

# Creación de VPN dinámica entre un ZyWALL USG y el software cliente VPN IPSec

1. En el USG empezamos a configurar la regla IPSec VPN accediendo al menú VPN Gateway y añadimos una nueva regla.

Hay que definir un nombre para la regla VPN, elegir en el campo My Address el interfaz WAN de salida que nos da acceso a Internet. Y como Peer seleccionar Dynamic Address.

The screenshot shows the ZyWALL VPN Gateway configuration page. The breadcrumb trail is "ZyWALL > VPN > IPSec VPN > VPN Gateway > Edit > #2". The "General Settings" section has "VPN Gateway Name" set to "Cliente". The "Gateway Settings" section has "My Address" set to "Interface" (wan1) with a "Static" address of "192.168.0.2/255.255.255.0". A red arrow points to this address. Below it, "Peer Gateway Address" is set to "Dynamic Address". A red text box on the right says: "En el mejor de los casos tendremos el router configurado en modo monopuesto. Y aquí se mostraría la IP pública contratada."

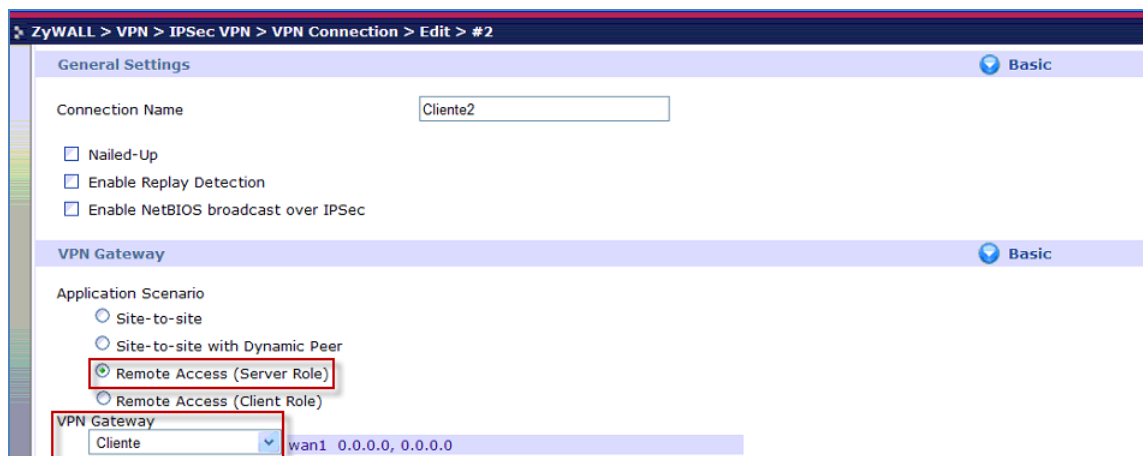
2. Definiremos una contraseña en el campo Pre-Shared Key, y definiremos los parámetros de autenticación y encriptación para la Fase1. Dejaremos marcada la casilla NAT Transversal para evitar problemas de NAT. Finalmente aceptamos y guardamos los cambios.

The screenshot shows the ZyWALL VPN Gateway configuration page, "Authentication" and "Phase 1 Settings" sections. The breadcrumb trail is "ZyWALL > VPN > IPSec VPN > VPN Gateway > Edit > #2". The "Authentication" section has "Pre-Shared Key" set to "1234567890". "Local ID Type" is "IP" with "Content" "1.1.1.1". "Peer ID Type" is "IP" with "Content" "2.2.2.2". The "Phase 1 Settings" section has "SA Life Time" set to "86400" (180 - 3000000 Seconds). "Negotiation Mode" is "Main". The "Proposal" table has "Encryption" set to "DES" and "Authentication" set to "MD5". The "Key Group" is "DH1". The "NAT Traversal" checkbox is checked. The "Dead Peer Detection (DPD)" checkbox is also checked.

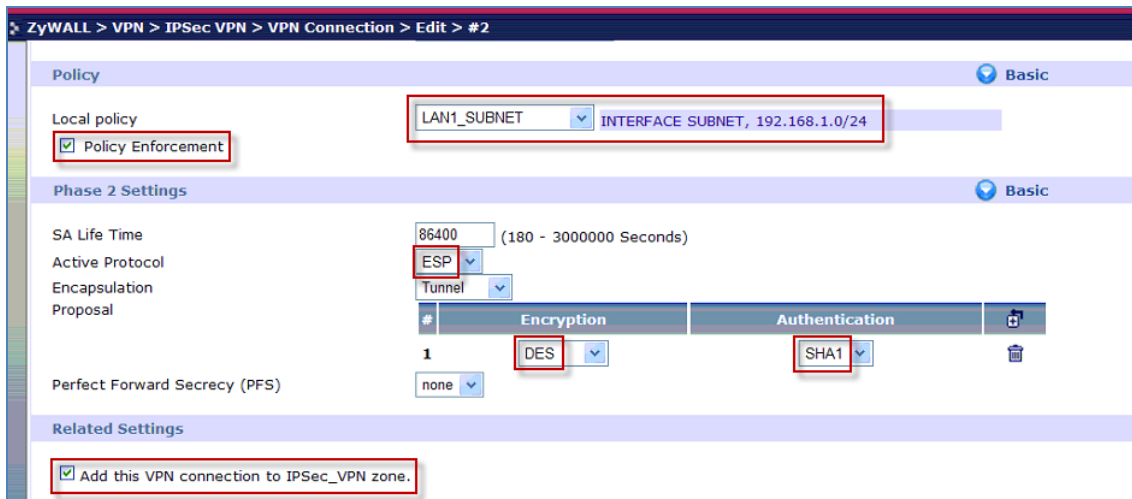
- Ahora pasamos a configurar la pestaña VPN Connection, donde nos aseguraremos que no tenemos marcadas las dos casillas de la parte superior.



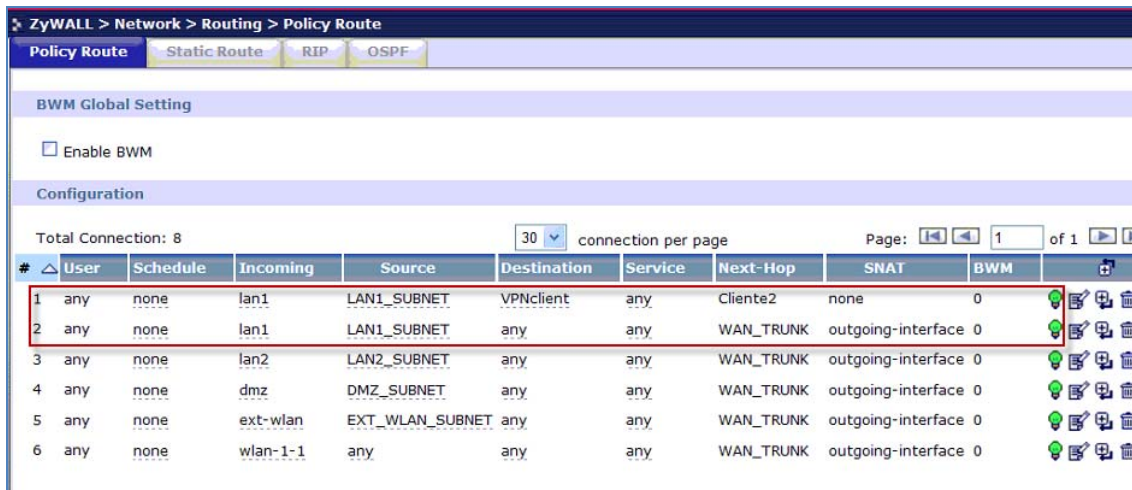
- En el campo Application Scenario seleccionamos Remote Access (Server Role), para que de esa forma se pueda conectar cualquier cliente VPN IPsec dinámico. En el campo VPN Gateway seleccionaremos la regla VPN que creamos en el punto 1.



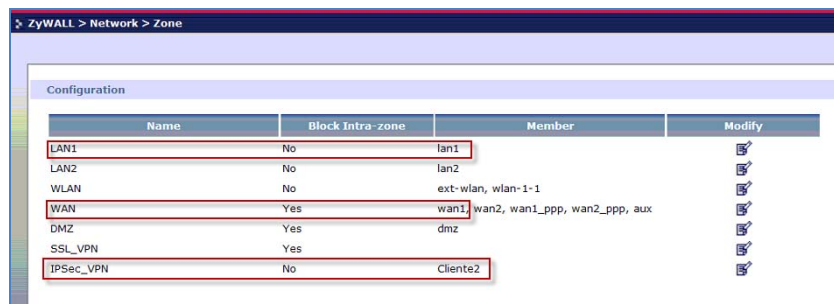
- En el campo Policy seleccionaremos el objeto de tipo address con la información de las IPs que queremos sean accesibles desde el software cliente VPN. En este ejemplo es el objeto LAN1\_SUBNET que engloba a toda la LAN1, pero se podría haber creado un objeto con un rango de IPs de la LAN1. Dejamos marcada la casilla Policy Enforcement, y seleccionamos los parámetros de autenticación y encriptación pertenecientes a la Fase2. Dejamos marcada la casilla "add this VPN Connection to IPSEC\_VPN zone", aplicamos y guardamos los cambios.



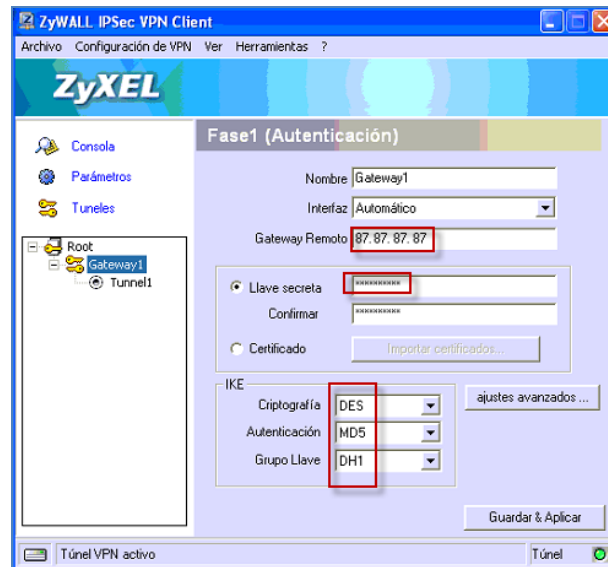
6. Entramos dentro del menú **Network > Routing > Policy Route**. Por defecto aparece la regla con origen LAN1\_SUBNET con destino any usando como Next-Hop el interface WAN\_TRUNK. Añadiremos una nueva regla, que la colocaremos en primer lugar, seleccionando como **Incoming** el interfaz lan1, y como origen el objeto LAN1\_SUBNET, destino un objeto de tipo address con la información Host con IP 0.0.0.0, y como **Next-Hop** seleccionamos VPN y el nombre de la VPN que hemos creado en los puntos anteriores.



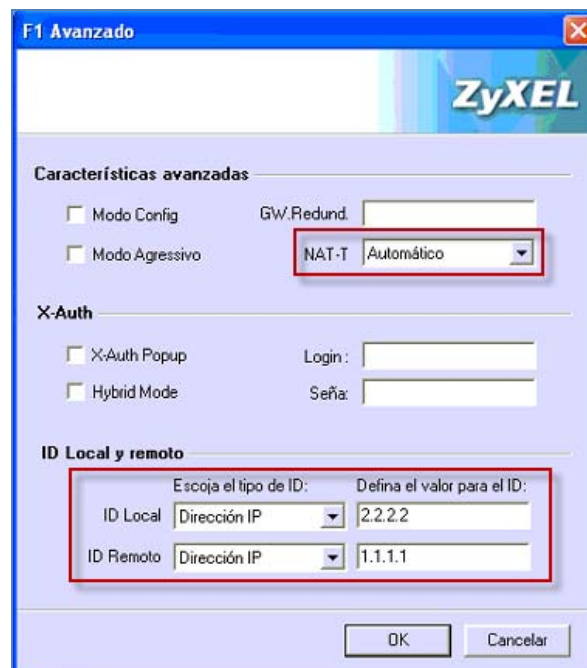
7. Entramos en **Network > Zone** y verificamos la configuración:



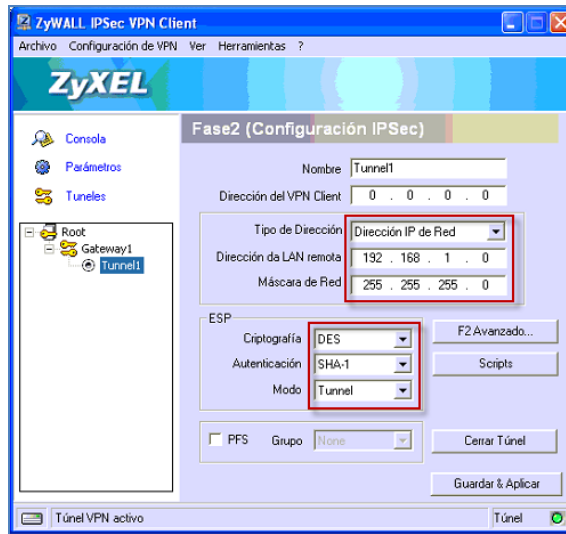
8. Una vez configurado el ZyWALL USG pasamos a configurar el software cliente VPN. Creamos una nueva configuración, y definimos como Gateway Remoto la dirección IP pública de la WAN del USG. Introducimos la misma Pre-Shared Key, y parámetros de autenticación y encriptación configurados en el USG, y guardamos los cambios.



9. En la misma ventana, pulsamos sobre “ajustes avanzados” y seleccionamos el NAT-T como automático, e introducimos los mismos ID local y remoto que se configuraron en el USG (a tener en cuenta que se colocan al revés).



10. Añadimos una Fase2, y seleccionamos la subred del ZyWALL USG, así como los parámetros de autenticación y encriptación.



11. La configuración VPN ya estaría finalizada, y ya se tendría conectividad entre el PC con el software cliente VPN instalado. Si se accede al USG, dentro del menú VPN > IPsec VPN > SA Monitor se puede ver el túnel establecido, las IPs del equipo local y remoto, así como el tráfico entrante y saliente.

