

# Conexión VPN remota

- Software de conexión VPN vs Dispositivo ZyXEL

# Introducción

- En este documento se verá cómo configurar los clientes de software de ZyXEL, ZyWALL IPSec VPN Client y ZyWALL Remote Security Client frente a un dispositivo ZyXEL con soporte de VPN.
- Los datos de la oficina serán:
  - IP pública de acceso: 88.88.88.88
  - Red local: 192.168.1.0/24
- La dirección IP del cliente será cualquiera (independientemente de si está en casa, en un hotel...)

**ZyWALL**

# VPN – ZyWALL –

VPN

VPN Rules (IKE) | VPN Rules (Manual) | SA Monitor | Global Setting

VPN Rules

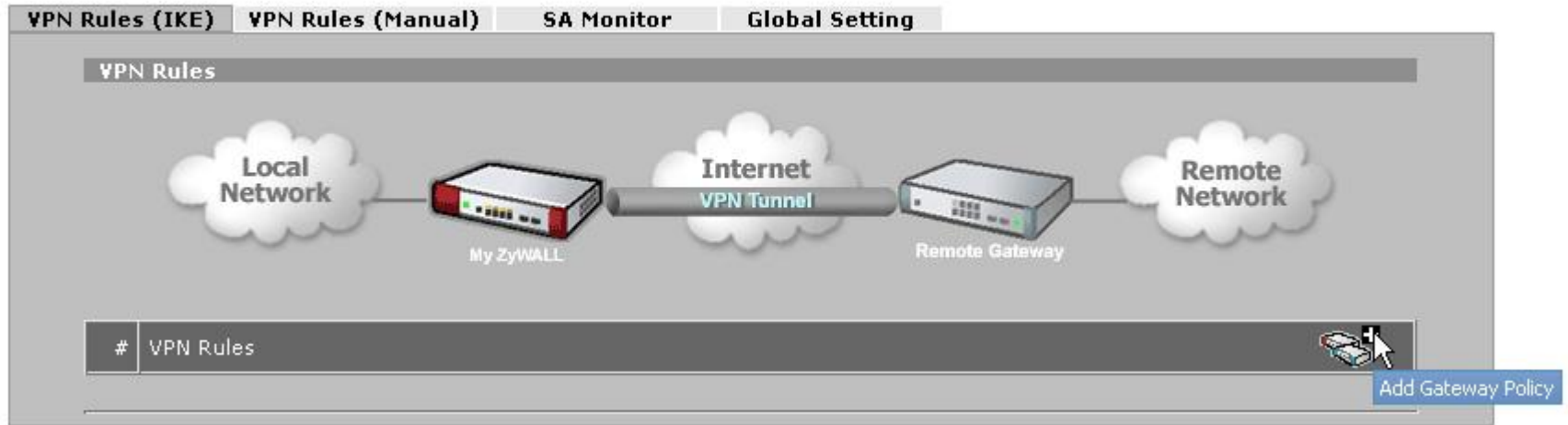
Local Network — My ZyWALL — Internet VPN Tunnel — Remote Gateway — Remote Network

#	VPN Rules

- **Seleccione en el ZyWALL la pestaña de configuración VPNs**

# VPN – ZyWALL –

## VPN



- **Añada una política de gateway**

# VPN – ZyWALL –


## VPN - GATEWAY POLICY - EDIT

**Property**

Name


NAT Traversal

**Gateway Policy Information**


 My ZyWALL

My Address  (Domain Name or IP Address)

My Domain Name  (See [DDNS](#))

 Primary Remote Gateway  (Domain Name or IP Address)

Enable IPsec High Availability

 Redundant Remote Gateway  (Domain Name or IP Address)

Fall back to Primary Remote Gateway when possible

Fall Back Check Interval\*  (180~86400 seconds)

\*Fall Back Check Interval: The time interval for checking availability of Primary Remote Gateway. IPsec SA life time will be superseded by this value when it is larger than this value.

- **Nómbrela y configure como dinámicas todas las IPs:**

- My Address: 0.0.0.0 para que salga por cualquiera de las interfaces, en caso de querer forzar una de ellas se debe poner la IP de la interfaz WAN en ella
- Primary Remote Gateway: **0.0.0.0** para que acepte conexiones desde cualquier ubicación, este paso es FUNDAMENTAL

# VPN – ZyWALL –

**Authentication Key**

Pre-Shared Key      123456789  
 Certificate      auto\_generated\_self\_signed\_cert (See [My Certificates](#))

Local ID Type      DNS  
Content      MainOffice

Peer ID Type      IP  
Content      0.0.0.0

**Extended Authentication**

Enable Extended Authentication (Search [Local User](#) first then [RADIUS](#))

Server Mode  
 Client Mode

User Name        
Password     

**IKE Proposal**

Negotiation Mode      Main  
Encryption Algorithm      DES  
Authentication Algorithm      MD5  
SA Life Time (Seconds)      28800  
Key Group      DH1

Enable Multiple Proposals

**Associated Network Policies**

#	Name	Local Network	Remote Network

Apply      Cancel

- **Preshared Key:**
  - 123456789
- **Local ID:**
  - DNS:MainOffice
- **Remote ID:**
  - IP:0.0.0.0
- **Parámetros IKE:**
  - Main/DES/MD5/28800/DH1
- **Se pulsa en Apply**

# VPN – ZyWALL –

## VPN

The screenshot displays the ZyWALL VPN configuration interface. At the top, there are four tabs: "VPN Rules (IKE)", "VPN Rules (Manual)", "SA Monitor", and "Global Setting". The "VPN Rules (Manual)" tab is selected. Below the tabs, a diagram illustrates the VPN setup: a "Local Network" cloud is connected to a "My ZyWALL" router, which is connected to an "Internet VPN Tunnel" cloud, which is connected to a "Remote Gateway" router, which is finally connected to a "Remote Network" cloud. Below the diagram is a table of VPN rules.

#	VPN Rules				
1	RoadWarriors	0.0.0.0	Dynamic		

At the bottom right of the interface, there is a blue button labeled "Add Network Policy".

- **Se añade ahora una política que identifique las red a la que se conectarán los clientes remotos**

# VPN – ZyWALL –

## VPN - NETWORK POLICY - EDIT

**Property**

Active

Name

Protocol

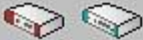
Nailed-Up

Allow NetBIOS broadcast Traffic Through IPSec Tunnel

Check IPSec Tunnel Connectivity  Log

Ping this Address

**Gateway Policy Information**

 Gateway Policy

- **Configure un nombre a la regla de redes locales a emplear**

# VPN – ZyWALL –

The screenshot shows the ZyWALL VPN configuration interface with three main sections:

- Local Network:** Address Type is set to Subnet Address. Starting IP Address is 192.168.1.0, Ending IP Address / Subnet Mask is 255.255.255.0, and Local Port is 0.
- Remote Network:** Address Type is set to Single Address. Starting IP Address is 0.0.0.0, Ending IP Address / Subnet Mask is 0.0.0.0, and Remote Port is 0.
- IPsec Proposal:** Encapsulation Mode is Tunnel, Active Protocol is ESP, Encryption Algorithm is DES, Authentication Algorithm is SHA1, SA Life Time (Seconds) is 28800, and Perfect Forward Secrecy (PFS) is NONE. There are checkboxes for Enable Replay Detection and Enable Multiple Proposals, both of which are unchecked.

Buttons for Apply and Cancel are visible at the bottom of the configuration area.

## ■ Red local:

- Configure el rango de direcciones/subred o una sola dirección a las que desea acceder desde remoto (**ponga aquí su subred / rango / dirección IP local**)

## ■ Red remota:

- Configúrela como dirección IP (**Single address**), para que espere sólo una dirección IP y con **0.0.0.0** para que permita cualquier IP

## ■ Parámetros IKE:

- Tunnel/ESP/DES/SHA1/28800/NONE

# VPN – ZyWALL –

## VPN

VPN Rules (IKE) | VPN Rules (Manual) | SA Monitor | Global Setting

VPN Rules

Local Network — My ZyWALL — Internet VPN Tunnel — Remote Gateway — Remote Network

#	VPN Rules				
1	RoadWarriors	0.0.0.0	Dynamic		
	OfficeNet	192.168.1.0 / 255.255.255.0	Any		

- Resumen de la configuración VPN con los parámetros requeridos

# Software Cliente

- ZyWALL Remote Security Client
- ZyWALL IPSec VPN Client

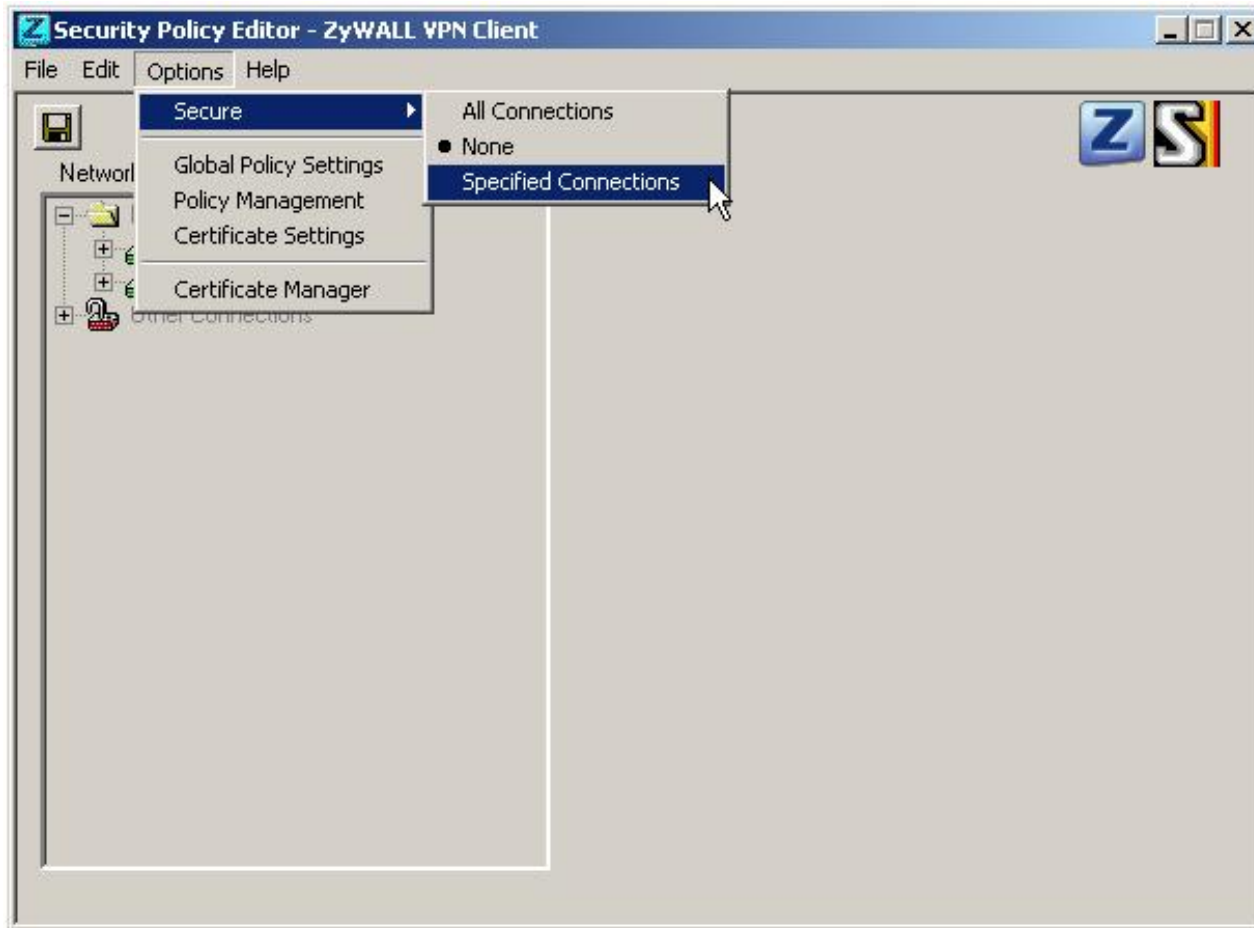
# ZyWALL Remote Security Client

# VPN – ZyWALL Remote Security Client –



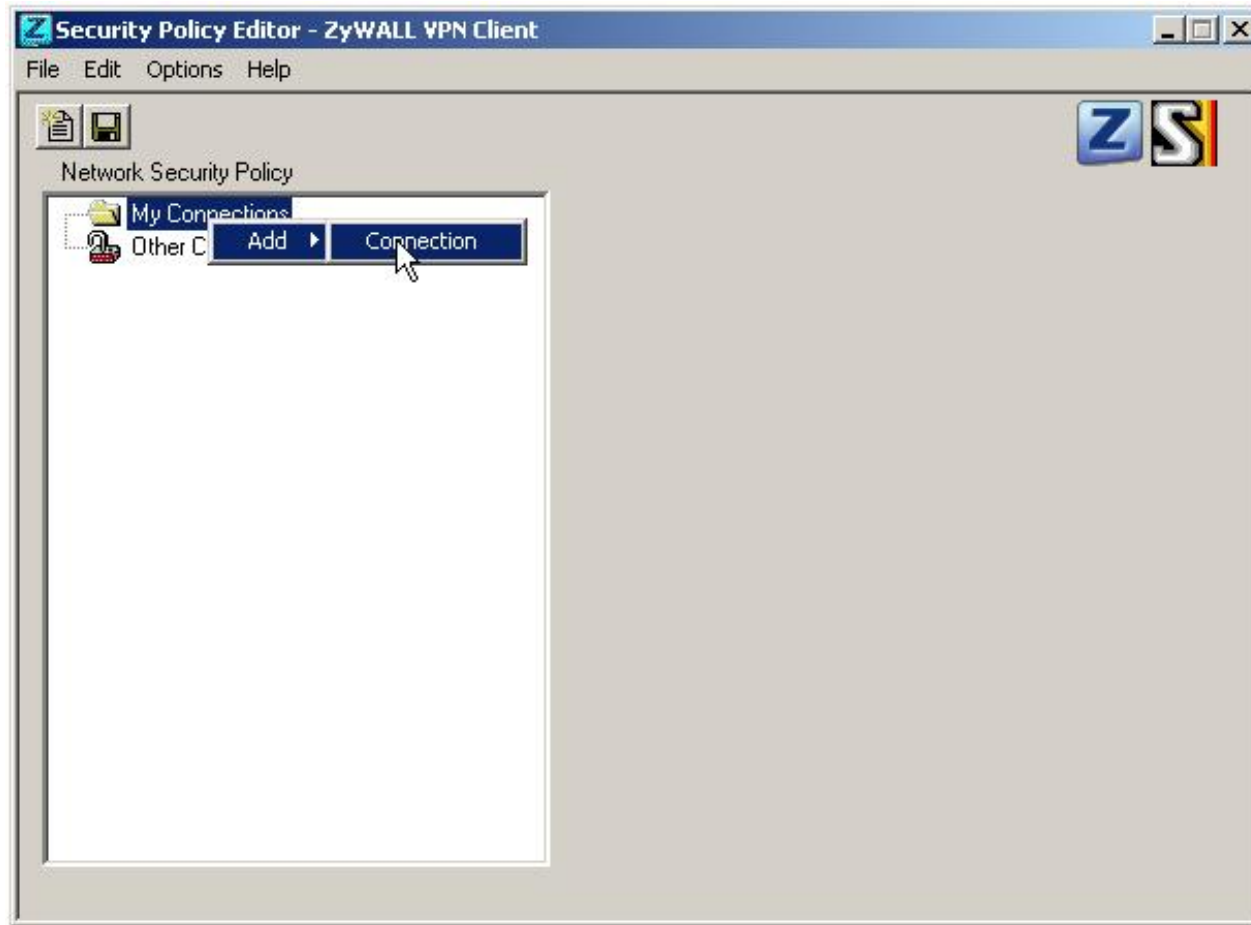
- En el área de notificación del sistema tendremos un icono que representa al software ZyWALL Remote Security Client
- Hacemos clic con el botón derecho sobre él y abrimos la interfaz de configuración de dicho software

# VPN – ZyWALL Remote Security Client –



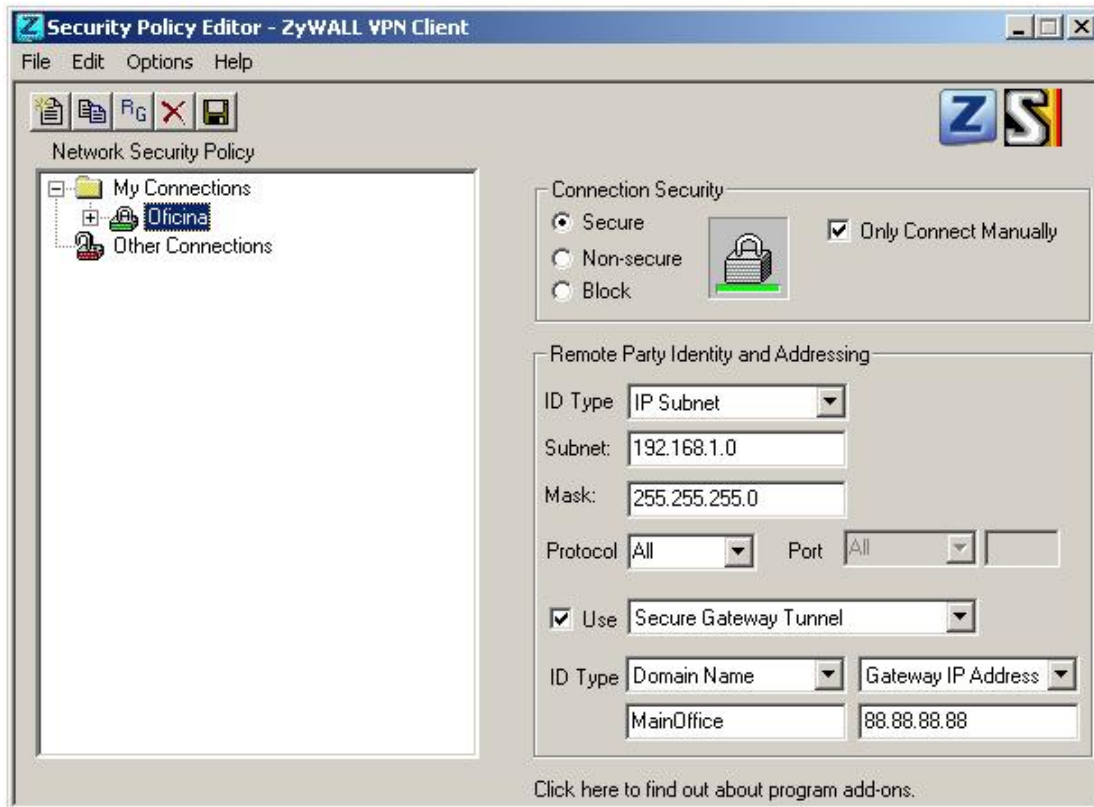
- **Seleccionar securizar “conexiones determinadas (*Specified Connections*)”**

# VPN – ZyWALL Remote Security Client –



- Con el botón derecho sobre “My connections” seleccione añadir conexión

# VPN – ZyWALL Remote Security Client –



## ■ Connection Security:

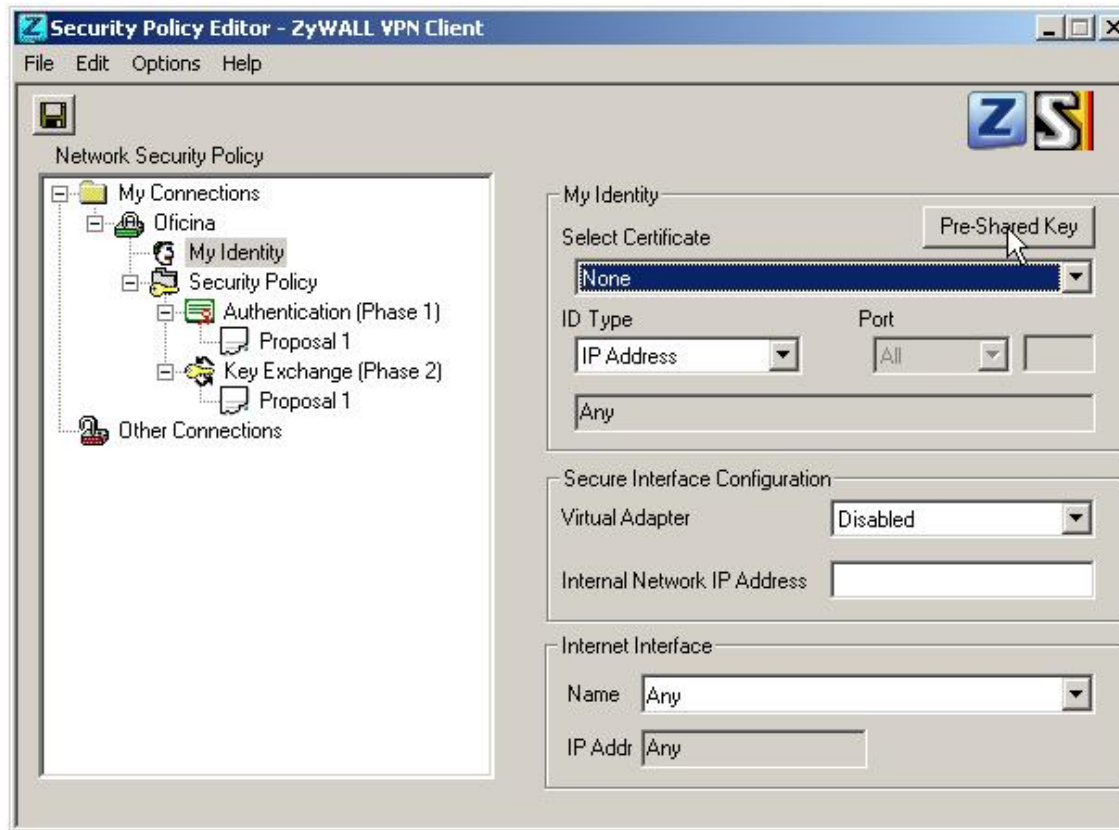
- *Secure*
- Defina también si desea conectar la VPN de modo manual sólo (*Only Connect Manually*)

## ■ Defina los parámetros remotos a los que se conectará, siendo la red remota la misma que ha configurado anteriormente como local

## ■ Use Secure Gateway Tunnel

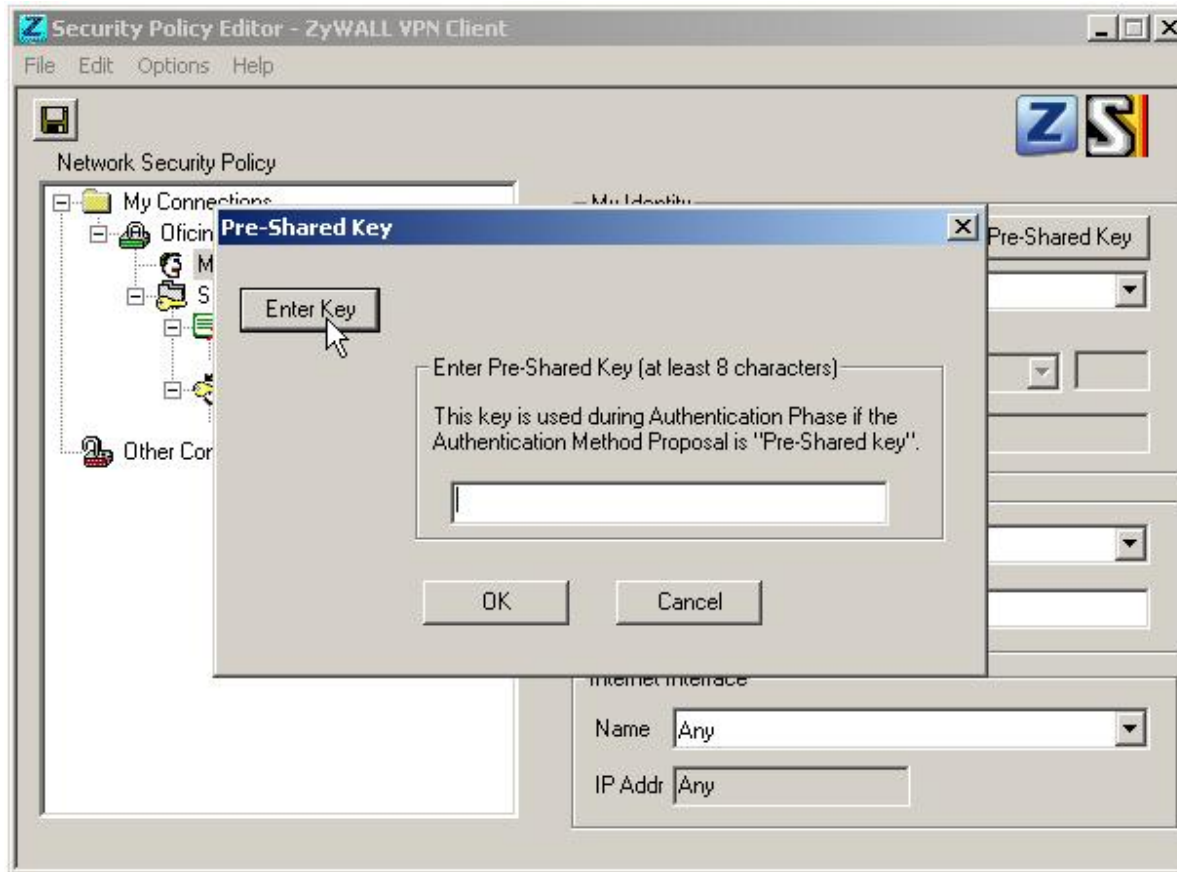
- *ID Type:DNS:MainOffice*
- *Gateway IP Address: la dirección IP pública (o nombre de host) de su ZyWALL remoto siendo aquí 88.88.88.88*

# VPN – ZyWALL Remote Security Client –



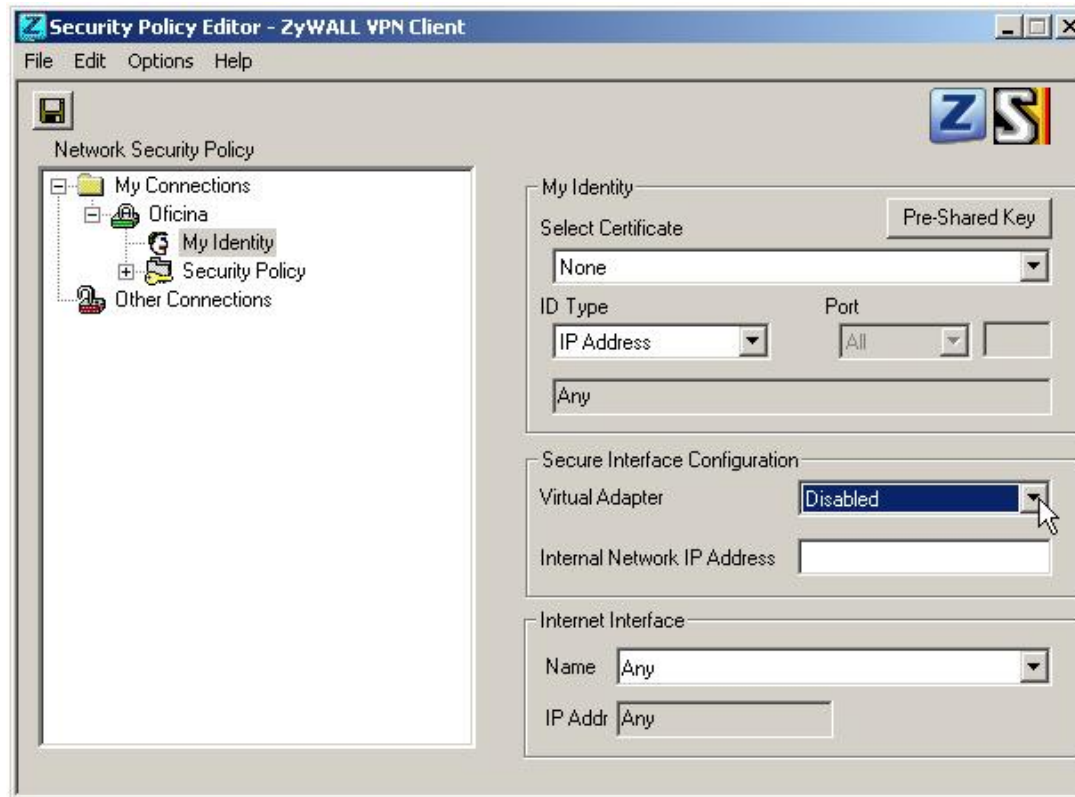
- Seleccionamos aquí como certificado “None” y pulsamos sobre “Pre-Shared Key”

# VPN – ZyWALL Remote Security Client –



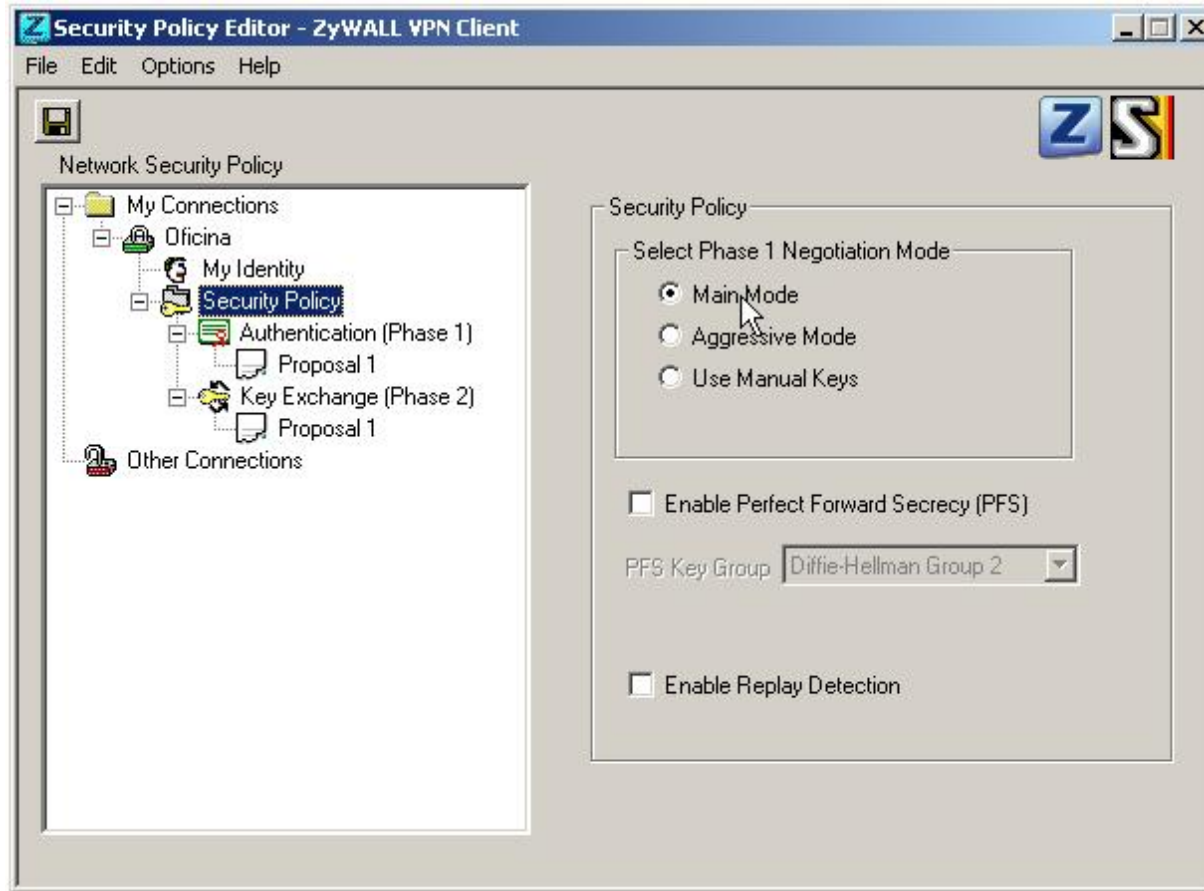
- Se introducirá en el campo en blanco (pulsando sobre “*Enter Key*” la misma clave precompartida que se ha configurado en el ZyWALL:
  - 123456789

# VPN – ZyWALL Remote Security Client –



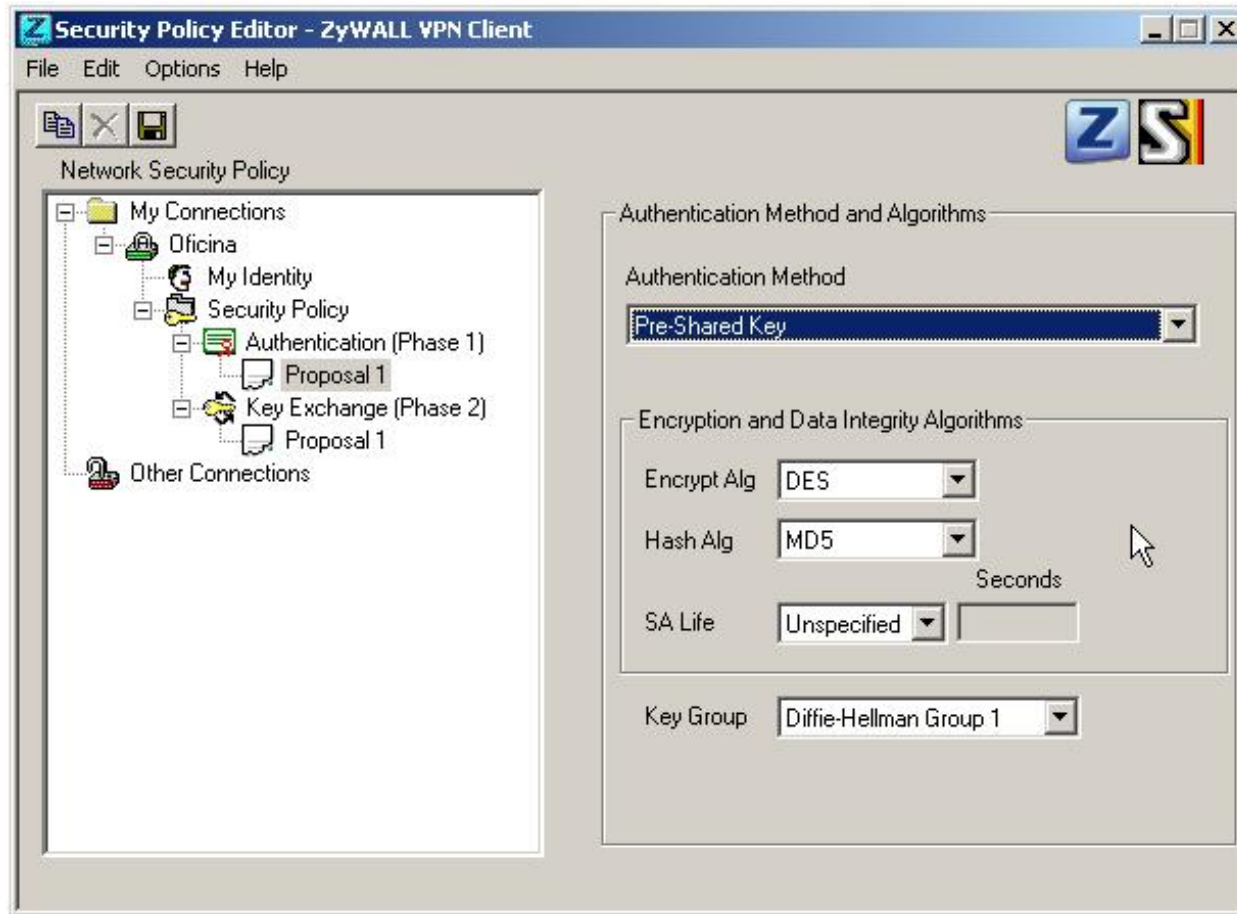
- **Se desactiva el empleo del “adaptador virtual”**
  - Se comentará posteriormente cómo habilitar su uso y su funcionalidad
- **Se emplea cualquier interfaz para el acceso a Internet (Any)**

# VPN – ZyWALL Remote Security Client –



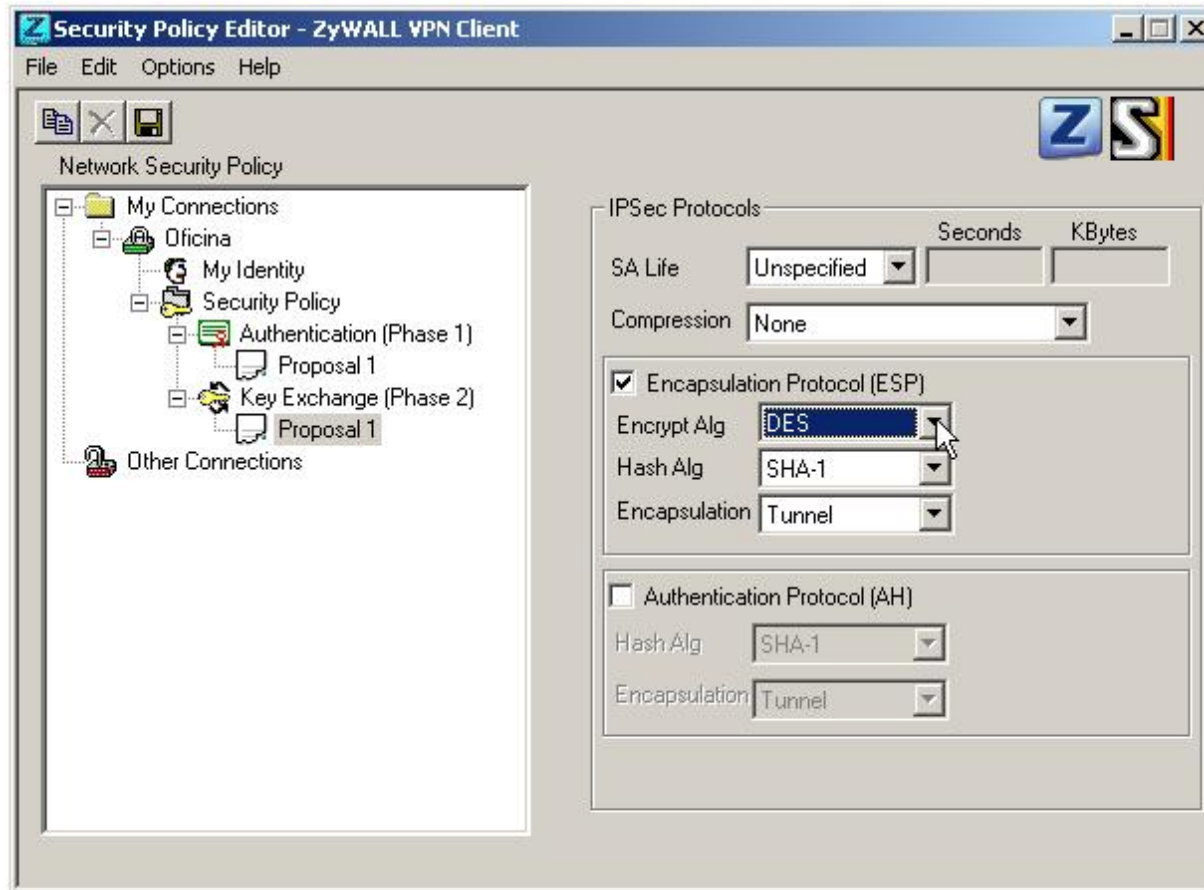
- Se seleccionan los mismos parámetros que en el ZyWALL:
  - Modo: *Main*

# VPN – ZyWALL Remote Security Client –



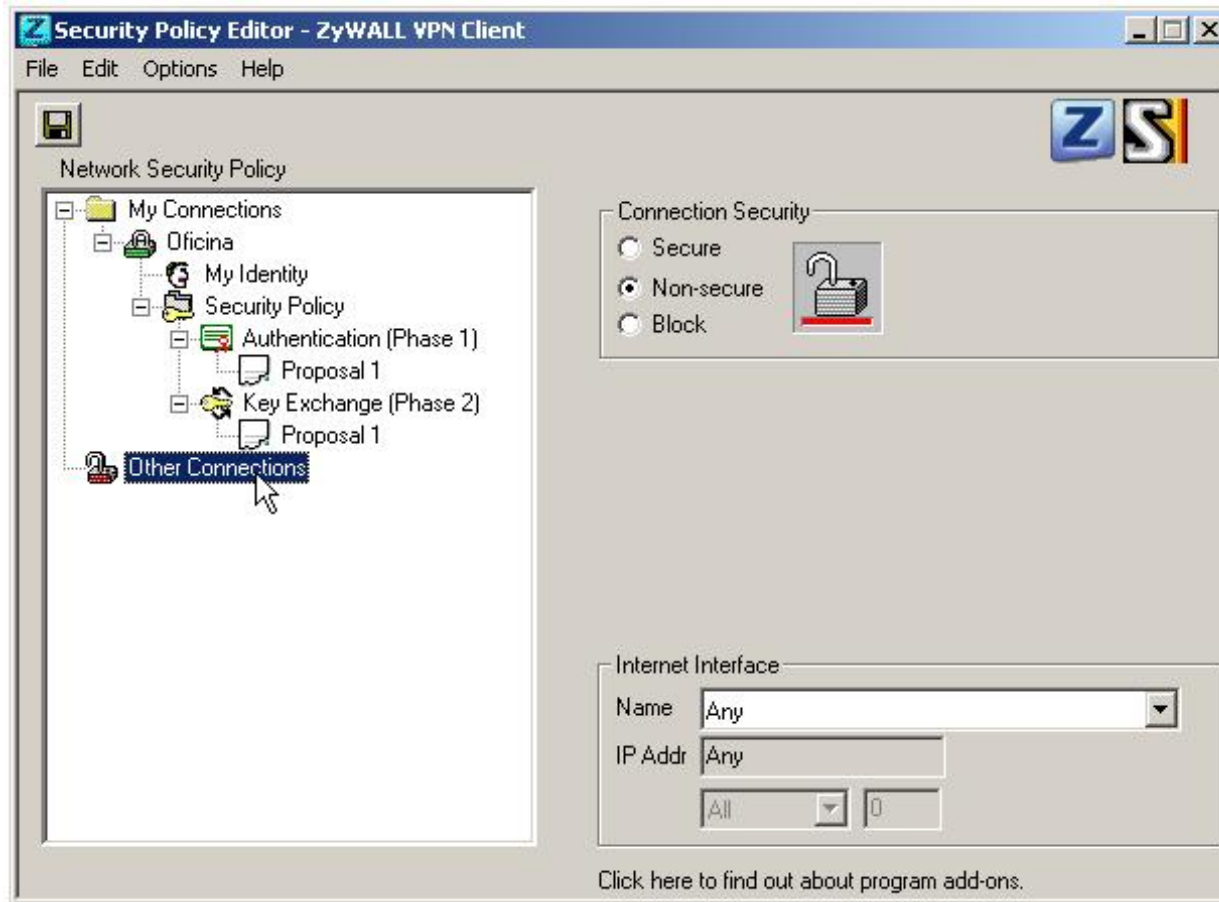
- *DES/MD5/DH1*

# VPN – ZyWALL Remote Security Client –



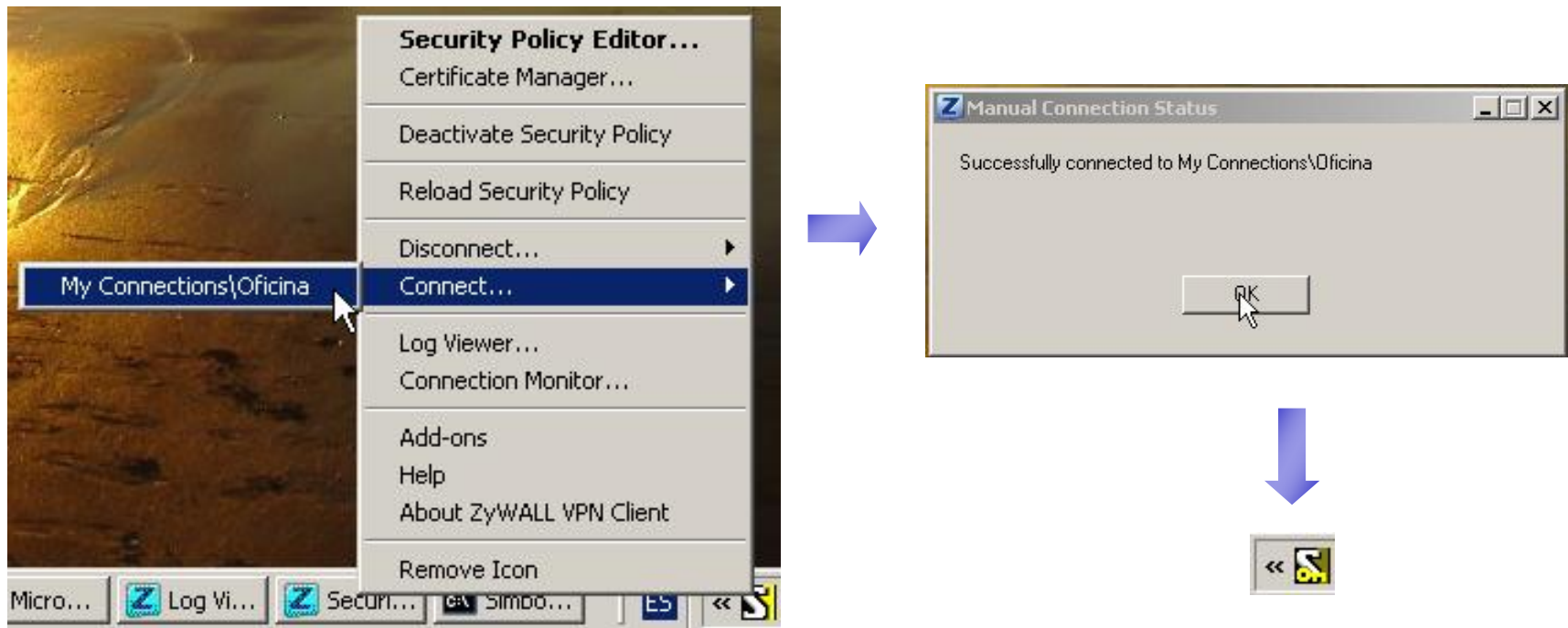
- **Seleccionar ESP:**
  - DES/SHA-1/Tunnel

# VPN – ZyWALL Remote Security Client –



- Seleccionar en “Other Connections” como “*Non-Secure*” para que el tráfico con destino a otras redes no sea enviado a través de una VPN

# VPN – ZyWALL Remote Security Client –



- Para levantar el túnel VPN se pulsa con el botón derecho del ratón sobre el icono y se selecciona “Connect...” y ahí se selecciona la conexión definida
- Se mostrará un mensaje de éxito si todo ha ido correctamente
- Se cambiará el icono a uno indicando que la comunicación está encriptada

# VPN – ZyWALL Remote Security Client –

```
C:\>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local        :

    Sufijo de conexión específica DNS :
    Dirección IP. . . . . : 192.168.167.222
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada  : 192.168.167.1

C:\>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:

Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms

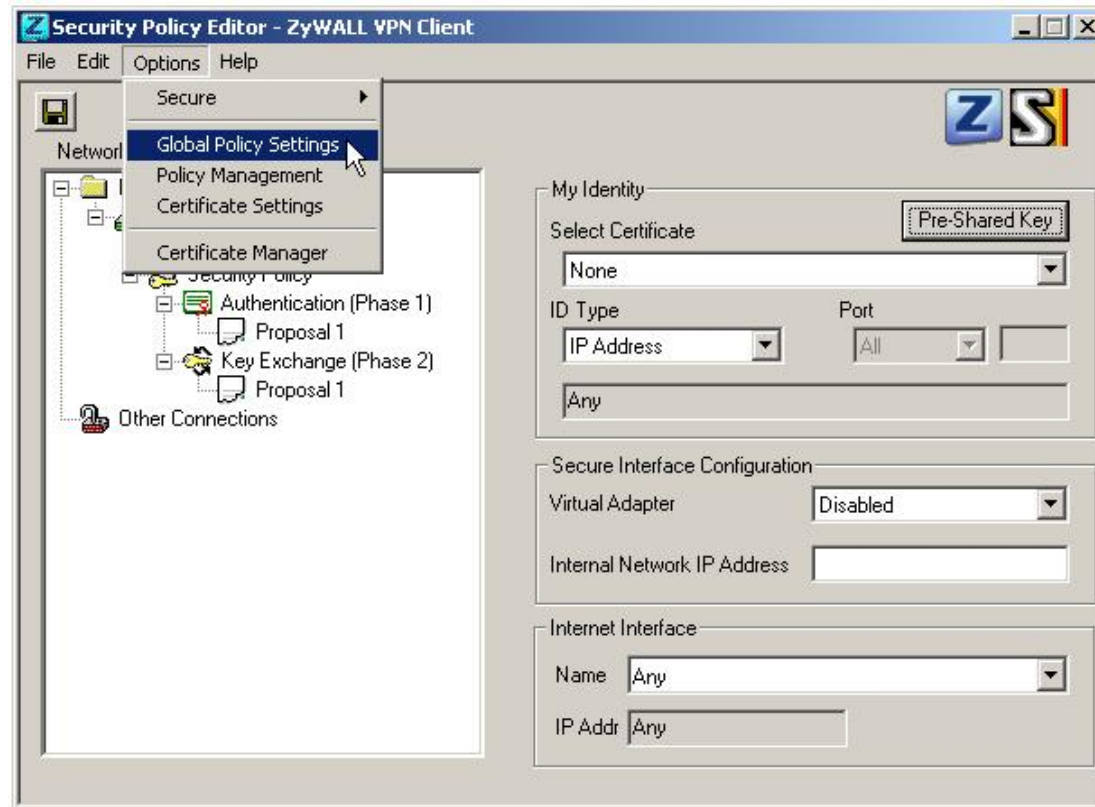
C:\>
```

- Se comprueba el funcionamiento del ping a la red local destino desde la red local origen

# **VPN – ZyWALL Remote Security Client – – Adaptador virtual –**

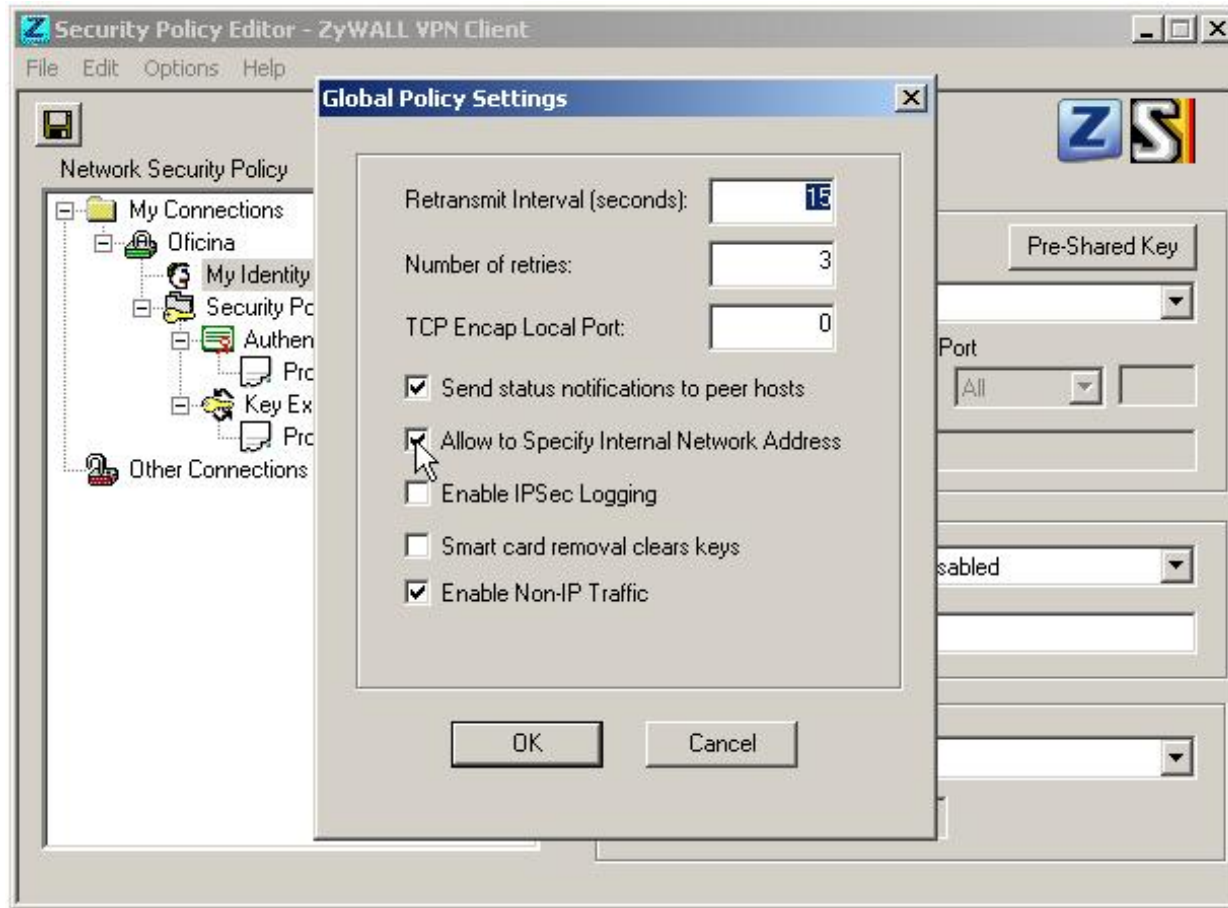
- **Mediante el uso del adaptador virtual se permite especificar la dirección IP desde la que se establece la VPN, es decir, independientemente de la IP que tenga configurada el PC se podrá decidir qué IP se emplea sobre la VPN**

# VPN – ZyWALL Remote Security Client – – Adaptador virtual –



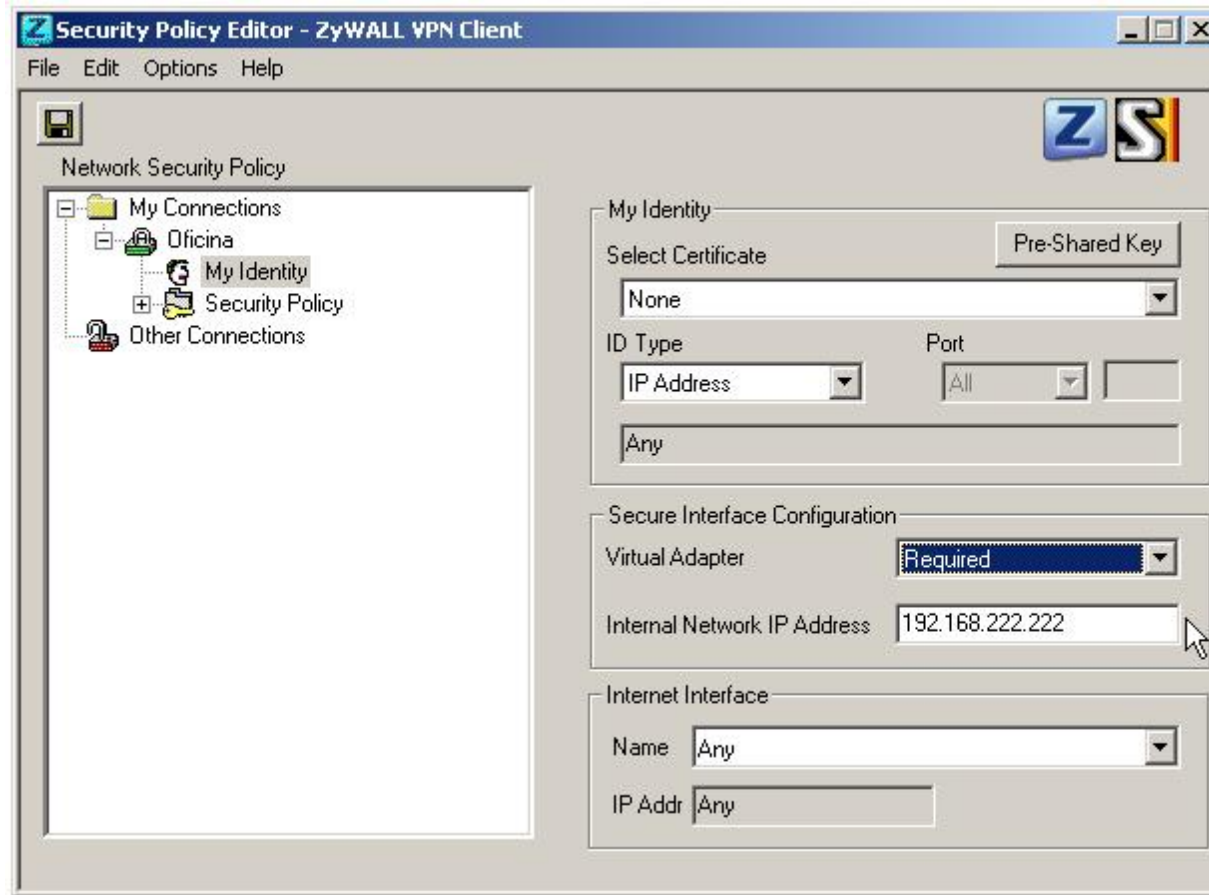
- **Veremos cómo habilitar el uso del adaptador virtual:**
  - *Options->Global Policy Settings*

# VPN – ZyWALL Remote Security Client – – Adaptador virtual –



- Y se marca **“Allow to Specify Internal Network Address”**

# VPN – ZyWALL Remote Security Client – – Adaptador virtual –



- Se cambia a “Required” y se especifica una dirección IP

# VPN – ZyWALL Remote Security Client –

## – Adaptador virtual –

```
C:\>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local           :

    Sufijo de conexión específica DNS :
    Dirección IP. . . . . : 192.168.167.222
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada   : 192.168.167.1

Adaptador PPP SafeNet Virtual Adapter Interface     :

    Sufijo de conexión específica DNS :
    Dirección IP. . . . . : 192.168.222.222
    Máscara de subred . . . . . : 255.255.255.255
    Puerta de enlace predeterminada   :

C:\>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:

Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (<0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms
```

- Se verifica el funcionamiento de la VPN y el uso del adaptador virtual para el establecimiento de la VPN

# ZyWALL IPSec VPN Client

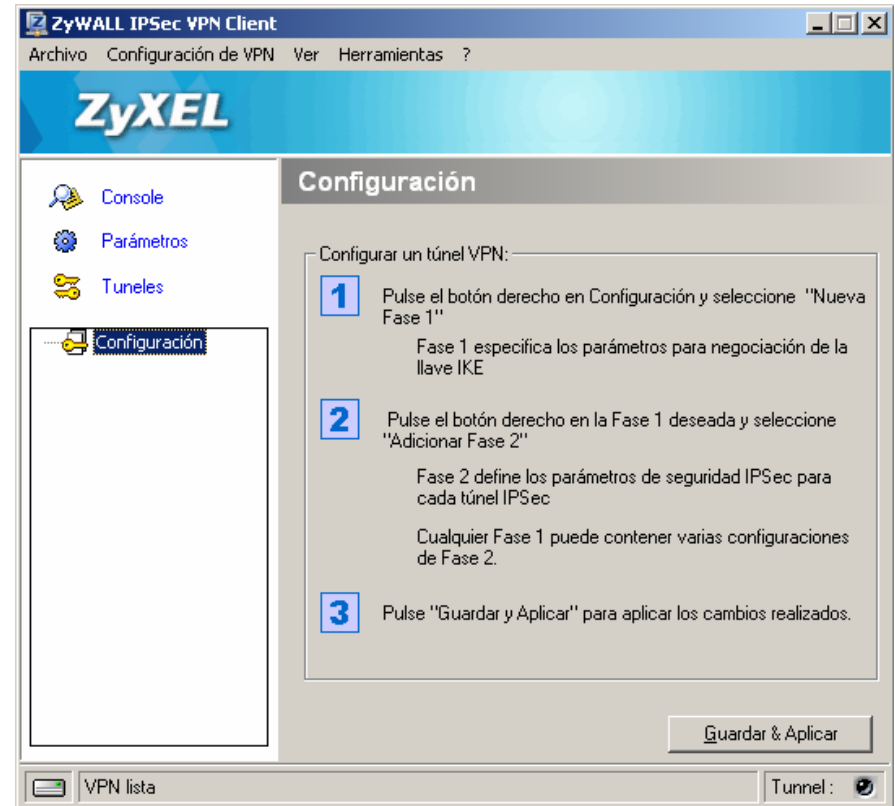
# VPN -ZyWALL IPSec VPN Client-



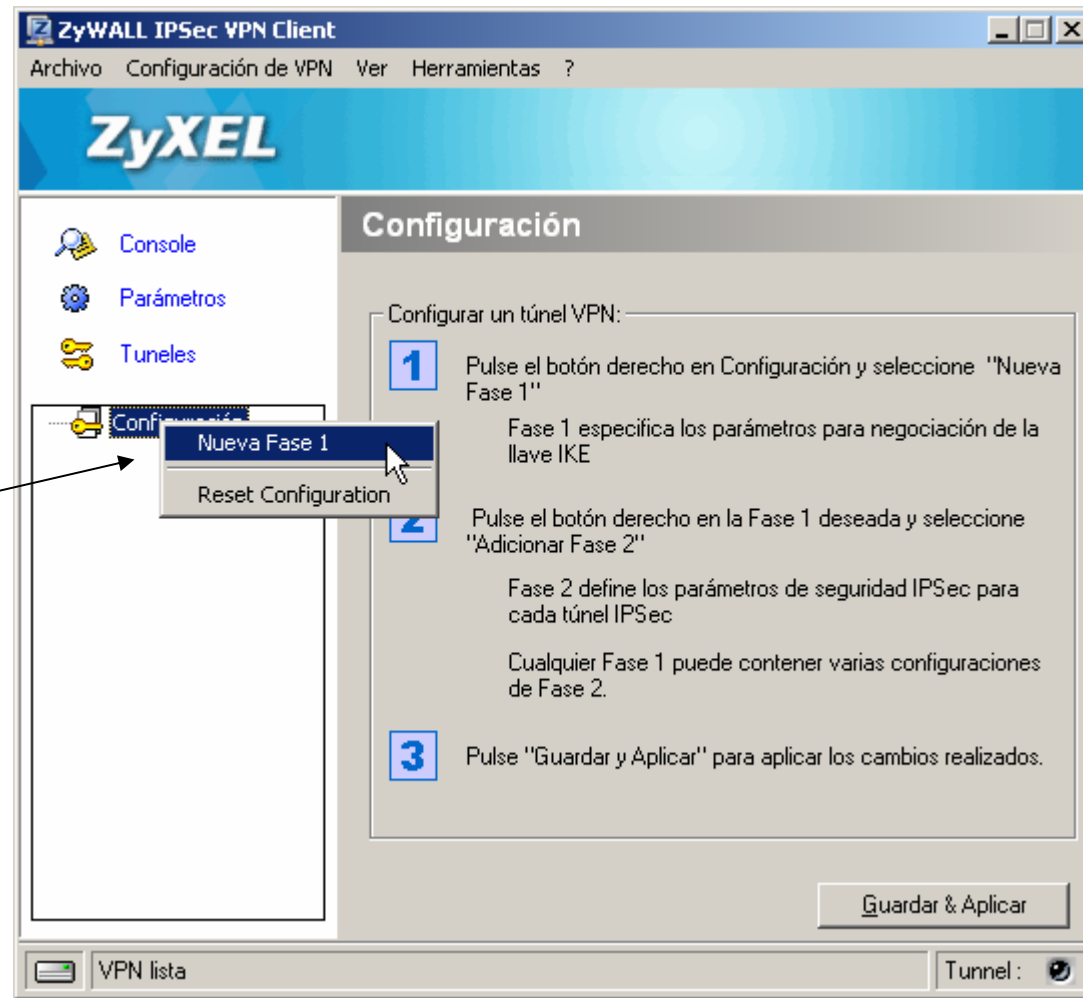
**Botón derecho del ratón sobre el icono**



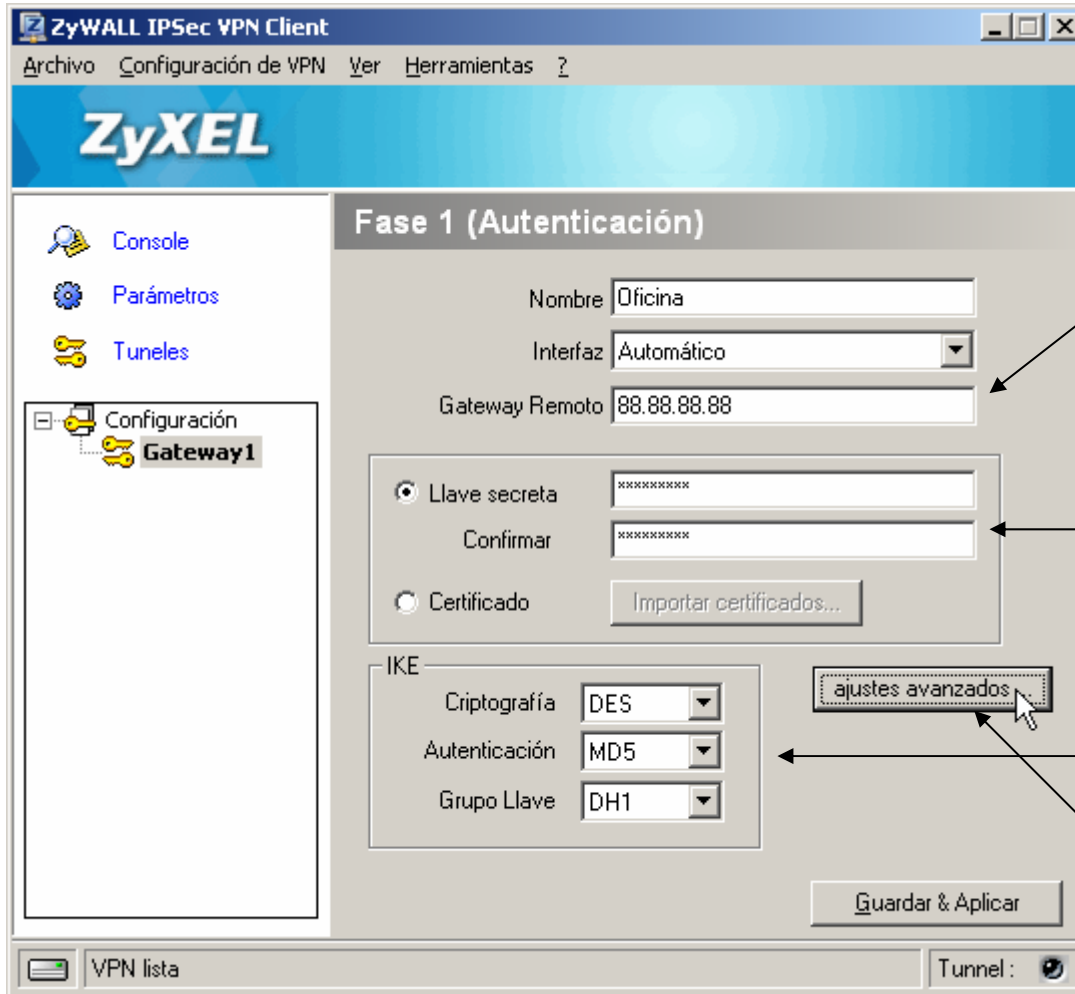
**Pulsar sobre esta pantalla *Ctrl+Enter* para abrir el menú siguiente**



# VPN -ZyWALL IPSec VPN Client-



# VPN -ZyWALL IPSec VPN Client-



## •Gateway remoto:

- la dirección IP del ZyWALL o equipo de seguridad al que se va a conectar, en este ejemplo:

**88.88.88.88**

## •Clave secreta:

- Clave secreta para el túnel, en este ejemplo:

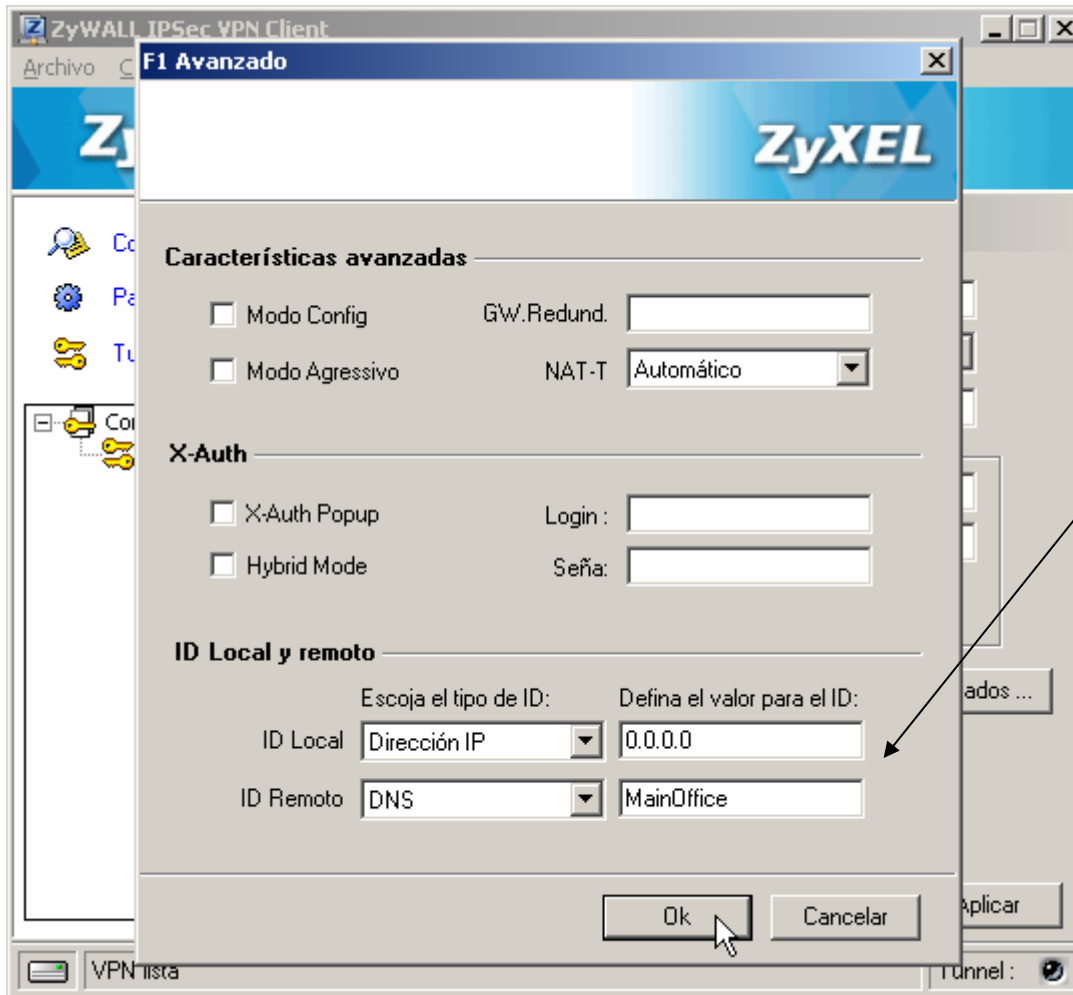
**123456789**

## •Parámetros IKE:

- DES/MD5/DH1**

- Se pulsa sobre avanzados por último en esta parte

# VPN -ZyWALL IPSec VPN Client-



•Se configuran el “Local ID” y el “Remote ID”:

•Local ID:

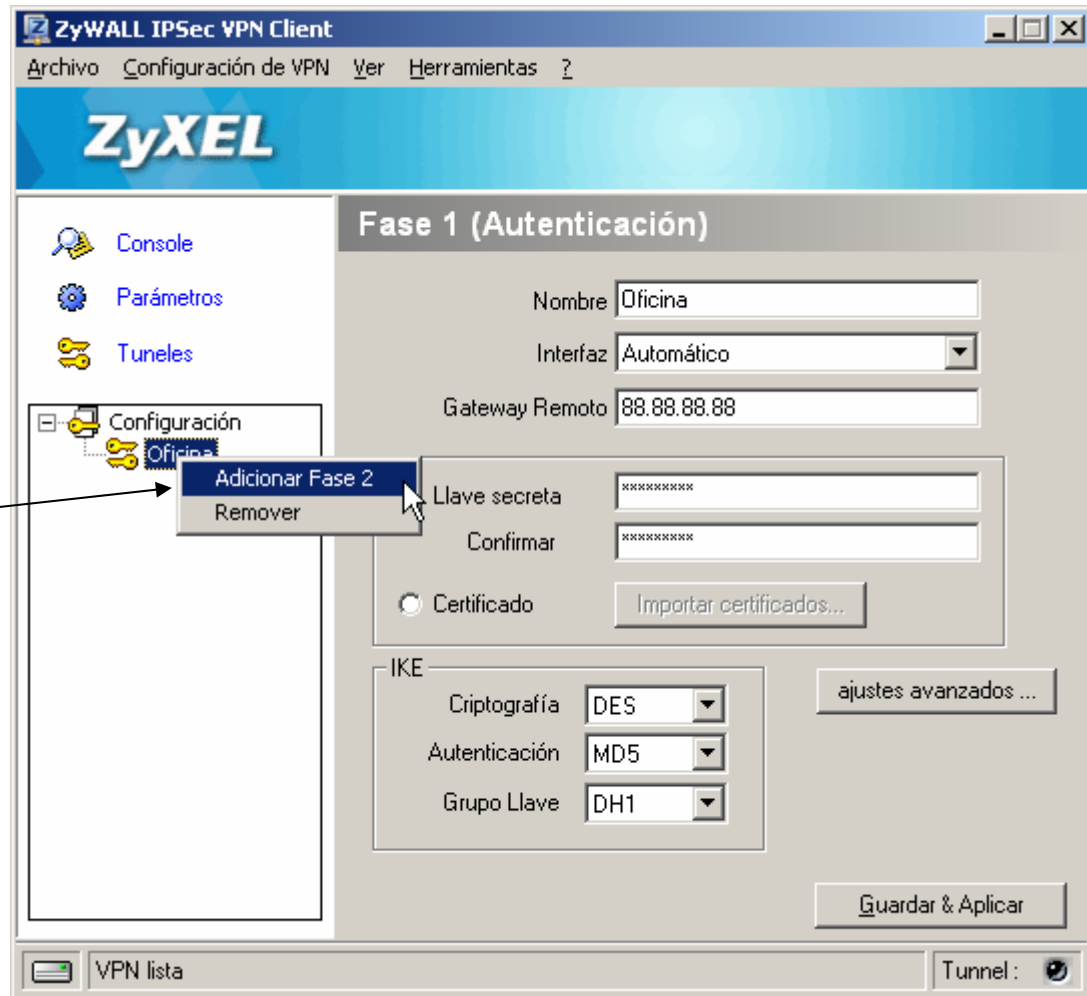
**IP:0.0.0.0**

•Remote ID:

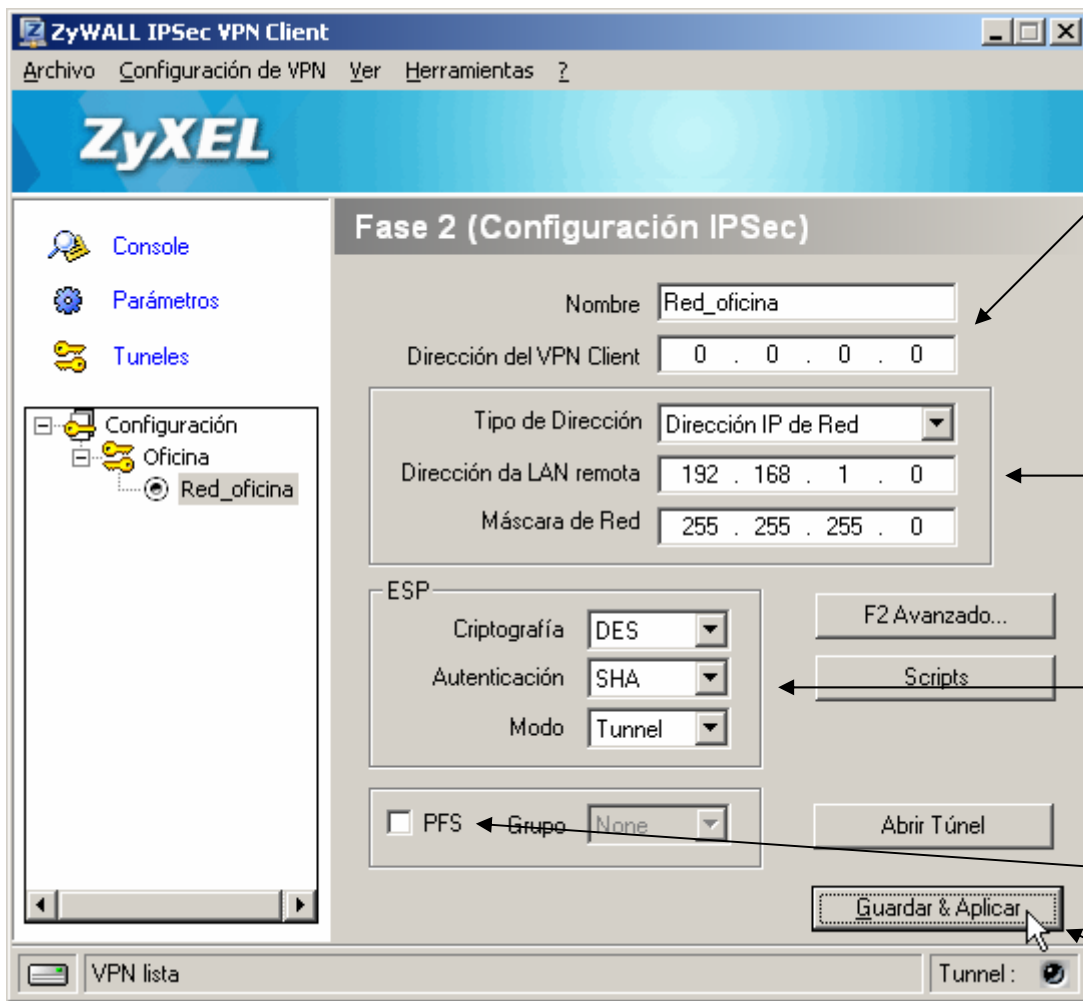
**DNS:MainOffice**

# VPN -ZyWALL IPSec VPN Client-

Botón derecho del ratón sobre “Oficina” y seleccionar “Adicionar Fase 2”



# VPN -ZyWALL IPSec VPN Client-



## •Nombre:

- Se da un nombre cualquiera

## •Dirección VPN Client:

- Ver apartado posterior

## •Rangos de red remota:

- Se configura la red de la oficina que está tras el ZyWALL:

**IP de red:**

**192.168.1.0/255.255.255.0**

## •Parámetros IPSec:

**•DES/SHA/Tunnel**

## •Se deshabilita el uso de PFS

- Se pulsa sobre guardar y aplicar

# VPN -ZyWALL IPSec VPN Client-

- Con “Ctrl+Enter” volvemos a la pantalla resumen y de conexiones
- Se pulsa sobre abrir el túnel y se ve como se establece al cambiar el icono de color



Pulsar sobre abrir para iniciar el túnel



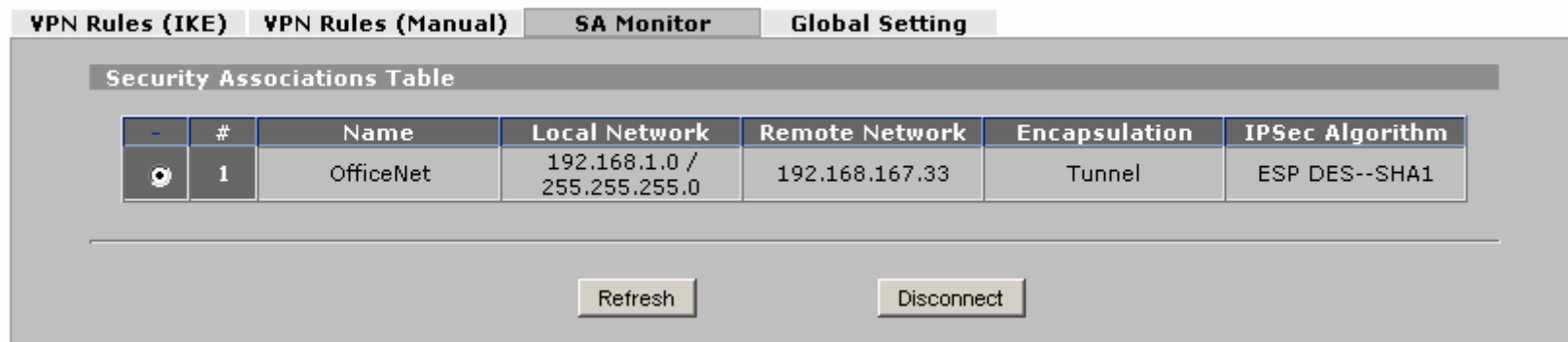
Túnel iniciado



# VPN -ZyWALL IPSec VPN Client-

- Se comprueba con el monitor VPN en el ZyWALL que se ha establecido

VPN



The screenshot shows the 'SA Monitor' tab in the ZyWALL VPN configuration interface. It displays a 'Security Associations Table' with the following data:

-	#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
<input checked="" type="radio"/>	1	OfficeNet	192.168.1.0 / 255.255.255.0	192.168.167.33	Tunnel	ESP DES--SHA1

Below the table are two buttons: 'Refresh' and 'Disconnect'.

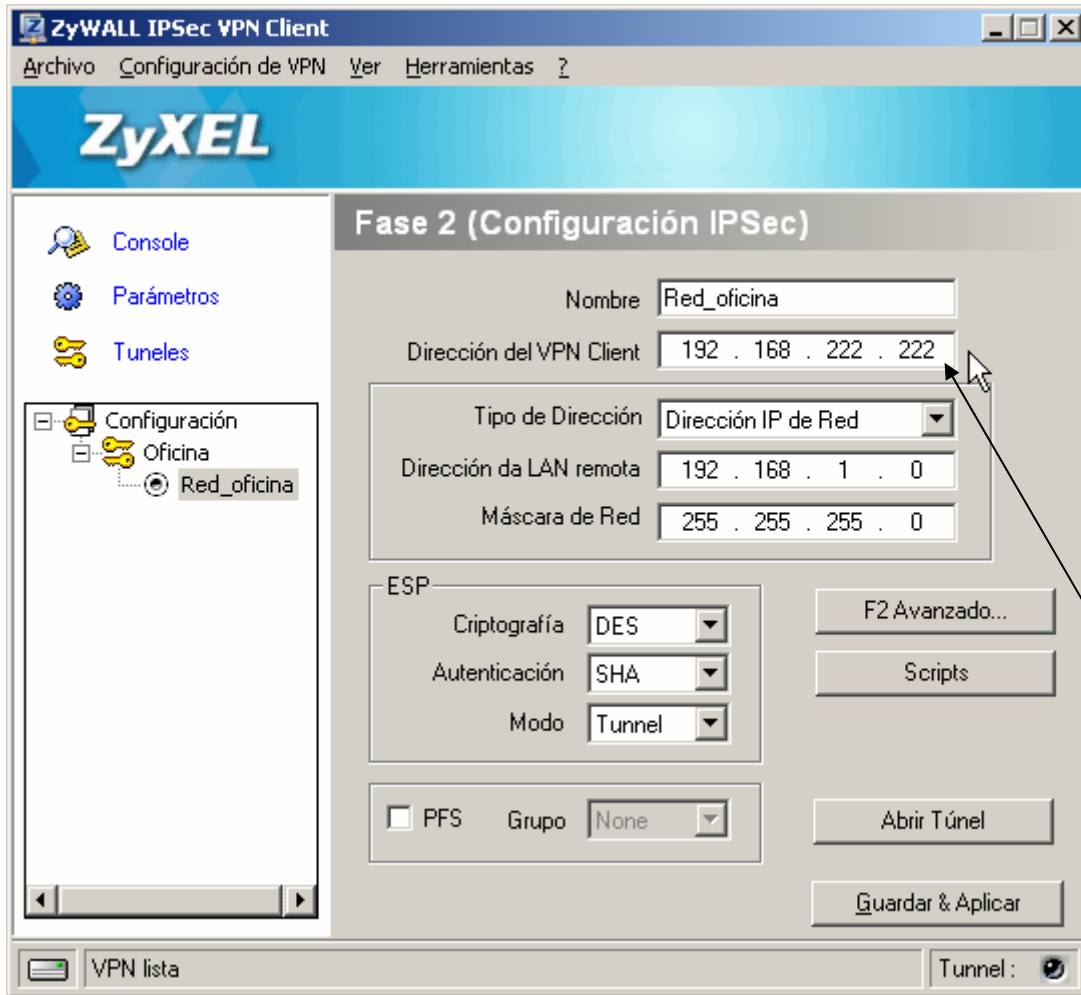
- Se comprueba su funcionamiento realizando un “ping” contra la red remota:

```
C:\>ping 192.168.1.1
Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 1ms, Media = 1ms
C:\>
```

# VPN -ZyWALL IPSec VPN Client- - Adaptador virtual -

- **Mediante el uso del adaptador virtual se permite especificar la dirección IP desde la que se establece la VPN, es decir, independientemente de la IP que tenga configurada el PC se podrá decidir qué IP se emplea sobre la VPN**

# VPN -ZyWALL IPSec VPN Client- - Adaptador virtual -



- En caso de querer emplear una IP definida localmente, un adaptador virtual se configuraría en el campo:

- **Dirección del VPN Client**

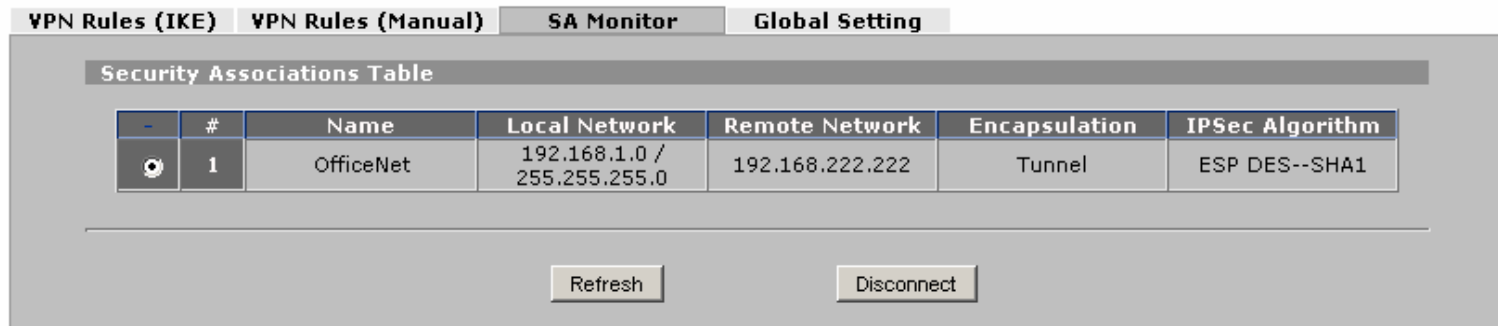
• Se usará para el ejemplo la siguiente IP:

**192.168.222.222**

# VPN -ZyWALL IPSec VPN Client- - Adaptador virtual -

- Se comprueba con el monitor de la VPN la IP que se recibe, en “*Remote network*”

VPN



The screenshot shows the 'SA Monitor' tab in the ZyWALL VPN configuration interface. It displays a 'Security Associations Table' with the following data:

-	#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
○	1	OfficeNet	192.168.1.0 / 255.255.255.0	192.168.222.222	Tunnel	ESP DES--SHA1

Below the table are two buttons: 'Refresh' and 'Disconnect'.

- Y que el ping continúa funcionando

```
C:\>ping 192.168.1.1
Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=254
Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 1ms, Media = 1ms
C:\>
```