

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**.

IPsec

Profile : PFSense1

Enable

Basic Advanced GRE Proposal Multiple SAs

Auto Dial-Out : Enable Disable

For Remote Dial-In User : Enable Disable

Dial-Out Through : wan2 Default WAN IP WAN Alias IP

Failover to :

Local IP / Subnet Mask : 192.168.239.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : [REDACTED]

Remote IP / Subnet Mask : 192.168.100.0 255.255.255.0/24

Add Save Profile Number Limit : 16

IP	Subnet Mask
No items to show.	

More Remote Subnet :

IKE Protocol : IKEv2

Auth Type : PSK

Preshared Key :

Security Protocol : ESP

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

Basic	Advanced	GRE	Proposal	Multiple SAs
Phase1 Key Life Time :	28800			
Phase2 Key Life Time :	3600			
Perfect Forward Secrecy Status :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Dead Peer Detection Status :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
DPD Delay :	30			
DPD Timeout :	120			
Ping to Keep Alive :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Route / NAT Mode :	Route			

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.)

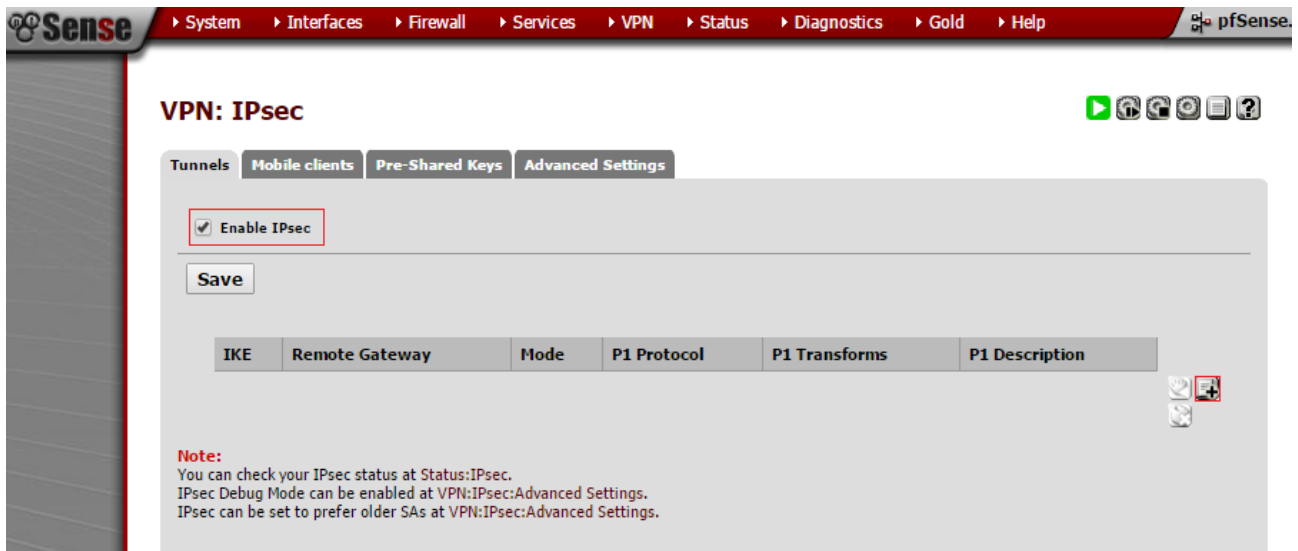
i. In Proposal Tab, select **acceptall** for Accepted Proposal [Dial-In]

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

Basic	Advanced	GRE	Proposal	Multiple SAs
IKE Phase1 Proposal [Dial-Out] :	AES256 G2			
IKE Phase1 Authentication [Dial-Out] :	SHA1			
IKE Phase2 Proposal [Dial-Out] :	AES256 with auth			
IKE Phase2 Authentication [Dial-Out] :	SHA1			
Accepted Proposal [Dial-In] :	acceptall			

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

VPN: IPsec: Edit Phase 1



Tunnels | Mobile clients | Pre-Shared Keys | **Advanced Settings**

General information

Disabled **Disable this phase1 entry**
Set this option to disable this phase1 without removing it from the list.

Key Exchange version **V2** ▼
Select the Internet Key Exchange protocol version to be used, IKEv1 or IKEv2.

Internet Protocol **IPv4** ▼
Select the Internet Protocol family from this dropdown.

Interface **WAN** ▼
Select the interface for the local endpoint of this phase1 entry.

Remote gateway **[redacted]**
Enter the public IP address or host name of the remote gateway

Description **toVigor3900**
You may enter a description here for your reference (not parsed).

Phase 1 proposal (Authentication)

Authentication method **Mutual PSK** ▼
Must match the setting chosen on the remote side.

My identifier **My IP address** ▼

Peer identifier **Peer IP address** ▼

Pre-Shared Key **pfsense**
Input your Pre-Shared Key string.

Phase 1 proposal (Algorithms)

Encryption algorithm **AES** ▼ **256 bits** ▼

Hash algorithm **SHA1** ▼
Must match the setting chosen on the remote side.

DH key group **2 (1024 bit)** ▼
Must match the setting chosen on the remote side.

Lifetime **28800** seconds

Advanced Options

Disable Rekey Whether a connection should be renegotiated when it is about to expire.

Disable Reauth Whether rekeying of an IKE_SA should also reauthenticate the peer. In IKEv1, reauthentication is always done.

Responder Only Enable this option to never initiate this connection from this side, only respond to incoming requests.

MOBIKE **Disable** ▼
Set this option to control the use of MOBIKE.

Dead Peer Detection **Enable DPD**

10 seconds
Delay between requesting peer acknowledgement.

5 retries
Number of consecutive failures allowed before disconnect.

Save

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

- Select LAN Subnet for Local Network
- Select Type Network then input Vigor3900's LAN network for Remote Network
- Select Phase 2 Proposal
- Input the Phase 2 Key Lifetime
- Click Save

Tunnels **Mobile clients** Pre-Shared Keys **Advanced Settings**

Enable IPsec

Save

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
V2	WAN 192.168.0.0/24		AES (256 bits)	SHA1	toVigor3900

Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods

VPN: IPsec: Edit Phase 2



Tunnels **Mobile clients** Pre-Shared Keys **Advanced Settings**

Disabled **Disable this phase2 entry**
Set this option to disable this phase2 entry without removing it from the list.

Mode Tunnel IPv4

Local Network
Type: LAN subnet
Address: / 128
In case you need NAT/BINAT on this network specify the address to be translated
Type: None
Address: / 0

Remote Network
Type: Network
Address: 192.168.239.0 / 24

Description
toVigor3900_p2
You may enter a description here for your reference (not parsed).

Phase 2 proposal (SA/Key Exchange)

Protocol ESP
ESP is encryption, AH is authentication only

Encryption algorithms

- AES auto
- AES128-GCM auto
- AES192-GCM auto
- AES256-GCM auto
- Blowfish auto
- 3DES
- CAST128
- DES

Hash algorithms

MD5

SHA1

SHA256

SHA384

SHA512

AES-XCBC

PFS key group off

Lifetime 3600 seconds

Advanced Options

Automatically ping host IP address

Save

5. Click Apply changes button for applying the changes.

VPN: IPsec



! The IPsec tunnel configuration has been changed. You must apply the changes in order for them to take effect. **Apply changes**

Tunnels | **Mobile clients** | **Pre-Shared Keys** | **Advanced Settings**

Enable IPsec

Save

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
<input type="checkbox"/>	WAN [REDACTED]		AES (256 bits)	SHA1	toVigor3900
+ - Show 1 Phase-2 entries					

Note:
 You can check your IPsec status at Status:IPsec.
 IPsec Debug Mode can be enabled at VPN:IPsec:Advanced Settings.
 IPsec can be set to prefer older SAs at VPN:IPsec:Advanced Settings.

VPN: IPsec



The changes have been applied successfully.

Close

Tunnels **Mobile clients** Pre-Shared Keys Advanced Settings

Enable IPsec

Save

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
<input type="checkbox"/> V2	WAN		AES (256 bits)	SHA1	toVigor3900

+ - Show 1 Phase-2 entries

Note:
You can check your IPsec status at Status:IPsec.
IPsec Debug Mode can be enabled at VPN:IPsec:Advanced Settings.
IPsec can be set to prefer older SAs at VPN:IPsec:Advanced Settings.

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

Firewall: Rules



Floating **WAN** LAN **IPsec**

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
No rules are currently defined for this interface All incoming connections on this interface will be blocked until you add pass rules. Click the button to add a new rule.									

pass match block reject log
 pass (disabled) match (disabled) block (disabled) reject (disabled) log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

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

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 IPsec
Choose which interface packets must be sourced on to match this rule.

TCP/IP Version IPv4 **Select the Internet Protocol version this rule applies to**

Protocol any
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify *TCP* here.

Source **not**
Use this option to invert the sense of the match.
Type: Network
Address: 192.168.239.0 / 24

Destination **not**
Use this option to invert the sense of the match.
Type: LAN net
Address: /

c. Click Apply changes.

Firewall: Rules



! The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

Apply changes

Floating **WAN** **LAN** **IPsec**

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	192.168.239.0/24	*	192.168.100.0/24	*	*	none	

pass
 pass (disabled)

match
 match (disabled)

block
 block (disabled)

reject
 reject (disabled)

log
 log (disabled)

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	██████████	██████████	██████████	██████████				Disconnected

Note:
You can configure IPsec here.

8. IPsec VPN tunnel is established.

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Gold > Help

pfSense

Status: IPsec



Overview Leases SAD SPD Logs

Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
toVigor3900	██████████	██████████ Port: 500	██████████	██████████ 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:

IP Protocol:

Source Address:

Count:

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.

VPN and Remote Access >> Connection Management >> Connection Management

Connection Management History

Dial-Out tool

IPsec PPTP SSL Profiles : Auto Refresh :

Green :Data is encrypted.
White :Data isn't encrypted

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte	TX Byte	
1	PfSense	IKEv2:IPsec/AES_HMAC...	wan2	██████████	192.168.100.0/24	00:01:20	480(bps)	960(bps)	720(Byte)	1.41 (KB)