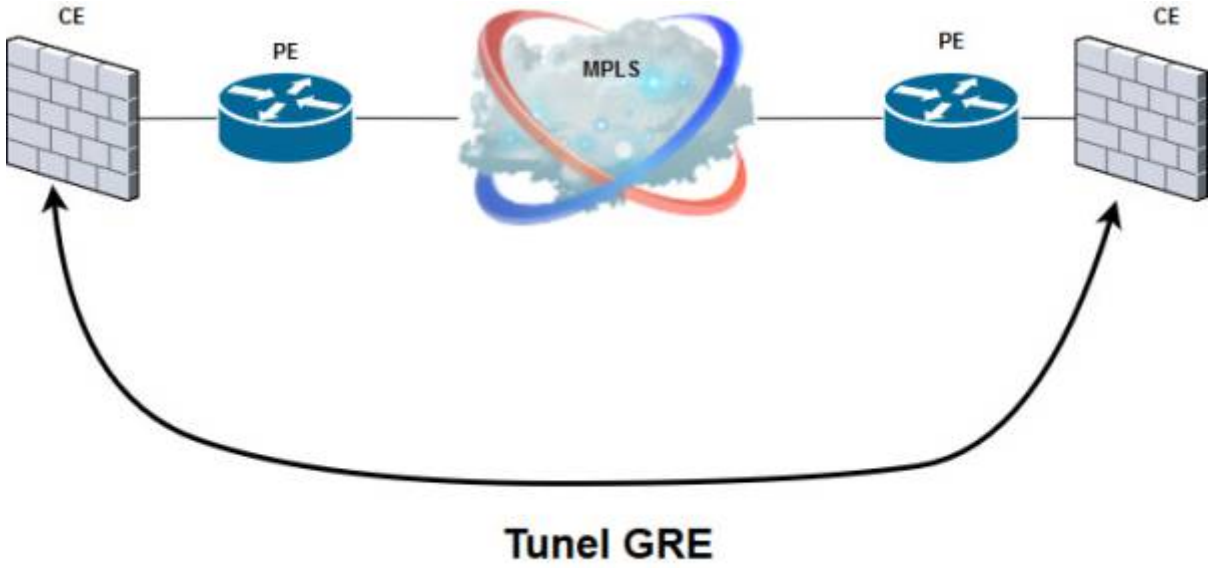
Tunel GRE entre dos cortafuegos Fortinet

GRE (Generic Routing Encapsulation)es un protocolo para el establecimiento de túneles entre sitios .https://es.wikipedia.org/wiki/GRE Basicamente con un tunel GRE encapsulamos cualquier trafico y lo enviamos al gateway remoto. Un tunel GRE puede usarse con o sin encriptación ipsec.

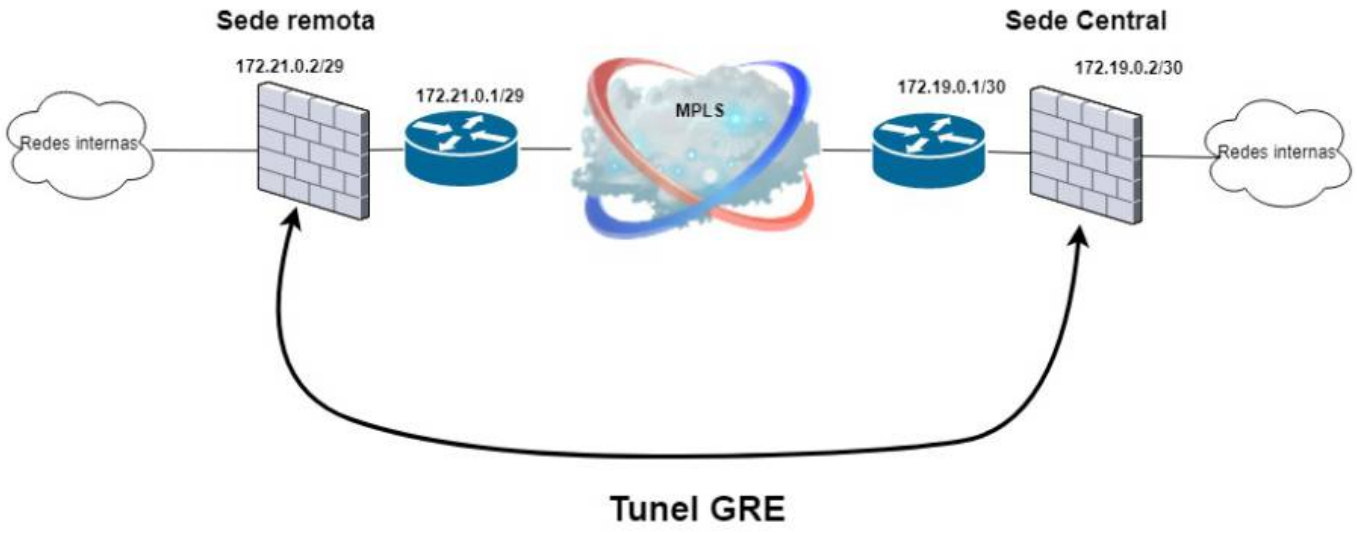


- CE → Router del cliente. en nuestro caso los fortigate (Customer Edge Router)
- PE → Router del proveedor de la conexión (Provider Edge Router)

Creación de un tunel GRE entre dos fortigate

En este ejemplo vamos a conectar dos sedes que tienen a su vez varias subredes internas con distintos rangos de ip y que el proveedor de la conexión MPLS no nos las tiene enrutadas y por tanto para que se vean las subredes internas de cada sede utilizaremos un tunel GRE a través de una conexión MPLS entre dichas sedes.

Hay que conectarse a los fortigate de cada sede para realizar la configuración. Con el proveedor de la conexión decidiremos un rango de red para utilizar en cada sede . Este rango es independiente del resto de redes que tengamos ya que es para conectar nuestro frewall con el router del proveedor. En este caso utilizamos las redes 172.21.0.0/29 para la sede remota y la 172.19.0.0/30 para la sede principal



Sede remota

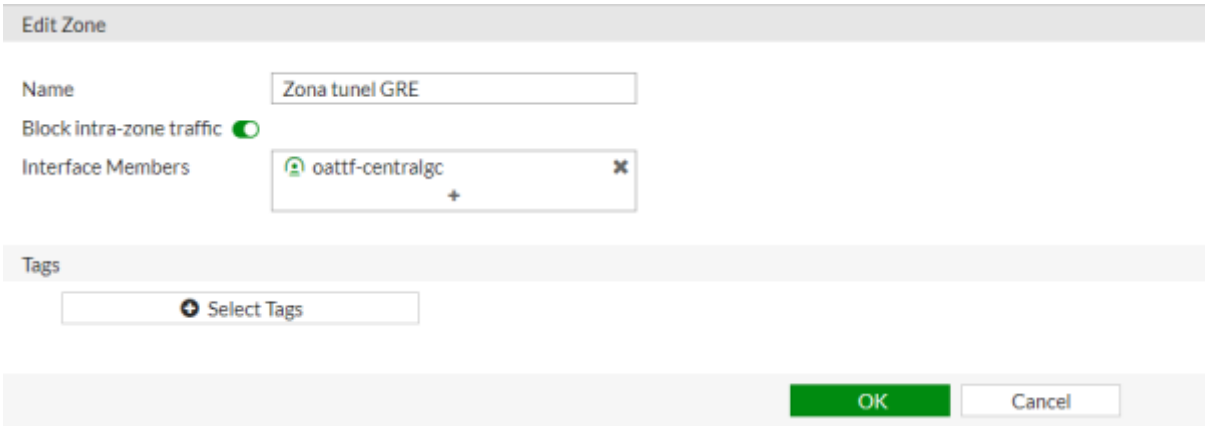
```
config system gre-tunnel
edit "gre-centralgc"
set interface "WAN2"
set remote-gw 172.19.0.2
set local-gw 172.21.0.2
next
end
```

- Habilitar una política de salida que permita el trafico de la zona interna al nuevo interfaz a-centralgc y otra que permita el trafico del nuevo interfaz a la zona interna
- Definir una ruta estática que indique como alcanzar el gateway remoto
- Definir rutas que indiquen que redes son alcanzables por el interfaz gre-tunnel o habilitar en enrutamiento dinámico.

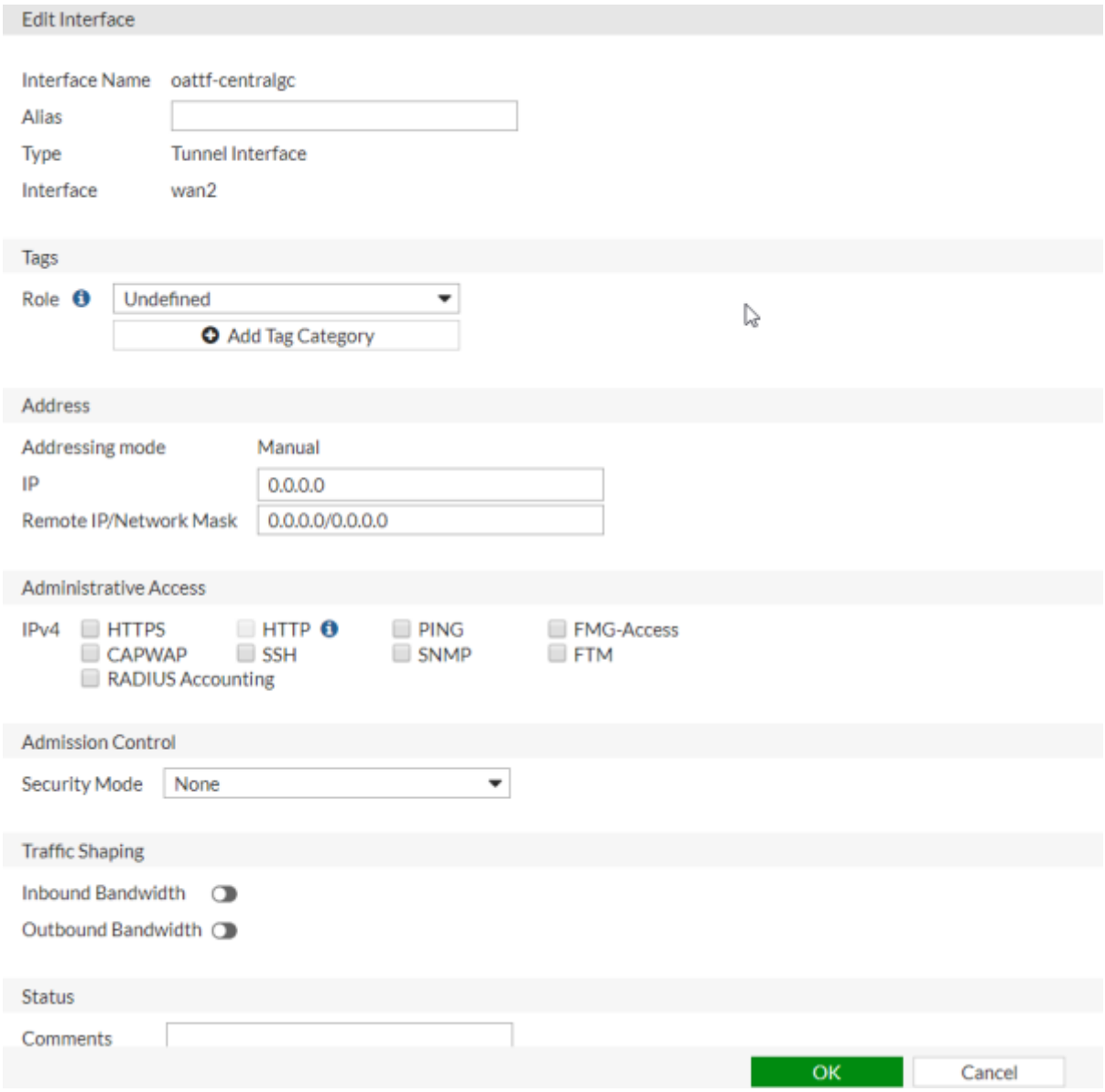
Sede Principal

```
config system gre-tunnel
edit "gre-remotogc"
set interface "port20"
set remote-gw 172.21.0.2
set local-gw 172.19.0.2
next
end
```

El siguiente paso será crear una zona y añadir el nuevo interfaz a dicha zona



Editamos el interfaz y le asignamos una ip local y le indicamos la ip remota (estas ips son distintas de las que usamos para crear el tunel. Son ips que nosotros mismo le damos a ese tunel para uso interno.



- Habilitar una política de salida que permita el trafico de la zona interna al nuevo interfaz a-centralgc y otra que permita el trafico del nuevo interfaz a la zona interna
- Definir una ruta estática que indique como alcanzar el gateway remoto
- Definir rutas que indiquen que redes son alcanzables por el interfaz gre-tunnel o habilitar en

enrutamiento dinámico.

Verificar tunel

```
diag system gre list
```

Referencias

- https://ccnadesdecero.es/tuneles-gre-caracteristicas-y-configuracion/
- http://www.mirazon.com/how-to-create-a-gre-tunnel-within-fortigate/

From:
http://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
http://wiki.intrusos.info/doku.php?id=hardware:fortigate:gre&rev=1566548417

Last update: **2023/01/18 14:16**