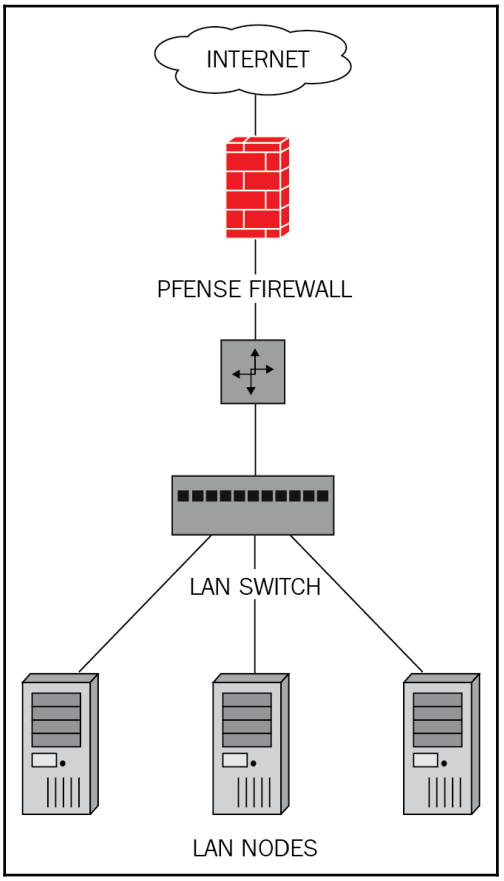
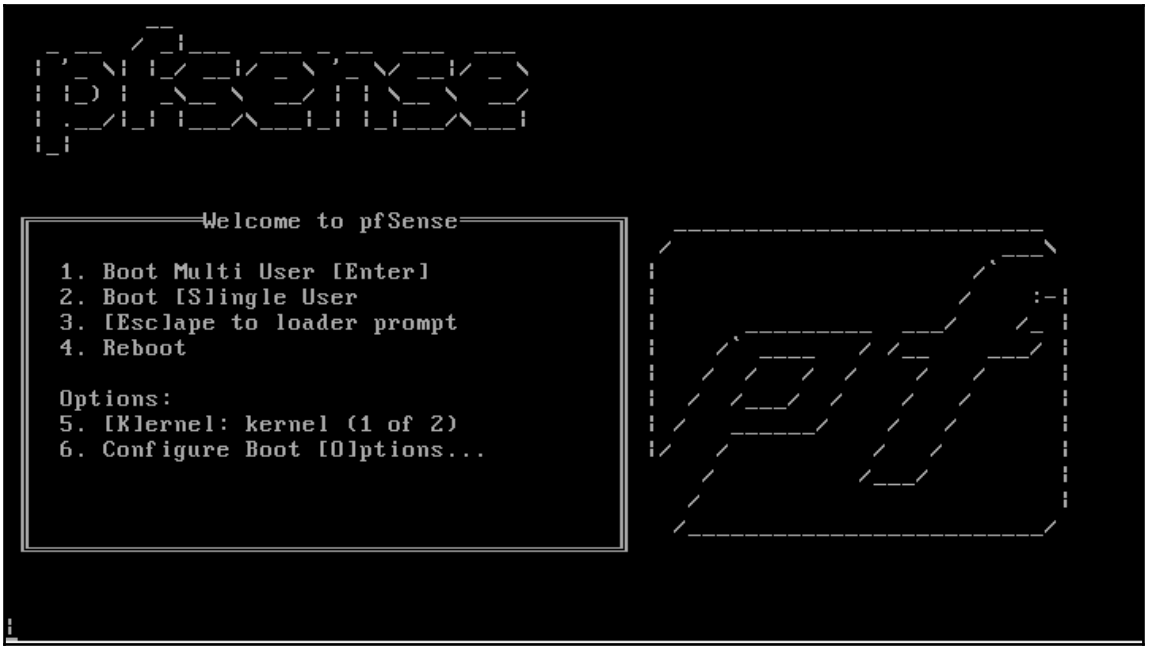
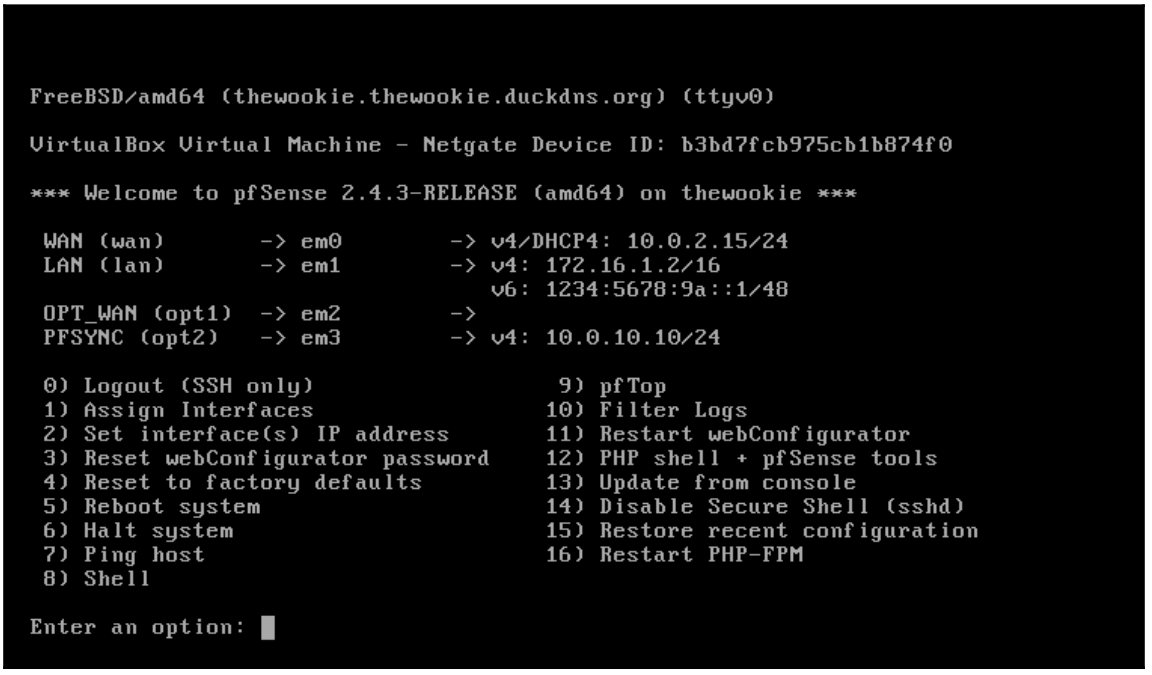
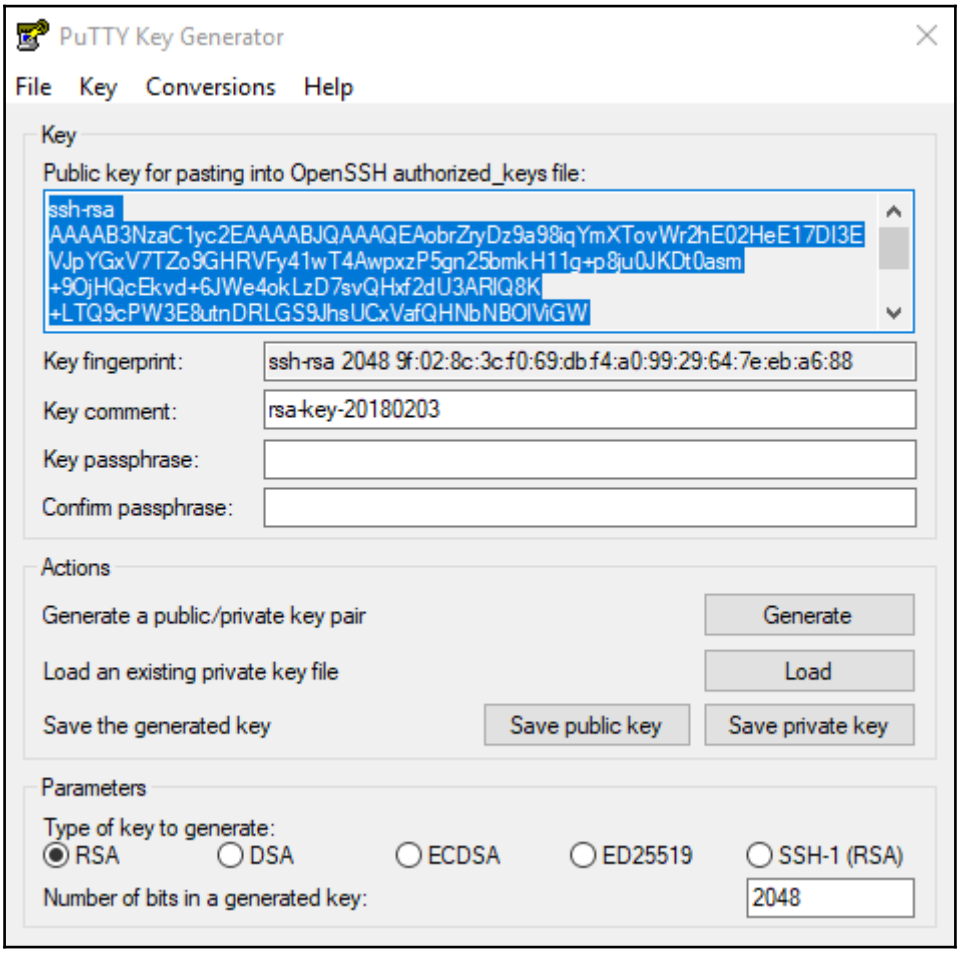
Chapter 1: Revisiting pfSense Basics

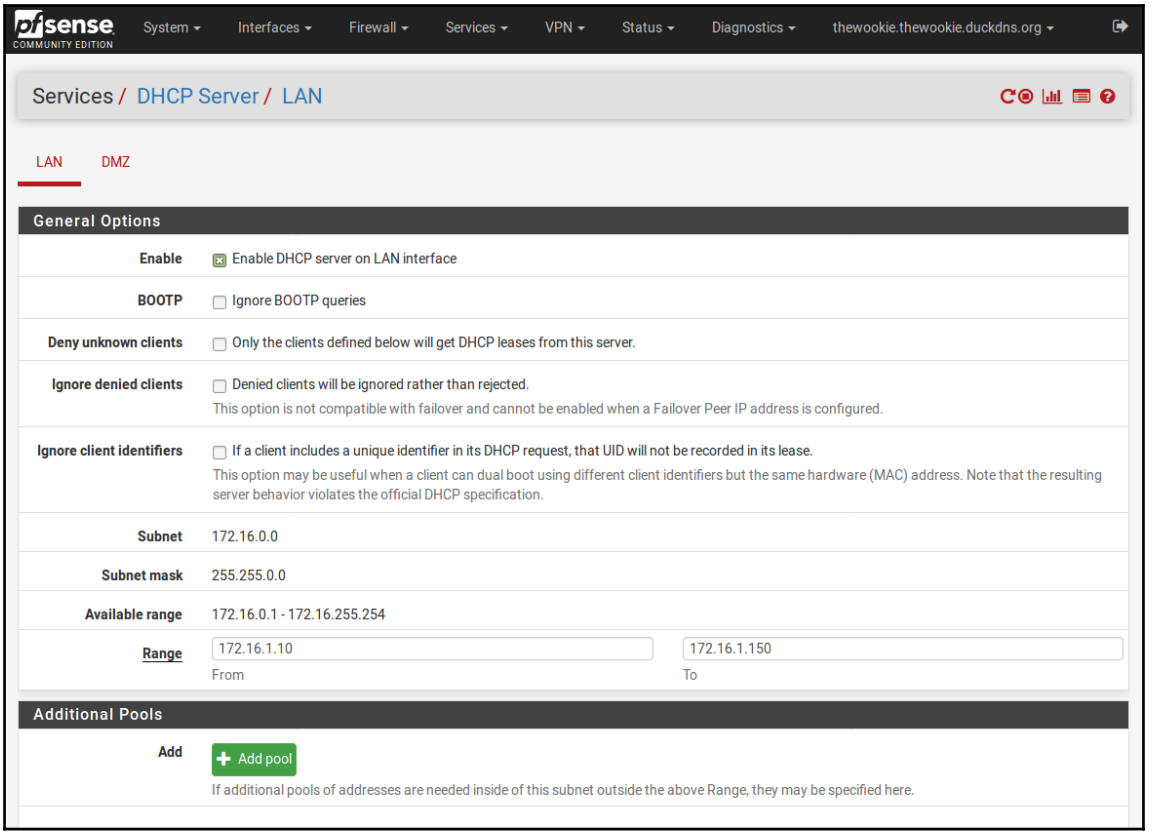


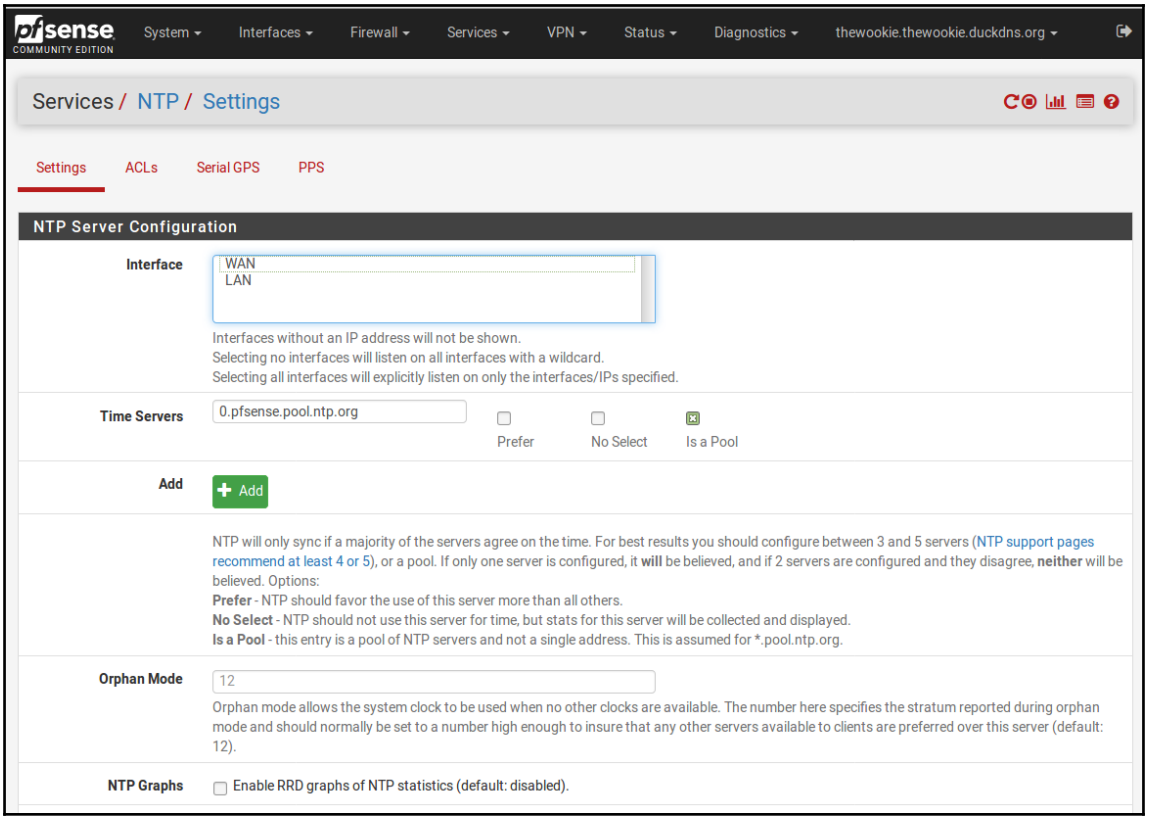

Welcome to pfSense
1. Boot Multi User [Enter]
2. Boot [S]ingle User
3. [Esc]ape to loader prompt
4. Reboot
Options:
5. [K]ernel: kernel (1 of 2)
6. Configure Boot [O]ptions...


FreeBSD/amd64 (thewookie.thewookie.duckdns.org) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: b3bd7fcb975cb1b874f0
*** Welcome to pfSense 2.4.3-RELEASE (amd64) on thewookie ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 172.16.1.2/16
v6: 1234:5678:9a::1/48
OPT_WAN (opt1) -> em2 ->
PFSYNC (opt2) -> em3 -> v4: 10.0.10.10/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Disable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

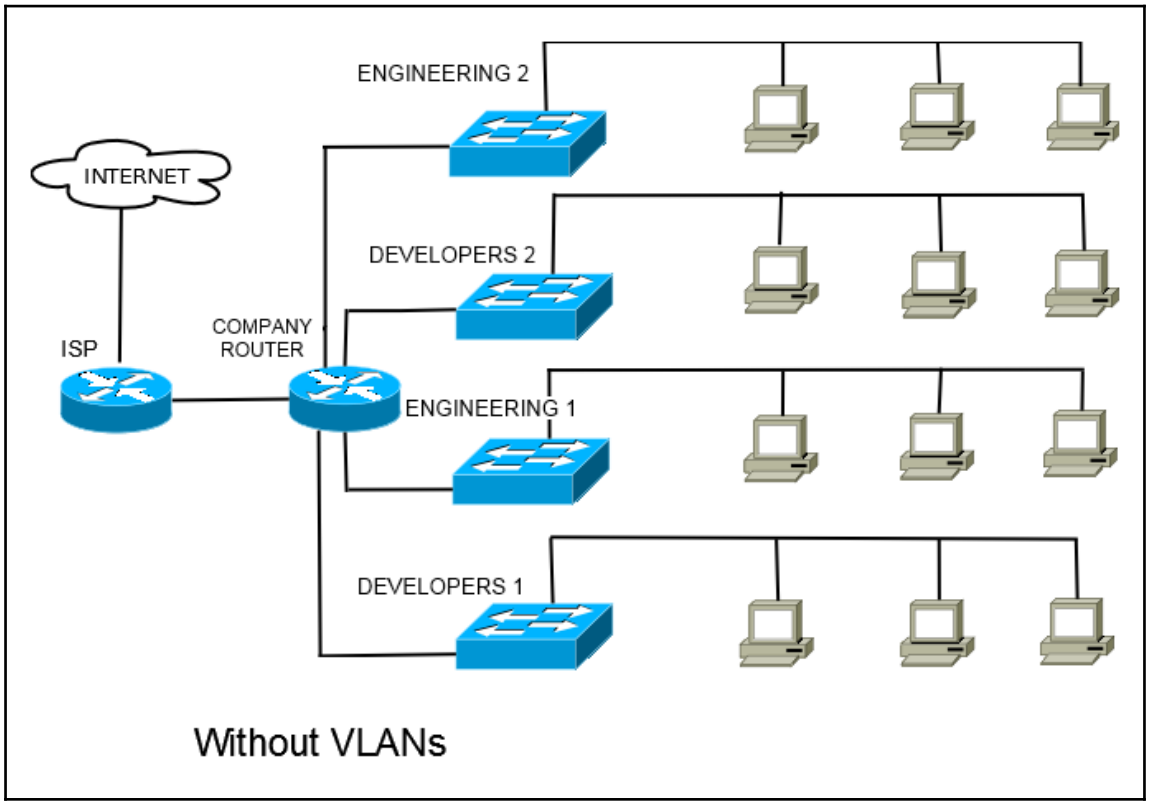
Chapter 2: Advanced pfSense Configuration

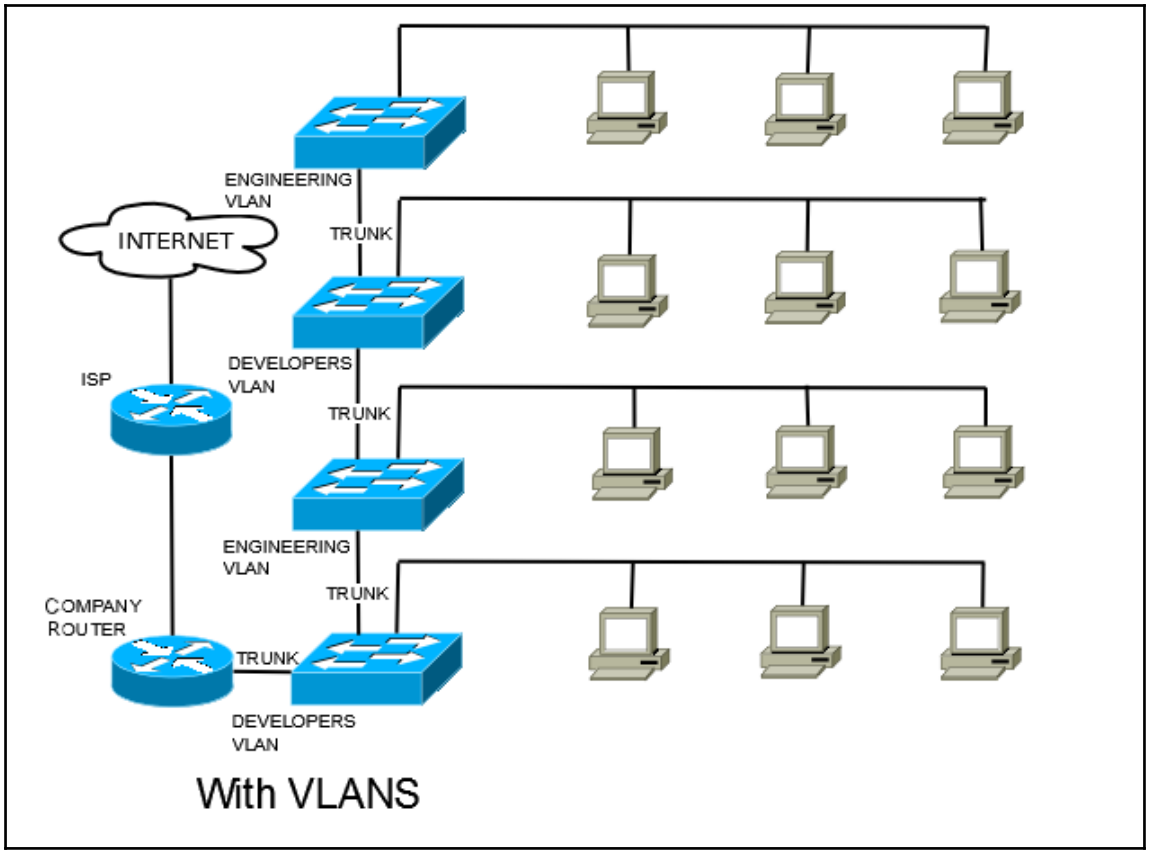


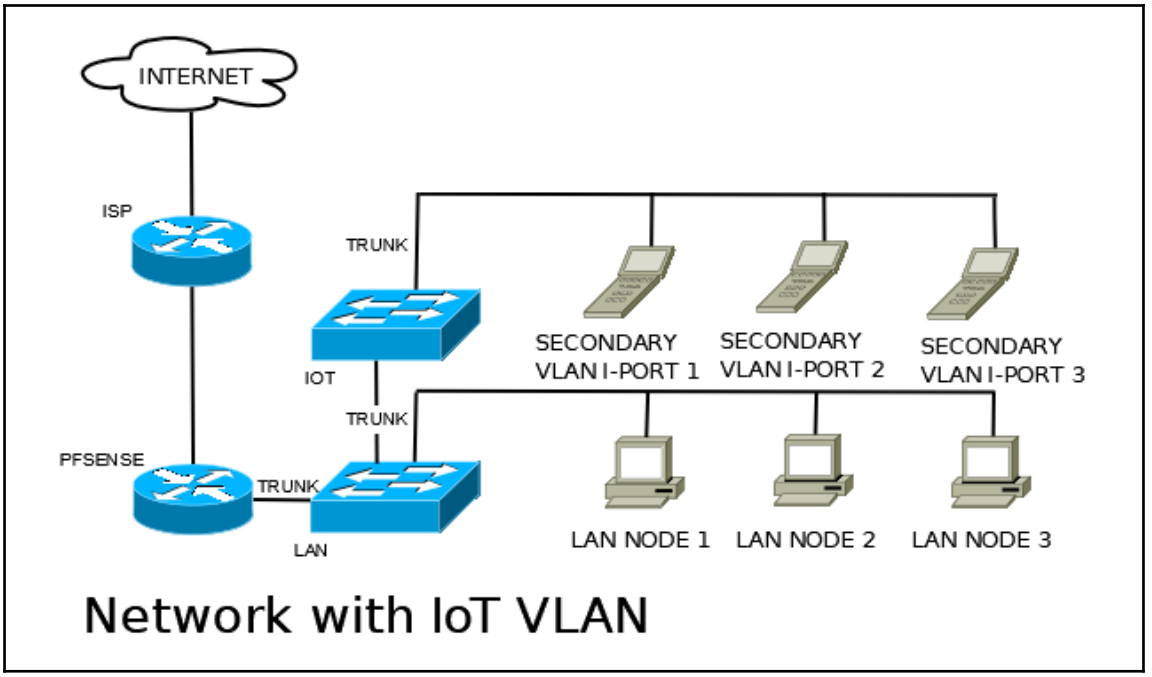

pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
thewookie.thewookie.duckdns.org
Services / DHCP Server / LAN
LAN
DMZ
General Options
Enable
Enable DHCP server on LAN interface
BOOTP
Ignore BOOTP queries
Deny unknown clients
Only the clients defined below will get DHCP leases from this server.
Ignore denied clients
Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers
If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet
172.16.0.0
Subnet mask
255.255.0.0
Available range
172.16.0.1 - 172.16.255.254
Range
172.16.1.10
From
172.16.1.150
To
Additional Pools
Add
Add pool
If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
thewookie.thewookie.duckdns.org
Services / NTP / Settings
Settings
ACLs
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
Is a Pool
Add
Add
NTP will only sync if a majority of the servers agree on the time. For best results you should configure between 3 and 5 servers (NTP support pages recommend at least 4 or 5), or a pool. If only one server is configured, it will be believed, and if 2 servers are configured and they disagree, neither will be believed. Options:
Prefer - NTP should favor the use of this server more than all others.
No Select - NTP should not use this server for time, but stats for this server will be collected and displayed.
Is a Pool - this entry is a pool of NTP servers and not a single address. This is assumed for *.pool.ntp.org.
Orphan Mode
12
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).

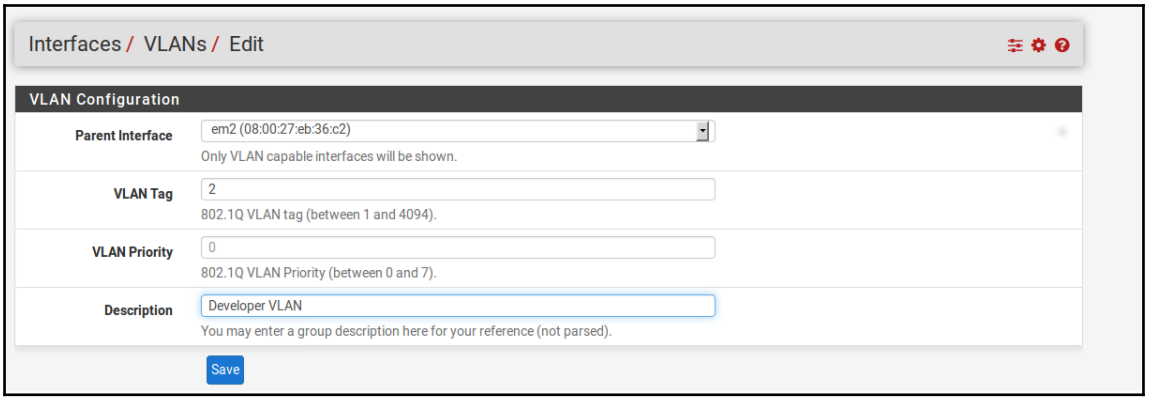
Chapter 3: VLANs

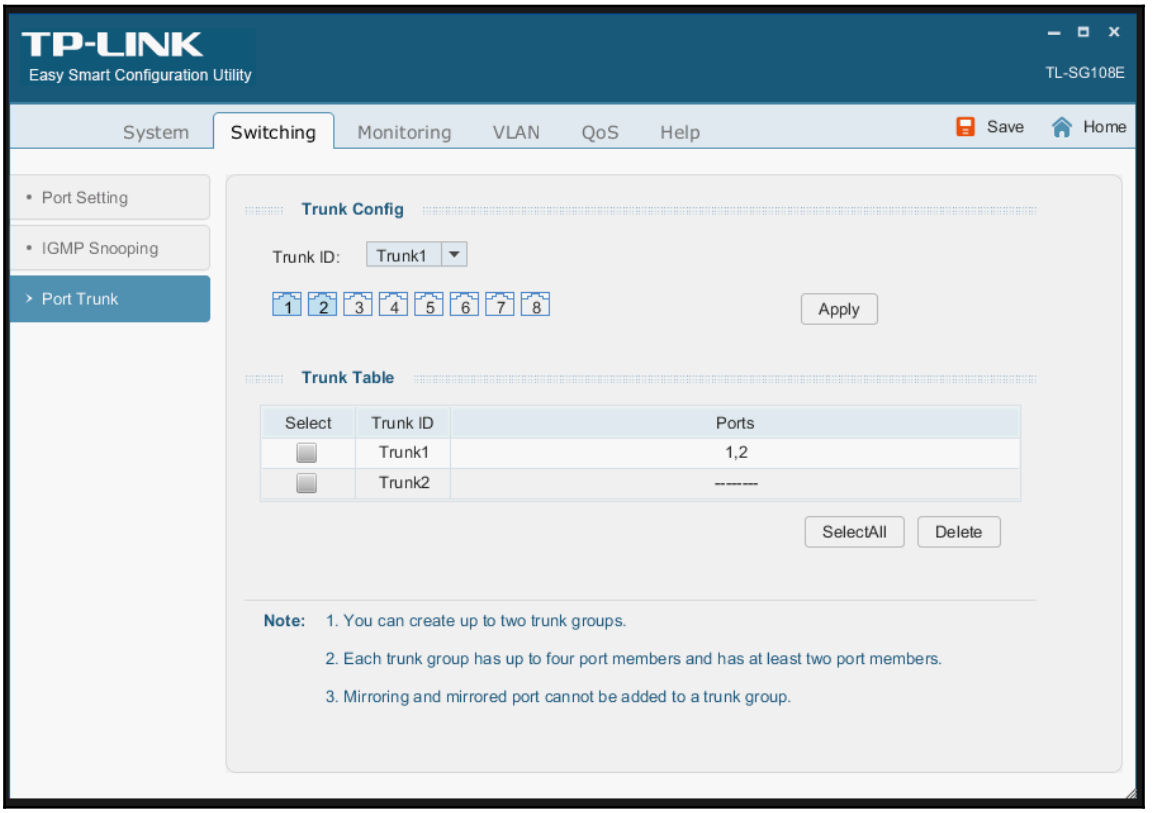



ENGINEERING
VLAN
INTERNET
TRUNK
DEVELOPERS
VLAN
ISP
TRUNK
ENGINEERING
VLAN
TRUNK
COMPANY
ROUTER
TRUNK
DEVELOPERS
VLAN
With VLANS



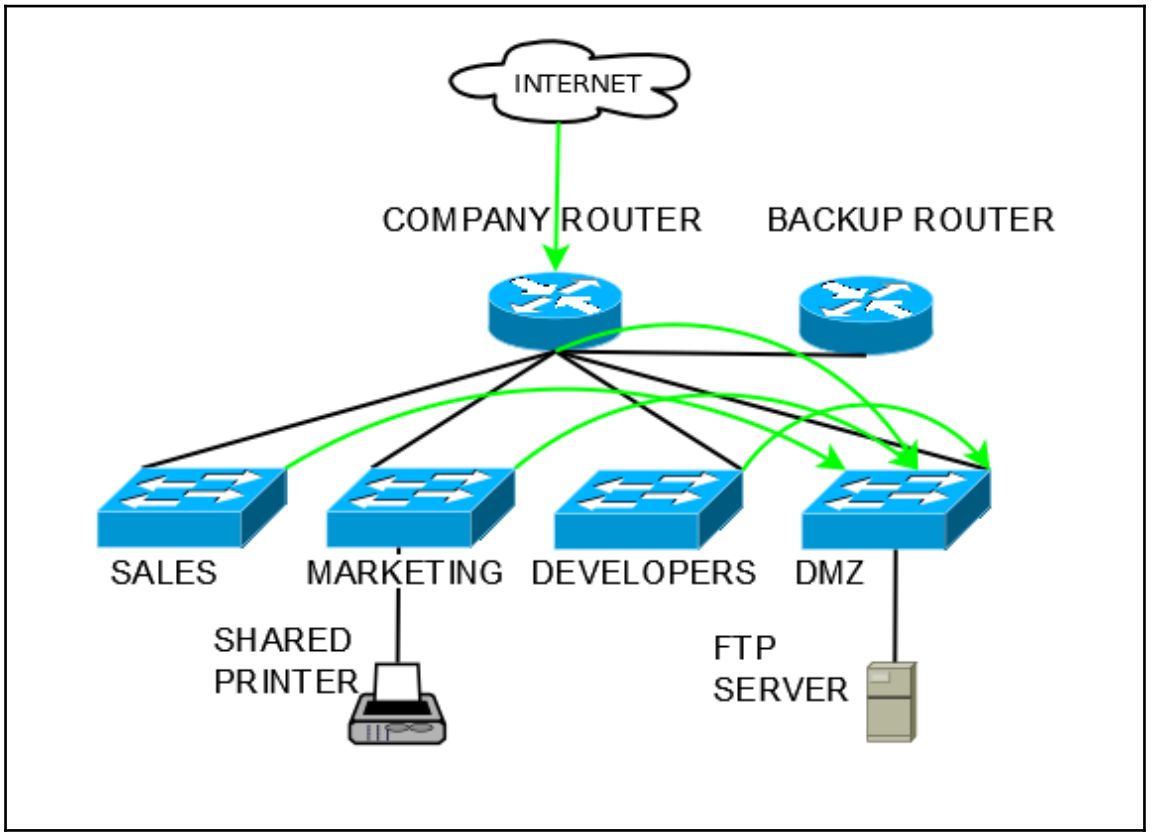

```
Enter the parent interface name for the new VLAN (or nothing if finished): em2
Enter the VLAN tag (1-4094): 3


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):
```

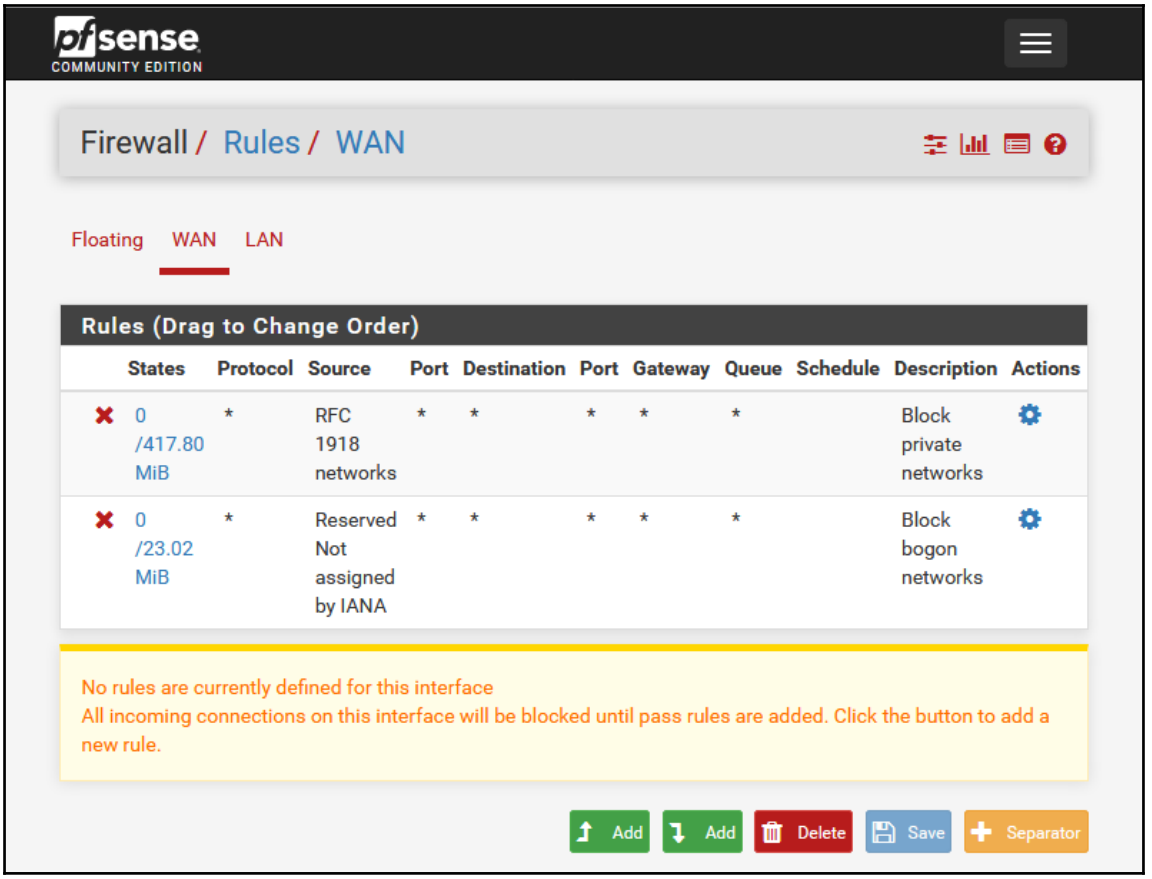

Interfaces / VLANs / Edit
VLAN Configuration
Parent Interface
em2 (08:00:27:eb:36:c2)
Only VLAN capable interfaces will be shown.
VLAN Tag
2
802.1Q VLAN tag (between 1 and 4094).
VLAN Priority
0
802.1Q VLAN Priority (between 0 and 7).
Description
Developer VLAN
You may enter a group description here for your reference (not parsed).
Save

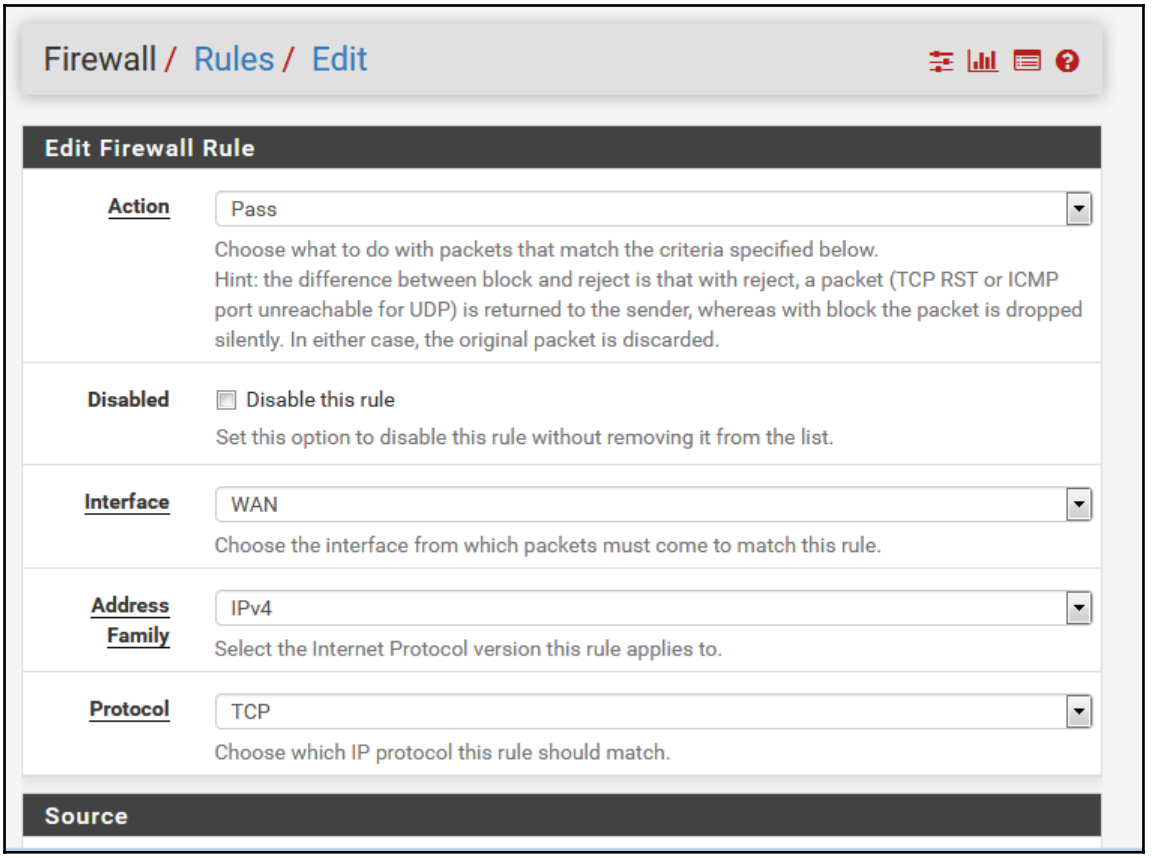

TP-LINK
Easy Smart Configuration Utility
TL-SG108E
System
Switching
Monitoring
VLAN
QoS
Help
Save
Home
Port Setting
IGMP Snooping
Port Trunk
Trunk Config
Trunk ID:
Trunk1
1 2 3 4 5 6 7 8
Apply
Trunk Table
Select
Trunk ID
Ports
Trunk1
1,2
Trunk2

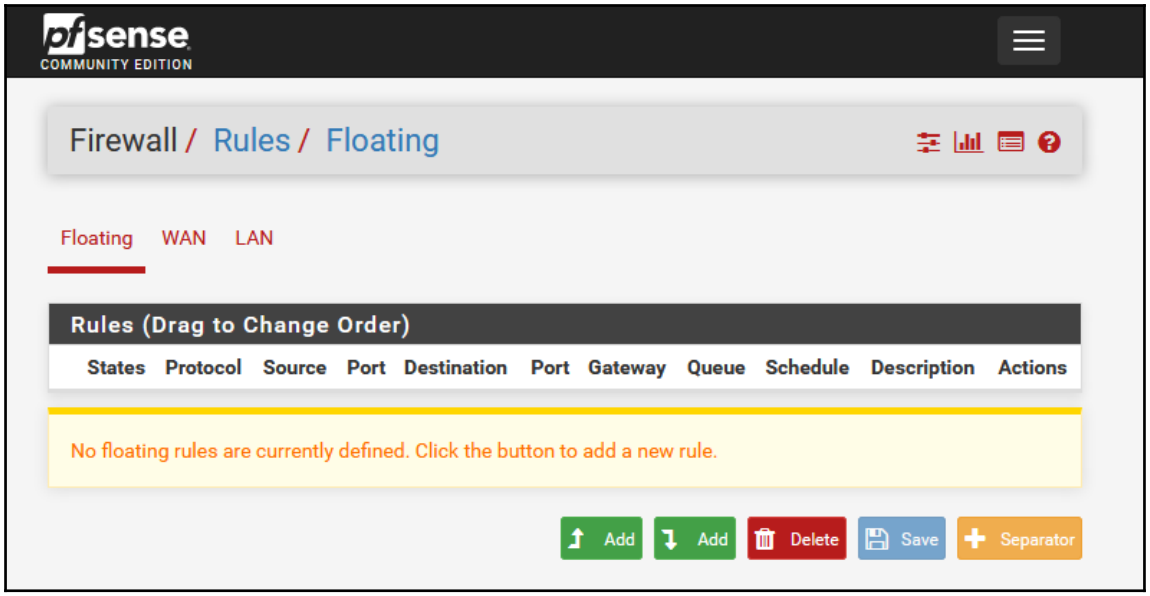
SelectAll
Delete
Note:
1. You can create up to two trunk groups.
2. Each trunk group has up to four port members and has at least two port members.
3. Mirroring and mirrored port cannot be added to a trunk group.

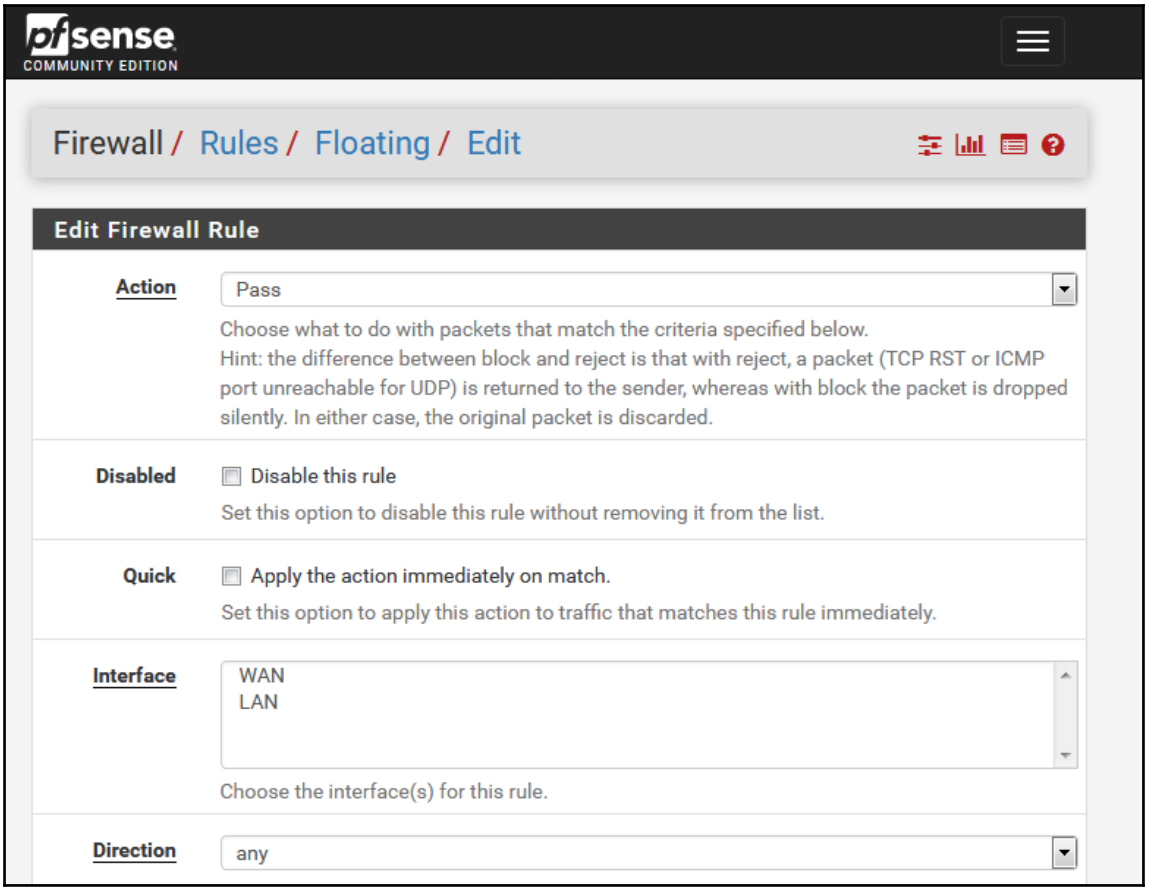
Chapter 4: Using pfSense as a Firewall

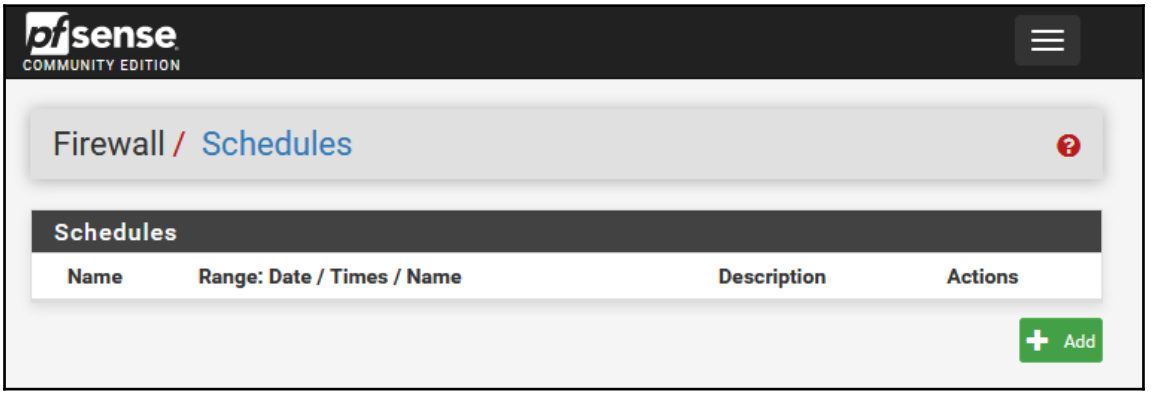


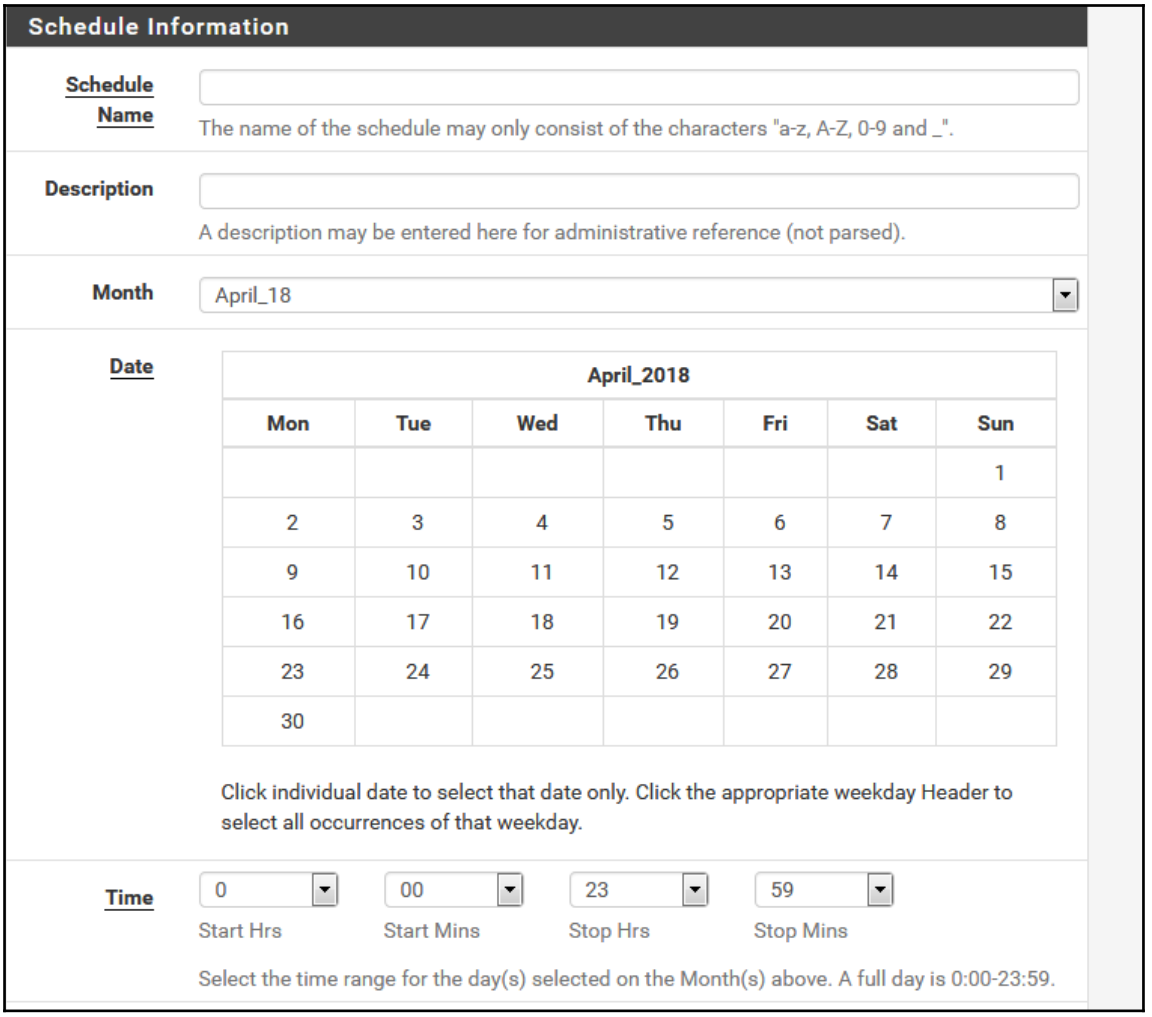

pfsense
COMMUNITY EDITION
Firewall / Rules / WAN
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0 /417.80 MiB
*
RFC 1918 networks
*
*
*
*
*
Block private networks
0 /23.02 MiB
*
Reserved Not assigned by IANA
*
*
*
*
*
Block bogon networks
No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.
Add
Add
Delete
Save
Separator


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
WAN
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


pfsense
COMMUNITY EDITION
Firewall / Rules / Floating
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
No floating rules are currently defined. Click the button to add a new rule.
Add
Add
Delete
Save
Separator


pfsense
COMMUNITY EDITION
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 to apply this action to traffic that matches this rule immediately.
Interface
WAN
LAN
Choose the interface(s) for this rule.
Direction
any


pfsense
COMMUNITY EDITION
Firewall / Schedules
Schedules
Name
Range: Date / Times / Name
Description
Actions
Add



Schedule Information

Schedule Name

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

Description

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

Month

April_18

Date

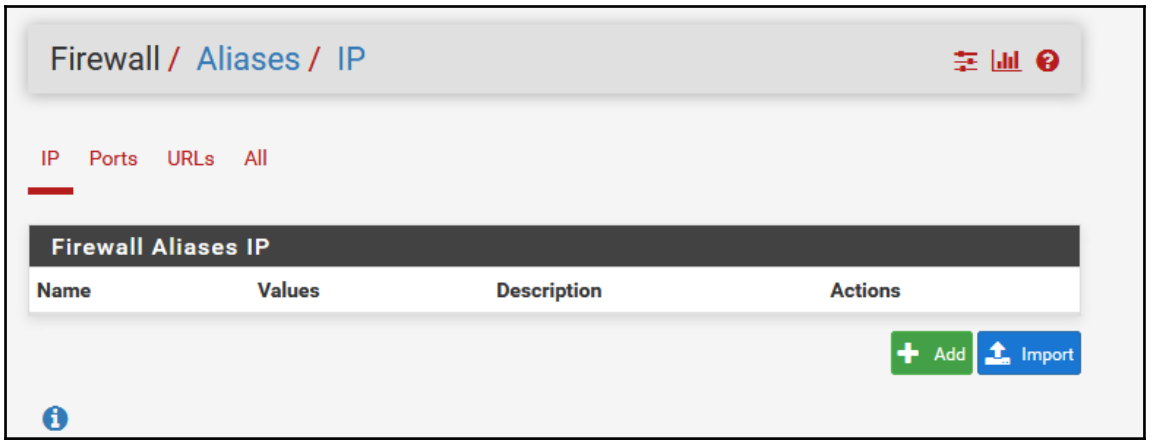
April_2018						
Mon	**Tue**	**Wed**	**Thu**	**Fri**	**Sat**	**Sun**
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

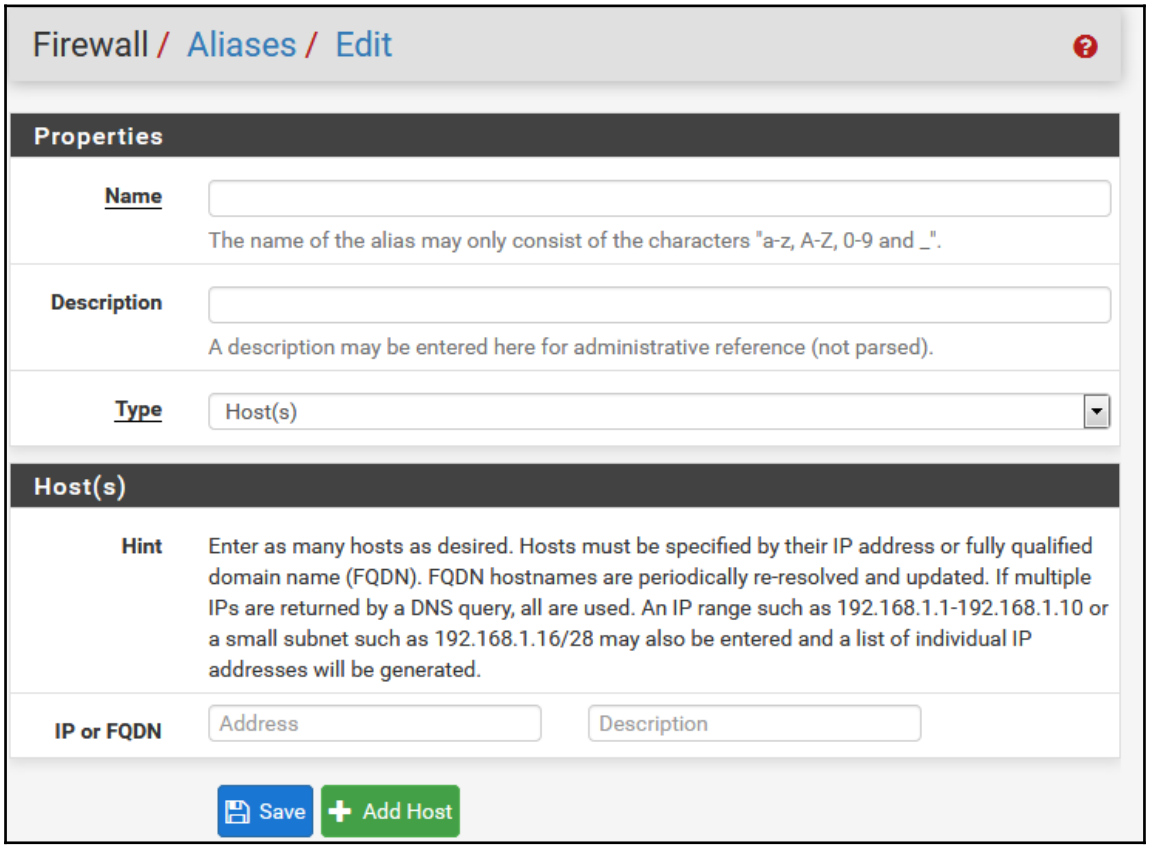
Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

Time

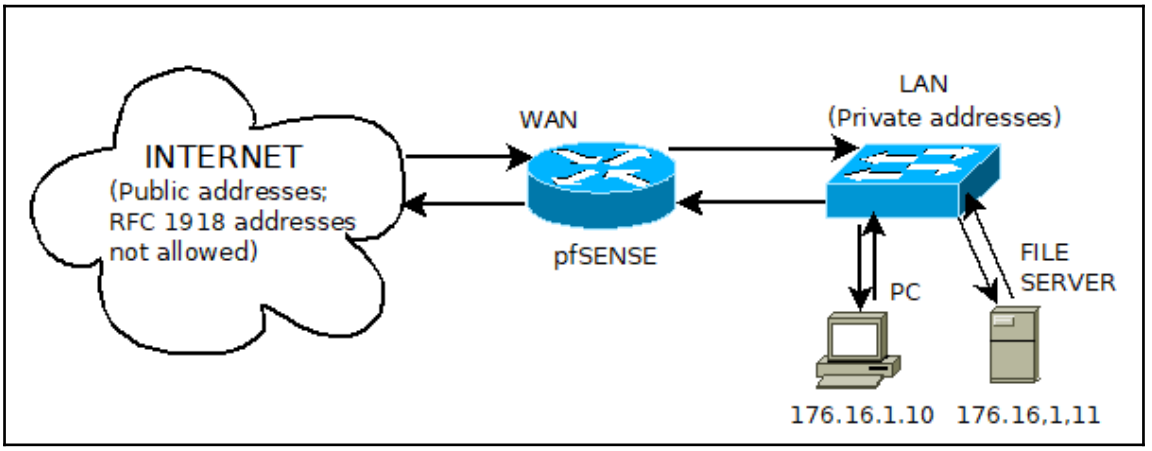
0	00	23	59
Start Hrs	Start Mins	Stop Hrs	Stop Mins

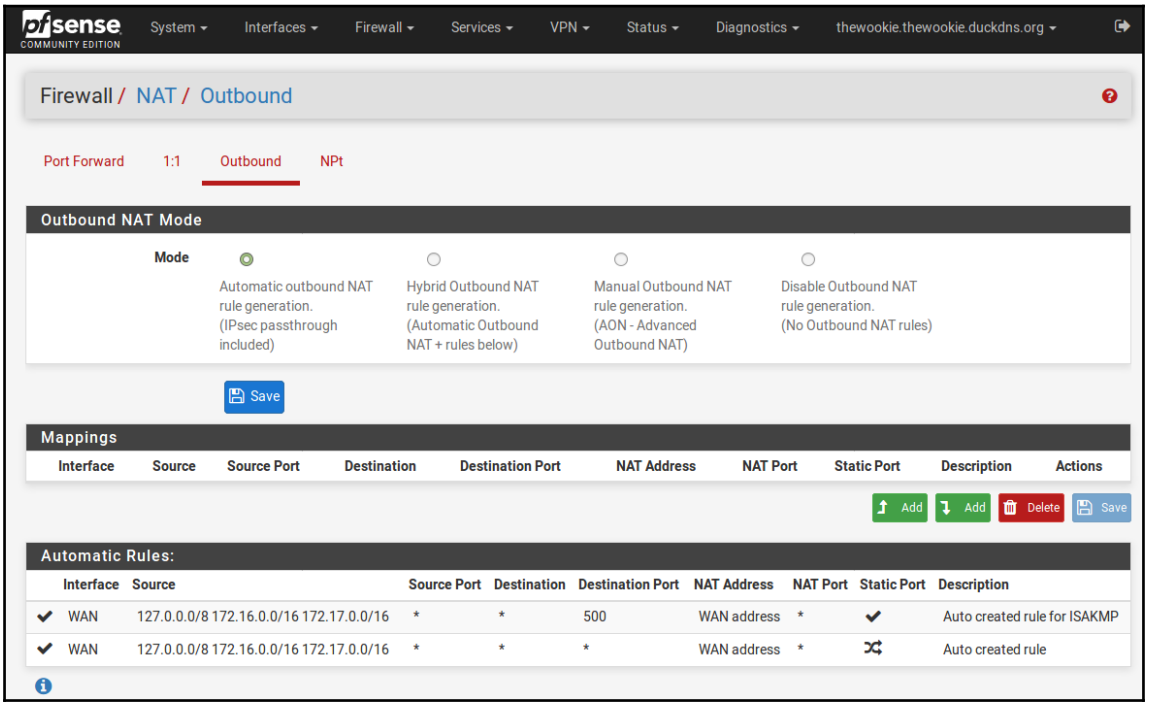
Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.


Firewall / Aliases / IP
IP
Ports
URLs
All
Firewall Aliases IP
Name
Values
Description
Actions
Add
Import


Firewall / Aliases / Edit
Properties
Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description
A description may be entered here for administrative reference (not parsed).
Type
Host(s)
Host(s)
Hint
Enter as many hosts as desired. 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. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.
IP or FQDN
Address
Description
Save
Add Host

Chapter 5: Network Address Translation

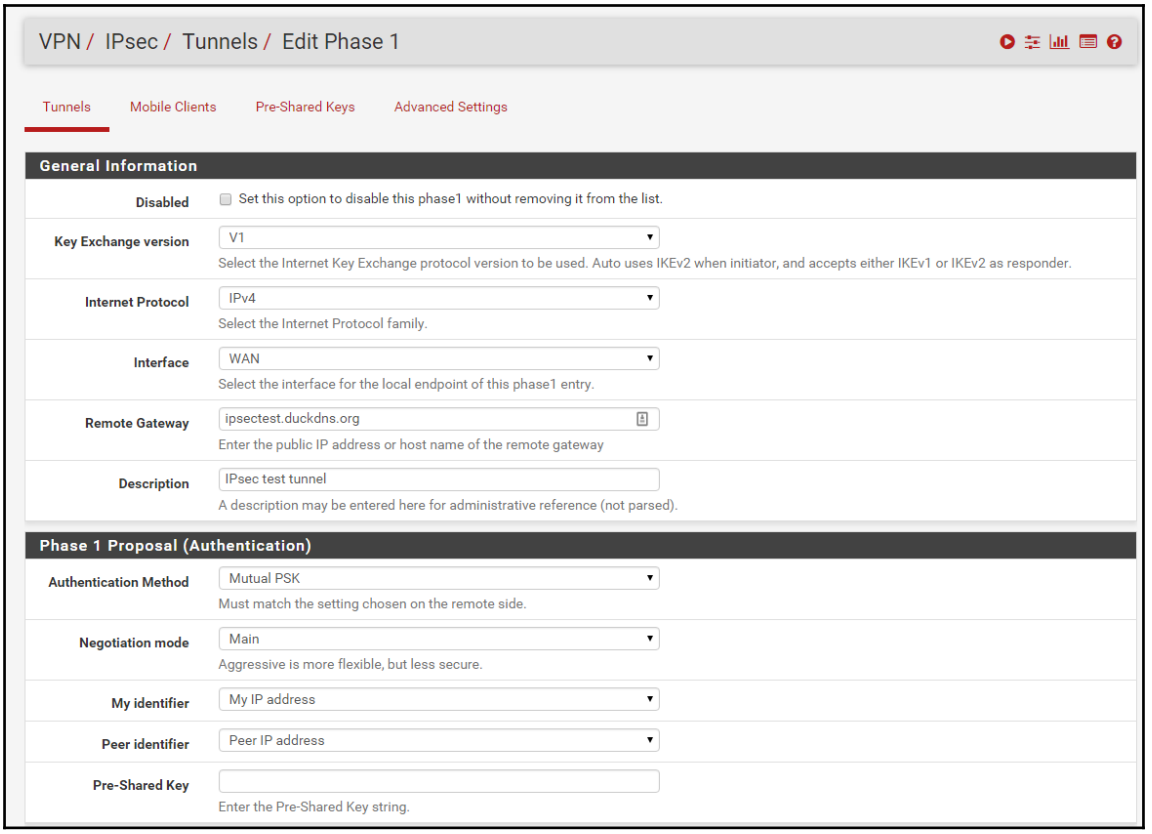


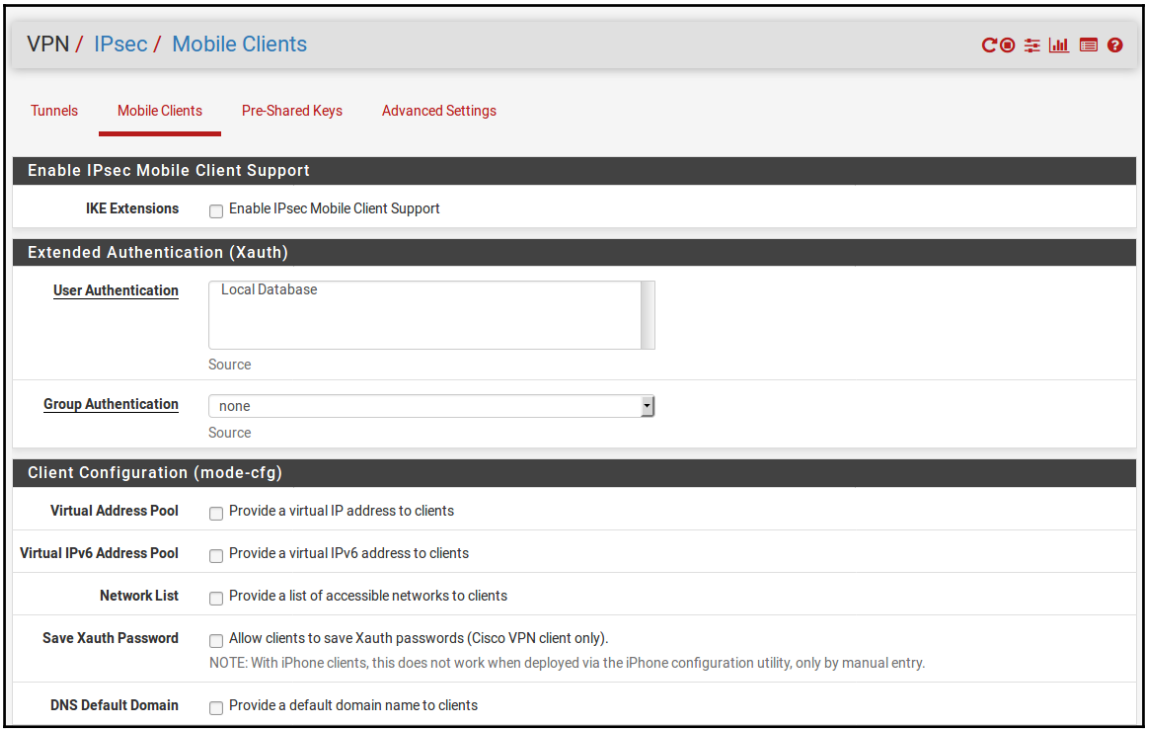


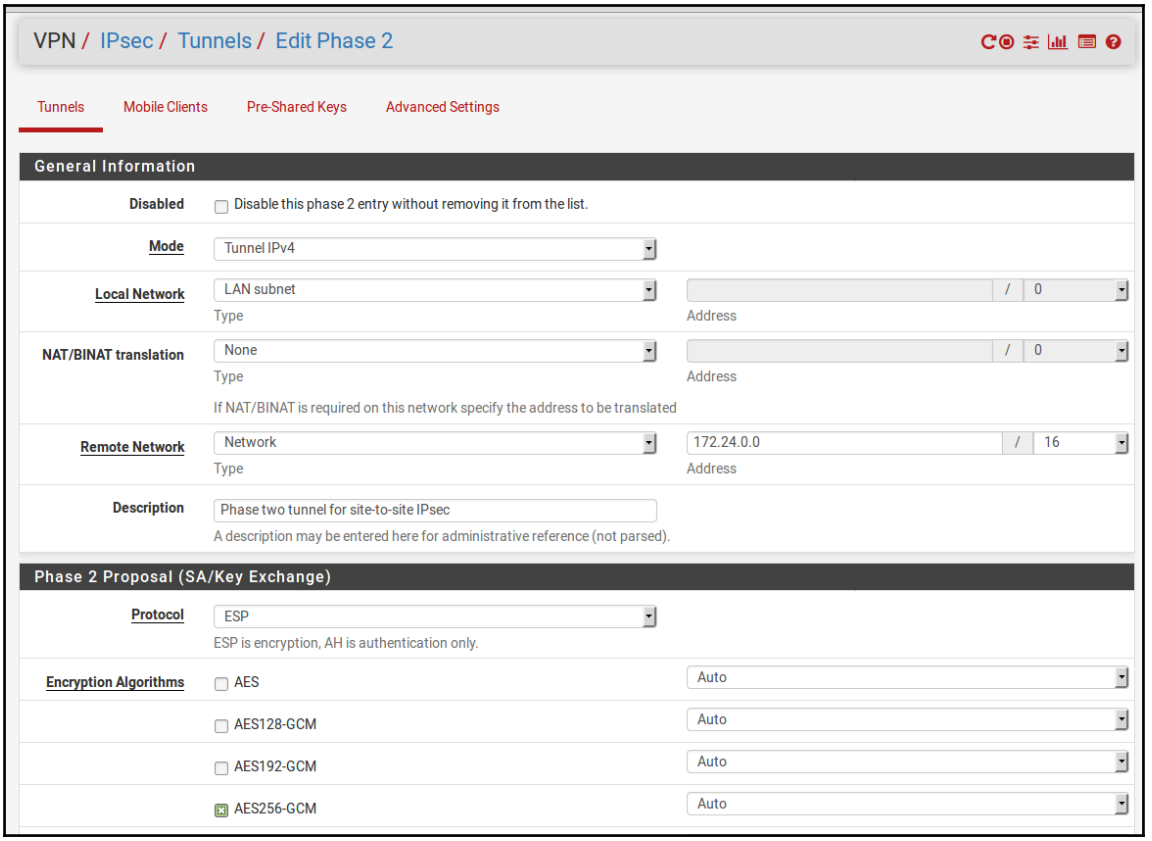
Chapter 7: Virtual Private Networks

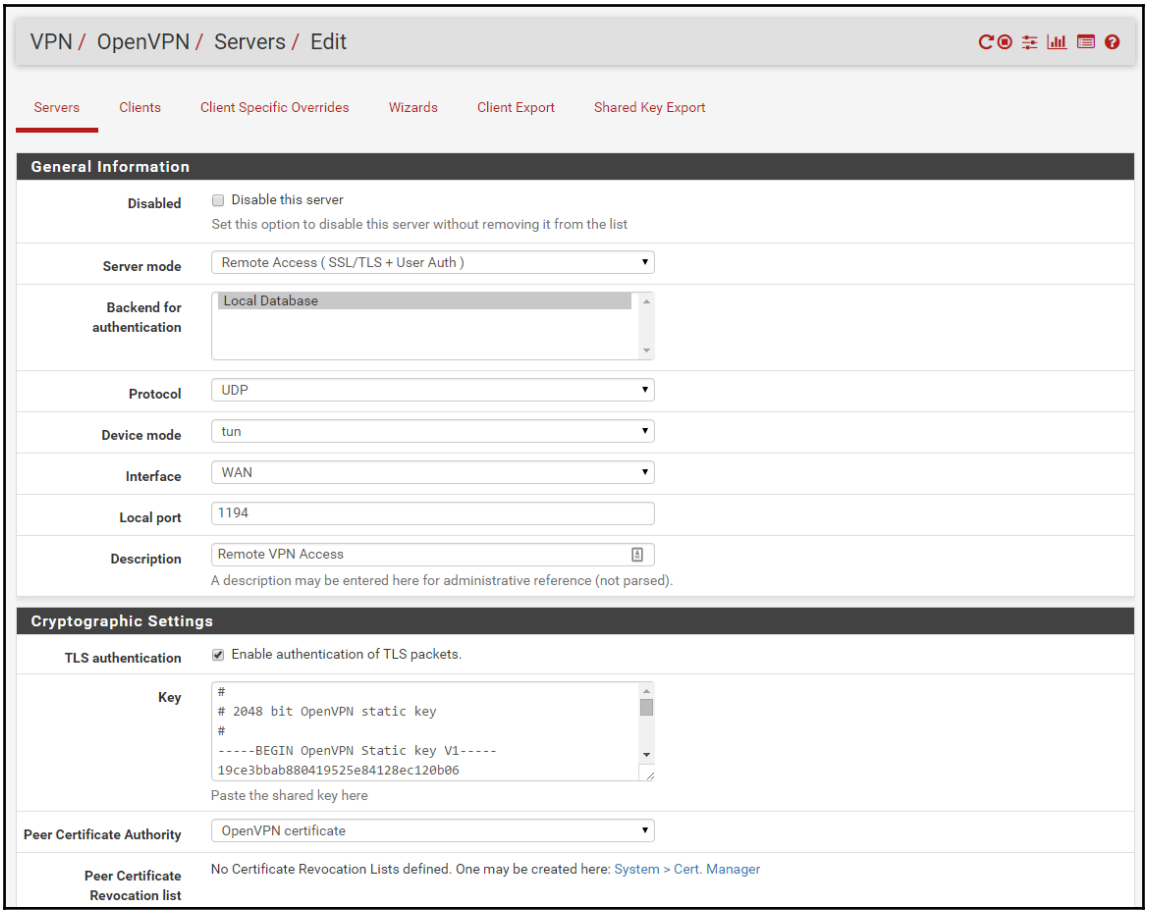
Shell Output - openvpn --show-ciphers

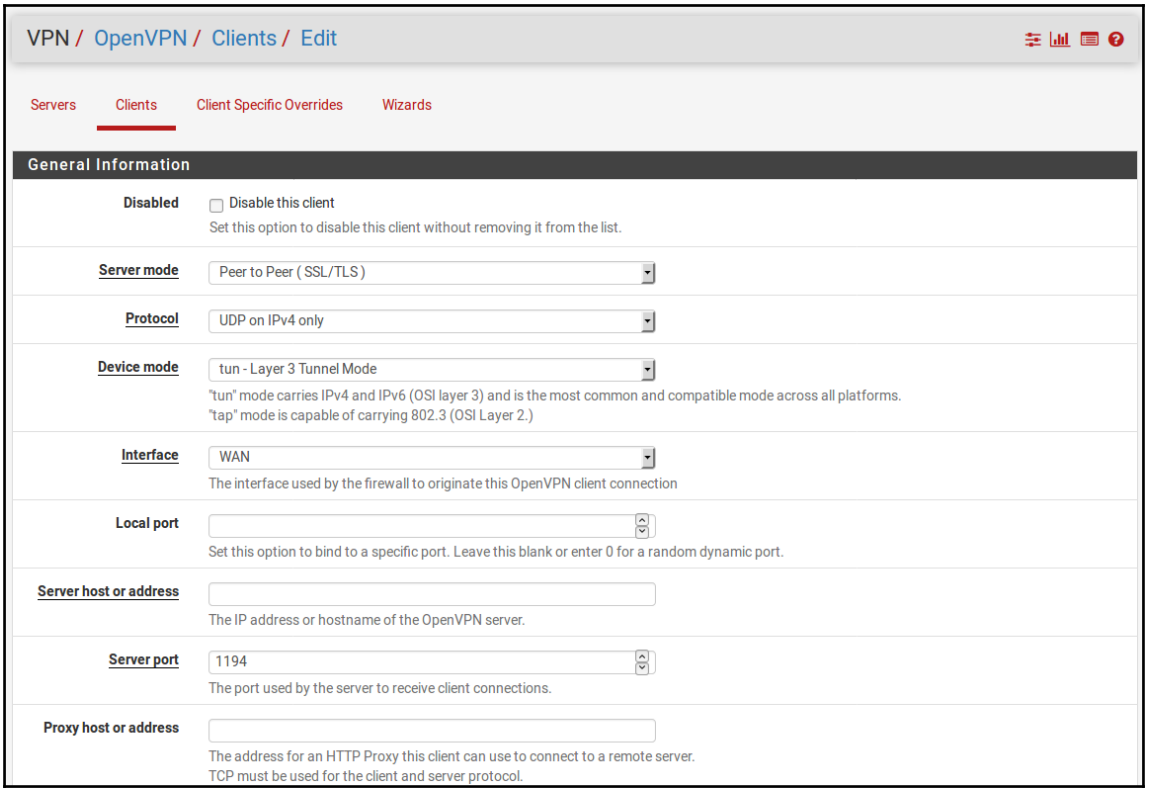
```
The following ciphers and cipher modes are available for use
with OpenVPN.  Each cipher shown below may be use as a
parameter to the --cipher option.  The default key size is
shown as well as whether or not it can be changed with the
--keysize directive.  Using a CBC or GCM mode is recommended.
In static key mode only CBC mode is allowed.

AES-128-CBC  (128 bit key, 128 bit block)
AES-128-CFB  (128 bit key, 128 bit block, TLS client/server mode only)
AES-128-CFB1  (128 bit key, 128 bit block, TLS client/server mode only)
AES-128-CFB8  (128 bit key, 128 bit block, TLS client/server mode only)
AES-128-GCM  (128 bit key, 128 bit block, TLS client/server mode only)
AES-128-OFB  (128 bit key, 128 bit block, TLS client/server mode only)
AES-192-CBC  (192 bit key, 128 bit block)
AES-192-CFB  (192 bit key, 128 bit block, TLS client/server mode only)
AES-192-CFB1  (192 bit key, 128 bit block, TLS client/server mode only)
AES-192-CFB8  (192 bit key, 128 bit block, TLS client/server mode only)
AES-192-GCM  (192 bit key, 128 bit block, TLS client/server mode only)
AES-192-OFB  (192 bit key, 128 bit block, TLS client/server mode only)
AES-256-CBC  (256 bit key, 128 bit block)
AES-256-CFB  (256 bit key, 128 bit block, TLS client/server mode only)
AES-256-CFB1  (256 bit key, 128 bit block, TLS client/server mode only)
AES-256-CFB8  (256 bit key, 128 bit block, TLS client/server mode only)
AES-256-GCM  (256 bit key, 128 bit block, TLS client/server mode only)
AES-256-OFB  (256 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-128-CBC  (128 bit key, 128 bit block)
CAMELLIA-128-CFB  (128 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-128-CFB1  (128 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-128-CFB8  (128 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-128-OFB  (128 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-192-CBC  (192 bit key, 128 bit block)
CAMELLIA-192-CFB  (192 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-192-CFB1  (192 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-192-CFB8  (192 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-192-OFB  (192 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-256-CBC  (256 bit key, 128 bit block)
CAMELLIA-256-CFB  (256 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-256-CFB1  (256 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-256-CFB8  (256 bit key, 128 bit block, TLS client/server mode only)
CAMELLIA-256-OFB  (256 bit key, 128 bit block, TLS client/server mode only)
SEED-CBC  (128 bit key, 128 bit block)
```

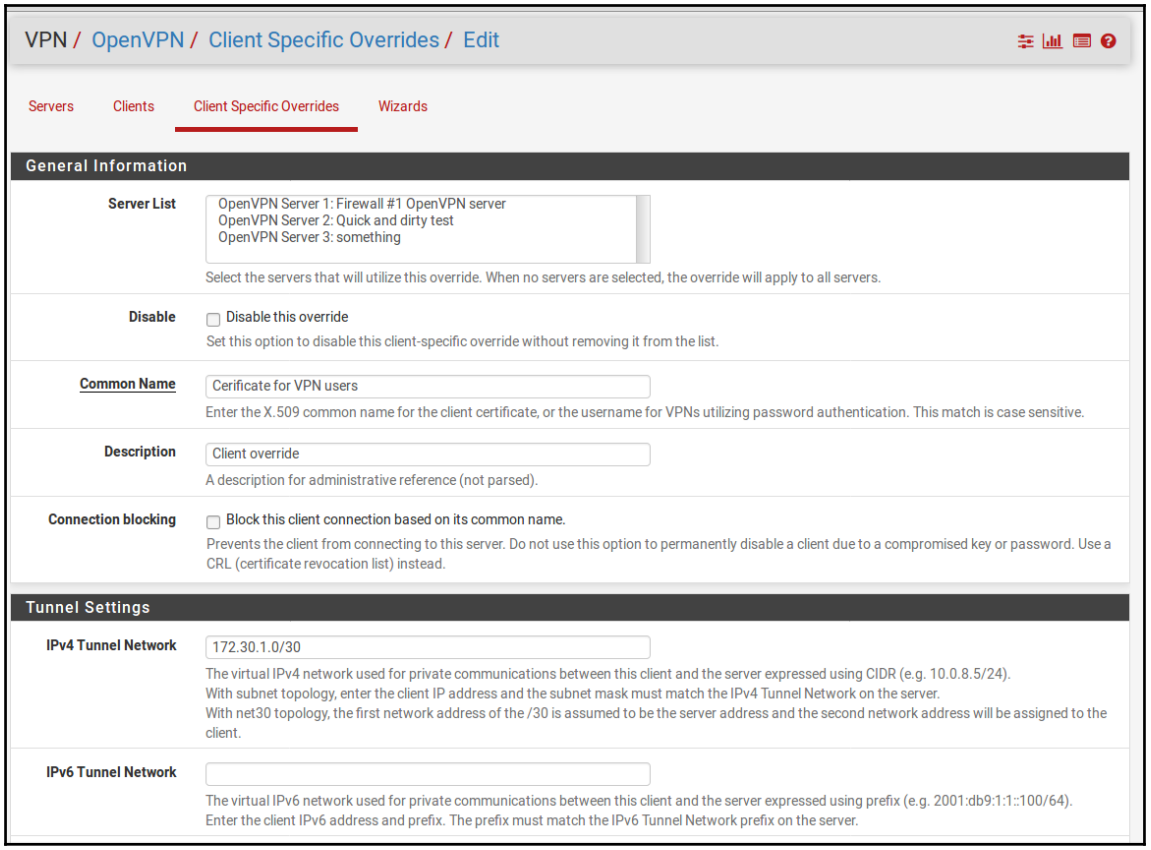

VPN / IPsec / Tunnels / Edit Phase 1
Tunnels
Mobile Clients
Pre-Shared Keys
Advanced Settings
General Information
Disabled
Set this option to disable this phase1 without removing it from the list.
Key Exchange version
V1
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when 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.

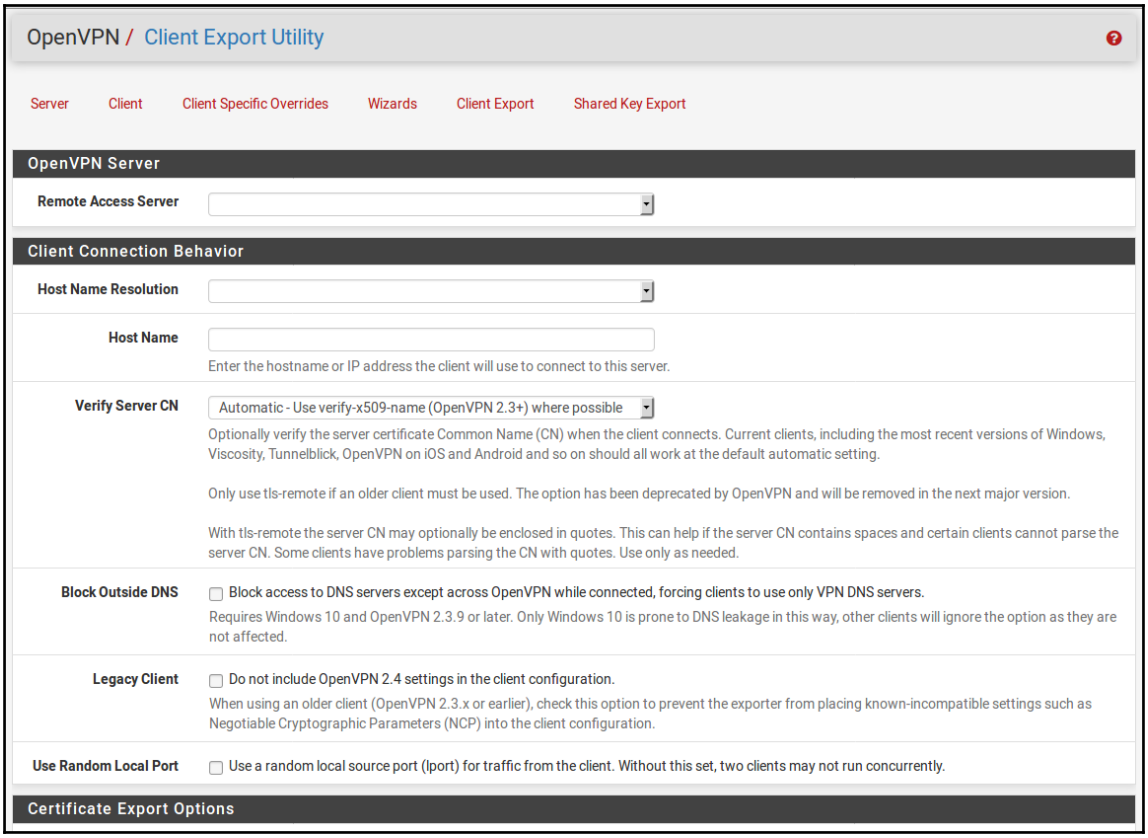

VPN / IPsec / Mobile Clients
Tunnels
Mobile Clients
Pre-Shared Keys
Advanced Settings
Enable IPsec Mobile Client Support
IKE Extensions
Enable IPsec Mobile Client Support
Extended Authentication (Xauth)
User Authentication
Local Database
Source
Group Authentication
none
Source
Client Configuration (mode-cfg)
Virtual Address Pool
Provide a virtual IP address to clients
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


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
LAN subnet
Type
Address
0
NAT/BINAT translation
None
Type
Address
If NAT/BINAT is required on this network specify the address to be translated
Remote Network
Network
Type
172.24.0.0
16
Address
Description
Phase two tunnel for site-to-site IPsec
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
AES128-GCM
AES192-GCM
AES256-GCM
Auto

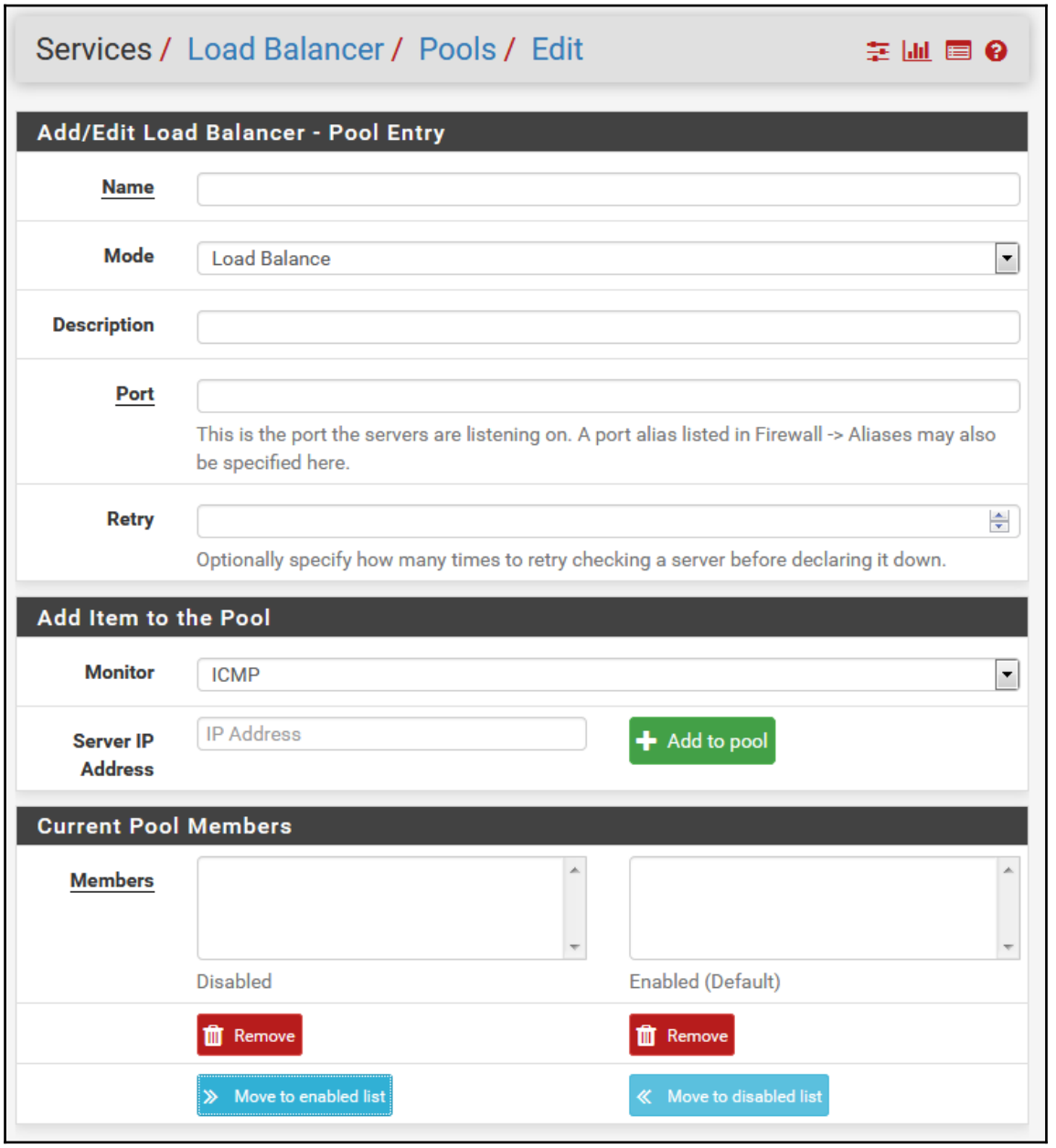

VPN / OpenVPN / Servers / Edit
Servers
Clients
Client Specific Overrides
Wizards
Client Export
Shared Key Export
General Information
Disabled
Disable this server
Set this option to disable this server without removing it from the list
Server mode
Remote Access (SSL/TLS + User Auth)
Backend for authentication
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


VPN / OpenVPN / Clients / Edit
Servers
Clients
Client Specific Overrides
Wizards
General Information
Disabled
Disable this client
Set this option to disable this client without removing it from the list.
Server mode
Peer to Peer (SSL/TLS)
Protocol
UDP on IPv4 only
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Interface
WAN
The interface used by the firewall to originate this OpenVPN client connection
Local port
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
Server host or address
The IP address or hostname of the OpenVPN server.
Server port
1194
The port used by the server to receive client connections.
Proxy host or address
The address for an HTTP Proxy this client can use to connect to a remote server.
TCP must be used for the client and server protocol.

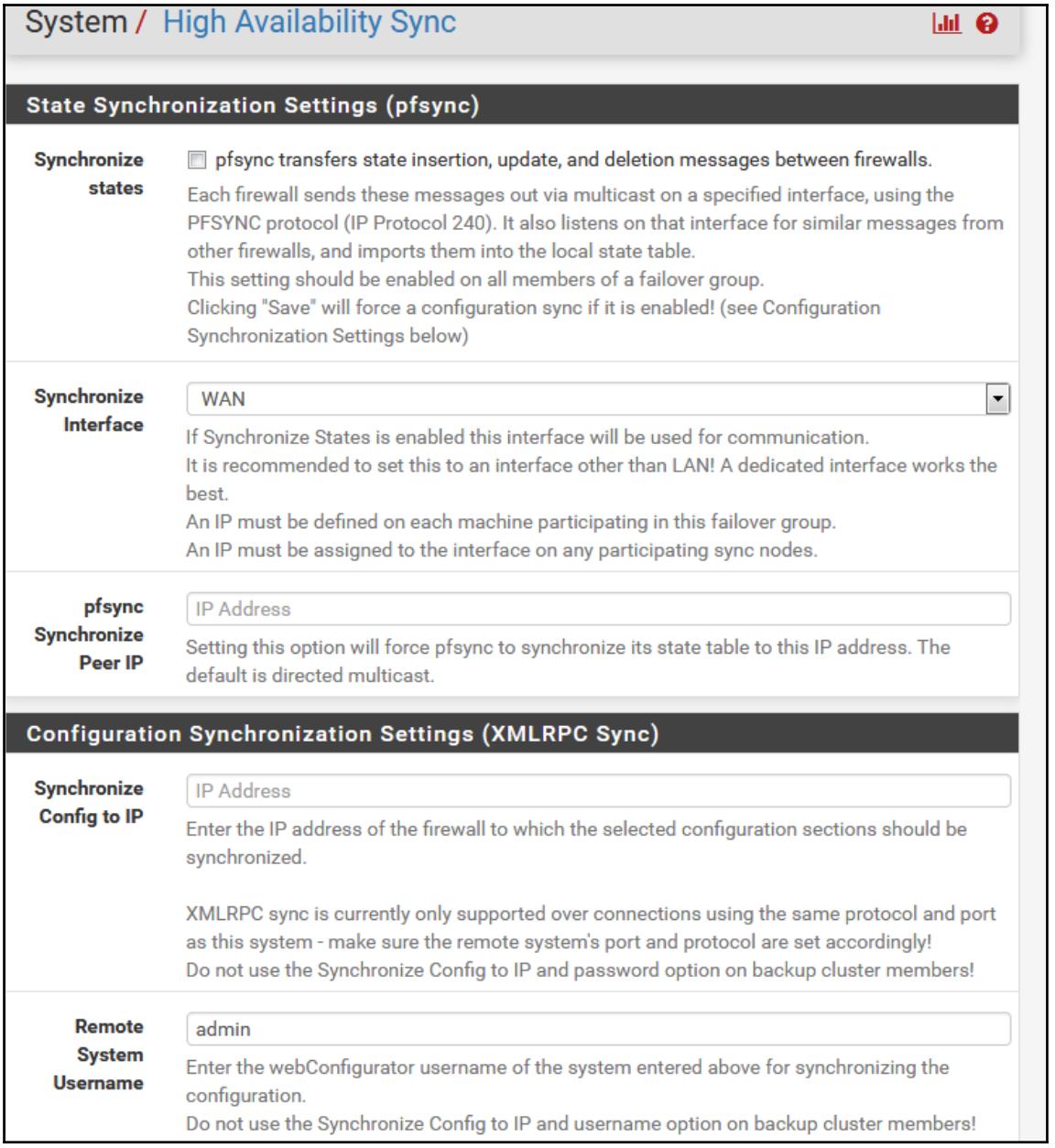

VPN / OpenVPN / Client Specific Overrides / Edit
Servers
Clients
Client Specific Overrides
Wizards
General Information
Server List
OpenVPN Server 1: Firewall #1 OpenVPN server
OpenVPN Server 2: Quick and dirty test
OpenVPN Server 3: something
Select the servers that will utilize this override. When no servers are selected, the override will apply to all servers.
Disable
Disable this override
Set this option to disable this client-specific override without removing it from the list.
Common Name
Cerificate for VPN users
Enter the X.509 common name for the client certificate, or the username for VPNs utilizing password authentication. This match is case sensitive.
Description
Client override
A description for administrative reference (not parsed).
Connection blocking
Block this client connection based on its common name.
Prevents the client from connecting to this server. Do not use this option to permanently disable a client due to a compromised key or password. Use a CRL (certificate revocation list) instead.
Tunnel Settings
IPv4 Tunnel Network
172.30.1.0/30
The virtual IPv4 network used for private communications between this client and the server expressed using CIDR (e.g. 10.0.8.5/24).
With subnet topology, enter the client IP address and the subnet mask must match the IPv4 Tunnel Network on the server.
With net30 topology, the first network address of the /30 is assumed to be the server address and the second network address will be assigned to the client.
IPv6 Tunnel Network
The virtual IPv6 network used for private communications between this client and the server expressed using prefix (e.g. 2001:db9:1:1::100/64).
Enter the client IPv6 address and prefix. The prefix must match the IPv6 Tunnel Network prefix on the server.


OpenVPN / Client Export Utility
Server
Client
Client Specific Overrides
Wizards
Client Export
Shared Key Export
OpenVPN Server
Remote Access Server
Client Connection Behavior
Host Name Resolution
Host Name
Enter the hostname or IP address the client will use to connect to this server.
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.
Block Outside DNS
Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Legacy Client
Do not include OpenVPN 2.4 settings in the client configuration.
When using an older client (OpenVPN 2.3.x or earlier), check this option to prevent the exporter from placing known-incompatible settings such as Negotiable Cryptographic Parameters (NCP) into the client configuration.
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

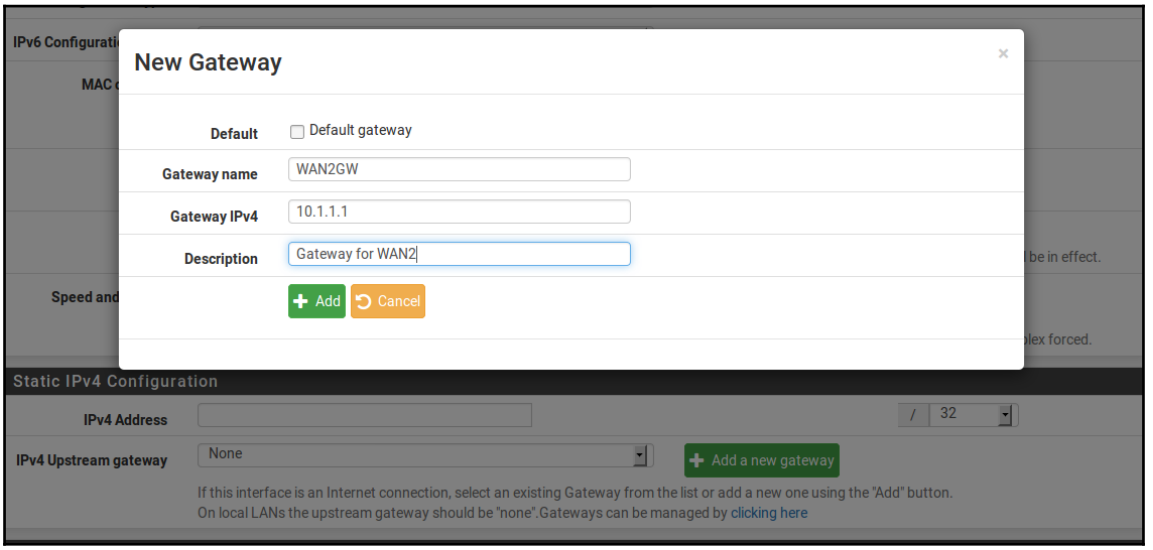
Chapter 8: Redundancy and High Availability

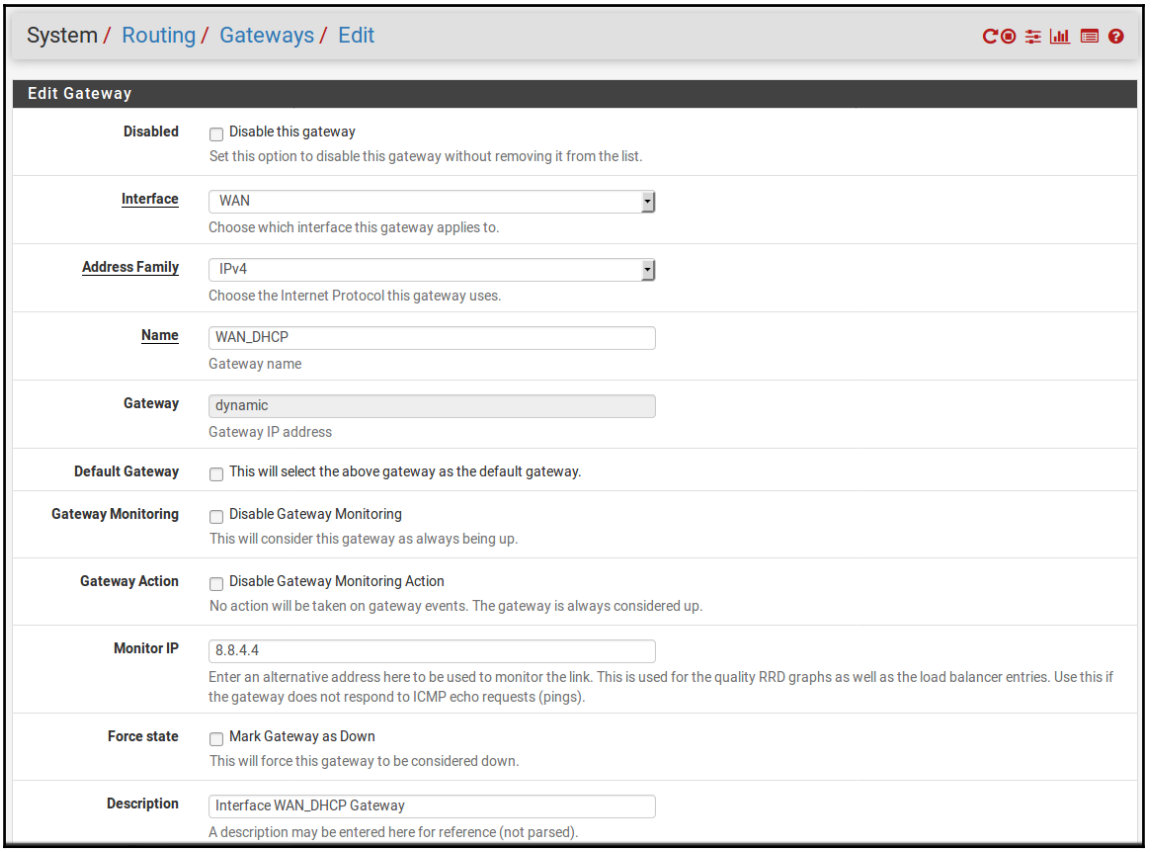


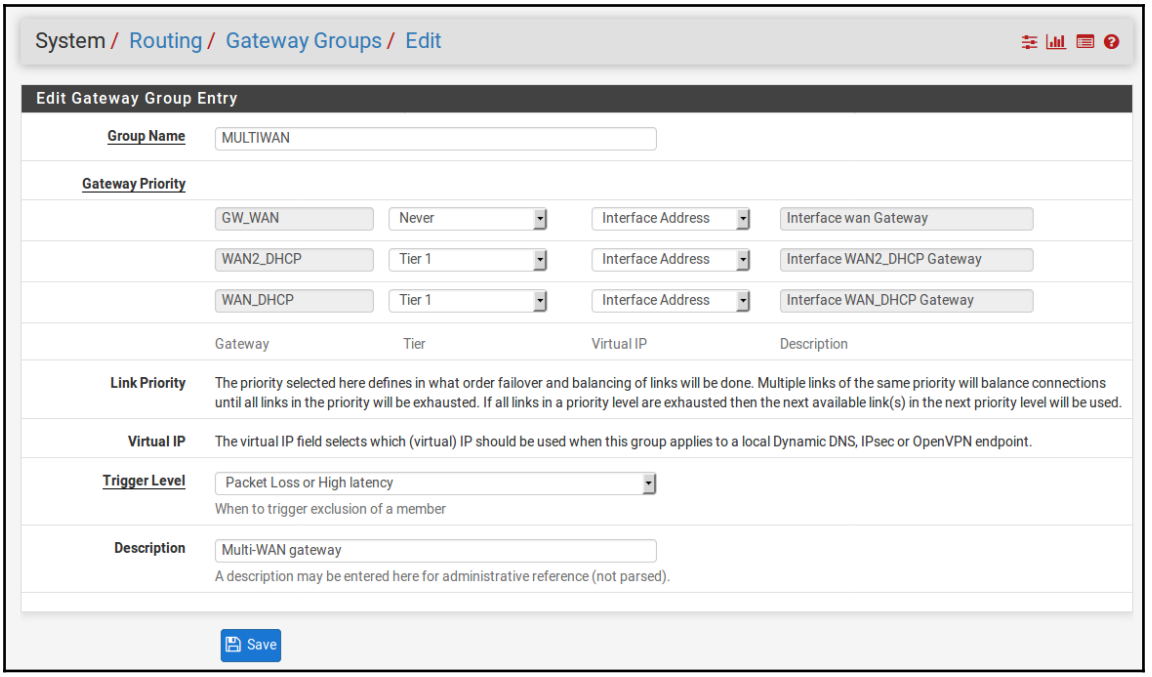
May 23 20:40:31	check_reload_status: Syncing firewall
May 23 20:40:33	php-fpm[42315]: /rc.filter_synchronize: Beginning XMLRPC sync to http://192.168.4.4:80.
May 23 20:40:40	php-fpm[42315]: /rc.filter_synchronize: XMLRPC sync successfully completed with http://192.168.4.4:80.
May 23 20:40:41	check_reload_status: 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...

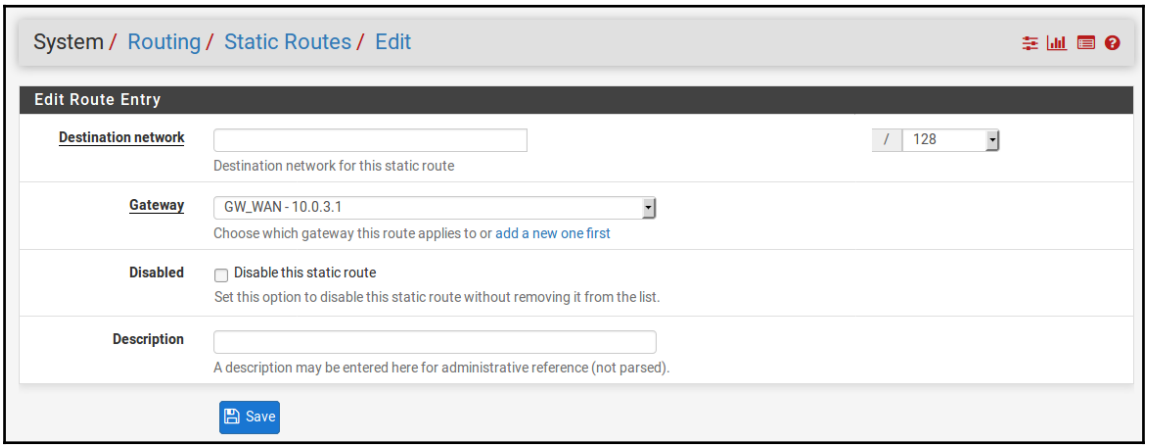

System / High Availability Sync
State Synchronization Settings (pfsync)
Synchronize states
pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface
WAN
If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.
pfsync Synchronize Peer IP
IP Address
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.
Configuration Synchronization Settings (XMLRPC Sync)
Synchronize Config to IP
IP Address
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!
Remote System Username
admin
Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Chapter 9: Multiple WANs

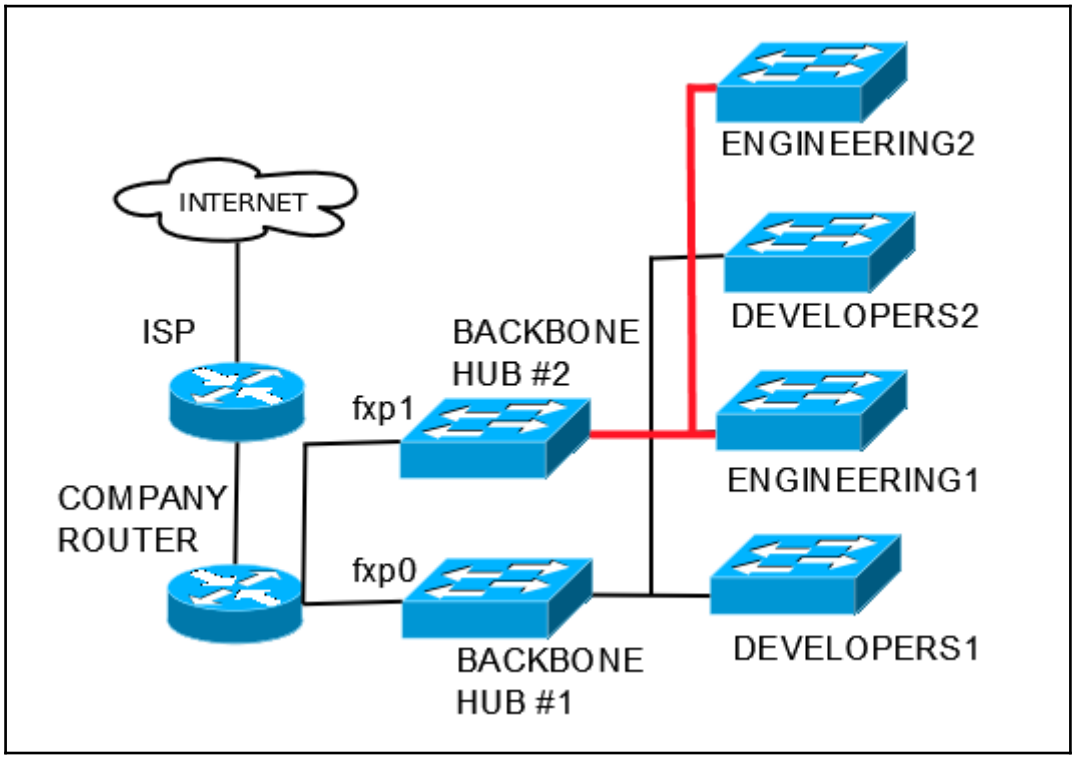


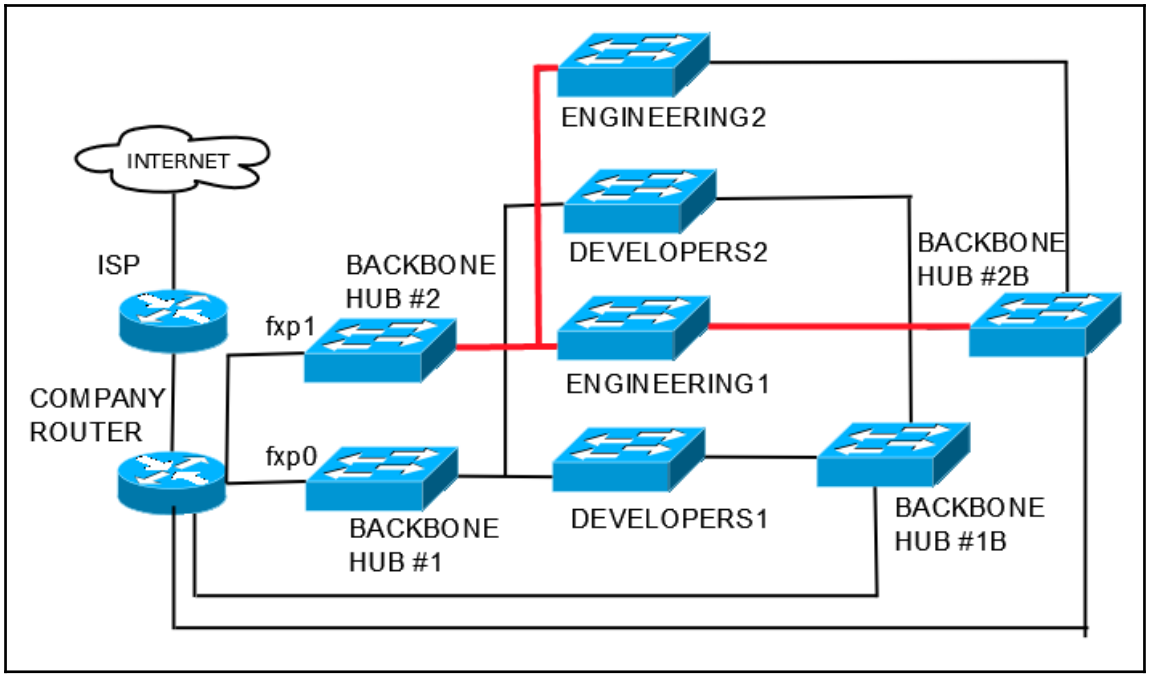

System / Routing / Gateways / Edit
Edit Gateway
Disabled
Disable this gateway
Set this option to disable this gateway without removing it from the list.
Interface
WAN
Choose which interface this gateway applies to.
Address Family
IPv4
Choose the Internet Protocol this gateway uses.
Name
WAN_DHCP
Gateway name
Gateway
dynamic
Gateway IP address
Default Gateway
This will select the above gateway as the default gateway.
Gateway Monitoring
Disable Gateway Monitoring
This will consider this gateway as always being up.
Gateway Action
Disable Gateway Monitoring Action
No action will be taken on gateway events. The gateway is always considered up.
Monitor IP
8.8.4.4
Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).
Force state
Mark Gateway as Down
This will force this gateway to be considered down.
Description
Interface WAN_DHCP Gateway
A description may be entered here for reference (not parsed).

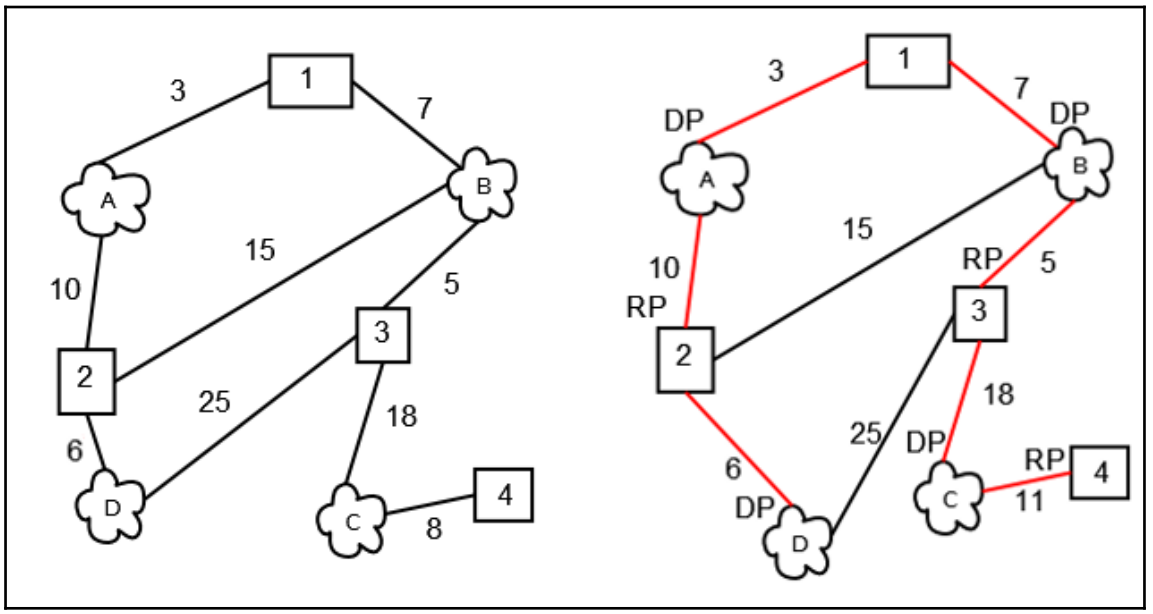

System / Routing / Gateway Groups / Edit
Edit Gateway Group Entry
Group Name
MULTIWAN
Gateway Priority
GW_WAN
Never
Interface Address
Interface wan Gateway
WAN2_DHCP
Tier 1
Interface Address
Interface WAN2_DHCP Gateway
WAN_DHCP
Tier 1
Interface Address
Interface WAN_DHCP Gateway
Gateway
Tier
Virtual IP
Description
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
Packet Loss or High latency
When to trigger exclusion of a member
Description
Multi-WAN gateway
A description may be entered here for administrative reference (not parsed).
Save

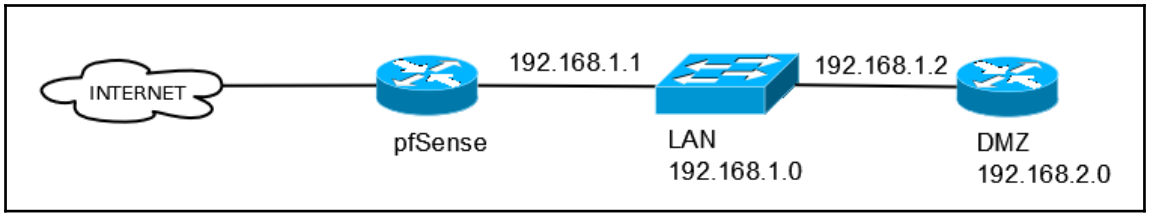

System / Routing / Static Routes / Edit
Edit Route Entry
Destination network
/ 128
Destination network for this static route
Gateway
GW_WAN - 10.0.3.1
Choose which gateway this route applies to or add a new one first
Disabled
Disable this static route
Set this option to disable this static route without removing it from the list.
Description
A description may be entered here for administrative reference (not parsed).
Save

Chapter 10: Routing and Bridging




ENGINEERING2
INTERNET
DEVELOPERS2
BACKBONE
HUB #2B
ISP
BACKBONE
HUB #2
fxp1
ENGINEERING1
COMPANY
ROUTER
fxp0
DEVELOPERS1
BACKBONE
HUB #1B
BACKBONE
HUB #1


1
3
7
A
B
15
10
5
3
2
25
18
6
D
C
4
8
1
3
7
DP
DP
A
B
15
10
RP
RP
5
3
2
18
25
DP
6
DP
RP
4
D
C
11


INTERNET
192.168.1.1
192.168.1.2
pfSense
LAN
192.168.1.0
DMZ
192.168.2.0

Chapter 11: Extending pfSense with Packages