



# ZyWALL USG-Series

---

Cómo configurar un One-to-One NAT





## Tabla de contenidos

Escenario.....	3
Inicio con objetos de tipo Address.....	4
Crear la regla de NAT.....	5
Crear la regla de Firewall.....	6



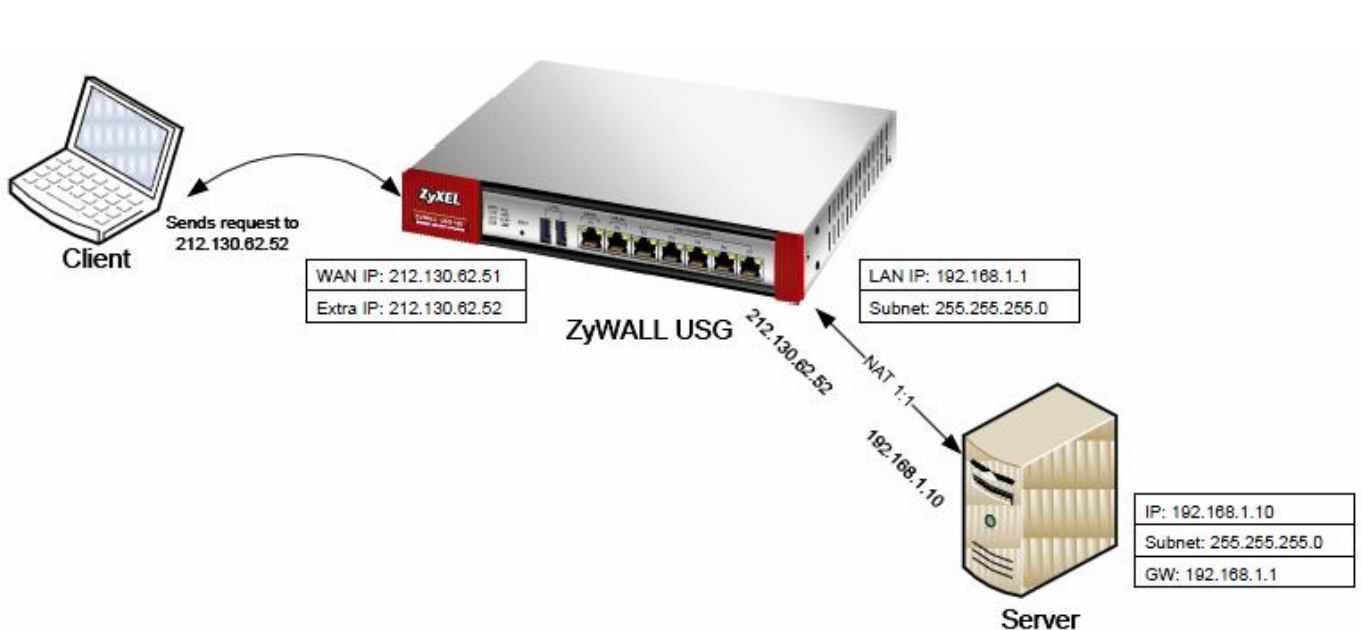


## Escenario

Esta guía describe cómo configurar 1:1 NAT en los equipos ZyWALL USG Series.

Los dispositivos ZyWALL USG pueden disponer de un pool de IPs públicas asociado sobre un mismo interfaz WAN. (Depende del tipo de líneas contratadas con el ISP)

En este ejemplo haciendo uso de la funcionalidad 1:1 NAT todas las peticiones que un cliente hace a través de Internet hacia la dirección IP 212.130.62.52 serán enviadas directamente al cliente interno asociado al 1:1 NAT, en este caso el servidor 192.168.1.10.



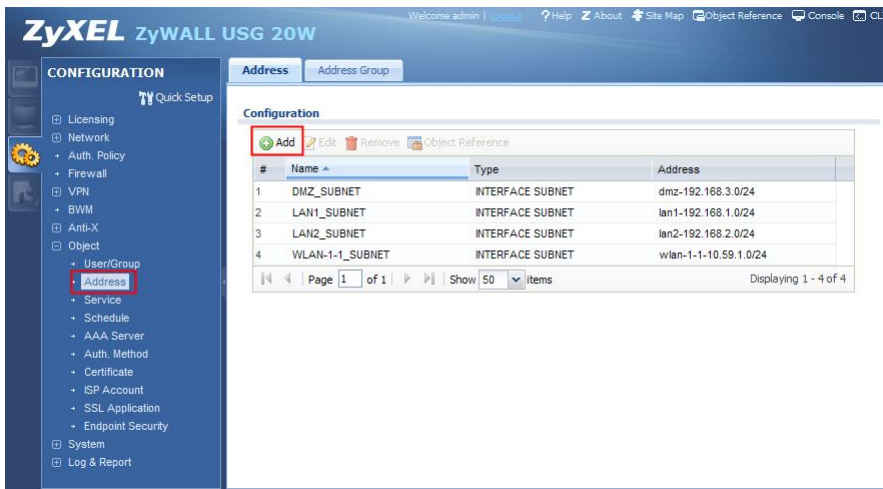


## Inicio con objetos de tipo address

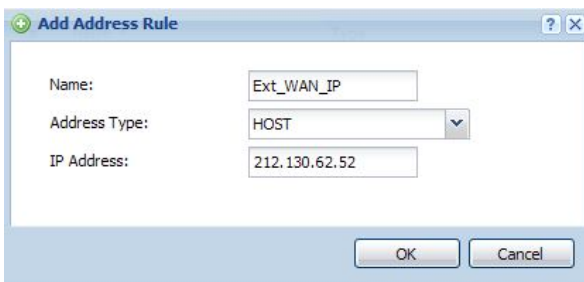
Para crear una regla de NAT One-to-One el camino más fácil es empezando a crear los objetos de tipo address.

En esta guía crearemos dos objetos, uno para indicar la dirección IP de la WAN secundaria, y otro para indicar la dirección IP del servidor interno.

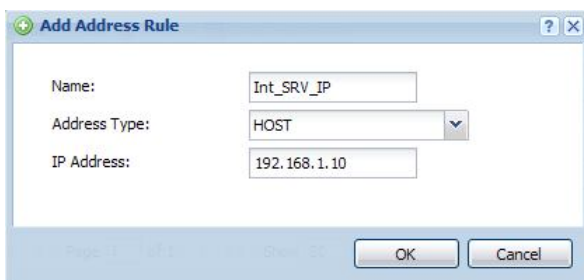
Para crear un objeto de tipo address nos vamos al menú Configuration > Object > Address. Hacemos clic sobre el botón "Add".



Indicaremos un nombre a la regla (Ext\_WAN\_IP), y seleccionaremos "HOST" como Address Type. Introduciremos manualmente la dirección IP de la WAN secundaria.



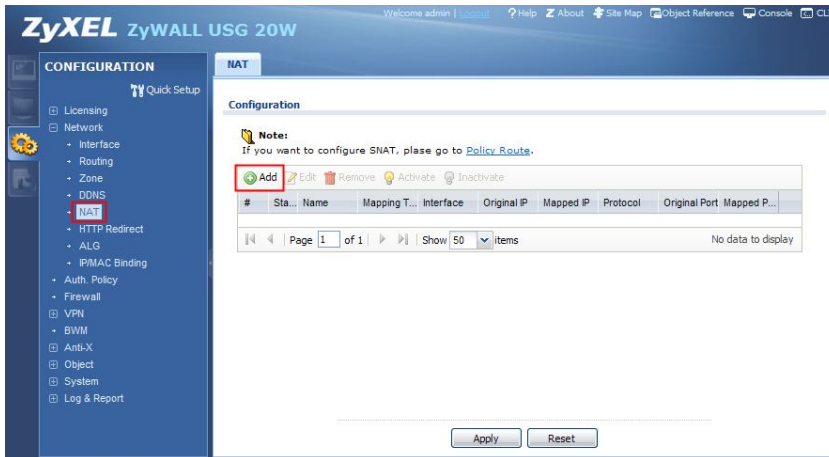
Utilice los mismos pasos para añadir el objeto de tipo Host con la IP del servidor interno:





## Crear la regla de NAT

Para crear la regla de NAT nos vamos al menú Configuration > Network > NAT, y hacemos click sobre el botón "Add".

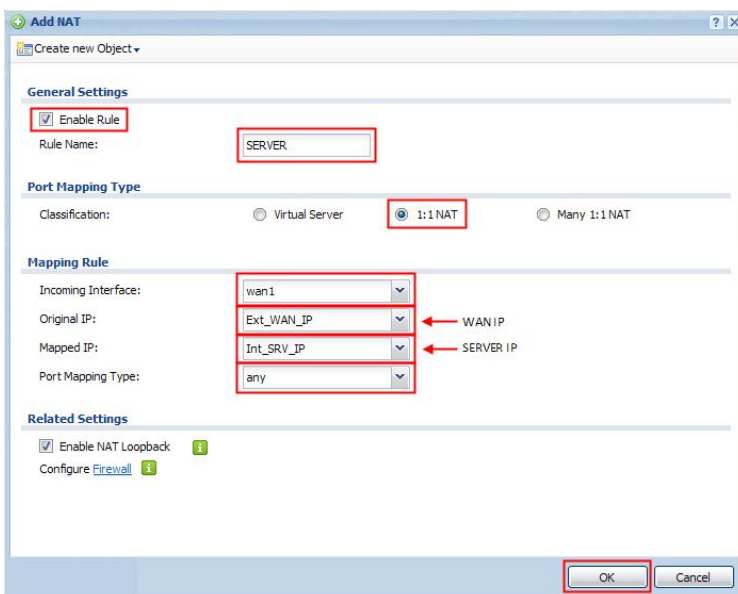


Habilitamos la regla, introducimos un nombre (SERVER) y seleccionamos 1:1 NAT.

Seleccionamos el incoming interface (normalmente WAN1 o ge2).

Seleccionamos el objeto creado anteriormente "Ext\_WAN\_IP" como Original IP, y seleccionamos el objeto "Int\_SRV\_IP" como Mapped IP. Configuramos el Port Mapping Type como "Any".

Hacemos click sobre el botón OK.



Nota: Se puede activar NAT Loopback para que los clientes internos puedan contactar con el servidor a través de su IP pública.

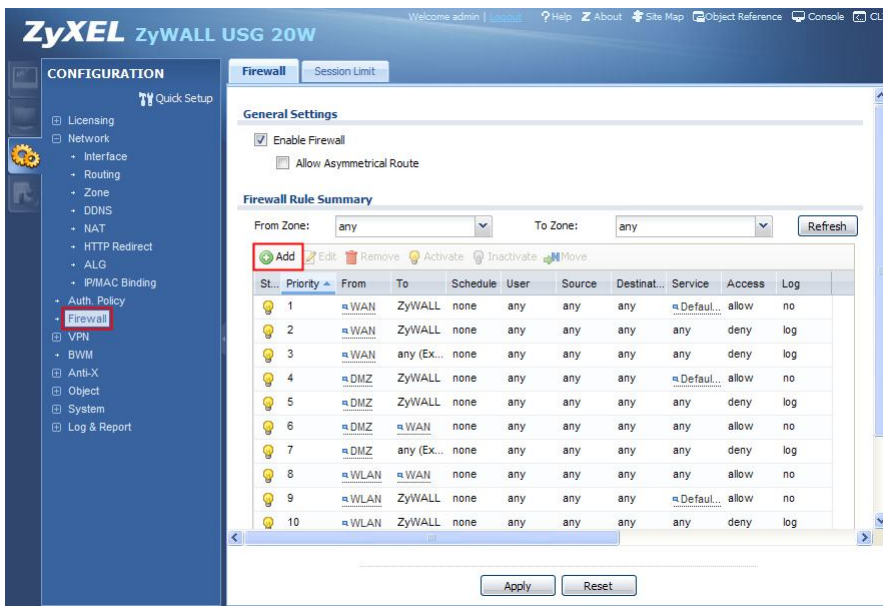




## Crear la regla de Firewall

Como paso final necesitamos crear una regla de Firewall para permitir el paso del tráfico hacia el servidor.

Para ello vamos al menú Configuration > Firewall, y hacemos click sobre el botón “Add”.



Seleccionamos el sentido del flujo de tráfico from WAN to LAN1. Seleccionamos el objeto “Int\_SRV\_IP” que contiene la IP del servidor interno en el campo Destination.

Seleccionamos el servicio o grupo de servicios preferido. En este caso se ha seleccionado HTTP.

Seleccionamos el campo Access como “Allow”. Habilitamos los Logs opcionalmente y hacemos click sobre el botón OK.

