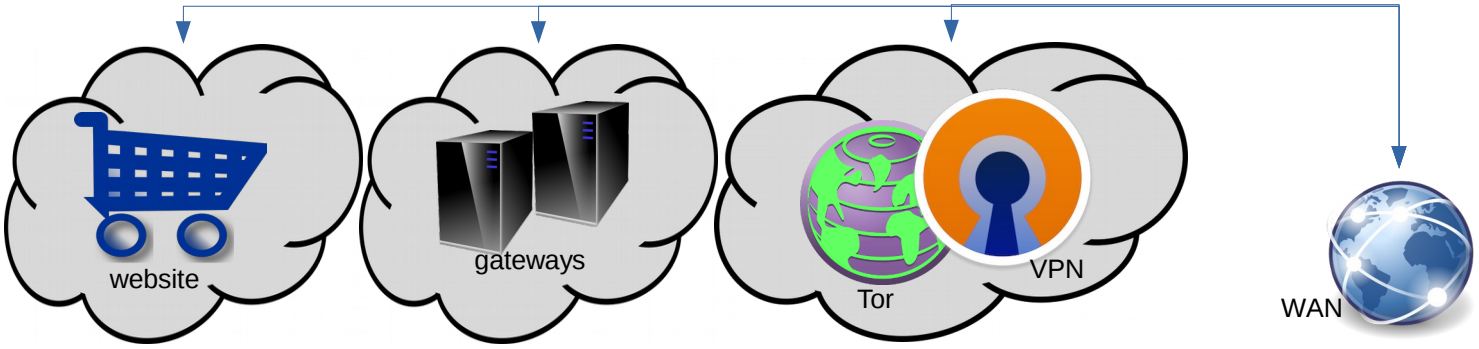
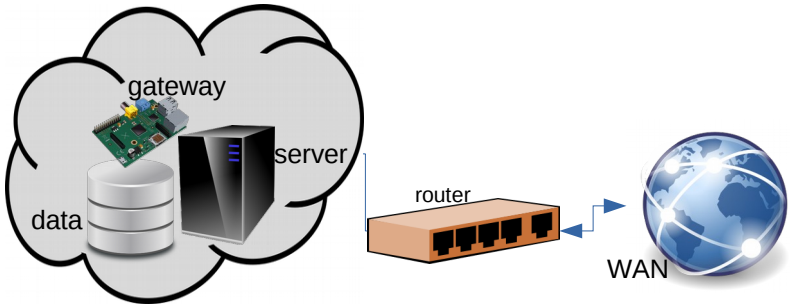
CoreAutoSSH is a portable administrative tool to access logical networks of computers through SSH tunnels across redundant physical networks.

A script file, an “ops” file, and credentials files are the only requirements. There is no requirement for, and no conflict from, system-wide installation, specialized network interfaces, or reserved IP ranges.

As a automatic last resort, the configuration can be set to access computers through a Tor/VPN address. As long as a WAN connection is available, the computer remains reachable.

CoreAutoSSH is an efficient means to access all computers in this complete network.

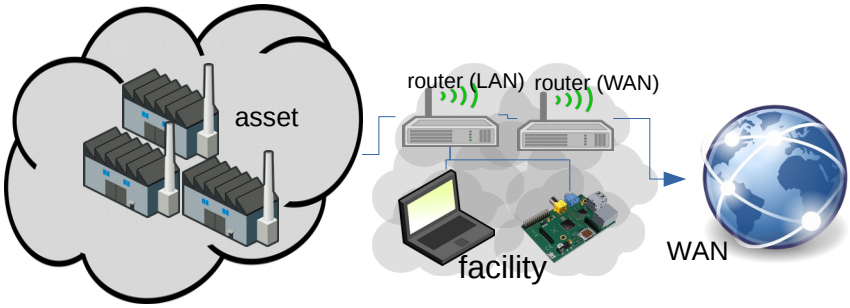




Gateway, Data, Server

Directly accessible computers. Likely just a single computer, or managed hosting.

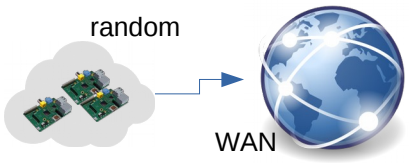
Typical use cases.
*) Default jump host for SSH, OpenVPN, etc (gateway).
*) Random data collection, mySQL cluster, etc (data).
*) Internal web pages, files (server).



Asset, Facility

Expensive capital equipment, on-site.
Often, assets are factory equipment (eg. 3D printers), facility is a “LapRack” - Laptop, RasPi, routers.

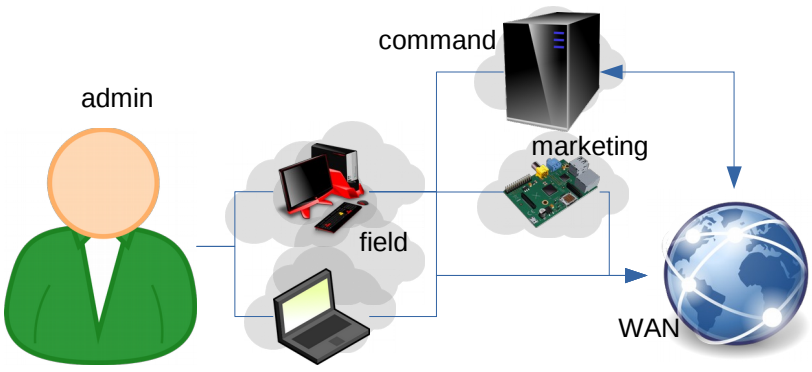
Typical use cases.
*) Remotely technical support.
*) Internal web pages, files.
*) Tunneling of web interfaces to public IP/ports for use without SSH client or VPN client.



Random

Inexpensive, possibly low-power, embedded. Usually a remote sensor or actuator.
Cannot maintain a continuous SSH or VPN tunnel, or does not require administration.

Typically will check in with a public web page, uploading data, downloading commands.
May include a command to connect SSH to a public IP/port for administration.



Field, Command, Marketing

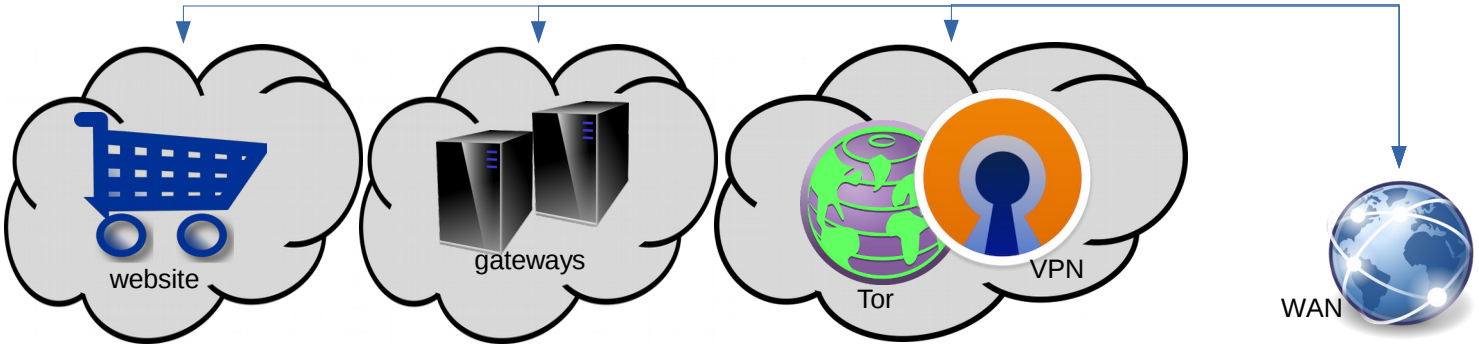
Administrator physical field computers (eg. laptop, desktop), command computer with public IP/port, and marketing computer connected continuously.

Typical use cases.
*) Field – a laptop or desktop with the software to access organization’s resources and provide technical support.
*) Command – port forwarding from public IP/port to field computers. An endpoint for reverse tunnels from random computers.
*) Marketing – Organization specific email, instant messaging.

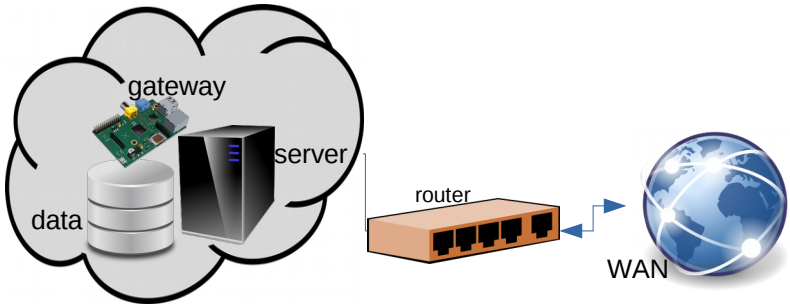
Network – Logical

netName=default

netPrefix=dflt
netStart=20000
offset=+100



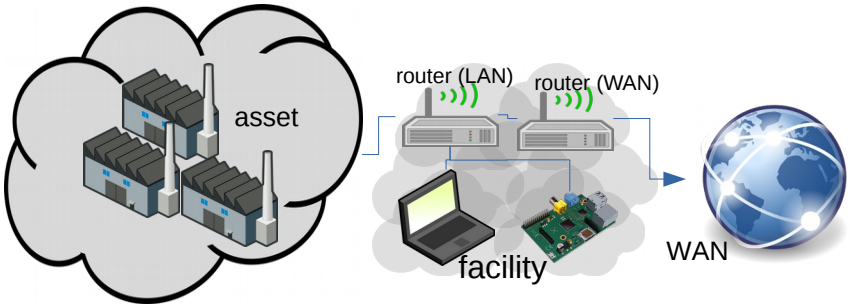
Gateway, Data, Server



gateway
gw-"$netName"
spare-"$netName"
data
data-"$netName" "$netPrefix"**d** 20008

server
server-"$netName" "$netPrefix"**srv** 20009

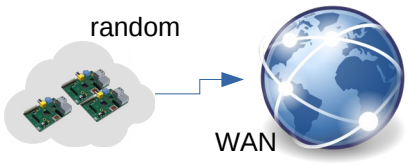
Asset, Facility



asset
a1-"$netName" a1 20010[+"$offset"]

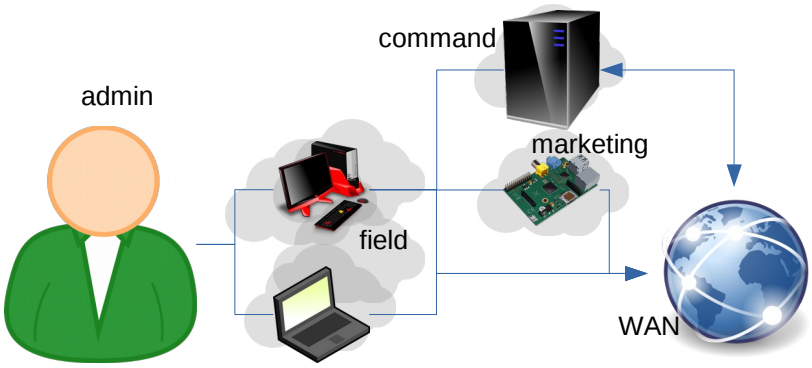
facility
pc-"$netName" "$netPrefix"**pc** 20001
raspi-"$netName" "$netPrefix"**rpi** 20002[+"$offset]
lan-"$netName" "$netPrefix"**l**
wan-"$netName" "$netPrefix"**w**

Random



https://example.com/random/report.php?name1=value1&name2=value2

Field, Command, Marketing



admin
example

command
example-cmd-"$netName" "exmp"**c** 20039

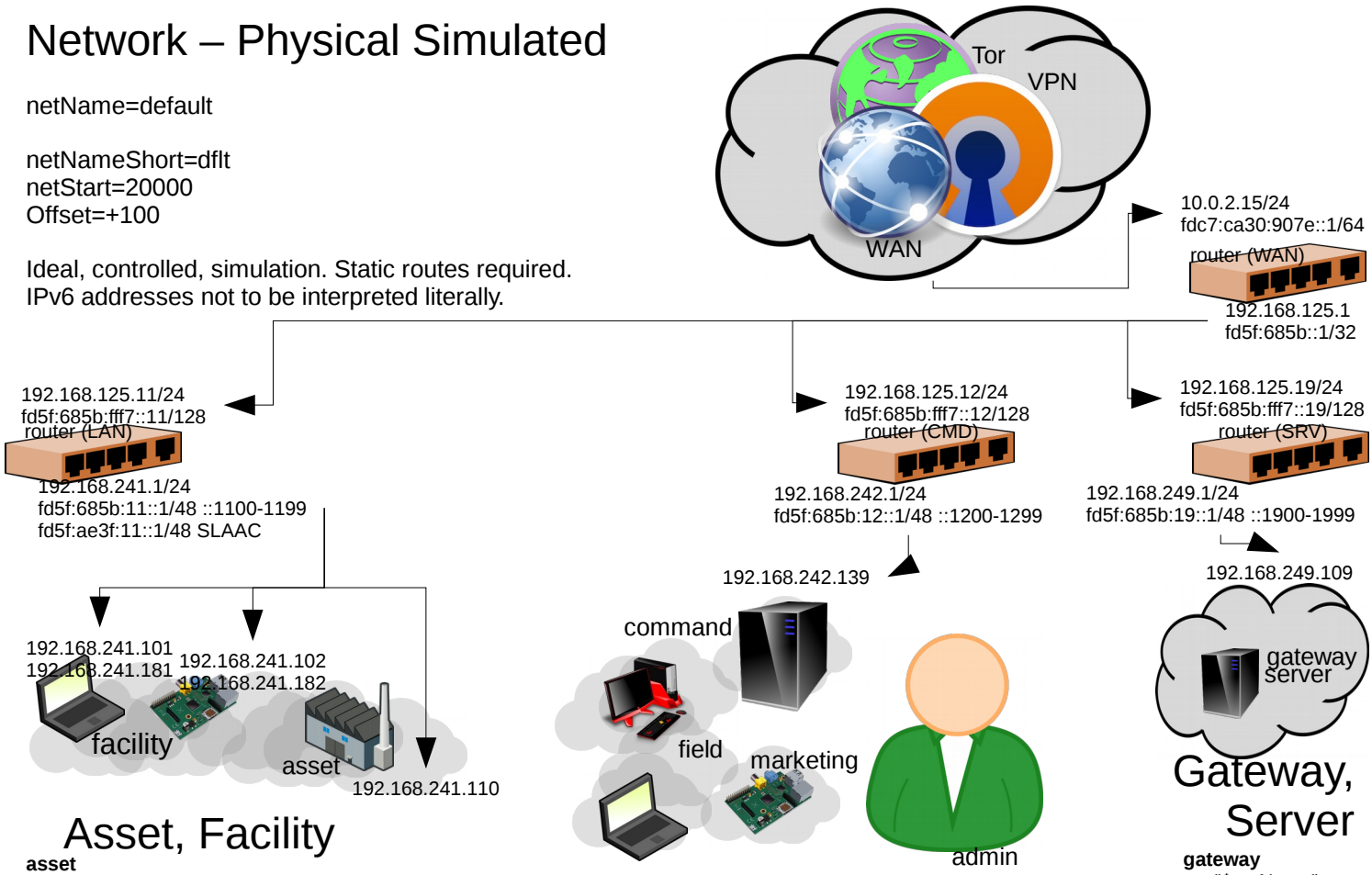
field
example-desk-"$netName" "exmp"**d** 20030
example-lap-"$netName" "exmp"**l** 20031
example-mrk-"$netName" "exmp"**m** 20035

Network – Physical Simulated

netName=default

netNameShort=dflt
netStart=20000
Offset=+100

Ideal, controlled, simulation. Static routes required.
IPv6 addresses not to be interpreted literally.



Asset, Facility

asset

a1-"$netName"	a1	20010["$offset"]
a2-"$netName"	a2	20011["$offset"]

facility

pc-"$netName"	"$netPrefix"**pc**	20001
raspi-"$netName"	"$netPrefix"**rpi**	20002["$offset]
lan-"$netName"	"$netPrefix"**l**	
wan-"$netName"	"$netPrefix"**w**	

Field, Command, Marketing

admin
example

command

example-cmd-"$netName"	"exmp"**c**	20039

field

example-desk-"$netName"	"exmp"**d**	20030
example-lap-"$netName"	"exmp"**l**	20031
example-mrk-"$netName"	"exmp"**m**	20035

Gateway, Server

gateway
gw-"$netName"

server
server-"$netName"
"$netPrefix"**srv**
20009

Typically, a short standard password is used.
root/6ddk0m
admin/6ddk0m
gateway/6ddk0m

commonadmin/6ddk0m
user/6ddk0m

For convenience, Router "WAN", IP 10.0.2.15 and/or 192.168.125.1, typically will accept and forward ports.
WARNING: Do not use ports >35500 . See "ubiquitous_bash.sh", "_get_ssh_external()" .

:30022	Router "WAN" SSH
:30043	Router "WAN" HTTPS
:30122	Router "LAN" SSH
:30143	Router "LAN" HTTPS
:30222	Router "CMD" SSH
:30243	Router "CMD" HTTPS
:30922	Router "SRV" SSH
:30943	Router "SRV" HTTPS
:20009	Server SSH

For convenience, Router "LAN", typically will accept and forward ports.

:30122	Router "LAN" SSH
:30143	Router "LAN" HTTPS

For convenience, Router "CMD", typically will accept and forward ports.

:30222	Router "CMD" SSH
:30243	Router "CMD" HTTPS

For convenience, Router "SRV", typically will accept and forward ports.

:30922	Router "SRV" SSH
:30943	Router "SRV" HTTPS
:20009	Server SSH

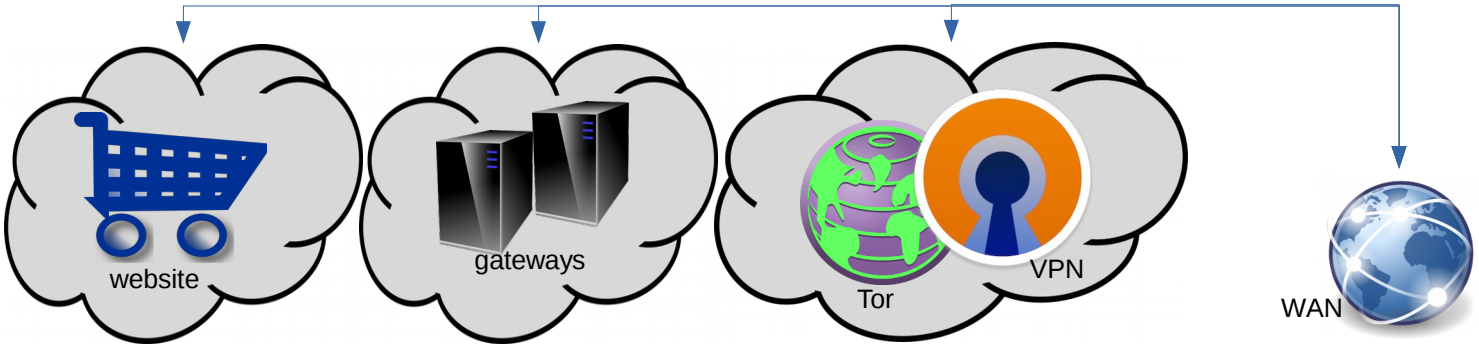
Typically all NAT will be bypassed through gateway server available.

10.0.2.15	:20009	Server SSH
192.168.125.1	:20009	Server SSH
192.168.125.19	:20009	Server SSH
192.168.249.1	:20009	Server SSH

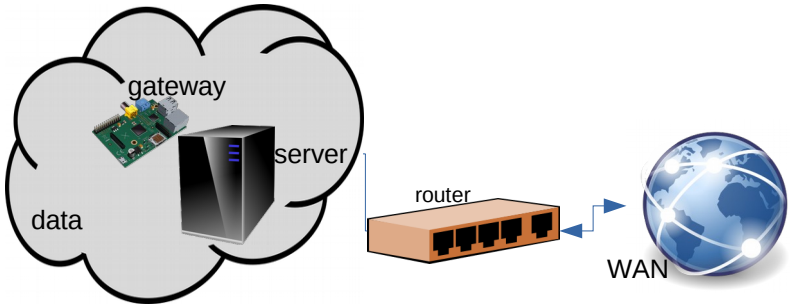
Network – Logical Simulated

netName=default

netPrefix=dflt
netStart=20000
offset=+100



Gateway, Data, Server



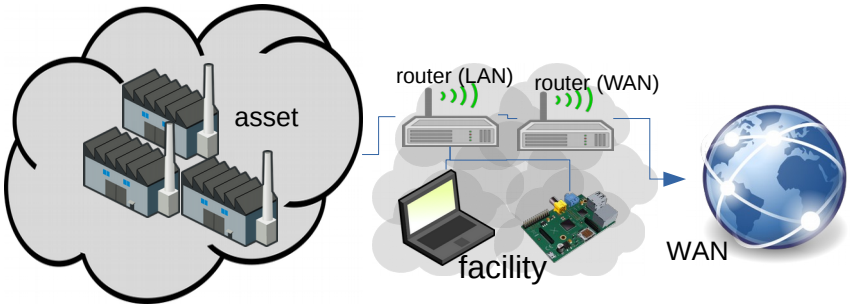
gateway
gw-"$netName"

data

server

server-"$netName"	"$netPrefix"**srv**	20009

Asset, Facility



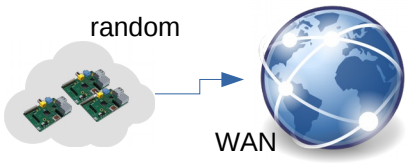
asset

a1-"$netName"	a1	20010[+"$offset"]
a2-"$netName"	a2	20011[+"$offset"]

facility

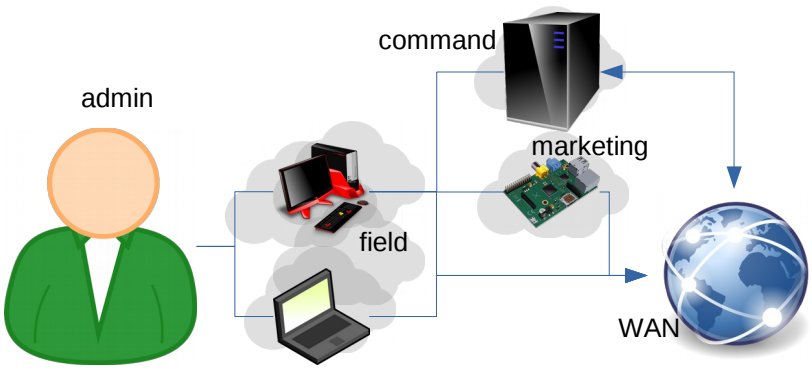
pc-"$netName"	"$netPrefix"**pc**	20001
raspi-"$netName"	"$netPrefix"**rpi**	20002[+"$offset]
lan-"$netName"	"$netPrefix"**l**	
wan-"$netName"	"$netPrefix"**w**	

Random



https://example.com/random/report.php?name1=value1&name2=value2

Field, Command, Marketing



admin
example

command

example-cmd-"$netName"	"exmp"**c**	20039

field

example-desk-"$netName"	"exmp"**d**	20030
example-lap-"$netName"	"exmp"**l**	20031
example-mrk-"$netName"	"exmp"**m**	20035

PFSense – IPv4, IPv6 (Simulated, WAN)

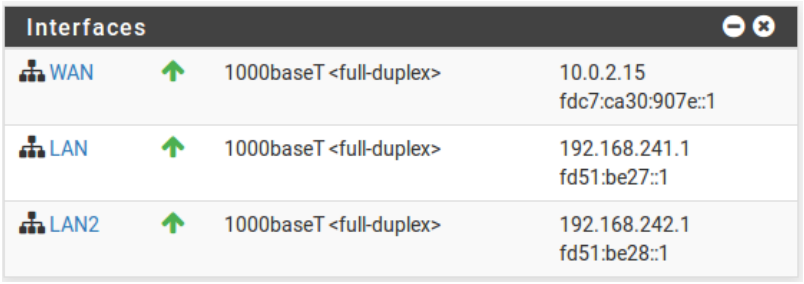
Configuration example only.
Addresses not to be interpreted literally.

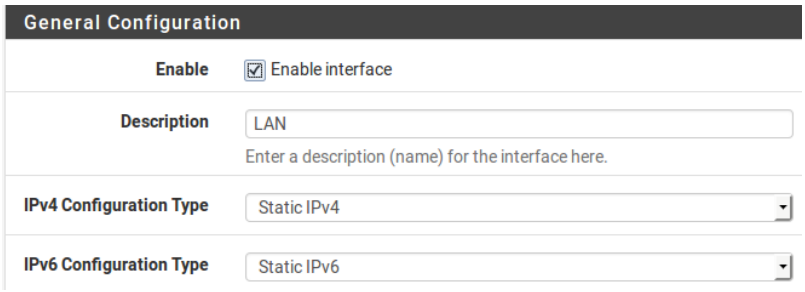
WAN (Simulated, bridge expected.)
10.0.2.15
fdc7:ca30:907e::1

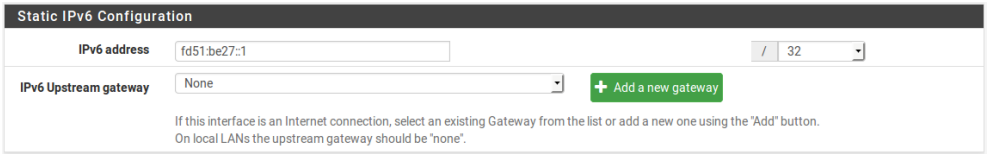
LAN1
192.168.241.1
fd51:be27::1

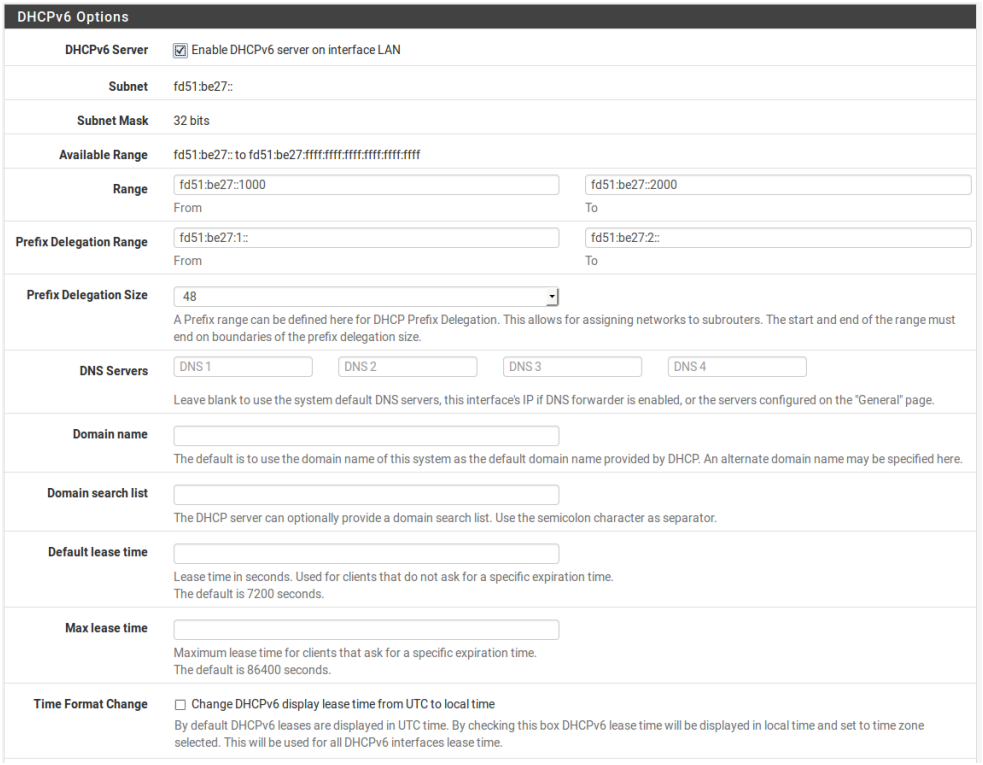
LAN2
192.168.242.1
fd51:be28::1

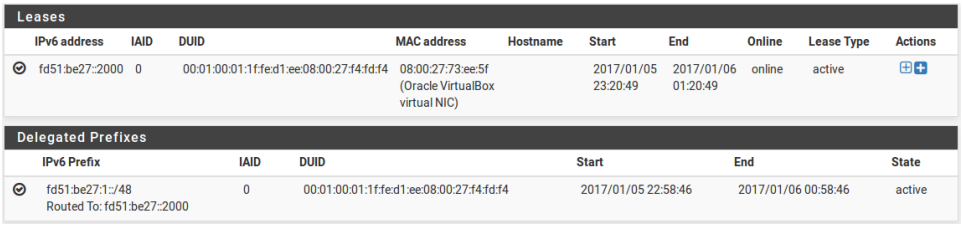
Static route example (if relevant).
network: fd5f:685b:11::/48
gateway: fdf5:685b:fff7::11











Success!
Client acquired a full /48 block for its subnet.

PFSense – IPv4, IPv6 (Simulated, LAN)

Configuration example only.
Addresses not to be interpreted literally.

WAN (simulated, NAT expected)
10.0.2.15
fdc7:ca30:907e::1

LAN1
192.168.241.1
fd51:be27::1

LAN2
192.168.242.1
fd51:be28::1

Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.241.12 fd51:be27::2000
LAN	↑	1000baseT <full-duplex>	192.168.1.1 fd51:be27:1:0:a00:27ff:fe9f:141d

General Configuration

Enable	☑ Enable interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	DHCP
IPv6 Configuration Type	DHCP6

DHCP6 Client Configuration

Options	☐ Advanced Configuration Use advanced DHCPv6 configuration options. ☐ Configuration Override Override the configuration from this file.
Use IPv4 connectivity as parent interface	☐ Request a IPv6 prefix/information through the IPv4 connectivity link
Request only an IPv6 prefix	☐ Only request an IPv6 prefix, do not request an IPv6 address
DHCPv6 Prefix Delegation size	48 The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP.
Send IPv6 prefix hint	☐ Send an IPv6 prefix hint to indicate the desired prefix size for delegation
Debug	☐ Start DHCP6 client in debug mode

General Configuration

Enable	☑ Enable interface
Description	LAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	Track Interface

Track IPv6 Interface

IPv6 Interface	WAN Selects the dynamic IPv6 WAN interface to track for configuration.
IPv6 Prefix ID	0 (**hexadecimal** from 0 to ffff)The value in this field is the (Delegated) IPv6 prefix ID.

DHCPv6 Options

DHCPv6 Server	☑ Enable DHCPv6 server on interface LAN
Subnet	Prefix Delegation
Subnet Mask	64 bits
Available Range	:: to ::ffff:ffff:ffff:ffff Prefix Delegation subnet will be appended to the beginning of the defined range
Range	::1000 From ::2000 To
Prefix Delegation Range	From To
Prefix Delegation Size	48 A Prefix range can be defined 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.
Domain name	The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain search list	The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default lease time	Lease time in seconds. Used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Max lease time	Maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Time Format Change	☐ Change DHCPv6 display lease time from UTC to local time By default DHCPv6 leases are displayed in UTC time. By checking this box DHCPv6 lease time will be displaye selected. This will be used for all DHCPv6 interfaces lease time.

Leases

IPv6 address	IAID	DUID	MAC address	Hostname	Start	End	Online	Lease Type	Actions
fd51:be27:1::2000	663741566	00:01:00:01:1f:ff:ee:cb:08:00:27:66:a2:4b	08:00:27:8f:e4:7e (Oracle VirtualBox virtual NIC)		2017/01/05 23:22:44	2017/01/06 01:22:44	online	active	

Delegated Prefixes

IPv6 Prefix	IAID	DUID	Start	End	State

Success!
Client computer has obtained an IPv6 address over DHCPv6, within the upstream prefix and client specified range.

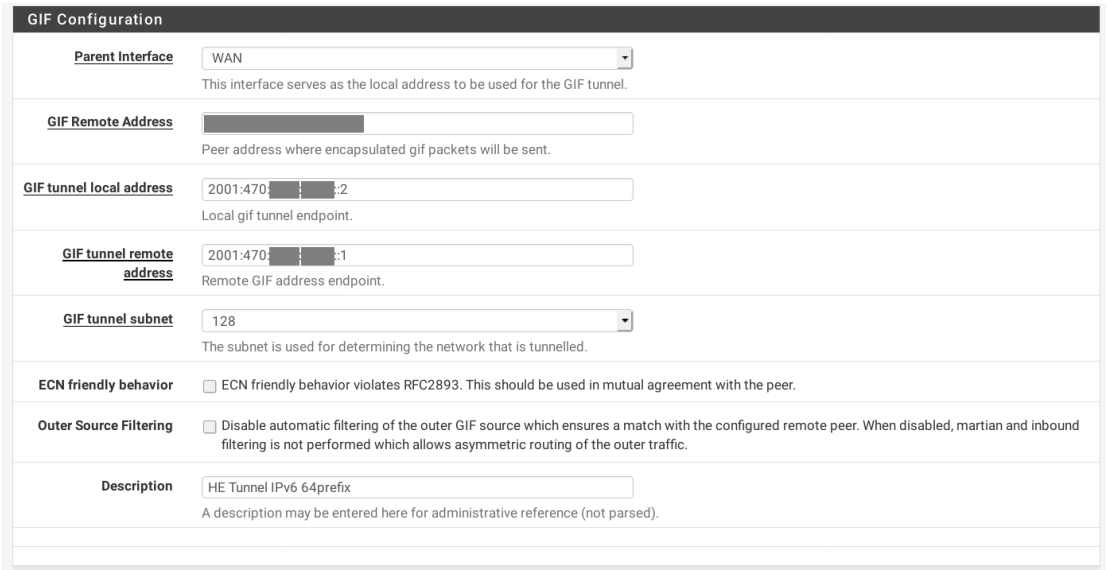
PFSense – IPv6 (Hurricane Electric)

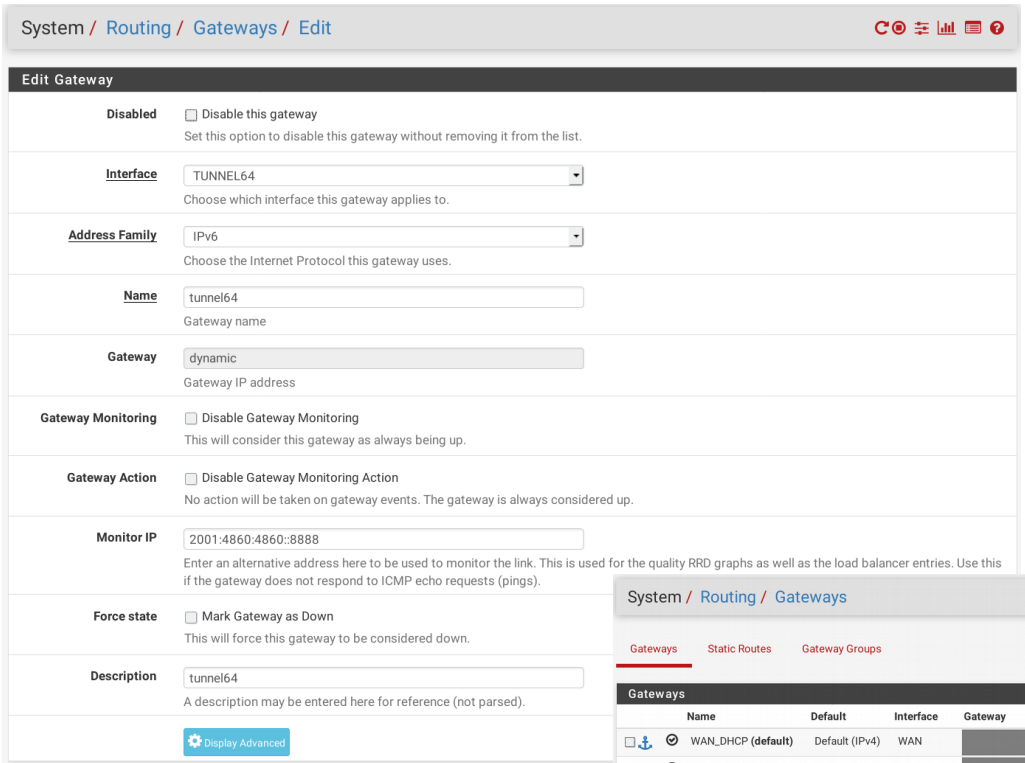
IPv6 Tunnel Endpoints

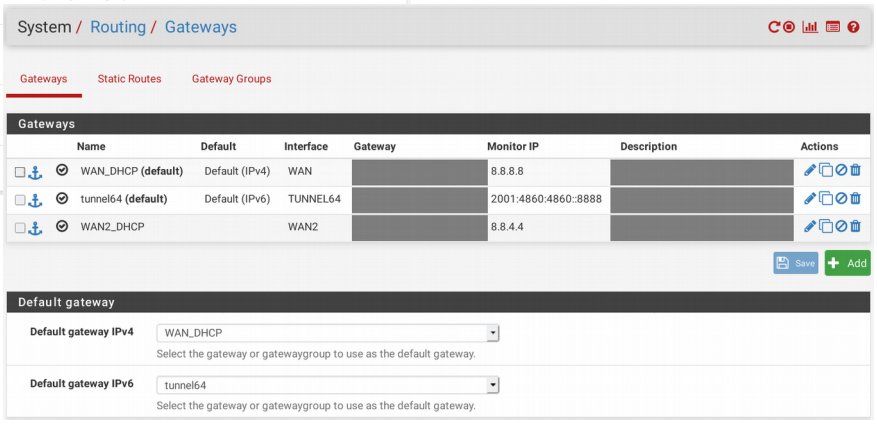
Server IPv4 Address:	<public IPv4>	
Server IPv6 Address:	<tunnel remote address>	2001:470:g:h::1/
Client IPv4 Address:	<public IPv4>	
Client IPv6 Address:	<tunnel local address>	2001:470:g:h::2

Routed IPv6 Prefixes

Routed /64:	2001:470:g:h::/64
Routed /48:	2001:470:i::/48 [X]







Interfaces / LAN ([redacted])

General Configuration

Enable ☑ Enable interface

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

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type Static IPv6

MAC Address 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 192.168.[redacted]:1 — 192.168.x.1 — / 24

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 area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

Static IPv6 Configuration

IPv6 address 2001:470:[redacted]:1 — 2001:470:i:x::1 — / 64

Use IPv4 connectivity as parent interface ☐ IPv6 will use the IPv4 connectivity link (PPPoE)

IPv6 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".

Reserved Networks

Block private networks and loopback addresses ☐
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks ☑
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.