watchdog", -2147199228, 't', 1);
      close(v6);
    }
   chdir("/");
```

#MalwareMustDie! Linux/Mirai ELF ARM Malware Reversing
@unixfreaxjp, Aug 29 2016

# Arris Example

**Backdoor #1 - Hard Coded SSH Creds -** remotessh/5SaP9I26

**Backdoor #2 - The magical port 49955 that keeps on giving - Injection/Default Creds of tech no pass**

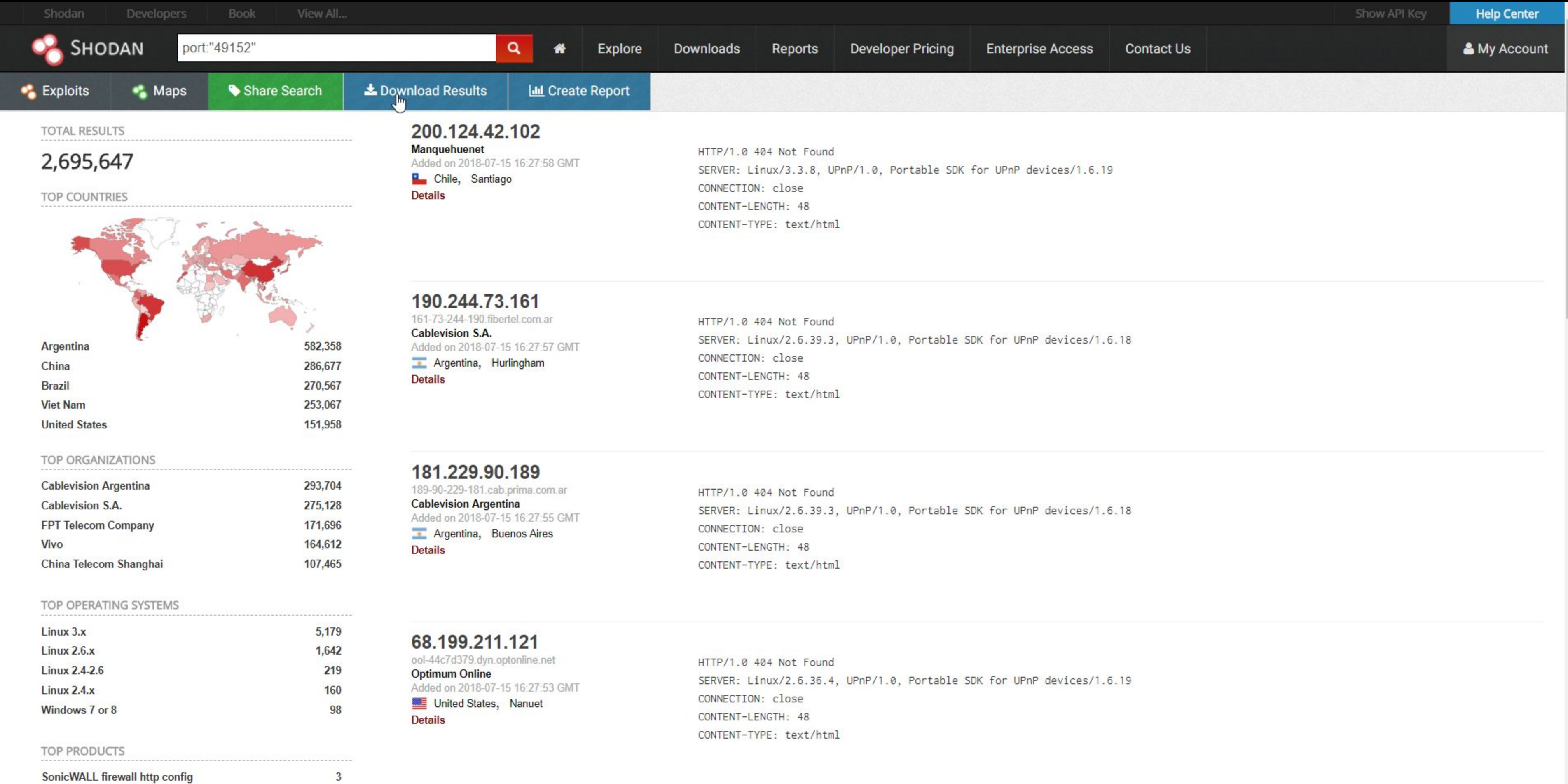
It’s probably worth noting that ISP’s could easily filter and stop the exploitation of this bug.

**Backdoor #3 - Hard Coded Creds via port 61001 -** bdctest/bdctes

Exploiting this flaw requires the attacker to know the device’s serial number, which would ultimately make this much harder to exploit but could still be a viable attack vector.

**Backdoor #4 - Firewall bypass via port 49152**

*Source: https://www.omnificentsystems.com/security/cable-modem-compromise-2017/*



port:"49152"

TOTAL RESULTS

2,695,647

TOP COUNTRIES

| | |
|---|---|
| Argentina | 582,358 |
| China | 286,677 |
| Brazil | 270,567 |
| Viet Nam | 253,067 |
| United States | 151,958 |

TOP ORGANIZATIONS

| | |
|---|---|
| Cablevision Argentina | 293,704 |
| Cablevision S.A. | 275,128 |
| FPT Telecom Company | 171,696 |
| Vivo | 164,612 |
| China Telecom Shanghai | 107,465 |

TOP OPERATING SYSTEMS

| | |
|---|---|
| Linux 3.x | 5,179 |
| Linux 2.6.x | 1,642 |
| Linux 2.4-2.6 | 219 |
| Linux 2.4.x | 160 |
| Windows 7 or 8 | 98 |

TOP PRODUCTS

| | |
|---|---|
| SonicWALL firewall http config | 3 |

**200.124.42.102**
**Manquehuenet**
Added on 2018-07-15 16:27:58 GMT
Chile, Santiago
Details

```
HTTP/1.0 404 Not Found
SERVER: Linux/3.3.8, UPnP/1.0, Portable SDK for UPnP devices/1.6.19
CONNECTION: close
CONTENT-LENGTH: 48
CONTENT-TYPE: text/html
```

**190.244.73.161**
161-73-244-190.fibertel.com.ar
**Cablevision S.A.**
Added on 2018-07-15 16:27:57 GMT
Argentina, Hurlingham
Details

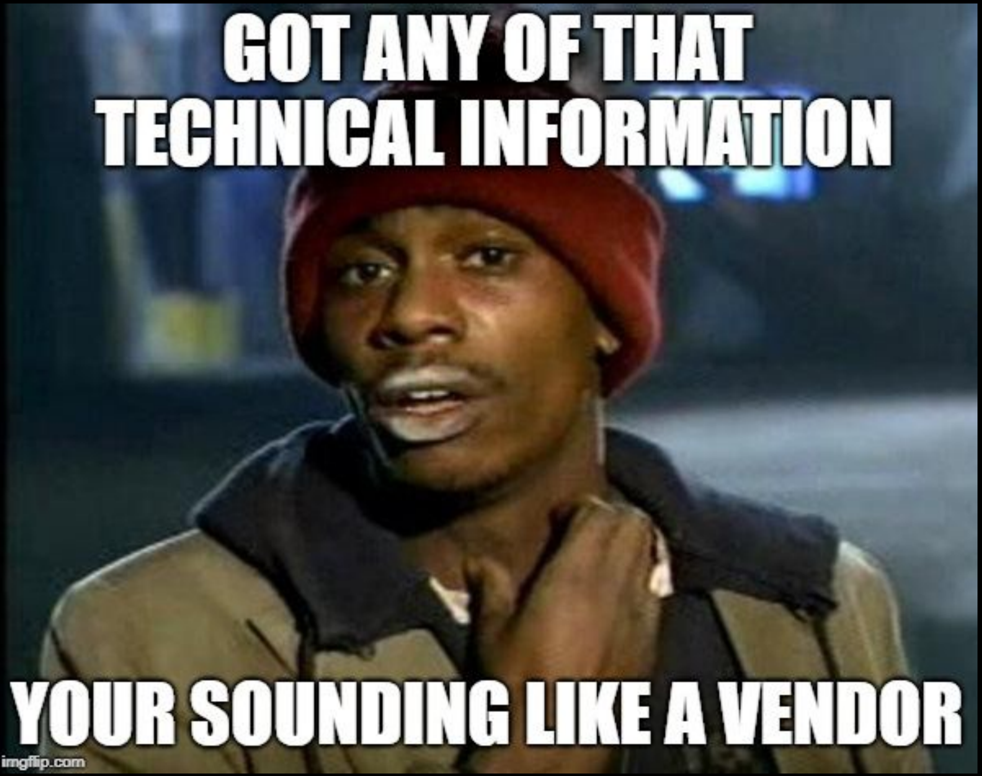
```
HTTP/1.0 404 Not Found
SERVER: Linux/2.6.39.3, UPnP/1.0, Portable SDK for UPnP devices/1.6.18
CONNECTION: close
CONTENT-LENGTH: 48
CONTENT-TYPE: text/html
```

**181.229.90.189**
189-90-229-181.cab.prima.com.ar
**Cablevision Argentina**
Added on 2018-07-15 16:27:55 GMT
Argentina, Buenos Aires
Details

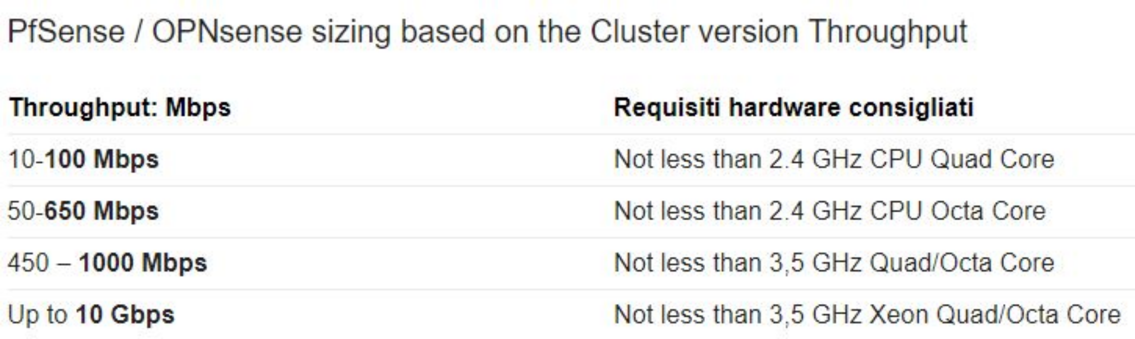
```
HTTP/1.0 404 Not Found
SERVER: Linux/2.6.39.3, UPnP/1.0, Portable SDK for UPnP devices/1.6.18
CONNECTION: close
CONTENT-LENGTH: 48
CONTENT-TYPE: text/html
```

**68.199.211.121**
ool-44c7d379.dyn.optonline.net
**Optimum Online**
Added on 2018-07-15 16:27:53 GMT
United States, Nanuet
Details

```
HTTP/1.0 404 Not Found
SERVER: Linux/2.6.36.4, UPnP/1.0, Portable SDK for UPnP devices/1.6.19
CONNECTION: close
CONTENT-LENGTH: 48
CONTENT-TYPE: text/html
```


GOT ANY OF THAT TECHNICAL INFORMATION
YOUR SOUNDING LIKE A VENDOR
imgflip.com

# What you will need



PfSense / OPNsense sizing based on the Cluster version Throughput

| **Throughput: Mbps** | **Requisiti hardware consigliati** |
|---|---|
| 10-**100 Mbps** | Not less than 2.4 GHz CPU Quad Core |
| 50-**650 Mbps** | Not less than 2.4 GHz CPU Octa Core |
| 450 – **1000 Mbps** | Not less than 3,5 GHz Quad/Octa Core |
| Up to **10 Gbps** | Not less than 3,5 GHz Xeon Quad/Octa Core |

If you have VDSL2 or ADSL/2+

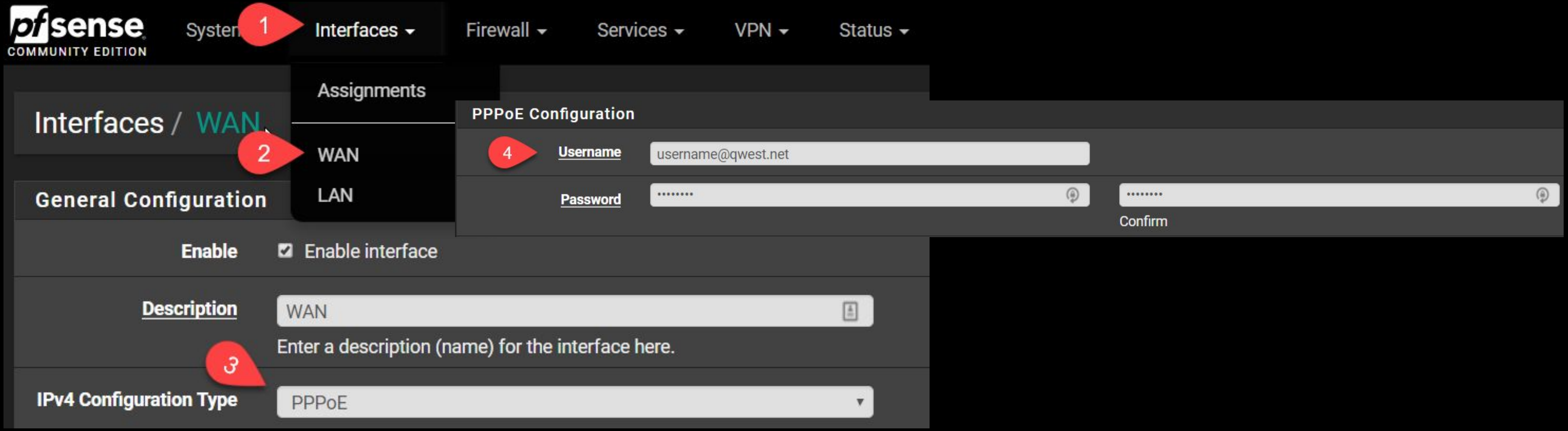
- A VDSL2/ADSL2+ modem/router on PCI-E card
- Example: https://www.draytek.com/en/products/products-a-z/router.all/vigornic-132-series

If you have FTTH

- 2 x GbE NIC’s, or 10GbE NIC’s to future proof

# How to configure

- Click on Interfaces then your WAN interface
- IPv4 Configuration Type needs to be set to PPPoE
- Under PPPoE configuration enter your PPPoE creds



Interfaces / WAN

General Configuration

Enable ☑ Enable interface

Description: WAN
Enter a description (name) for the interface here.

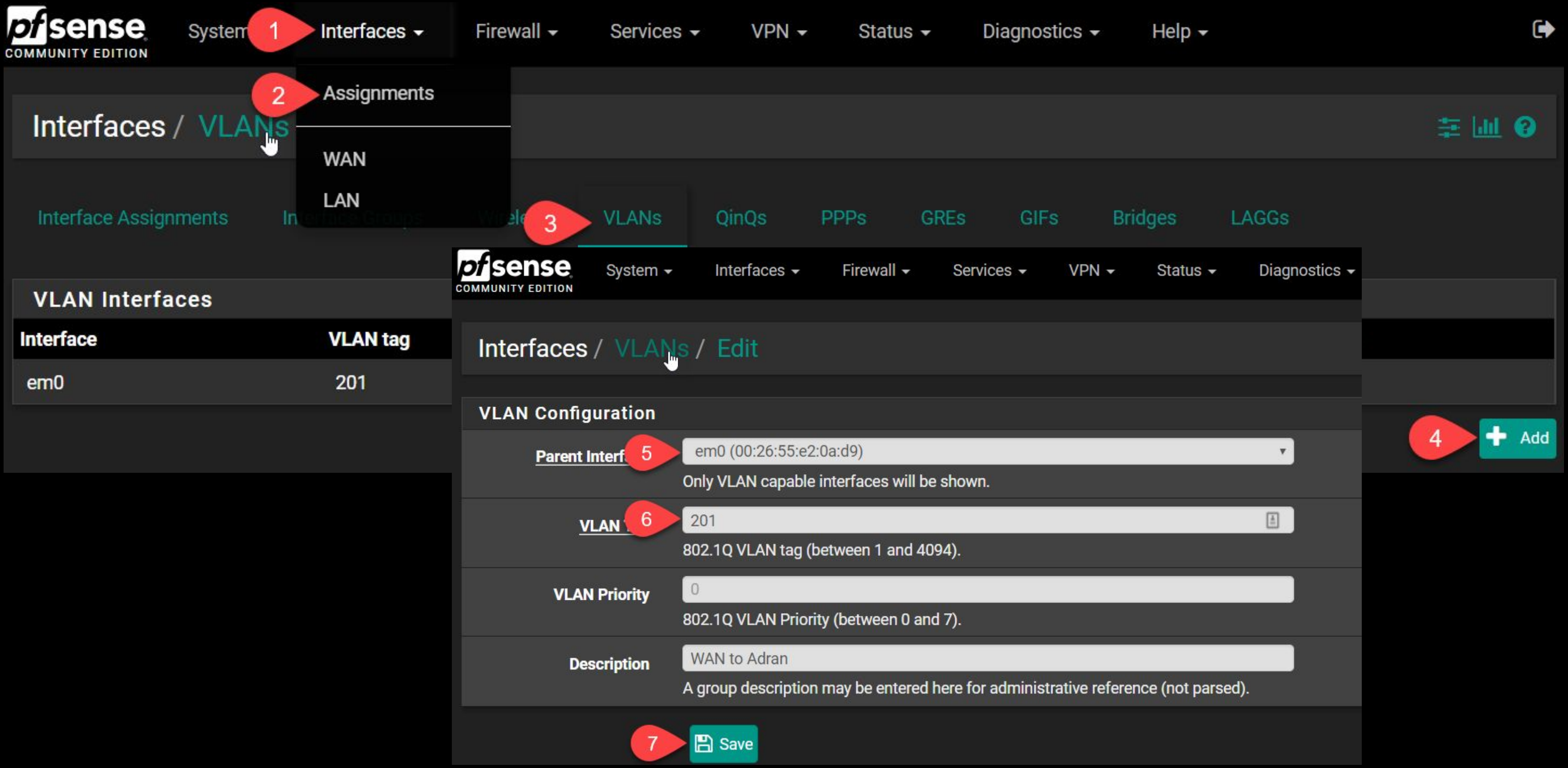
IPv4 Configuration Type: PPPoE

PPPoE Configuration

Username: username@qwest.net

Password: •••••••• Confirm: ••••••••

# If you have CenturyLink FTTH



Interfaces / VLANs

VLAN Interfaces

| Interface | VLAN tag |
|---|---|
| em0 | 201 |

Interfaces / VLANs / Edit

VLAN Configuration

Parent Interf: em0 (00:26:55:e2:0a:d9)

Only VLAN capable interfaces will be shown.

VLAN: 201

802.1Q VLAN tag (between 1 and 4094).

VLAN Priority: 0

802.1Q VLAN Priority (between 0 and 7).

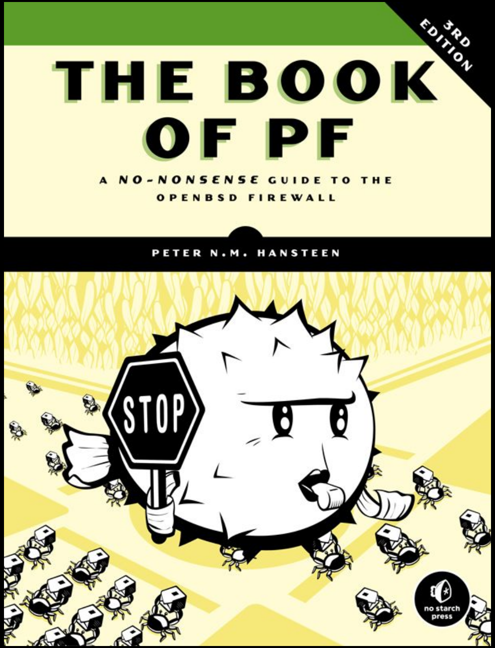
Description: WAN to Adran

A group description may be entered here for administrative reference (not parsed).

# Potential Gotcha’s

- If you have a virtual machine you will want to make sure you VLAN tag in PFSense or Hypervisor not both.
- If you have a virtual machine make sure the ports are static otherwise you will be playing the unplug, swap cords and swap VLAN tagged port Hokey Pokey.

# Feeling like hard mode?


3RD EDITION
THE BOOK OF PF
A NO-NONSENSE GUIDE TO THE OPENBSD FIREWALL
PETER N.M. HANSTEEN
STOP
no starch press