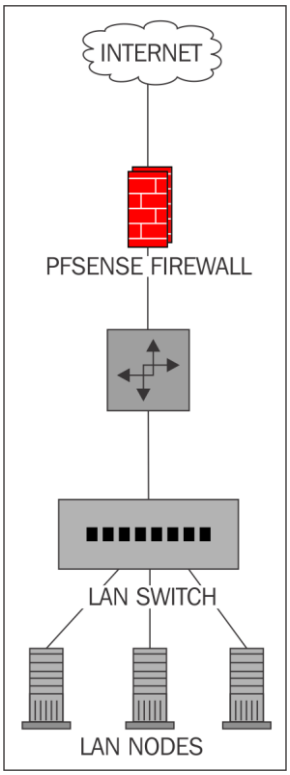
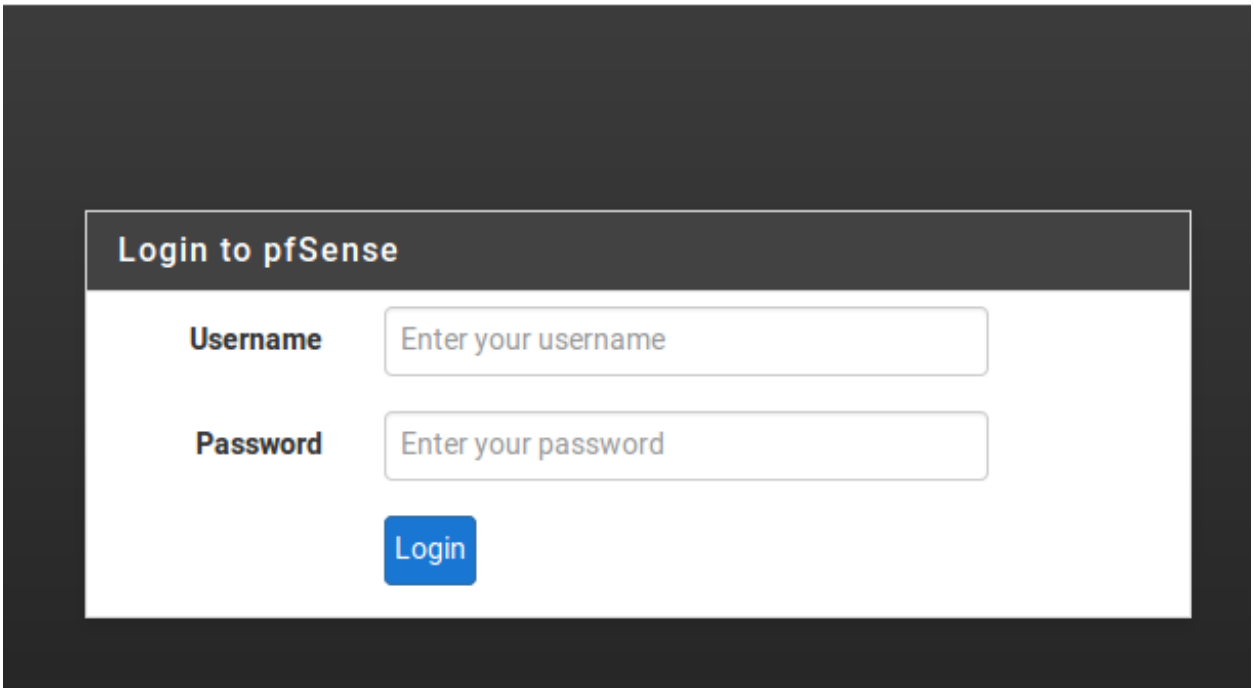
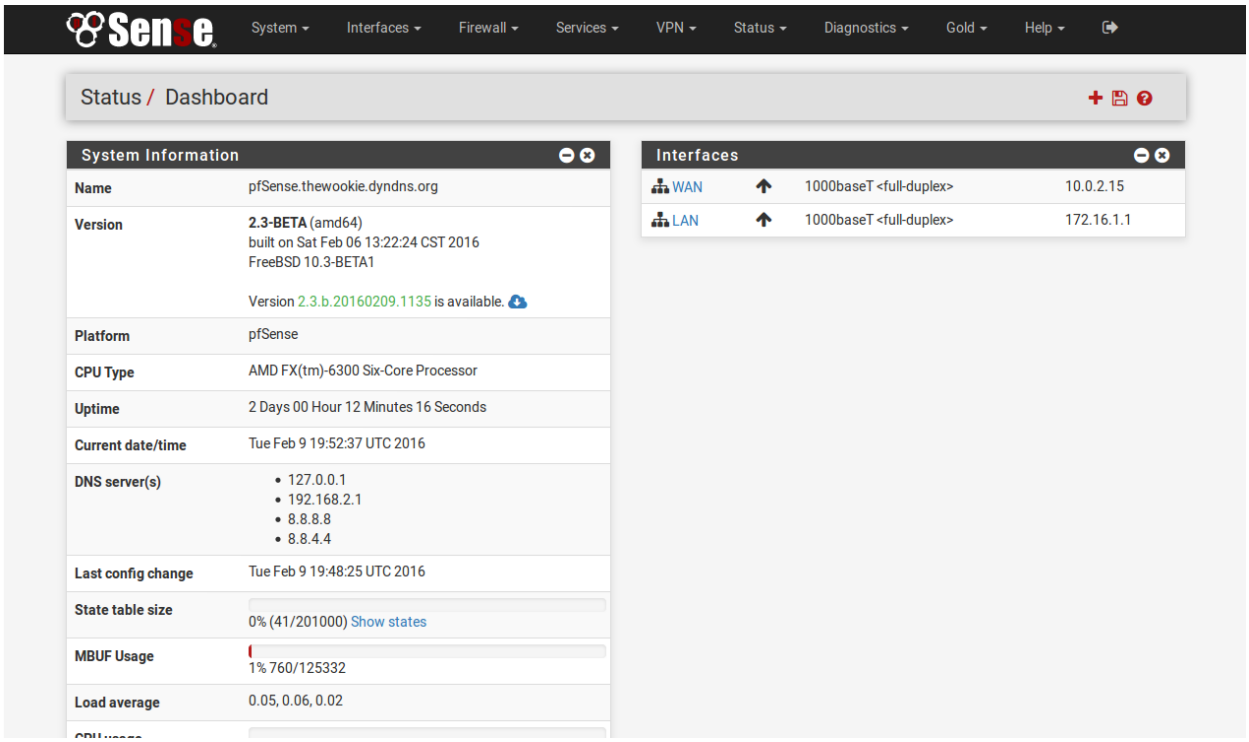
Chapter 1: pfSense Essentials




Login to pfSense
Username
Enter your username
Password
Enter your password
Login


System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Status / Dashboard
System Information
Name
pfSense.thewookie.dyndns.org
Version
2.3-BETA (amd64)
built on Sat Feb 06 13:22:24 CST 2016
FreeBSD 10.3-BETA1
Version 2.3.b.20160209.1135 is available.
Platform
pfSense
CPU Type
AMD FX(tm)-6300 Six-Core Processor
Uptime
2 Days 00 Hour 12 Minutes 16 Seconds
Current date/time
Tue Feb 9 19:52:37 UTC 2016
DNS server(s)
127.0.0.1
192.168.2.1
8.8.8.8
8.8.4.4
Last config change
Tue Feb 9 19:48:25 UTC 2016
State table size
0% (41/201000) Show states
MBUF Usage
1% 760/125332
Load average
0.05, 0.06, 0.02
Interfaces
WAN
1000baseT <full-duplex>
10.0.2.15
LAN
1000baseT <full-duplex>
172.16.1.1

Advanced DHCP6 Client Configuration

Information only

☐ Exchange Information Only

Only exchange informational configuration parameters with servers.

Send options

DHCP send options to be sent when requesting a DHCP lease. [option declaration [, ...]]
Value Substitutions: {interface}, {hostname}, {mac_addr_asciiCD}, {mac_addr_hexCD}
Where C is U(pper) or L(ower) Case, and D is \" :-.\" Delimiter (space, colon, hyphen, or period) (omitted for none).
Some DHCP services may require certain options be or not be sent.

Request Options

DHCP request options to be sent when requesting a DHCP lease. [option [, ...]]
Some DHCP services may require certain options be or not be requested.

Scripts

Absolute path to a script invoked on certain conditions including when a reply message is received.
[/[dirname/[.../]]filename[.ext]].

Identity Association Statement

☐ Non-Temporary Address Allocation — id-assoc na ID | IPv6 address | pltime | vltime

☐ Prefix Delegation — id-assoc pd ID | IPv6 prefix | pltime | vltime

Prefix interface statement

Prefix Interface sla-id | sla-len

Authentication statement

Authname | Protocol | Algorithm | RDM

Keyinfo statement

Keyname | Realm

Keys

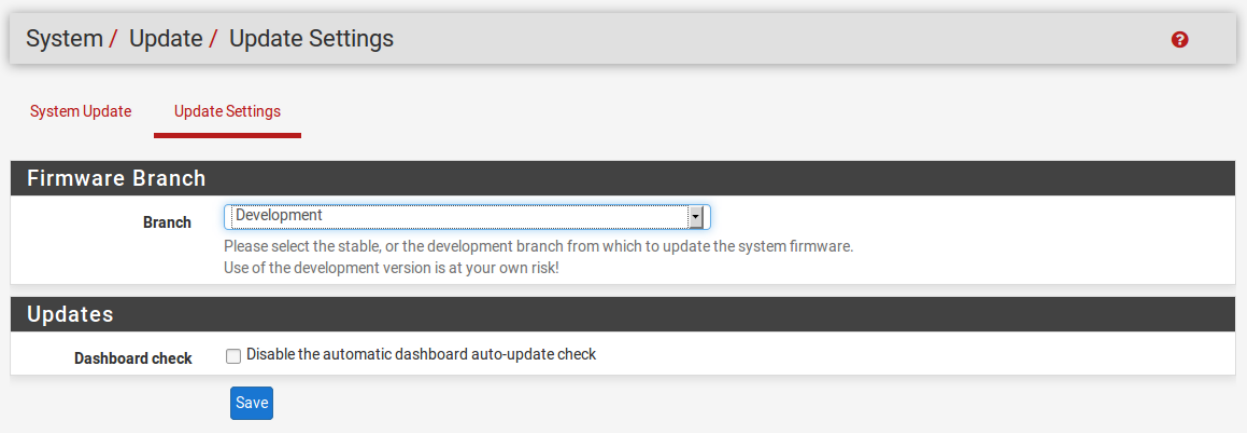
Authorized SSH Keys


```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDk6ha0TfTL7nW4Rdi7D9ax
oMlbQJehVcUh9NW3KZD8YhXo5RJr91aueFujQxp2vcybaZaSbX6g
qfa/fyfe6vIDA1LmwymC6RKwr9N4r2kbOZ5kJ2YtMGaqFBjvsCt0
9yYKxa6R7B2Fsk6Z00UKOVmWorupwppV2KvXTXrWHapozVxlaZlb
mwSOCkTO2SAF0PfLlGxKO6ZcpewFHad2s7by+OcUAl
```


Enter authorized SSH keys for this user

IPsec Pre-Shared Key

```
        php56-dom: 5.6.17 -> 5.6.18 [pfSense]
        php56-curl: 5.6.17 -> 5.6.18 [pfSense]
        php56-ctype: 5.6.17 -> 5.6.18 [pfSense]
        php56-bz2: 5.6.17 -> 5.6.18 [pfSense]
        php56-bcmath: 5.6.17 -> 5.6.18 [pfSense]
        php56: 5.6.17 -> 5.6.18 [pfSense]
        pfSense-repo-devel: 2.3.b.20160206.1322 -> 2.3.b.20160212.0356 [pfSense-
core]
        pfSense-rc: 2.3.b.20160206.1322 -> 2.3.b.20160212.0356 [pfSense-core]
        pfSense-kernel-pfSense: 2.3.b.20160206.1322 -> 2.3.b.20160212.0356 [pfSe
nse-core]
        pfSense-default-config: 2.3.b.20160206.1322 -> 2.3.b.20160212.0356 [pfSe
nse-core]
        pfSense-base: 2.3.b.20160206.1322 -> 2.3.b.20160212.0356 [pfSense-core]
        pfSense: 2.3.b.20160205.0822 -> 2.3.b.20160212.0922 [pfSense]
        openldap-client: 2.4.43 -> 2.4.44 [pfSense]
        filterdns: 1.0_7 -> 1.0_8 [pfSense]
        ca_root_nss: 3.20.1 -> 3.21 [pfSense]

The process will require 706 KiB more space.
45 MiB to be downloaded.

**** WARNING ****
Reboot will be required!!
Proceed with upgrade? (y/N)
```



Diagnostics / Backup/Restore

Config History | Backup/Restore

Backup configuration

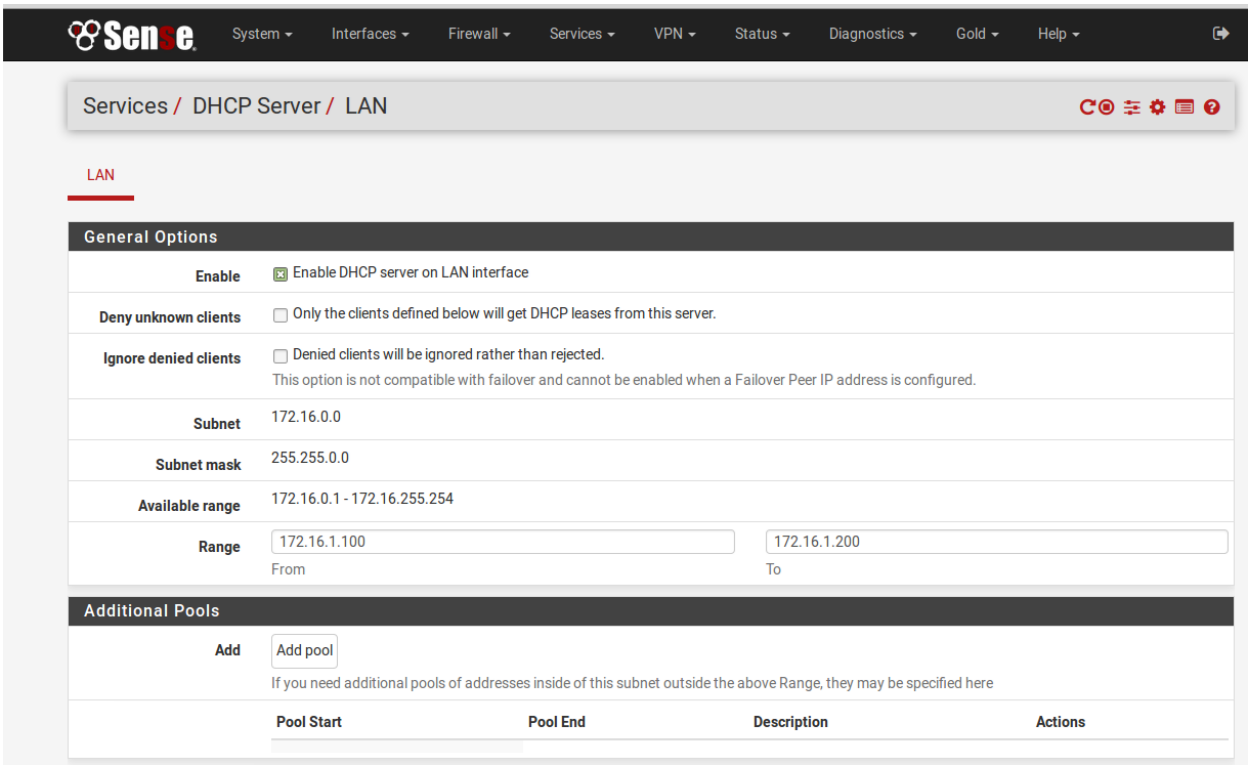
Backup area	All
Skip packages	☐ Do not backup package information.
Skip RRD data	☒ Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)
Encryption	☐ Encrypt this configuration file.
	Download configuration as XML

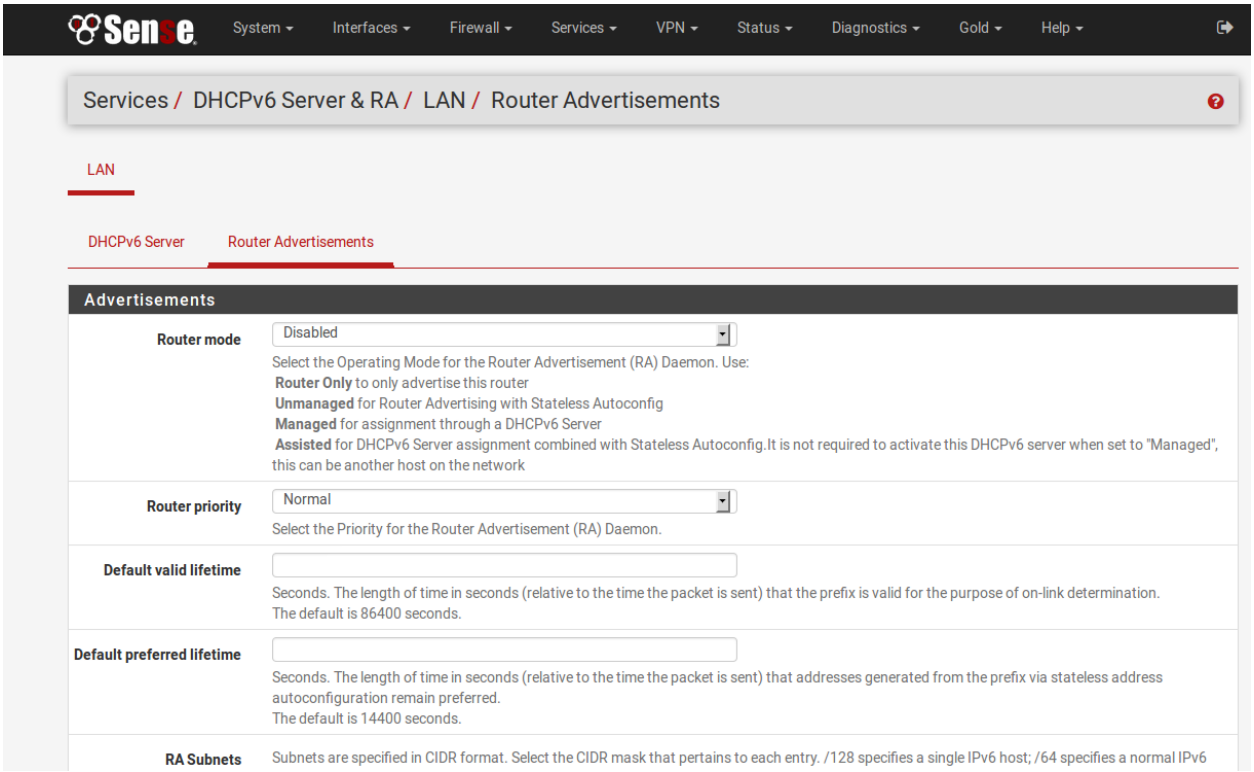
Restore backup

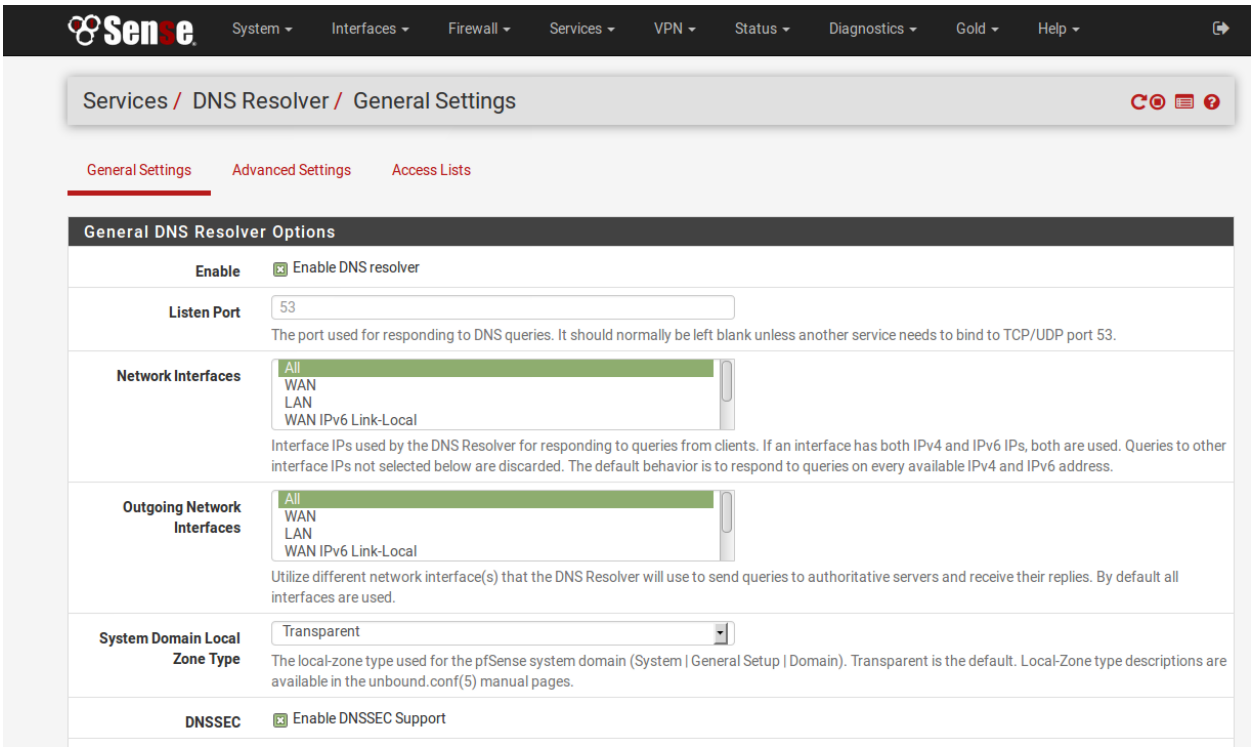
	Open a pfSense configuration XML file and click the button below to restore the configuration.
Restore area	All
Configuration file	Browse... No file selected.
Encryption	☐ Configuration file is encrypted.
	Restore Configuration The firewall will reboot after restoring the configuration.

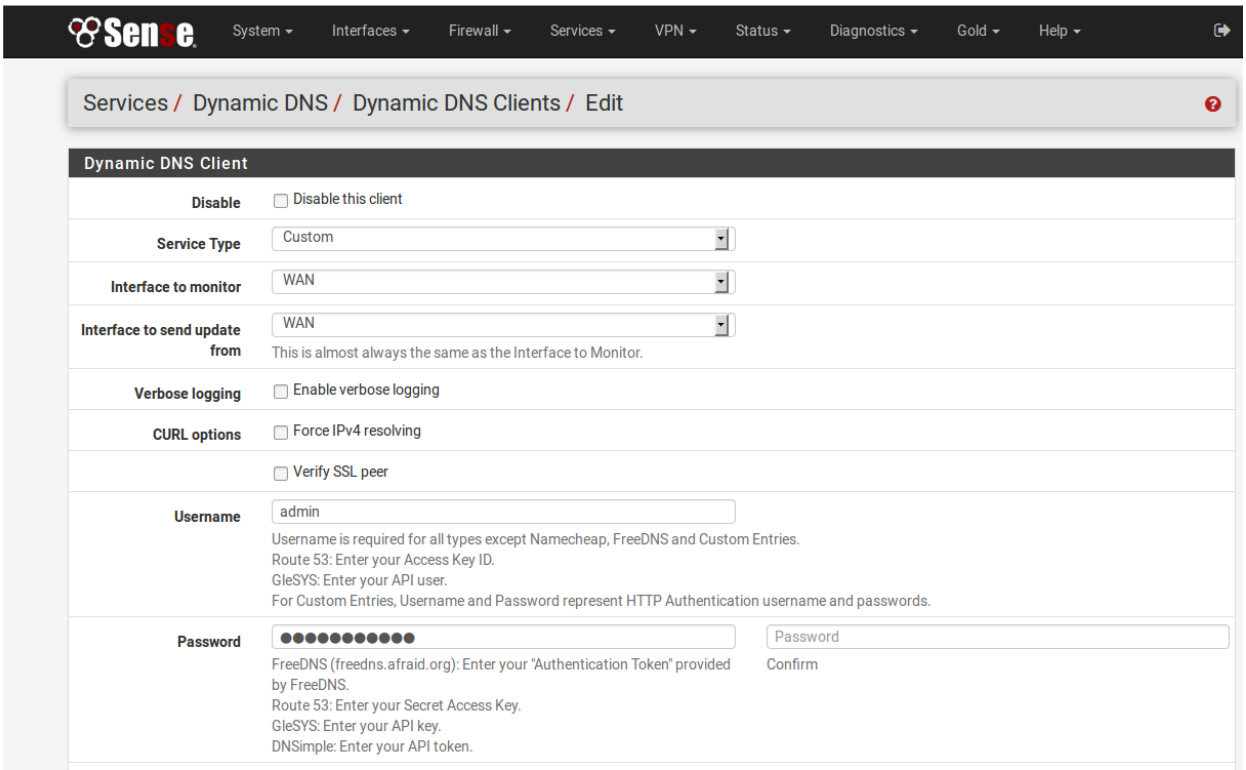
Chapter 2: Advanced pfSense Configuration

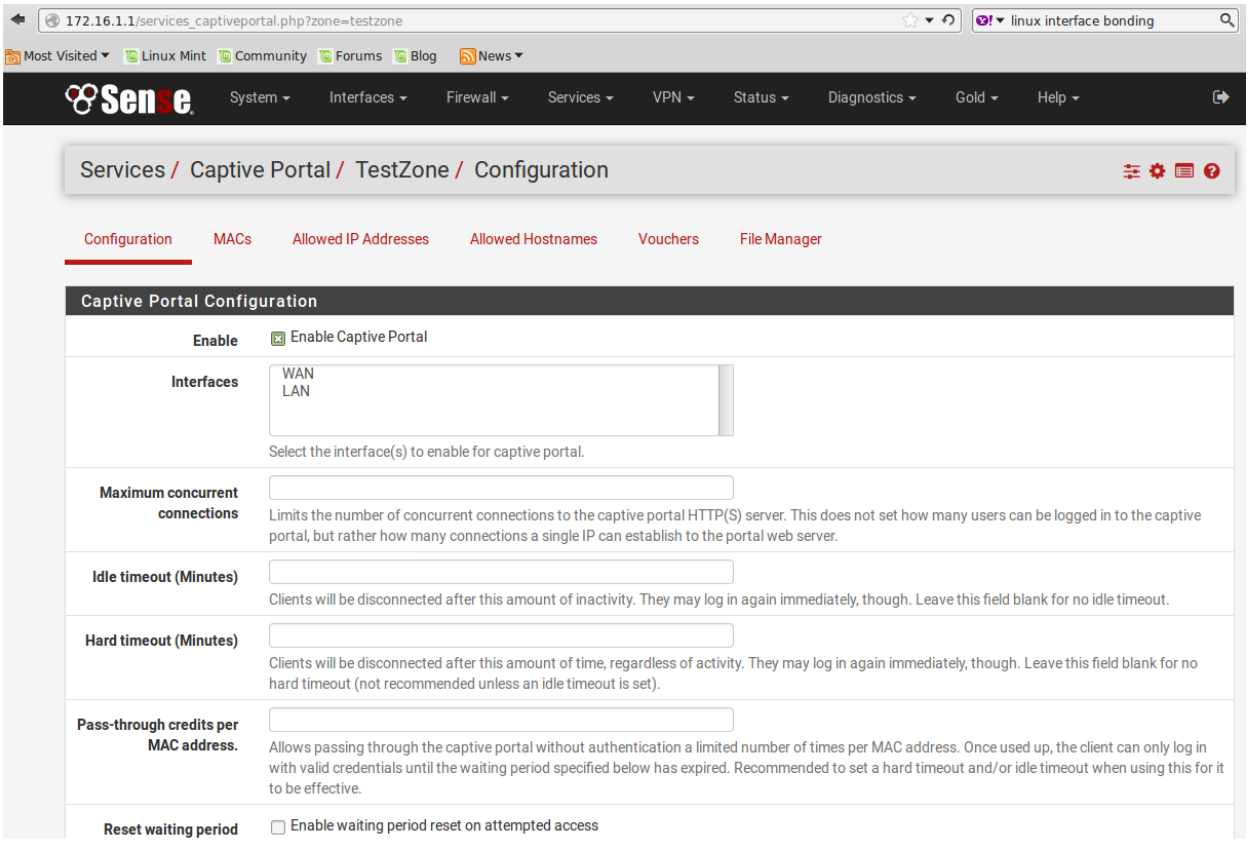
```
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.16.1.100
Enter the end address of the IPv4 client address range: 172.16.1.200

Do you want to enable the DHCP6 server on LAN? (y/n) y
Enter the start address of the IPv6 client address range: 1234:5678:9a::10
Enter the end address of the IPv6 client address range: 1234:5678:9a::100

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 172.16.1.1/16


The IPv6 LAN address has been set to 1234:5678:9a::1/48
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://172.16.1.1/
                http://[1234:5678:9a::1]/

Press <ENTER> to continue.
```

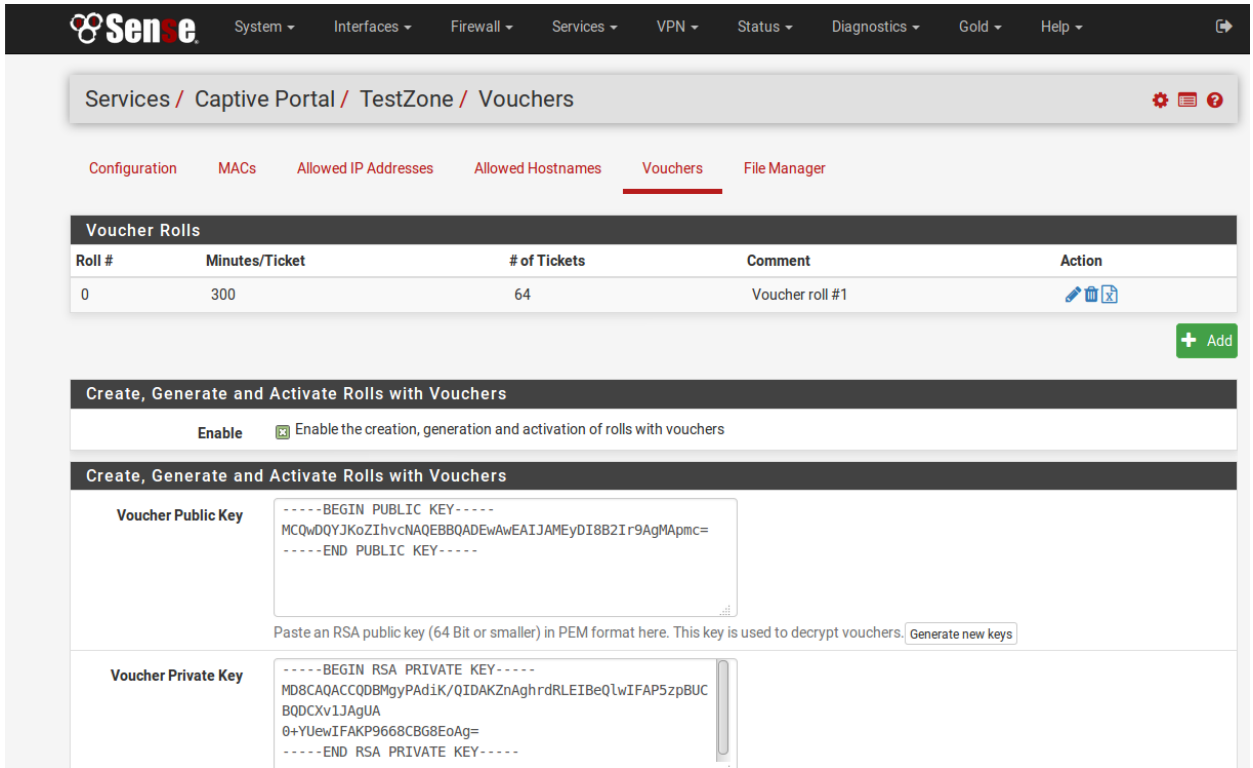


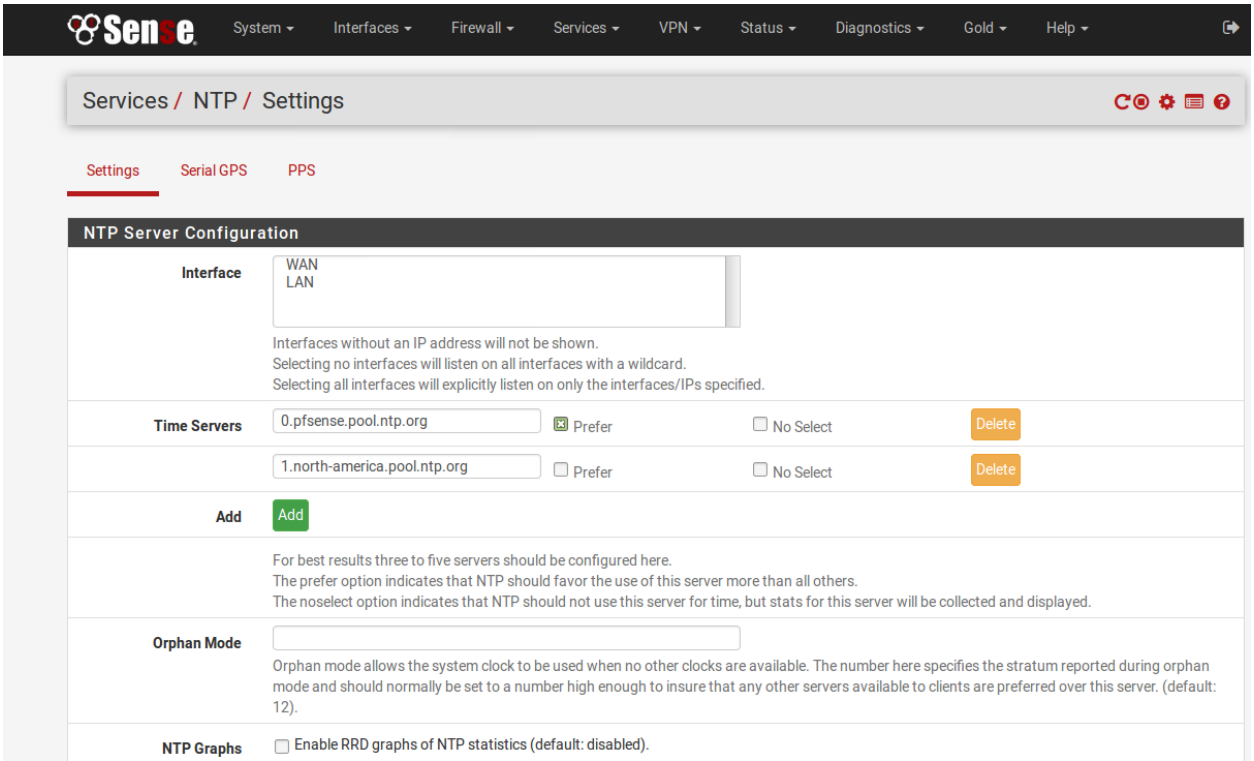

System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / DHCPv6 Server & RA / LAN / Router Advertisements
LAN
DHCPv6 Server
Router Advertisements
Advertisements
Router mode
Disabled
Select the Operating Mode for the Router Advertisement (RA) Daemon. Use:
Router Only to only advertise this router
Unmanaged for Router Advertising with Stateless Autoconfig
Managed for assignment through a DHCPv6 Server
Assisted for DHCPv6 Server assignment combined with Stateless Autoconfig.It is not required to activate this DHCPv6 server when set to "Managed", this can be another host on the network
Router priority
Normal
Select the Priority for the Router Advertisement (RA) Daemon.
Default valid lifetime
Seconds. The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination.
The default is 86400 seconds.
Default preferred lifetime
Seconds. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred.
The default is 14400 seconds.
RA Subnets
Subnets are specified in CIDR format. Select the CIDR mask that pertains to each entry. /128 specifies a single IPv6 host; /64 specifies a normal IPv6

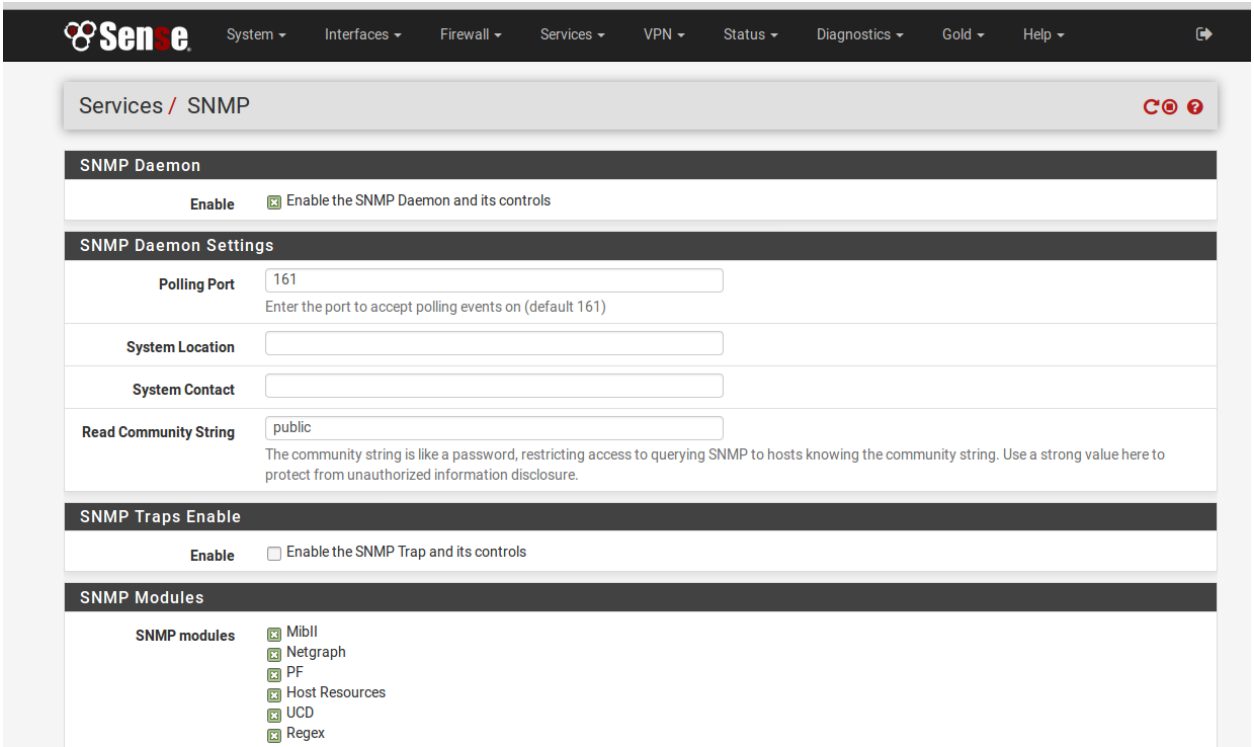

System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / DNS Resolver / General Settings
General Settings
Advanced Settings
Access Lists
General DNS Resolver Options
Enable
Enable DNS resolver
Listen Port
53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.
Network Interfaces
All
WAN
LAN
WAN IPv6 Link-Local
Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.
Outgoing Network Interfaces
All
WAN
LAN
WAN IPv6 Link-Local
Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.
System Domain Local Zone Type
Transparent
The local-zone type used for the pfSense system domain (System | General Setup | Domain). Transparent is the default. Local-Zone type descriptions are available in the unbound.conf(5) manual pages.
DNSSEC
Enable DNSSEC Support

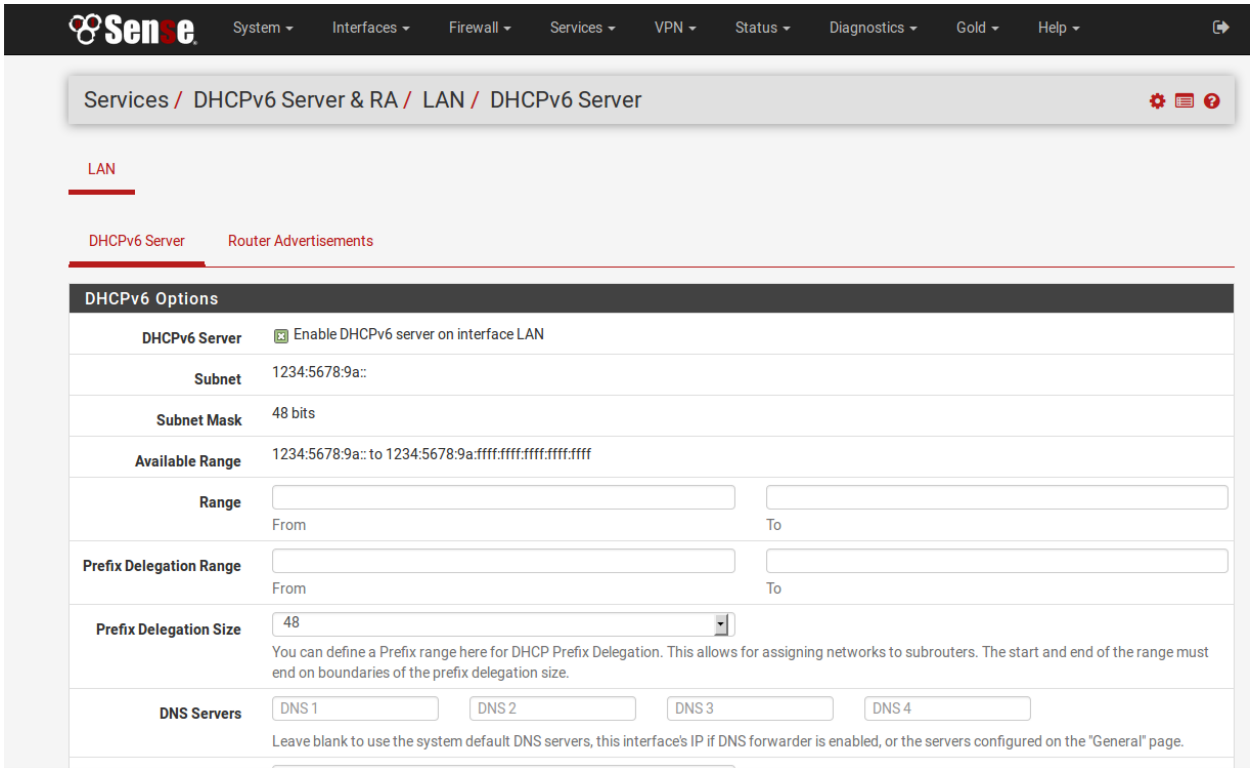

System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / Dynamic DNS / Dynamic DNS Clients / Edit
Dynamic DNS Client
Disable
Disable this client
Service Type
Custom
Interface to monitor
WAN
Interface to send update from
WAN
This is almost always the same as the Interface to Monitor.
Verbose logging
Enable verbose logging
CURL options
Force IPv4 resolving
Verify SSL peer
Username
admin
Username is required for all types except Namecheap, FreeDNS and Custom Entries.
Route 53: Enter your Access Key ID.
GleSYS: Enter your API user.
For Custom Entries, Username and Password represent HTTP Authentication username and passwords.
Password
Password
Confirm
FreeDNS (freedns.afraid.org): Enter your "Authentication Token" provided by FreeDNS.
Route 53: Enter your Secret Access Key.
GleSYS: Enter your API key.
DNSimple: Enter your API token.


172.16.1.1/services_captiveportal.php?zone=testzone
linux interface bonding
Most Visited
Linux Mint
Community
Forums
Blog
News
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / Captive Portal / TestZone / Configuration
Configuration
MACs
Allowed IP Addresses
Allowed Hostnames
Vouchers
File Manager
Captive Portal Configuration
Enable
Enable Captive Portal
Interfaces
WAN
LAN
Select the interface(s) to enable for captive portal.
Maximum concurrent connections
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.
Idle timeout (Minutes)
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout (Minutes)
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Pass-through credits per MAC address.
Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.
Reset waiting period
Enable waiting period reset on attempted access


Sense
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / Captive Portal / TestZone / Vouchers
Configuration
MACs
Allowed IP Addresses
Allowed Hostnames
Vouchers
File Manager
Voucher Rolls
Roll #
Minutes/Ticket
# of Tickets
Comment
Action
0
300
64
Voucher roll #1
Add
Create, Generate and Activate Rolls with Vouchers
Enable
Enable the creation, generation and activation of rolls with vouchers
Create, Generate and Activate Rolls with Vouchers
Voucher Public Key
-----BEGIN PUBLIC KEY-----
MCQwDQYJKoZIhvcNAQEBBQADEwAwEAIJAMEyDI8B2Ir9AgMApmc=
-----END PUBLIC KEY-----
Paste an RSA public key (64 Bit or smaller) in PEM format here. This key is used to decrypt vouchers.
Generate new keys
Voucher Private Key
-----BEGIN RSA PRIVATE KEY-----
MD8CAQACCQDBMgyPAdiK/QIDAKZnAghrdRLEIBeQlwIFAP5zpBUC
BQDCXv1JAgUA
0+YUewIFAKP9668CBG8EoAg=
-----END RSA PRIVATE KEY-----


Sense
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / NTP / Settings
Settings
Serial GPS
PPS
NTP Server Configuration
Interface
WAN
LAN
Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.
Time Servers
0.pfsense.pool.ntp.org
Prefer
No Select
Delete
1.north-america.pool.ntp.org
Prefer
No Select
Delete
Add
Add
For best results three to five servers should be configured here.
The prefer option indicates that NTP should favor the use of this server more than all others.
The noselect option indicates that NTP should not use this server for time, but stats for this server will be collected and displayed.
Orphan Mode
Orphan mode allows the system clock to be used when no other clocks are available. The number here specifies the stratum reported during orphan mode and should normally be set to a number high enough to insure that any other servers available to clients are preferred over this server. (default: 12).
NTP Graphs
Enable RRD graphs of NTP statistics (default: disabled).


System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / SNMP
SNMP Daemon
Enable
Enable the SNMP Daemon and its controls
SNMP Daemon Settings
Polling Port
161
Enter the port to accept polling events on (default 161)
System Location
System Contact
Read Community String
public
The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.
SNMP Traps Enable
Enable
Enable the SNMP Trap and its controls
SNMP Modules
SNMP modules
MibII
Netgraph
PF
Host Resources
UCD
Regex


System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / DHCPv6 Server & RA / LAN / DHCPv6 Server
LAN
DHCPv6 Server
Router Advertisements
DHCPv6 Options
DHCPv6 Server
Enable DHCPv6 server on interface LAN
Subnet
1234:5678:9a::
Subnet Mask
48 bits
Available Range
1234:5678:9a:: to 1234:5678:9a:ffff:ffff:ffff:ffff:ffff
Range
From
To
Prefix Delegation Range
From
To
Prefix Delegation Size
48
You can define a Prefix range here for DHCP Prefix Delegation. This allows for assigning networks to subrouters. The start and end of the range must end on boundaries of the prefix delegation size.
DNS Servers
DNS 1
DNS 2
DNS 3
DNS 4
Leave blank to use the system default DNS servers, this interface's IP if DNS forwarder is enabled, or the servers configured on the "General" page.

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Services / DNS Forwarder

General DNS Forwarder Options

Enable
☐ Enable DNS forwarder

DHCP Registration
☐ Register DHCP leases in DNS forwarder
If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

Static DHCP
☐ Register DHCP static mappings in DNS forwarder
If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

Prefer DHCP
☐ Resolve DHCP mappings first
If this option is set, then DHCP mappings will be resolved before the manual list of names below. This only affects the name given for a reverse lookup (PTR).

DNS Query Forwarding
☐ Query DNS servers sequentially
If this option is set, pfSense DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified (*System - General Setup - DNS Servers*), rather than all at once in parallel.

☐ Require domain
If this option is set, pfSense DNS Forwarder (dnsmasq) will not forward A or AAAA queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from /etc/hosts or DHCP then a "not found" answer is returned.

☐ Do not forward private reverse lookups
If this option is set, pfSense DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1918) to upstream name servers. Any entries in the Domain Overrides section forwarding private "n.n.n.in-addr.arpa" names to a specific server are still forwarded. If the IP to name is not known from /etc/hosts, DHCP or a specific domain override then a "not found" answer is immediately

Services / Dynamic DNS / RFC 2136 Clients / Edit

RFC 2136 Client

Enable ☐

Interface WAN

Hostname
Fully qualified hostname of the host to be updated

TTL (seconds)

Key name
This must match the setting on the DNS server.

Key Type ○ Zone ○ Host ○ User

Key
Paste an HMAC-MD5 key here.

Server

Protocol ☐ Use TCP instead of UDP

Use public IP ☐ If the interface IP is private, attempt to fetch and use the public IP instead.

Record Type ○ A (IPv4) ○ AAAA (IPv6) ○ Both

Description
You may enter a description here for your reference (not parsed).

Save

System / User Manager / Groups / Edit

Users | Groups | Settings | Authentication Servers

Group Properties

Defined by	
Group name	captiveportal
Description	Captive portal group Group description, for your own information only
Group membership	admin Not members Move to "Members" > Hold down CTRL (pc)/COMMAND (mac) key to select multiple items Members < Move to "Not members

Assigned Privileges

Name	Description
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.

Add

Diagnostics / Command Prompt

Shell Output - ntpq -p

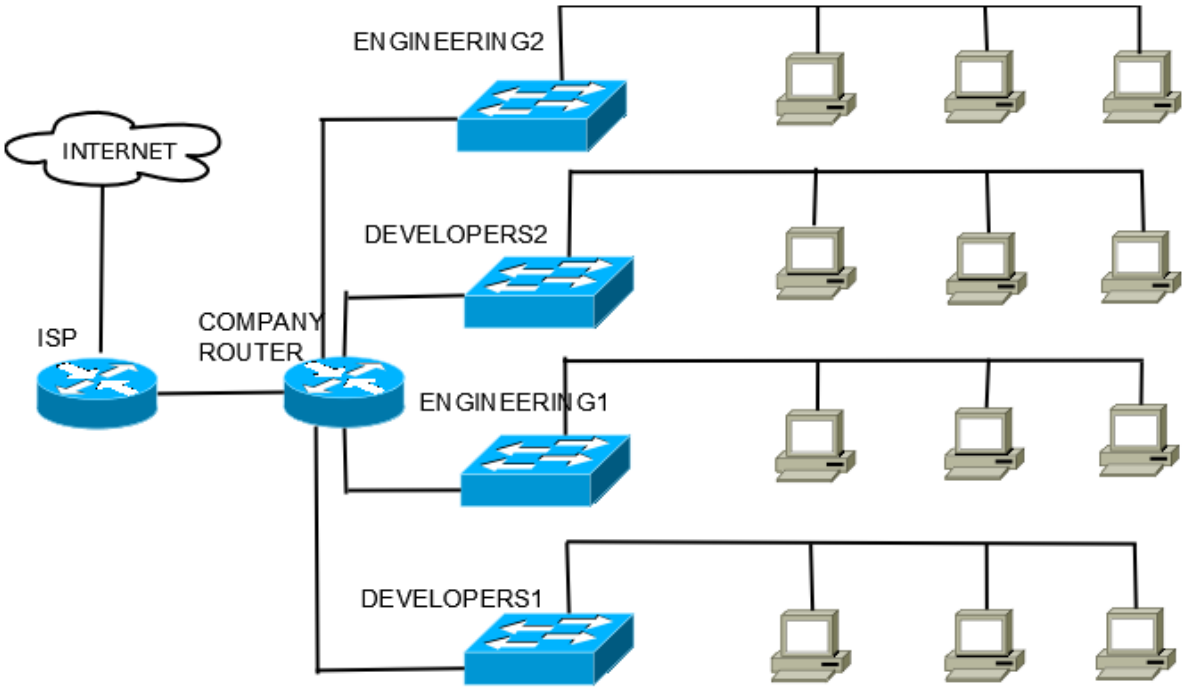
```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*199.102.46.78   .GPS.            1 u  123  512  337   39.233   -1.902   1.757
+104.131.53.252  209.51.161.238   2 u   21  512  377   13.670   -0.210   1.760
```

Execute Shell Command

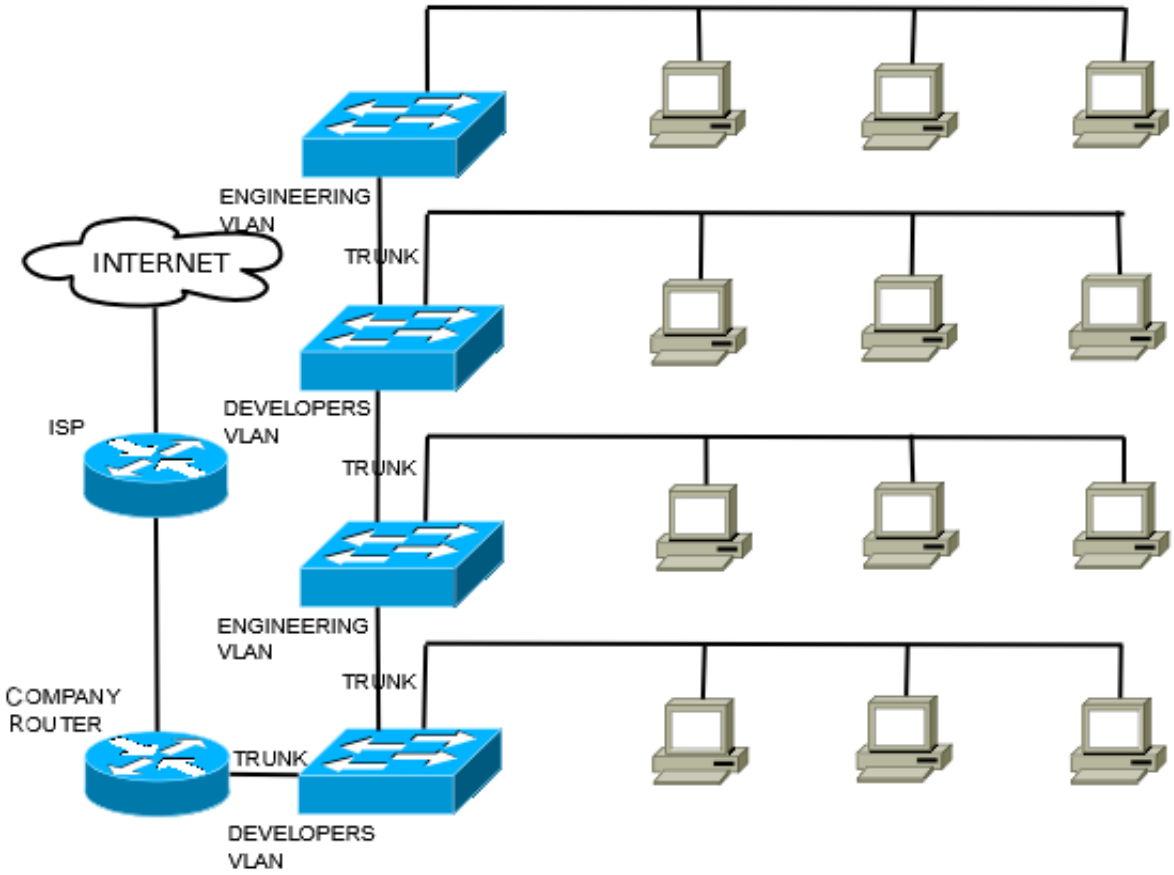
ntpq -p

< Execute > Clear

Chapter 3: Working with VLANs



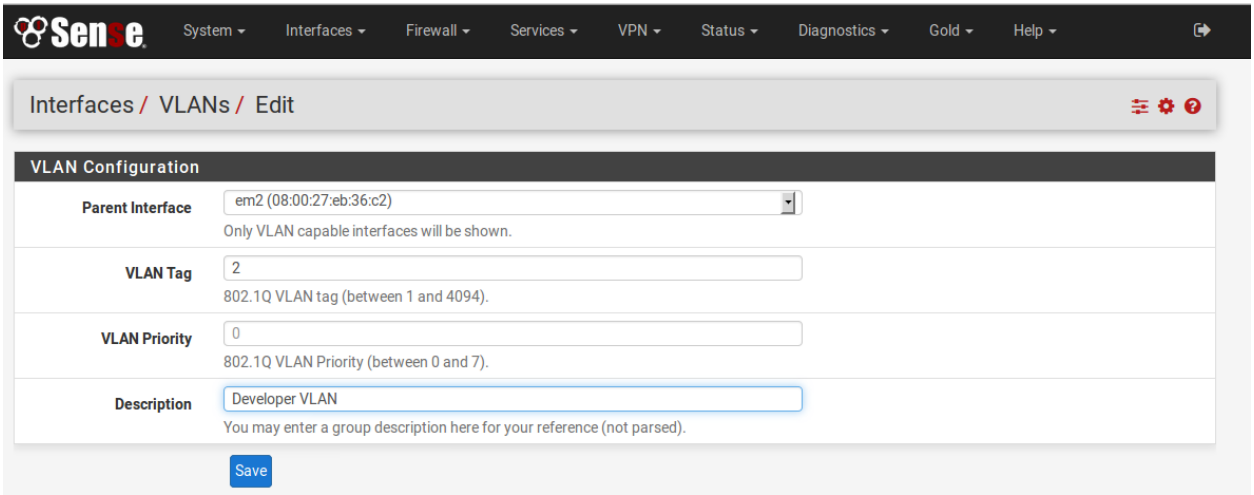
Without VLANs



With VLANS

```
Enter the parent interface name for the new VLAN (or nothing if finished): em2
Enter the VLAN tag (1-4094): 3


VLAN Capable interfaces:

em0     08:00:27:32:4b:fc   (up)
em1     08:00:27:ce:ff:d1   (up)
em2     08:00:27:eb:36:c2   (up)

Enter the parent interface name for the new VLAN (or nothing if finished):


VLAN interfaces:

em2_vlan2       VLAN tag 2, parent interface em2
em2_vlan3       VLAN tag 3, parent interface em2

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em2_vlan2 em2_vlan3 or a):
```

```
(em0 em1 em2 em2_vlan2 em2_vlan3 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em2_vlan2 em2_vlan3 a or nothing if finished): em1

Optional interface 1 description found: DEVELOPERS
Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em2_vlan2 em2_vlan3 a or nothing if finished): em2_vlan2

Optional interface 2 description found: ENGINEERING
Enter the Optional 2 interface name or 'a' for auto-detection
(em2 em2_vlan3 a or nothing if finished): em2_vlan3

Enter the Optional 3 interface name or 'a' for auto-detection
(em2 a or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2_vlan2
OPT2 -> em2_vlan3

Do you want to proceed [y|n]?
```



Interfaces / DEVELOPERS

General Configuration

Enable	Enable interface
Description	DEVELOPERS Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC controls	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	172.17.1.1	/ 32

pfSense System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Interfaces / QinQs / Edit

QinQ Configuration

Parent interface	em2 (08:00:27:eb:36:c2) Only QinQ capable interfaces will be shown.
First level tag	4 This is the first level VLAN tag. On top of this are stacked the member VLANs defined below.
Option(s)	Adds interface to QinQ interface groups Allows rules to be written more easily
Description	VLAN for super-secret app development project You may enter a description here for your reference (not parsed).
Member(s)	You can specify ranges in the inputs below. Enter a range (2-3) or individual numbers. Click "Duplicate" as many times as needed to add new inputs
Tag(s)	2 Delete Add

Save

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Interfaces / LAGGs / Edit

LAGG Configuration

Parent Interfaces

em2 (08:00:27:eb:36:c2)
em2_4 (08:00:27:eb:36:c2)
em2_4_2 (08:00:27:eb:36:c2)

Choose the members that will be used for the link aggregation.

LAGG Protocol

NONE

- **NONE**
  This protocol is intended to do nothing: it disables any traffic without disabling the lagg interface itself
- **LACP**
  Supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP) and the Marker Protocol. LACP will negotiate a set of aggregable links with the peer in to one or more Link Aggregated Groups. Each LAG is composed of ports of the same speed, set to full-duplex operation. The traffic will be balanced across the ports in the LAG with the greatest total speed, in most cases there will only be one LAG which contains all ports. In the event of changes in physical connectivity, Link Aggregation will quickly converge to a new configuration.
- **FAILOVER**
  Sends and receives traffic only through the master port. If the master port becomes unavailable, the next active port is used. The first interface added is the master port; any interfaces added after that are used as failover devices.
- **FEC**
  Supports Cisco EtherChannel. This is a static setup and does not negotiate aggregation with the peer or exchange frames to monitor the link.
- **LOADBALANCE**
  Balances outgoing traffic across the active ports based on hashed protocol header information and accepts incoming traffic from any active port. This is a static setup and does not negotiate aggregation with the peer or exchange frames to monitor the link. The hash includes the Ethernet source and destination address, and, if available, the VLAN tag, and the IP source and destination address
- **ROUNDROBIN**
  Distributes outgoing traffic using a round-robin scheduler through all active ports and accepts incoming traffic from any active port

Save

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

DEVELOPERS

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to

Protocol

any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match. DEVELOPERS net Source Address /

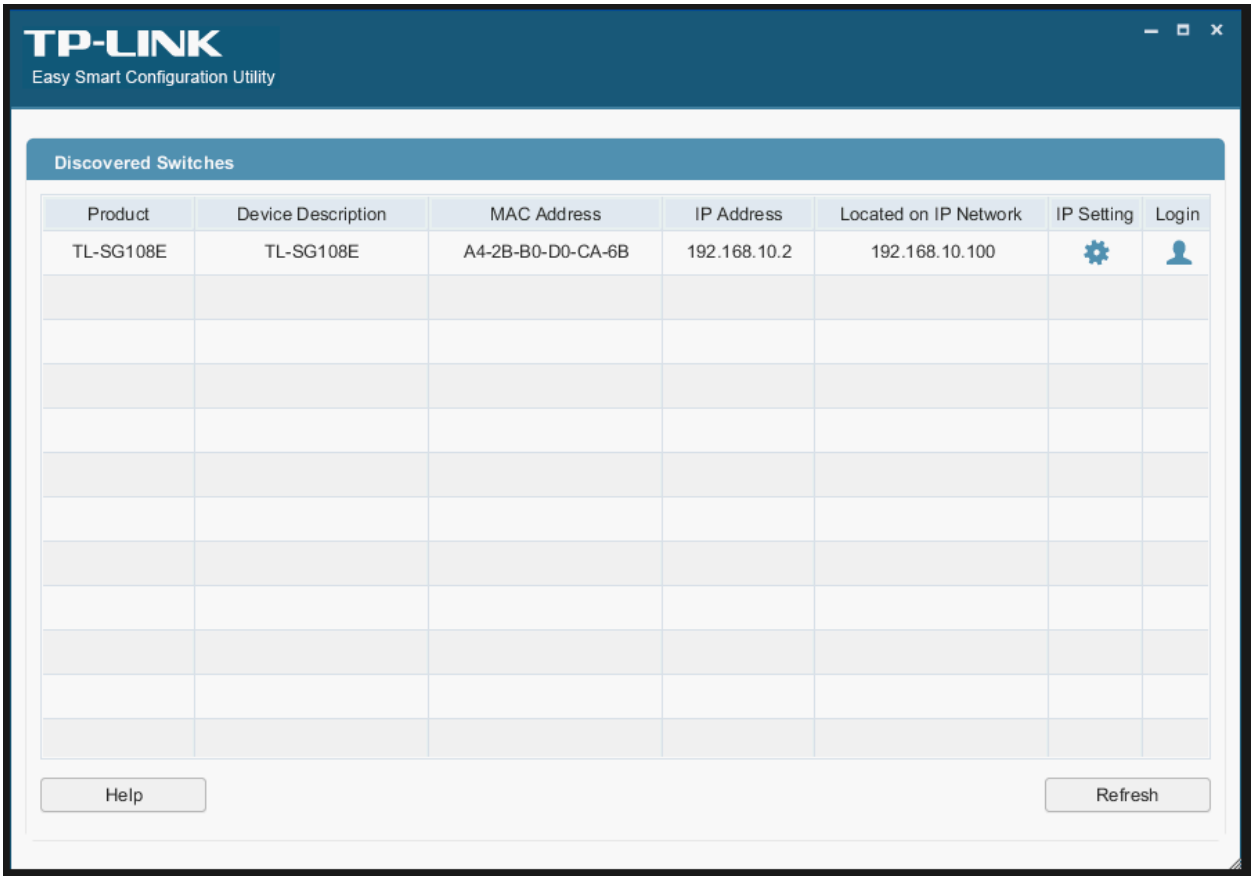
Show advanced

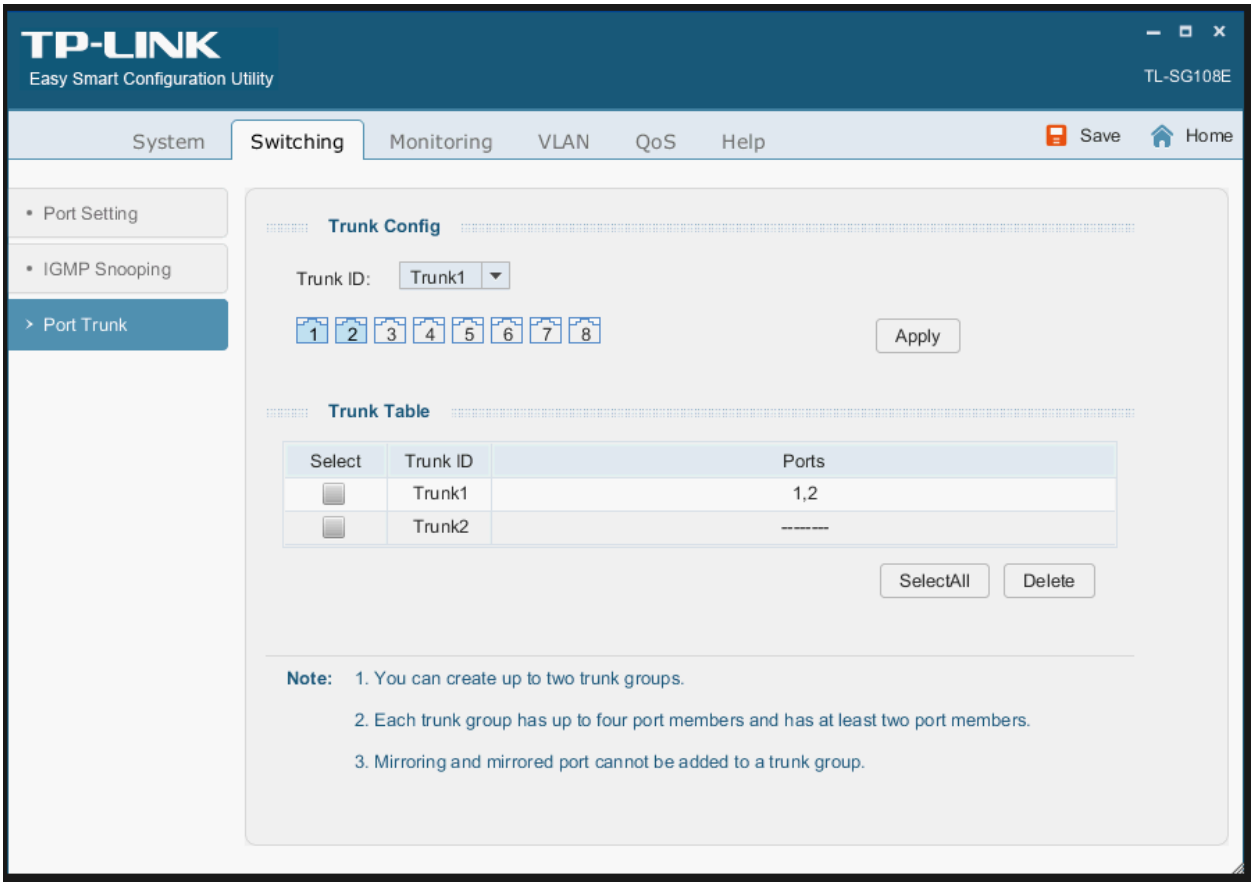
Show advanced

Destination

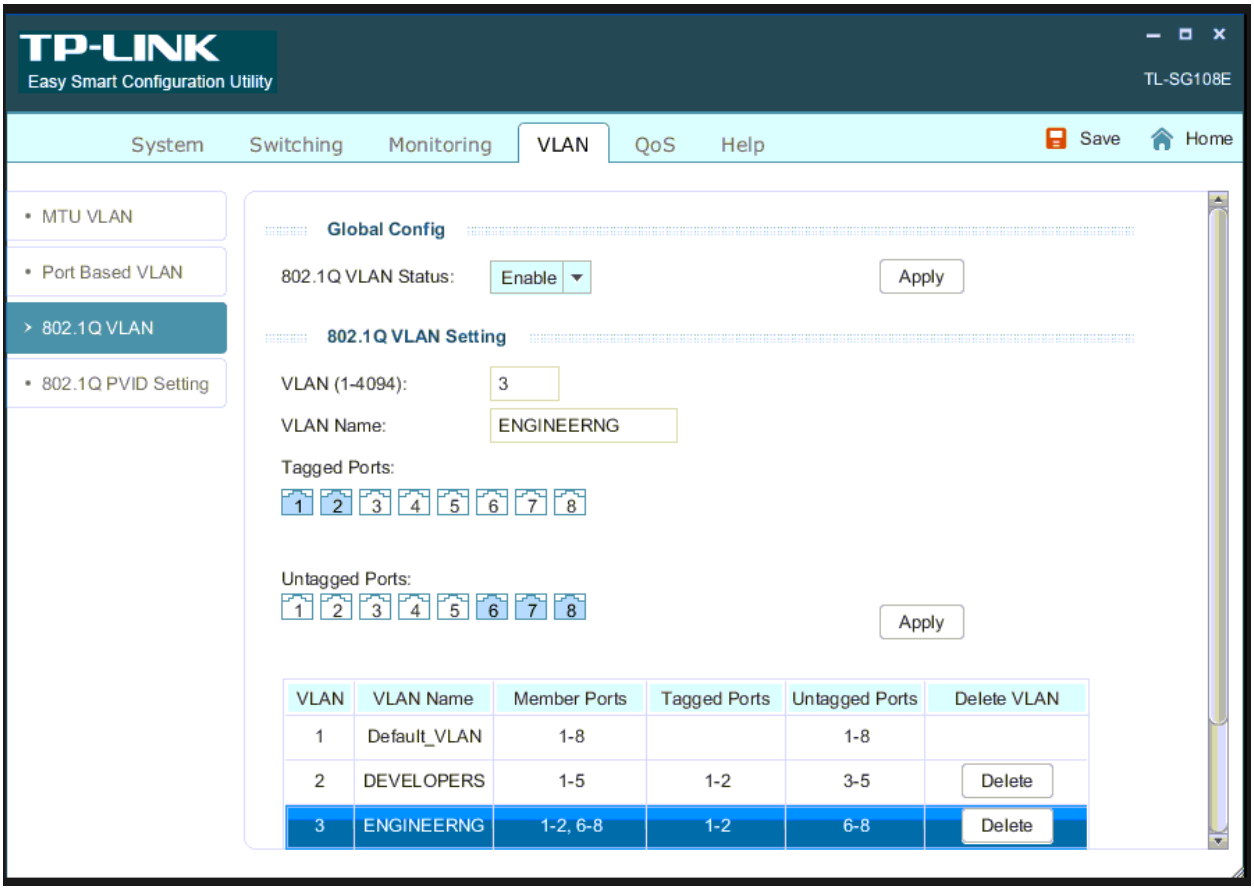
Destination

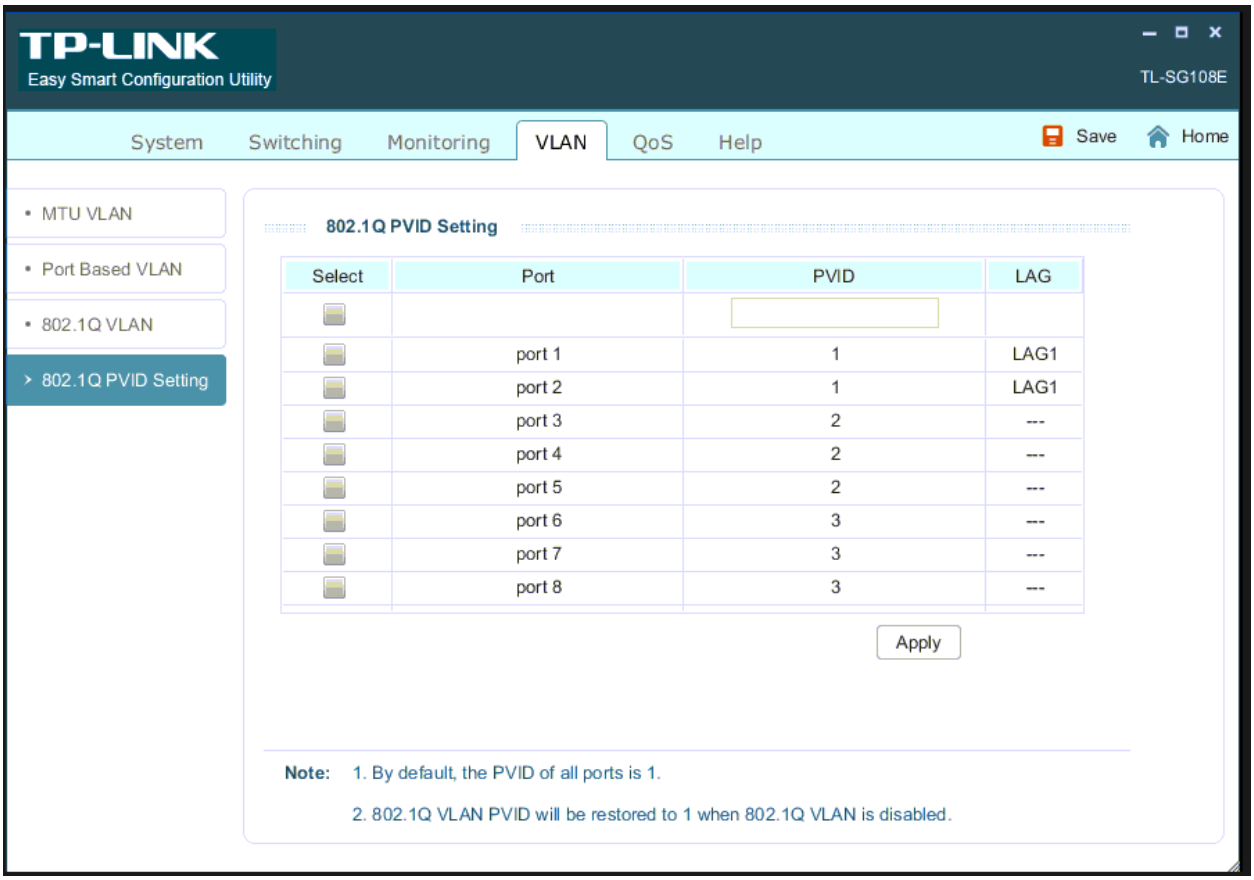
☐ Invert match. any Destination Address /


TP-LINK
Easy Smart Configuration Utility
Discovered Switches
Product
Device Description
MAC Address
IP Address
Located on IP Network
IP Setting
Login
TL-SG108E
TL-SG108E
A4-2B-B0-D0-CA-6B
192.168.10.2
192.168.10.100
Help
Refresh

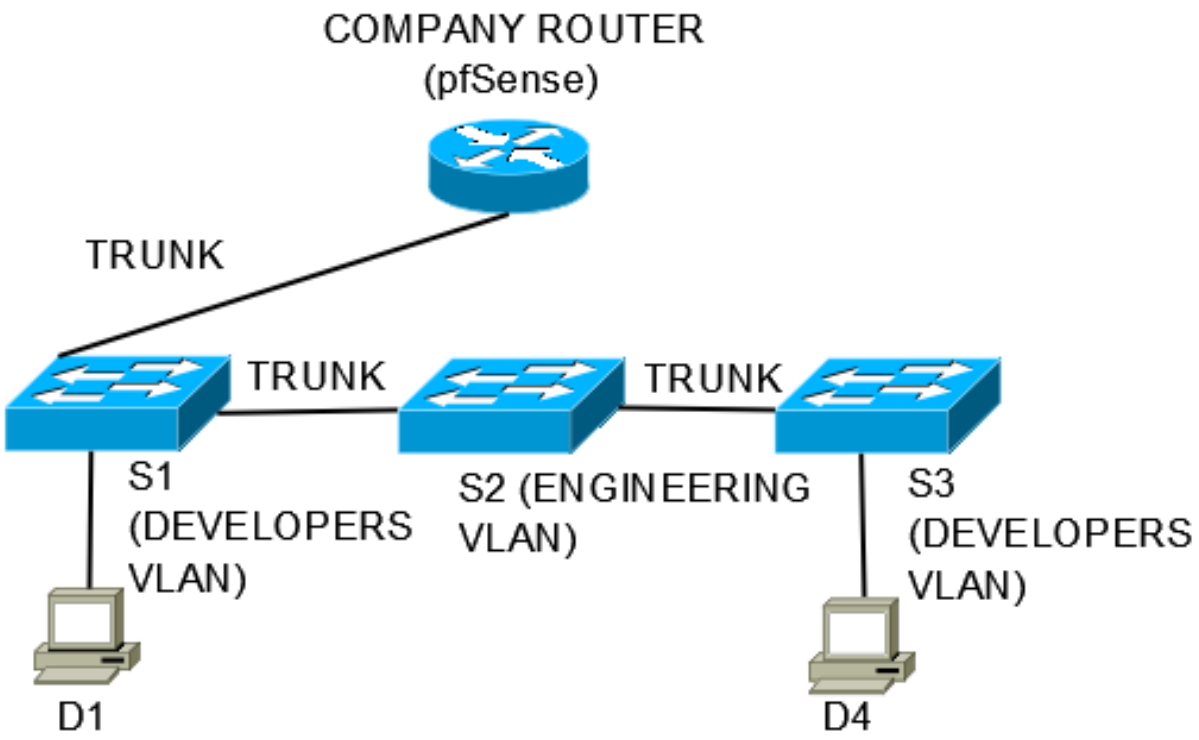

TP-LINK
Easy Smart Configuration Utility
TL-SG108E
System
Switching
Monitoring
VLAN
QoS
Help
Save
Home
Port Setting
IGMP Snooping
Port Trunk
Trunk Config
Trunk ID:
Trunk1
1 2 3 4 5 6 7 8
Apply
Trunk Table
Select
Trunk ID
Ports
Trunk1
1,2
Trunk2

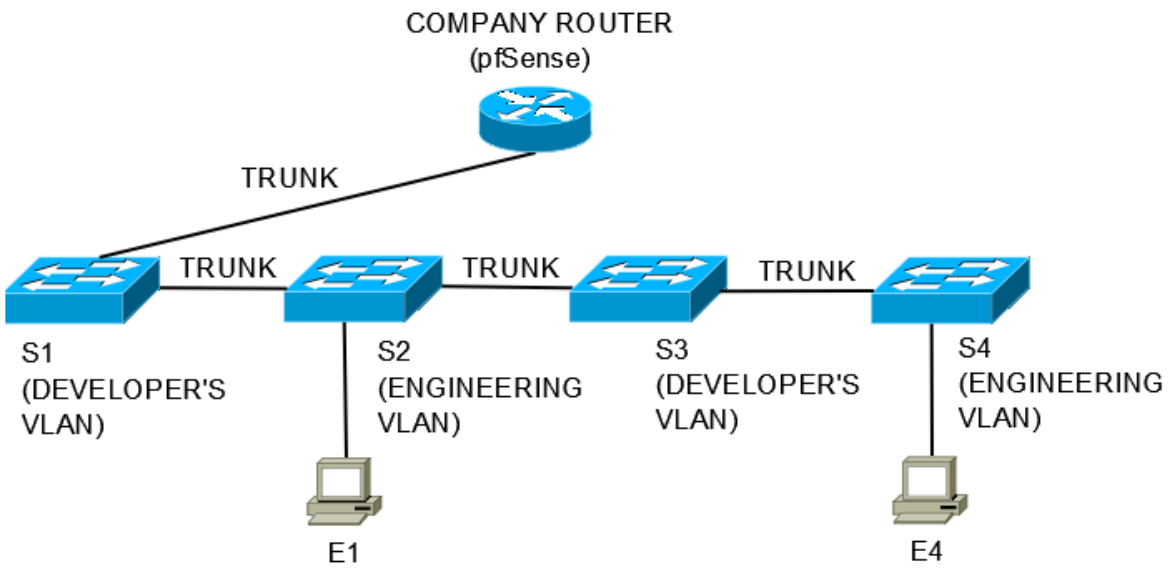
SelectAll
Delete
Note: 1. You can create up to two trunk groups.
2. Each trunk group has up to four port members and has at least two port members.
3. Mirroring and mirrored port cannot be added to a trunk group.


TP-LINK
Easy Smart Configuration Utility
TL-SG108E
System
Switching
Monitoring
VLAN
QoS
Help
Save
Home
MTU VLAN
Port Based VLAN
802.1Q VLAN
802.1Q PVID Setting
Global Config
802.1Q VLAN Status:
Enable
Apply
802.1Q VLAN Setting
VLAN (1-4094):
3
VLAN Name:
ENGINEERNG
Tagged Ports:
1 2 3 4 5 6 7 8
Untagged Ports:
1 2 3 4 5 6 7 8
Apply
VLAN | VLAN Name | Member Ports | Tagged Ports | Untagged Ports | Delete VLAN
1 | Default_VLAN | 1-8 | | 1-8 |
2 | DEVELOPERS | 1-5 | 1-2 | 3-5 | Delete
3 | ENGINEERNG | 1-2, 6-8 | 1-2 | 6-8 | Delete


TP-LINK
Easy Smart Configuration Utility
TL-SG108E
System
Switching
Monitoring
VLAN
QoS
Help
Save
Home
MTU VLAN
Port Based VLAN
802.1Q VLAN
802.1Q PVID Setting
802.1Q PVID Setting
Select
Port
PVID
LAG
port 1
1
LAG1
port 2
1
LAG1
port 3
2
---
port 4
2
---
port 5
2
---
port 6
3
---
port 7
3
---
port 8
3

Apply
Note: 1. By default, the PVID of all ports is 1.
2. 802.1Q VLAN PVID will be restored to 1 when 802.1Q VLAN is disabled.


COMPANY ROUTER
(pfSense)
TRUNK
TRUNK
TRUNK
S1
(DEVELOPERS
VLAN)
S2 (ENGINEERING
VLAN)
S3
(DEVELOPERS
VLAN)
D1
D4



192.168.20.100 - PuTTY

```
SW1# ping 172.16.1.101
Sending 5, 100-byte ICMP echoes to 172.16.1.101, timeout is 2 sec:
!!!!!
Success rate is 100 percent
SW1#
```

192.168.20.100 - PuTTY

```
SW1# ping 172.16.1.104
Sending 5, 100-byte ICMP echoes to 172.16.1.104, timeout is 2 sec:
.....
Success rate is 0 percent
SW1#
```

192.168.20.100 - PuTTY

```
SW3# ping 172.16.1.104
Sending 5, 100-byte ICMP echoes to 172.16.1.104, timeout is 2 sec:
!!!!!
Success rate is 100 percent
SW3#
```

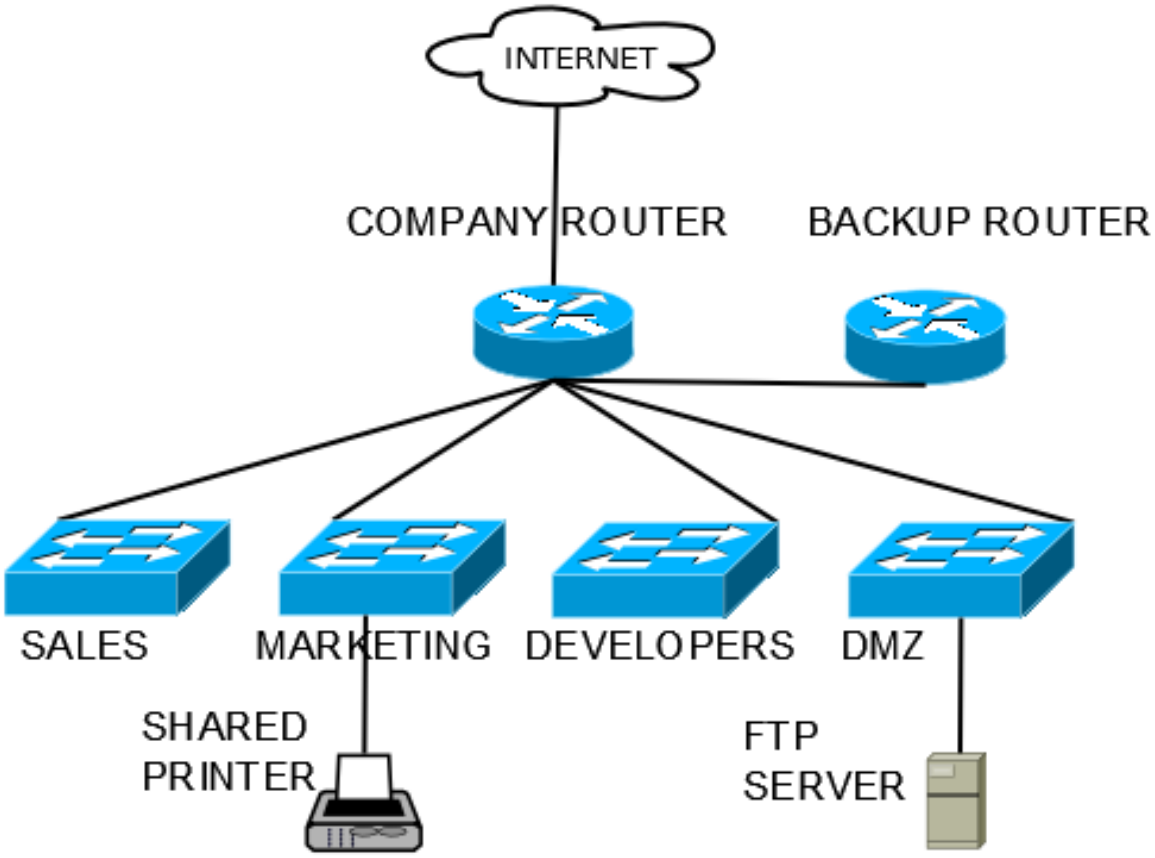
192.168.20.100 - PuTTY

```
SW3# ping 172.17.1.1
Sending 5, 100-byte ICMP echoes to 172.17.1.1, timeout is 2 sec:
.....
Success rate is 0 percent
SW3#
```

192.168.20.100 - PuTTY

```
SW1# ping 172.17.1.1
Sending 5, 100-byte ICMP echoes to 172.17.1.1, timeout is 2 sec:
.....
Success rate is 0 percent
SW1#
```

Chapter 4: pfSense as a Firewall



Firewall / Rules / Edit

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface DEVELOPERS

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to

Protocol TCP

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match. DEVELOPERS net | Source Address /

Show advanced Show advanced

Destination

Destination ☐ Invert match. WAN address | Destination Address /

Destination port range any (From) | Custom | any (To) | Custom

Firewall / Rules / Floating / Edit

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Quick ☐ Apply the action immediately on match.

Set this option if you need to apply this action to traffic that matches this rule immediately.

Interface SuperSecret, WAN, DMZ, DEVELOPERS

Choose the interface(s) for this rule.

Direction any

Floating

Address Family IPv4

Select the Internet Protocol version this rule applies to

Protocol TCP

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match. any | Source Address /

Schedule Information

Schedule Name LUNCH_TIME

This schedule is in use so the name may not be modified!

Description Lunch time rule

You may enter a description here for your reference (not parsed).

Month March_16

Date

March_2016						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

Time

12	00	13	00
Start Hrs	Start Mins	Stop Hrs	Stop Mins

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

Time range description Lunch time

You may enter a description here for your reference (not parsed).

Add Time Clear selection

Firewall / NAT / Outbound

Port Forward 1:1 Outbound NPt

General Logging Options

Mode

- (●) Automatic outbound NAT rule generation. (IPsec passthrough included)
- ( ) Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- ( ) Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- ( ) Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
	WAN	127.0.0.0/8	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP - localhost to WAN	
	WAN	127.0.0.0/8	*	*	*	WAN address	*	NO	Auto created rule - localhost to WAN	
	WAN	172.16.0.0/16	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP - LAN to WAN	
	WAN	172.16.0.0/16	*	*	*	WAN address	*	NO	Auto created rule - LAN to WAN	
	WAN	172.17.0.0/16	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP - DEVELOPERS to WAN	
	WAN	172.17.0.0/16	*	*	*	WAN	*	NO	Auto created rule - DEVELOPERS to WAN	

pfSense System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Firewall / Aliases / Edit

Properties

Name SLASHDOT

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description Alias for slashdot.org

You may enter a description here for your reference (not parsed).

Type Host(s)

Host(s)

Hint Enter as many hosts as you would like. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. You may also enter an IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 and a list of individual IP addresses will be generated.

IP or FQDN 216.34.181.45 / 32 slashdot IP address

Save Add Host

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface WAN

Address type Single address

Address(es) 10.0.2.100 / 8

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password ●●●●●●●●●●●● Virtual IP Password

Enter the VHID group password. Confirm

VHID Group 1

Enter the VHID group that the machines will share

Advertising frequency 1 Base 0 Skew

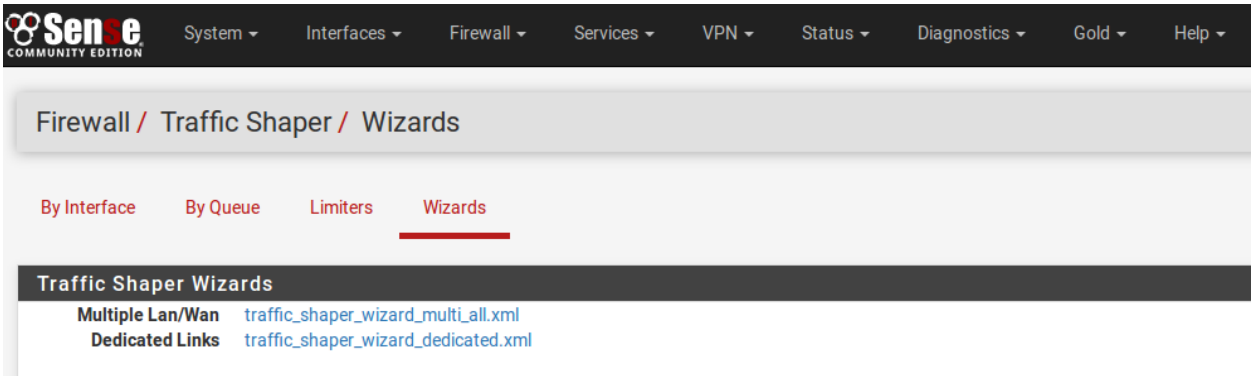
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

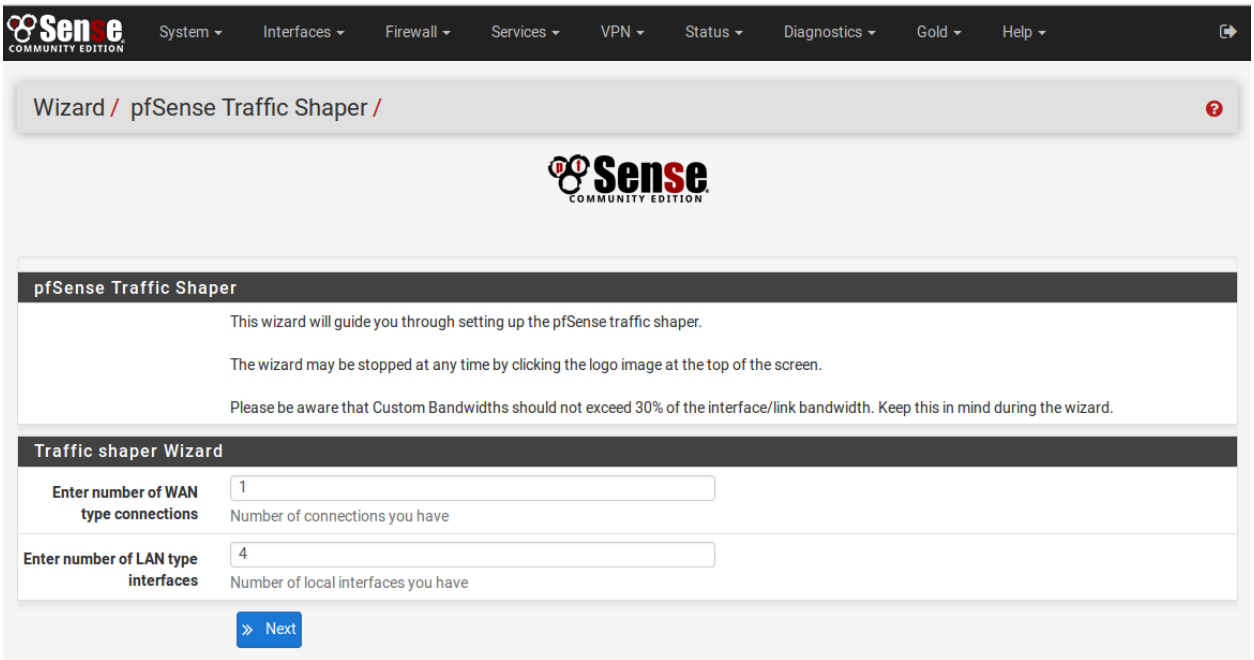
Description Firewall CARP VIP

You may enter a description here for your reference (not parsed).

Save

Chapter 5: Traffic Shaping





pfSense COMMUNITY EDITION

Voice over IP

Voice over IP

enable ☒ Prioritize Voice over IP traffic.

VOIP specific settings

Provider Generic (lowdelay)

Choose Generic if your provider isn't listed.

Upstream SIP Server

(Optional) If this is chosen, the provider field will be overridden. This allows you to provide the IP address of the **remote** PBX or SIP Trunk to prioritize. NOTE: You can also use a Firewall Alias in this location.

Connection WAN #1

Upload 1

Units Mbit/s

Connection LAN #1

Download 500

Units Kbit/s

pfSense COMMUNITY EDITION

Peer to Peer networking

Peer to Peer networking

Enable ☒ Lower priority of Peer-to-Peer traffic

This will lower the priority of P2P traffic below all other traffic. Please check the items that you would like to prioritize lower than normal traffic.

p2p Catch all

p2pCatchAll ☒ When enabled, all uncategorized traffic is fed to the p2p queue.

Bandwidth 10

Bandwidth %

The limit you want to apply.

Enable/Disable specific P2P protocols

Aimster ☐ Aimster and other P2P using the Aimster protocol and ports

BitTorrent ☒ Bittorrent and other P2P using the Torrent protocol and ports

BuddyShare ☐ BuddyShare and other P2P using the BuddyShare protocol and ports

CuteMX ☐ CuteMX and other P2P using the CuteMX protocol and ports

DCplusplus ☐ DC++ and other P2P using the DC++ protocol and ports

DCC ☒ irc DCC file transfers

DirectConnect ☐ DirectConnect and other P2P using the DirectConnect protocol and ports

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Wizard / pfSense Traffic Shaper / Reload Profile

Reload Profile

After pressing Finish the system will load the new profile.
Please note that this may take a moment.
Also note that the traffic shaper is stateful meaning that only new connections will be shaped.
If this is an issue please reset the state table after loading the profile.

» Finish

Shaper configuration

Shaper configuration

Connection #1 parameters

Local interface	DMZ
Local interface	CBQ
WAN Interface	WAN
WAN Interface	CBQ
Upload	50
Upload	Mbit/s
Download	
Download	Mbit/s

» Next

Firewall / Traffic Shaper / By Interface

By Interface | By Queue | Limiters | Wizards

- WAN
  - qInternet
    - qACK
    - qOthersDefault
    - qP2P
    - qVoIP
    - qGames
    - qOthersHigh
    - qOthersLow
- DMZ
  - qInternet
    - qACK
    - qP2P
    - qVoIP
    - qGames
    - qOthersHigh
    - qOthersLow
- DEVELOPERS
  - qInternet
    - qACK
    - qP2P
    - qVoIP
    - qGames
    - qOthersHigh
    - qOthersLow
- ENGINEERING
  - qInternet
    - qACK

Enable/Disable ☒ Enable/disable discipline and its children

Name qOthersHigh

Enter the name of the queue here. Do not use spaces and limit the size to 15 characters.

Priority 4

For hfsc, the range is 0 to 7. The default is 1. Hfsc queues with a higher priority are preferred in the case of overload.

Queue Limit

Queue limit in packets.

Scheduler options ☐ Default Queue ☐ Random Early Detection ☐ Random Early Detection In and Out ☒ Explicit Congestion Notification ☐ Codel Active Queue

Select options for this queue

Description

Service Curve (sc)

Bandwidth 8.997 %

Choose the amount of bandwidth for this queue

Max bandwidth for queue. ☐ Upper Limit

m1 d m2

Firewall / Traffic Shaper / Limiters

By Interface | By Queue | Limiters | Wizards

- qDOWNLOAD
  - qDLDEV
  - qDLENG
- qUPLOAD
  - qULDEV
  - qULENG

New Limiter

Limiters

Enable ☒ Enable limiter and its children

Name qDOWNLOAD

Bandwidth

Bandwidth	Bw type	Schedule	
100	Mbit/s	none	Delete

Add Schedule

Mask None

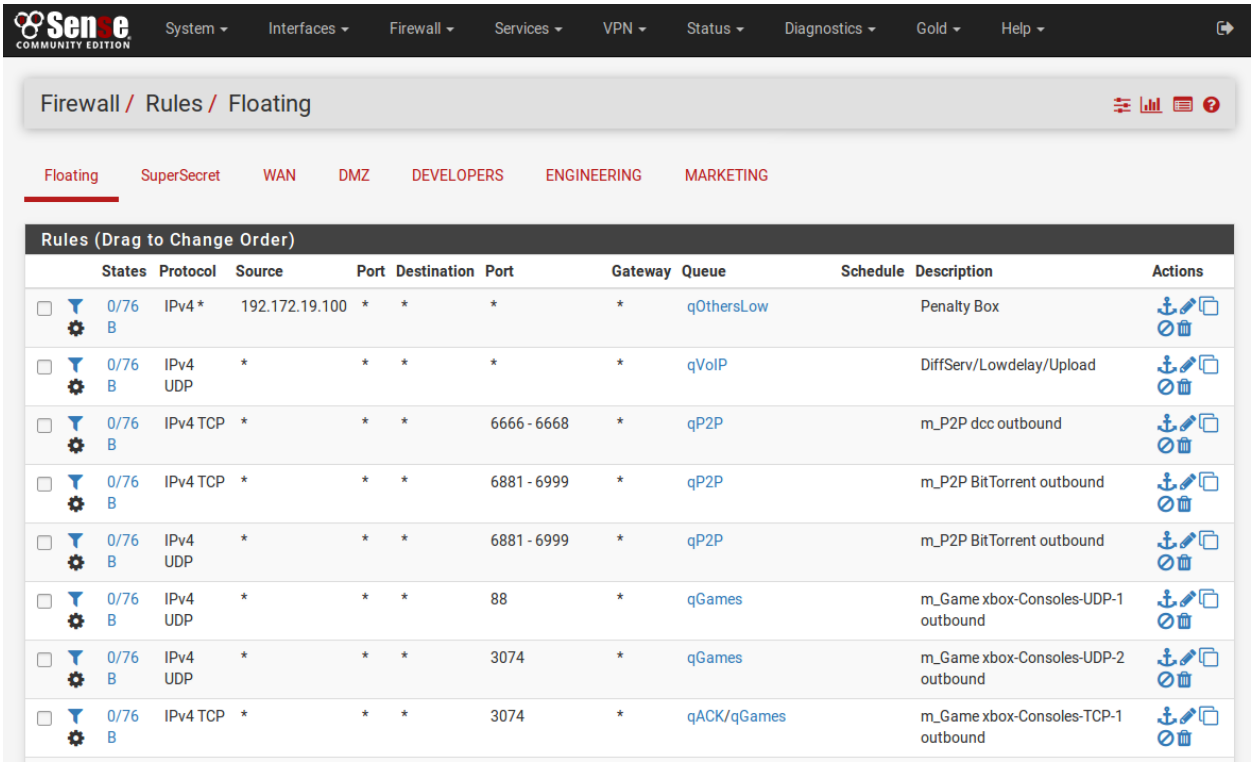
If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host.

32 — IPV4 mask bits 255.255.255.255/?

128 — IPV6 mask bits ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/?

Description Download queue for DEVELOPERS/ENGINEERING

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



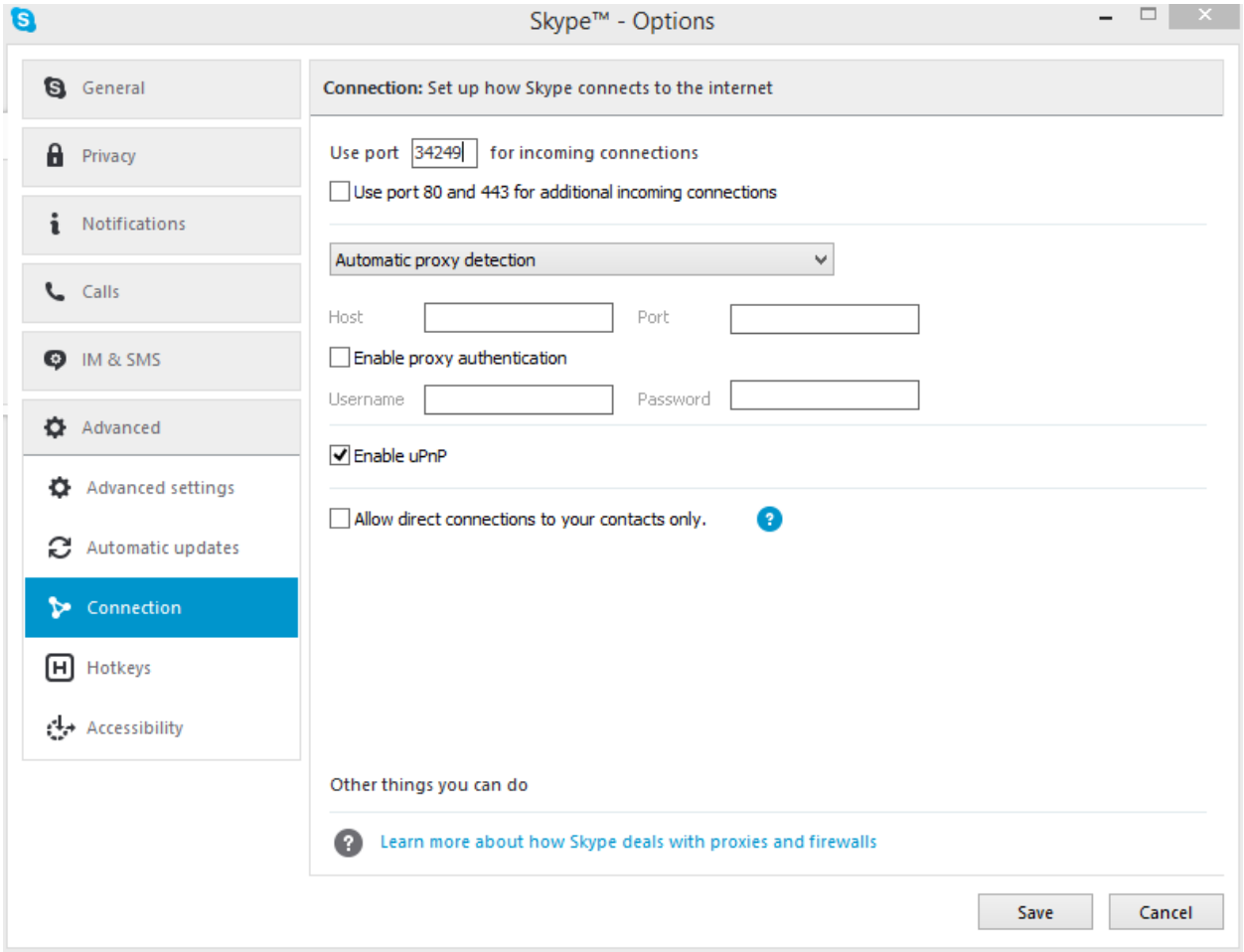
pfSense COMMUNITY EDITION | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Gold | Help

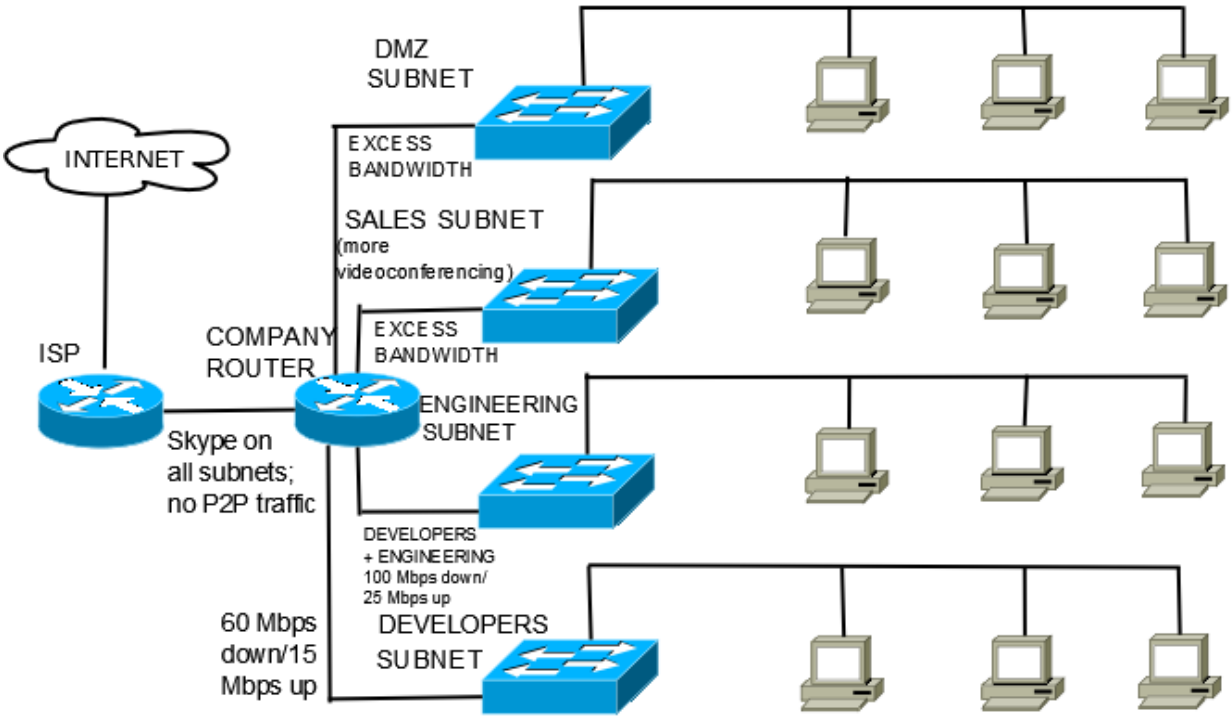
Firewall / Rules / Floating

Floating | SuperSecret | WAN | DMZ | DEVELOPERS | ENGINEERING | MARKETING

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0/76 B	IPv4 *	192.172.19.100	*	*	*	*	qOthersLow		Penalty Box	
	0/76 B	IPv4 UDP	*	*	*	*	*	qVoIP		DiffServ/Lowdelay/Upload	
	0/76 B	IPv4 TCP	*	*	*	6666 - 6668	*	qP2P		m_P2P dcc outbound	
	0/76 B	IPv4 TCP	*	*	*	6881 - 6999	*	qP2P		m_P2P BitTorrent outbound	
	0/76 B	IPv4 UDP	*	*	*	6881 - 6999	*	qP2P		m_P2P BitTorrent outbound	
	0/76 B	IPv4 UDP	*	*	*	88	*	qGames		m_Game xbox-Consoles-UDP-1 outbound	
	0/76 B	IPv4 UDP	*	*	*	3074	*	qGames		m_Game xbox-Consoles-UDP-2 outbound	
	0/76 B	IPv4 TCP	*	*	*	3074	*	qACK/qGames		m_Game xbox-Consoles-TCP-1 outbound	


Skype™ - Options
General
Privacy
Notifications
Calls
IM & SMS
Advanced
Advanced settings
Automatic updates
Connection
Hotkeys
Accessibility
Connection: Set up how Skype connects to the internet
Use port 34249 for incoming connections
Use port 80 and 443 for additional incoming connections
Automatic proxy detection
Host
Port
Enable proxy authentication
Username
Password
Enable uPnP
Allow direct connections to your contacts only.
Other things you can do
Learn more about how Skype deals with proxies and firewalls
Save
Cancel


DMZ
SUBNET
INTERNET
EXCESS
BANDWIDTH
SALES SUBNET
(more
videoconferencing)
ISP
COMPANY
ROUTER
EXCESS
BANDWIDTH
ENGINEERING
SUBNET
Skype on
all subnets;
no P2P traffic
DEVELOPERS
+ ENGINEERING
100 Mbps down/
25 Mbps up
60 Mbps
down/15
Mbps up
DEVELOPERS
SUBNET

Chapter 6: Virtual Private Networks

VPN / IPsec / Tunnels / Edit Phase 1

Tunnels | Mobile Clients | Pre-Shared Keys | Advanced Settings

General Information

Disabled	☐ Set this option to disable this phase1 without removing it from the list.
Key Exchange version	V1 Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.
Internet Protocol	IPv4 Select the Internet Protocol family.
Interface	WAN Select the interface for the local endpoint of this phase1 entry.
Remote Gateway	ipsectest.duckdns.org Enter the public IP address or host name of the remote gateway
Description	IPsec test tunnel A description may be entered here for administrative reference (not parsed).

Phase 1 Proposal (Authentication)

Authentication Method	Mutual PSK Must match the setting chosen on the remote side.
Negotiation mode	Main Aggressive is more flexible, but less secure.
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	Enter the Pre-Shared Key string.

VPN / IPsec / Tunnels / Edit Phase 2

Tunnels | Mobile Clients | Pre-Shared Keys | Advanced Settings

General Information

Disabled	☐ Disable this phase 2 entry without removing it from the list.	
Mode	Tunnel IPv4	
Local Network	Network Type	192.168.2.0 / 24 Address
NAT/BINAT translation	None Type If NAT/BINAT is required on this network specify the address to be translated	/ 0 Address
Remote Network	Network Type	192.168.40.0 / 24 Address
Description	IPsec test tunnel - phase 2 A description may be entered here for administrative reference (not parsed).	

Phase 2 Proposal (SA/Key Exchange)

Protocol	ESP ESP is encryption, AH is authentication only.	
Encryption Algorithms	☑ AES	256 bits
	☐ AES128-GCM	Auto
	☐ AES192-GCM	Auto
	☐ AES256-GCM	Auto
	☐ Blowfish	Auto

VPN / IPsec / Mobile Clients

Tunnels | Mobile Clients | Pre-Shared Keys | Advanced Settings

Enable IPsec Mobile Client Support

IKE Extensions	☑ Enable IPsec Mobile Client Support

Extended Authentication (Xauth)

User Authentication	Local Database Source
Group Authentication	system Source

Client Configuration (mode-cfg)

Virtual Address Pool	☑ Provide a virtual IP address to clients
	192.168.2.40 / 24 Network configuration for Virtual Address Pool
Virtual IPv6 Address Pool	☐ Provide a virtual IPv6 address to clients
Network List	☐ Provide a list of accessible networks to clients
Save Xauth Password	☑ Allow clients to save Xauth passwords (Cisco VPN client only). NOTE: With iPhone clients, this does not work when deployed via the iPhone configuration utility, only by manual entry.
DNS Default Domain	☑ Provide a default domain name to clients
	localdomain Specify domain as DNS Default Domain
Split DNS	☐ Provide a list of split DNS domain names to clients. Enter a space separated list.

VPN / IPsec / Mobile Clients

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Support for IPsec Mobile Clients is enabled but a Phase 1 definition was not found.
Please click Create to define one.

Create Phase 1

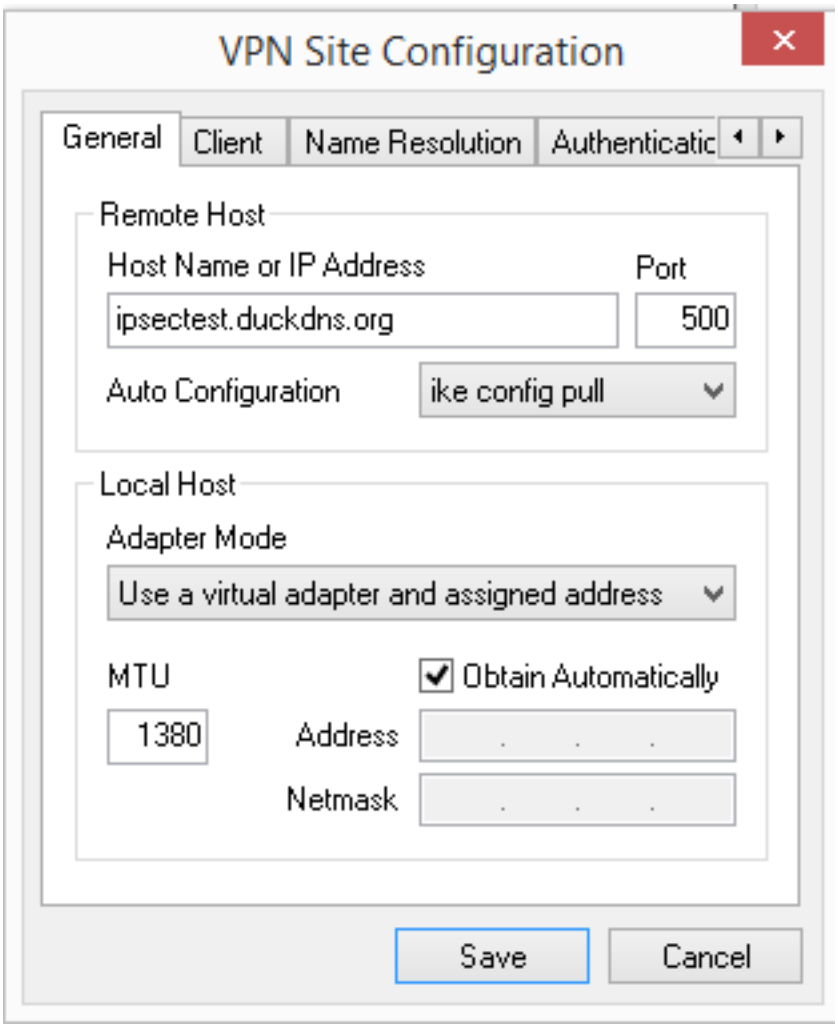
Tunnels | Mobile Clients | Pre-Shared Keys | Advanced Settings

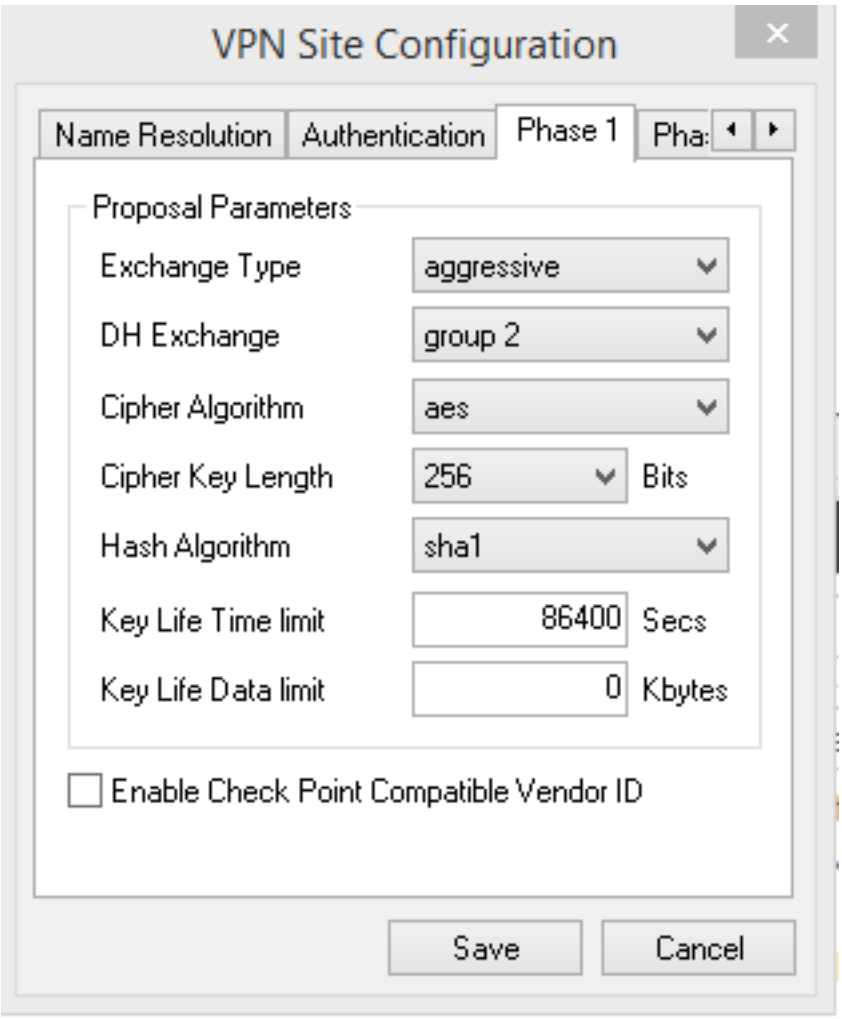
Enable IPsec Mobile Client Support

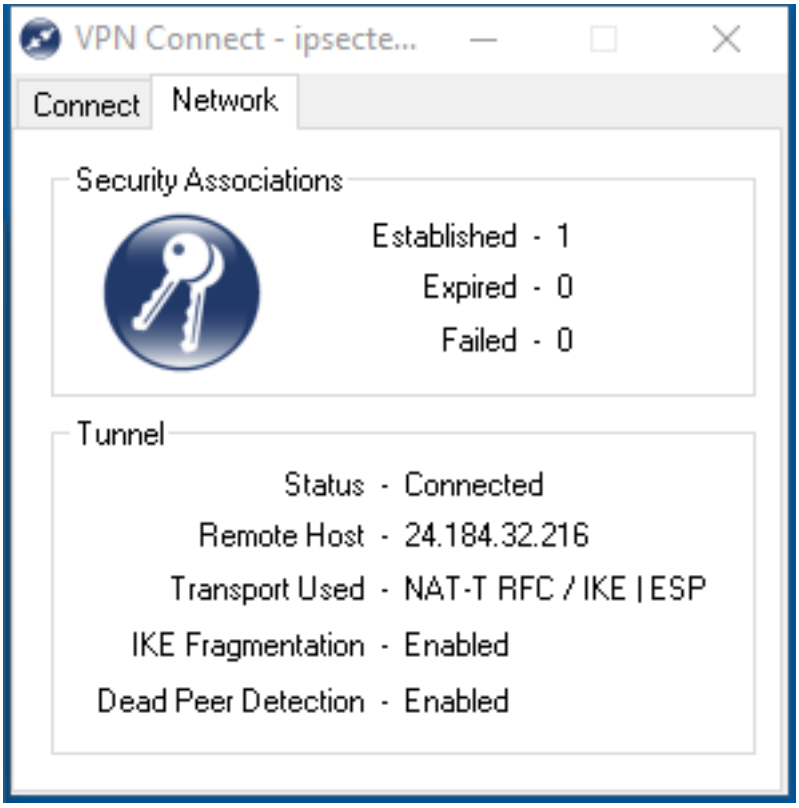
IKE Extensions	☑ Enable IPsec Mobile Client Support

Extended Authentication (Xauth)

User Authentication	Local Database Source
Group Authentication	system Source


VPN Site Configuration
General
Client
Name Resolution
Authenticatic
Remote Host
Host Name or IP Address
Port
ipsectest.duckdns.org
500
Auto Configuration
ike config pull
Local Host
Adapter Mode
Use a virtual adapter and assigned address
MTU
Obtain Automatically
1380
Address
Netmask
Save
Cancel


VPN Site Configuration
Name Resolution
Authentication
Phase 1
Pha:
Proposal Parameters
Exchange Type
aggressive
DH Exchange
group 2
Cipher Algorithm
aes
Cipher Key Length
256
Bits
Hash Algorithm
sha1
Key Life Time limit
86400
Secs
Key Life Data limit
0
Kbytes
Enable Check Point Compatible Vendor ID
Save
Cancel


VPN Connect - ipsecte...
Connect
Network
Security Associations
Established - 1
Expired - 0
Failed - 0
Tunnel
Status - Connected
Remote Host - 24.184.32.216
Transport Used - NAT-T RFC / IKE | ESP
IKE Fragmentation - Enabled
Dead Peer Detection - Enabled

VPN / L2TP / Configuration

Configuration | Users

Enable L2TP

Enable [x] Enable LT2P server

Configuration

Interface WAN

Server address 192.168.5.254

Enter the IP address the L2TP server should give to clients for use as their "gateway". Typically this is set to an unused IP just outside of the client range.

NOTE: This should NOT be set to any IP address currently in use on this firewall.

Remote address range 192.168.5.0 / 24

Specify the starting address for the client IP address subnet.

Number of L2TP users 25

Secret ••••••• ••••••• Confirm

Specify optional secret shared between peers. Required on some devices/setups.

Authentication type CHAP

Specifies the protocol to use for authentication.

Primary L2TM DNS server 8.8.8.8

Secondary L2TM DNS server 8.8.4.4

RADIUS

Enable [ ] Use a RADIUS server for authentication

VPN / OpenVPN / Servers / Edit

Servers | Clients | Client Specific Overrides | Wizards | Client Export | Shared Key Export

General Information

Disabled	☐ Disable this server Set this option to disable this server without removing it from the list
Server mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	Local Database
Protocol	UDP
Device mode	tun
Interface	WAN
Local port	1194
Description	Remote VPN Access A description may be entered here for administrative reference (not parsed).

Cryptographic Settings

TLS authentication	☑ Enable authentication of TLS packets.
Key	# # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 19ce3bbab880419525e84128ec120b06 Paste the shared key here
Peer Certificate Authority	OpenVPN certificate
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager

OpenVPN / Client Export Utility

Server | Client | Client Specific Overrides | Wizards | Client Export | Shared Key Export

OpenVPN Server

Remote Access Server: Remote VPN Access UDP:1194

Client Connection Behavior

Host Name Resolution: Interface IP Address

Verify Server CN: Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible

Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting.

Only use tls-remote if an older client must be used. The option has been deprecated by OpenVPN and will be removed in the next major version.

With tls-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain clients cannot parse the server CN. Some clients have problems parsing the CN with quotes. Use only as needed.

Use Random Local Port: ☑ Use a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently.

Certificate Export Options

Microsoft Certificate Storage: ☐ Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate: ☐ Use a password to protect the pkcs12 file contents or key in Viscosity bundle.

Proxy Options

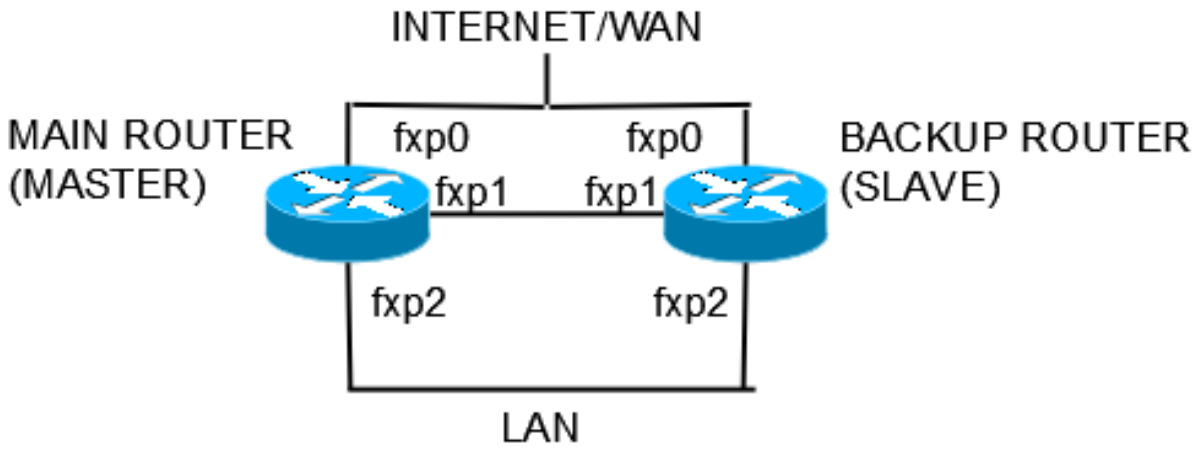
Use A Proxy: ☐ Use proxy to communicate with the OpenVPN server.

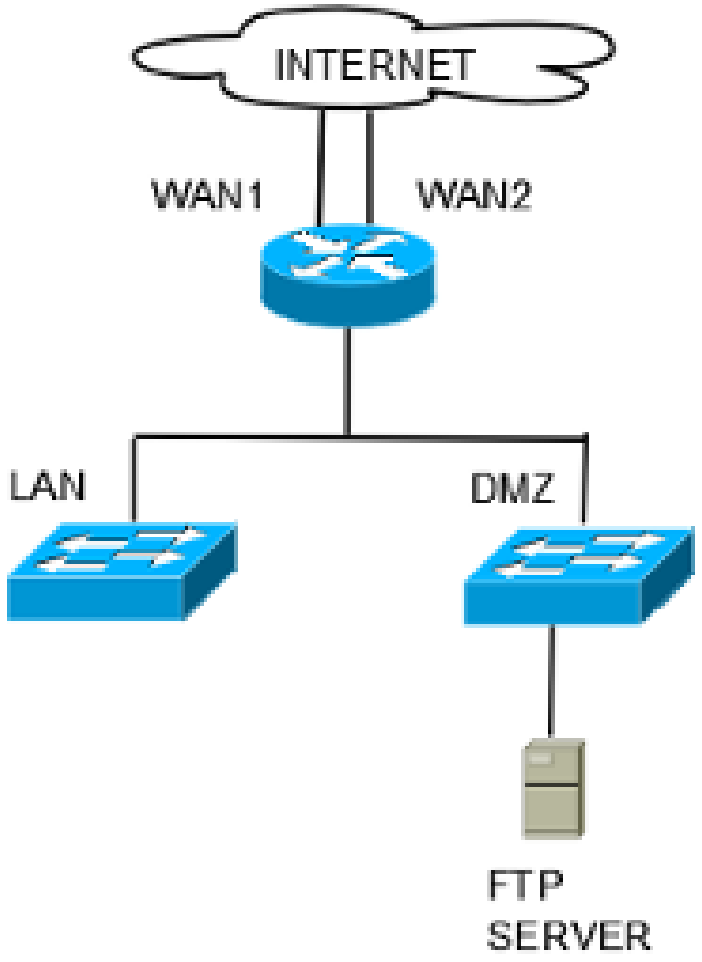
Management Interface

Management Interface: ☐ Use the OpenVPNManager Management Interface.

This will activate management interface in the generated .ovpn configuration and include the OpenVPNManager program in the Windows Installers.

Chapter 7: Redundancy and High Availability





New Gateway

Default	☐ Default gateway
Gateway name	WAN2GW
Gateway IPv4	10.1.1.1
Description	Gateway for WAN2

+ Add Cancel

System / Routing / Gateway Groups / Edit

Edit Gateway Group Entry

Group Name	MULTIWAN
Gateway Priority	

Gateway	Tier	Virtual IP	Description
WAN_DHCP	Tier 1	Interface Address	Interface WAN_DHCP Gateway
WAN2_DHCP	Tier 1	Interface Address	Interface WAN2_DHCP Gateway

Link Priority	The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.
Virtual IP	The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.
Trigger Level	Member down When to trigger exclusion of a member
Description	Gateway group for multi-WAN A description may be entered here for administrative reference (not parsed).

Save

Gateway Monitoring

State Killing on Gateway Failure	☐ Flush all states when a gateway goes down The monitoring process will flush all states when a gateway goes down if this box is checked.
Skip rules when gateway is down	☐ Do not create rules when gateway is down By default, when a rule has a gateway specified and this gateway is down, the rule is created omitting the gateway. This option overrides that behavior by omitting the entire rule instead.

Services / Load Balancer / Pools / Edit

Add/Edit Load Balancer - Pool Entry

Name	WEBPOOL
Mode	Load Balance
Description	Web server load balancing pool
Port	80 This is the port the servers are listening on. A port alias listed in Firewall -> Aliases may also be specified here.
Retry	1 Optionally specify how many times to retry checking a server before declaring it down.

Add Item to the Pool

Monitor	ICMP	
Server IP Address	IP Address	Add to pool

Current Pool Members

Members		172.16.1.10 172.16.1.11 172.16.1.12 172.16.1.13
	Disabled	Enabled (Default)
	Remove	Remove
	Move to enabled list	Move to disabled list

Status / Load Balancer / Pools

Pools | Virtual Servers

Load Balancer Pools

Name	Mode	Servers	Monitor	Description
WEBPOOL	Load balancing	172.16.1.10:80 (100.00%) 172.16.1.11:80 (0.00%) 172.16.1.12:80 (0.00%) 172.16.1.13:80 (0.00%)	ICMP	Web server load balancing pool

Save Reset

Status / CARP

Temporarily Disable CARP | Enter Persistent CARP Maintenance Mode

CARP Interfaces

CARP Interface	Virtual IP	Status
WAN1@1	10.0.2.1/24	MASTER
LAN@2	172.16.1.10/24	MASTER

pfSync Nodes

- 388bc6c4
- 6562a1ee
- c87ed532

Translation

Address Host Alias: DUALWAN (Alias with both virtual WAN IPs)

Pool options Default

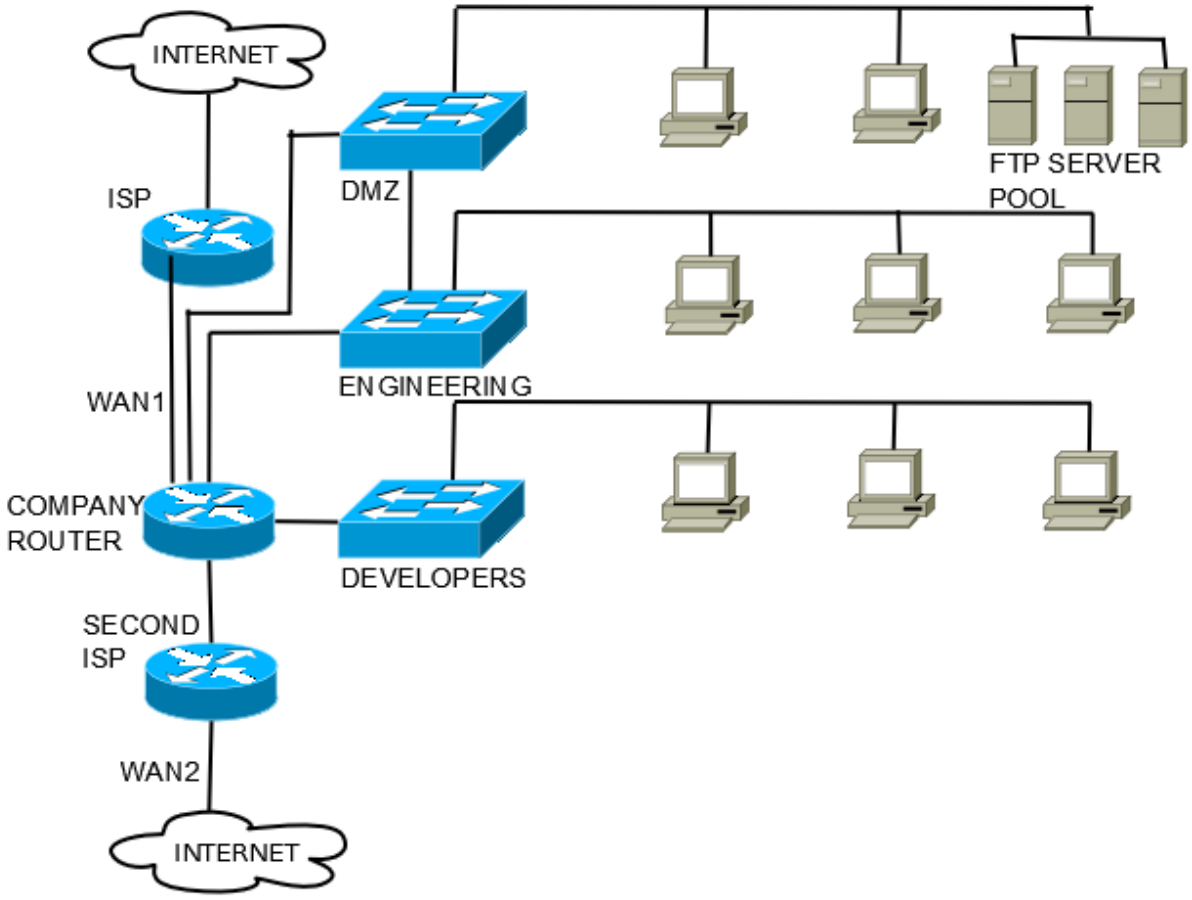
Only Round Robin types work with Host Aliases. Any type can be used with a Subnet.

- Round Robin: Loops through the translation addresses.
- Random: Selects an address from the translation address pool at random.
- Source Hash: Uses a hash of the source address to determine the translation address, ensuring that the redirection address is always the same for a given source.
- Bitmask: Applies the subnet mask and keeps the last portion identical; 10.0.1.50 -> x.x.x.50.
- Sticky Address: The Sticky Address option can be used with the Random and Round Robin pool types to ensure that a particular source address is always mapped to the same translation address.

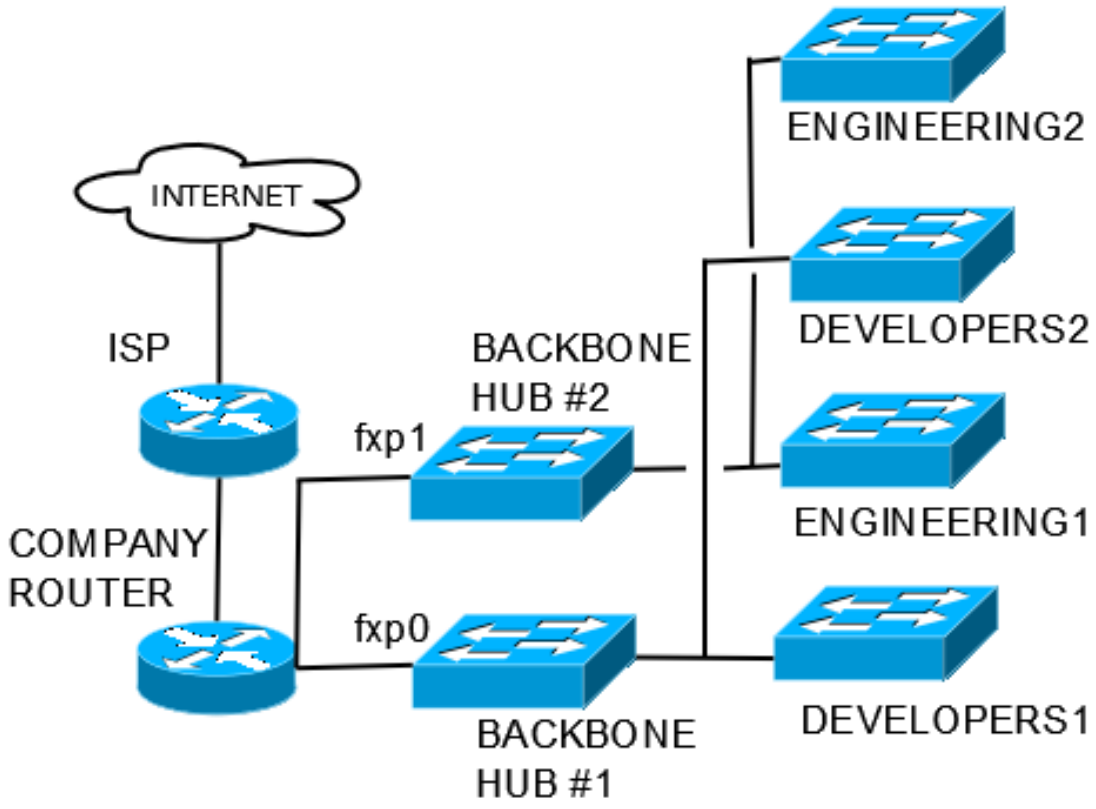
Port Static port

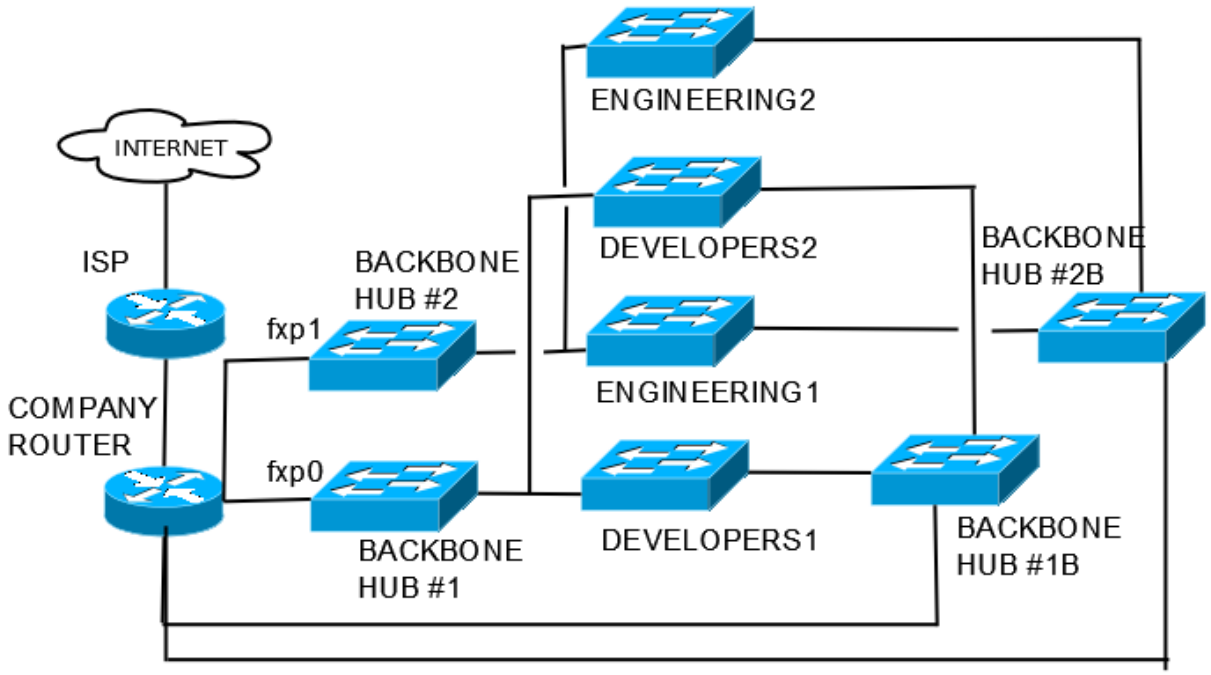
Enter the source port or range for the outbound NAT mapping.

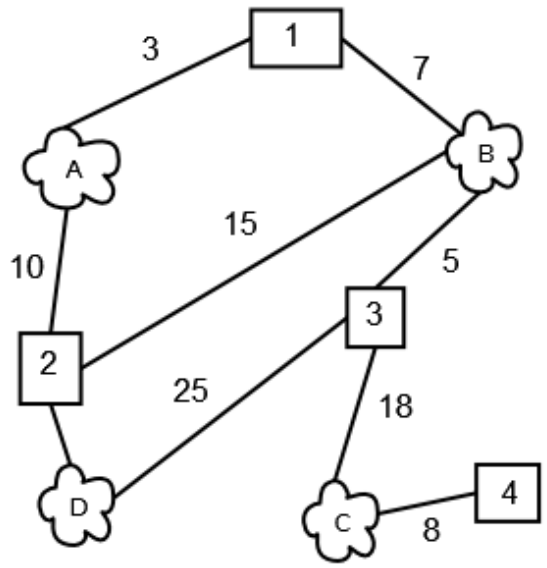
May 23 20:40:31	check_reload_status: Syncing firewall
May 23 20:40:33	php-fpm[42315]: /rc.filter_synchronize: Beginning XMLRPC sync to http://192.168.4.4:80.
May 23 20:40:40	php-fpm[42315]: /rc.filter_synchronize: XMLRPC sync successfully completed with http://192.168.4.4:80.
May 23 20:40:41	check_reload_status: Syncing firewall
May 23 20:40:42	php-fpm[20136]: /system_hasync.php: waiting for pfsync...
May 23 20:41:14	php-fpm[20136]: /system_hasync.php: pfsync done in 30 seconds.
May 23 20:41:14	php-fpm[20136]: /system_hasync.php: Configuring CARP settings finalize...

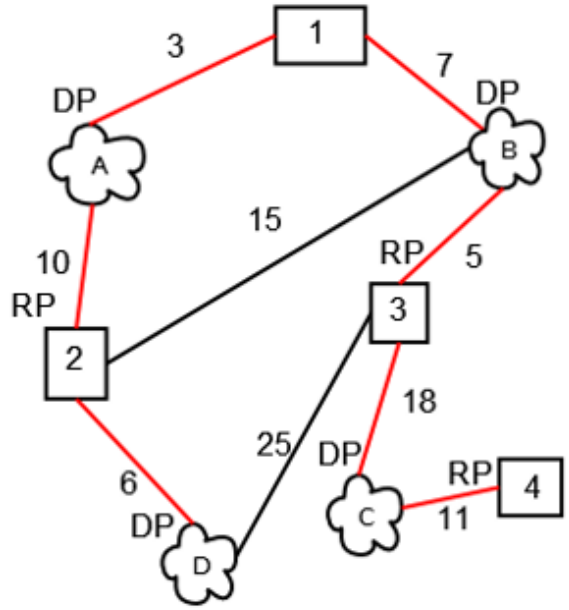

INTERNET
ISP
DMZ
FTP SERVER
POOL
ENGINEERING
WAN1
COMPANY
ROUTER
DEVELOPERS
SECOND
ISP
WAN2
INTERNET

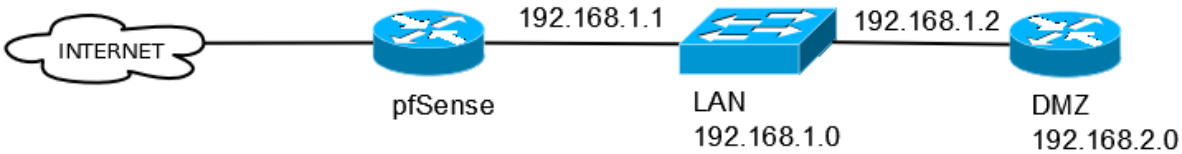
Chapter 8: Routing and Bridging

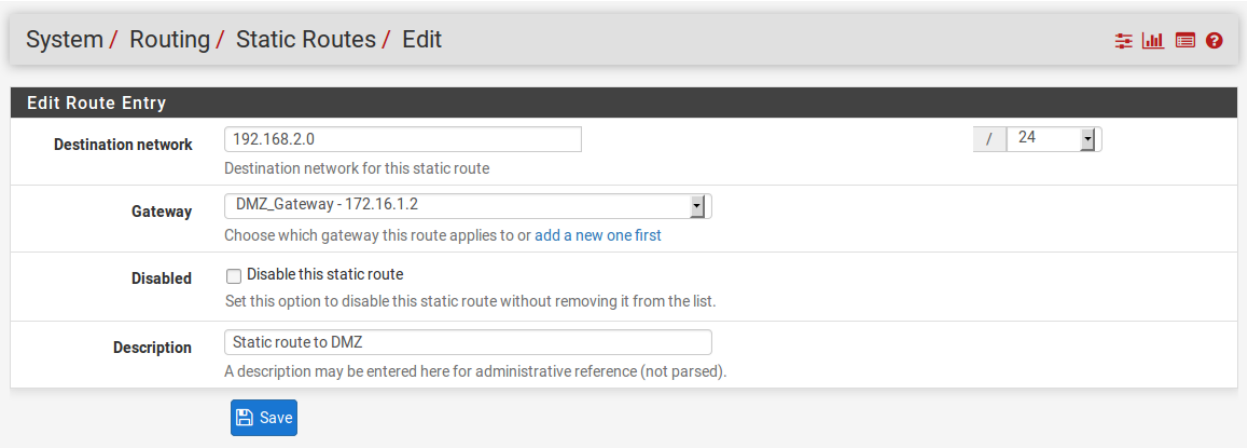


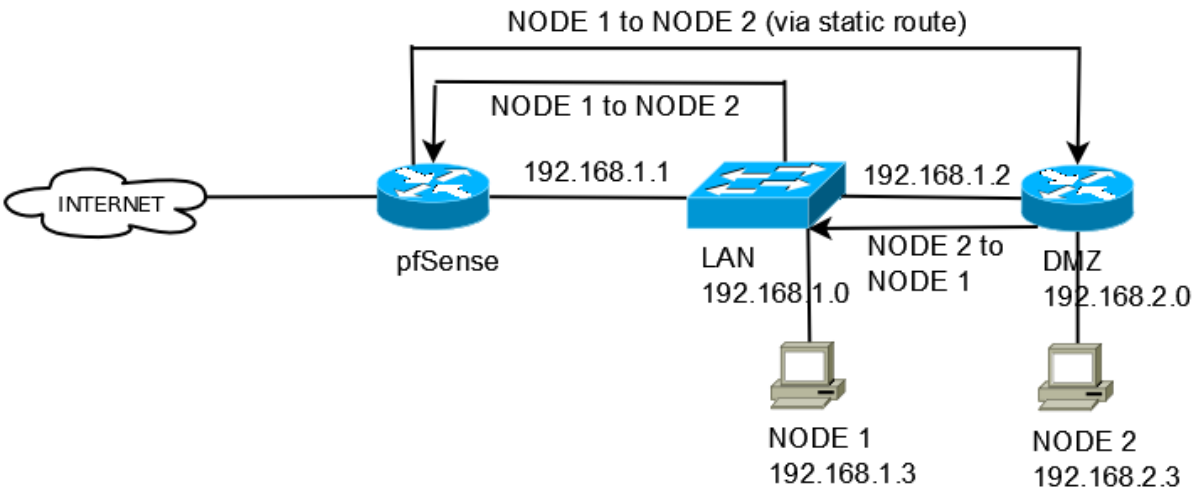



1
2
3
4
A
B
C
D
3
7
10
15
5
25
18
8


1
2
3
4
A
B
C
D
DP
DP
RP
RP
DP
DP
RP
3
7
10
15
5
18
25
6
11


INTERNET
192.168.1.1
192.168.1.2
pfSense
LAN
192.168.1.0
DMZ
192.168.2.0


System / Routing / Static Routes / Edit
Edit Route Entry
Destination network
192.168.2.0
/ 24
Destination network for this static route
Gateway
DMZ_Gateway - 172.16.1.2
Choose which gateway this route applies to or add a new one first
Disabled
Disable this static route
Set this option to disable this static route without removing it from the list.
Description
Static route to DMZ
A description may be entered here for administrative reference (not parsed).
Save



Static route filtering ☐ Bypass firewall rules for traffic on the same interface

This option only applies if one or more static routes have been defined. If it is enabled, traffic that enters and leaves through the same interface will not be checked by the firewall. This may be desirable in some situations where multiple subnets are connected to the same interface.

TCP Flags **Any flags.**

Use this to choose TCP flags that must be set or cleared for this rule to match.

No pfSync ☐ Prevent states created by this rule to be sync'ed over pfsync.

State type Sloppy

Select which type of state tracking mechanism to use. If in doubt, use keep state

Sloppy: works with all IP protocols

Interfaces / OPT1

General Configuration

Enable	☐ Enable interface
Description	OPT1 Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC controls	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	192.0.20.1 / 29
IPv4 Upstream gateway	None Add a new gateway If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local LANs the upstream gateway should be "none".Gateways can be managed by clicking here

Package / Services: RIP / ROUTED Settings

ROUTED Settings

General Options

Enable RIP	☒ Enables the Routing Information Protocol daemon.
Interfaces	LAN WAN loopback Select the interfaces that RIP will bind to. You can use the CTRL or COMMAND key to select multiple interfaces.
RIP Version	RIP Version 2
RIPv2 password	Specify a RIPv2 password. This password will be sent in the clear on all RIPv2 responses received and sent.
no_ag	☐ Turns off aggregation of subnets in RIPv1 and RIPv2 responses.
no_super_ag	☐ Turns off aggregation of networks into supernets in RIPv2 responses.

Save

Package / Services: OpenBGPD / Settings

Settings | Neighbors | Groups | Raw config | Status

General Options

Autonomous Systems (AS) Number	Set the local autonomous system number to as-number.
Holdtime	Set the holdtime in seconds. The holdtime is reset to its initial value every time either a KEEPALIVE or an UPDATE message is received from the neighbor. If the holdtime expires the session is dropped. The default is 90 seconds. Neighboring systems negotiate the holdtime used when the connection is established in the OPEN messages. Each neighbor announces its configured hold- time; the smaller one is then agreed upon.
fib-update	yes If set to no, do not update the Forwarding Information Base a.k.a. the kernel routing table. The default is yes.
Listen on IP	Specify the local IP address bgpd(8) should listen on, or leave blank to bind to all IPs.
Router IP	Set the router ID to the given IP address, which must be local to the machine.
CARP Status IP	none Used to determine the CARP status. When the CARP vhid is in BACKUP status, bgpd will not be started.
Networks	Announce the specified network as belonging to our AS. If set to "(inet|inet6)connected", inet or inet6 routes to directly attached networks will be announced. If set to "(inet|inet6) static", all inet or inet6 static routes will be announced.

Services / Quagga OSPFd / Global Settings

Global Settings | Interface Settings | Raw Config | Status

General Options

Master Password	Password to access the Zebra and OSPF management daemons. Required.
Logging	☐ If set to yes, Logs will be written via syslog.
Log Adjacency Changes	☐ If set to yes, adjacency changes will be written via syslog.
Router ID	Specify the Router ID. RID is the highest logical (loopback) IP address configured on a router. For more information on router identifiers see wikipedia.
Area	OSPFd area for this instance of OSPF. For more information on Areas see wikipedia.
Disable FIB updates (Routing table)	☐ Disables the updating of the host routing table(turns into stub router).
Redistribute connected subnets	☐ Enables the redistribution of connected networks (Default no)
Redistribute default route	☐ Enables the redistribution of a default route to this device (Default no)
Redistribute static	☐ Enables the redistribution of static routes (only works if you are using quagga static routes)

Interfaces / Bridges / Edit

Bridge Configuration

Member Interfaces

WAN
LAN

Interfaces participating in the bridge.

Description

Advanced Options

Hide Advanced

Advanced Configuration

Cache Size

Set the size of the bridge address cache. The default is 2000 entries.

Cache expire time

Set the timeout of address cache entries to this number of seconds. If seconds is zero, then address cache entries will not be expired. The default is 1200 seconds.

Span Port

WAN
LAN

Add the interface named by interface as a span port on the bridge. Span ports transmit a copy of every frame received by the bridge. This is most useful for snooping a bridged network passively on another host connected to one of the span ports of the bridge.
The span interface cannot be part of the bridge member interfaces.

Edge Ports

WAN
LAN

Set interface as an edge port. An edge port connects directly to end stations and cannot create bridging loops in the network; this allows it to transition straight to forwarding.

Gateway WAN2_DHCP - 192.168.1.1 - Interface WAN2_DHCP Gateway

Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.

Diagnostics / Routes

Routing Table Display Options

Resolve names Enable

Enabling name resolution may cause the query to take longer. It can be stopped at any time by clicking the Stop button in the browser.

Rows to display 100

Filter

Use a regular expression to filter IP address or hostnames.

Update

IPv4 Routes

Destination	Gateway	Flags	Use	Mtu	Netif	Expire
default	10.0.2.2	UGS	37245	1500	em0	
8.8.8.8	192.168.1.1	UGHS	116670	1500	em3	
10.0.2.0/24	link#1	U	4	1500	em0	
10.0.2.15	link#1	UHS	0	16384	lo0	
127.0.0.1	link#8	UH	6612	16384	lo0	
167.206.245.135	10.0.2.2	UGHS	366872	1500	em0	
167.206.245.136	10.0.2.2	UGHS	0	1500	em0	
172.16.0.0/16	link#2	U	478848	1500	em1	

Chapter 9: Extending pfSense with Packages

System / Package Manager / Package Installer

pfSense-pkg-nut installation successfully completed.

Installed Packages | Available Packages | Package Installer

Package Installation

```
    NET_SNMP_MIB_MODULES="host smux mibII/mta_sendmail ucd-snmp/diskio"
    NET_SNMP_LOGFILE=/var/log/snmpd.log
    NET_SNMP_PERSISTENTDIR=/var/net-snmp

     to define default values (or to override the defaults).  To avoid being
     prompted during the configuration process, you should (minimally) define
     the first two variables. (NET_SNMP_SYS_*)

     You may also define the following to avoid all interactive configuration:

    BATCH="yes"
Message from pfSense-pkg-nut-2.3.0:
Please visit Services - NUT to configure your UPS.
>>> Cleaning up cache... done.
Success
```

```
[2.3.2-DEVELOPMENT][root@pfSense.thewookie.dyndns.org]/root: pfSsh.php playback
installpkg "pfSense-pkg-squid"

Starting the pfSense developer shell....

Installing package "squid"... Done.
[2.3.2-DEVELOPMENT][root@pfSense.thewookie.dyndns.org]/root:
```

Package / Proxy Server: General Settings / General

General | Remote Cache | Local Cache | Antivirus | ACLs | Traffic Mgmt | Authentication | Users | Real Time | Sync

Squid General Settings

Enable Squid Proxy
Check to enable the Squid proxy.
Note: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data
If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Note: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Proxy Interface(s)
LAN
WAN2
WAN
loopback
The interface(s) the proxy server will bind to.
Note: Use CTRL + click to select multiple interfaces.

Proxy Port
3128
This is the port the proxy server will listen on.
(Default: 3128)

ICP Port
This is the port the proxy server will send and receive ICP queries to and from neighbor caches.
Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow Users on Interface
If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.
There will be no need to add the interface's subnet to the list of allowed subnets.

Patch Captive Portal
This feature was removed - see Bug #5594 for details!
If you were using this feature, double-check '/etc/inc/captiveportal.inc' content for sanity.

Package / Reverse Proxy Server: General / General

General | Web Servers | Mappings | Redirects | Real Time | Sync

Squid Reverse Proxy General Settings

Reverse Proxy Interface(s)
LAN
WAN2
WAN
loopback
The interface(s) the reverse-proxy server will bind to (usually WAN).

User Defined Reverse Proxy IPs
Squid will additionally bind to these user-defined IPs for reverse proxy operation. Useful for virtual IPs such as CARP.
Note: Separate entries by semi-colons (;)

Important: Any entry here must be a valid, locally configured IP address.

External FQDN
The external fully qualified domain name of the WAN IP address.

Reset TCP Connections on Unauthorized Requests
If checked, the reverse proxy will reset the TCP connection if the request is unauthorized.

Squid Reverse HTTP Settings

Enable HTTP Reverse Proxy
If checked, the proxy server will act in HTTP reverse mode.
Important: You must add a proper firewall rule with destination matching the 'Reverse Proxy Interface(s)' address.

Package / Proxy filter SquidGuard: General settings / General settings

General settings | Common ACL | Groups ACL | Target categories | Times | Rewrites | Blacklist | Log | XMLRPC Sync

General Options

Enable — Check this option to enable squidGuard.

Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details.

The Save button at the bottom of this page must be clicked to save configuration changes.

To activate squidGuard configuration changes, **the Apply button must be clicked.**

Apply

SquidGuard service state: **STARTED**

LDAP Options

Enable LDAP Filter — Enable options for setup ldap connection to create filters with ldap search

LDAP DN

Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)

LDAP DN Password

Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z\/][a-zA-Z0-9/_\-\.\/\:\%\+\?=&]

Strip NT domain name — Strip NT domain name component from user names (/ or \ separated).

Strip Kerberos Realm — Strip Kerberos Realm component from user names (@ separated).

Package / Diagnostics: ntopng Settings / ntopng Settings

ntopng Settings | Access ntopng

General Options

Enable ntopng — Check this to enable ntopng.

Keep Data/Settings — Keep ntopng settings, graphs and traffic data. (Default: on)

Note: If 'Keep Data/Settings' is disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade!

ntopng Admin Password

Enter the password for the ntopng GUI. Minimum 5 characters.

Confirm ntopng Admin Password

Interface

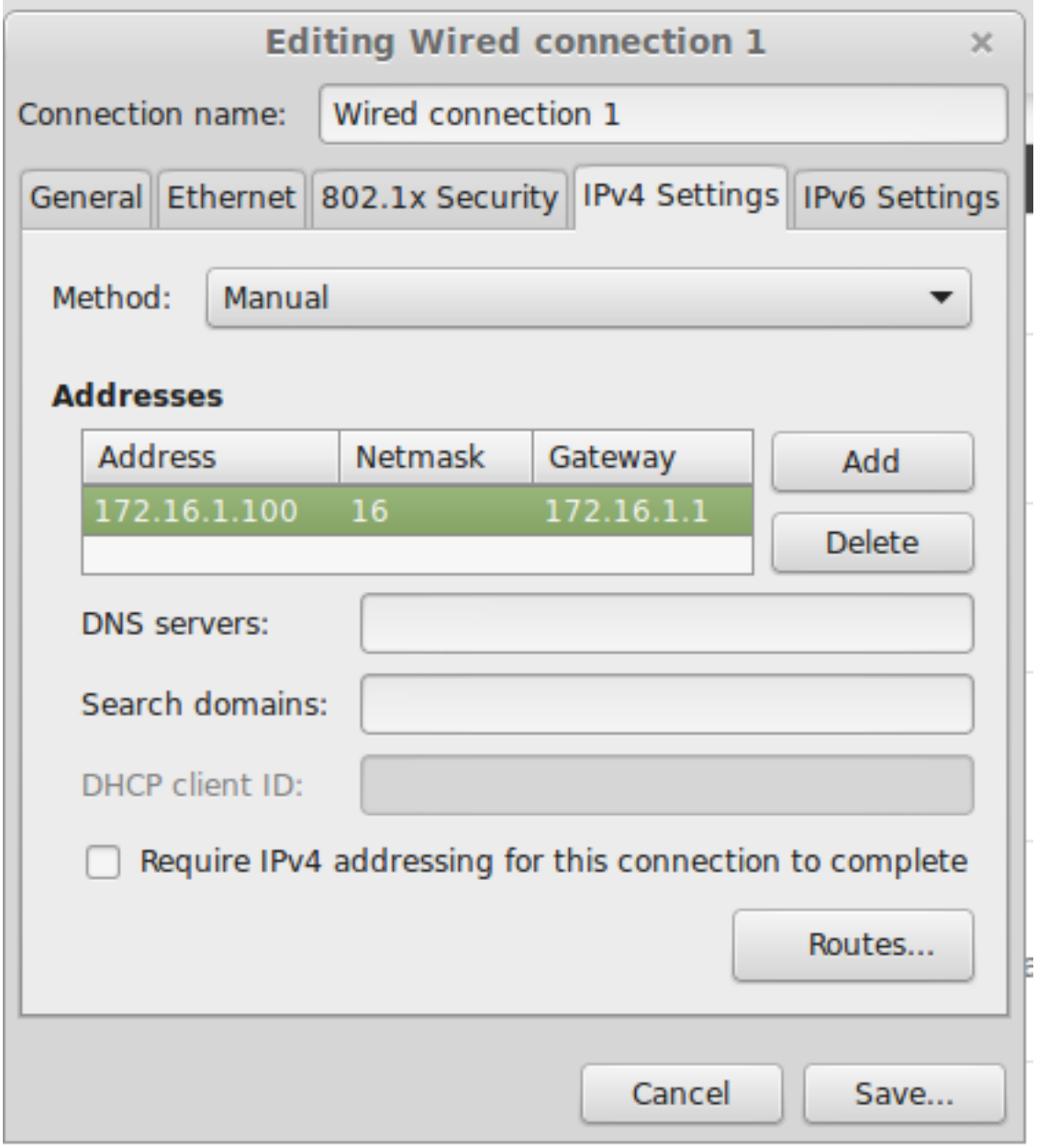
LAN
DEVELOPERS
WAN

DNS Mode — Decode DNS responses and resolve local numeric IPs only (default)

Configures how name resolution is handled.

Additionally, GeoIP Data can provide location information about IP addresses.
This product includes GeoLite data created by MaxMind, available from http://www.maxmind.com

Update GeoIP Data


Editing Wired connection 1
Connection name:
Wired connection 1
General
Ethernet
802.1x Security
IPv4 Settings
IPv6 Settings
Method:
Manual
Addresses
Address
Netmask
Gateway
172.16.1.100
16
172.16.1.1
Add
Delete
DNS servers:
Search domains:
DHCP client ID:
Require IPv4 addressing for this connection to complete
Routes...
Cancel
Save...

Advanced Log Filter

Last 50 General Log Entries. (Maximum 50)

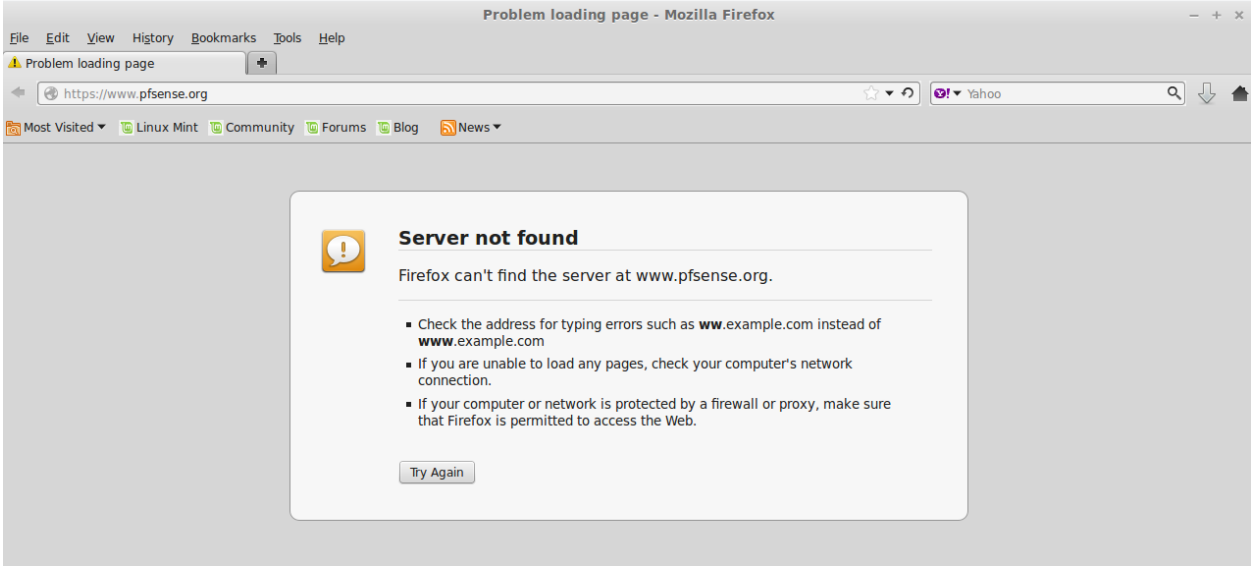
Time	Process	PID	Message
Jun 19 07:00:00	php		[pfBlockerNG] Starting cron process.
Jun 19 07:00:00	php		[pfBlockerNG] No changes to Firewall rules, skipping Filter Reload
Jun 19 08:00:00	php		[pfBlockerNG] Starting cron process.
Jun 19 08:00:00	php		[pfBlockerNG] No changes to Firewall rules, skipping Filter Reload
Jun 19 09:00:00	php		[pfBlockerNG] Starting cron process.
Jun 19 09:00:00	php		[pfBlockerNG] No changes to Firewall rules, skipping Filter Reload
Jun 19 09:09:11	check_reload_status		updating dyndns WAN_DHCP
Jun 19 09:09:11	check_reload_status		Restarting ipsec tunnels
Jun 19 09:09:11	check_reload_status		Restarting OpenVPN tunnels/interfaces
Jun 19 09:09:11	check_reload_status		Reloading filter
Jun 19 09:09:14	xinetd	23114	Starting reconfiguration
Jun 19 09:09:14	xinetd	23114	Swapping defaults
Jun 19 09:09:14	xinetd	23114	readjusting service 6969-udp
Jun 19 09:09:14	xinetd	23114	Reconfigured: new=0 old=1 dropped=0 (services)
Jun 19 09:09:27	php-fpm	76391	/rc.newipsecdns: IPSEC: One or more IPsec tunnel endpoints has changed its IP. Refreshing.
Jun 19 09:09:27	php-fpm	76391	/rc.newipsecdns: WARNING: Setting i_dont_care_about_security_and_use_aggressive_mode_psk option because a phase 1 is configured using aggressive mode with pre-shared keys. This is not a secure configuration.
Jun 19 09:09:27	check_reload_status		Reloading filter
Jun 19 09:09:29	xinetd	23114	Starting reconfiguration

```
pfTop: Up State 1-22/113, View: default, Order: none, Cache: 10000      01:39:09
1404                                                                            P
R     D SRC                    DEST                   STATE   AGE   EXP  PKTS BYTES
udp   O ::1[27947]             ::1[9364]               2:2   92359    54  8393  401K
udp   I ::1[27947]             ::1[9364]               2:2   92359    54  8393  401K
udp   O ::1[48209]             ::1[42864]              2:2   2073m    54 10952  521K
udp   I ::1[48209]             ::1[42864]              2:2   2073m    54 10952  521K
udp   O ::1[52063]             ::1[34528]              2:2   2072m    54 10951  521K
udp   I ::1[52063]             ::1[34528]              2:2   2072m    54 10951  521K
udp   O ::1[59438]             ::1[48690]              2:2   2066m    54 10930  520K
udp   I ::1[59438]             ::1[48690]              2:2   2066m    54 10930  520K
udp   O ::1[35274]             ::1[3070]               2:2   2066m    54 10929  520K
udp   I ::1[35274]             ::1[3070]               2:2   2066m    54 10929  520K
udp   O ::1[25677]             ::1[6184]               2:2   2065m    54 10927  520K
udp   I ::1[25677]             ::1[6184]               2:2   2065m    54 10927  520K
udp   O ::1[47219]             ::1[16977]              2:2   2065m    54 10926  520K
udp   I ::1[47219]             ::1[16977]              2:2   2065m    54 10926  520K
udp   O ::1[5982]              ::1[63669]              2:2   2062m    54 10918  519K
udp   I ::1[5982]              ::1[63669]              2:2   2062m    54 10918  519K
udp   O ::1[59055]             ::1[20342]              2:2   2062m    54 10916  519K
udp   I ::1[59055]             ::1[20342]              2:2   2062m    54 10916  519K
udp   O ::1[6847]              ::1[29159]              2:2   2061m    54 10914  519K
udp   I ::1[6847]              ::1[29159]              2:2   2061m    54 10914  519K
udp   O ::1[36976]             ::1[35431]              2:2   2061m    54 10913  519K
udp   I ::1[36976]             ::1[35431]              2:2   2061m    54 10913  519K
```

Terminal

```
user@user-VirtualBox ~ $ ping -c 10 google.com
PING google.com (167.206.145.49): 56 data bytes
64 bytes from 167.206.145.49: icmp_seq=0 ttl=57 time=11.112 ms
64 bytes from 167.206.145.49: icmp_seq=1 ttl=57 time=18.449 ms
64 bytes from 167.206.145.49: icmp_seq=2 ttl=57 time=18.932 ms
64 bytes from 167.206.145.49: icmp_seq=3 ttl=57 time=17.847 ms
64 bytes from 167.206.145.49: icmp_seq=4 ttl=57 time=12.325 ms
64 bytes from 167.206.145.49: icmp_seq=5 ttl=57 time=10.854 ms
64 bytes from 167.206.145.49: icmp_seq=6 ttl=57 time=12.973 ms
64 bytes from 167.206.145.49: icmp_seq=7 ttl=57 time=16.351 ms
64 bytes from 167.206.145.49: icmp_seq=8 ttl=57 time=12.255 ms
64 bytes from 167.206.145.49: icmp_seq=9 ttl=57 time=20.017 ms
--- google.com ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max/stddev = 10.854/15.112/20.017/3.368 ms
user@user-VirtualBox ~ $
```

```
C:\>tracert google.com

Tracing route to google.com [167.206.252.99]
over a maximum of 30 hops:

  1    <1 ms    <1 ms     1 ms  pfSense.localdomain [192.168.2.1]
  2    16 ms    22 ms    18 ms  pfSense.localdomain [192.168.2.1]
  3     9 ms     8 ms     9 ms  67.59.248.125
  4    11 ms    10 ms    11 ms  ool-4353f894.dyn.optonline.net [67.83.248.148]
  5    14 ms     9 ms    24 ms  65.19.119.159
  6     8 ms    12 ms     9 ms  167.206.252.99

Trace complete.

C:\>
```


Problem loading page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Problem loading page
https://www.pfsense.org
Yahoo
Most Visited
Linux Mint
Community
Forums
Blog
News
Server not found
Firefox can't find the server at www.pfsense.org.
Check the address for typing errors such as ww.example.com instead of www.example.com
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
Try Again