

ZyWALL USG-Series

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



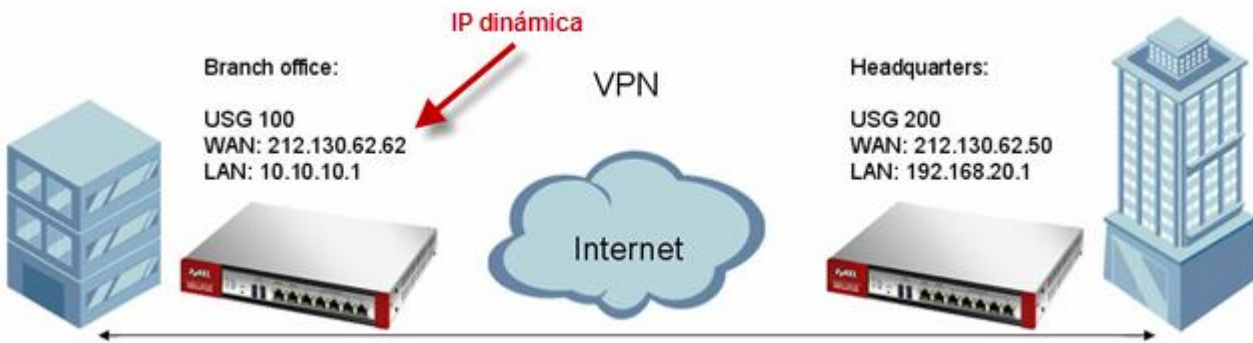


Tabla de contenido

Introducción.....	3
ZyWALL USG 100	4
Creando los objetos de tipo address.....	4
Creando la regla de VPN Gateway.....	4
Creando la regla de VPN Connection.....	5
ZyWALL USG 200	6
Creando los objetos 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 explica cómo configurar una conexión Site-to-site VPN con peer dinámico como la mostrada en la siguiente figura:



En el escenario superior los clientes de la sede “Branch office” quieren tener acceso a toda la subred de la sede “Headquarters” y viceversa.

La configuración será la misma independientemente del modelo de ZyWALL USG que esté usando. En este ejemplo haremos uso de un ZyWALL USG100 y de un ZyWALL USG200.

Para realizar este escenario se necesita configurar los siguientes parámetros en ambos ZyWALL USG:

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

Después de configurar estos tres parámetros en ambos ZyWALL USG, tendrá establecida la conexión.





ZyWALL USG 100

Creando los objetos de tipo address

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

Ahora cree una dirección de subred que contenga la subred de la LAN del ZyWALL USG remoto tal y como se indica en la siguiente figura:

The screenshot shows the 'Add Address Rule' dialog box with the following fields:

- Name: Headquarters_Subnet
- Address Type: SUBNET
- 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”.

Debe de asegurar que la regla esté habilitada. Rellene el campo “Interface” seleccionando el interfaz WAN del ZyWALL USG 100 que utilizará para establecer la VPN.

Para el “Peer Gateway Address” deberá de elegir “Static Address” e indicar la dirección IP del interfaz WAN del ZyWALL USG200 en el campo “Primary”.

Además deberá de introducir una clave en el campo “Pre-Shared Key” para la conexión VPN. Esta clave debe de ser la misma que la que se configure en el ZyWALL USG 200.

The screenshot shows the 'Add VPN Gateway' dialog box with the following settings:

- 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
 - Dynamic Address
 - Fall back to Primary Peer Gateway when possible
 - Fall Back Check Interval: 300 (60-86400 seconds)
- 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 click sobre el botón “Add”.

Debe de asegurar que la regla esté habilitada. Bajo el parámetro “Application Scenario” seleccione “Site-to-site”. Asegure que selecciona la regla de VPN Gateway correcta, en este ejemplo la denominada “Headquarters”.

Como Local policy seleccione el objeto LAN1_SUBNET correspondiente al ZyWALL USG 100, y como Remote policy seleccione el objeto de tipo Address que hemos creado en el primer punto de configuración, y que corresponde con la subred remota del ZyWALL USG 200.

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

Una vez realizado habrá finalizado la configuración requerida en su ZyWALL USG 100.



ZyWALL USG 200

Creando los objetos de tipo address

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

Ahora cree una dirección de subred que contenga la subred de la LAN del ZyWALL USG remoto tal y como se indica 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”.

Debe de asegurar que la regla esté habilitada. Rellene el campo “Interface” seleccionando el interfaz WAN del ZyWALL USG 200 que utilizará para establecer la VPN.

Para el “Peer Gateway Address” deberá de elegir “Dynamic Address”, ya que la dirección IP pública del interfaz WAN del ZyWALL USG 100 es dinámica y cambiante.

Además deberá de introducir una clave en el campo “Pre-Shared Key” para la conexión VPN. Esta clave debe de ser la misma que la que se configure en el ZyWALL USG 100.

The screenshot shows a dialog box titled "Add VPN Gateway" with a "Show Advanced Settings" button. 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
- Domain Name / IP:
- Peer Gateway Address: Static Address (Primary: 0.0.0.0, 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 click sobre el botón “Add”.

Debe de asegurar que la regla esté habilitada. Bajo el parámetro “Application Scenario” seleccione “Remote Access (Server Role)”. Asegure que selecciona la regla de VPN Gateway correcta, en este ejemplo la denominada “Branch_Office”.

Como Local policy seleccione el objeto LAN1_SUBNET correspondiente al ZyWALL USG 200, y como Remote policy seleccione el objeto de tipo Address que hemos creado en el primer punto de configuración, y que corresponde con la subred remota del ZyWALL USG 100.

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

Una vez realizado 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 se lanzará manualmente desde la sede con IP dinámica seleccionando la regla de VPN Connection y haciendo click sobre el botón “Connect” dentro del menú Configuration > VPN > IPSec VPN > VPN Connection.

Alternativamente se puede editar la regla de VPN Connection, y mostrando la configuración avanzada haciendo click sobre el botón “Show Advanced Settings” podremos habilitar la opción “Nailed-Up”. Con el Nailed-Up habilitado el túnel VPN se conectará automáticamente una vez que el ZyWALL USG se inicie.

Todos los dispositivos de la sede “Branch Office” tendrá acceso a los dispositivos de red de la sede “Headquarters” y viceversa.





```
c:\ Prompt
Configurazione IP di Windows

Scheda Ethernet LAN:

    Suffisso DNS specifico per connessione:
    Indirizzo IP . . . . . : 192.168.20.33
    Subnet mas . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.20.1

C:\Documents and Settings\l.lobue>ping 192.168.10.1

Esecuzione di Ping 192.168.10.1 con 32 byte di dati:

Risposta da 192.168.10.1: byte=32 durata=3ms TTL=62
Risposta da 192.168.10.1: byte=32 durata=2ms TTL=62
Risposta da 192.168.10.1: byte=32 durata=2ms TTL=62
Risposta da 192.168.10.1: byte=32 durata=2ms TTL=62

Statistiche Ping per 192.168.10.1:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 2ms, Massimo = 3ms, Medio = 2ms
```

