

VPN entre 2 PFSENSE con IPSEC

jueves, 26 de octubre de 2023 10:49

Configuración de VPN (IPSEC con clave compartida) mediante Firewalls Pfsense

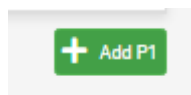
Vamos a configurar una VPN mediante IPSEC con clave compartida (protocolo para crear túneles cifrados en internet) site-to-site “Sitio a Sitio” utilizando pfsense, esta conexión nos permitirá enlazar 2 ubicaciones, en nuestro caso la oficina de Madrid con la de Barcelona y a la inversa para que los dispositivos de cada oficina se puedan ver entre las ubicaciones.

Configuración VPN Oficina Madrid

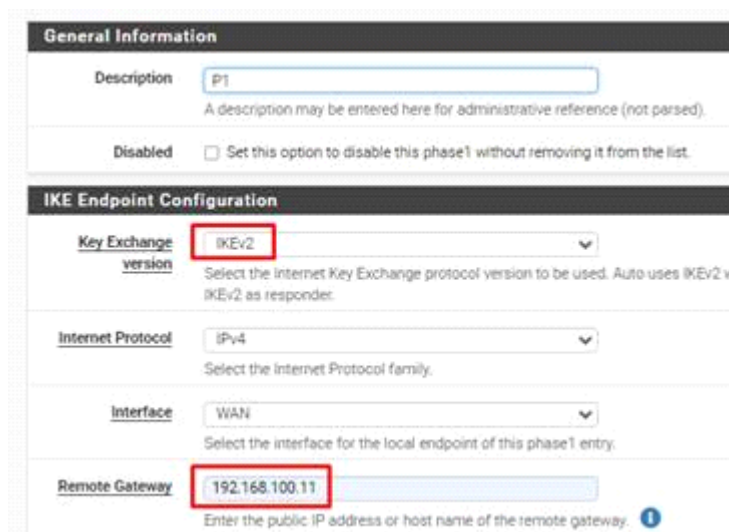
1. Accedemos al apartado VPN-Ipsec:



2. Dentro de Tunnels, pulsamos en Add p1 para configurar la primera parte del túnel Ipsec:



3. Indicamos que utilice la versión IKEv2 y que como Remote Gateway utilice la IP pública del pfsense de **Barcelona**:



4. Configuramos la autenticación con una clave compartida, que deberá tener el mismo nombre en la configuración de **Barcelona**. En el apartado de algoritmo a utilizar, dejamos el por defecto:

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: TestVPN
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)
Algorithm, Key length, Hash, DH Group

[Delete](#)

- Terminada la primera parte, configuramos la segunda entrando en Show Phase 2 Entries – Add p2:
- Configuramos esta parte 2, indicando que utilizará como Remote Network, la red local del pfsense de **Barcelona**:

General Information

Description: P2
A description may be entered here for administrative reference (not parsed).

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

Mode: Tunnel IPv4

Phase 1: P1 (IKE ID 1)

Networks

Local Network: LAN subnet
Type: Address: / 0
Local network component of this IPsec security association.

NAT/BINAT translation: None
Type: Address: / 0
If NAT/BINAT is required on this network specify the address to be translated

Remote Network: Network
Type: Address: 192.168.11.0 / 24
Remote network component of this IPsec security association.

- El algoritmo de encriptación que vamos a utilizar será solo el AES256-GCM de 2048bit:

Phase 2 Proposal (SA/Key Exchange)

Protocol ESP
 Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication only.

Encryption Algorithms

☐ AES 128 bits

☐ AES128-GCM 128 bits

☐ AES192-GCM Auto

☒ AES256-GCM Auto

☐ CHACHA20-POLY1305

Hash Algorithms ☐ SHA1 ☒ SHA256 ☒ SHA384 ☐ SHA512
 Note: Hash is ignored with GCM algorithms. SHA1 provides 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.

8. Por último, creamos una regla para permitir el tráfico entre Madrid y Barcelona, añadiendo como origen la red de Barcelona y como destino la de Madrid:

Floating WAN LAN **IPsec**

Rules (Drag to Change Order)

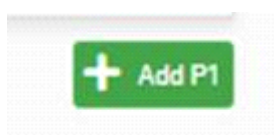
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 *	192.168.11.0/24	*	192.168.10.0/24	*	*

Configuración VPN Oficina Barcelona

1. Accedemos al apartado VPN-Ipsec:



2. Dentro de Tunnels, pulsamos en Add p1 para configurar la primera parte del túnel Ipsec:



- Indicamos que utilice la versión IKEv2 y que como Remote Gateway utilice la IP pública del pfsense de **Madrid**:

General Information

Description: P1
A description may be entered here for administrative reference (not parsed).

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

IKE Endpoint Configuration

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

Internet Protocol: IPv4
Select the Internet Protocol family.

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

Remote Gateway: 192.168.100.10
Enter the public IP address or host name of the remote gateway.

- Configuramos la autenticación con una clave compartida, que tendrá como nombre, el asignado con anterioridad a Madrid. En el apartado de algoritmo a utilizar, dejamos el por defecto:

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: TestVPN
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
Key length: 128 bits
Hash: SHA256
DH Group: 14 (2048)
[Delete](#)

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

- Terminada la primera parte, configuramos la segunda entrando en Show Phase 2 Entries – Add p2:
- Configuramos esta parte 2, indicando que utilizará como Remote Network, la red local del pfsense de **Madrid**:

General Information

Description: P2
A description may be entered here for administrative reference (not parsed).

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

Mode: Tunnel IPv4

Phase 1: P1 (IKE ID 1)

Networks

Local Network: LAN subnet / 0
Type: Address
Local network component of this IPsec security association.

NAT/BINAT translation: None / 0
Type: Address
If NAT/BINAT is required on this network specify the address to be translated

Remote Network: Network 192.168.10.0 / 24
Type: Address
Remote network component of this IPsec security association.

7. El algoritmo de encryptación que vamos a utilizar será solo el AES256-GCM de 2048bit:

Phase 2 Proposal (SA/Key Exchange)

Protocol: ESP
Encapsulating Security Payload (ESP) performs encryption and authentication, Authenti Header (AH) is authentication only.

Encryption Algorithms:

- ☐ AES 128 bits
- ☐ AES128-GCM 128 bits
- ☐ AES192-GCM Auto
- ☒ AES256-GCM Auto
- ☐ CHACHA20-POLY1305

Hash Algorithms:

- ☐ SHA1
- ☒ SHA256
- ☐ SHA384
- ☐ SHA512
- ☐ AES-

Note: Hash is ignored with GCM algorithms. SHA1 provides 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.

8. Por último, creamos una regla para permitir el tráfico entre Barcelona y Madrid, añadiendo como origen la red de Madrid y como destino la de Barcelona:

Floating WAN LAN **IPsec**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.10.0/24	*	192.168.11.0/24	*

Comprobaciones

-Realizamos un ping desde un cliente de la oficina de Madrid hacia un cliente de la oficina de Barcelona:

```
C:\Users\User01>ping 192.168.11.201

Haciendo ping a 192.168.11.201 con 32 bytes de datos:
Respuesta desde 192.168.11.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.11.201: bytes=32 tiempo=2ms TTL=126
Respuesta desde 192.168.11.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.11.201: bytes=32 tiempo=1ms TTL=126

Estadísticas de ping para 192.168.11.201:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 2ms, Media = 1ms
```

-Realizamos un ping desde un cliente de la oficina de Barcelona hacia un cliente de la oficina de Madrid:

```
C:\Users\Adrian>ping 192.168.10.201

Haciendo ping a 192.168.10.201 con 32 bytes de datos:
Respuesta desde 192.168.10.201: bytes=32 tiempo=2ms TTL=126
Respuesta desde 192.168.10.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.10.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.10.201: bytes=32 tiempo=1ms TTL=126

Estadísticas de ping para 192.168.10.201:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 2ms, Media = 1ms
```

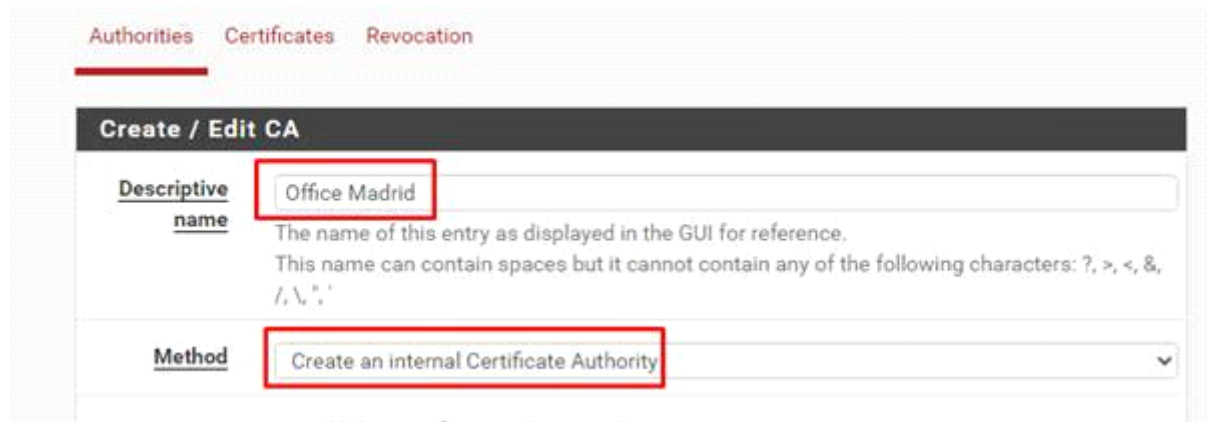
Configuración de VPN (IPSEC con Entidad Certificadora) mediante Firewalls Pfsense

El objetivo de esta práctica es implementar a la VPN entre la oficina de Madrid y Barcelona el uso de entidad certificadora mediante el protocolo IPSEC, este método es mucho más eficaz y seguro que el uso de una clave precompartida, aunque es más complejo de configurar. Dependiendo de la configuración elegida, podemos usar una CA (autoridad de certificación) compartida entre las oficinas que conforman la VPN o, utilizar una CA única

para cada oficina, nosotros utilizaremos la segunda opción.

Creación CA en Madrid y Barcelona:

1. El primer paso es, crear la autoridad certificada de **Madrid** dentro de **System** > **Certificates** > **Authorities** > **Add** (añadimos un nombre y los demás valores por defecto):



Authorities Certificates Revocation

Create / Edit CA



Descriptive name

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, *, '.

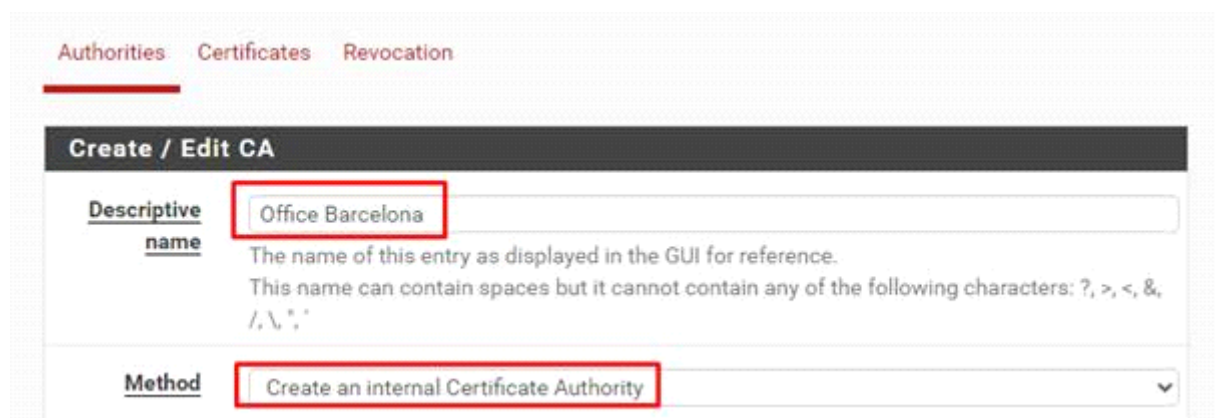
Method

2. Una vez creada la CA de Madrid, procedemos a exportar la clave pulsando en este icono, la cual utilizaremos más tarde:



Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Office Madrid	✓	self-signed	0	CN=internal-ca Valid From: Mon, 30 Oct 2023 18:44:40 +0100 Valid Until: Thu, 27 Oct 2033 19:44:40 +0200		   

3. A continuación, creamos la entidad certificada de **Barcelona** y exportamos la clave, siguiendo los pasos utilizados en Madrid:






Authorities Certificates Revocation

Create / Edit CA

Descriptive name

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, *, '.

Method

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Office Barcelona	✓	self- signed	0	CN=internal-ca  Valid From: Mon, 30 Oct 2023 18:50:00 +0100 Valid Until: Thu, 27 Oct 2033 19:50:00 +0200		    

Importación de CA en Madrid y Barcelona:

1. Importamos la CA de **Barcelona** en la oficina de **Madrid** dentro de **System > Certificates > Authorities > Add...** asignamos el nombre dado al CA de Barcelona y en este caso tenemos que indicarle que queremos importar un certificado ya existente:

Authorities Certificates Revocation

Create / Edit CA

Descriptive name Office Barcelona
 The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

Method Import an existing Certificate Authority

2. Dentro de Certificate data, pegamos el contenido del CA de Barcelona exportado anteriormente:











Existing Certificate Authority

Certificate data

```
-----BEGIN CERTIFICATE-----
MIIDHzCCAhugAwIBAgIIW1329/SPKRkwdQYJKoZIhvcNAQELBQAwFjEUMBIGA1UE
AwdMLawsBZXXJuYVwrtY2EwHhcNMjMxMDM0MTc1MDAwHhcNMjMxMDI3MTc1MDAw
MRQwEgYDVQQDEwtbnRlcm5hbC1jYTCASiWdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBBAOhEUBhL+wwtbQvjqRuo8dxdNsB4CeKnaocQa0CITGNCnrXUj8Vhd1Ev

```

Paste a certificate in X.509 PEM format here.

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Office Madrid	✓	Office Barcelona	0	CN=internal-ca  Valid From: Mon, 30 Oct 2023 18:44:40 +0100 Valid Until: Thu, 27 Oct 2033 19:44:40 +0200		    
Office Barcelona	✗	self- signed	1	CN=internal-ca  Valid From: Mon, 30 Oct 2023 18:50:00 +0100 Valid Until: Thu, 27 Oct 2033 19:50:00 +0200		  

3. Terminado el paso en Madrid, realizamos lo mismo, pero en **Barcelona**, importamos la CA de Madrid dentro de Barcelona:

Authorities Certificates Revocation

Create / Edit CA

Descriptive name Office Madrid







The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, *, '.

Method Import an existing Certificate Authority

Existing Certificate Authority

Certificate data

```
-----BEGIN CERTIFICATE-----
MIIDMzCCAhuGAwIBAgIIGbG/RUIf2I4wDQYJKoZIhvcNAQELBQAwFjEUM8IGA1UE
AxPLaw50ZXJ1YWhrtY2EwHhcNMjMxMDM0NDQwWWhcNMjMxMDI3MTc0NDQwWjAN
HRQwEgYDVQQDEwtbnRlcm5hcC1jYjYTCASiOQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAAOjqF19ZwJhDnygbVGH9HRIxLwn0rPa7b2+4+bYZZa2ANX34Hx13tne+
```

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Office Barcelona	✓	Office Madrid	0	CN=internal-ca Valid From: Mon, 30 Oct 2023 18:50:00 +0100 Valid Until: Thu, 27 Oct 2023 19:50:00 +0200		  
Office Madrid	✗	self-signed	1	CN=internal-ca Valid From: Mon, 30 Oct 2023 18:44:40 +0100 Valid Until: Thu, 27 Oct 2023 19:44:40 +0200		  

Creación de certificados de punto final en Madrid y Barcelona:

1. Creamos el certificado de punto final en Madrid dentro de **System > Certificates > Certificates > Add**:

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name Office Madrid Certificate

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, *, '.

2. Indicamos que use la CA creada anteriormente en Madrid:

Internal Certificate

Certificate authority Office Madrid

the certificate invalid.

Common Name office-madrid-certificate

3. Asignamos la IP pública de Madrid:

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type User Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

Type	Value
IP address	192.168.57.134 IP PÚBLICA DE MADRID

Office Madrid Certificate	Office Madrid	CN=office-madrid-certificate
User Certificate		Valid From: Mon, 30 Oct 2023 19:19:50 +0100
CA: No		Valid Until: Thu, 27 Oct 2033 20:19:50 +0200
Server: No		

4. Realizamos la misma operación con **Barcelona**:

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name Office Barcelona Certificate

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters

Internal Certificate

Certificate authority Office Barcelona

Common Name office-barcelona-certificate

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type User Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

Type	Value
IP address	192.168.57.135

Office Barcelona Certificate Office CN=office-barcelona-certificate ⓘ
User Certificate Barcelona
CA: No Valid From: Mon, 30 Oct 2023 19:23:22 +0100
Server: No Valid Until: Thu, 27 Oct 2033 20:23:22 +0200

Creación de túnel entre Madrid y Barcelona:

-Asignamos la dirección Pública de Barcelona y le indicamos que utilice el certificado de Madrid junto a la autoridad certificada de Barcelona.

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

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

IKE Endpoint Configuration

Key Exchange version ⓘ
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 ⓘ
Select the Internet Protocol family.

Interface ⓘ
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.

Phase 1 Proposal (Authentication)

Authentication Method ⓘ
Must match the setting chosen on the remote side.

My identifier ⓘ

Peer identifier ⓘ

My Certificate ⓘ
Select a certificate which identifies this firewall. The certificate must have at least one non-wildcard SAN.

Peer Certificate Authority ⓘ
Select a certificate authority to validate the peer certificate.

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm

Algorithm Key length Hash DH Group

-Entramos en la fase 2 de configuración del túnel:

192.168.57.135

+ Show Phase 2 Entries (0)

-Añadimos la red local de Barcelona utilizando el algoritmo AES256-GCM

The screenshot shows the configuration interface for IPsec. Under the 'Networks' section, the 'Remote Network' is configured with the address '192.168.11.0/24', which is highlighted with a red box and labeled 'red local de barcelona'. Below this, the 'Phase 2 Proposal (SA/Key Exchange)' section shows the 'Protocol' set to 'ESP'. Under 'Encryption Algorithms', 'AES256-GCM' is selected and highlighted with a red box, while 'AES', 'AES128-GCM', and 'AES192-GCM' are unselected.

-Configuramos una regla para permitir las conexiones desde la oficina de Madrid, indicando que el origen es la red local de Madrid y el destino la LAN net:

Rules (Drag to Change Order)										
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.10.0/24 *	LAN net	*	*	none		permitir conexión desde madrid

Creación de túnel entre Barcelona y Madrid:

-Asignamos la dirección Pública de Madrid y le indicamos que utilice el certificado de Barcelona junto a la autoridad certificada de Madrid.

General Information	
Description	vpn-to-madrid <small>A description may be entered here for administrative reference (not parsed).</small>
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE Endpoint Configuration	
Key Exchange version	IKEv2 <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
Internet Protocol	IPv4 <small>Select the Internet Protocol family.</small>
Interface	WAN <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	192.168.57.134 ip publica de madrid <small>Enter the public IP address or host name of the remote gateway.</small>
Phase 1 Proposal (Authentication)	
Authentication Method	Mutual Certificate <small>Must match the setting chosen on the remote side.</small>
My identifier	My IP address
Peer identifier	Peer IP address
My Certificate	Office Barcelona Certificate <small>Select a certificate which identifies this firewall. The certificate must have at least one non-wildcard SAN.</small>
Peer Certificate Authority	Office Madrid <small>Select a certificate authority to validate the peer certificate.</small>
Phase 1 Proposal (Encryption Algorithm)	
Encryption Algorithm	AES256-GCM 128 bits SHA256 14 (2048 bit) Delete <small>Algorithm Key length Hash DH Group</small>

-Entramos en la fase 2 de configuración del túnel:

192.168.57.135
+ Show Phase 2 Entries (0)

-Añadimos la red local de Madrid utilizando el algoritmo AES256-GCM

Networks

Local Network LAN subnet / 0
 Type Address
 Local network component of this IPsec security association.

NAT/BINAT translation None / 0
 Type Address
 If NAT/BINAT is required on this network specify the address to be translated

Remote Network Network 192.168.10.0 red local de madrid / 24
 Type Address
 Remote network component of this IPsec security association.

Phase 2 Proposal (SA/Key Exchange)

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

Encryption Algorithms

☐ AES 128 bits

☐ AES128-GCM 128 bits

☐ AES192-GCM Auto

☒ AES256-GCM Auto

-Configuramos una regla para permitir las conexiones desde la oficina de Barcelona, indicando que el origen es la red local de Barcelona y el destino la LAN net:

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.11.0/24 *	LAN net	*	*	none		permitir conexiones desde barcelona

Las direcciones IP públicas no corresponden con las adecuadas, debido a que he tenido que realizar el documento en casa, por la falta de asistencia a clase del día 30/10.

Comprobaciones:

-Realizamos un ping entre un cliente de Madrid y uno de Barcelona:


```

C:\Users\Adrian>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::225e:eb4:61e1:9877%5
    IPv4 Address. . . . . : 192.168.10.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

C:\Users\Adrian>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:
Reply from 192.168.11.2: bytes=32 time=1ms TTL=126
Reply from 192.168.11.2: bytes=32 time=4ms TTL=126
Reply from 192.168.11.2: bytes=32 time=4ms TTL=126
Reply from 192.168.11.2: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

```

-Realizamos un ping entre un cliente de Barcelona y uno de Madrid:

```

C:\Users\Adrian>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3732:ee6a:1700:2fa2%5
    IPv4 Address. . . . . : 192.168.11.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.11.1

C:\Users\Adrian>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=3ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=3ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms

```