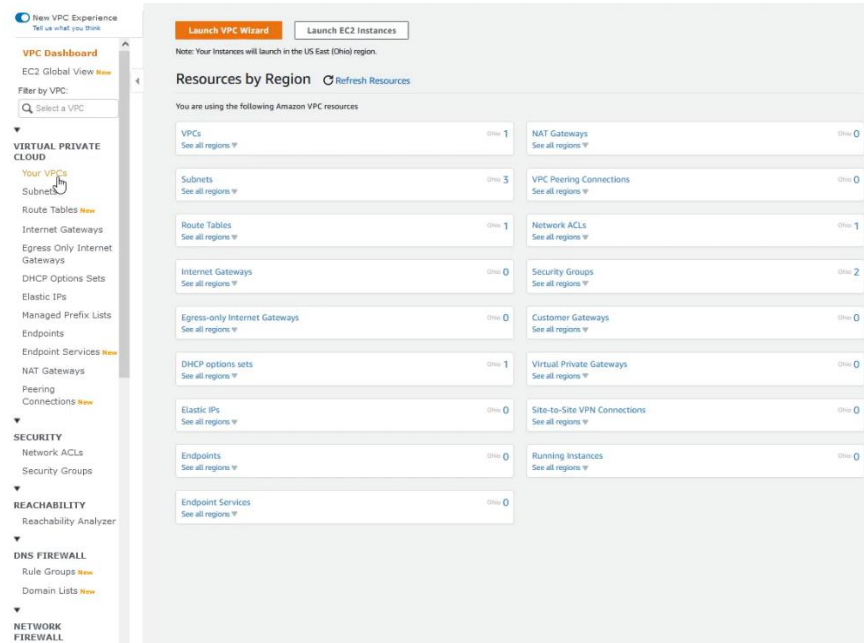


Universidad Mariano Gálvez de Guatemala
ingeniería en sistemas
Seguridad y Auditoria de sistemas

Implementación de pfSense con red en AWS

Eliezer Osbaldo Méndez Valle | 7690-14-9683 | Sección A
Geoffrey Estiven Hernández Franco | 7690-14-3807
Sergio Alexander Tzalam Lopez | 7690-16-3621

Lo primero para crear nuestra implementación es necesario crear VPC

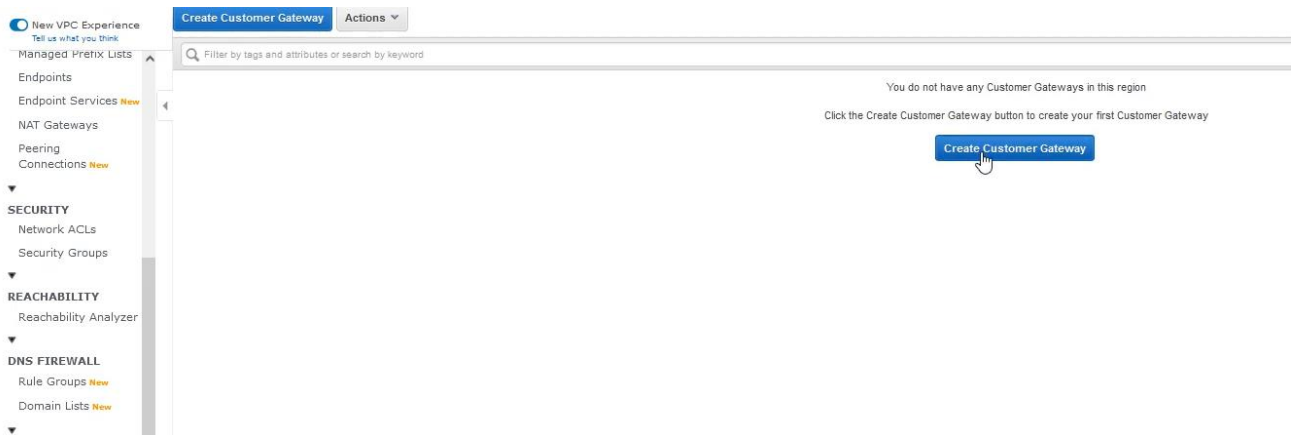


Procedemos a ingresar los datos, la cual creamos como pesense_vpc con los siguientes datos.

The screenshot shows the 'Create VPC' wizard in the AWS Management Console. The 'VPC settings' section includes a 'Name tag - optional' field with the value 'PFSENSE_VPC', an 'IPv4 CIDR block' field with the value '172.16.0.0/16', and an 'IPv6 CIDR block' section where 'No IPv6 CIDR block' is selected. The 'Tenancy' is set to 'Default'. The 'Tags' section shows a key-value pair with 'Name' as the key and 'PFSENSE_VPC' as the value. At the bottom right, there are 'Cancel' and 'Create VPC' buttons, with a mouse cursor clicking on the 'Create VPC' button.

Procedemos a dar clic en crear vpc

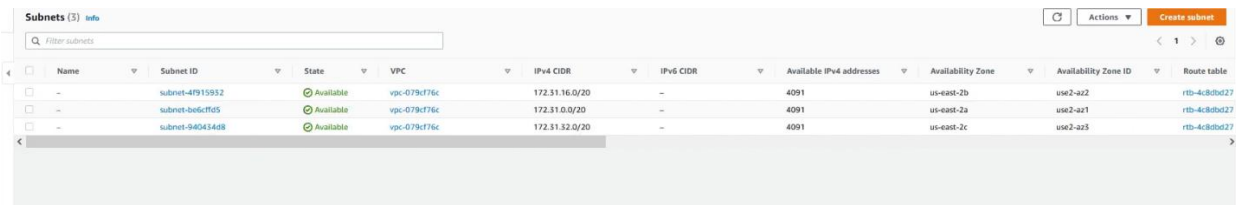
Lo siguiente es crear el Peering que va a apuntar a nuestro end-point.



Ingresamos el nombre, ingresamos el BGP ASN , que será el sistema autónomo del Peer, se debe de tomar en cuenta que la VPN debe de ser ruteable. Para la IP se ingresa nuestra IP pública.

A screenshot of the 'Create Customer Gateway' form in the AWS Management Console. The form includes the following fields: 'Name' (REMOTE-PEER-PFSENSE), 'Routing' (Dynamic selected, Static unselected), 'BGP ASN*' (51), 'IP Address' (189.146.178.148), 'Certificate ARN' (Select Certificate ARN dropdown), and 'Device' (Pfsense). There are information icons (i) next to the Name, BGP ASN, IP Address, and Device fields. At the bottom, there is a '* Required' label, a 'Cancel' button, and a 'Create Customer Gateway' button. A mouse cursor is pointing at the 'Create Customer Gateway' button.

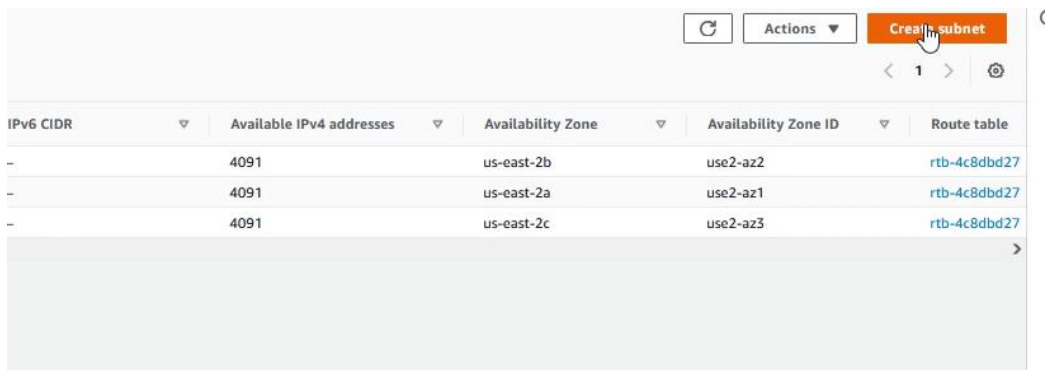
Luego procedemos a crear las Subnets, como se pueden visualizar ya hay registradas las que viene de forma predefinida en aw.



The screenshot shows the AWS Subnets console with a list of three subnets. The table has columns for Name, Subnet ID, State, VPC, IPv4 CIDR, IPv6 CIDR, Available IPv4 addresses, Availability Zone, Availability Zone ID, and Route table.

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID	Route table
-	subnet-47915932	Available	vpc-079cf76c	172.31.16.0/20	-	4091	us-east-2b	use2-az2	rtb-4c8dbd27
-	subnet-ba6cfff5	Available	vpc-079cf76c	172.31.0.0/20	-	4091	us-east-2a	use2-az1	rtb-4c8dbd27
-	subnet-9a041488	Available	vpc-079cf76c	172.31.32.0/20	-	4091	us-east-2c	use2-az3	rtb-4c8dbd27

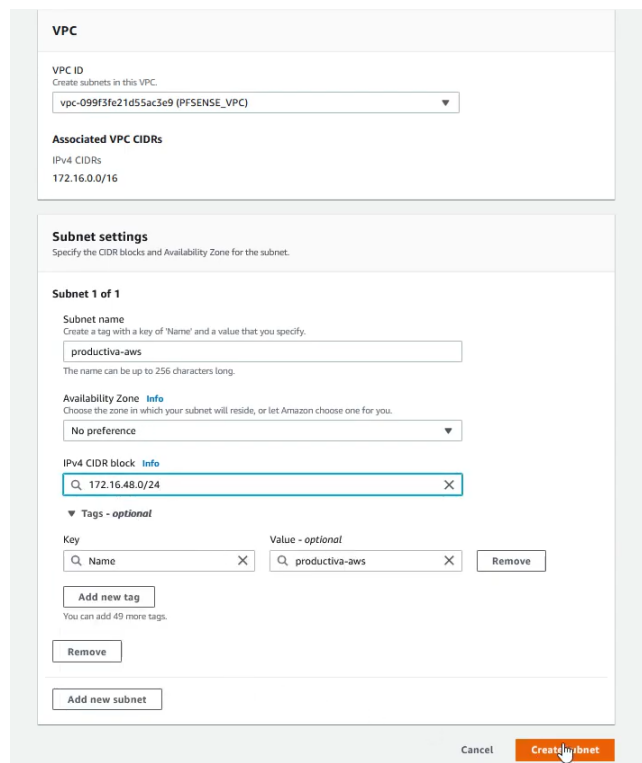
Procedemos a crear la nueva subnet.



The screenshot shows the AWS Subnets console with the 'Create subnet' button highlighted. Below the button is a table showing available subnets.

IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID	Route table
-	4091	us-east-2b	use2-az2	rtb-4c8dbd27
-	4091	us-east-2a	use2-az1	rtb-4c8dbd27
-	4091	us-east-2c	use2-az3	rtb-4c8dbd27

Ingresamos los datos, el nombre, le indicamos el rango de IP, y luego clic en Crear Subnet.



The screenshot shows the AWS 'Create subnet' form. It includes sections for VPC, Subnet settings, and Tags.

VPC

VPC ID
Create subnets in this VPC.
vpc-099f3fe21d55a3e9 (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 Remove

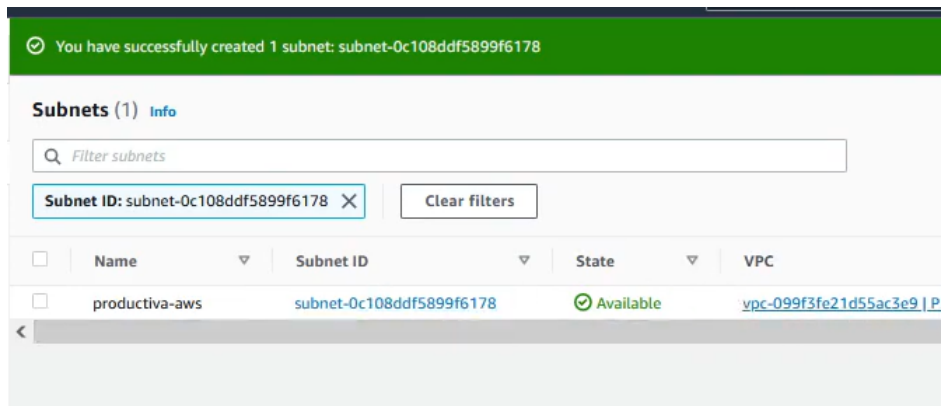
Add new tag
You can add 49 more tags.

Remove

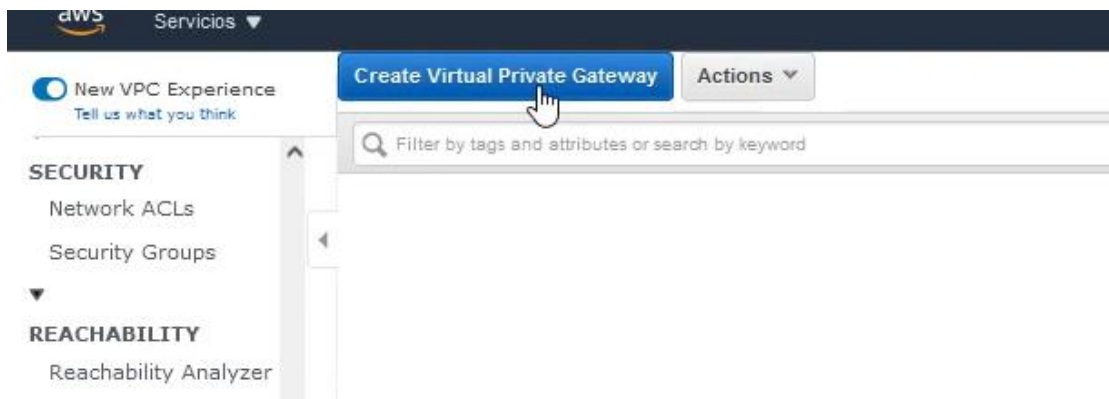
Add new subnet

Cancel Create subnet

Como podremos ver nuestra subnet ya fue creada correctamente



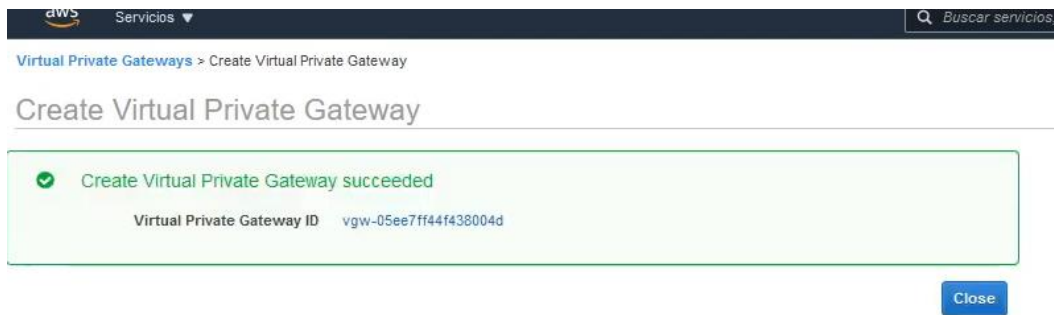
Luego lo que prosigue es crear la Gateway privado, este sirve para que nuestro trafico salga a nuestro Gateway privado para luego adjuntarlo a nuestro VPC



Le damos un nombre, y seleccionamos Amazon default ASN, que lo que va a hacer es darle el sistema autónomo de amazon



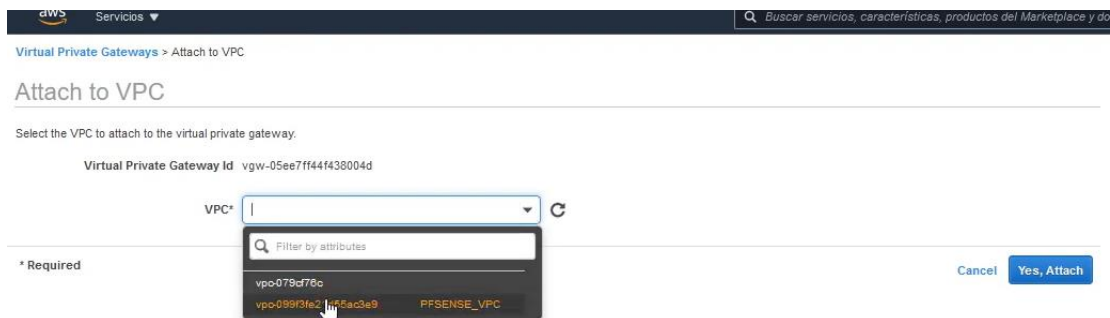
Procedemos a crearlo



Luego ya nos aparecerá en el listado, lo seleccionamos y lo asignaremos al VPC, clic en Actions luego en Attach to VPC



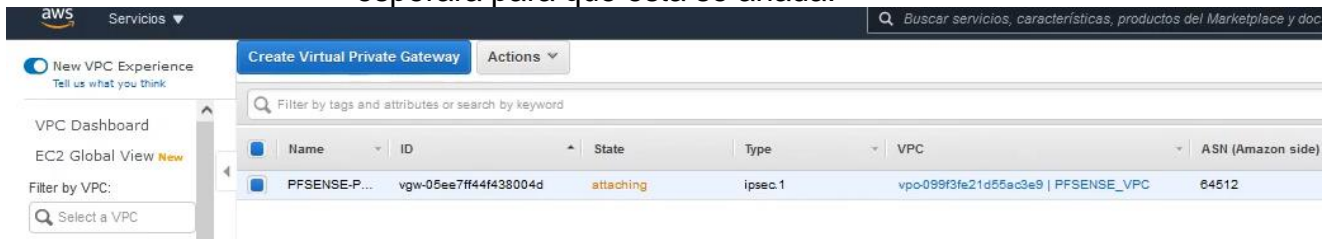
Luego seleccionamos la vpc que ya habiamos creado anteriormente



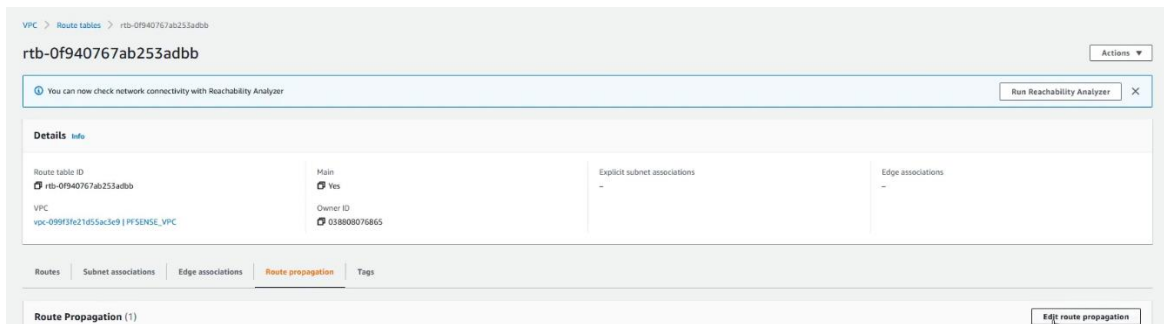
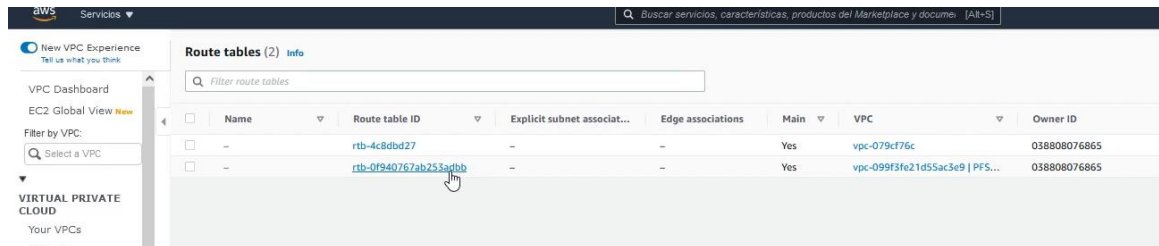
presionamos Yes, Attach.



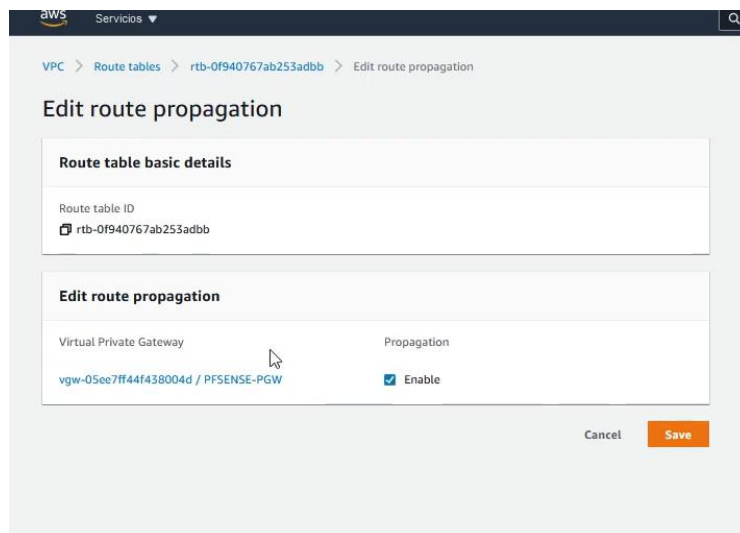
Como podremos ver ya nos aparece asignada a nuestra VPC ya solo es de esperara para que esta se añada.



Lo que prosigue es realizar la degeneración de BGP sobre las routing tables.



Procedemos a habilitar la propagación



Como podemos ver ahora en propagación ya nos aparece YES, y como podemos ver va a propagar la red que se encuentre asociada al privado Gateway.

Route propagation successfully updated for route table rtb-0f940767ab253adbb.

VPC > Route tables > rtb-0f940767ab253adbb

rtb-0f940767ab253adbb

🔔 You can now check network connectivity with Reachability Analyzer

Details [Info](#)

Route table ID 🔑 rtb-0f940767ab253adbb	Main 🔑 Yes	Explicit subnet associations -
VPC vpc-099f3fe21d55ac3e9 PFSENSE_VPC	Owner ID 🔑 038808076865	

[Routes](#) | [Subnet associations](#) | [Edge associations](#) | **[Route propagation](#)** | [Tags](#)

Route Propagation (1)

🔍 Find virtual private gateway

Virtual Private Gateway	▼	Propagation
vgw-05ec7ff44f438004d / PFSENSE-PGW		Yes

Luego procedemos a crear la VPN site to site.

aws Servicios

🔍 Buscar servicios, características, productos del Marketplace y documentos... [Alt+S]

New VPC Experience
Tell us what you think

Create VPN Connection Download Configuration Actions

Filter by tags and attributes or search by keyword

You do not have any VPN Connections in this region
Click the Create VPN Connection button to create your first VPN Connection

Create VPN Connection

DNS FIREWALL
Rule Groups [New](#)
Domain Lists [New](#)

NETWORK FIREWALL
Firewalls
Firewall policies
Network Firewall rule

Colocaremos los parametros minimos solicitados para crearla con la gateway y privatw gateway , los parametros que se dejaron en blanco es para que estas tomen los datos predefinidos por defecto.

aws

Servicios ▼

Buscar servicios, caract...

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

El inside IPv4 se dejará en blanco para que tome los datos predefinidos de AWS.
Tomara un segmento 30 del segmento 254.0.0/16 esto para que no pueda ser ruteado.

aws

Servicios

Buscar servicios, ca

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 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

Advanced Options for Tunnel 2

☒ Use Default Options

☐ Edit Tunnel 2 Options

VPN connection charges apply once this step is complete. [View Rates](#)

* Required

A /30 CIDR in the 169.254.0.0/16 range.

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) ⓘ

Phase 2 Lifetime (seconds) ⓘ

Rekey Margin Time (seconds) ⓘ

Rekey Fuzz (percentage) ⓘ

Replay Window Size (packets) ⓘ

DPD Timeout (seconds) ⓘ

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

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) ⓘ

Phase 2 Lifetime (seconds) ⓘ

Rekey Margin Time (seconds) ⓘ

Rekey Fuzz (percentage) ⓘ

Replay Window Size (packets) ⓘ

DPD Timeout (seconds) ⓘ

DPD Timeout Action ☒ Clear ☐ Restart ☐ None

Startup Action ☒ Add ⓘ ☐ Start

Procedemos a crearla y ya se nos mostrara en el listado de VPN connection.

aws Servicios

[New VPC Experience](#)
Tell us what you think

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

	Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Address	Inside Ip Version	Type	Category	VPN
	S29-PFSSEN...	vpn-0de9ead4203fa01f	pending	vgw-05ee7f944f38004d PFS...		cgw-05005088ased3aaf RE...	188.146.178.148	IPv4	ipsecl	VPN	vpn

DNS FIREWALL
Rule Groups [New](#)
Domain Lists [New](#)

NETWORK FIREWALL

Ahora en pfsense ingresaremos la configuraciones en relación a las realizadas a AWS.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

VPN / IPsec / Tunnels / Edit Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Disabled ☐ Set this option to disable this phase1 without removing it from the list.

Key Exchange version IKEv2
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
Enter the public IP address or host name of the remote gateway.

Description
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.
[Generate new Pre-Shared Key](#)

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm AES 128 bits SHA256 14 (2048 bit) [Delete](#)

Algorithm Key length Hash DH Group

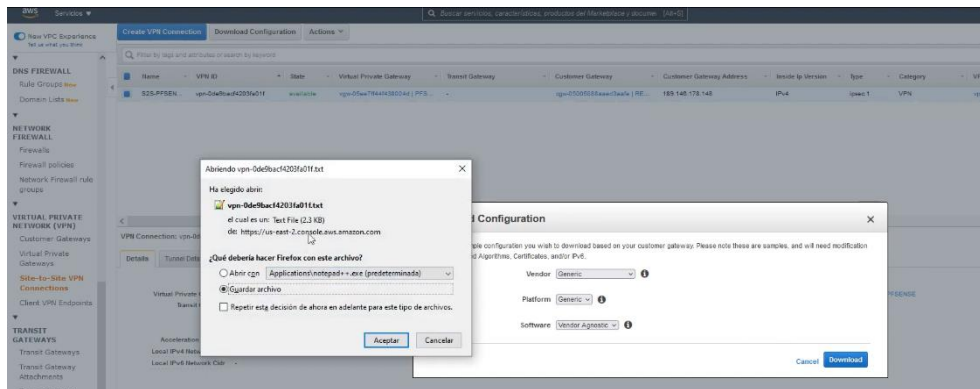
Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm [+ Add Algorithm](#)

Para realizar las configuraciones AWS nos facilita un archivo donde vienen todos las indicaciones para realizar la configuración en pfSense. Nos dirigimos a site-to-site VPN conection y damos clic en Download configuration.



Se procederá a descargar el archivo.



Como podremos ver dentro del archivo vienen todos los datos necesarios para configurar nuestro pfSense.

```
18 IPsec Tunnel #1
19 =====
20 #1: Internet Key Exchange Configuration
21
22 Configure the IKE SA as follows:
23 Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group 2.
24 Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.
25 You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.
26 NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.
27
28 Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
29 The address of the external interface for your customer gateway must be a static address.
30 Your customer gateway may reside behind a device performing network address translation (NAT).
31 To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall rules to unblock UDP port 4500.
32 | If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling NAT-T. If you are using an Accelerated VPN, make sure that NAT-T is enabled.
33 - IKE version : IKEv1
34 - Authentication Method : Pre-Shared Key
35 - Pre-Shared Key : mT8fF33pr08PmvuePg2vhpA4Fvyu4T.R
36 - Authentication Algorithm : sha1
37 - Encryption Algorithm : aes-128-cbc
38 - Lifetime : 28800 seconds
39 - Phase 1 Negotiation Mode : main
40 - Diffie-Hellman : Group 2
41
42 #2: IPsec Configuration
43
44 Configure the IPsec SA as follows:
45 Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.
46 Please note, you may use these additionally supported IPsec parameters for encryption like AES256 and other DH groups like 2, 5, 14-18, 22, 23, and 24.
47 NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.
48
49 Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
50 - Protocol : esp
51 - Authentication Algorithm : hmac-sha1-96
52 - Encryption Algorithm : aes-128-cbc
53 - Lifetime : 3600 seconds
54 - Mode : tunnel
55 - Perfect Forward Secrecy : Diffie-Hellman Group 2
56
57 IPsec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We
58 recommend configuring DPD on your endpoint as follows:
59 - DPD Interval : 10
60 - DPD Retries : 3
61
62 IPsec ESP (Encapsulating Security Payload) inserts additional
63 headers to transmit packets. These headers require additional space,
64 which reduces the amount of space available to transmit application data.
65 To limit the impact of this behavior, we recommend the following
66 configuration on your Customer Gateway:
67 - TCP MSS Adjustment : 1379 bytes
68 - Clear Don't Fragment Bit : enabled
69 - Fragmentation : Before encryption
70
71 #3: Tunnel Interface Configuration
72 =====
```

Podremos ver en el documento las dos interfaces con que se creo el tunnel

```

91 -----
92 Outside IP Addresses:
93   - Customer Gateway      : 189.146.178.148
94   - Virtual Private Gateway : 3.128.85.177
95
96 Inside IP Addresses
97   - Customer Gateway      : 169.254.27.114/30
98   - Virtual Private Gateway : 169.254.27.113/30
99
00 Configure your tunnel to fragment at the optimal size:
01   - Tunnel interface MTU   : 1436 bytes
02
03 #4: Border Gateway Protocol (BGP) Configuration:

```

Antes de ingresar los datos de AWS tenemos que configurar pfSense de la siguiente manera.

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.
[Generate new Pre-Shared Key](#)

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm AES256-GCM 128 bits SHA256 14 (2048 bit) [Delete](#)
Algorithm Key length Hash 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 [+ 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

mT8fF33pr08PnvuePgZvhpA4Fwyu4TR

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.

[Generate new Pre-Shared Key](#)

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm

AES256-GCM

Algorithm

128 bits

Key length

SHA256

Hash

14 (2048 bit)

DH Group

Delete

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

+ 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	<input type="text" value="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	<input type="text" value="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	<input type="text" value="Default"/>	Set this option to force specific initiation/responder behavior for child SA (P2) entries
Child SA Close Action	<input type="text" value="Default"/>	Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)
NAT Traversal	<input type="text" value="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	<input type="text" value="Disable"/>	Set this option to control the use of MOBIKE
Gateway duplicates	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> 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	<input type="text" value="Remote IKE Port"/>	<input type="text" value="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	<input checked="" type="checkbox"/> Enable DPD	
Delay	<input type="text" value="10"/>	Delay between requesting peer acknowledgement.
Max failures	<input type="text" value="3"/>	Number of consecutive failures allowed before disconnect.
<div></div>		

nsense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

VPN / IPsec / Tunnels / Edit Phase 2

Tunnels

Mobile Clients

Pre-Shared Keys

Advanced Settings

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 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 3600.

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

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 3600.

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



Procedemos a dar clic en guardar.




Y luego en aplicar cambios.

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

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect.

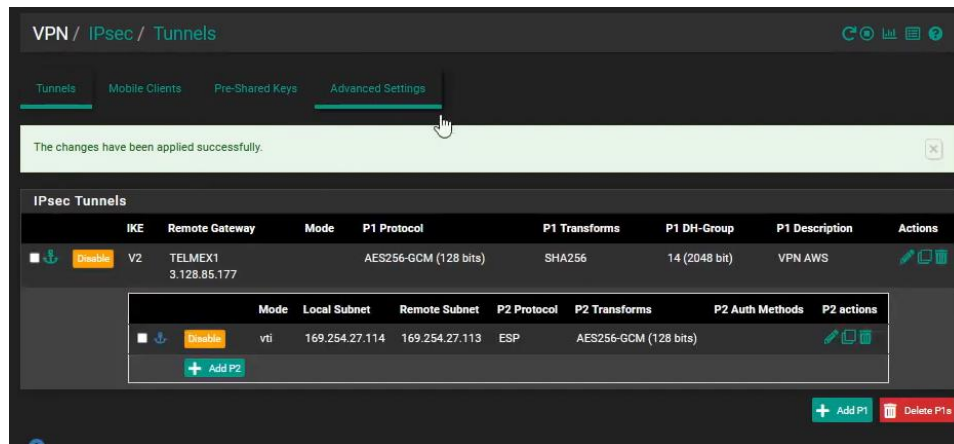


IPsec Tunnels

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
 Disable	V2	TELMEX1 3.128.85.177		AES256-GCM (128 bits)	SHA256	14 (2048 bit)	VPN AWS	  

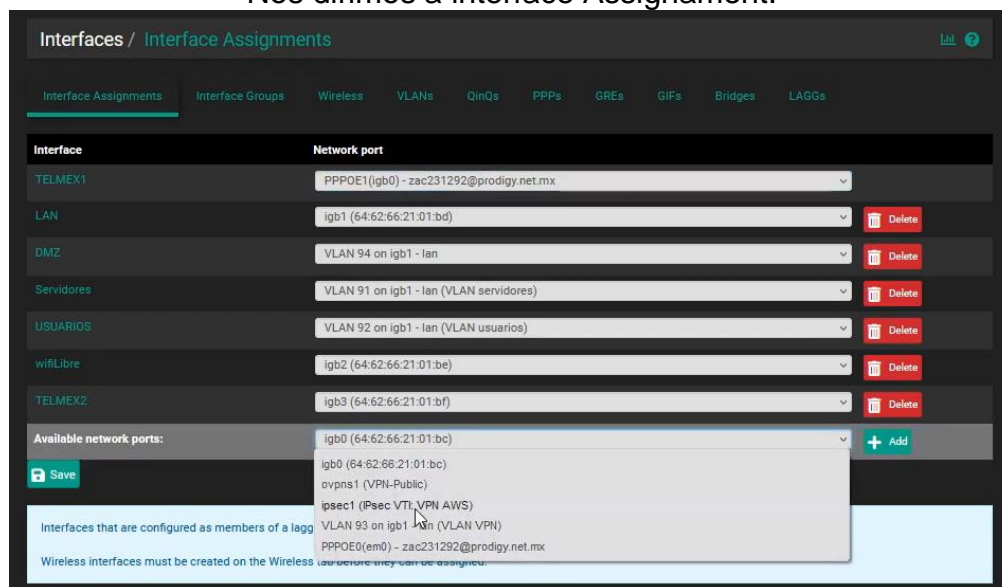
[+ Show Phase 2 Entries \(1\)](#)

[+ Add P1](#) [Delete P1](#)



Luego procedemos a complementar los datos con los del archivo descargarlo en aws.

Nos dirigimos a interface Assignment.



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

mT8tF33pr08PnvuPqZvhpA4Fwyu4T.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.

[Generate new Pre-Shared Key](#)

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm

AES256-GCM

128 bits

SHA256

14 (2048 bit)

Delete

AlgorithmKey lengthHashDH 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

+ 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 / Interface Assignments

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface	Network port
TELMEX1	PPPOE1(igb0) - zac231292@prodigy.net.mx
LAN	igb1 (64:62:66:21:01:bd) <div>Delete</div>
DMZ	VLAN 94 on igb1 - lan <div>Delete</div>
Servidores	VLAN 91 on igb1 - lan (VLAN servidores) <div>Delete</div>
USUARIOS	VLAN 92 on igb1 - lan (VLAN usuarios) <div>Delete</div>
wifiLibre	igb2 (64:62:66:21:01:be) <div>Delete</div>
OPT5	ipsec1 (IPsec VT: VPN AWS) <div>Delete</div>
TELMEX2	igb3 (64:62:66:21:01:bf) <div>Delete</div>
Available network ports:	igb0 (64:62:66:21:01:bc) <div>+ Add</div>

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

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

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.

Save

System / [Advanced](#) / [Firewall & NAT](#)

Admin Access
Firewall & NAT
Networking
Miscellaneous
System Tunables
Notifications

Firewall Advanced

IP Do-Not-Fragment compatibility
☒ Clear invalid DF bits instead of dropping the packets

This allows for communications with hosts that generate fragmented packets with the don't fragment (DF) bit set. Linux NFS is known to do this. This will cause the filter to not drop such packets but instead clear the don't fragment bit.

IP Random id generation
☐ Insert a stronger ID into IP header of packets passing through the filter.

Replaces the IP identification field of packets with random values to compensate for operating systems that use predictable values. This option only applies to packets that are not fragmented after the optional packet reassembly.

Firewall Optimization Options
Normal

The default optimization algorithm

Disable Firewall
☐ Disable all packet filtering.

Note: This converts pfSense into a routing only platform!
Note: This will also turn off NAT! To only disable NAT, and not firewall rules, visit the [Outbound NAT](#) page.

Disable Firewall Scrub
☐ Disables the PF scrubbing option which can sometimes interfere with NFS traffic.

Firewall Adaptive Timeouts
240000
480000

When the number of state entries exceeds this value, adaptive scaling begins. All timeout values are scaled linearly with factor (adaptive.end - number of states) / (adaptive.end - adaptive.start). Defaults to 60% of the Firewall Maximum States value

When reaching this number of state entries, all timeout values become zero, effectively purging all state entries immediately. This value is used to define the scale factor, it should not actually be reached (set a lower state limit, see below). Defaults to 120% of the Firewall Maximum States value

Timeouts for states can be scaled adaptively as the number of state table entries grows. Leave blank to use default values, set to 0 to disable Adaptive Timeouts.

Firewall Maximum States
400000

Maximum number of connections to hold in the firewall state table.
Note: Leave this blank for the default. On this system the default size is: 1615000

Firewall Maximum Table Entries
400000

Maximum number of table entries for systems such as aliases, sshguard, snort, etc, combined.
Note: Leave this blank for the default. On this system the default size is: 400000

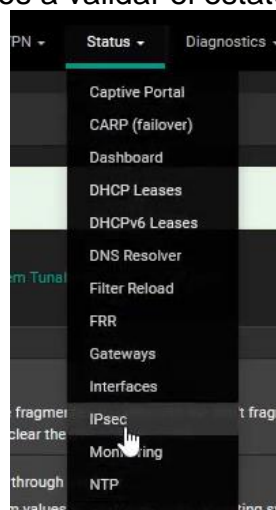
Firewall Maximum Fragment Entries
5000

Maximum number of packet fragments to hold for reassembly by scrub rules. Leave this blank for the default (5000)

Static route filtering
☐ Bypass firewall rules for traffic on the same interface

This option only applies if one or more static routes have been defined. If it is enabled, traffic that enters and leaves through the same interface will not be checked by the firewall. This may be desirable in some situations where multiple subnets are connected to the same interface.

Procedemos a validar el estatus de IPsec



Status / IPsec / Overview

Overview Leases SADs SPDs

IPsec Status

IPsec ID	Description	Local	Remote	Role	Timers	Algo	Status
	VPN AWS	ID: 189.146.178.148 Host: 189.146.178.148	ID: 3.128.85.177 Host: 3.128.85.177				Disconnected Connect VPN

1

Status / IPsec / Overview

Overview Leases SADs SPDs

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

[Show child SA entries \(1\)](#)

1

Damos clic en SADs y podremos ver que ya esta tanto recibiendo como enviando trafico de AWS.

Status / IPsec / SADs

Overview Leases SADs SPDs

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.	Data
189.146.178.148[4500]	3.128.85.177[4500]		c801bfff8	aes-gcm-16		5124 B Delete
3.128.85.177[4500]	189.146.178.148[4500]		cd46bd58	aes-gcm-16		1829 B Delete

1