fortigate, vpn, sede

# Conexión de sedes mediante una VPN

Vamos a realizar una conexión entre sedes, teniendo en cada sede un equipo fortigate. Para ello tenemos que crear una conexión VPN en cada sede.

#### Creamos la VPN en la sede central

Utilizamos el asistente para realizar la configuración. Para ello vamos al menú de la izquierda y seleccionamos VPN→IPsec→Wizard y seleccionamos la opción Site to Site - Fortigate

FORTINET	FortiGate	520B	
System Router Policy & Objects		VPN Setup     Authentication     Policy & Routi	VPN Creation Wizard
Security Profiles		Name vpn a central Template	
Psec     Tunnels     Wizard     Tunnel Template	25	Dialup - FortiClient (Windows, Mac OS, Android)     Site to Site - FortiGate     Dialup - iOS (Native)	
9 🛃 SSL 9 🕎 Monitor		Dialup - Android (Native L2TP/IPsec)	
		<ul> <li>Site to Site - Cisco</li> <li>Custom VPN Tunnel (No Template)</li> </ul>	
		< Back: Next > Cance	ef

Definimos en remote gateway la ip pública del equipo al que vamos a conectarnos, la interfaz de salida por la que vamos a conectar y el tipo de autenticación que vamos a usar en ambos extremos.



VPN Setup 2 Authentication 3 Policy & Routing				
vpn a central : Site to Site - FortiGate				
Bemete Cateway				
Remote Gateway	ip pública equipo remoto			
Outgoing Interface	WAN 1			
Authentication Method	Pre-shared Key			
Pre-shared Key	I			
	Hide Characters			
< Back Next	> Cancel			

Definimos el interfaz de entrada de la red local, el direccionamiento ip de la red local y el de la la red remota

VPN Setup 💙	✓ Authentication	3 Policy & Routing	
	fgdg : Site to	Site - FortiGate	
Local Interface			•
Local Subnets			2
< Back	Creste	Cance	

Al finalizar el asistente nos creará las políticas, las rutas, los grupos y objetos necesarios.

### Creamos la VPN en la oficina remota

Seguimos los mismo pasos que cuando creamos la VPN en la sede central, pero cambiando los parámetros del gateway remoto, puerto, etc con los nuevos valores .

VPN Setup 2 Authority	entication 3 Policy & Routing			
vpn a	central : Site to Site - FortiGate			
Remote Gateway Outgoing Interface Authentication Method Pre-shared Key	ip pública equipo remoto WAN 1 ▼ ● Pre-shared Key ○ Signature ••••••• ☐ ☐ ✓ Hide Characters			
< Back Next > Cancel				
VPN Setup 🔀 Aut	hentication 3 Policy & Routing			
f	fgdg : Site to Site - FortiGate			
Local Interface	-			
Local Subnets				
Remote Subnets				
< Back	Canc			

## Conexión de la sede al AD

Deberemos abrir ciertos puertos desde dicha oficina a nuestros servidores del dominio. En concreto para servidores de domino con Windows 2012 Server

Puertos de cliente	Puerto del servidor	Servicio
-49152 65535/UDP	123/UDP	W32Time
-49152 65535/TCP	135/TCP	Asignador de extremos RPC
-49152 65535/TCP	464/TCP/UDP	Cambio de contraseña de Kerberos
-49152 65535/TCP	49152-65535/TCP	RPC de LSA, SAM, Netlogon (*)
-49152 65535/TCP/UDP	389/TCP/UDP	LDAP

Puertos de cliente	Puerto del servidor	Servicio
-49152 65535/TCP	636/TCP	LDAP SSL
-49152 65535/TCP	3268/TCP	CATÁLOGO GLOBAL LDAP
-49152 65535/TCP	3269/TCP	LDAP SSL DE GC
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
-49152 65535/TCP	-49152 65535/TCP	FRS RPC
-49152 65535/TCP/UDP	88/TCP/UDP	Kerberos
-49152 65535/TCP/UDP	445/TCP	SMB
-49152 65535/TCP	49152-65535/TCP	DFSR RPC

#### Referencias

 https://support.microsoft.com/es-es/help/179442/how-to-configure-a-firewall-for-domains-and-tr usts

From: http://wiki.intrusos.info/ - **LCWIKI** 

Permanent link: http://wiki.intrusos.info/doku.php?id=hardware:fortigate:conectarsede



Last update: 2023/01/18 14:36