

## Creación de VPC en Frankfurt y VPN con ella

Resumiendo los pasos son:

1. Creamos la VPC
2. Creamos las subnets
3. Creamos el internet Gateway
4. Creamos tabla de enrutamiento público
5. Creamos Nat Gateway
6. Modificamos tabla enrutamiento por defecto (privado)
7. Modificar redes públicas para auto asignar Ip publica.

### 1- Creamos la VPC

con el nombre: EDT VPC BRS y el CIDR Block simétrico al de producción. 10.100.16.0/21

#### Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an /

Name tag  ⓘ

IPv4 CIDR block\*  ⓘ

IPv6 CIDR block ☒ No IPv6 CIDR Block ⓘ ☐ Amazon provided IPv6 CIDR block

Tenancy  ⓘ

\* Required

La veremos disponible en Francfort:

Create VPC

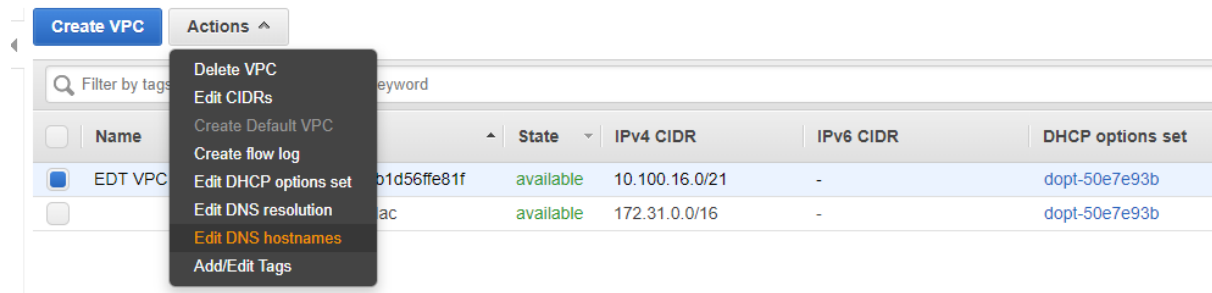
Actions

Filter by tags and attributes or search by keyword

1 to 2 of

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main Route table
<input checked="" type="checkbox"/>	EDT VPC BRS	vpc-04476fb1d56ffe81f	available	10.100.16.0/21	-	dopt-50e7e93b	rtb-0991e46e36562c58e   RT_...
<input type="checkbox"/>		vpc-c7232dac	available	172.31.0.0/16	-	dopt-50e7e93b	rtb-ac65e5c6

Habilitamos para esta VPC la opción DNS hostnames:



Marcamos el check:

[VPCs](#) > Edit DNS hostnames

## Edit DNS hostnames

VPC ID vpc-04476fb1d56ffe81f

DNS hostnames ☒ enable

\* Required

### 2- Creamos las subnets:

Simétricas a producción:

Create subnet

Actions

Filter by tags and attributes or search by keyword

1 to 7 of 7

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone
<input type="checkbox"/>	Public Subnet 1	subnet-03971a9441054af60	available	vpc-04476fb1d56ffe81f   E...	10.100.16.0/23	506	-	eu-central-1a
<input type="checkbox"/>	Private subnet 1	subnet-02144e0e07536b579	available	vpc-04476fb1d56ffe81f   E...	10.100.18.0/23	507	-	eu-central-1a
<input type="checkbox"/>	Public subnet 2	subnet-069f3f43f39e31b87	available	vpc-04476fb1d56ffe81f   E...	10.100.20.0/23	507	-	eu-central-1b
<input type="checkbox"/>	Private subnet 2	subnet-082c2ce6debe26be9	available	vpc-04476fb1d56ffe81f   E...	10.100.22.0/23	507	-	eu-central-1b
<input type="checkbox"/>		subnet-e96b58a4	available	vpc-c7232dac	172.31.0.0/20	4091	-	eu-central-1c
<input type="checkbox"/>		subnet-bf689ed5	available	vpc-c7232dac	172.31.16.0/20	4091	-	eu-central-1a
<input type="checkbox"/>		subnet-23476b5e	available	vpc-c7232dac	172.31.32.0/20	4091	-	eu-central-1b

### 3- Creamos el internet Gateway:

Para esto, primero se crea y luego se Atacha a la VPC que hemos creado:

Create internet gateway

Actions

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	ID	State	VPC	Owner
<input checked="" type="checkbox"/>	IG_EDT_VPC_BRS	igw-0970ea10ce3...	attached	vpc-04476fb1d56f..	713035683533
<input type="checkbox"/>		igw-ffc3ce97	attached	vpc-c7232dac	713035683533

#### 4- Creamos las tablas de enrutamiento para las redes públicas:

Creamos una nueva tabla de enrutamiento que asignaremos a las redes públicas:

Con nombre: RT\_Subnets\_publicas y en la VPC que hemos creado.

[Route Tables](#) > Create route table

### Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag  ⓘ

VPC\*  ↕ ⓘ

\* Required

Una vez creada la seleccionamos y en la pestaña Routes añadimos la linea de la salida por defecto usando el Internet Gateway que hemos creado.

Create route table		Actions			
Filter by tags and attributes or search by keyword					
<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Main	VPC ID
<input type="checkbox"/>	RT_Subnets_privadas	rtb-0991e46e36562c58e	-	Yes	vpc-04476fb1d56ffe81f   EDT VPC BRS
<input checked="" type="checkbox"/>	RT_Subnets_publicas	rtb-0ca2ee05efe94dbb1	2 subnets	No	vpc-04476fb1d56ffe81f   EDT VPC BRS
<input type="checkbox"/>		rtb-ac65e5c6	-	Yes	vpc-c7232dac

Route Table: rtb-0ca2ee05efe94dbb1

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.16.0/21	local	active	No
0.0.0.0/0	igw-0970ea10ce309cb16	active	No

Y ahora en las pestaña "Subnet Associations" le asociamos las dos subnets publicas que hemos creado:

Create route table

Actions

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Main	VPC ID
<input type="checkbox"/>	RT_Subnets_privadas	rtb-0991e46e36562c58e	-	Yes	vpc-04476fb1d56ffe81f   EDT VPC BRS
<input checked="" type="checkbox"/>	RT_Subnets_publicas	rtb-0ca2ee05efe94dbb1	2 subnets	No	vpc-04476fb1d56ffe81f   EDT VPC BRS
<input type="checkbox"/>		rtb-ac65e5c6	-	Yes	vpc-c7232dac

Route Table: rtb-0ca2ee05efe94dbb1

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit subnet associations

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-03971a9441054af60   Public Subnet 1	10.100.16.0/23	-
subnet-069f3f43f39e31b87   Public subnet 2	10.100.20.0/23	-

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-02144e0e07536b5...	10.100.18.0/23	-
subnet-082c2ce6debe26b...	10.100.22.0/23	-

## 5- Creamos el NAT Gateway:

Creamos el NAT Gateway en una de las subnets publicas y le asociamos una nueva ip fotante:

[NAT Gateways](#) > Create NAT Gateway

## Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more.](#)

Subnet\*   

Elastic IP Allocation ID\*  

Create New EIP

New EIP (35.158.253.97) creation successful.

\* Required



## 6- Modificamos la tabla de enrutamiento por defecto asociada ahora solo a las redes privadas:

Añadimos en esta tabla de enrutamiento la línea que envía la salida por defecto al Nat Gateway creado:

Create route table

Actions

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Main	VPC ID
<input checked="" type="checkbox"/>	RT_Subnets_privadas	rtb-0991e46e36562c58e	-	Yes	vpc-04476fb1d56ffe81f   EDT VPC BRS
<input type="checkbox"/>	RT_Subnets_publicas	rtb-0ca2ee05efe94dbb1	2 subnets	No	vpc-04476fb1d56ffe81f   EDT VPC BRS
<input type="checkbox"/>		rtb-ac65e5c6	-	Yes	vpc-c7232dac

Route Table: rtb-0991e46e36562c58e

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit routes

View

All routes

Destination	Target	Status
10.100.16.0/21	local	active
0.0.0.0/0	nat-0a05c3f781436e911	active

En la pestaña “subnet associations” vemos que la tienen asociada por defecto las privadas.

Create route table

Actions

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Main	VPC ID
<input checked="" type="checkbox"/>	RT_Subnets_privadas	rtb-0991e46e36562c58e	-	Yes	vpc-04476fb1d56ffe81f   EDT VPC BRS
<input type="checkbox"/>	RT_Subnets_publicas	rtb-0ca2ee05efe94dbb1	2 subnets	No	vpc-04476fb1d56ffe81f   EDT VPC BRS
<input type="checkbox"/>		rtb-ac65e5c6	-	Yes	vpc-c7232dac

Route Table: rtb-0991e46e36562c58e

Summary

Routes

Subnet Associations

Route Propagation

Tags

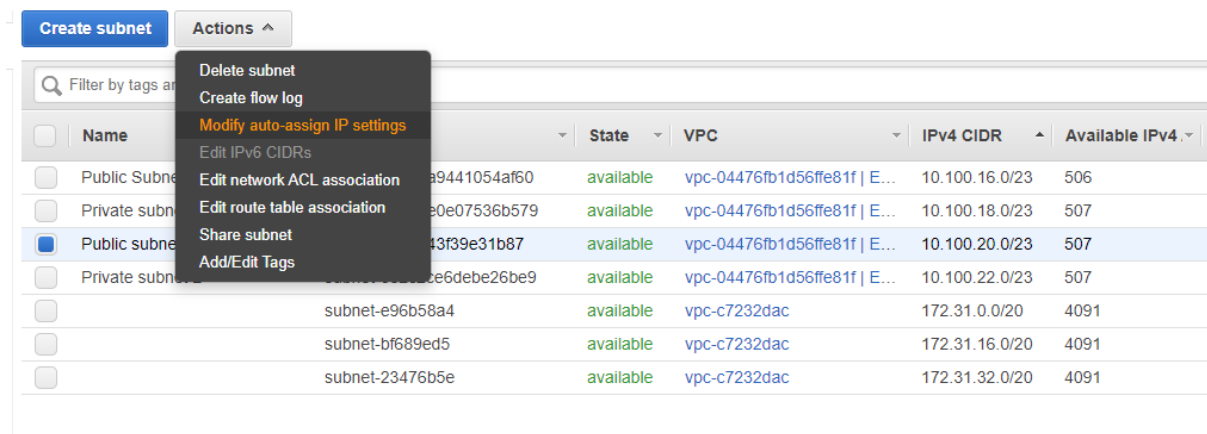
Edit subnet associations

Subnet ID	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations.		

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-02144e0e07536b5...	10.100.18.0/23	-
subnet-082c2ce6debe26b...	10.100.22.0/23	-

## Modificar redes públicas para auto asignar IPS públicas:



<input type="checkbox"/>	Name	ID	State	VPC	IPv4 CIDR	Available IPv4
<input type="checkbox"/>	Public Subnet	subnet-09441054af60	available	vpc-04476fb1d56ffe81f   E...	10.100.16.0/23	506
<input type="checkbox"/>	Private subnet	subnet-0e07536b579	available	vpc-04476fb1d56ffe81f   E...	10.100.18.0/23	507
<input checked="" type="checkbox"/>	Public subnet	subnet-069f3f43f39e31b87	available	vpc-04476fb1d56ffe81f   E...	10.100.20.0/23	507
<input type="checkbox"/>	Private subnet	subnet-0ce6debe26be9	available	vpc-04476fb1d56ffe81f   E...	10.100.22.0/23	507
<input type="checkbox"/>		subnet-e96b58a4	available	vpc-c7232dac	172.31.0.0/20	4091
<input type="checkbox"/>		subnet-bf689ed5	available	vpc-c7232dac	172.31.16.0/20	4091
<input type="checkbox"/>		subnet-23476b5e	available	vpc-c7232dac	172.31.32.0/20	4091


Marcamos el check de “Enable auto-assign public IPv4 address”

[Subnets](#) > Modify auto-assign IP settings

## Modify auto-assign IP settings

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for an instance I

**Subnet ID** subnet-069f3f43f39e31b87

**Auto-assign IPv4** ☒ Enable auto-assign public IPv4 address 

\* Required

Lo hacemos en las dos subnets públicas.

Desplegamos una máquina de pruebas en una subnet pública para ver si funciona bien.

## Creación de VPN con AWS

Los pasos son: Creamos primero:

1. El **Customer Gateway** (CG\_EDT). con la IP de nuestra salida a internet
2. Luego el **Virtual Private Gateway** (VPG\_EDT). Que es el Gateway donde dirigiremos el tráfico de red para llegar a las oficinas
3. Por ultimo la **VPN Connection** (VPN\_Connection\_EDT): Donde configuramos la utilización de los dos objetos creados anteriormente. Creamos nuestro customer Gateway:
4. **Atachamos** el VPG con nuestra VPN Connection.
5. En VPC, nos aseguramos que se propagan las tablas de enrutamiento.
6. Sacamos un script de configuración en el apartado VPN Connection para SonicWall.
7. Configuramos nuestro SonicWall

En nuestro SonicWall tenemos configuradas las salidas a internet de la siguiente manera:

TME Interfaz X1 IP 83.56.31.144

Colt interfaz X3 IP 217.111.173.210

Vamos a configurar las VPN con esta nueva IP de salida de Colt:

Nuestra nueva IP de salida es 217.111.173.210:

[Customer Gateways](#) > Create Customer Gateway

## Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either :

Name CG\_EDT



Routing ☐ Dynamic  
☒ Static

IP Address 217.111.173.210



Certificate ARN Select Certificate ARN



\* Required

Create Customer Gateway

Actions

Filter by tags and attributes or search by keyword

	Name	ID	State	Type	IP Address	BGP ASN	VPC
<input type="checkbox"/>	CG_EDT	cgw-07df73eb6820ec823	available	ipsec.1	217.111.173.210	65000	-
<input checked="" type="checkbox"/>		cgw-0e8d80653021c82e9	deleted	ipsec.1	217.111.173.210	65000	-

Creamos el Virtual Private Gateway

[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

VPG\_EDT

ASN

☒

Amazon default ASN

☐

Custom ASN

\* Required

Se crea detached:

Create Virtual Private Gateway

Actions

Filter by tags and attributes or search by keyword

	Name	ID	State	Type	VPC	ASN (Amazon side)
<input checked="" type="checkbox"/>	VPG_EDT	vgw-06c5cb1f4400c2212	detached	ipsec.1	-	64512



## Y por último nuestra VPN Connections

[VPN Connections](#) > Create VPN Connection

### Create VPN Connection

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

Name tag	<input type="text" value="VPN_Connection_EDT"/>													
Virtual Private Gateway	<input type="text" value="vgw-06c5cb1f4400c2212"/>													
<table><tr><td colspan="3">Filter by attributes</td></tr><tr><th>VPN Gateway ID</th><th>Name tag</th><th>VPC ID</th></tr><tr><td>vgw-06c5cb1f4400c2212</td><td>VPG_EDT</td><td>-</td></tr></table>			Filter by attributes			VPN Gateway ID	Name tag	VPC ID	vgw-06c5cb1f4400c2212	VPG_EDT	-			
Filter by attributes														
VPN Gateway ID	Name tag	VPC ID												
vgw-06c5cb1f4400c2212	VPG_EDT	-												
Customer Gateway	<input checked="" type="radio"/> Existing <input type="radio"/> New													
Customer Gateway ID	<input type="text" value="cgw-07df73eb6820ec823"/>													
<table><tr><td colspan="4">Filter by attributes</td></tr><tr><th>Customer Gateway ID</th><th>Name tag</th><th>IP Address</th><th>Certificate ARN</th></tr><tr><td>cgw-07df73eb6820ec823</td><td>CG_EDT</td><td>217.111.173.210</td><td></td></tr></table>			Filter by attributes				Customer Gateway ID	Name tag	IP Address	Certificate ARN	cgw-07df73eb6820ec823	CG_EDT	217.111.173.210	
Filter by attributes														
Customer Gateway ID	Name tag	IP Address	Certificate ARN											
cgw-07df73eb6820ec823	CG_EDT	217.111.173.210												
Routing Options	<input type="radio"/> Dynamic (requires BGP) <input checked="" type="radio"/> Static													
Static IP Prefixes	<table><tr><th>IP Prefixes</th><th>Source</th><th>State</th><td></td></tr><tr><td><input type="text" value="10.1.0.0/22"/></td><td>-</td><td>-</td><td></td></tr></table> <div>Add Another Rule</div>		IP Prefixes	Source	State		<input type="text" value="10.1.0.0/22"/>	-	-					
IP Prefixes	Source	State												
<input type="text" value="10.1.0.0/22"/>	-	-												

Seleccionamos como VPG el que hemos creado y como CG el creado antes.

Dejamos los demas parametros por defecto:

### Tunnel Options

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

Inside IP CIDR for Tunnel 1	<input type="text" value="Generated by Amazon"/>	
Pre-Shared Key for Tunnel 1	<input type="text" value="Generated by Amazon"/>	
Inside IP CIDR for Tunnel 2	<input type="text" value="Generated by Amazon"/>	
Pre-shared key for Tunnel 2	<input type="text" value="Generated by Amazon"/>	
Advanced Options for Tunnel 1	<input checked="" type="radio"/> Use Default Options <input type="radio"/> Edit Tunnel 1 Options	
Advanced Options for Tunnel 2	<input checked="" type="radio"/> Use Default Options <input type="radio"/> Edit Tunnel 2 Options	

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


Una vez creada nuestra VPC, attachamos nuestro VPG a ella:

[Virtual Private Gateways](#) > Attach to VPC

## Attach to VPC

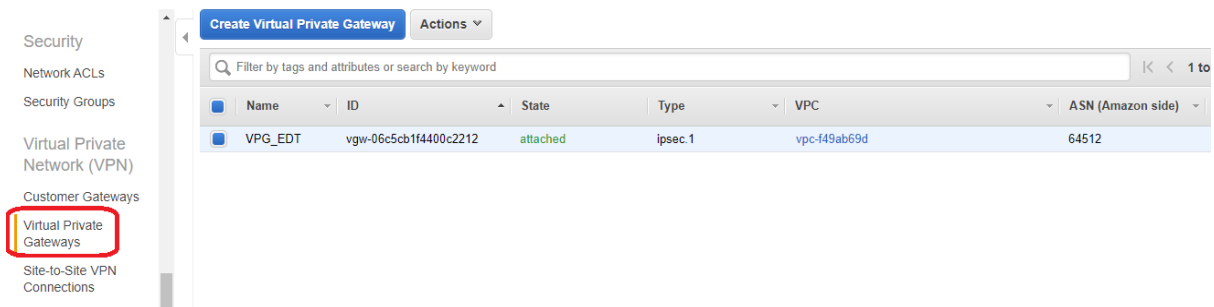
Select the VPC to attach to the virtual private gateway.

**Virtual Private Gateway Id** vgw-06c5cb1f4400c2212

**VPC\***  

\* Required

Comprobamos que esta attachada.



The screenshot shows the AWS Management Console interface for Virtual Private Gateways. On the left sidebar, the 'Virtual Private Gateways' option is highlighted with a red box. The main content area displays a table with the following data:

Name	ID	State	Type	VPC	ASN (Amazon side)
VPG_EDT	vgw-06c5cb1f4400c2212	attached	ipsec.1	vpc-f49ab69d	64512

Para finalizar en el epígrafe VPC nos aseguramos que se propagan las tablas de enrutamiento:

VPC Dashboard

Filter by VPC:

Q Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Create route table

Actions

Filter by tags and attributes or search by keyword

	Name	Route Table ID	Explicit subnet association	Main	VPC ID	Owner
		rtb-fc083495	-	Yes	vpc-f49ab69d	713035683533

Route Table: rtb-fc083495

SummaryRoutesSubnet AssociationsRoute PropagationTags

Edit route propagation

Virtual Private Gateway	Propagate
<a href="#">vgw-06c5cb1f4400c2212   VPG_EDT</a>	Yes

En sonicWall:

VPN Policy - Google Chrome

No es seguro | 10.1.1.4/vpnConfig\_6\_0.html#

SonicWALL | Network Security Appliance

General Network Proposals Advanced

### Security Policy

Policy Type: Site to Site

Authentication Method: IKE using Preshared Secret

Name: VPN-Paris

Ipssec Primary Gateway Name or Address: 15.188.0.31

Ipssec Secondary Gateway Name or Address: 15.188.19.53

### IKE Authentication

Shared Secret: .....

Confirm Shared Secret: .....

Local IKE ID: IPv4 Address 217.111.173.210

Peer IKE ID: IPv4 Address 15.188.0.31

☒ Mask Shared Secret


Ready

OK Cancel Help

En rojo las de AWS y en verde la nuestra.

VPN Policy - Google Chrome

No es seguro | 10.1.1.4/vpnConfig\_6\_0.html#

 SonicWALL | Network Security Appliance

General

Network

Proposals

Advanced

Local Networks

☐ Choose local network from list

--Select Local Network--

☐ Local network obtains IP addresses using DHCP through this VPN Tunnel

☒ Any address

Remote Networks

☐ Use this VPN Tunnel as default route for all Internet traffic

☐ Destination network obtains IP addresses using DHCP through this VPN Tunnel

☒ Choose destination network from list

AWSPARIS

Ready

OK

Cancel

Help

General Network Proposals **Advanced**

☒ Enable Keep Alive

☐ Suppress automatic Access Rules creation for VPN Policy

☐ Disable IPsec Anti-Replay

☐ Require authentication of VPN clients by XAUTH

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

WXA Group: None

☐ Apply NAT Policies

☐ Allow SonicPointN Layer 3 Management

Management via this SA: ☐ HTTPS ☐ SSH ☐ SNMP

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional): 0.0.0.0

VPN Policy bound to: Interface X3

☒ Preempt Secondary Gateway

Primary Gateway Detection Interval (seconds) 28800

Ready

OK Cancel Help

Ponemos la interface X3 que es la salida por Colt

En este punto ya la tenemos lista

## Cambiamos nuestra interfaz de salida para salir por la IP de TME

Creamos un **nuevo Customer Gateway** con la IP de TME lo llamamos CG\_EDT\_TME

[Customer Gateways](#) > Create Customer Gateway

### Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a

Name CG\_EDT\_TME

Routing ☐ Dynamic  
☒ Static

IP Address 83.56.31.144

Certificate ARN Select Certificate ARN

\* Required

EL **Virtual Private Gateway** no lo tocamos: No se deatacha de la VPC.

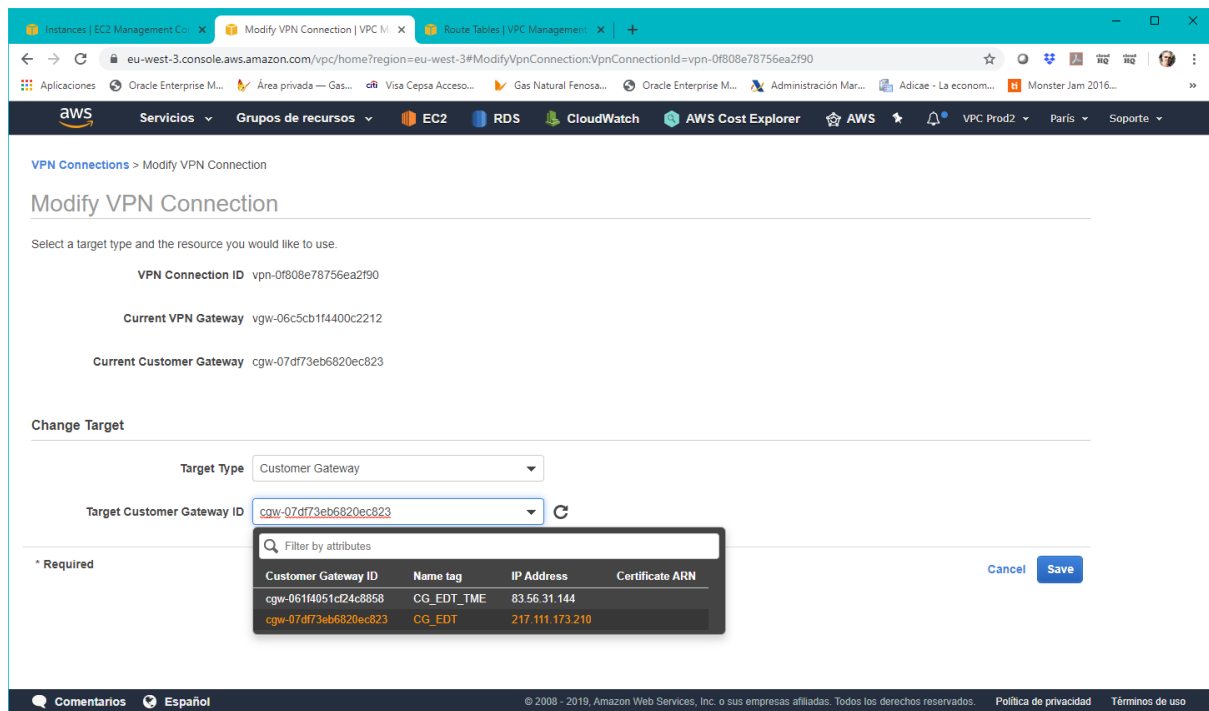
**Modificamos la VPN Connection**, para utilizar el nuevo Customer Gateway:

VPN Connection: vpn-0f808e78756ea2f90

Property	Value	Property	Value
VPN ID	vpn-0f808e78756ea2f90	State	available
Virtual Private Gateway	vgw-06c5cb1f4400c2212   VPG_EDT	Customer Gateway	cgw-07df73eb6820ec823   CG_EDT
Transit Gateway	-	Customer Gateway Address	217.111.173.210
Type	ipsec.1	Category	VPN
VPC	vpc-f49ab69d	Routing	Static
Authentication Type	Pre Shared Key		

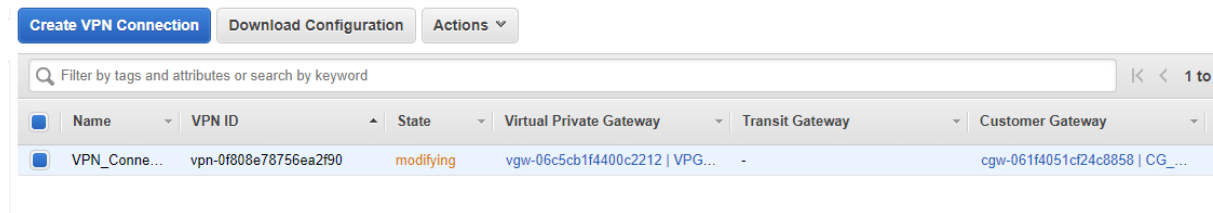
Seleccionamos “Modificar la VPN Connection”:

Y en la pantalla siguiente seleccionamos “Modificar el Customer Gateway”

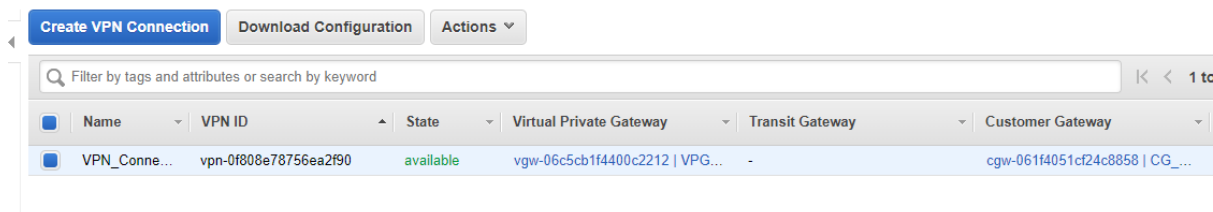


Ponemos el de TME y salvamos.

La VPN Connection se queda un rato en Modifying




Cuando esté disponible podemos seguir:



**En nuestro SonicWall:**  
Cambiamos nuestra IP:



No es seguro | 10.1.1.4/vpnConfig\_6\_0.html

 SonicWALL | Network Security Appliance

General

Network

Proposals

Advanced

Security Policy

Policy Type:

Site to Site

Authentication Method:

IKE using Preshared Secret

Name:

VPN-Paris

IPsec Primary Gateway Name or Address:

15.188.0.31

IPsec Secondary Gateway Name or Address:

15.188.19.53

IKE Authentication

Shared Secret:

.....

Confirm Shared Secret:

.....

Local IKE ID:

IPv4 Address

☒ Mask Shared Secret

83.56.31.144

Peer IKE ID:

IPv4 Address

15.188.0.31

Ready

OK


Cancel

Help

Seleccionamos la interface X1 que es la de la salida por TME

VPN Policy - Google Chrome

No es seguro | 10.1.1.4/vpnConfig\_6\_0.html#

 SonicWALL | Network Security Appliance

General Network Proposals **Advanced**

### Advanced Settings

☒ Enable Keep Alive

☐ Suppress automatic Access Rules creation for VPN Policy

☐ Disable IPsec Anti-Replay

☐ Require authentication of VPN clients by XAUTH

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

WXA Group: **None**

☐ Apply NAT Policies

☐ Allow SonicPointN Layer 3 Management

Management via this SA: ☐ HTTPS ☐ SSH ☐ SNMP

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional): 0.0.0.0

VPN Policy bound to: **Interface X1**

☒ Preempt Secondary Gateway

Primary Gateway Detection Interval (seconds) 28800

**Ready**

OK Cancel Help

y damos OK.