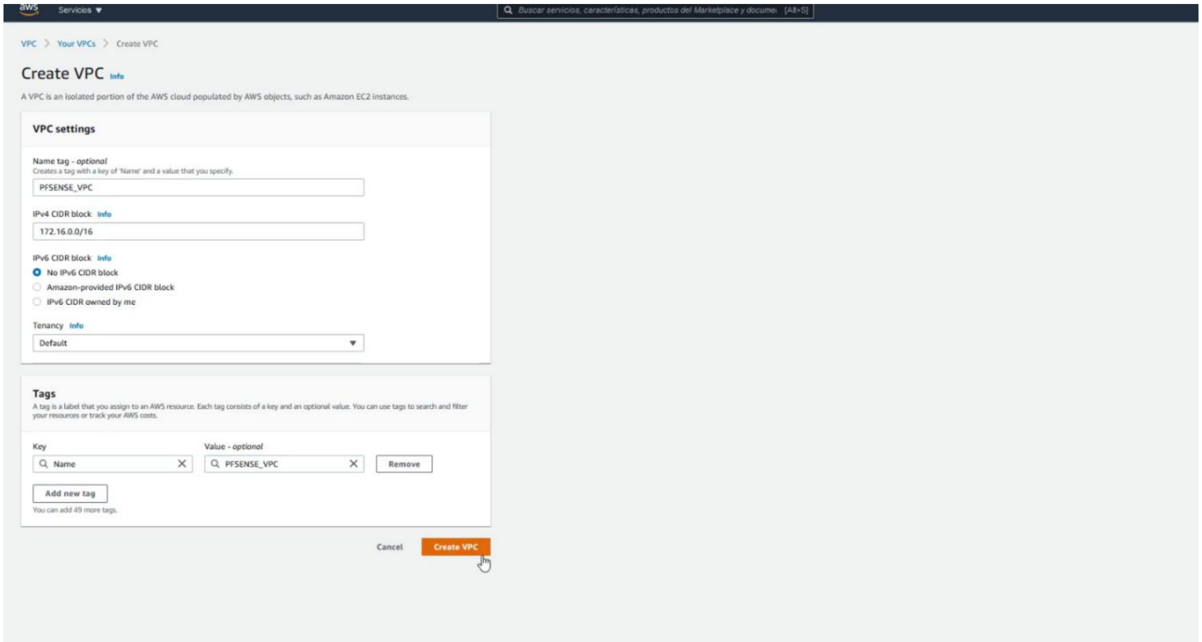
Universidad Mariano Gálvez de Guatemala
ingeniería en sistemas
Seguridad y Auditoria de sistemas
Proyecto Final: Implementación de PFSENSE

Luis Fernando Puluc Barrios
7690-16-5181

Cristian Alejandro Gómez Pérez
7690-10-9778

Para la implementación de pfsense es necesario la creación de una VPC la cual configuraremos de la siguiente manera.
En el menú izquierdo seleccionamos Your VPCs y procedemos a crearla.

Procedemos a ingresar los datos, la cual creamos como pesense_vpc con los siguientes datos.


aws
Services ▼
Buscar servicios, características, productos del Marketplace y docume [Alt+S]
VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
PFSENSE_VPC

IPv4 CIDR block Info
172.16.0.0/16

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy Info
Default

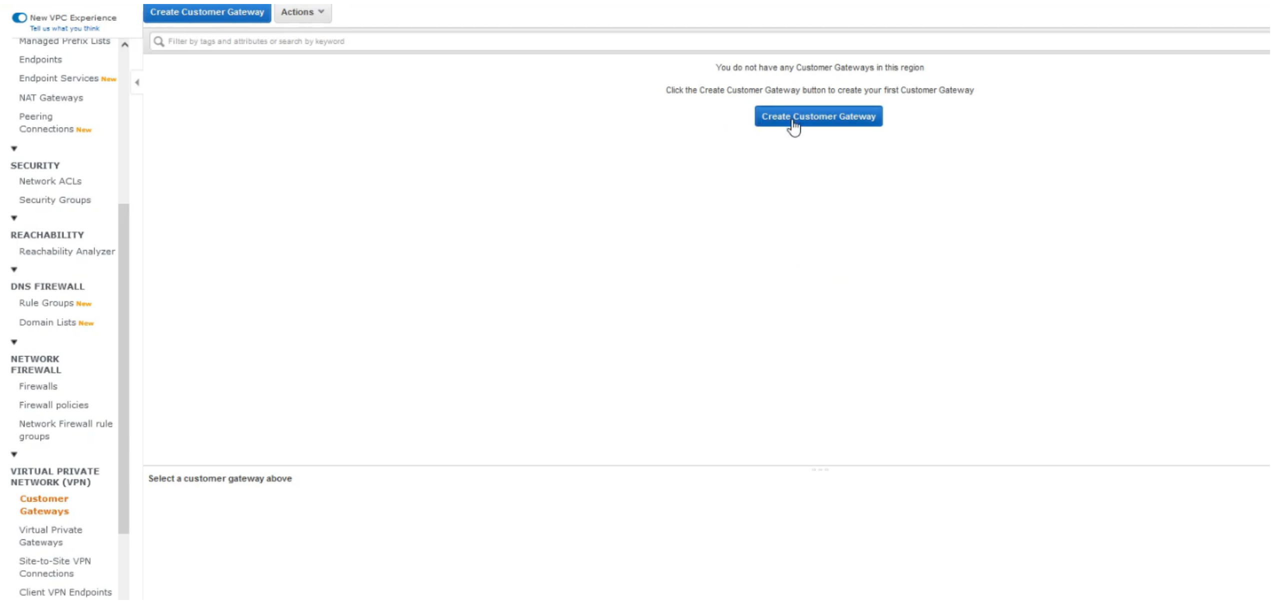
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	PFSENSE_VPC

You can add 49 more tags.

Es necesario crear el Peering Connectios para que este apunte a nuestro end-point.

.

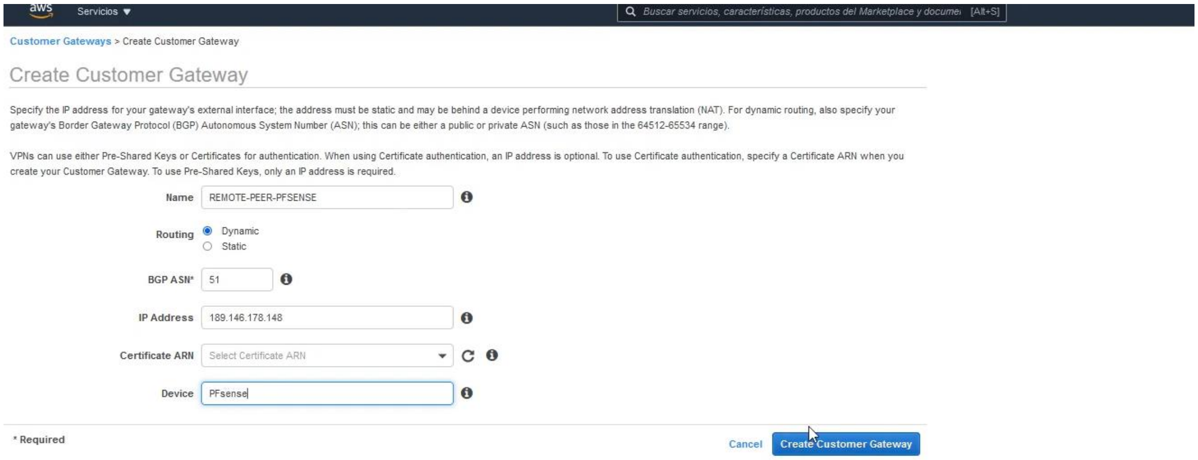


You do not have any Customer Gateways in this region

Click the Create Customer Gateway button to create your first Customer Gateway

Select a customer gateway above

Prcedemos a dar clic en créate customer Gateway luego ingresaremos el BGP ASN este es el sistema autono del Peering Connectios


aws
Servicios
Buscar servicios, características, productos del Marketplace y docume [Alt+S]
Customer Gateways > Create Customer Gateway
Cancel
Create Customer Gateway

Create Customer Gateway

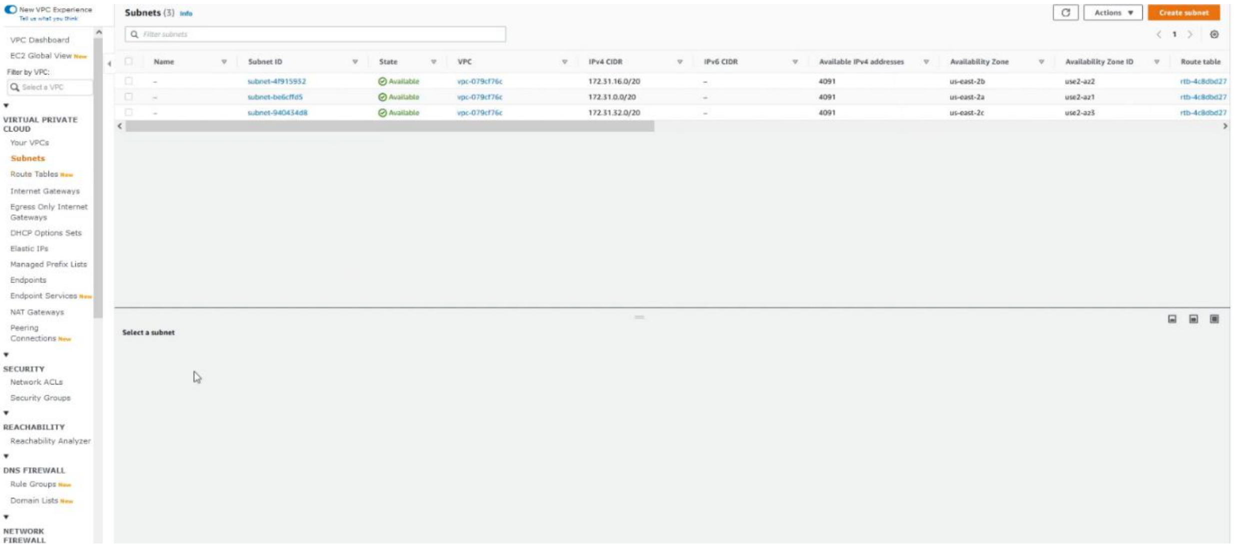
Specify the IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

VPNs can use either Pre-Shared Keys or Certificates for authentication. When using Certificate authentication, an IP address is optional. To use Certificate authentication, specify a Certificate ARN when you create your Customer Gateway. To use Pre-Shared Keys, only an IP address is required.

Name	REMOTE-PEER-PFSENSE
Routing	● Dynamic ○ Static
BGP ASN*	51
IP Address	189.146.178.148
Certificate ARN	Select Certificate ARN
Device	PFsense

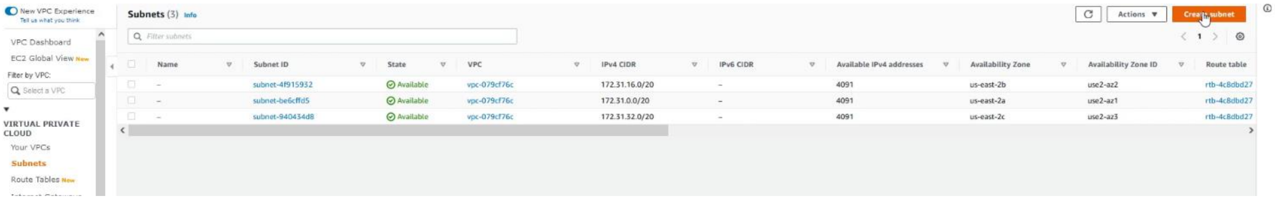
* Required

Es necesario crear Subnets, ya por defecto AWS nos proporciona una cantidad de subnet por default, procedemos a agregar una nueva.



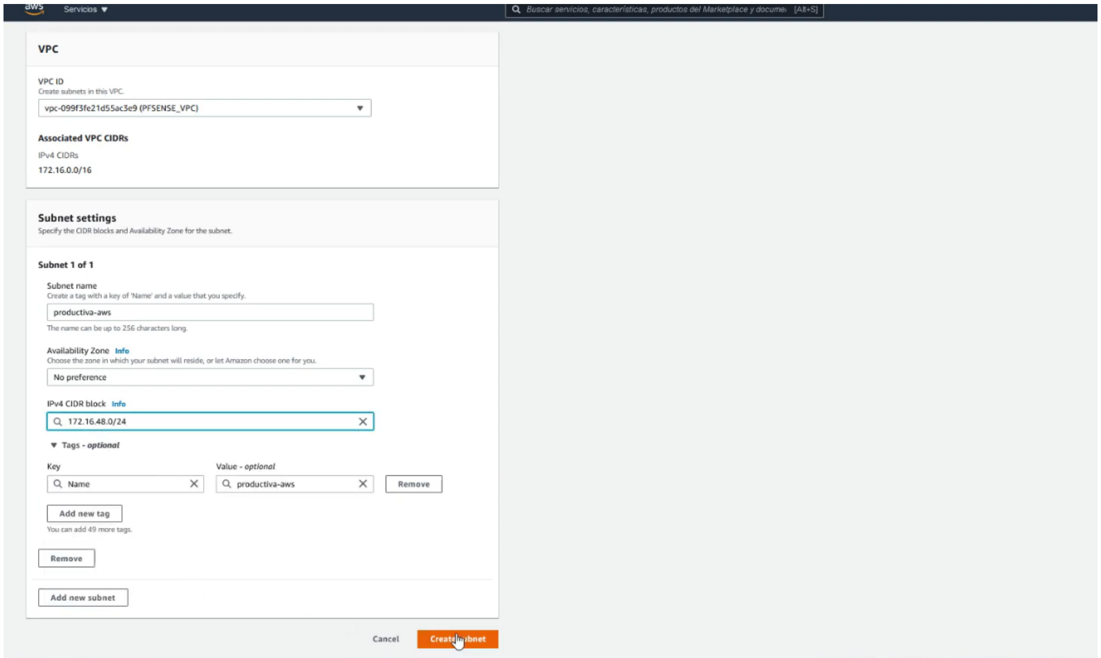
Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID	Route table
–	subnet-4f915932	Available	vpc-079cf76c	172.31.16.0/20	–	4091	us-east-2b	use2-az2	rtb-4c8dbd27
–	subnet-be6cffd5	Available	vpc-079cf76c	172.31.0.0/20	–	4091	us-east-2a	use2-az1	rtb-4c8dbd27
–	subnet-940434d8	Available	vpc-079cf76c	172.31.32.0/20	–	4091	us-east-2c	use2-az3	rtb-4c8dbd27

Procedemos a crear la nueva subnet.



Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID	Route table
–	subnet-4f915932	Available	vpc-079cf76c	172.31.16.0/20	–	4091	us-east-2b	use2-az2	rtb-4c8dbd27
–	subnet-be6cffd5	Available	vpc-079cf76c	172.31.0.0/20	–	4091	us-east-2a	use2-az1	rtb-4c8dbd27
–	subnet-940434d8	Available	vpc-079cf76c	172.31.32.0/20	–	4091	us-east-2c	use2-az3	rtb-4c8dbd27

Ingresamos el rango de IP a utilizar y procedemos a crear la subnet.


aws
Servicios ▼
Buscar servicios, características, productos del Marketplace y docume [Alt+S]
Add new tag
Remove
Add new subnet
Cancel
Create subnet

VPC

VPC ID
Create subnets in this VPC.
vpc-099f3fe21d55ac3e9 (PFSENSE_VPC)

Associated VPC CIDRs
IPv4 CIDRs
172.16.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
productiva-aws
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

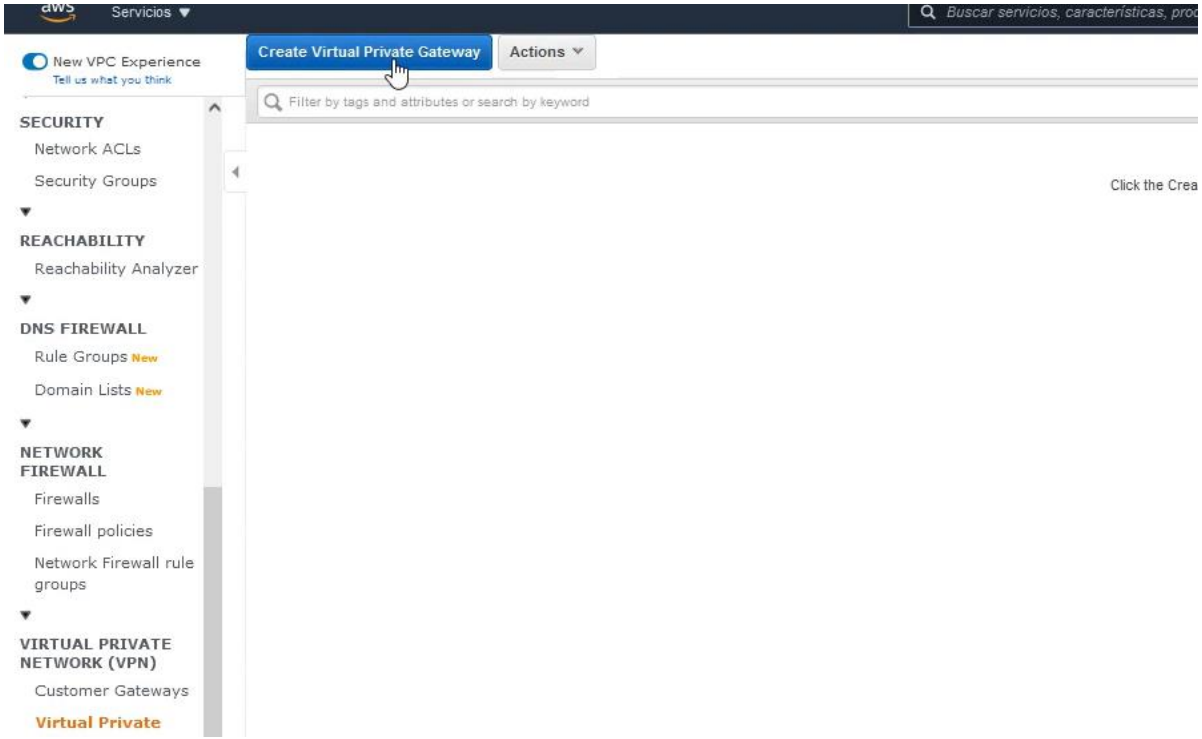
IPv4 CIDR block Info
172.16.48.0/24

▼ Tags - *optional*

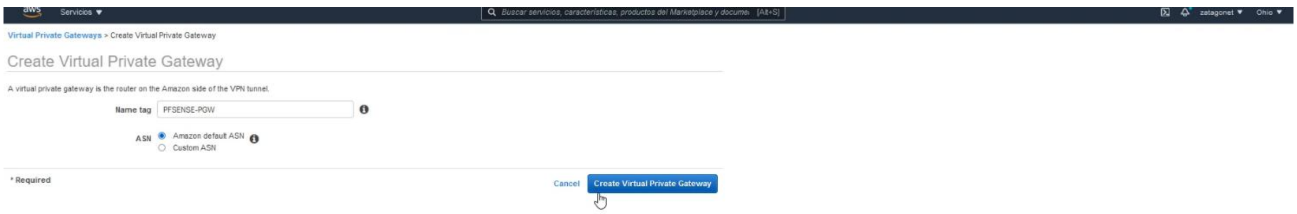
Key	Value - *optional*
Name	productiva-aws

You can add 49 more tags.

Es necesario crear la Gateway private, esta se utilizara para dirigier el trafico de nuestro Gateway private a nuestro VPC.



Al momento de crearla es necesario asignarle en ASN default de aws, este permitirá que tome el sistema autónomo de aws.



aws
Servicios ▼
Buscar servicios, características, productos del Marketplace y docume [Alt+S]
zatagonet ▼
Ohio ▼
Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

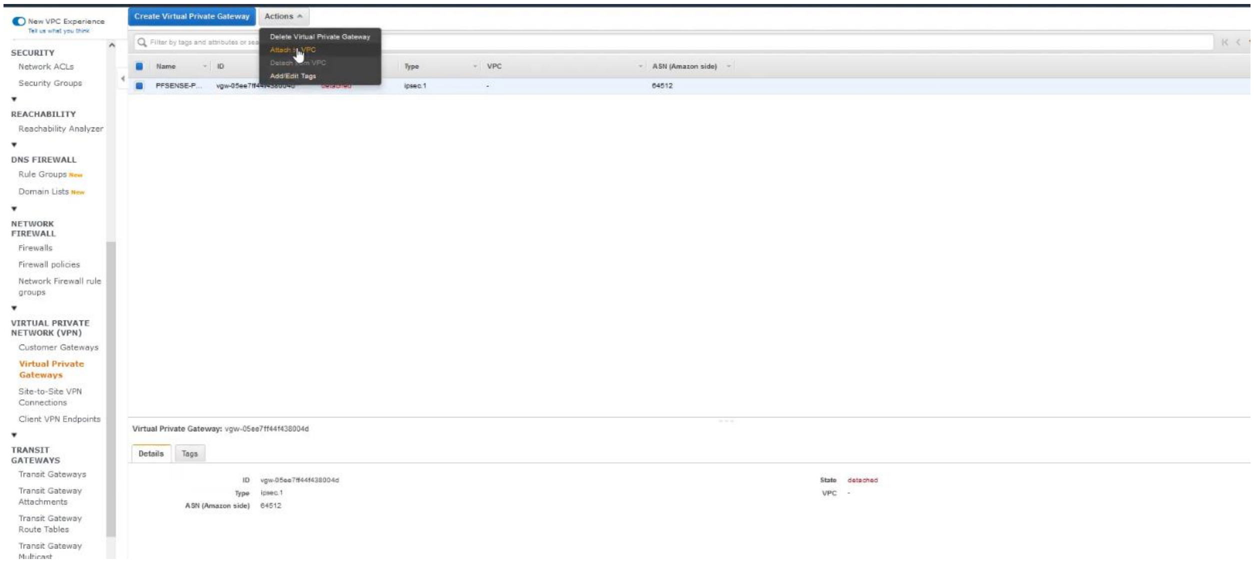
Name tag: PFSENSE-PGW

ASN: ● Amazon default ASN ○ Custom ASN

* Required

Cancel
Create Virtual Private Gateway

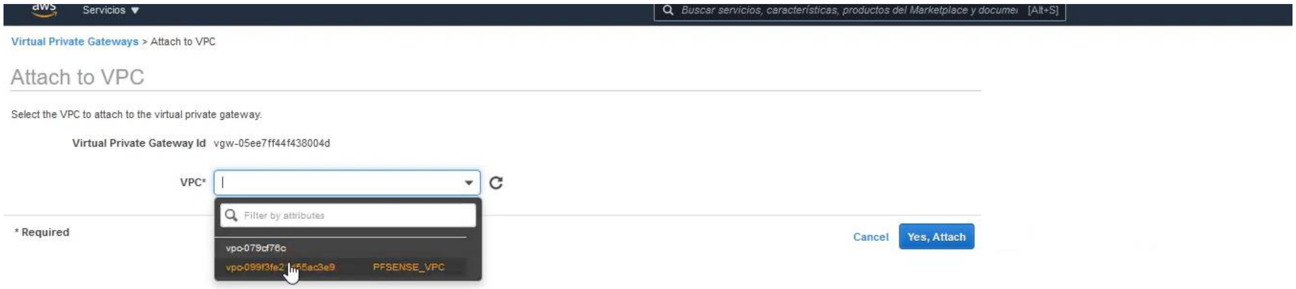
Luego de haberla creado es necesario añadirla a nuestra VPC



Name	ID		Type	VPC	ASN (Amazon side)
PFSENSE-P...	vgw-05ee7ff44f438004d	detached	ipsec.1	-	64512

Virtual Private Gateway: vgw-05ee7ff44f438004d

ID: vgw-05ee7ff44f438004d
Type: ipsec.1
ASN (Amazon side): 64512
State: detached
VPC: -


Servicios ▼
Buscar servicios, características, productos del Marketplace y documen [Alt+S]
Filter by attributes
Cancel
Yes, Attach

Virtual Private Gateways > Attach to VPC

Attach to VPC

Select the VPC to attach to the virtual private gateway.

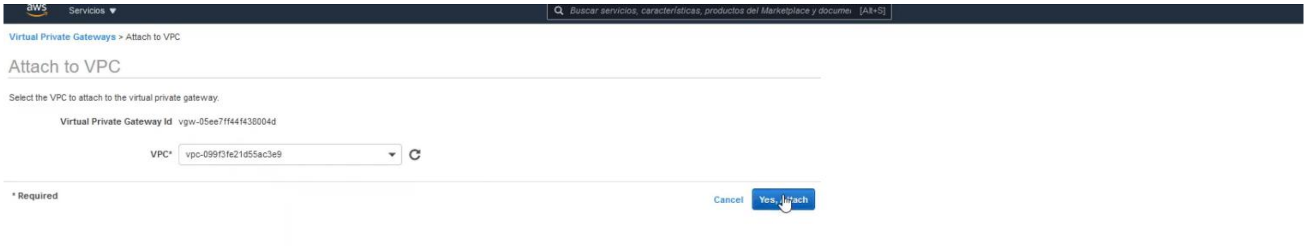
Virtual Private Gateway Id vgw-05ee7ff44f438004d

VPC* |

vpc-079cf76c

vpc-099f3fe21d55ac3e9 PFSENSE_VPC

* Required


Servicios ▼
Buscar servicios, características, productos del Marketplace y documen [Alt+S]
Cancel
Yes, Attach

Virtual Private Gateways > Attach to VPC

Attach to VPC

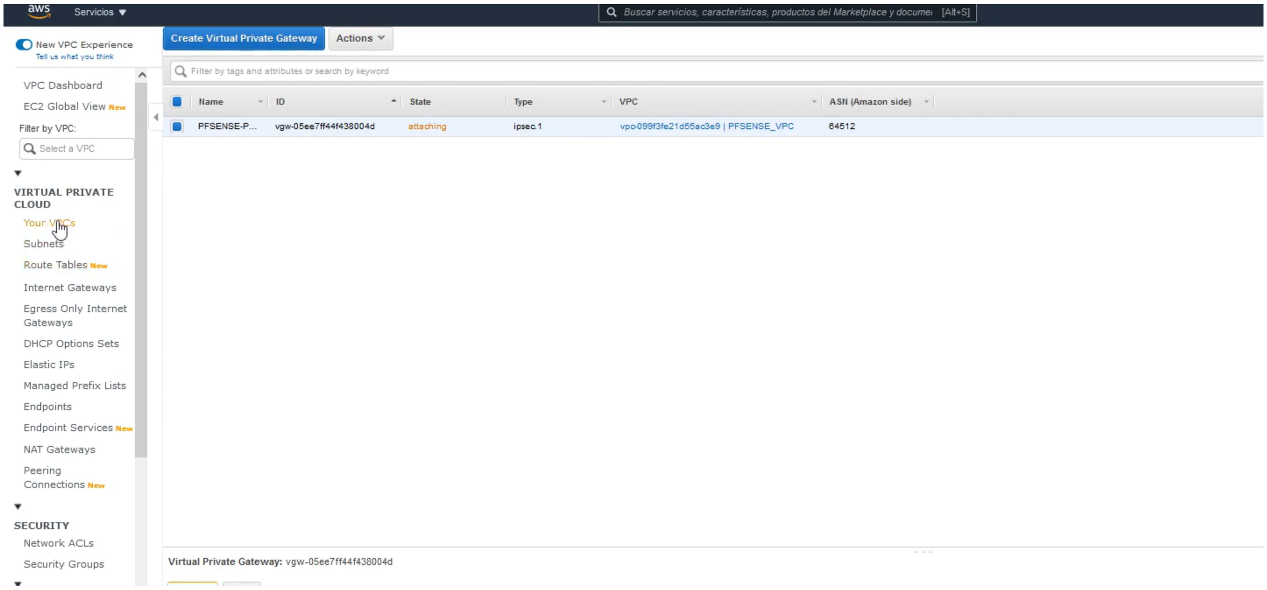
Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id vgw-05ee7ff44f438004d

VPC* vpc-099f3fe21d55ac3e9

* Required

La VPC ya fue asignada a nuestra Gateway.

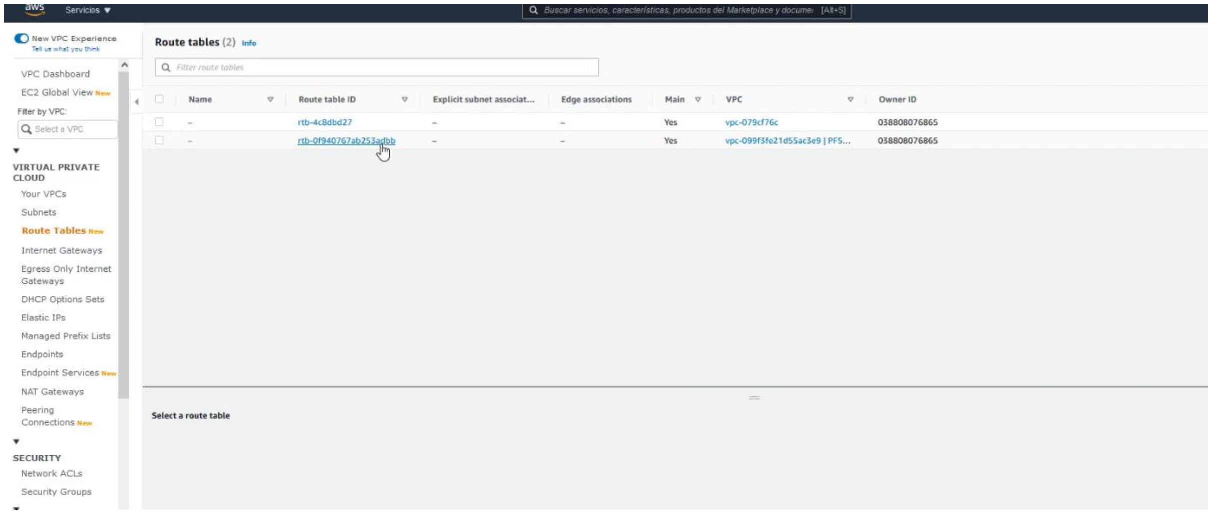


Name	ID	State	Type	VPC	ASN (Amazon side)
PFSENSE-P...	vgw-05ee7ff44f438004d	attaching	ipsec.1	vpc-099f3fe21d55ac3e9 | PFSENSE_VPC	64512

Virtual Private Gateway: vgw-05ee7ff44f438004d

Es necesario realizar la degeneración de BGP sobre la tabla de ruteo.

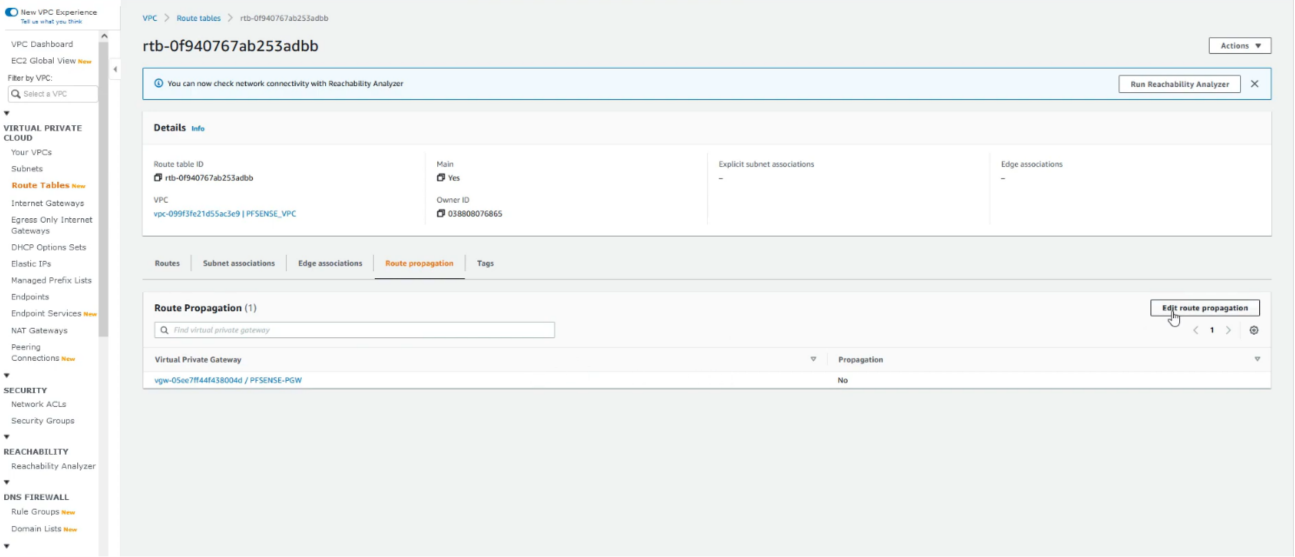
Precedemos a activarlo.



Route tables (2)

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
–	rtb-4c8dbd27	–	–	Yes	vpc-079cf76c	038808076865
–	rtb-0f940767ab253adbb	–	–	Yes	vpc-099f3fe21d55ac3e9 | PFS...	038808076865

Select a route table



rtb-0f940767ab253adbb

You can now check network connectivity with Reachability Analyzer

Details

Route table ID: rtb-0f940767ab253adbb

VPC: vpc-099f3fe21d55ac3e9 | PFSENSE_VPC

Main: Yes

Owner ID: 038808076865

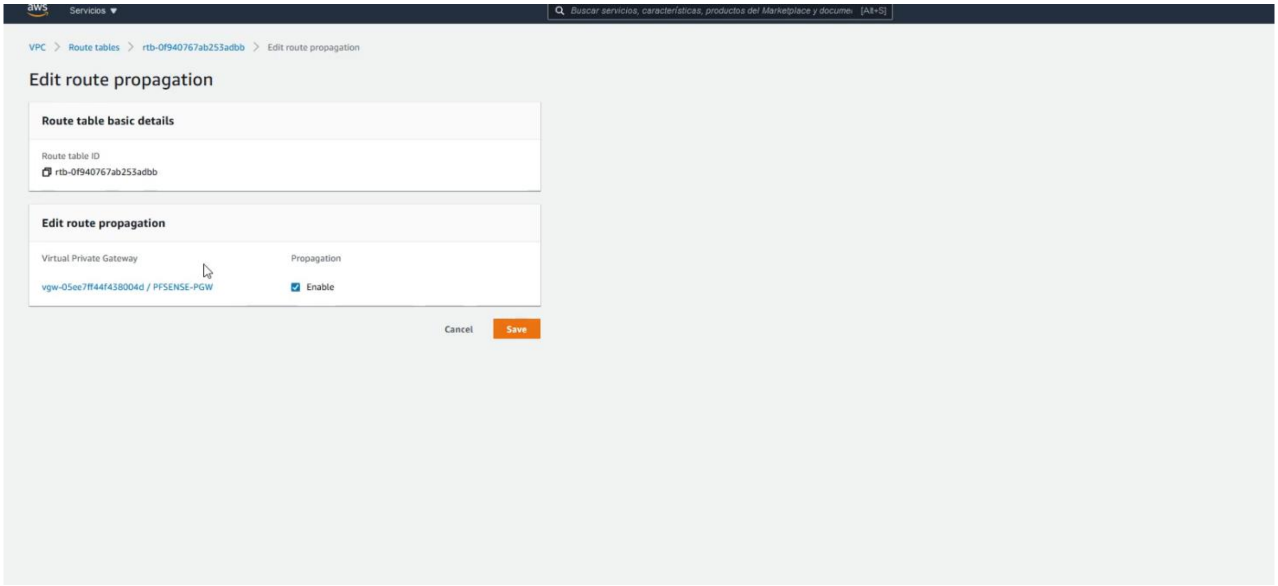
Explicit subnet associations: –

Edge associations: –

Route Propagation (1)

Virtual Private Gateway	Propagation
vgw-05ee7ff44f438004d / PFSENSE-PGW	No

Procedemos a habilitar la propagación


aws
Servicios
Buscar servicios, características, productos del Marketplace y docume [Alt+S]
VPC > Route tables > rtb-0f940767ab253adbb > Edit route propagation
Cancel
Save

Edit route propagation

Route table basic details

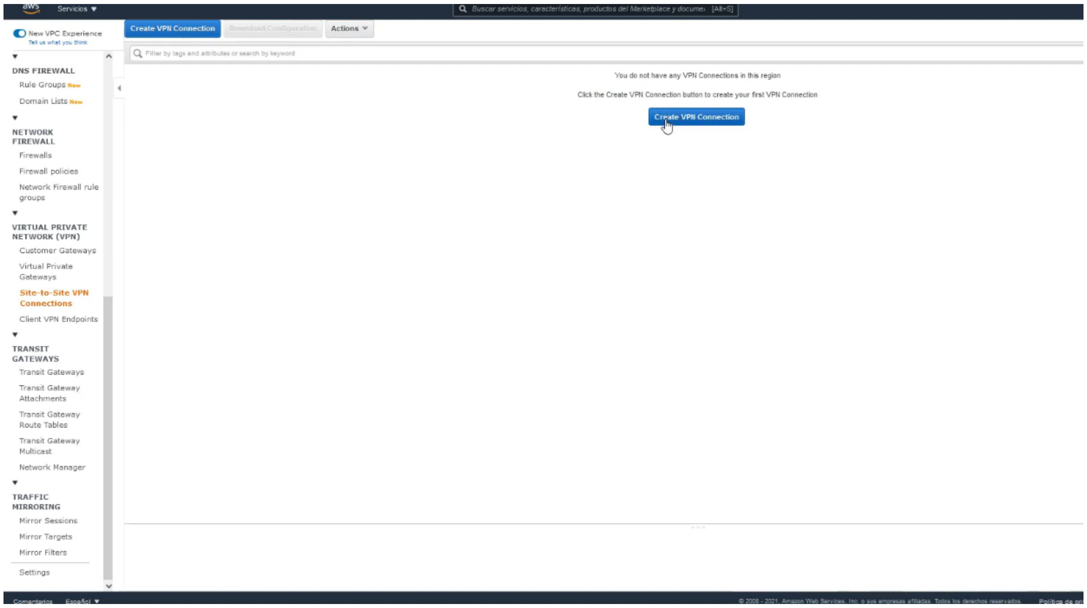
Route table ID: rtb-0f940767ab253adbb

Edit route propagation

Virtual Private Gateway	Propagation
vgw-05ee7ff44f438004d / PFSENSE-PGW	☑ Enable

Habilitamos con clic la propagación y procedemos a guardar.

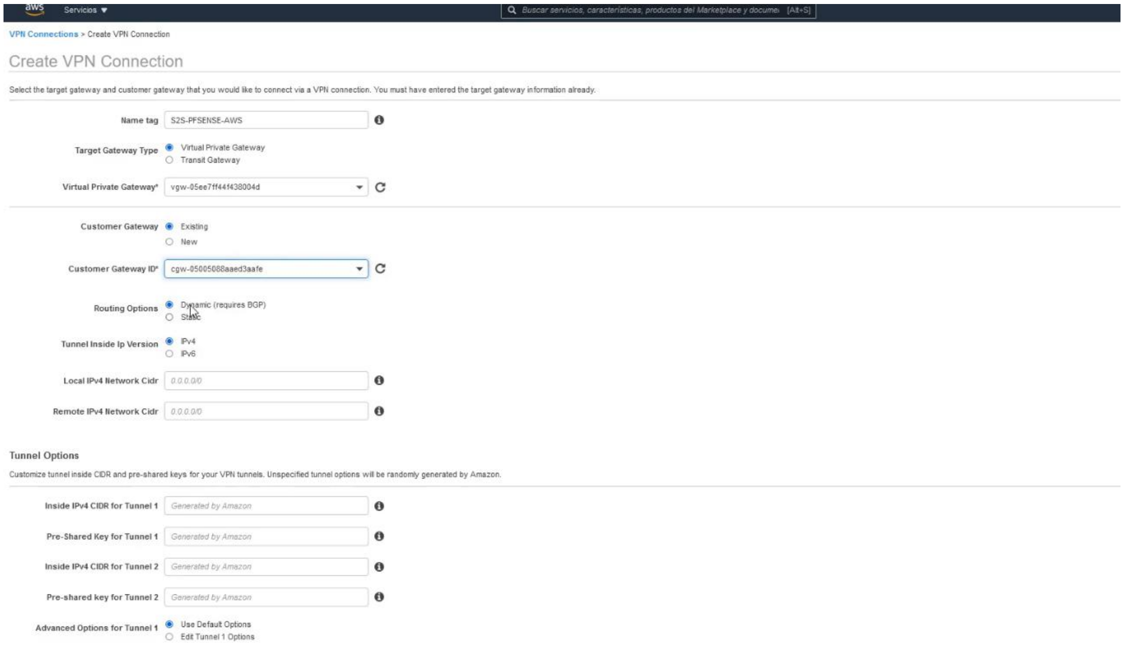
Es necesario crear la VPN site-to-site, por lo que procedemos a crearla.



You do not have any VPN Connections in this region

Click the Create VPN Connection button to create your first VPN Connection

Ingresamos los paremetros necesarios con las configuraciones anteriormente creadas y los datos que dejaremos en blanco tomaran los datos predefinidos de AWS


aws
Servicios ▼
Buscar servicios, características, productos del Marketplace y docume [Alt+S]
VPN Connections > Create VPN Connection

Create VPN Connection

Select the target gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the target gateway information already.

Name tag: S2S-PFSENSE-AWS

Target Gateway Type: ● Virtual Private Gateway ○ Transit Gateway

Virtual Private Gateway*: vgw-05ee7ff44f438004d

Customer Gateway: ● Existing ○ New

Customer Gateway ID*: cgw-05005088aaed3aafe

Routing Options: ● Dynamic (requires BGP) ○ Static

Tunnel Inside Ip Version: ● IPv4 ○ IPv6

Local IPv4 Network Cidr: 0.0.0.0/0

Remote IPv4 Network Cidr: 0.0.0.0/0

Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IPv4 CIDR for Tunnel 1: Generated by Amazon

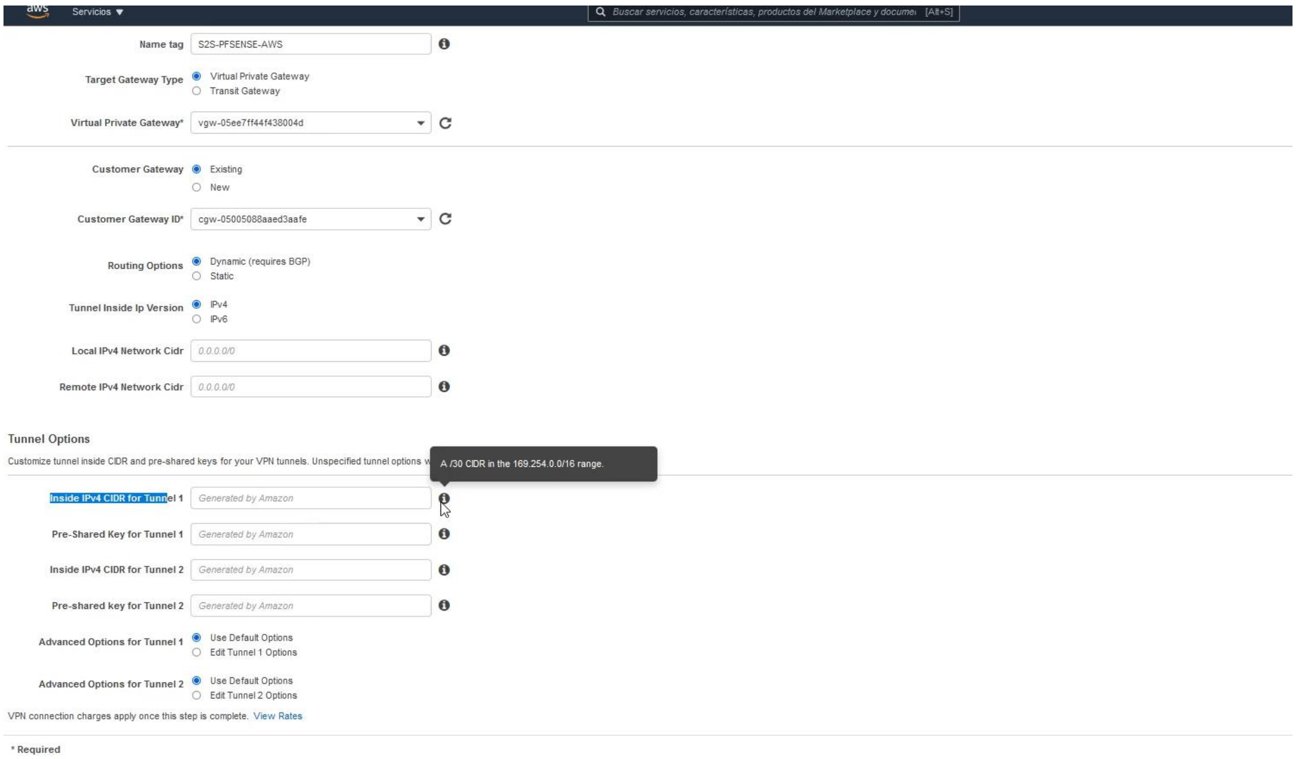
Pre-Shared Key for Tunnel 1: Generated by Amazon

Inside IPv4 CIDR for Tunnel 2: Generated by Amazon

Pre-shared key for Tunnel 2: Generated by Amazon

Advanced Options for Tunnel 1: ● Use Default Options ○ Edit Tunnel 1 Options

Como podemos ver AWS nos asigna de forma automática los segmentos.



aws
Servicios ▼
Buscar servicios, características, productos del Marketplace y docume [Alt+S]

Name tag: S2S-PFSENSE-AWS

Target Gateway Type: ● Virtual Private Gateway ○ Transit Gateway

Virtual Private Gateway*: vgw-05ee7ff44f438004d

Customer Gateway: ● Existing ○ New

Customer Gateway ID*: cgw-05005088aaed3aafe

Routing Options: ● Dynamic (requires BGP) ○ Static

Tunnel Inside Ip Version: ● IPv4 ○ IPv6

Local IPv4 Network Cidr: 0.0.0.0/0

Remote IPv4 Network Cidr: 0.0.0.0/0

Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options w

A /30 CIDR in the 169.254.0.0/16 range.

Inside IPv4 CIDR for Tunnel 1: Generated by Amazon

Pre-Shared Key for Tunnel 1: Generated by Amazon

Inside IPv4 CIDR for Tunnel 2: Generated by Amazon

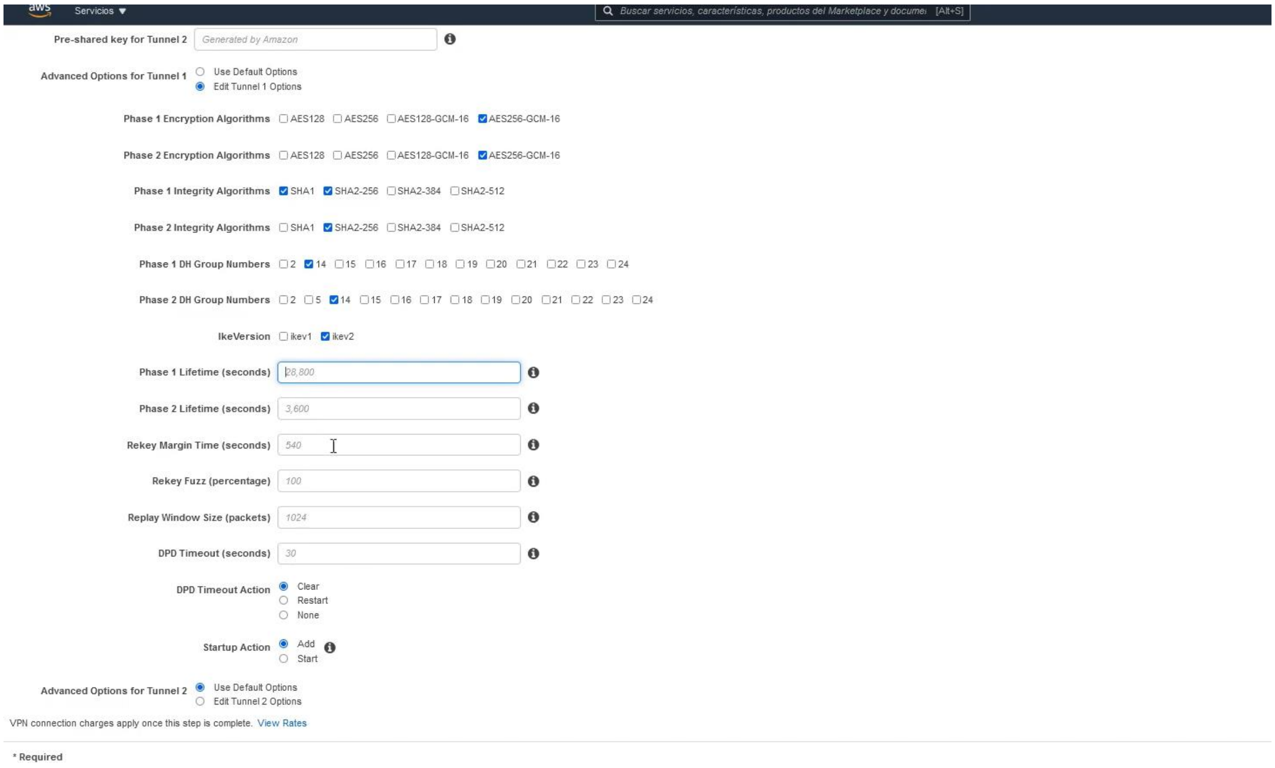
Pre-shared key for Tunnel 2: Generated by Amazon

Advanced Options for Tunnel 1: ● Use Default Options ○ Edit Tunnel 1 Options

Advanced Options for Tunnel 2: ● Use Default Options ○ Edit Tunnel 2 Options

VPN connection charges apply once this step is complete. View Rates

* Required



aws
Servicios ▼
Buscar servicios, características, productos del Marketplace y docume [Alt+S]

Pre-shared key for Tunnel 2: Generated by Amazon

Advanced Options for Tunnel 1: ○ Use Default Options ● Edit Tunnel 1 Options

Phase 1 Encryption Algorithms: □ AES128 □ AES256 □ AES128-GCM-16 ☑ AES256-GCM-16

Phase 2 Encryption Algorithms: □ AES128 □ AES256 □ AES128-GCM-16 ☑ AES256-GCM-16

Phase 1 Integrity Algorithms: ☑ SHA1 ☑ SHA2-256 □ SHA2-384 □ SHA2-512

Phase 2 Integrity Algorithms: □ SHA1 ☑ SHA2-256 □ SHA2-384 □ SHA2-512

Phase 1 DH Group Numbers: □ 2 ☑ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24

Phase 2 DH Group Numbers: □ 2 □ 5 ☑ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24

IkeVersion: □ ikev1 ☑ ikev2

Phase 1 Lifetime (seconds): 28,800

Phase 2 Lifetime (seconds): 3,600

Rekey Margin Time (seconds): 540

Rekey Fuzz (percentage): 100

Replay Window Size (packets): 1024

DPD Timeout (seconds): 30

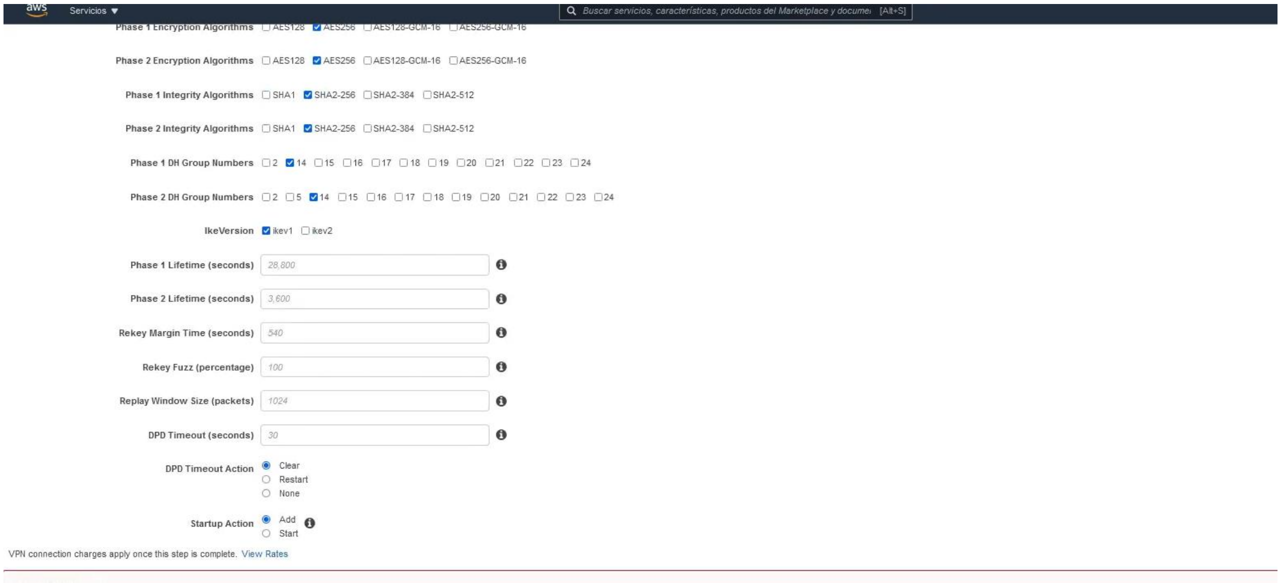
DPD Timeout Action: ● Clear ○ Restart ○ None

Startup Action: ● Add ○ Start

Advanced Options for Tunnel 2: ● Use Default Options ○ Edit Tunnel 2 Options

VPN connection charges apply once this step is complete. View Rates

* Required



aws
Servicios ▼
Buscar servicios, características, productos del Marketplace y docume [Alt+S]

Phase 1 Encryption Algorithms ☐ AES128 ☑ AES256 ☐ AES128-GCM-16 ☐ AES256-GCM-16

Phase 2 Encryption Algorithms ☐ AES128 ☑ AES256 ☐ AES128-GCM-16 ☐ AES256-GCM-16

Phase 1 Integrity Algorithms ☐ SHA1 ☑ SHA2-256 ☐ SHA2-384 ☐ SHA2-512

Phase 2 Integrity Algorithms ☐ SHA1 ☑ SHA2-256 ☐ SHA2-384 ☐ SHA2-512

Phase 1 DH Group Numbers ☐ 2 ☑ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24

Phase 2 DH Group Numbers ☐ 2 ☐ 5 ☑ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24

IkeVersion ☑ ikev1 ☐ ikev2

Phase 1 Lifetime (seconds) 28,800

Phase 2 Lifetime (seconds) 3,600

Rekey Margin Time (seconds) 540

Rekey Fuzz (percentage) 100

Replay Window Size (packets) 1024

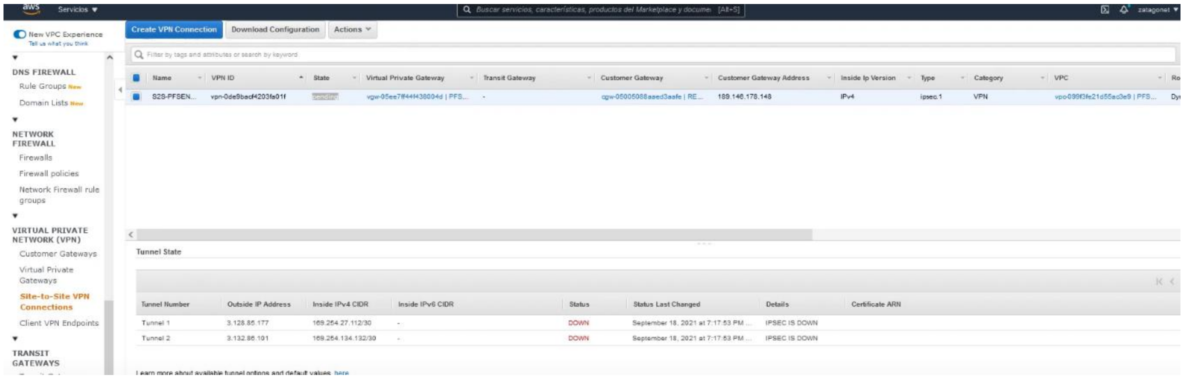
DPD Timeout (seconds) 30

DPD Timeout Action ● Clear ○ Restart ○ None

Startup Action ● Add ○ Start

VPN connection charges apply once this step is complete. View Rates

Luego de proceder a guardar validamos su creación correctamente.



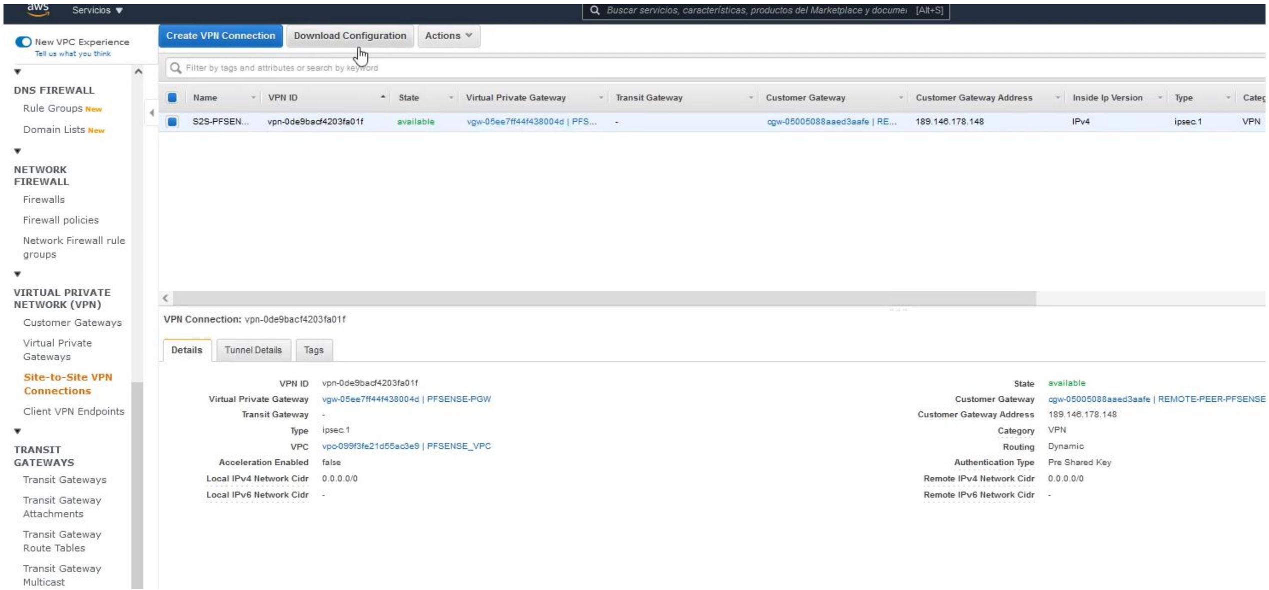
Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Address	Inside Ip Version	Type	Category	VPC	Ro
S2S-PFSEN...	vpn-0de9bacf4203fa01f	pending	vgw-05ee7ff44f438004d | PFS...	-	cgw-05005088aaed3aafe | RE...	189.146.178.148	IPv4	ipsec.1	VPN	vpc-099f3fe21d55ac3e9 | PFS...	Dy

Tunnel State

Tunnel Number	Outside IP Address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Status Last Changed	Details	Certificate ARN
Tunnel 1	3.128.85.177	169.254.27.112/30	-	DOWN	September 18, 2021 at 7:17:53 PM ...	IPSEC IS DOWN	
Tunnel 2	3.132.86.101	169.254.134.132/30	-	DOWN	September 18, 2021 at 7:17:53 PM ...	IPSEC IS DOWN	

Learn more about available tunnel options and default values. here

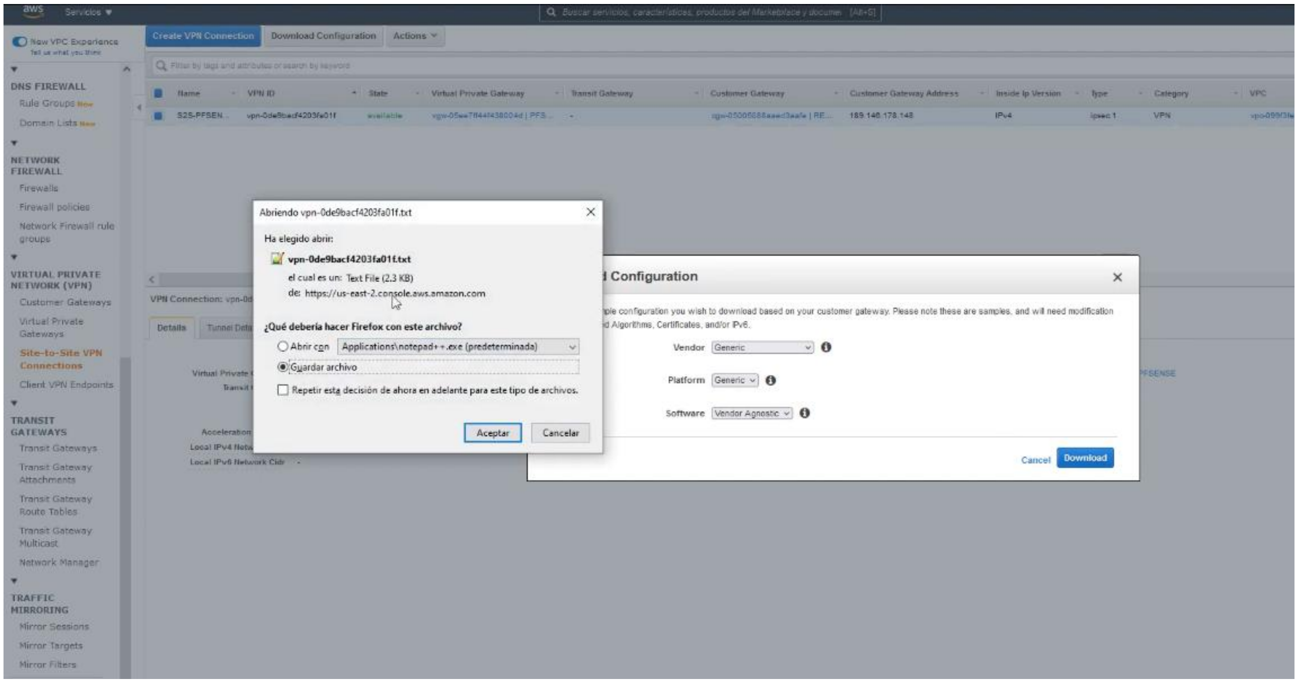
Para realizar la configuración de PFSENSE AWS nos facilita las configuraciones en un TXT el cual trae todos los parámetros para la configuración de pfsense



Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Address	Inside Ip Version	Type	Categ
S2S-PFSEN...	vpn-0de9bacf4203fa01f	available	vgw-05ee7ff44f438004d | PFS...	-	cgw-05005088aaed3aafe | RE...	189.146.178.148	IPv4	ipsec.1	VPN

VPN Connection: vpn-0de9bacf4203fa01f

VPN ID	vpn-0de9bacf4203fa01f	State	available
Virtual Private Gateway	vgw-05ee7ff44f438004d | PFSENSE-PGW	Customer Gateway	cgw-05005088aaed3aafe | REMOTE-PEER-PFSENSE
Transit Gateway	-	Customer Gateway Address	189.146.178.148
Type	ipsec.1	Category	VPN
VPC	vpc-099f3fe21d55ac3e9 | PFSENSE_VPC	Routing	Dynamic
Acceleration Enabled	false	Authentication Type	Pre Shared Key
Local IPv4 Network Cidr	0.0.0.0/0	Remote IPv4 Network Cidr	0.0.0.0/0
Local IPv6 Network Cidr	-	Remote IPv6 Network Cidr	-



Abriendo vpn-0de9bacf4203fa01f.txt

Ha elegido abrir:

vpn-0de9bacf4203fa01f.txt

el cual es un: Text File (2.3 KB)

de: https://us-east-2.console.aws.amazon.com

¿Qué debería hacer Firefox con este archivo?

○ Abrir con Applications\notepad++.exe (predeterminada)

● Guardar archivo

□ Repetir esta decisión de ahora en adelante para este tipo de archivos.

Aceptar | Cancelar

d Configuration

nple configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification d Algorithms, Certificates, and/or IPv6.

Vendor: Generic

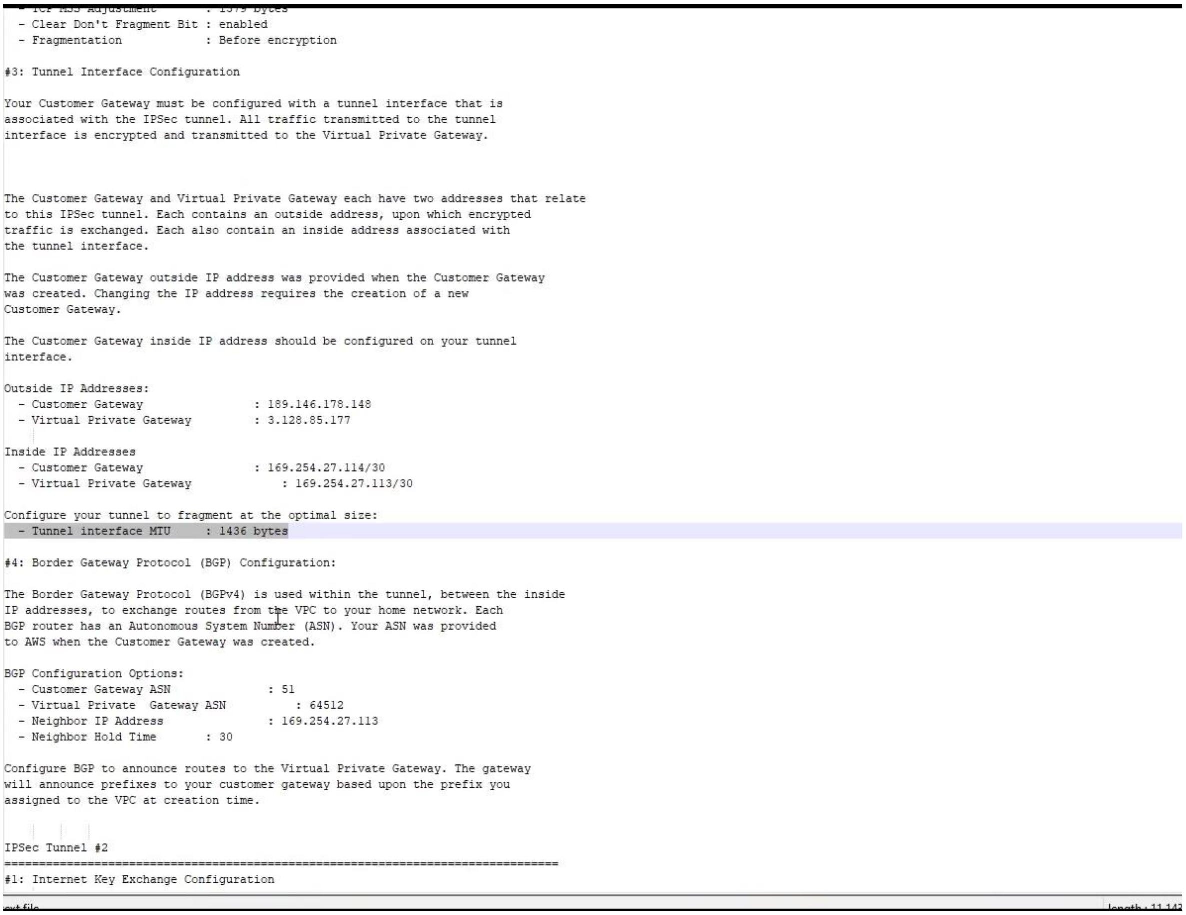
Platform: Generic

Software: Vendor Agnostic

Cancel | Download

Luego de guardarlos procedemos a realizar la configuración de pfsense con las configuraciones necesarias locales y luego la de aws de la siguiente manera.

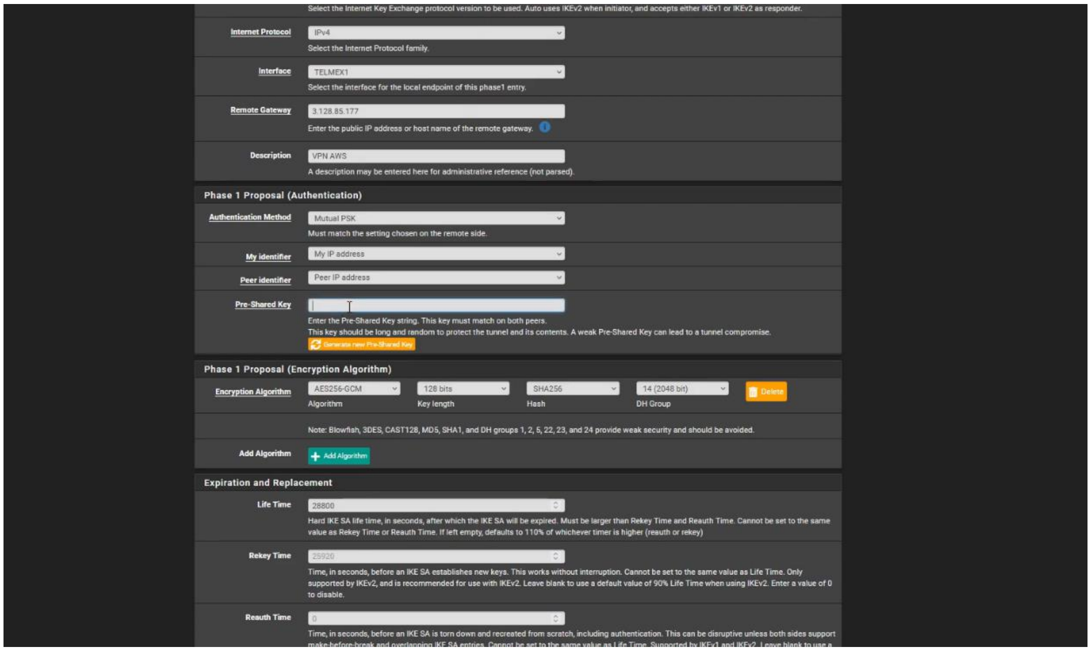
Validando el archivo descargado de aws



```
  - TCP MSS Adjustment       : 1379 bytes
  - Clear Don't Fragment Bit : enabled
  - Fragmentation            : Before encryption

#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is
associated with the IPSec tunnel. All traffic transmitted to the tunnel
interface is encrypted and transmitted to the Virtual Private Gateway.



The Customer Gateway and Virtual Private Gateway each have two addresses that relate
to this IPSec tunnel. Each contains an outside address, upon which encrypted
traffic is exchanged. Each also contain an inside address associated with
the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer Gateway
was created. Changing the IP address requires the creation of a new
Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel
interface.

Outside IP Addresses:
  - Customer Gateway               : 189.146.178.148
  - Virtual Private Gateway        : 3.128.85.177

Inside IP Addresses
  - Customer Gateway               : 169.254.27.114/30
  - Virtual Private Gateway            : 169.254.27.113/30

Configure your tunnel to fragment at the optimal size:
  - Tunnel interface MTU     : 1436 bytes

#4: Border Gateway Protocol (BGP) Configuration:

The Border Gateway Protocol (BGPv4) is used within the tunnel, between the inside
IP addresses, to exchange routes from the VPC to your home network. Each
BGP router has an Autonomous System Number (ASN). Your ASN was provided
to AWS when the Customer Gateway was created.

BGP Configuration Options:
  - Customer Gateway ASN             : 51
  - Virtual Private  Gateway ASN         : 64512
  - Neighbor IP Address              : 169.254.27.113
  - Neighbor Hold Time       : 30

Configure BGP to announce routes to the Virtual Private Gateway. The gateway
will announce prefixes to your customer gateway based upon the prefix you
assigned to the VPC at creation time.


IPSec Tunnel #2
================================================================================
#1: Internet Key Exchange Configuration
```

Realizamos las siguiente configuraciones con PFSENSE

Para que PFSENSE funcione con AWS y las configuraciones coincidan con las realizadas con AWS se debe de configurar de la siguiente manera con los siguientes parámetros.



Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol: IPv4
Select the Internet Protocol family.

Interface: TELMEX1
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway: 3.128.85.177
Enter the public IP address or host name of the remote gateway.

Description: VPN AWS
A description may be entered here for administrative 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:
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm: AES256-GCM (Algorithm), 128 bits (Key length), SHA256 (Hash), 14 (2048 bit) (DH Group)

Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

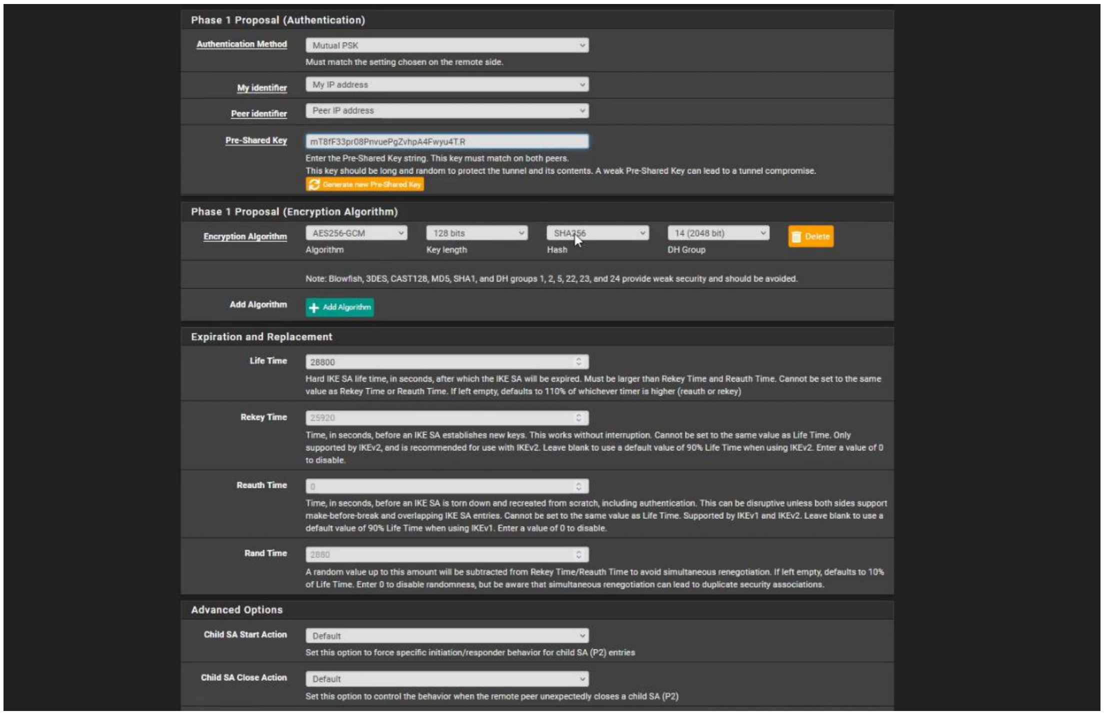
Add Algorithm

Expiration and Replacement

Life Time: 28800
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

Rekey Time: 25920
Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.

Reauth Time: 0
Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a



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: mT8fF33pr08PnvuePgZvhpA4Fwyu4T.R
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm: AES256-GCM (Algorithm), 128 bits (Key length), SHA256 (Hash), 14 (2048 bit) (DH Group)

Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm

Expiration and Replacement

Life Time: 28800
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

Rekey Time: 25920
Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.

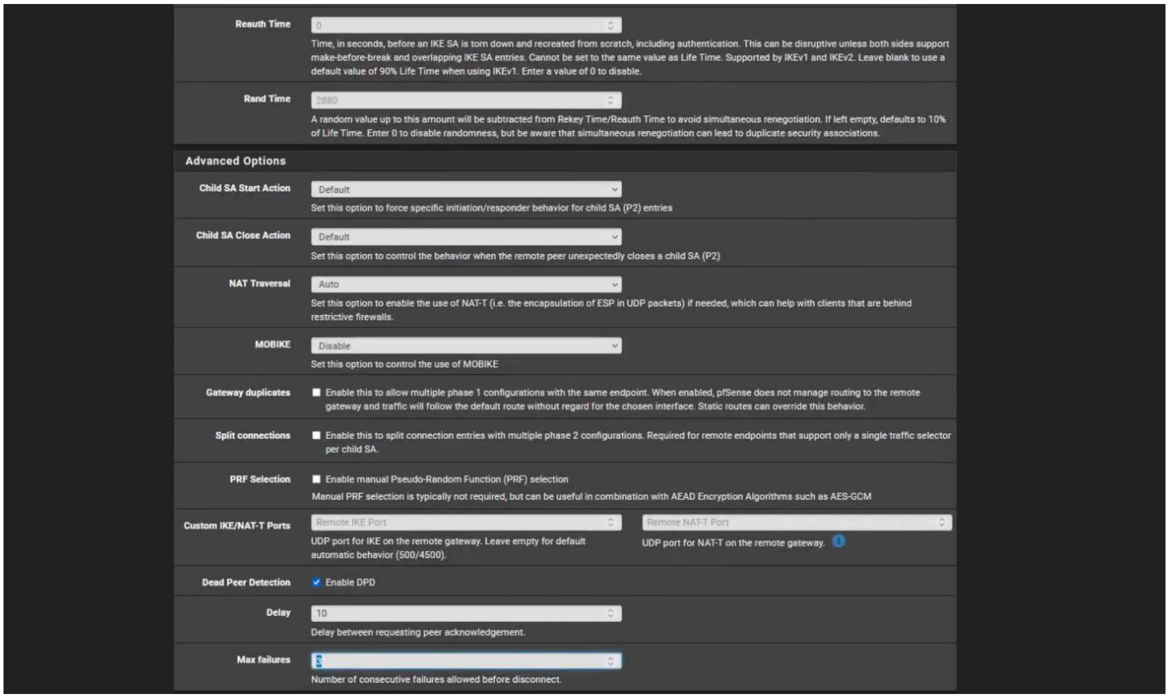
Reauth Time: 0
Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.

Rand Time: 2880
A random value up to this amount will be subtracted from Rekey Time/Reauth Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Advanced Options

Child SA Start Action: Default
Set this option to force specific initiation/responder behavior for child SA (P2) entries

Child SA Close Action: Default
Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)



Reauth Time 0

Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.

Rand Time 2880

A random value up to this amount will be subtracted from Rekey Time/Reauth Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Advanced Options

Child SA Start Action Default

Set this option to force specific initiation/responder behavior for child SA (P2) entries

Child SA Close Action Default

Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)

NAT Traversal Auto

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.

MOBIKE Disable

Set this option to control the use of MOBIKE

Gateway duplicates □ Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pfSense does not manage routing to the remote gateway and traffic will follow the default route without regard for the chosen interface. Static routes can override this behavior.

Split connections □ Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.

PRF Selection □ Enable manual Pseudo-Random Function (PRF) selection

Manual PRF selection is typically not required, but can be useful in combination with AEAD Encryption Algorithms such as AES-GCM

Custom IKE/NAT-T Ports Remote IKE Port | Remote NAT-T Port

UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500).

UDP port for NAT-T on the remote gateway.

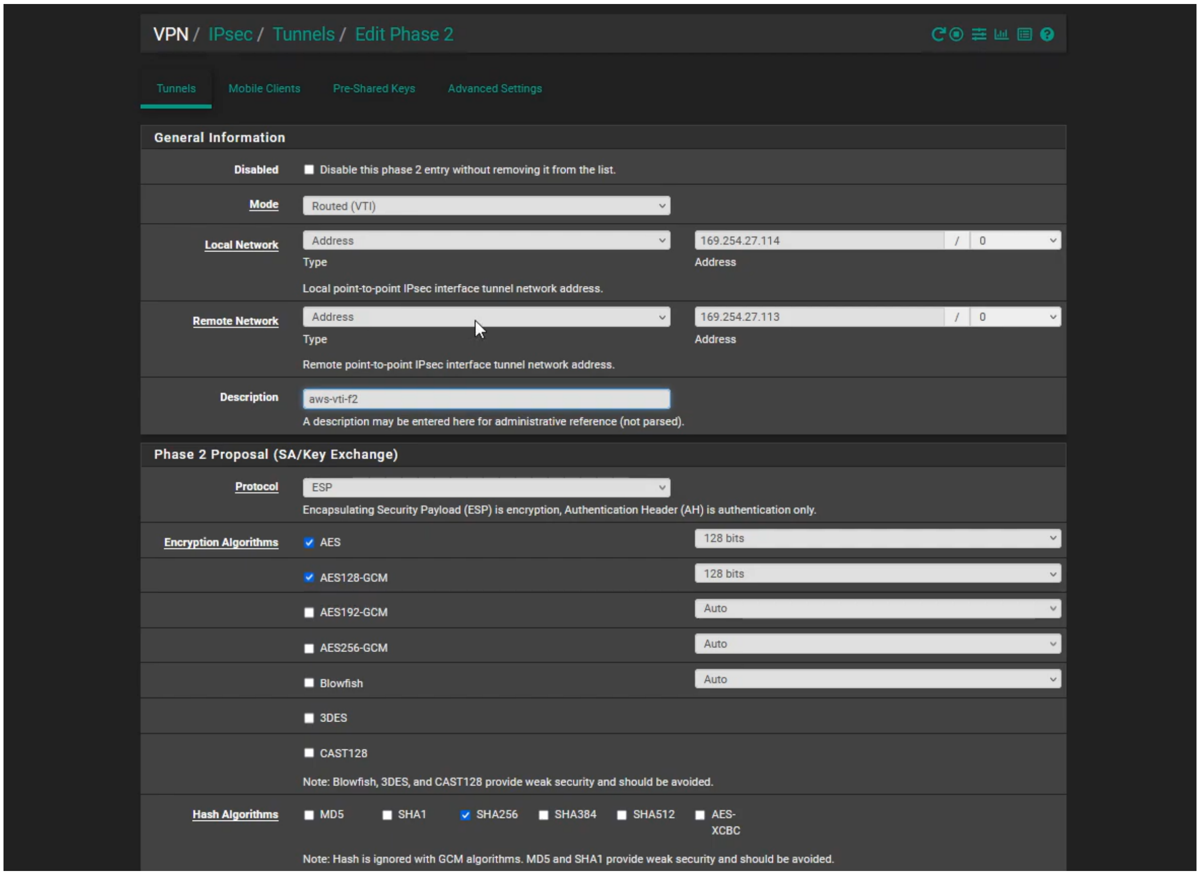
Dead Peer Detection ☑ Enable DPD

Delay 10

Delay between requesting peer acknowledgement.

Max failures 3

Number of consecutive failures allowed before disconnect.



VPN / IPsec / Tunnels / Edit Phase 2

General Information

Disabled □ Disable this phase 2 entry without removing it from the list.

Mode Routed (VTI)

Local Network Address | 169.254.27.114 / 0

Type | Address

Local point-to-point IPsec interface tunnel network address.

Remote Network Address | 169.254.27.113 / 0

Type | Address

Remote point-to-point IPsec interface tunnel network address.

Description aws-vti-f2

A description may be entered here for administrative reference (not parsed).

Phase 2 Proposal (SA/Key Exchange)

Protocol ESP

Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.

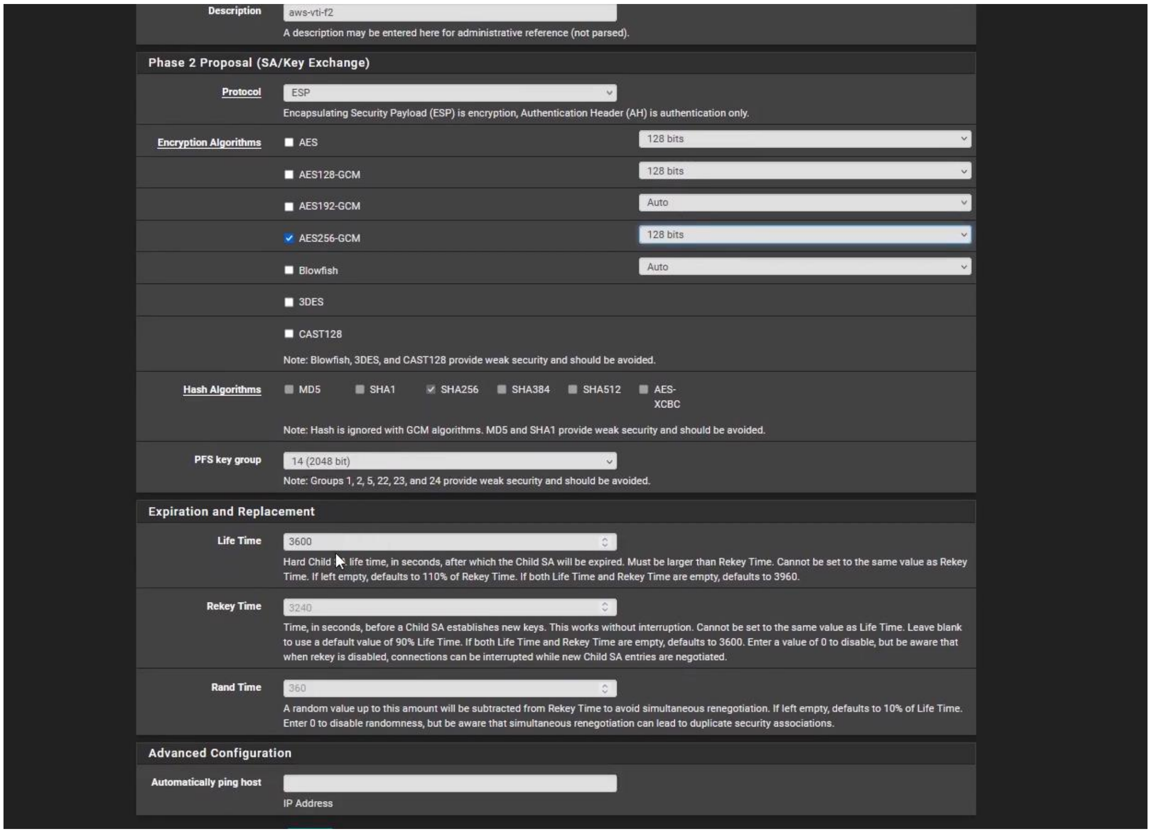
Encryption Algorithms

- ☑ AES — 128 bits
- ☑ AES128-GCM — 128 bits
- □ AES192-GCM — Auto
- □ AES256-GCM — Auto
- □ Blowfish — Auto
- □ 3DES
- □ CAST128

Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.

Hash Algorithms □ MD5 □ SHA1 ☑ SHA256 □ SHA384 □ SHA512 □ AES-XCBC

Note: Hash is ignored with GCM algorithms. MD5 and SHA1 provide weak security and should be avoided.



Description aws-vti-f2

A description may be entered here for administrative reference (not parsed).

Phase 2 Proposal (SA/Key Exchange)

Protocol ESP

Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.

Encryption Algorithms	□ AES	128 bits
	□ AES128-GCM	128 bits
	□ AES192-GCM	Auto
	☑ AES256-GCM	128 bits
	□ Blowfish	Auto
	□ 3DES	
	□ CAST128	

Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.

Hash Algorithms □ MD5 □ SHA1 ☑ SHA256 □ SHA384 □ SHA512 □ AES-XCBC

Note: Hash is ignored with GCM algorithms. MD5 and SHA1 provide weak security and should be avoided.

PFS key group 14 (2048 bit)

Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Expiration and Replacement

Life Time 3600

Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.

Rekey Time 3240

Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.

Rand Time 360

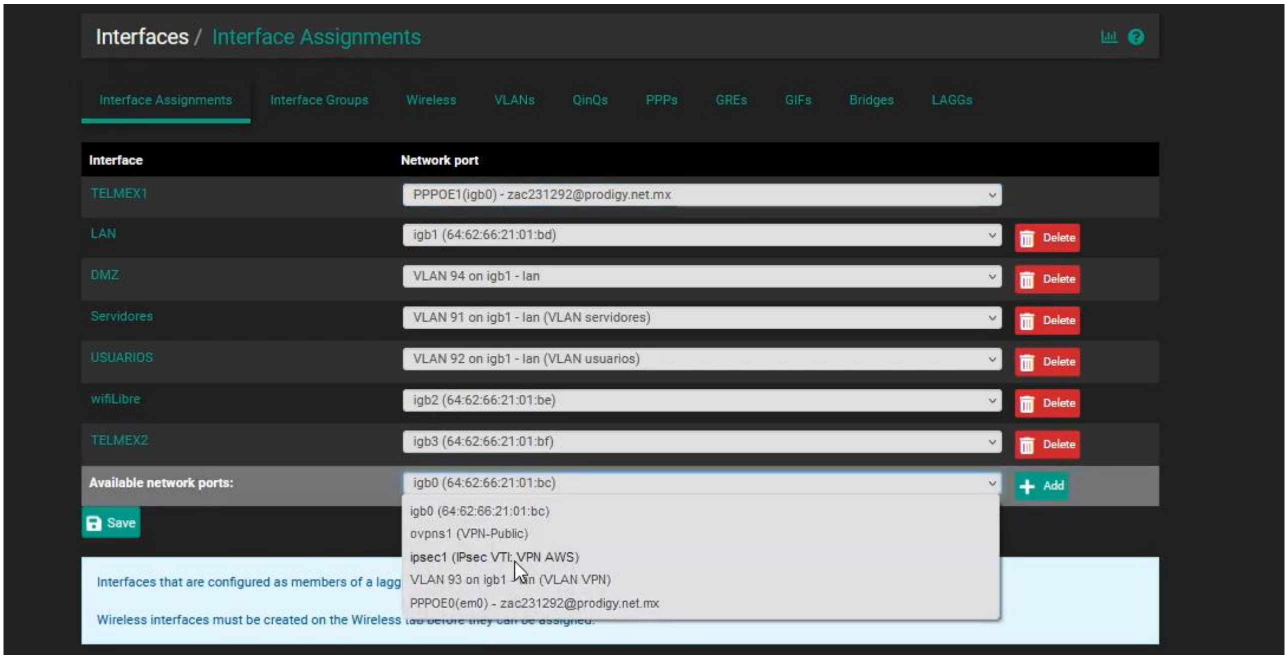
A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Advanced Configuration

Automatically ping host

IP Address

Luego con PFSENSE ya configurado ingresamos los datos obtenidos de la VPN de AWS:



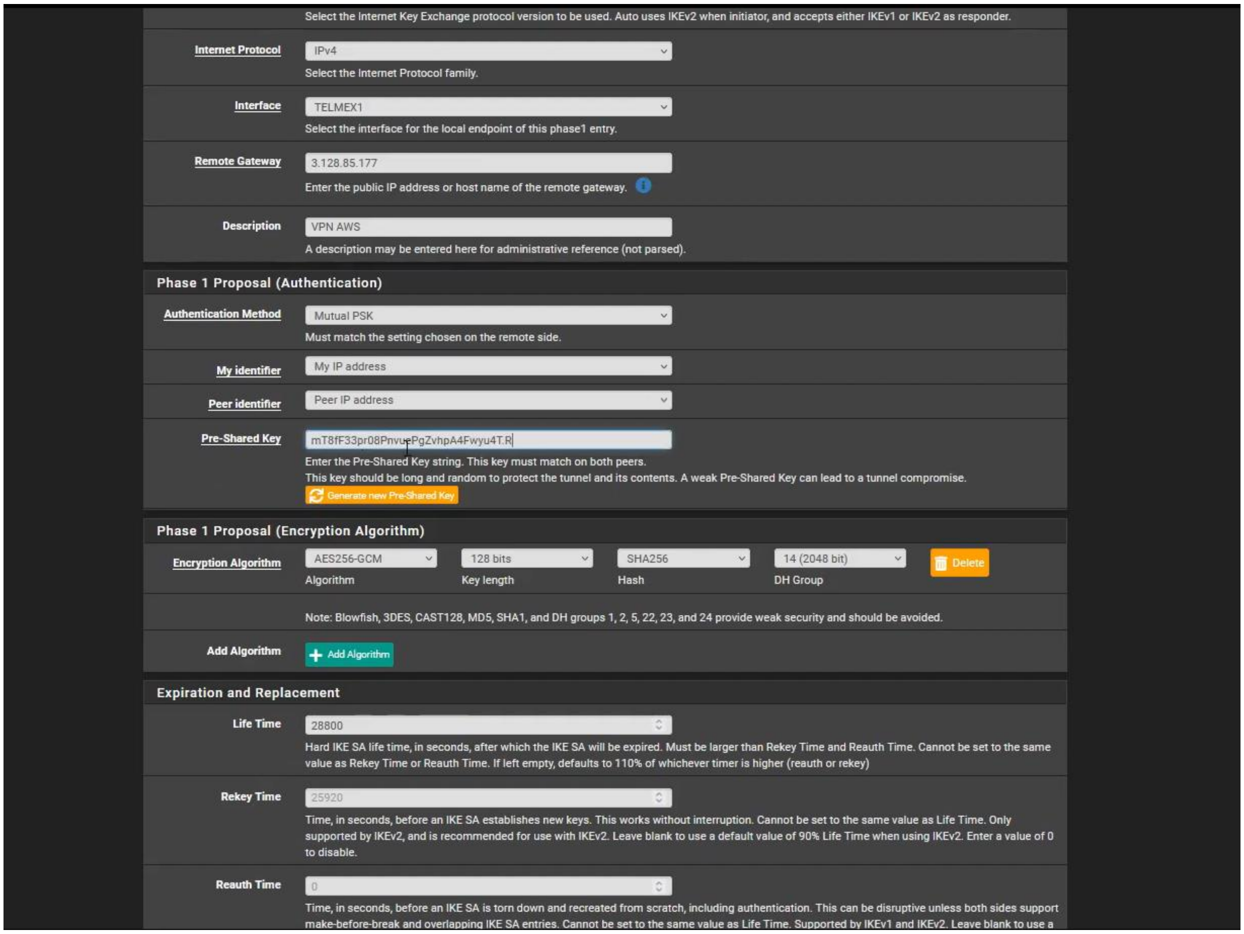
Interfaces / Interface Assignments

Interface	Network port
TELMEX1	PPPOE1(igb0) - zac231292@prodigy.net.mx
LAN	igb1 (64:62:66:21:01:bd)
DMZ	VLAN 94 on igb1 - lan
Servidores	VLAN 91 on igb1 - lan (VLAN servidores)
USUARIOS	VLAN 92 on igb1 - lan (VLAN usuarios)
wifiLibre	igb2 (64:62:66:21:01:be)
TELMEX2	igb3 (64:62:66:21:01:bf)
Available network ports:	igb0 (64:62:66:21:01:bc)

igb0 (64:62:66:21:01:bc)
ovpns1 (VPN-Public)
ipsec1 (IPsec VTI: VPN AWS)
VLAN 93 on igb1 - lan (VLAN VPN)
PPPOE0(em0) - zac231292@prodigy.net.mx

Interfaces that are configured as members of a lagg

Wireless interfaces must be created on the Wireless tab before they can be assigned.



Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol: IPv4
Select the Internet Protocol family.

Interface: TELMEX1
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway: 3.128.85.177
Enter the public IP address or host name of the remote gateway.

Description: VPN AWS
A description may be entered here for administrative 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: mT8fF33pr08PnvuePgZvhpA4Fwyu4T.R
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm

Algorithm	Key length	Hash	DH Group
AES256-GCM	128 bits	SHA256	14 (2048 bit)

Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

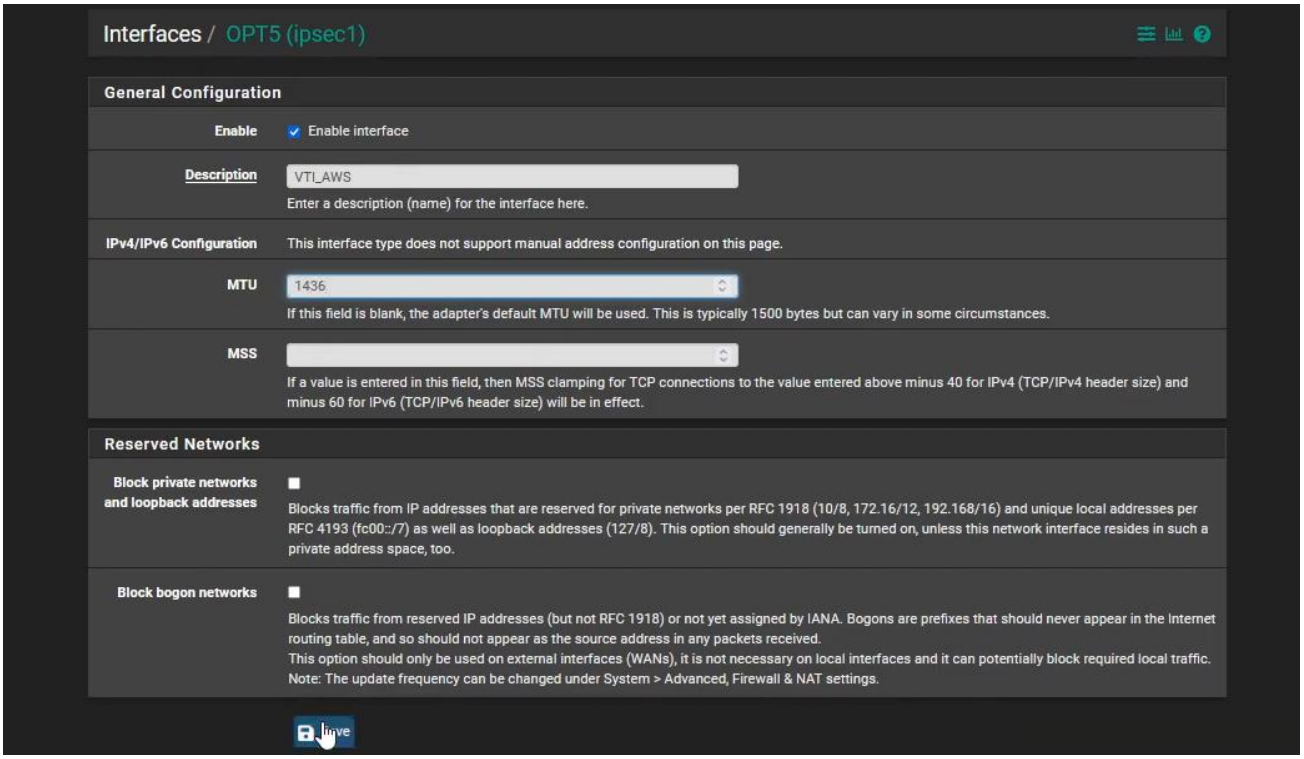
Add Algorithm

Expiration and Replacement

Life Time: 28800
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

Rekey Time: 25920
Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.

Reauth Time: 0
Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a



Interfaces / OPT5 (ipsec1)

General Configuration

Enable ☑ Enable interface

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

IPv4/IPv6 Configuration This interface type does not support manual address configuration on this page.

MTU 1436
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 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

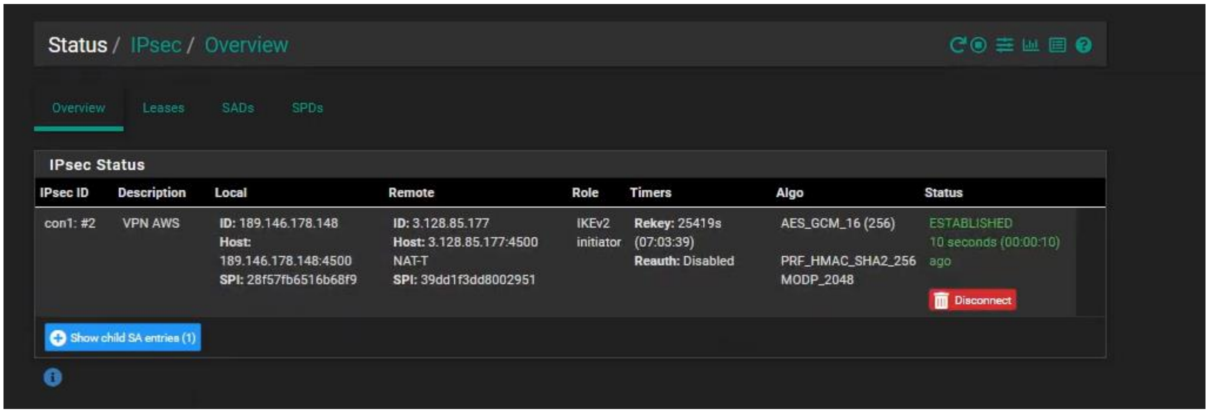
Reserved Networks

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.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Y prodedemos a guardar

Para validar que nuestro PFSENSE ya este capturando el trafico verificaremos su estatus.

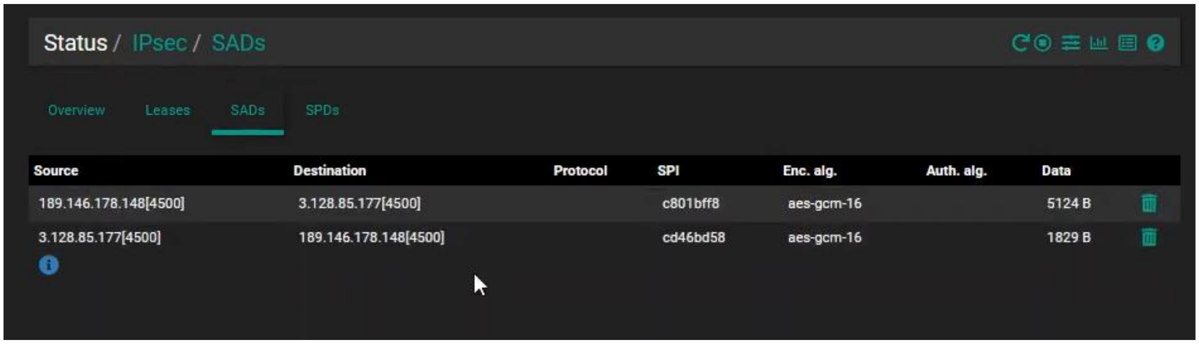


Status / IPsec / Overview

IPsec Status

IPsec ID	Description	Local	Remote	Role	Timers	Algo	Status
con1: #2	VPN AWS	**ID:** 189.146.178.148 **Host:** 189.146.178.148:4500 **SPI:** 28f57fb6516b68f9	**ID:** 3.128.85.177 **Host:** 3.128.85.177:4500 NAT-T **SPI:** 39dd1f3dd8002951	IKEv2 initiator	**Rekey:** 25419s (07:03:39) **Reauth:** Disabled	AES_GCM_16 (256) PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED 10 seconds (00:00:10) ago Disconnect

Como podemos ver en Data ya esta controlando el trafico de nuestra red virtual de AWS.



Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.	Data
189.146.178.148[4500]	3.128.85.177[4500]		c801bff8	aes-gcm-16		5124 B
3.128.85.177[4500]	189.146.178.148[4500]		cd46bd58	aes-gcm-16		1829 B