fortigate, vpn, ipsec

VPN

Crear una VPN usando IPSec

En un fortigate las VPNs pueden ser **policy-base** o **route-base**. Hay pequeñas diferencias entre una y otra y por lo general se emplea la **route-base** debido a que es más flexible y sencilla de configurar.

Una conexión VPN mediante ipsec se establece mediante dos fases. Las parámetros de cada fase deben de coincidir en ambos extremos de la conexión VPN, exceptuando las ips de los gateway de cada extremo.

Los pasos para crear una VPN mediante IPSEC son los siguientes:

1. previamente definir los usuarios y grupos que vamos a utilizar en la conexión
2. Definir los parámetros de la Fase1
3. Definir los parámetros de la Fase2
4. Especificar las reglas de acceso

Crear usuarios/grupos de usuarios para la autenticación

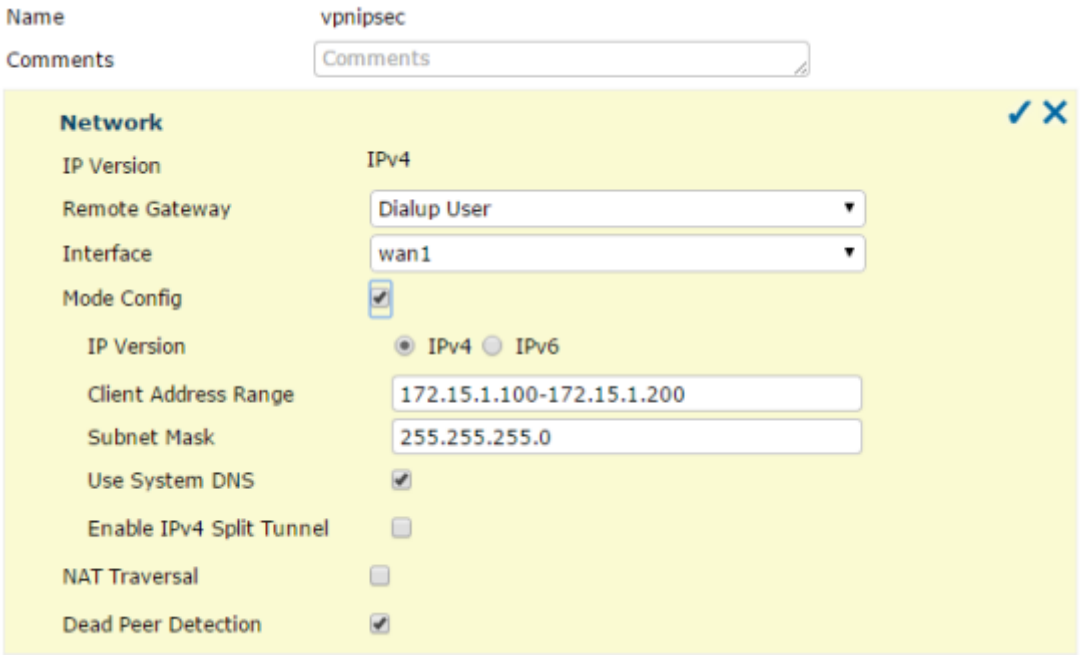
Para crear los usuarios vamos a Usuarios & Dispositivos→Usuario →Crear Nuevo

Creamos un grupo para los accesos por vpn → Usuario & Dispositivo →Grupo de Usuario → Crear nuevo

Añadimos el usuario creado al grupo de acceso por vpn

Crear VPN

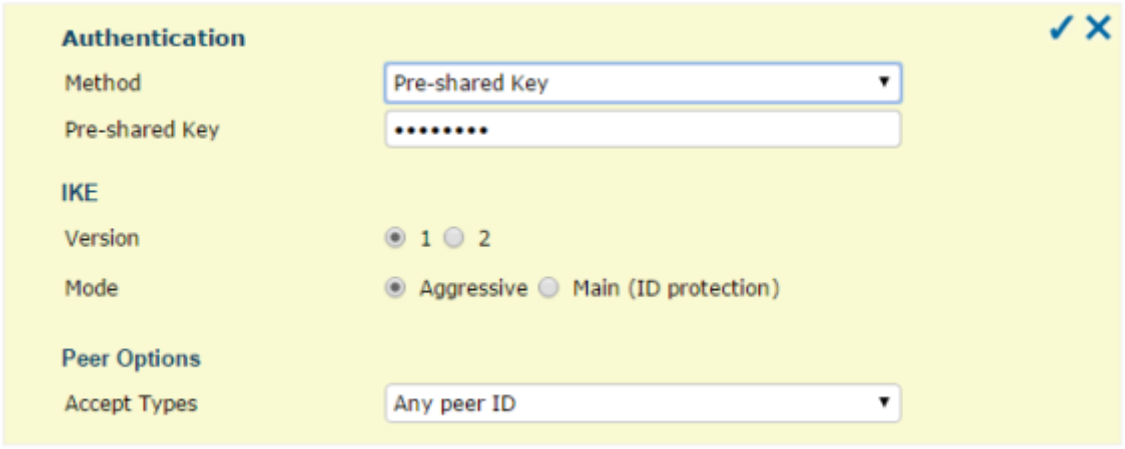
Ejemplo de una VPN ipsec



El rango de direcciones ip no tienen que coincidir con ningún otro que tengamos en la red

Fase 1

La fase1 tiene dos modos agresivo y principal/main. **Agresivo** → Modo más rápido. Va sin encriptar el primer paquete de autenticación , recomendado para clientes remotos. **Principal/main**→ Modo más seguro. El primer paquete de autenticación va encriptado, recomendado para site-to-site.



En las versiones anteriores a la 5.2 al pulsar en la fase 1 sobre avanzado si marcamos la casilla Habilitar IPSEC en modo interfaz estamos habilitando la VPN en modo route-based. Si no la marcamos entonces el modo es policy-based

Phase 1 Proposal

Los parámetros que pongamos en este apartado deben de ser los mismos que luegos pongamos en la configuración del Forticlient

EL Valor que pongamos el el **Diffie-Hellman Group** determina la fortaleza de la clave de intercambio . Un número alto implica más seguridad, pero también más tiempo para procesarla

- Diffie-Hellman group 1 - 768 bit - No recomendado
- Diffie-Hellman group 2 - 1024 bit - No recomendado
- Diffie-Hellman group 5 - 1536 bit - No recomendado
- Diffie-Hellman group 14 - 2048 bit – Mínimo aceptable
- Diffie-Hellman group 19 - 256 bit elliptic curve – ACEPTABLE
- Diffie-Hellman group 20 - 384 bit elliptic curve – Next Generation Encryption
- Diffie-Hellman group 21 - 521 bit elliptic curve – Next Generation Encryption

El DHG debe de ser el mismo en ambos extremos de la conexión

XAUTH

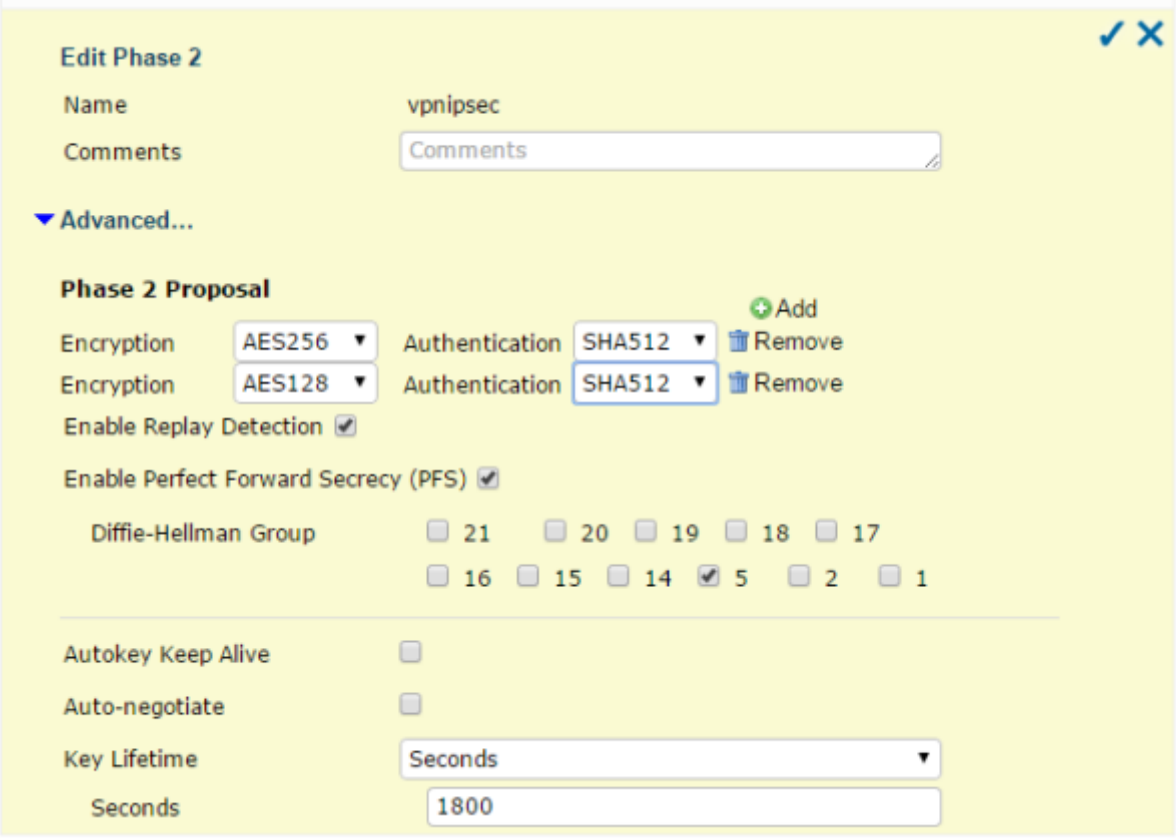
Si queremos que el usuario a su vez se autentifique

Split Tunneling

Si está activado los usuarios usan su propia conexión a Internet. Si está desactivado y habilitamos las políticas necesarias, el usuario navegara a internet a través del Fortigate

Fase 2

Los parámetros deben de coincidir con los que luegos pongamos en el cliente



La encriptación más segura que tenemos con esta versión es la AES256 con la autenticación SHA512

PFS **Perfect Forward Secrecy hace que la generación de las claves de intercambio sean más seguras ya que se asegura de no utilizar claves anteriores

Debug de la conexión VPN

Para hacer un debug de la conexíon IPSEC hay que ejecutar los siguientes comandos:

1. Habilitar el modo debug

```
diag debug enable
```

2. Para ver los mensaje ipsec

```
 diag debug app ike -1
```

3. Para saber si tenemos problemas con una política del firewall

```
diag debug flow
```

4. Para salir del modo debug

```
diag debug reset
```

```
diag debug disable
```

Verificar parámetros vpn

```
diag vpn tunnel list
```

Con este comando obtenemos datos como el número de paquetes encriptados/desencriptados. Bytes enviados/recibidos

```
diag vpn ike config list
```

Referencias

- http://soclevelone.com/index.php/2018/05/20/setting-vpn-ipsec-tunnel-with-fortigate/
- http://cookbook.fortinet.com/ipsec-vpn-troubleshooting/
- VPN con certificados http://docs.fortinet.com/fos50hlp/50/index.html#page/FortiOS%25205.0%2520Help/Certificates.077.33.html
- http://docs.fortinet.com/fgt/handbook/50/fortigate-ipsec-50.pdf
- http://docs.fortinet.com/fos50hlp/50/index.html#page/FortiOS%25205.0%2520Help/IntroVPN.html
- http://itsecworks.wordpress.com/2012/03/22/debugging-fortigate-vpns/
- http://www.soportejm.com.sv/kb/index.php/article/ipsec-dialup
- http://www.bujarra.com/hacer-una-vpn-con-ipsec-en-fortigate/
- http://firewallguru.blogspot.com.es/2009/05/creating-self-signed-certificates-for.html