

# VPN entre 2 PFSENSE con OpenVPN

martes, 31 de octubre de 2023 10:57

El objetivo de esta práctica es configurar una VPN en nuestros servidores pfsense, utilizando el protocolo **OpenVPN** utilizando entidades certificadoras.

1. El primer paso será crear una entidad certificadora en el servidor de Madrid:

The screenshot shows the 'Create / Edit CA' form in the pfSense web interface. The 'Descriptive name' field is set to 'Cert-Madrid'. The 'Method' is 'Create an internal Certificate Authority'. The 'Trust Store' checkbox is unchecked. The 'Randomize Serial' checkbox is also unchecked. Below the form, the 'Common Name' is set to 'Cert-Madrid'.

Below the form, the 'Certificate Authorities' table is displayed:

Name	Internal	Issuer	Certificates	Distinguished Name
Cert-Madrid	✓	self-signed	0	CN=Cert-Madrid Valid From: Tue, 31 Oct 2023 08:58:03 +0100 Valid Until: Fri, 28 Oct 2033 09:58:03 +0200

2. Descargamos el certificado y su clave, ya que luego será necesario para exportarlas al servidor de Barcelona:

The screenshot shows the 'Certificate Authorities' table. The 'Actions' column for the 'Cert-Madrid' entry has a red box around the download icon (a key with a downward arrow).

3. A continuación, creamos un certificado de tipo servidor en el servidor de Madrid:

The screenshot shows the 'Add/Sign a New Certificate' form in the pfSense web interface. The 'Method' is 'Create an internal Certificate'. The 'Descriptive name' field is set to 'Certificate-Madrid'. The 'Common Name' is set to 'Certificate-Madrid'.

**Certificate Type** Server Certificate

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

**Alternative Names**

Type	Value	Action
FQDN or Hostname	pfsense.cr.loc	Delete
IP address	192.168.100.10	Delete

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the ce  
sinninn CA may innore or channe these values

4. Creamos otro certificado en Madrid, pero ahora de tipo usuario para el servidor de Barcelona:

System / Certificates / Certificates / Edit

Authorities **Certificates** Certificate Revocation

**Add/Sign a New Certificate**

**Method** Create an internal Certificate

**Descriptive name** Certificate-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: ?, >, <.

**Common Name** Certificate-Barcelona

**Certificate Attributes**

**Attribute Notes** The following attributes are added to certificates and requests when they are created or signed selected mode.  
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

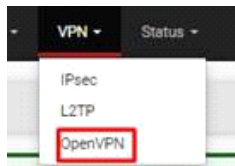
**Alternative Names**

Type	Value	Action
FQDN or Hostname	pfsense.cr.loc	Delete
IP address	192.168.100.11	Delete

5. Descargamos el certificado y la clave del certificado de tipo usuario creado para Barcelona:

Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (65380e4cdd0a) Server Certificate CA: No Server: Yes	self-signed	O=pfsense webConfigurator Self-Signed Certificate, CN=pfsense-65380e4cdd0a Valid From: Wed, 25 Oct 2023 10:50:44 +0200 Valid Until: Tue, 26 Nov 2024 09:50:44 +0100	webConfigurator	
Certificate-Madrid Server Certificate CA: No Server: Yes	Cert-Madrid	CN=Certificate-Madrid Valid From: Tue, 31 Oct 2023 09:04:04 +0100 Valid Until: Fri, 28 Oct 2023 10:04:04 +0200		
<b>Certificate-Barcelona User Certificate</b> CA: No Server: No	Cert-Madrid	CN=Certificate-Barcelona Valid From: Tue, 31 Oct 2023 09:08:23 +0100 Valid Until: Fri, 28 Oct 2023 10:08:23 +0200		

6. Una vez configurado los certificados, configuramos el protocolo OpenVPN:
  - Accedemos al protocolo:

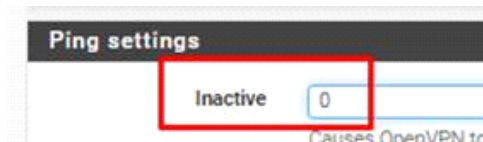


- Dentro de servers pulsamos en ADD...asignamos una descripción para saber que es la configuración de la VPN de Madrid:

- Indicamos que use el certificado de Madrid creado en el servidor de Madrid:

- Asignamos un rango de IP para la configuración del túnel.
- En el apartado IPv4 Local Network utilizamos la Red Local de Madrid.
- Utilizamos la Red Local de Barcelona para la configuración de IPv4 Remote network.

- Tenemos que indicar, que no queremos que se cierre la conexión VPN, esto se hace añadiendo un 0 en el apartado **Inactive**:



- Guardamos la configuración y vemos que se ha creado correctamente:

OpenVPN Servers				
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description
WAN	UDP4 / 1194 (TUN)	10.0.1.0/24	Mode: Peer to Peer (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN-Madrid

- Editamos la configuración para copiar su clave TLS y la guardamos en un **archivo.txt**, que será exportada al servidor de Barcelona:



- A continuación, tenemos que crear un override de clientes para asociar una subred a un certificado, así podremos enrutar, **asignamos el mismo common Name que al certificado creado de Barcelona**:

Servers Clients **Client Specific Overrides** Wizards

**General Information**

Description **Barcelona-VPN**  
A description of this override for administrative reference.

Disable ☐ Disable this override  
Set this option to disable this client-specific override without removing it from the list.

**Override Configuration MISMO NOMBRE QUE EL CERT DE BARCELONA**

Common Name **Certificate-Barcelona**  
Enter the X.509 common name for the client certificate, or the username for VPNs until  
Enter 'DEFAULT' to override default client behavior.

**Tunnel Settings**

IPv4 Tunnel Network **10.0.1.0/24 MISMA SUBRED**  
The virtual IPv4 network or network type alias with a single entry used for private communications between CIDR (e.g. 10.0.8.5/24).  
With subnet topology, enter the client IP address and the subnet mask must match the IPv4 Tunnel Network.  
With net30 topology, the first network address of the /30 is assumed to be the server address and the second client.

IPv6 Tunnel Network  
The virtual IPv6 network or network type alias with a single entry used for private communications between prefix (e.g. 2001:db9:1:1::100/64).  
Enter the client IPv6 address and prefix. The prefix must match the IPv6 Tunnel Network prefix on the server.

IPv4 Local Network/s  
These are the IPv4 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of CIDR ranges or host/network type aliases.  
NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

IPv6 Local Network/s  
These are the IPv6 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of IP/PREFIX networks.  
NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

IPv4 Remote Network/s **192.168.11.0/24 RED LOCAL BARCELONA**  
These are the IPv4 client-side networks that will be routed to this client specifically using route, so that a client can reach a specific network. May be left blank if there are no clients.

9. Configuramos reglas, para poder permitir la comunicación entre Madrid y Barcelona:

- Primera regla:

Firewall / Rules / Edit

**Edit Firewall Rule**

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** WAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** UDP  
Choose which IP protocol this rule should match.

**Source**  
**Source** ☐ Invert match any  
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases its default value, any.

**Destination**  
**Destination** ☐ Invert match This firewall (self)  
**Destination Port Range** OpenVPN (1194) OpenVPN (1194)  
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**  
**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using the Status: System Logs: Settings page).

**Description** Acceder a VPN  
A description may be entered here for administrative reference. A maximum of 1024 characters will be used in the rules.

- Segunda regla:

**Edit Firewall Rule**

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** LAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** Any  
Choose which IP protocol this rule should match.

**Source**  
**Source** ☐ Invert match LAN net  
Source Address: /

**Destination**  
**Destination** ☐ Invert match Network  
192.168.11.0 / 24  
RED LOCAL BARCELONA

- Tercera regla:

**Edit Firewall Rule**

**Action** Pass  
 Choose what to do with packets that match the criteria specified below.  
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
 Set this option to disable this rule without removing it from the list.

**Interface** OpenVPN  
 Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
 Select the Internet Protocol version this rule applies to.

**Protocol** Any  
 Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match Network 192.168.11.0  
RED LOCAL BARCELONA

**Destination**

**Destination** ☐ Invert match LAN net Destination Address

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description** Trafico-BarcelonaToMadrid  
 A description may be entered here for administrative reference. A maximum of 32 characters will be used in the ruleset and displayed in the firewall.

10. Ya hemos terminado la configuración de Madrid, ahora vamos a importar los certificados en el servidor de Barcelona:

- Dentro de **Authorities** asignamos el mismo nombre que al **CA** de Madrid e importamos el **.cert** y el **.key** de Madrid:





System / Certificates / Certificates / Edit

Authorities

Certificates

Certificate Revocation

Add/Sign a New Certificate

Method

Import an existing Certificate

Descriptive name

Certificate-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: ?, >, <, &, /, \, " , ' ,

Import Certificate

Certificate Type

☒ X.509 (PEM)
 ☐ PKCS #12 (PFX)

Certificate data

```

L190Jv1+0f1HQk81tCseV
YnrTuJQvycZtkX8+OgD1vm78VILLhsxck/1KX6hDPk8
0ByywEk4dXwZ14vPmy2u
/BKyHg==
-----END CERTIFICATE-----

```

Paste a certificate in X.509 PEM format here.

Private key data

```

oDQFKwQcvtqHbn4Y7pP0P
Gs+USV2xnN18pG8BP1IATHoOcci1ps5C2owD4cF1dKu
+Swz44y1J6HSDQ02XHZjW
eH833/LJ3Fuz0KwyFaiNBingSq==
-----END PRIVATE KEY-----

```

Paste a private key in X.509 PEM format here. This field may remain empty in certain cases, such as

Certificate-Barcelona	Cert-Madrid	CN=Certificate-Barcelona
CA: No		Valid From: Tue, 31 Oct 2023 09:08:23 +0100
Server: No		Valid Until: Fri, 28 Oct 2033 10:08:23 +0200

11. Por último, configuramos el cliente VPN en Barcelona:



VPN / OpenVPN / Clients / Edit

Servers Clients Client Specific Overrides Wizards

### General Information

**Description** Barcelona-VPN Mismo nombre que al cliente de Madrid  
 A description of this VPN for administrative reference.

**Disabled** ☐ Disable this client  
 Set this option to disable this client without removing it from the list.

### Mode Configuration

**Server mode** Peer to Peer ( SSL/TLS )

**Device mode** tun - Layer 3 Tunnel Mode  
 "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compat  
 "tap" mode is capable of carrying 802.3 (OSI Layer 2.)

### Endpoint Configuration

**Protocol** UDP on IPv4 only

**Interface** WAN  
 The interface used by the firewall to originate this OpenVPN client connection

**Local port**  
 Set this option to bind to a specific port. Leave this blank or enter 0 for a random dy

**Server host or address** 192.168.100.10 IP PUBLICA MADRID  
 The IP address or hostname of the OpenVPN server.

**Server port** 1194

-Pegamos el contenido del fichero TLS, creado anteriormente en Madrid:

### Cryptographic Settings

**TLS Configuration** ☒ Use a TLS Key  
 A TLS key enhances security of an OpenVPN connection by req  
 perform a TLS handshake. This layer of HMAC authentication al  
 dropped, protecting the peers from attack or unauthorized conn  
 data.

☐ Automatically generate a TLS Key.

**TLS Key**

```
1a40b4f09a38e95adc65d794eb033cf3
168114a2f979fcde4153c80e61c1dd35
01adb5b7682edc5b4574ada263012325
b3fab0f1d52666463ad3f9be83dac0a9
-----END OpenVPN Static key V1-----
```

the client must be set to 1. Both may be set to omit the direction, in v

**Peer Certificate Authority** Cert-Madrid

**Peer Certificate Revocation list** No Certificate Revocation Lists defined. One may be created here: Sy

**Client Certificate** Certificate-Barcelona (CA: Cert-Madrid)

**Tunnel Settings**

**IPv4 Tunnel Network**  **misma subred**

This is the IPv4 virtual network or network type alias with a single entry used and the server expressed using CIDR notation (e.g. 10.0.8.0/24).

This should be left blank in most cases as servers typically provide addresses.

The second usable address in this network will be assigned to the client virtual interface when using SSL/TLS and TUN modes or the interface address network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which dynamically. This mode is not compatible with several options, including Exit

**IPv6 Tunnel Network**

This is the IPv6 virtual network or network alias with a single entry used for the server expressed using CIDR notation (e.g. fe80::/64). When set static use be assigned to the client virtual interface. Leave blank if the server is capable

**IPv4 Remote network(s)**  **RED LOCAL MADRID**

IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN

12. Creamos una regla para permitir la comunicación entre Madrid y Barcelona mediante la VPN:

**Edit Firewall Rule**

**Action**

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface**

Choose the interface from which packets must come to match this rule.

**Address Family**

Select the Internet Protocol version this rule applies to.

**Protocol**

Choose which IP protocol this rule should match.

**Source** **RED LOCAL MADRID**

**Source** ☐ Invert match

**Destination**

**Destination** ☐ Invert match

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description**

Reiniciamos los servicios de las dos oficinas dentro de Status > OpenVPN...

**Comprobaciones:**

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

```

C:\Users\User01>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

    Sufijo DNS específico para la conexión. . . : cr.loc
    Vínculo: dirección IPv6 local. . . . . : fe80::ee45:e7cc:fa70:e2d8%13
    Dirección IPv4. . . . . : 192.168.10.201
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.10.1

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=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

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

C:\Users\User01>tracert 192.168.11.201

Traza a 192.168.11.201 sobre caminos de 30 saltos como máximo.

 1  <1 ms    <1 ms    <1 ms  pfsense.cr.loc [192.168.10.1]
 2  1 ms     <1 ms    <1 ms  10.0.1.0
 3  1 ms     1 ms     1 ms   192.168.11.201

Traza completa.

```

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

```

C:\Users\Adrian>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

    Sufijo DNS específico para la conexión. . . : home.arpa
    Vínculo: dirección IPv6 local. . . . . : fe80::a3ed:2a87:e038:b82f%13
    Dirección IPv4. . . . . : 192.168.11.201
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.11.1

C:\Users\Adria>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=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
Respuesta desde 192.168.10.201: bytes=32 tiempo=2ms 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

C:\Users\Adrian>tracert 192.168.10.201

Traza a 192.168.10.201 sobre caminos de 30 saltos como máximo.

 1  <1 ms    <1 ms    <1 ms  pfsense.home.arpa [192.168.11.1]
 2  1 ms     1 ms     1 ms   10.0.1.1
 3  1 ms     1 ms     1 ms   192.168.10.201

Traza completa.

```

-Si queremos configurar valencia, dentro de Madrid tenemos que...

-Crear un certificado para valencia:

**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: ?, >, <, &, /, \, ", '.

---

**Internal Certificate**

**Certificate authority**

**Key type**

The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

**Digest Algorithm**

The digest method used when the certificate is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

**Lifetime (days)**

The length of time the signed certificate will be valid, in days.  
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

**Common Name**

The following certificate subject components are optional and may be left blank.

**Country Code**

**State or Province**

**City**

**Organization**

**Organizational Unit**

---

**Certificate Attributes**

**Attribute Notes** The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending selected mode.  
For Internal Certificates, these attributes are added directly to the certificate as shown.

**Certificate Type**

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

**Alternative Names**

<input type="text" value="FQDN or Hostname"/>	<input type="text" value="pfsense3.cr.loc"/>	<input type="button" value="Delete"/>
<input type="text" value="IP address"/>	<input type="text" value="192.168.100.12"/>	<input type="button" value="Delete"/>

-Añadimos su IP remota en el server:

**VPN / OpenVPN / Servers**

**Servers** **Clients** **Client Specific Overrides** **Wizards**

**OpenVPN Servers**

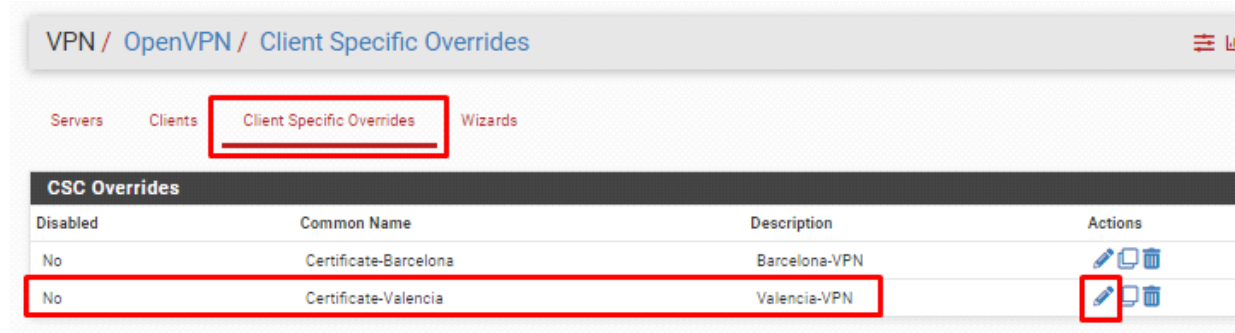
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.1.0/24	Mode: Peer to Peer ( SSL/TLS ) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN-Madrid	<input type="button" value="Edit"/> <input type="button" value="Clone"/> <input type="button" value="Delete"/>

network.

**IPv4 Remote network(s)**

IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN Expressed as a comma-separated list of one or more CIDR ranges or host/net here. May be left blank for non site-to-site VPN.

**-Creamos un nuevo override:**



**General Information**

Description:   
A description of this override for administrative reference.

Disable: ☐ Disable this override  
Set this option to disable this client-specific override without removing it from the list.

**Override Configuration**

Common Name:  mismo nombre que el certificado de valencia  
Enter the X.509 common name for the client certificate, or the username for VPNs utilizing password authentication. This match is case sensitive. Enter "DEFAULT" to override default client behavior.

Connection blocking: ☐ Block this client connection based on its common name.  
Prevents the client from connecting to this server. Do not use this option to permanently disable a client due to a compromised key or password. Use a CRL (certificate revocation list) instead.

Server List:   
Select the servers that will utilize this override. When no servers are selected, the override will apply to all servers.

**Tunnel Settings**

IPv4 Tunnel Network:  misma subred que en barcelona  
The virtual IPv4 network or network type alias with a single entry used for private communications between this client and the server expressed using CIDR (e.g. 10.0.8.5/24).  
With subnet topology, enter the client IP address and the subnet mask must match the IPv4 Tunnel Network on the server.  
With net30 topology, the first network address of the /30 is assumed to be the server address and the second network address will be assigned to the client.

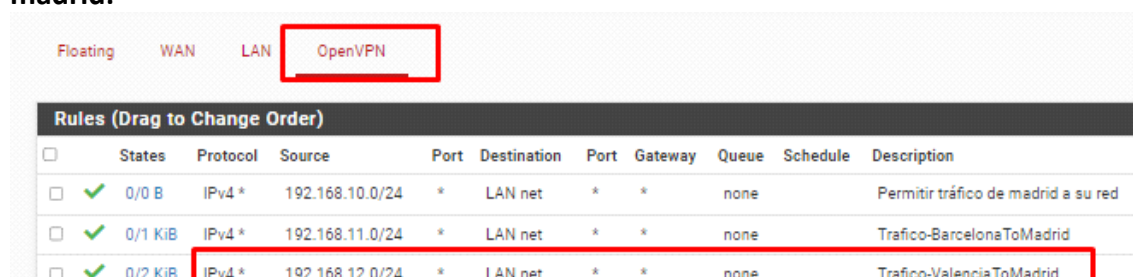
IPv6 Tunnel Network:   
The virtual IPv6 network or network type alias with a single entry used for private communications between this client and the server expressed using prefix (e.g. 2001:db9:1:1::100/64).  
Enter the client IPv6 address and prefix. The prefix must match the IPv6 Tunnel Network prefix on the server.

IPv4 Local Network/s:   
These are the IPv4 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases.  
NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

IPv6 Local Network/s:   
These are the IPv6 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more IP/PREFIX networks.  
NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

IPv4 Remote Network/s:  red local de valencia

**-Añadimos una regla en Madrid, para permitir tráfico de valencia a madrid:**



## Dentro de valencia...

### -Importamos el CA de Madrid:

Authorities Certificates Revocation

#### Create / Edit CA

**Descriptive name**  MISMO NOMBRE QUE EL CA DE 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**

**Trust Store** ☐ Add this Certificate Authority to the Operating System Trust Store  
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

**Randomize Serial** ☐ Use random serial numbers when signing certificates  
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically checked for uniqueness instead of using the sequential value from Next Certificate Serial.

#### Existing Certificate Authority

**Certificate data**   
Paste a certificate in X.509 PEM format here. CERT DE MADRID

**Certificate Private Key (optional)**   
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate. KEY DE MADRID

**Next Certificate Serial**   
Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is checked.

### -Importamos el certificado de Valencia que hemos creado en Madrid:



Authorities **Certificates** Certificate Revocation

### Edit an Existing Certificate

<b>Method</b>	<input type="button" value="Edit an existing certificate"/> <input type="button" value="IMPORT AN EXISTING CERTIFICATE NO EDIT"/>
<b>Descriptive name</b>	<input type="text" value="Certificate-Valencia"/> <b>MISMO NOMBRE QUE EL CERTIFICADO DE VALENCIA</b>
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: ?, >, <, &, /, \, *, '	
<b>Subject</b>	CN=Certificate-Valencia

### Edit Certificate

**Certificate Type**

☒ X.509 (PEM)
 ☐ PKCS #12 (PFX)

<b>Certificate data</b>	<pre>-----BEGIN CERTIFICATE----- MIIDSjCCApqgAwIBAgIBBjANBgkqhkiG9w0BAQsFADANMRQwEgYDVQQDEwZDZXJ0 LU1hZHZpZDAeFw0yMzEwMzEwMDM2MDdaFw0zMzEwMjg0MDM2MDdaMB8xHTAbBgNV BAMTFEN1cnRpZmljYXR1LVZhbGVuY2l0hMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A MIIBCgKCAQEAnGpAdAaF1Jf35y5OfQqtKTsaMqYcfnGD2Af1P5E9nVJAZqw8vIK1 -----</pre> <p>Paste a certificate in X.509 PEM format here.</p>
<b>Private key data</b>	<pre>-----BEGIN PRIVATE KEY----- MIIEvgIBADANBgkqhkiG9w0BAQFAASCBAgEAAoIBAQCcakB0B0wU1/fn Lk59Cq0pOxoyphx+cYPYB/U/kT2dukBmrDy8grwCvWz5XUymP3GMMt05nDQUQLf mbAiC1YM0L+63VEbejk+d11Y56zBGSz1bzY1ud8QsRxlReRsyRBwmMYIK402MG0z BTkgLctmbV9xeLxN4nuilVXFmk167yI6oKYSukEoJz8Pudz6KwBNhIucMLHw+z77 -----</pre> <p>Paste a private key in X.509 PEM format here. This field may remain empty in certain cases, such as when the private key is stored on a PKCS#11 token.</p>

**-Configuramos el cliente VPN en Valencia:**



Servers **Clients** Client Specific Overrides Wizards

## General Information

**Description** Valencia-VPN **MISMO NOMBRE QUE EL CLIENTE DE VALENCIA EN MADRID**  
A description of this VPN for administrative reference.

**Disabled** ☐ Disable this client  
Set this option to disable this client without removing it from the list.

**Unique VPN ID** Client 1 (ovpnc1)

## Mode Configuration

**Server mode** Peer to Peer ( SSL/TLS )

**Device mode** tun - Layer 3 Tunnel Mode

"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across a  
"tap" mode is capable of carrying 802.3 (OSI Layer 2)

## Endpoint Configuration

**Protocol** UDP on IPv4 only

**Interface** WAN

The interface used by the firewall to originate this OpenVPN client connection

**Local port**  
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.

**Server host or address** 192.168.100.10 **IP PUBLICA DE MADRID**  
The IP address or hostname of the OpenVPN server.

**Server port** 1194  
The port used by the server to receive client connections.

## Cryptographic Settings

**TLS Configuration** ☒ Use a TLS Key  
A TLS key enhances security of an OpenVPN connection by requiring a TLS handshake. This layer of HMAC authentication is dropped, protecting the peers from attack or unauthorized connection data.

☐ Automatically generate a TLS Key.

## TLS Key

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
6509d30b1d58e5b690a628158db05123
```

Paste the TLS key here.

PEGAMOS EL CONTENIDO DEL FICHERO TLS  
QUE HEMOS PEGADO TAMBIEN A BARCELONA

control channel obfuscation.

**TLS keydir direction** Use default direction

The TLS Key Direction must be set to complementary values on the client and server. The client must be set to 1. Both may be set to omit the direction, in which case the

**Peer Certificate Authority** Cert-Madrid CA DE MADRID

**Peer Certificate Revocation list** No Certificate Revocation Lists defined. One may be created here: [System > Cert. I](#)

**Client Certificate** Certificate-Valencia CERT DE VALENCIA CA: Cert-Madrid, In Use

AFS-128-CRC (128 bit key 128 bit block) AFS-256-GCM

---

**Tunnel Settings**

**IPv4 Tunnel Network** 10.0.1.0/24 MISMA SUBRED QUE A BARCELONA

This is the IPv4 virtual network or network type alias with a single entry used for private communication and the server expressed using CIDR notation (e.g. 10.0.8.0/24).

This should be left blank in most cases as servers typically provide addresses to clients dynamically.

The second usable address in this network will be assigned to the client virtual interface. Ensure it matches the server when using SSL/TLS and TUN modes or the interface address may not be correct. A network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot receive addresses dynamically. This mode is not compatible with several options, including Exit Notify, and Inactive

**IPv6 Tunnel Network**

This is the IPv6 virtual network or network alias with a single entry used for private communication and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the :: address will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses

**IPv4 Remote network(s)** 192.168.10.0/24 RED LOCAL DE MADRID

IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established by changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges or aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site

**-Creamos una regla para permitir el tráfico entre Madrid y Valencia:**



```

C:\Users\User01>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

    Sufijo DNS específico para la conexión. . . : cr.loc
    Vínculo: dirección IPv6 local. . . : fe80::ee45:e7cc:fa70:e2d8%13
    Dirección IPv4. . . . . : 192.168.10.201
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : 192.168.10.1

C:\Users\User01>ping 192.168.12.202

Haciendo ping a 192.168.12.202 con 32 bytes de datos:
Respuesta desde 192.168.12.202: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.12.202: bytes=32 tiempo=2ms TTL=126
Respuesta desde 192.168.12.202: bytes=32 tiempo=2ms TTL=126
Respuesta desde 192.168.12.202: bytes=32 tiempo=2ms TTL=126

Estadísticas de ping para 192.168.12.202:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\User01>tracert 192.168.12.202

Traza a 192.168.12.202 sobre caminos de 30 saltos como máximo.

 1    <1 ms    <1 ms    <1 ms    pfsense.cr.loc [192.168.10.1]
 2     1 ms     1 ms     <1 ms     10.0.1.0
 3     1 ms     <1 ms    <1 ms     192.168.12.202

Traza completa.

```

#### -Valencia-Madrid:

```

C:\Users\Adrian>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

    Sufijo DNS específico para la conexión. . . : cr.loc
    Vínculo: dirección IPv6 local. . . : fe80::ec3b:fc37:5b4b:1491%5
    Dirección IPv4. . . . . : 192.168.12.202
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : 192.168.12.1

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=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
Respuesta desde 192.168.10.201: bytes=32 tiempo=2ms 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

C:\Users\Adrian>tracert 192.168.10.201

Traza a 192.168.10.201 sobre caminos de 30 saltos como máximo.

 1    <1 ms    <1 ms    <1 ms    pfsense3.cr.loc [192.168.12.1]
 2     1 ms     <1 ms    <1 ms     10.0.1.1
 3     1 ms     1 ms     1 ms     192.168.10.201

Traza completa.

```