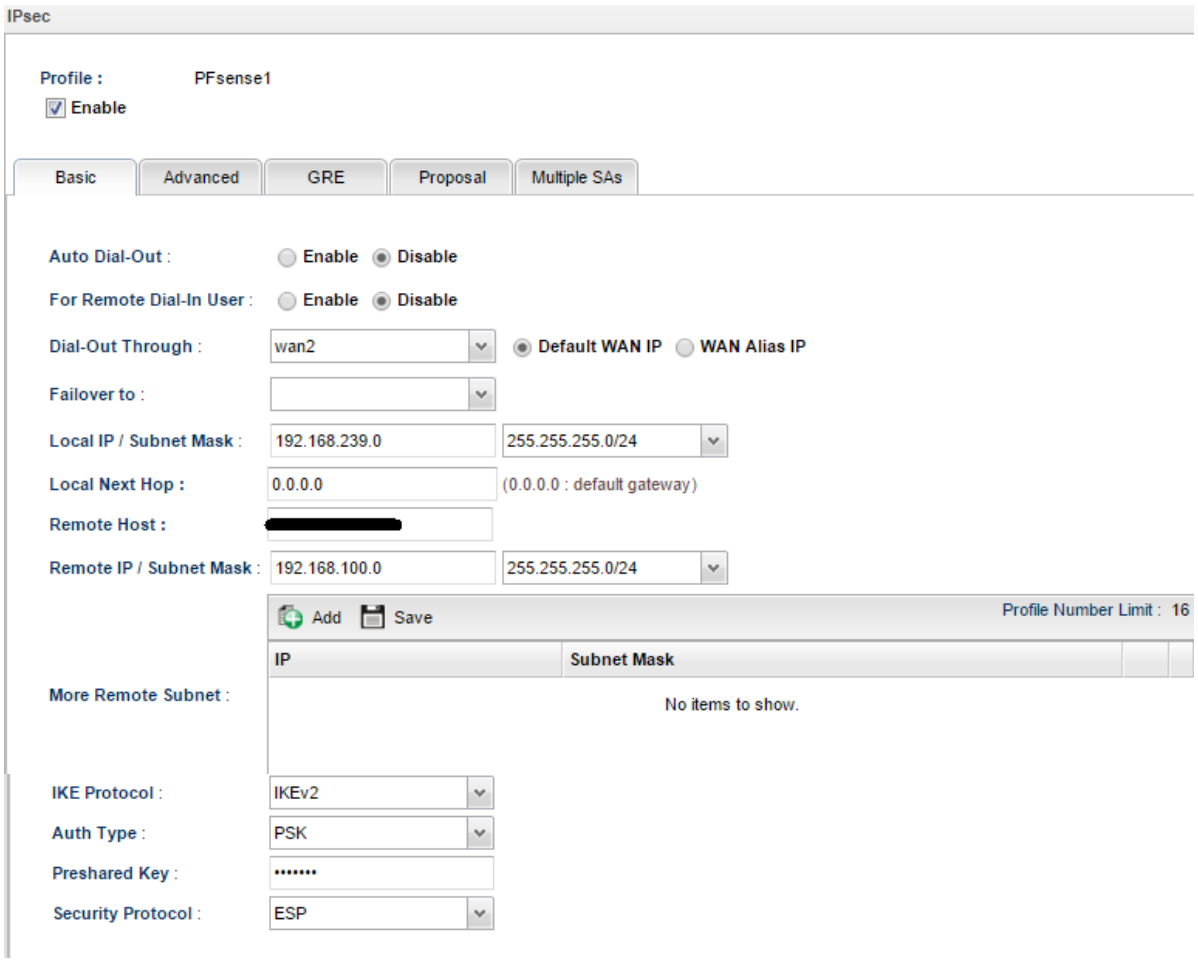
Set up IPsec Tunnel between PfSense and Vigor3900

This document introduces how to set up IPsec tunnel between PfSense and Vigor3900 with IKEv2 protocol.

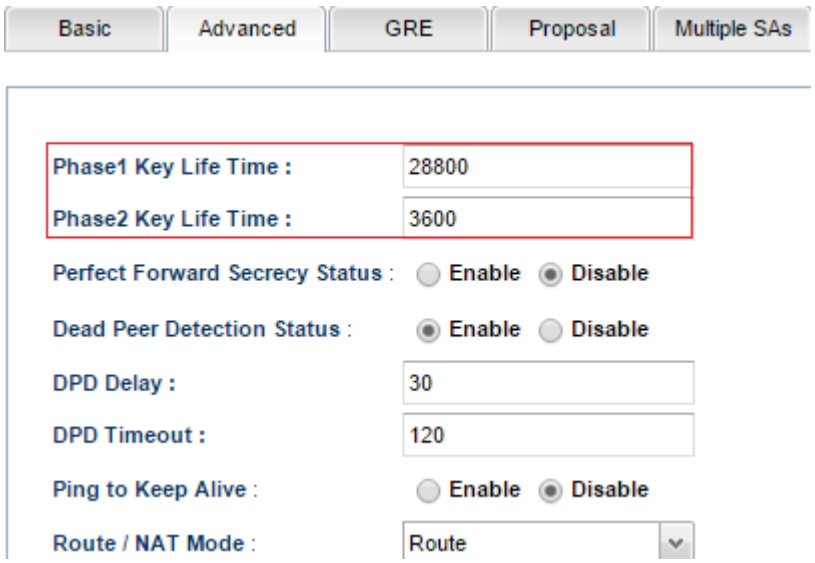
In this document, both Vigor3900 and PfSense are using Static IP WAN to establish IPsec Tunnel.

Vigor3900 Setup

1. Go to **VPN and Remote Access** >> **VPN Profile** >> **IPsec** click **Add** to add a new profile:
   a. In Basic tab, enter **Profile** name and **Enable** this profile
   b. Enter **Local IP /Subnet Mask** as the LAN network on Vigor3900.
   c. Enter PfSense WAN IP in **Remote Host**
   d. Enter **Remote IP/ Subnet Mask** as the PfSense LAN network.
   e. Select IKEv2 as **IKE Protocol**. (IKEv2 is supported since firmware version 1.3.0)
   f. Enter **Pre-Shared** Key.



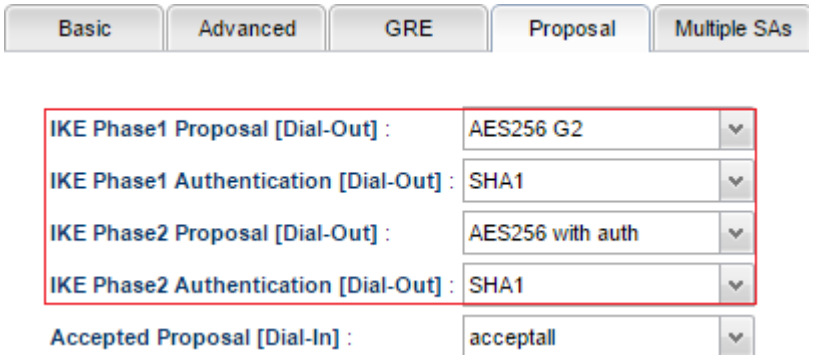
g. In Advanced tab, enter Phase1 and Phase2 Key Lifetime.



h. In Proposal Tab, select the accurate proposal that match the proposal setting on PfSense. PfSense doesn't accept more than one phase 1 proposal, so Auto option is not suitable. (The step could be ignored if Vigor3900 acts as Dial In side.)

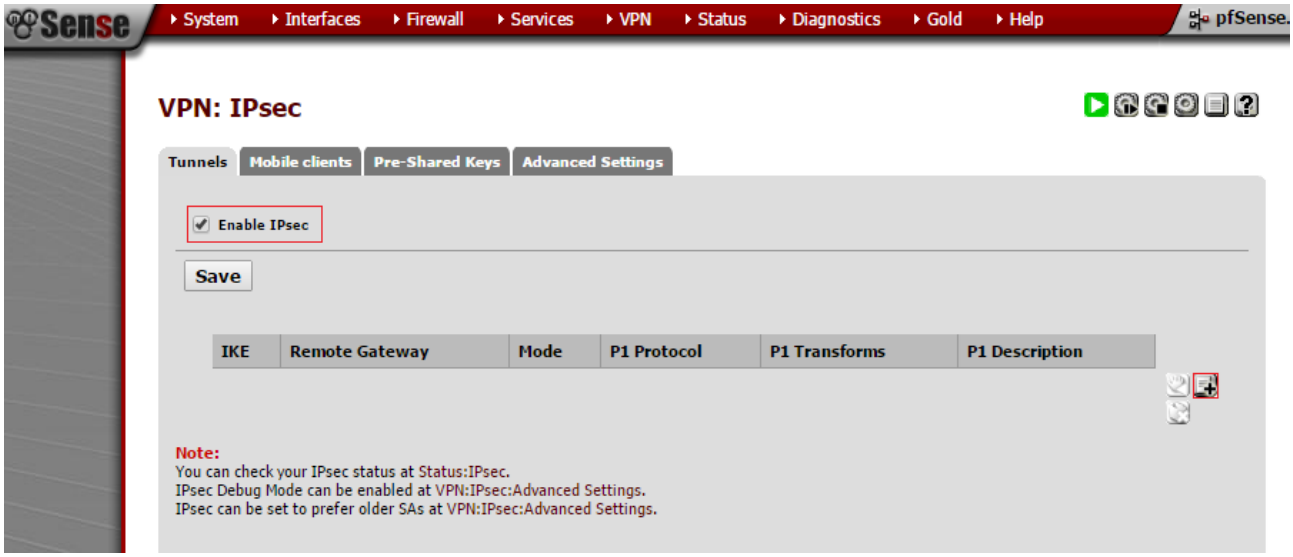
i. In Proposal Tab, select **acceptall** for Accepted Proposal [Dial-In]

j. Click **Apply** to save the profile.

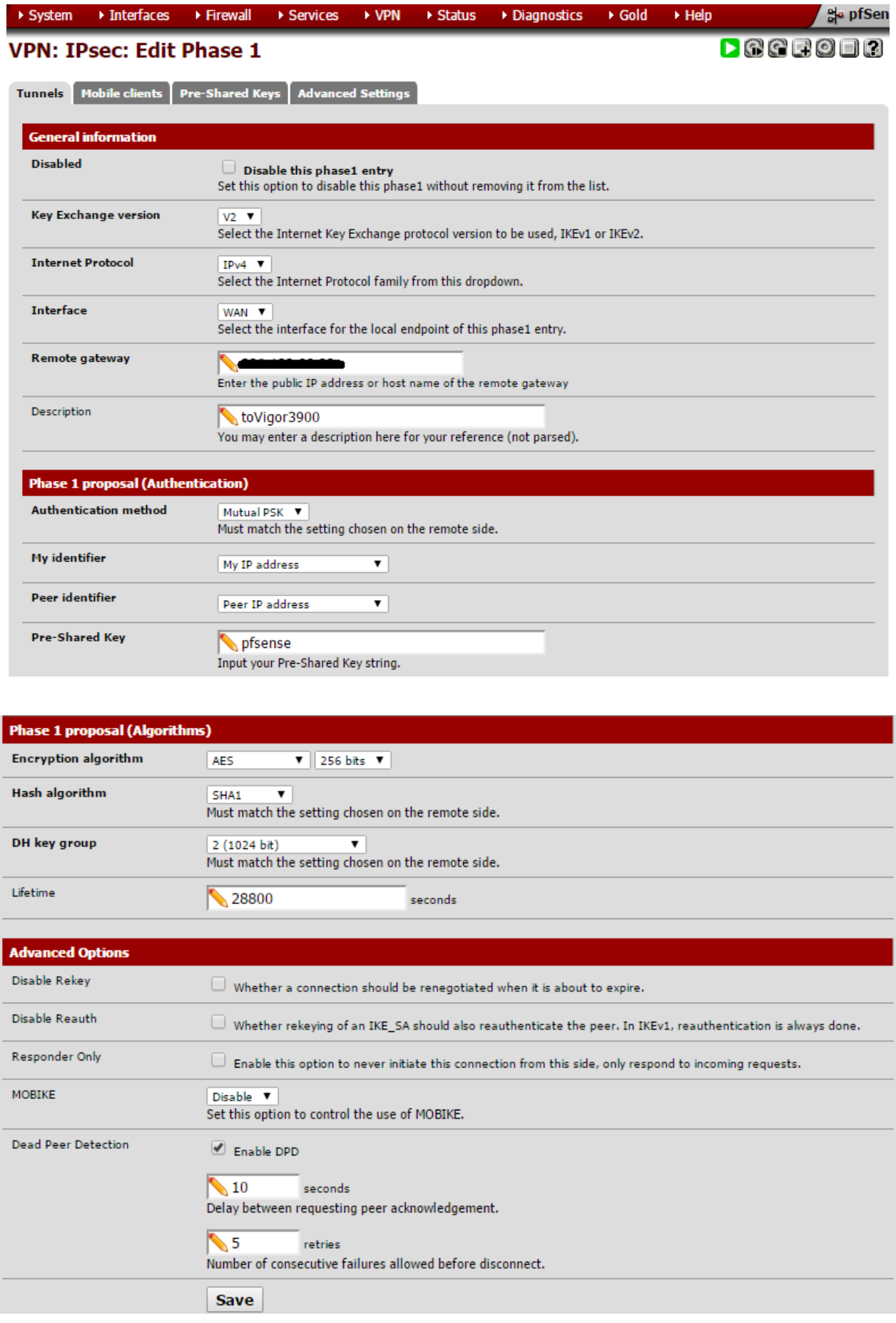


PfSense Setup

2. Tick Enable IPsec option and click + to create VPN Phase 1 profile.

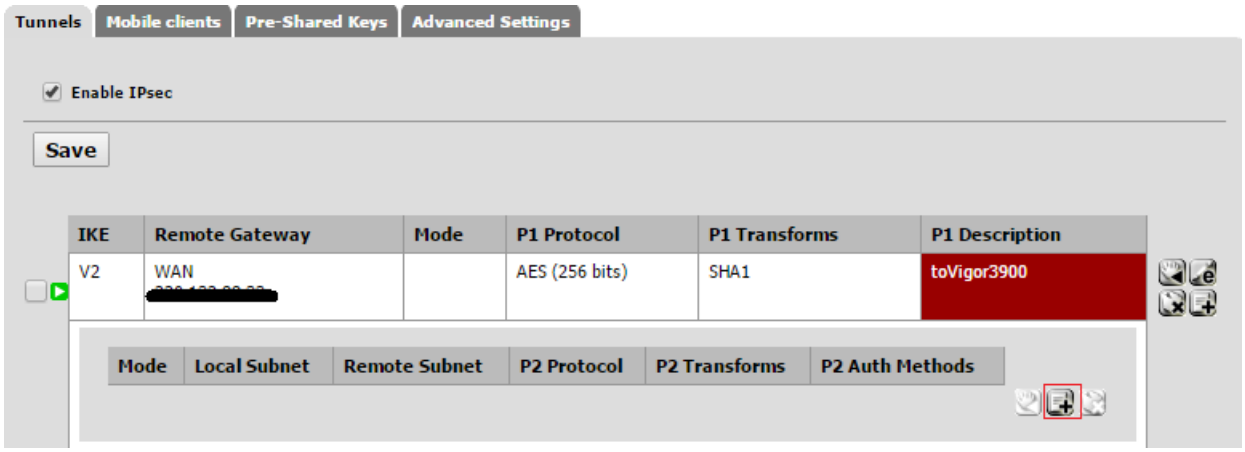


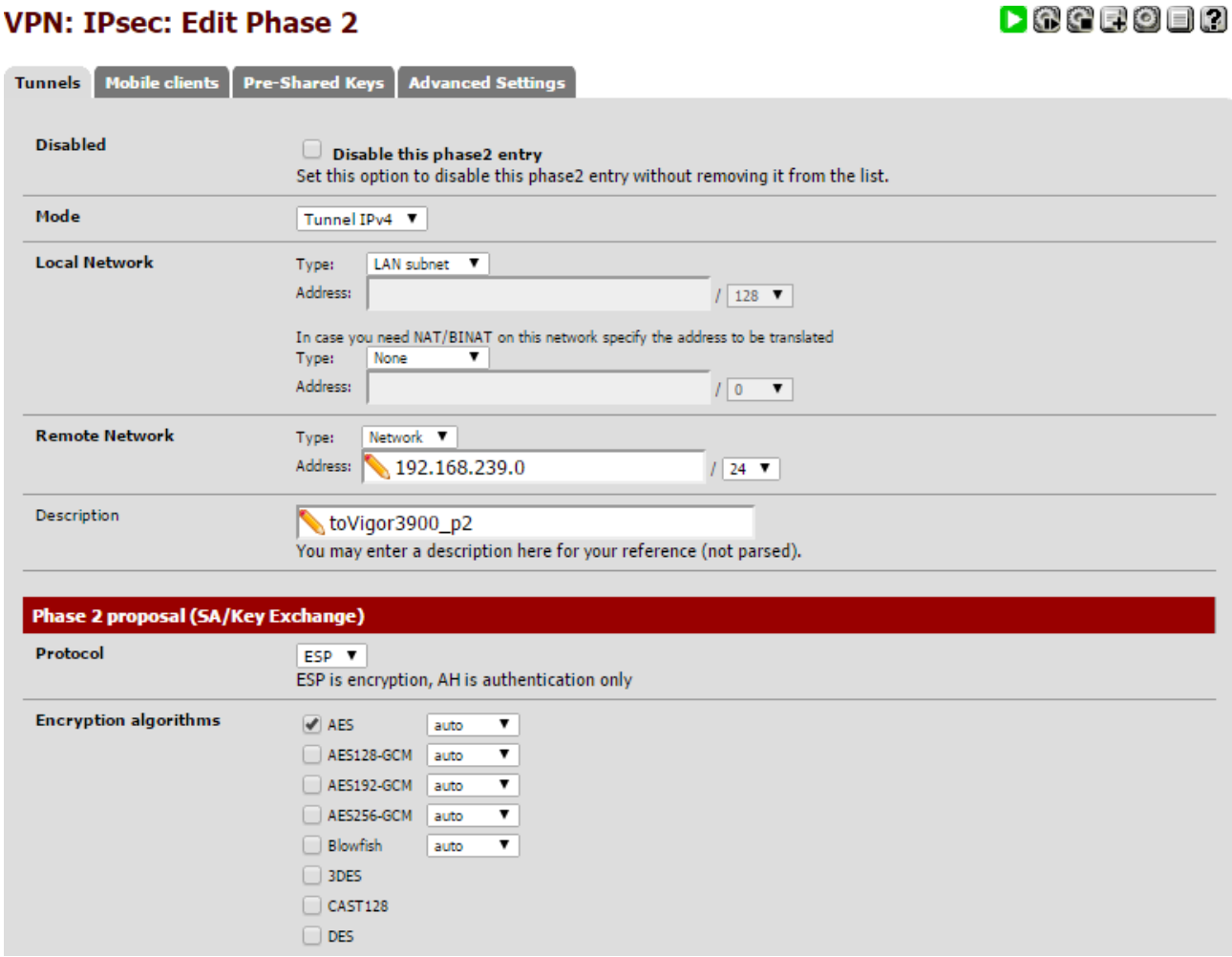
3. Input IPsec Phase1 settings.
   a. Select Key Exchange Version **v2**
   b. Input Vigor3900's WAN IP as the **Remote Gateway**
   c. Input Profile Description
   d. Input **Pre-Shared Key**
   e. Select **AES256 SHA1** with DH Group **G2** as **Phase 1 Proposal**
   f. Input p1 lifetime as 28800
   g. Enable DPD
   h. Click Save

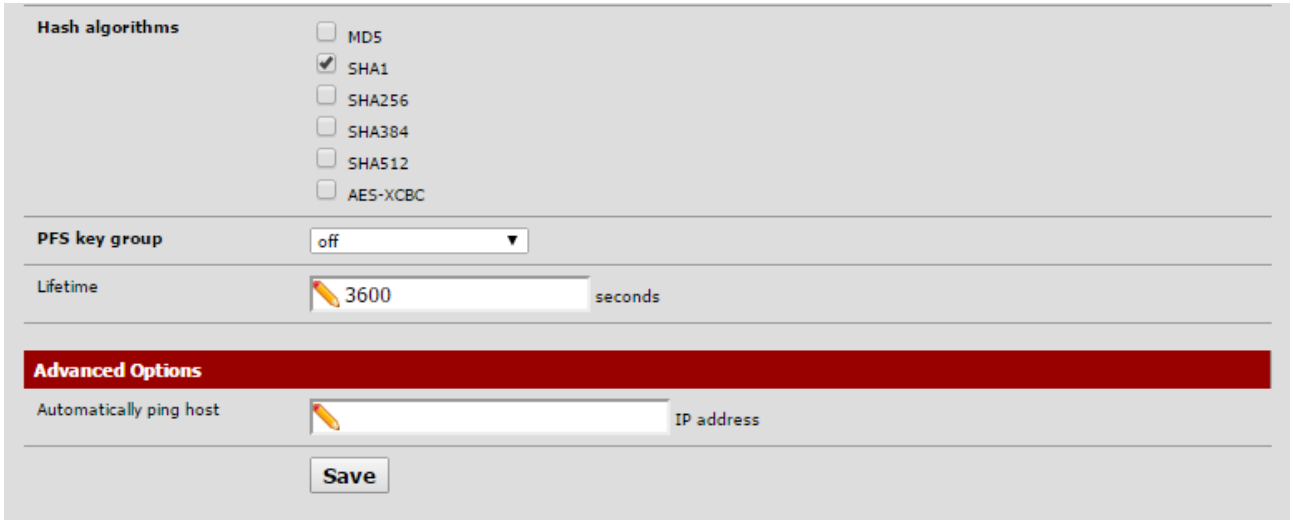


4. Click the VPN phase 1 profile we just created then click + to create phase 2 profile.

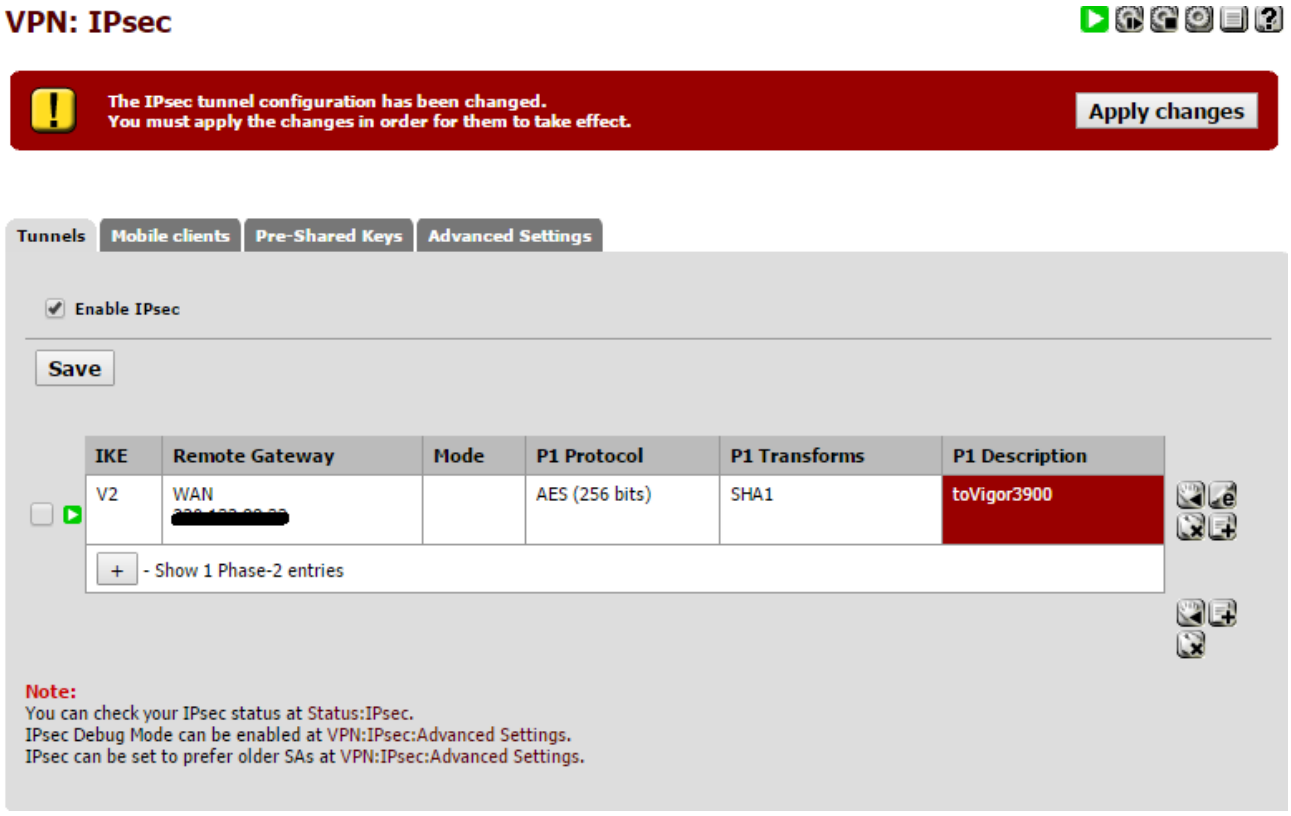
a. Select LAN Subnet for Local Network
b. Select Type Network then input Vigor3900's LAN network for Remote Network
c. Select Phase 2 Proposal
d. Input the Phase 2 Key Lifetime
e. Click Save

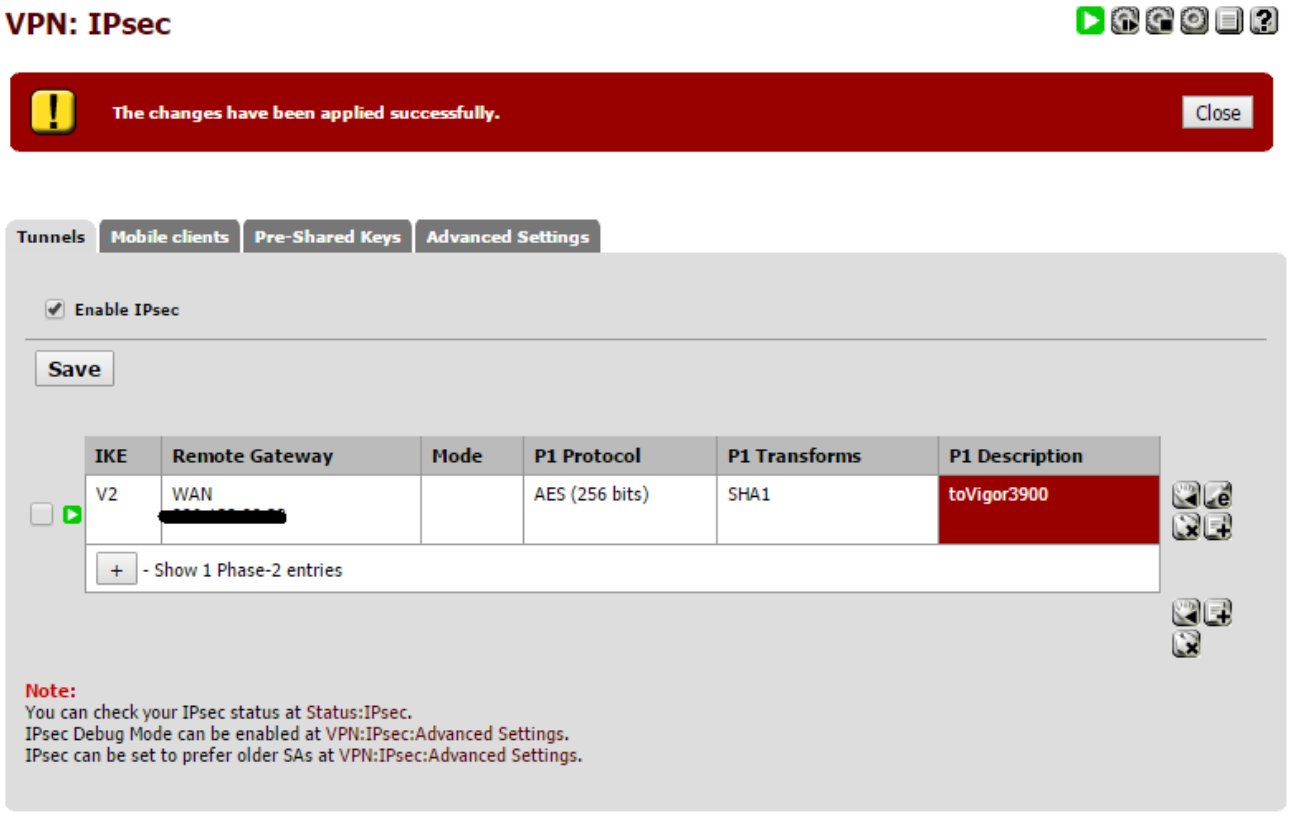




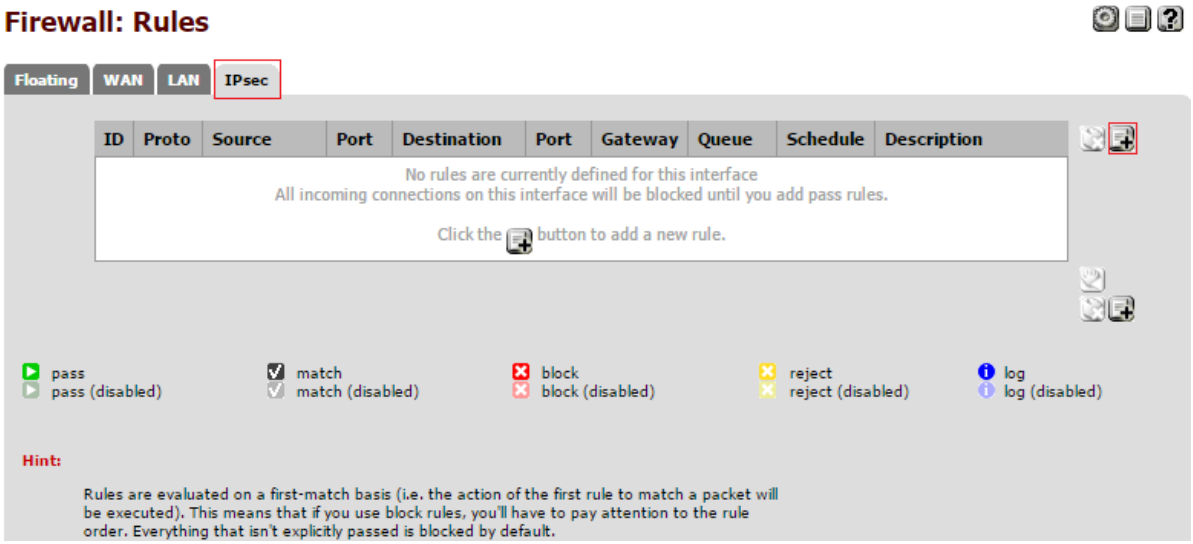


5. Click Apply changes button for applying the changes.

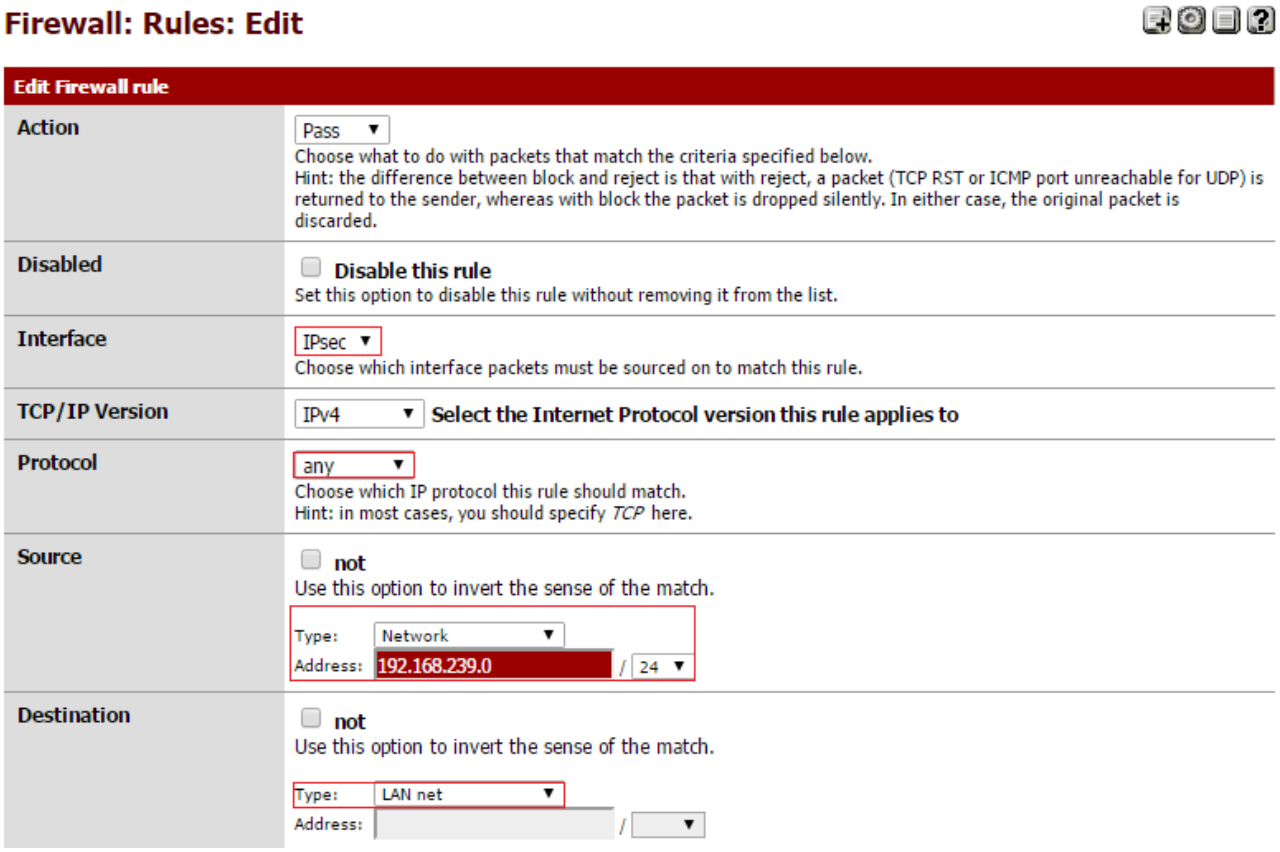




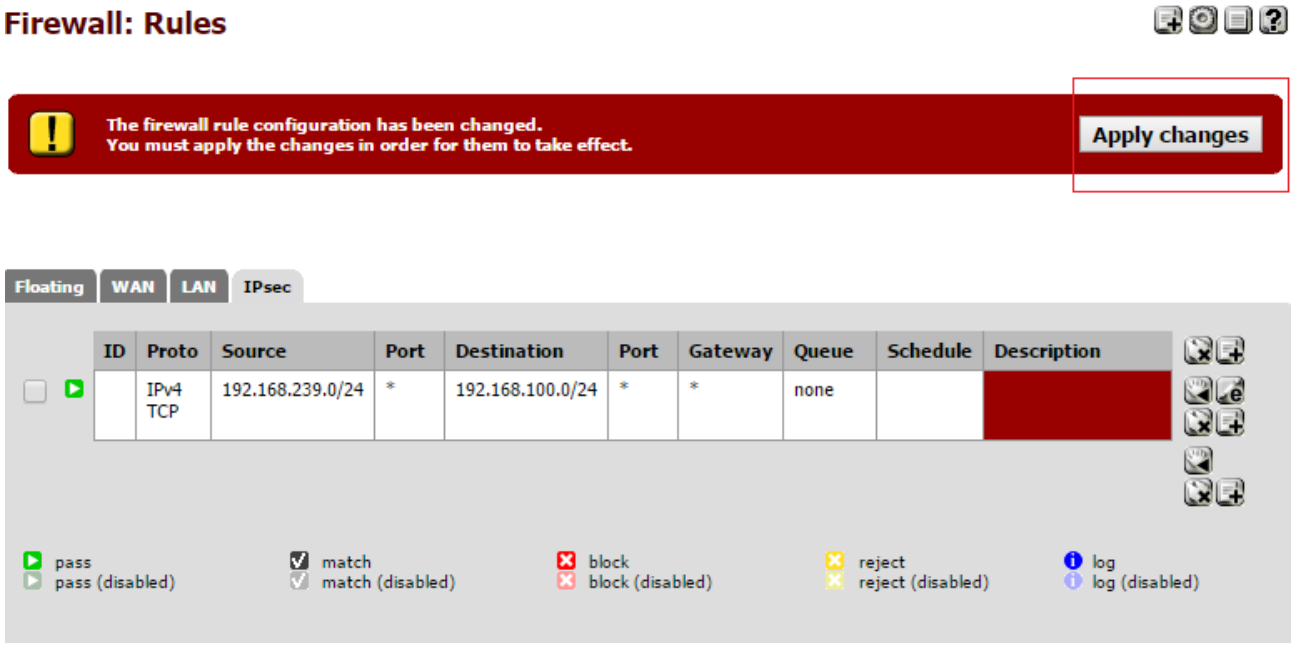
6. Create Firewall IPsec Rule for allowing Vigor3900 local network to access Pfsense local network.
   a. Click + in IPsec tab.



   b. Select IPsec for Interface, any for Protocol, input Vigor3900 local network for Source and select LAN net for Destination then click Save.



c. Click Apply changes.



Establish IPsec

7. Go to Status: IPsec page. Click Connect button to establish the VPN tunnel.

Status: IPsec

Overview | Leases | SAD | SPD | Logs

Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
toVigor3900	[redacted]	[redacted]	[redacted]	[redacted]				Disconnected

Note:
You can configure IPsec here.

8. IPsec VPN tunnel is established.

System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Gold | Help | pfSen

Status: IPsec

Overview | Leases | SAD | SPD | Logs

Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
toVigor3900	[redacted]	[redacted] Port: 500	[redacted]	[redacted] Port: 500	IKEv2 initiator	7 hours	AES_CBC:256 HMAC_SHA1_96:0 PRF_HMAC_SHA1 MODP_1024	established 0 seconds ago
+ - Show child SA entries								

9. PfSense is able to ping remote computer through the IPsec tunnel now. We can verify this via Diagnostics: Ping.

Diagnostics: Ping

Ping

Host	192.168.239.10
IP Protocol	IPv4
Source Address	LAN1
Count	3
	Ping

Ping output:

```
PING 192.168.239.10 (192.168.239.10) from 192.168.100.1: 56 data bytes
64 bytes from 192.168.239.10: icmp_seq=0 ttl=127 time=207.521 ms
64 bytes from 192.168.239.10: icmp_seq=1 ttl=127 time=207.736 ms
64 bytes from 192.168.239.10: icmp_seq=2 ttl=127 time=207.454 ms

--- 192.168.239.10 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 207.454/207.570/207.736/0.120 ms
```

10. Check the IPsec VPN Connection Status on Vigor3900.