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

Configurar servidor DHCP

ir al interfaz WAN por el que se van a validar los clientes y marcar la opción de habilitar **DHCP Server**

Dar de alta en los objetos del firewall la red que hemos creado. Objetos del firewall→dirección→crear nuevo

Crear usuarios/grupos de usuarios para la autenticación

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

Creamos el grupo → Usuario & Dispositivo →Grupo de Usuario → Crear nuevo

Fase 1

La fase1 tiene dos modos agresivo y principal/main.

Agresivo

Principal/main

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 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 salir del modo debug

```
diag debug disable
diag debug app ike 0
```

Referencias

- 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/