

fortigate, vpn, ipsec

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. Los 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

The screenshot shows the FortiGate configuration page for a new VPN named 'vpnipsec'. The 'Name' field is filled with 'vpnipsec' and the 'Comments' field is empty. Below this is a yellow configuration box titled 'Network' with a close button (X) in the top right corner. Inside the box, the following settings are visible:

- IP Version:** IPv4
- Remote Gateway:** Dialup User
- Interface:** wan1
- Mode Config:** ☒
- IP Version:** ☒ IPv4 ☐ IPv6
- Client Address Range:** 172.15.1.100-172.15.1.200
- Subnet Mask:** 255.255.255.0
- Use System DNS:** ☒
- Enable IPv4 Split Tunnel:** ☐
- NAT Traversal:** ☐
- Dead Peer Detection:** ☒



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.

Authentication

Method: Pre-shared Key

Pre-shared Key:

IKE

Version: ☒ 1 ☐ 2

Mode: ☒ Aggressive ☐ Main (ID protection)

Peer Options

Accept Types: Any peer ID



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 luego pongamos en la configuración del Forticlient



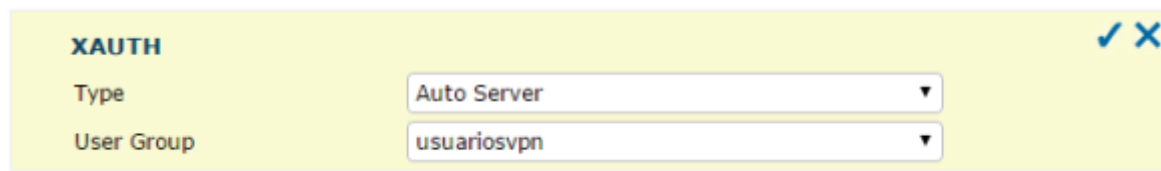
EL Valor que pongamos en el **Diffie-Hellman Group** determina la fortaleza de la clave de intercambio. Un número alto implica más seguridad, pero también más tiempo para procesarla.



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

XAUTH

Si queremos que el usuario a su vez se autentifique



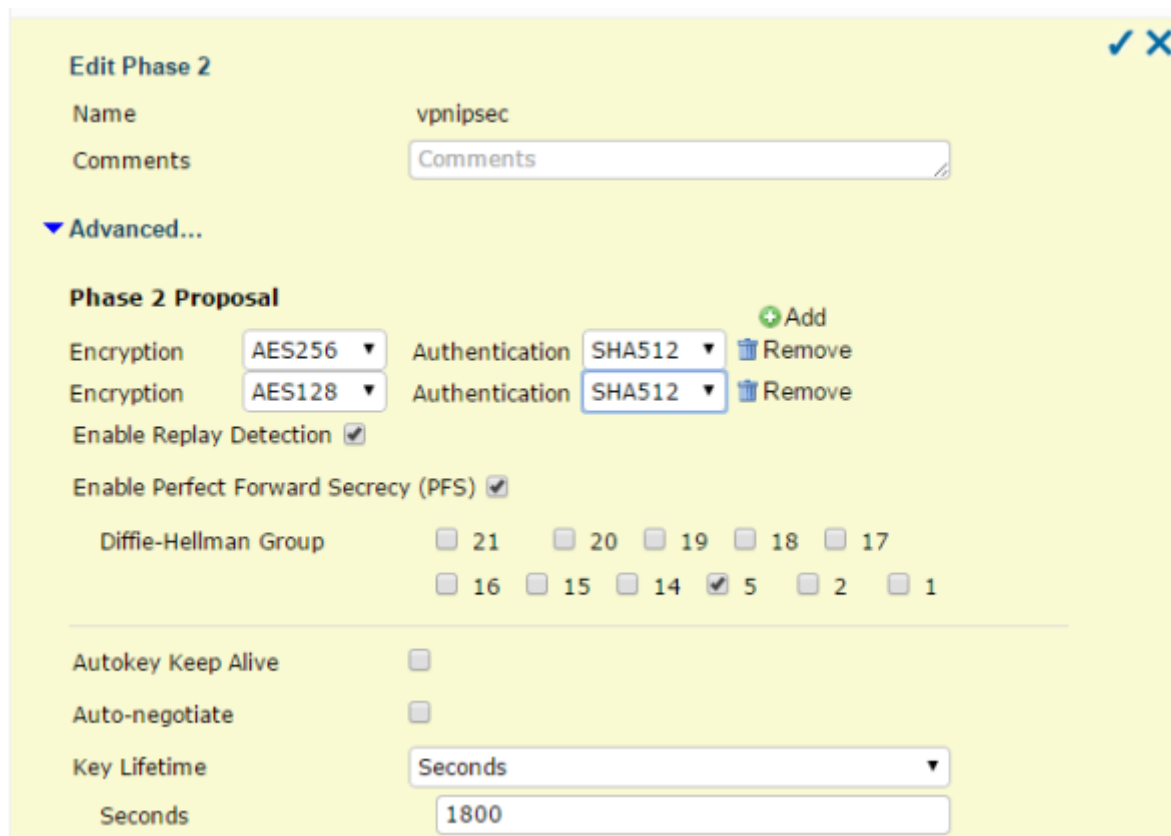
XAUTH ✓ ✕

Type: Auto Server

User Group: usuariosvpn

Fase 2

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



Edit Phase 2 ✓ ✕

Name: vpnipsec

Comments: Comments

▼ Advanced...

Phase 2 Proposal

Encryption: AES256 Authentication: SHA512 Add Remove

Encryption: AES128 Authentication: SHA512 Remove

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☒

Diffie-Hellman Group: ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☐ 14 ☒ 5 ☐ 2 ☐ 1

Autokey Keep Alive ☐

Auto-negotiate ☐

Key Lifetime: Seconds

Seconds: 1800



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 conexión 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 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://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>

From:

<https://intrusos.info/> - LCWIKI

Permanent link:

<https://intrusos.info/doku.php?id=hardware:fortigate:vpn&rev=1523014930>

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

