

fortigate, vpn, ipsec

VPN 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.

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

1. Definir los parámetros de la Fase1
2. Definir los parámetros de la Fase2
3. Especificar las direcciones de origen y de destino

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 configuration page for a VPN named 'vpnipsec'. The 'Network' tab is selected, showing the following settings:

- Name:** vpnipsec
- Comments:** Comments
- IP Version:** IPv4
- Remote Gateway:** Dialup User
- Interface:** wan1
- Mode Config:** ☒
- IP Version (under Mode Config):** ☒ 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

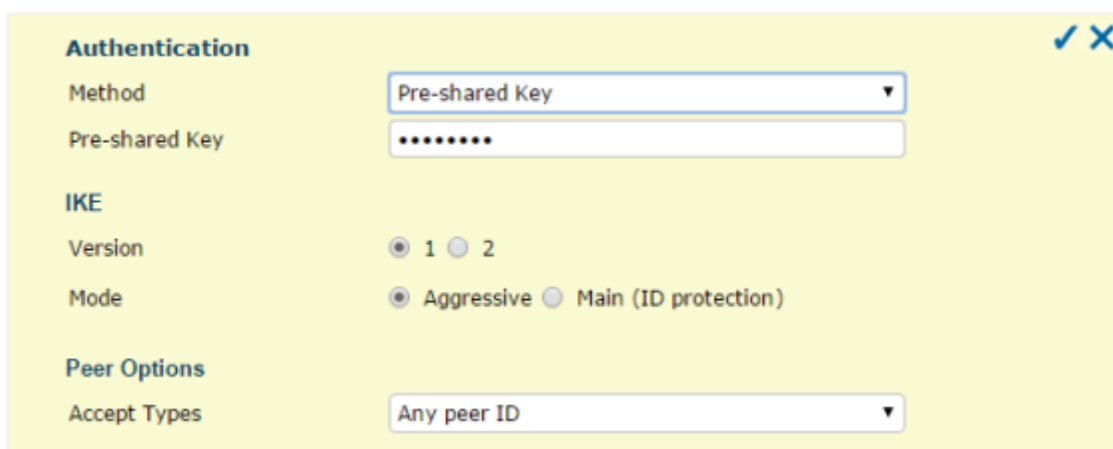
La fase1 tiene dos modos agresivo y principal/main.

Agresivo

Va sin encriptar el primer paquete de autenticación , recomendado para clientes remotos

Principal/main

El primer paquete de autenticación va encriptado, recomendado para site-to-site



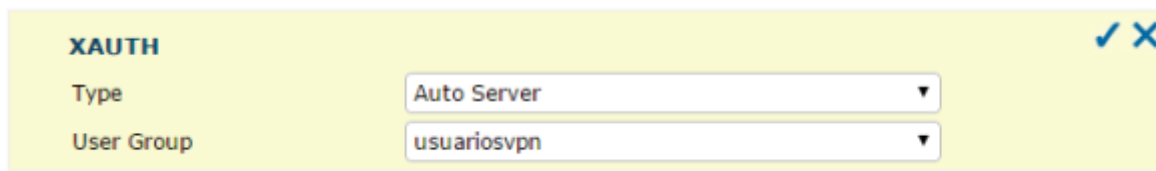
En las versiones anteriores a la 5.2 al pulsar en la fase 1 sobre avanzado si marcamos la casilla Habilitar IPSEC en modo interfaz estamos habilitando la VPN en modo route-based. Si no la marcamos entonces el modo es policy-based

Phase 1 Proposal

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

XAUTH

Si queremos que el usuario a su vez se autentifique



Fase 2

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

Edit Phase 2 ✓ X

Name: vpnipsec

Comments:

▼ Advanced...

Phase 2 Proposal

Encryption: AES256 Authentication: SHA512

Encryption: AES128 Authentication: SHA512

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

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 disable  
diag debug app ike 0
```

Verificar parámetros vpn

```
diag vpn ike config list
```

Referencias

- 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.soprotejm.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:

<http://wiki.intrusos.info/> - **LCWIKI**

Permanent link:

<http://wiki.intrusos.info/doku.php?id=hardware:fortigate:vpn&rev=1430128813>

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

