

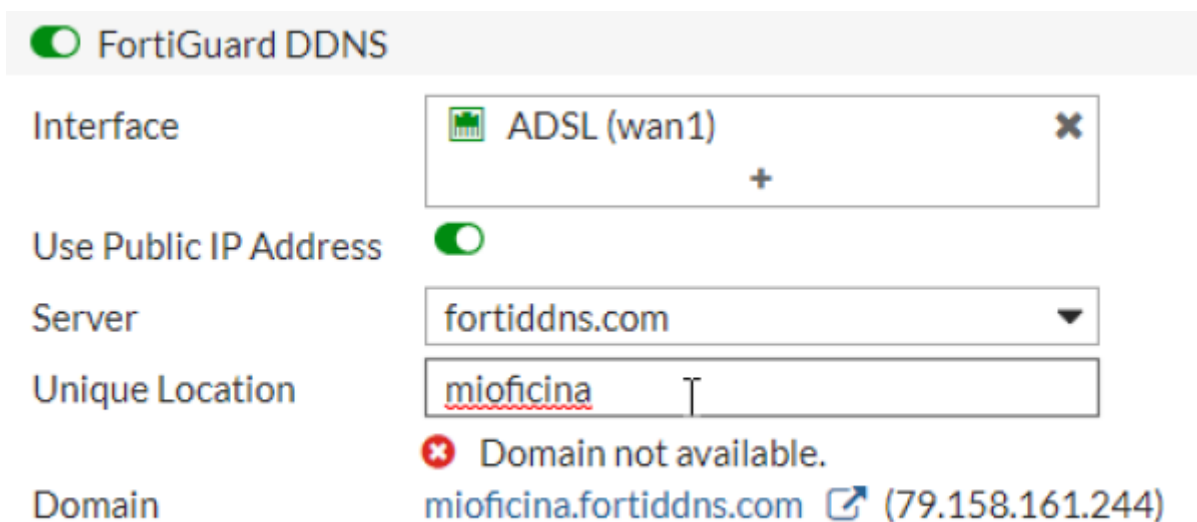
VPN sede remota a central

Vamos a conectar mediante una conexión de ADSL o FFTH con una ip dinámica, una oficina remota a la central mediante una conexión vpn Lo primero es cambiar el router de nuestro operador por un <https://naseros.com/2020/05/19/sustitucion-hgu-movistar-y-o2-por-un-router-neutro/> o bien poner el router del operador en modo bridge.

Al no disponer de ip fija no podemos establecer a priori la puerta de enlace origen/destino del túnel vpn, por lo que lo primero que necesitamos es configurar nuestro cortafuegos con el DDNS de forma que nos podamos conectar con él mediante un nombre dns

Para ello tenemos que ir a la GUI de nuestro firewall Network → DNS y activar la opción Fortiguard DDNS

configuramos dicha opción y en la casilla **Unique Location** ponemos un nombre que sea único y que utilizaremos para obtener la ip.



Creamos una vpn en la oficina remota

Network → SD-WAN → En SD-WAN interface members → Create New

FortiGate 101E FWR0022

Dashboard > SD-WAN

Security Fabric >

FortiView >

Network >

Interfaces

DNS

DNS Servers

Packet Capture

SD-WAN ☆

SD-WAN Rules

Performance SLA

Static Routes

Policy Routes

RIP

OSPF

BGP

Multicast

FortiExtender

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

Log & Report >

Monitor >

Name SD-WAN

Type SD-WAN Interface

Status Enable Disable

SD-WAN Interface Members

+ Create New Edit Delete

Interfaces	Gateway	Cost
ADSL (wan1)	192.168.144.1	0
Datos Vodafone (wan2)	0.0.0.0	0

SD-WAN Usage

Bandwidth Volume Sessions

Upstream

Downstream

100%

100%

Apply

En el desplegable que se nos abre , seleccionamos el botón +VPN

New SD-WAN Member

Interface

Gateway

Cost

Status

Search

+ VPN

mgmt

dmz

ha1

ha2

Rellenamos los datos para conectarnos a la sede central

Create IPsec VPN for SD-WAN members

1 Authentication

Name: vpn a central

Remote device: IP Address Dynamic DNS

Remote IP address: [Empty field]

Outgoing Interface: ADSL (wan1) [Close]

Authentication method: Pre-shared Key Signature

Pre-shared key: [Empty field]

vpn a central: Site to Site - FortiGate (SD-WAN)

The diagram illustrates a central Data Center (represented by a blue server icon) connected to two remote sites. On the left, 'This FortiGate' (represented by a FortiGate router icon) is connected to the Data Center via a green line labeled 'VPN Tunnel'. On the right, 'Devices' (represented by a server rack icon) are also connected to the Data Center via a black line.

< Back Create Cancel

Creamos una vpn en la sede central



Es muy importante definir en la configuración del tunel IPSEC de cada sede las redes internas que se vayan a utilizar, o de lo contrario no funcionará . También se puede utilizar la 0.0.0.0/0.0.0.0 para permitir todas

Referencias

- <https://naseros.com/2017/08/03/como-configurar-el-router-de-movistar-en-modo-bridge/>
- <https://naseros.com/2020/05/19/sustitucion-hgu-movistar-y-o2-por-un-router-neutro/>

Last update:
2023/01/18 hardware:fortigate:vpn:sedeacentral <https://intrusos.info/doku.php?id=hardware:fortigate:vpn:sedeacentral&rev=1609275446>
14:38

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

Permanent link:
<https://intrusos.info/doku.php?id=hardware:fortigate:vpn:sedeacentral&rev=1609275446>

Last update: **2023/01/18 14:38**

