

Site-to-site VPN pfSense and Amazon VPC

(Panopto Tip: press play to continue with video)

[Follow Link to copy of this page in another Window](#)

Heitor Lessa

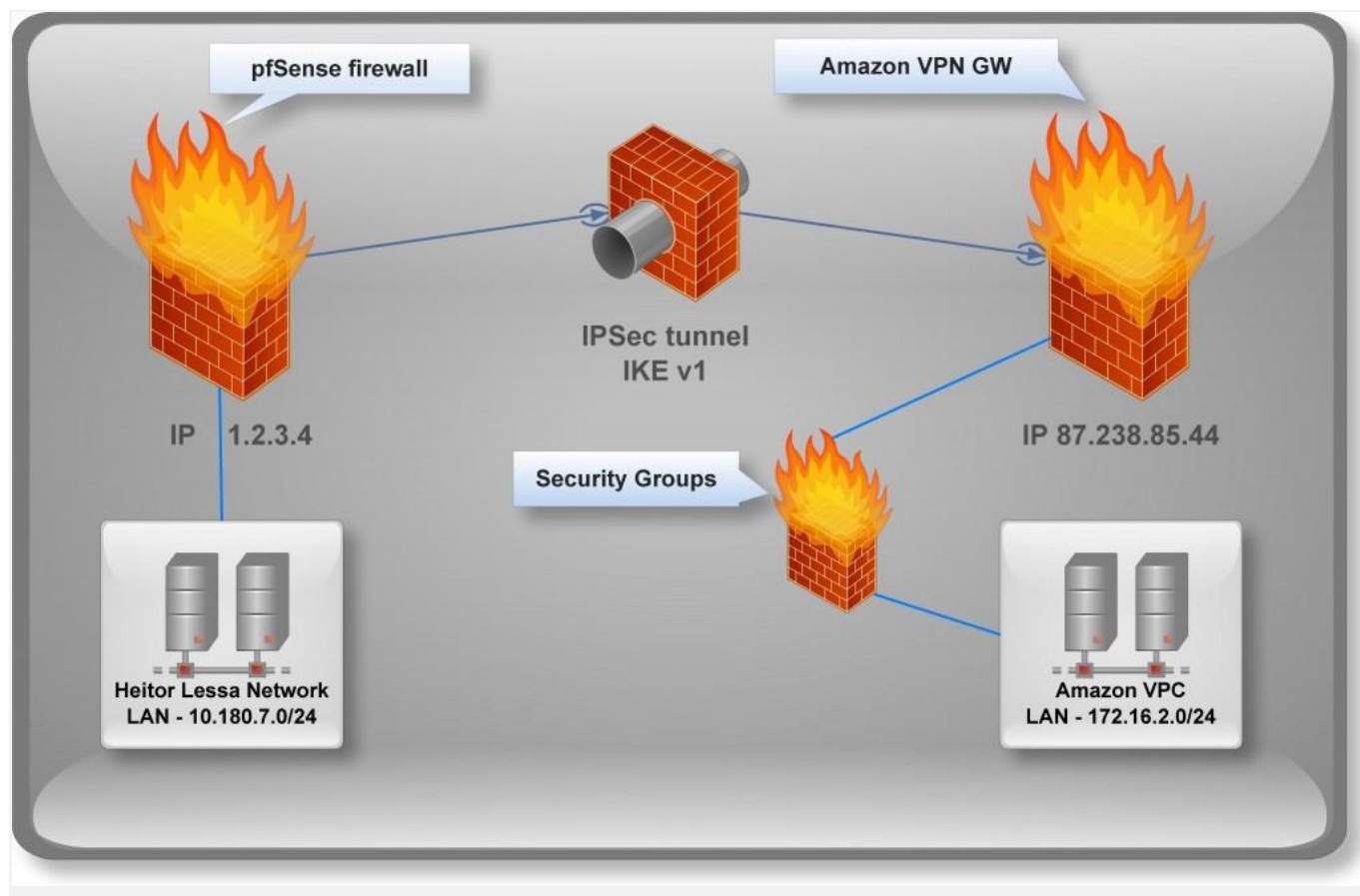
Original site: <https://heitorlessa.com/site-to-site-vpn-pfsense-and-amazon-vpc-2184196822fo>

How to create a **Site-to-site VPN** between **pfSense** and **Amazon VPC** using **Virtual Private Gateway** feature.

Best to follow this in pfSense version 2.2.2

From here, I presume that you already know what is [pfSense](#) and [Amazon VPC](#), however instead of creating an instance in **Amazon** and use an **IPsec** software, we will be using here a VPN Gateway in Amazon that can be created quite easily.

Basically, we will be setting up an **IPsec VPN** using **IKEv1** because IKEv2 its not supported by Amazon (learnt in the hardest way unfortunately), and this tunnel will share static routes. Follow below an image I created specifically for this article that will help you to have a better overview:

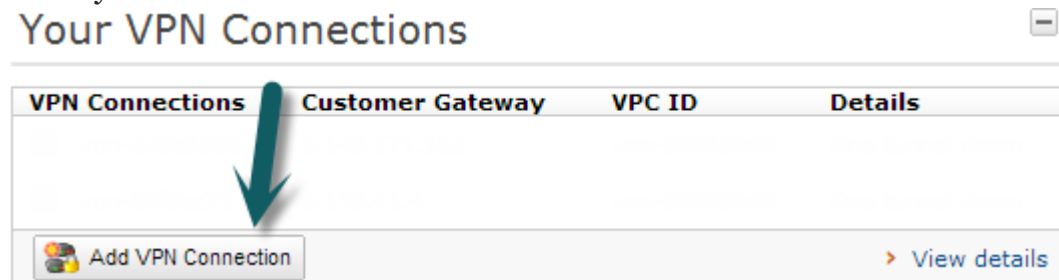


VPN overview

I would say this is a very straightforward and basic one which is really stable, however if you are looking for a **VPN** using **BGP** protocol with **pfSense** — [check out this well written article](#).

Starting from scratch, we will need to create a **VPG in Amazon** as below:

Go to your Amazon VPC dashboard and select the button **Add a VPN connection**



pfSense Amazon VPC — New VPN connection

A new window will show up to fill out the a form as follow:

Add VPN Connection

Cancel

Please select the VPC to attach the VPN connection to. Then, select an existing Customer Gateway or enter the internet-routable IP address for a new Customer Gateway (router) for your side of the VPN Connection. The address must be static and can't be behind a device performing network address translation (NAT).

VPC ID:

(172.16.2.0/24)

Customer Gateway:

1.2.3.4

Select an existing IP address or enter a new one, e.g. 192.0.2.1

Specify the routing for the VPN Connection (Help me choose)

☐ Use dynamic routing (requires BGP)

☒ Use static routing

Specify the IP prefixes for the network on your side of the VPN Connection

IP Prefix:

Add

10.180.7.0/24

Remove

(e.g. 192.168.0.0/16)

pfSense Amazon VPC — Customer gateway and network

As you see, you firstly have to choose your VPC subnet (172.16.2.0/24 in this case), then **your external IP** in Customer Gateway, your LAN subnet (10.180.7.0/24) in **IP Prefix** and finally select **Add/Yes create** to finish the **VPN creation**.

It will take few minutes to create the **VPN gateway** in Amazon and you should see the image below until complete.

Add VPN Connection

Creating your VPN Connection ...

pfSense Amazon VPC — Creating your VPN

Once completed, go to **VPN Connection** option in the left-side menu as shown:

VPC: All VPCs

[Create VPN Connection](#) [Delete](#) [Download Configuration](#)

Viewing: All VPN Connections

ID	State	Virtual Private Gateway	Customer Gateway	Type	VPC	Routing
<input checked="" type="checkbox"/> vpn-75cdf901	available	vgw-54300420	cgw-25b58151	ipsec.1	vpc-b93339d0 (172.16.2.0/24)	Static

1 VPN Connection selected

VPN Connection: vpn-75cdf901

[Details](#) [Static Routes](#) [Tags](#)

VPN Tunnel	IP Address	Status	Status Last Changed
Tunnel 1	87.238.85.40	DOWN	2013-04-27 16:52 GMT
Tunnel 2	87.238.85.44	DOWN	2013-04-27 16:51 GMT

pfSense Amazon VPC — VPN connection

Note we have a button on top “Download configuration” and we also have two Tunnels, however Amazon does not offer a configuration file for pfSense. But the Phase1 and Phase2 settings will be default (until they change of course) for all **VPNs** created in **VPC**, apart of course the password and IPs.

Also, we will be using the second tunnel as I had so much trouble (connection dropped very often) using the first one.

Download any configuration (we will be using Fortinet as an example) and get the password from there:

Download Configuration [Cancel](#)

Please choose the configuration to download based on your type of customer gateway.

Vendor: Fortinet

Platform: Fortigate 40+ Series

Software: FortiOS 4.0+ (GUI)

[Cancel](#) [Yes, Download](#)

pfSense Amazon VPC — Download VPC configuration

Open the text file downloaded previously and look for the **Pre-Shared key** in the **second peer** as shown below:

```
Go to VPN-->IPSec--> AutoKey, create Phase 1

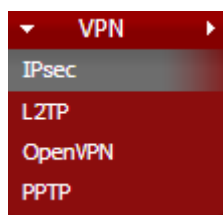
a. Name: Amazon-IKE-vpn-75cdf901-1
b. Remote Gateway: Static
c. IP address: 87.238.85.44
d. Local Interface: wan1
e. Mode: Main
f. Authentication Method: Pre-shared Key
g. Pre-Shared Key: YoO3Vco5laGhiLSI1HCgdqPA_ekqJcD5

Select Advanced:
h. Ike Version: 1
i. Local-gateway: Select Specify and enter 1.2.3.4
j. Encryption: aes128
k. Authentication: sha1
l. DH group: 2
m. Keylife: 28800 seconds
n. Select Dead Peer Detection Enable
j. Click ok
```

pfSense Amazon VPC — Pre-shared key

pfSense configuration

Open up your **pfSense** dashboard and go to **VPN → IPsec**:



pfSense Amazon VPC — IPsec option

Then add a new Phase1 entry (clicking on button +) and fill out the **Phase1** as follows:

General information	
Disabled	<input type="checkbox"/> Disable this phase1 entry Set this option to disable this phase1 without removing it from the list.
Interface	WAN ▼ Select the interface for the local endpoint of this phase1 entry.
Remote gateway	87.238.85.44 Enter the public IP address or host name of the remote gateway
Description	Amazon VPC 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.
Negotiation mode	main ▼ Aggressive is more flexible, but less secure.
My identifier	My IP address ▼
Peer identifier	Peer IP address ▼
Pre-Shared Key	<input type="text"/> Input your pre-shared key string.
Policy Generation	Default ▼ When working as a responder (as with mobile clients), this controls how policies are generated based on SA proposals.
Proposal Checking	Default ▼ Specifies the action of lifetime length, key length, and PFS of the phase 2 selection on the responder side, and the action of lifetime check in phase 1.
Encryption algorithm	AES ▼ 128 bits ▼
Hash algorithm	SHA1 ▼ Must match the setting chosen on the remote side.
DH key group	2 ▼ 1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit Must match the setting chosen on the remote side.
Lifetime	28800 ▼ seconds
Advanced Options	
NAT Traversal	Enable ▼ Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
Dead Peer Detection	<input checked="" type="checkbox"/> Enable DPD 10 seconds Delay between requesting peer acknowledgement. 2 retries Number of consecutive failures allowed before disconnect.

pfSense Amazon VPC — Phase1

Once saved, expand the VPN configuration clicking in “+” and then create a new Phase2 entry as follows:

Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
WAN 87.238.85.44	main	AES (128 bits)	SHA1	Amazon VPC
<div> <div>+</div> <div>- Show 0 Phase-2 entries</div> </div>				

pfSense Amazon VPC — Creating phase2

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

Fill out the form as follows:

Disabled

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

Mode

Tunnel

Local Network

Type: LAN subnet
Address: / 0

Remote Network

Type: Network
Address: 172.16.2.0 / 24

Description

Amazon VPC
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 128 bits
☐ Blowfish auto
☐ 3DES
☐ CAST128
☐ DES

Hint: use 3DES for best compatibility or if you have a hardware crypto accelerator card. Blowfish is usually the fastest in software encryption.

Hash algorithms

☒ SHA1
☐ MD5

PFS key group

2
1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit

Lifetime

3600 seconds

Advanced Options

Automatically ping host

172.16.2.X IP address

pfSense Amazon VPC — Phase2

It's pretty much the same phase1 concerning Encryption and Hash algorithm, however note that we **Lifetime** has changed here, because all configuration must match in both sides (that's the way IPsec works).

Note in the last field “Automatically ping host” we have defined a 172.16.2.X which should be replaced to any host you have in Amazon, this keeps the tunnel UP and also brings the tunnel UP if there is any traffic.

Save and apply the changes in pfSense. By now, we have to configure a firewall rule under IPsec interface to allow traffic going through both ends. So, go to firewall -> Rules and then select IPsec interface there.

Firewall: Rules

FloatingWANLANIPsec

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule
	*	Amazon VPC SUBNET	*	LAN net	*	*	none	

pfSense Amazon VPC — IPsec firewall rules

Basically, all you need to do is create a firewall rule allowing traffic from Amazon VPC Subnet (172.16.2.0/24) to your LAN subnet (10.180.7.0/24 in this case).

Amazon side

Briefly, we need to add a route to all our instances in that specific VPC subnet (172.16.2.0/24) and create a new rule in Security Group allowing traffic from our network.

Starting with routes, go to “Route tables” in the left-side menu, select **your subnet** (172.16.2.0/24 in this case), choose “Route propagation” option at the bottom, and then select your Virtual Private Gateway recently created. This will automatically create a route to your network in all instances that are in such subnet — It may take few minutes to propagate to all your instances.

Route Tables ←

Internet Gateways
DHCP Options Sets
Elastic IPs

SECURITY

Network ACLs
Security Groups

VPN CONNECTIONS

Customer Gateways
Virtual Private Gateways
VPN Connections

1 Route Table selected

Route Table: rtb-

Routes Associations **Route Propagation** Tags

Select the virtual private gateways which are allowed to update this route table.

Virtual Private Gateways

vgw-

Select a Virtual Private Gateway ↓

pfSense Amazon VPC — Route table VGW

Choose then “Routes” option to see if your route was added correctly:

Route Table: rtb-

Routes Associations Route Propagation Tags

Destination	Target	Status	Propagated
172.16.2.0/24	local	active	No
10.180.7.0/24	vgw-	active	Yes

pfSense Amazon VPC — VPC routes

Note that we have two routes and two targets (Local|VGW), so we can confirm that our route was propagated to all instances in that VPC (Propagated = yes).

As a last thing, **don't forget** to update your Security Groups to allow traffic from your network ;)

Results

Check the VPN status on pfSense going to Status → IPsec, if not connected you can do a ping from your machine to any machine in Amazon forcing any sort of traffic through the VPN:

Status: IPsec

Overview SAD SPD Logs					
Local IP	Remote IP	Local Network	Remote Network	Description	Status
	87.238.85.44	LAN	172.16.2.0/24	Amazon VPC	▶

pfSense Amazon VPC — Tunnel UP

```
C:\Users\hlessa>ping 172.16.2.X

Pinging 172.16.2.X with 32 bytes of data:
Reply from 172.16.2.X: bytes=32 time=25ms TTL=62
Reply from 172.16.2.X: bytes=32 time=33ms TTL=62
Reply from 172.16.2.X: bytes=32 time=27ms TTL=62
Reply from 172.16.2.X: bytes=32 time=34ms TTL=62

Ping statistics for 172.16.2.X:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 34ms, Average = 29ms
```

pfSense Amazon VPC — Ping results

In case your VPN is still down, look into IPsec logs (Status → Logs → IPsec) and look for error there — They are always very helpful. But even though you could not figure out by yourself, feel free to post a comment here and I would be grateful to help.

PS: If you are experiencing some packet fragmentation, consider tuning your MTU/MSS accordingly.

Stay connected to the next tip if you use SFTP.