

ZyWALL USG-Series

Cómo configurar una conexión Site-to-site VPN entre dos ZyWALL USG series.





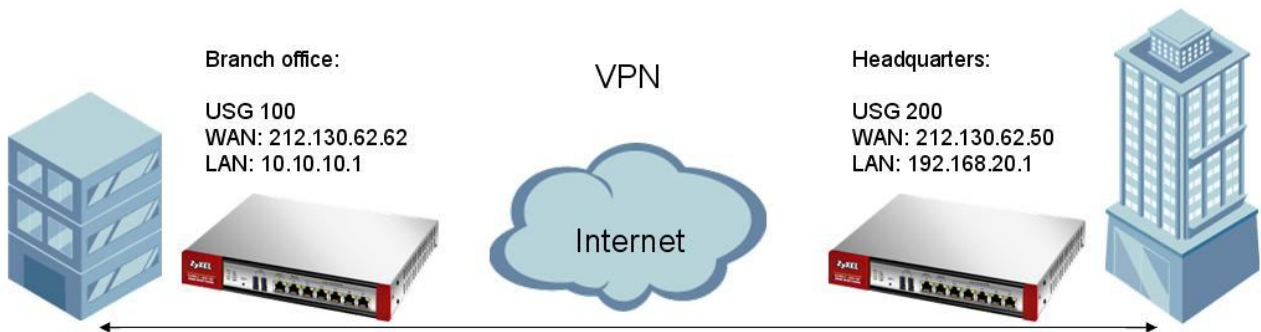
Tabla de contenidos

Introducción.....	3
ZyWALL USG 100	4
Creando el objeto de tipo Address.....	4
Creando la regla de VPN Gateway.....	4
Creando la regla de VPN Connection.....	5
ZyWALL USG 200	6
Creando el objeto de tipo Address.....	6
Creando la regla de VPN Gateway.....	6
Creando la regla de VPN Connection.....	7
Establecer la Conexión.....	7



Introducción

Esta guía indica cómo configurar una conexión site-to-site VPN basándose en la siguiente figura:



En el escenario de arriba los clientes del “Branch office” quieren tener acceso a toda la subred remota de “Headquarters” y viceversa. La configuración será la misma para cualquier modelo ZyWALL USG que esté usando. En este ejemplo vamos a utilizar un ZyWALL USG100 y un ZyWALL USG200.

Tenga en cuenta que ambos dispositivos tienen asociados en su interfaz WAN la dirección IP pública de la línea DSL de cada sede, y que el direccionamiento IP de la LAN es totalmente diferente entre sedes.

Para realizar este escenario necesita crear los siguientes objetos y reglas en ambos USG:

- Objeto de tipo Address para indicar la subred remota.
- Regla de VPN Gateway.
- Regla de VPN Connection.

Después de configurar estos tres parámetros en ambos ZyWALL USG, podrá establecer la conexión.



ZyWALL USG 100

Creando el objeto de tipo Address

Vaya al menú Configuration > Object > Address, y haga clic sobre el botón “Add”.

Ahora cree una dirección de subred que contenga el direccionamiento de subred de la LAN del ZyWALL USG opuesto como la mostrada en la siguiente figura:

The screenshot shows a dialog box titled "Add Address Rule". It contains the following fields:
Name: Headquarters_Subnet
Address Type: SUBNET (dropdown menu)
Network: 192.168.20.0
Netmask: 255.255.255.0
Buttons: OK, Cancel

Creando la regla de VPN Gateway

Vaya al menú Configuration > VPN > IPsec VPN > VPN Gateway, y haga click sobre el botón “Add”.

Habilite e indique un nombre para la regla de VPN Gateway. Rellene el campo “Interface” con la dirección IP del interfaz WAN del ZyWALL USG100.

Para la dirección IP del Peer Gateway deberá seleccionar una dirección estática, e introducir la dirección IP del interfaz WAN del ZyWALL USG200 remoto.

Necesitará introducir una contraseña como Pre-Shared Key de la conexión VPN. Ésta debe de coincidir con la configurada en el ZyWALL USG 200 remoto.

The screenshot shows a dialog box titled "Add VPN Gateway" with "Show Advanced Settings" checked. It is divided into several sections:
General Settings:
- Enable
- VPN Gateway Name: Headquartes
Gateway Settings:
My Address:
- Interface: wan1, Static -- 212.130.62.62/255.255.255.192
- Domain Name / IP
Peer Gateway Address:
- Static Address: Primary 212.130.62.50, Secondary 0.0.0.0
- Fall back to Primary Peer Gateway when possible
- Fall Back Check Interval: 300 (60-86400 seconds)
- Dynamic Address
Authentication:
- Pre-Shared Key: 12345678
- Certificate: default (See My Certificates)
Buttons: OK, Cancel



Creando la regla de VPN Connection

Vaya al menú Configuration > VPN > IPSec VPN > VPN Connection, y haga clic sobre el botón “Add”. Habilite e indique un nombre para la regla.

Seleccione “Site-to-site” como Application Scenario. Asegure que selecciona la regla de VPN Gateway correcta, en este ejemplo “Headquarters”.

Como “Local policy” seleccione la subred de la LAN del propio ZyWALL, en este caso el ZyWALL USG 100. Como “Remote policy” debe de indicar el objeto de tipo Address que creamos en el primer punto de esta guía.

Add VPN Connection

Show Advanced Settings Create new Object

General Settings

Enable

Connection Name: Headquarters_Connection

VPN Gateway

Application Scenario

Site-to-site

Site-to-site with Dynamic Peer

Remote Access (Server Role)

Remote Access (Client Role)

VPN Gateway: Headquarters wan1 212.130.62.50 0.0.0.0

Policy

Local policy: LAN1_SUBNET INTERFACE SUBNET, 10.10.10.0/24

Remote policy: Headquartes_Subnet SUBNET, 192.168.20.0/24

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Related Settings

OK Cancel

De esta forma habrá finalizado la configuración requerida en su ZyWALL USG 100.



ZyWALL USG 200

Creando el objeto de tipo Address

Vaya al menú Configuration > Object > Address, y haga clic sobre el botón “Add”.

Ahora cree una dirección de subred que contenga el direccionamiento de subred de la LAN del ZyWALL USG opuesto como la mostrada en la siguiente figura:

The screenshot shows a dialog box titled "Add Address Rule". It contains the following fields:
Name: Branch_Office_Subnet
Address Type: SUBNET (dropdown menu)
Network: 10.10.10.0
Netmask: 255.255.255.0
Buttons: OK, Cancel

Creando la regla de VPN Gateway

Vaya al menú Configuration > VPN > IPSec VPN > VPN Gateway, y haga click sobre el botón “Add”.

Habilite e indique un nombre para la regla de VPN Gateway. Rellene el campo “Interface” con la dirección IP del interfaz WAN del ZyWALL USG200.

Para la dirección IP del Peer Gateway deberá seleccionar una dirección estática, e introducir la dirección IP del interfaz WAN del ZyWALL USG100 remoto.

Necesitará introducir una contraseña como Pre-Shared Key de la conexión VPN. Ésta debe de coincidir con la configurada en el ZyWALL USG100 remoto.

The screenshot shows a dialog box titled "Add VPN Gateway" with "Show Advanced Settings" checked. It is divided into three sections:
General Settings:
- Enable:
- VPN Gateway Name: Branch_Office
Gateway Settings:
- My Address: Interface (wan1) Static -- 212.130.62.50/255.255.255.192
- Peer Gateway Address: Static Address
 - Primary: 212.130.62.62
 - Secondary: 0.0.0.0
 - Fall back to Primary Peer Gateway when possible
 - Fall Back Check Interval: 300 (60-86400 seconds)
- Dynamic Address
Authentication:
- Pre-Shared Key: 12345678
- Certificate: default (See My Certificates)
Buttons: OK, Cancel



Creando la regla de VPN Connection

Vaya al menú Configuration > VPN > IPSec VPN > VPN Connection, y haga clic sobre el botón “Add”. Habilite e indique un nombre para la regla.

Seleccione “Site-to-site” como Application Scenario. Asegure que selecciona la regla de VPN Gateway correcta, en este ejemplo “branco_Office_Subnet”.

Como “Local policy” seleccione la subred de la LAN del propio ZyWALL, en este caso el ZyWALL USG 200. Como “Remote policy” debe de indicar el objeto de tipo Address que creamos en el primer punto de esta guía.

The screenshot shows the 'Add VPN Connection' configuration window. The 'General Settings' section has 'Enable' checked and 'Connection Name' set to 'Branch_Office_Connection'. The 'VPN Gateway' section has 'Application Scenario' set to 'Site-to-site' and 'VPN Gateway' set to 'Branch_Office' with IP 'wan1 212.130.62.62 0.0.0.0'. The 'Policy' section has 'Local policy' set to 'LAN1_SUBNET' (INTERFACE SUBNET, 192.168.20.0/24) and 'Remote policy' set to 'Branch_Office_Subnet' (SUBNET, 10.10.10.0/24). The 'Phase 2 Settings' section has 'SA Life Time' set to '86400' (180 - 3000000 Seconds). The 'Related Settings' section is empty. 'OK' and 'Cancel' buttons are at the bottom right.

De esta forma habrá finalizado la configuración requerida en su ZyWALL USG 200.

Establecer la Conexión

Ambos ZyWALL USG han quedado configurados. La única cosa que falta es establecer la conexión VPN.

La conexión VPN se puede establecer manualmente seleccionando en la regla de VPN Connection y pulsando sobre el botón “Connect” desde el menú Configuration > VPN > IPSec VPN > VPN Connection.

Alternativamente puede editar la regla de VPN Connection, haga click sobre el botón “Show Advance Settings” y habilite el Nailed-Up. Teniendo la opción Nailed-Up habilitada el túnel VPN se conectará automáticamente cuando el ZyWALL USG se inicie.

Todos los dispositivos de la “Branch Office” ahora serán capaces de acceder a los dispositivos de red y computadoras de la subred “Headquarters” y viceversa.