

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 'Name' field is filled with 'vpnipsec' and there is a 'Comments' field below it. The configuration is divided into a 'Network' section (highlighted in yellow) and other options. In the 'Network' section, 'IP Version' is set to 'IPv4', 'Remote Gateway' is 'Dialup User', 'Interface' is 'wan1', and 'Mode Config' is checked. Below this, 'IP Version' is set to 'IPv4' (radio button selected), 'Client Address Range' is '172.15.1.100-172.15.1.200', 'Subnet Mask' is '255.255.255.0', 'Use System DNS' is checked, 'Enable IPv4 Split Tunnel' is unchecked, 'NAT Traversal' is unchecked, and 'Dead Peer Detection' is checked. There are checkmark and close icons in the top right of the yellow box.

Name	vpnipsec
Comments	Comments
Network	
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 no tienen que coincidir con ningún otro que tengamos en la red

Fase 1

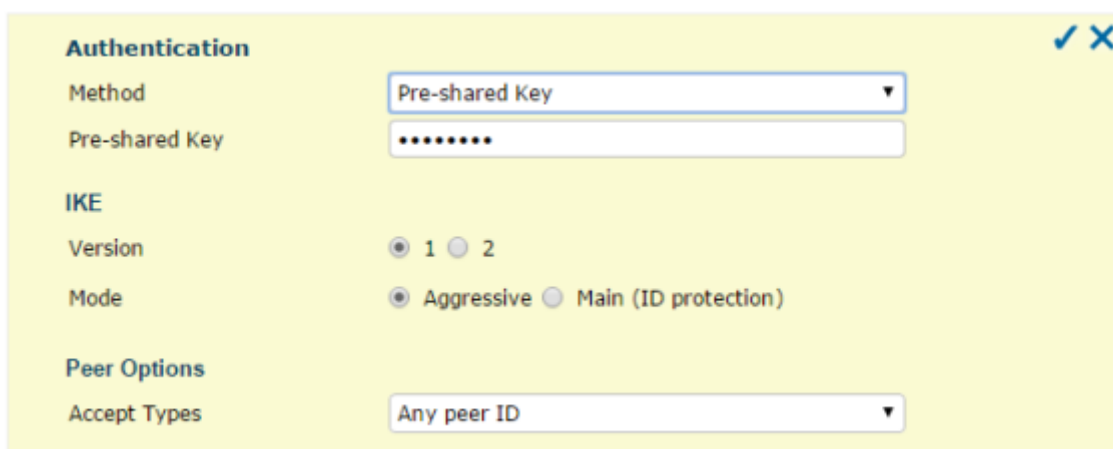
La fase1 tiene dos modos agresivo y principal/main.

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



Authentication

Method: Pre-shared Key

Pre-shared Key:

IKE

Version: ☒ 1 ☐ 2

Mode: ☒ Aggressive ☐ Main (ID protection)

Peer Options

Accept Types: Any peer ID

Enable IPSEC Interface mode



En la fase uno al pulsar 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

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.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:

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

Permanent link:

<http://wiki.intrusos.info/doku.php?id=hardware:fortigate:vpn&rev=1430128162>

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

