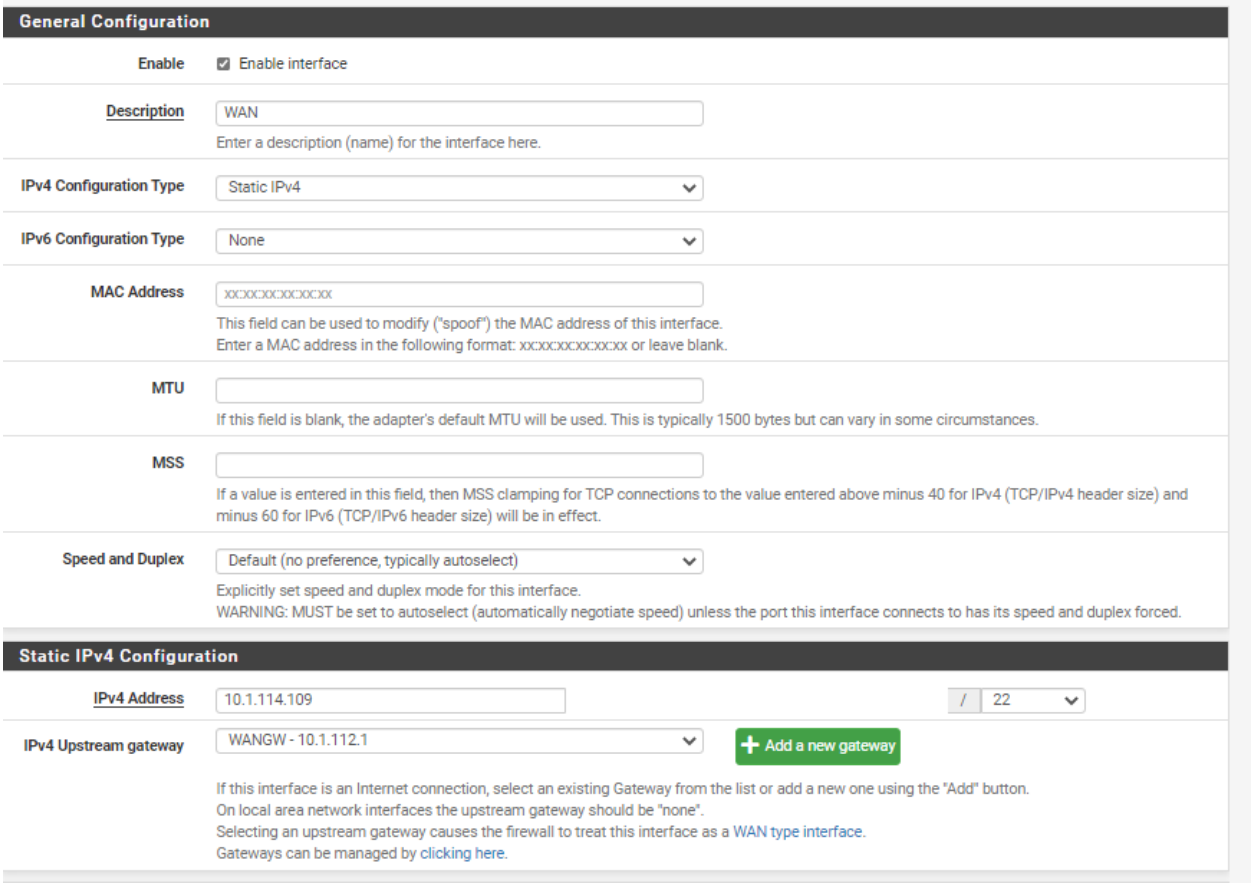
Configuring Interfaces

Configuring your interfaces is very straightforward and allows for connectivity on the server.

1. Select 'Interfaces' at the top of the browser, and select the chosen interface to configure

2. Choose the Configuration type and enter the description for the interface.

3. Choose your IP address and the upstream gateway (if it is a WAN address)



4. Save your configuration

5. Make sure to set up both a WAN and LAN interface.

Create Certificates

Certificates allow the SSL/TLS method used in the VPN to work. You will create multiple certificates for both the Server and Client, as well as an Authoritative Certificate used for both.

Create Cert Authority

1. Select 'System' and go to the 'Cert Managers' section.
2. In the CA's tab, create a new CA.
   - Descriptive Name - S2SCA
   - Method - Create an Internal Certificate Authority
   - Randomize Serial - Yes
   - Key Type - RSA, 2048
   - Digest Algorithm - sha256
   - Common Name - S2SCA
3. Save the CA

Create Server cert

1. Go to the 'Certificates' tab and add a new cert
   - Descriptive name - serverA
   - Cert Authority - S2SCA
   - Key Type - RSA, 2048
   - Digest Algorithm -sha256
   - Lifetime - 398
   - Common Name - serverA
   - Certificate Type - Server Certificate
2. Save the cert

Create User Cert

1. Go to the 'Certificates' tab and add a new cert
   - Descriptive name - clientA
   - Certificate Authority - S2SCA
   - Key Type - RSA, 2048
   - Digest Algorithm - sha256
   - Lifetime - 3650
   - Common name - clientA
   - Certificate type - User Certificate
2. Save the cert

Export the Certs

1. In the ‘CA’ tab, click on the  for the CA you just made to export it.
2. In the ‘Certificates’ tab, click on the  , and the  to export the certificate and the private key.

Import the Certs

1. On the OpenVPN client, navigate to ‘System’ section and select ‘Cert Manager’
2. On the ‘CAs’ tab, add a new CA

Descriptive name - S2SCA
Method - Import an existing Certificate Authority
Certificate Data - Open the CA certificate file in a text editor on the client PC, copy and paste the text into this field.

3. Save the config.

1. Navigate to the ‘Certificates’ tab, and add a new cert

Method - Import an existing Certificate
Descriptive name - clientA VPN Certificate
Certificate Type - X.509 (PEM)
Certificate Data - Open the client Certificate file in a text editor and paste it into this field
Private Key Data - Open the private key file in a text editor and paste it into this field

2. Save the config

Configure Firewall

Server rules

Multiple Firewall rules must be made to allow internet and other services to be accessed by users in HQ, as well as over the VPN.

1. Select 'Firewall', and go to the 'Rules' section.
2. In the WAN tab, click "Add" with the upright arrow.
3. Create 4 Rules, each for Ports 80 (HTTP), 443 (HTTPS), 53 (DNS), and one for Ipv4 ICMP protocol. This ensures the Internet connection is secure and only allows specific traffic to travel through the firewall.

☐	✓	0 /0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none	Allow HTTP through firewall	
☐	✓	0 /1 KiB	IPv4 ICMP any	*	*	*	*	*	none	Allow ICMP through firewall	
☐	✓	0 /0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none	Allow HTTPS through firewall	
☐	✓	0 /0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none	Allow DNS through firewall	

4. Now go the LAN tab, and create the same rules for your LAN interface. Do this for OP1 as well.
5. In the OpenVPN tab, do the same as well.

Client rules

You need to open the VPN tunnel for any specified traffic in order for the tunnel to be functional.

1. On the PFSense Client, Navigate to the 'OpenVPN' in the 'Firewall' section
2. Create a new rule that allows all on the OpenVPN (It is recommended to create specific rules instead of opening all ports).
3. Do this for LAN and WAN.

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	6 /134.05 MiB	IPv4 *	*	*	*	*	*	none		Allow all on OpenVPN	

Configure OpenVPN Site-to-Site tunnel with SSL/TLS.

OpenVPN Server config

You first want to Configure the VPN Server on the PFSense server located in HQ.

1. Select 'VPN' and go the 'OpenVPN' section.
2. In the 'Servers' tab, add a new server.

Choose a description (I chose HQ S2S VPN)
Server mode - Peer to Peer (SSL/TLS)
Device Mode - tun
Protocol - UDP on IPv4 only
Interface - WAN
Local Port - 1194
Use a TLS key - YES
COPY THE TLS KEY (IMPORTANT)
TLS Key Usage Mode - TLS Authentication
Peer Certificate Authority - S2SCA
Server Certificate - serverA
IPv4 Tunnel Network - 10.3.100.0/30
Ipv4 Local Network(s) - 10.20.10.0/24, 10.10.10.0/24, 10.10.20.0/24, 10.10.30.0/24, 172.16.10.0/24, 192.168.1.8/29
IPv4 Remote networks - 10.20.10.0/24

3. Save the config

OpenVPN Client Config

Now you will be configuring the VPN client on the other PFsense server located in VS.

1. On the VPN client, select 'VPN' and go to the 'OpenVPN' section.
2. In the 'Clients' tab, add a new client.

Choose a description (VS S2S VPN Client)
Server mode - Peer to Peer (SSL/TLS)
Device mode - tun
Protocol - UDP on IPv4 Only
Interface - WAN

Local port - 1194
Server host or address - 10.1.114.109
Server port - 1194
Use a TLS key - YES
TLS Key - **Paste the TLS KEY copied earlier from the server**
Tls Key Usage Mode - TLS Authentication
Peer Certificate Authority - S2SCA
Client Certificate - clientA VPN Certificate
IPv4 Tunnel Network - 10.3.100.0/30
IPv4 Remote Network(s) - 192.168.1.8/29, 10.10.10.0/24, 10.10.20.0/24, 10.10.30.0/24, 10.10.0.0/16, 192.168.1.4/30, 172.16.10.0/24

3. Save the config

Configure Web Filtering

Download pfBlockerNG

1. Install the pfBlockerNG package from: System>Package Manager
2. Open the pfBlockerNG window

Enable pfBlockerNG - YES

3. In the Ipv4 tab, Create a new Alias

Alias Name - BadIps
List Description - Blocking known Malicious IP addresses
Ipv4 List - http://www.spamhaus.org/drop/drop.txt
Ipv4 List - https://www.spamhaus.org/drop/edrop.txt
Ipv4 List - https://feeds.dshield.org/top10-2.txt
List Action - Deny both
Update Frequency - Once a day
Enable Logging - Enable

4. OPTIONAL - Create a custom Ipv4 list of specific websites/addresses you think should be blocked.
5. Save your Alias.
6. Go to the DNSBL Tab

Enable DNSBL - YES
DNSBL Virtual IP - (Any Ip in an Isolated Range than what is used in the Network)
DNSBL Firewall Rule - LAN
List Action - Deny Both
Enable Logging - Enable

7. Save your Config

Nat/Port Forwarding

Open port 80 (HTTP) directed to your webserver.

1. In the pfsense webconfig, go to Firewall>NAT>Port Forward
2. Create a new Port Forward entry.

Interface - WAN
Address Family - IPv4
Protocol - TCP
Destination - WAN address
Destination port range - HTTP
Redirect target IP - 192.168.1.6
Redirect target port - HTTP

3. Create a second Port Forward entry for HTTPS port.
4. Save both entries.