

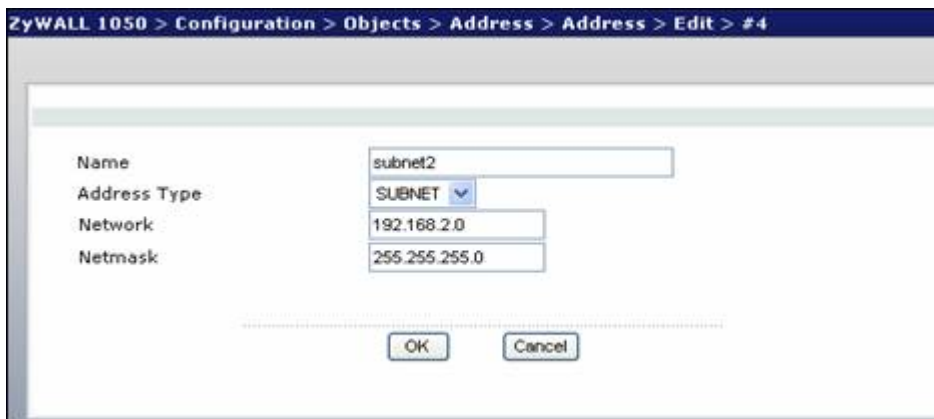
Configuración VPN entre un ZyWALL 1050 y el ZyWALL VPN Client:

Este cuadro es un resumen de la configuración que vamos a realizar en ambos extremos:

ZyWALL 1050	ZyWALL VPN Client
My address: ge2(10.59.1.45) Secure gateway address: 0.0.0.0 Local: 192.168.2.0/24 Remote: 0.0.0.0/24	My address: Any Secure gateway address: 10.59.1.45 Local: Any Remote: 192.168.2.0/24
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1
Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None	Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None

Sigue paso a paso la siguiente configuración:

- 1) Logéate en el interfaz GUI del ZyWALL 1050 GUI y dirígete a **Configuration > Objects > Address** para crear un objeto de tipo "address" (local subnet) para acceso remoto.



The screenshot shows the ZyWALL 1050 GUI configuration page for creating a new address object. The breadcrumb navigation at the top reads "ZyWALL 1050 > Configuration > Objects > Address > Address > Edit > #4". The form contains the following fields:

Name	subnet2
Address Type	SUBNET
Network	192.168.2.0
Netmask	255.255.255.0

At the bottom of the form are two buttons: "OK" and "Cancel".

- 2) Crea otro objeto de tipo "address" para el host remote. La **Dirección IP Address** del host debe ser **0.0.0.0**, de esta forma el usuario remote se conectará dinámicamente.



The screenshot shows the ZyWALL 1050 GUI configuration page for creating a new address object. The breadcrumb navigation at the top reads "ZyWALL 1050 > Configuration > Objects > Address > Address > Edit > #4". The form contains the following fields:

Name	VPNclient
Address Type	HOST
IP Address	0.0.0.0

At the bottom of the form are two buttons: "OK" and "Cancel".

- 3) Dirígete a **Configuration > Network > IPSec VPN > VPN Gateway** para crear el gateway para el cliente VPN remote. Debido a que este tipo de VPN se inicia desde el usuario remoto, el **Secure Gateway** debe ser configurado como dinámico, 0.0.0.0. También, los VPN remotos deben de guardar coherencia entre ellos en cuanto a los parámetros, tales como Pre-Shared Key, ID Type, propuesta de "Encryption" y propuesta de "Authentication", etc ...

VPN Gateway Name	remoteaccess								
IKE Phase 1									
Negotiation Mode	Main								
Proposal	<table border="1"><thead><tr><th>#</th><th>Encryption</th><th>Authentication</th><th></th></tr></thead><tbody><tr><td>1</td><td>DES</td><td>MD5</td><td></td></tr></tbody></table>	#	Encryption	Authentication		1	DES	MD5	
#	Encryption	Authentication							
1	DES	MD5							
Key Group	DH1								
SA Life Time (Seconds)	86400 <180 - 3000000>								
<input type="checkbox"/> NAT Traversal									
<input checked="" type="checkbox"/> Dead Peer Detection (DPD)									
Property									
My Address	<input checked="" type="radio"/> Interface: ge2 DHCP client -- 10.59.1.45/255.255.255.0								
<input type="radio"/> Domain Name									
Secure Gateway Address	1. 0.0.0.0 2. 0.0.0.0								
Authentication Method									
<input checked="" type="radio"/> Pre-Shared Key	123456789								
<input type="radio"/> Certificate	(See My Certificates)								
Local ID Type	IP								
Content	0.0.0.0								
Peer ID Type	Any								
Content									
Extended Authentication									
<input type="checkbox"/> Enable Extended Authentication									
age	Ready								

- 4) Para crear la regla VPN, dirígete a **Configuration > Network > IPsec VPN > VPN Connection**. Configura la **Policy** como se definió en el paso 1 y paso 2. La política remota debe ser una dirección de host dinámica. Hemos configurado la **VPN Gateway** como dinámica como se definió en el paso 3.

VPN Connection

Connection Name: remoteaccess

VPN Gateway

Name: remoteaccess (Add New VPN Gateway)
ge2 remoteaccess

Phase 2

Active Protocol: ESP
Encapsulation: Tunnel
Proposal:

#	Encryption	Authentication	
1	DES	MD5	

SA Life Time (Seconds): 86400 (180 - 3000000)
Perfect Forward Secrecy (PFS): none

Policy

Policy Enforcement

Local policy: subnet2 (SUBNET, 192.168.2.0/24)
Remote policy: VPNclient (HOST, 0.0.0.0)

Property

Nailed-Up
 Enable Replay Detection
 Enable NetBIOS broadcast over IPsec

Advanced ...

Inbound/Outbound traffic NAT

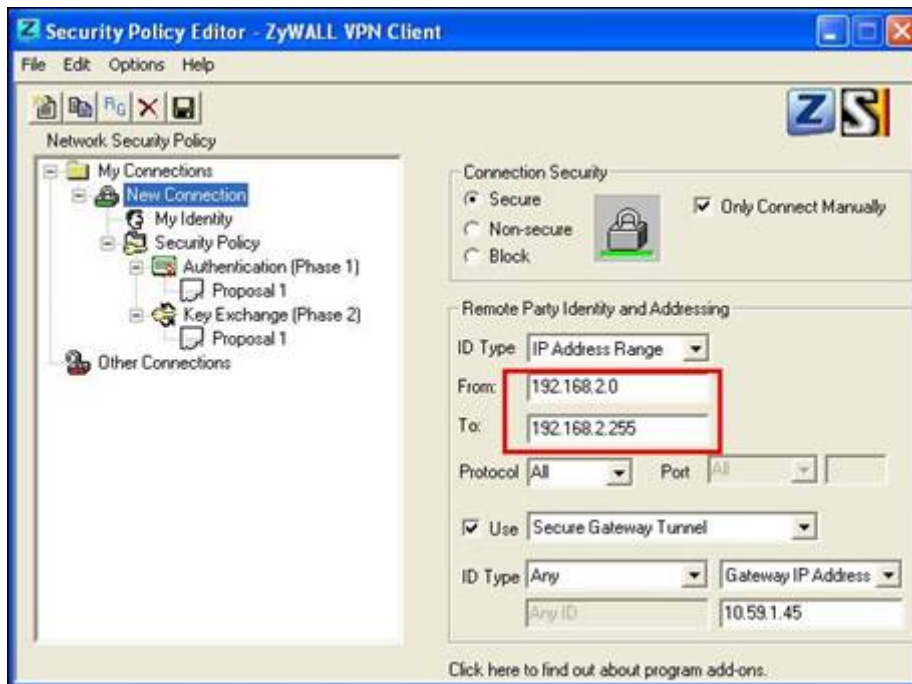
Outbound Traffic

Source NAT

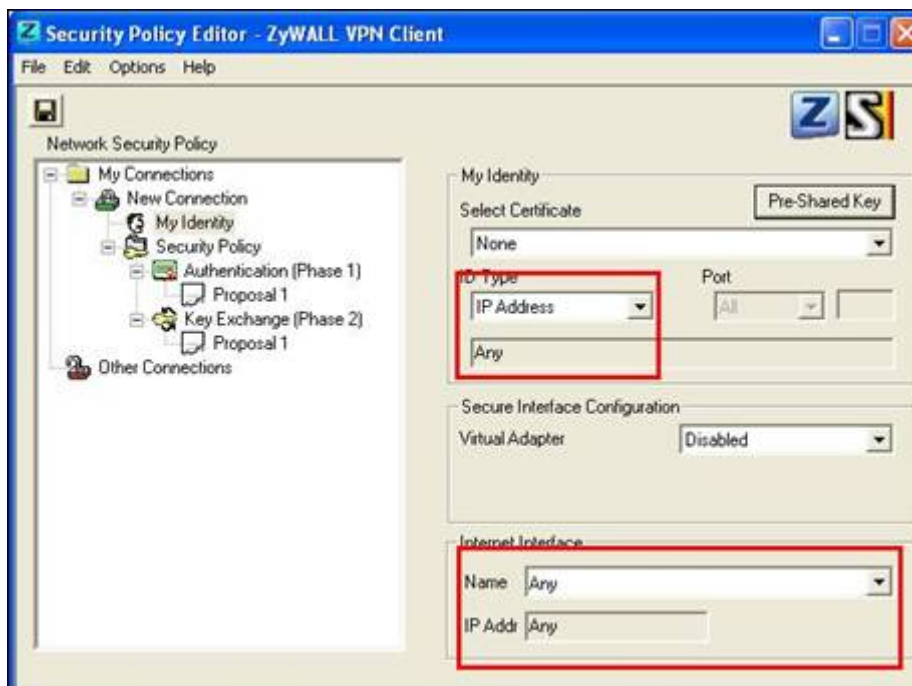
Source: [dropdown]
Destination: [dropdown]

Page: **Ready.**

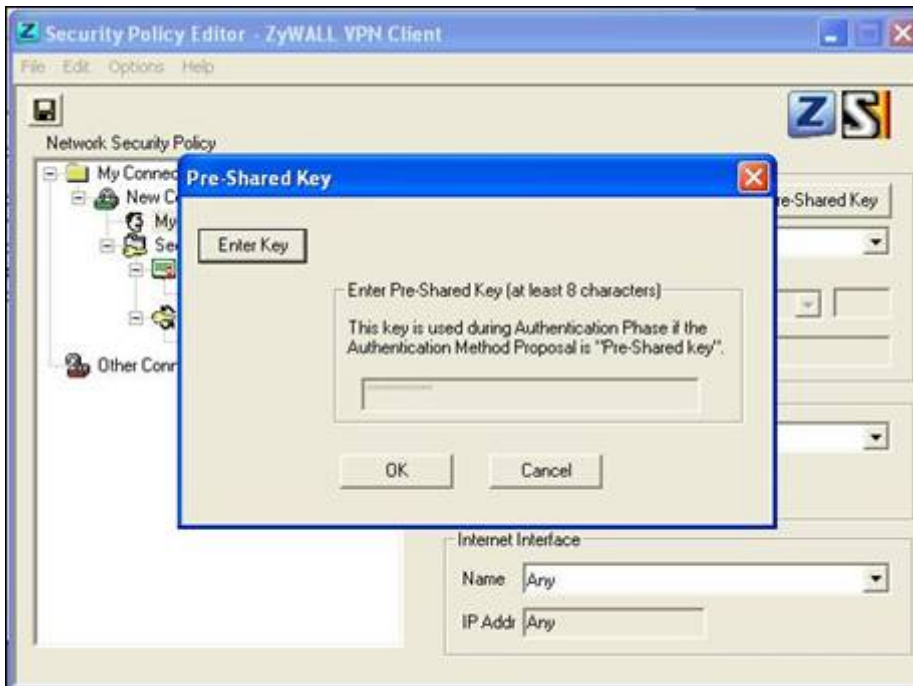
- 5) En el Host Remoto configure el ZyXEL VPN Client. Crearemos una **New Connection** para configurar el acceso a la subnet remota 192.168.2.x



En el apartado **My Identity**, hay que seleccionar el local ID type como Any.



Nota: No se olvide de introducir la Pre-Shared Key pulsando el botón **Pre-Shared Key**.



El último paso que queda es dirigirse al **Security Policy** para configurar los parámetros para la Phase1 y Phase 2. Después de guardar la configuración, la conexión VPN debe ser inicializada desde el host.

