

Apéndice IV

Definición de VPN entre dos sedes

Apéndice IV - Ejemplo VPN -

■ Sede central:

- Dispone de dos líneas ADSL
 - IP1: 80.0.0.1
 - IP2: 81.1.1.1
- Rango de red local
 - 192.168.2.0/255.255.255.0

■ Oficina remota

- Dispone de una línea ADSL
 - IP: 99.0.0.1
- Rango de red local
 - 192.168.3.0/255.255.255.0

Apéndice IV - Definir VPN central -

■ Definir gateways remotos (I)

VPN - GATEWAY POLICY - EDIT

Property

Name: SedeCentral

NAT Traversal

Gateway Policy Information

My ZyWALL

My Address: 0.0.0.0 (Domain Name or IP Address)

My Domain Name: None (See [DDNS](#))

Primary Remote Gateway: 99.0.0.1 (Domain Name or IP Address)

Enable IPSec High Availability

Redundant Remote Gateway: (Domain Name or IP Address)

Fail back to Primary Remote Gateway when possible

Fail Back Check Interval*: (180~86400 seconds)

*Fail 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 IPSec SA life time will be superseded by this value when it is larger than this value.

Authentication Key

Pre-Shared Key: 123456789

Certificate: auto_generated_self_signed_cert (See [My Certificates](#))

Local ID Type: IP

Content: 1.1.1.1

Peer ID Type: IP

Content: 2.2.2.2

■ Definir como gateway local: 0.0.0.0 (así decidirá de modo automático la IP a emplear)

■ Definir el gateway remoto, la situación del otro extremo de la VPN

■ Definir la clave precompartida

■ Definir los campos de autenticación “main”, lo que para un extremo es local para el otro extremo de la VPN será remoto

Apéndice IV - Definir VPN central -

▪ Definir gateways remotos (II)

The screenshot displays the configuration interface for a VPN gateway. It is divided into three main sections:

- Extended Authentication:** This section contains a checkbox for "Enable Extended Authentication" which is unchecked. Below it are radio buttons for "Server Mode" and "Client Mode", with "Client Mode" selected. To the right of these options is the text "(Search [Local User](#) first then [RADIUS](#))". Below the radio buttons are two input fields labeled "User Name" and "Password".
- IKE Proposal:** This section contains several configuration options:
 - Negotiation Mode: A dropdown menu set to "Main".
 - Encryption Algorithm: A dropdown menu set to "DES".
 - Authentication Algorithm: A dropdown menu set to "MD5".
 - SA Life Time (Seconds): An input field containing the value "28800".
 - Key Group: A dropdown menu set to "DH1".
 - Enable Multiple Proposals: An unchecked checkbox.
- Associated Network Policies:** This section features a table with the following structure:

#	Name	Local Network	Remote Network

At the bottom of the interface, there are two buttons: "Apply" and "Cancel".

- Mantener sin marcar la opción de “*Enable Extended Authentication*”
- Definir las opciones de IKE, deberán ser las mismas que en el extremo remoto

Apéndice IV - Definir VPN central -

▪ Definir políticas de red (I)

VPN - NETWORK POLICY - EDIT

The screenshot shows the configuration window for a VPN Network Policy. It is titled "VPN - NETWORK POLICY - EDIT". The window is divided into two main sections: "Property" and "Gateway Policy Information".

Property Section:

- Active
- Name: RedesCentralOficina
- Protocol: 0
- Nailed-Up
- Allow NetBIOS broadcast Traffic Through IPsec Tunnel
- Check IPsec Tunnel Connectivity
- Log: Log
- Ping this Address: 0 . 0 . 0 . 0 . 0

Gateway Policy Information Section:

- Gateway Policy: SedeCentral

- Se marca como activa la política de red que se va a definir
- Se habilita la opción de *“Nailed-Up”* para que se mantenga la VPN levantada
- Si se desea que funcione el “entorno de red” se debe marcar la opción *“Allow NetBIOS...”*

Apéndice IV - Definir VPN central -

▪ Definir políticas de red (II)

The screenshot displays a configuration window for a VPN. It is divided into three main sections: Local Network, Remote Network, and IPsec Proposal.

- Local Network:** Features a cloud icon with an 'L'. The 'Address Type' is set to 'Subnet Address'. The 'Starting IP Address' is 192.168.2.0, and the 'Ending IP Address / Subnet Mask' is 255.255.255.0. The 'Local Port' is set to Start 0 and End 0.
- Remote Network:** Features a cloud icon with an 'R'. The 'Address Type' is set to 'Subnet Address'. The 'Starting IP Address' is 192.168.3.0, and the 'Ending IP Address / Subnet Mask' is 255.255.255.0. The 'Remote Port' is set to Start 0 and End 0.
- IPsec Proposal:** Includes several dropdown menus: 'Encapsulation Mode' (Tunnel), 'Active Protocol' (ESP), 'Encryption Algorithm' (DES), 'Authentication Algorithm' (SHA1), and 'Perfect Forward Secrecy (PFS)' (NONE). The 'SA Life Time (Seconds)' is set to 28800. There are two checkboxes: 'Enable Replay Detection' and 'Enable Multiple Proposals', both of which are currently unchecked.

At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

- Se define la red local (que en el otro extremo será remota)
- Se define la red remota (que en el otro extremo será local)
- Se definen los campos de seguridad de IPsec (deben ser los mismos en el extremo remoto de la VPN)

Apéndice IV - Definir VPN remota -

■ Definir gateways remotos (I)

VPN - GATEWAY POLICY - EDIT

Property

Name: OficinaRemota

NAT Traversal

Gateway Policy Information

My ZyWALL

My Address: 0.0.0.0 (Domain Name or IP Address)

My Domain Name: None (See [DDNS](#))

Primary Remote Gateway: 80.0.0.1 (Domain Name or IP Address)

Enable IPSec High Availability

Redundant Remote Gateway: 81.1.1.1 (Domain Name or IP Address)

Fail back to Primary Remote Gateway when possible

Fail Back Check Interval*: 28800 (180~86400 seconds)

*Fail 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.

Authentication Key

Pre-Shared Key: 123456789

Certificate: auto_generated_self_signed_cert (See [My Certificates](#))

Local ID Type: IP

Content: 2.2.2.2

Peer ID Type: IP

Content: 1.1.1.1

Definir como gateway local: 0.0.0.0 (así decidirá de modo automático la IP a emplear)

Definir el gateway remoto, la situación del otro extremo de la VPN

Se define “Alta disponibilidad” del enlace, puesto que el ZyWALL de la central tiene 2 posibles accesos de entrada

Definir la clave precompartida

Definir los campos de autenticación “main”, lo que para un extremo es local para el otro extremo de la VPN será remoto

Apéndice IV - Definir VPN remota -

▪ Definir gateways remotos (II)

The screenshot displays the configuration interface for a remote VPN gateway. It is divided into three main sections:

- Extended Authentication:** Contains a checkbox for "Enable Extended Authentication" (unchecked). Below it are radio buttons for "Server Mode" and "Client Mode" (selected). A note indicates to search for "Local User" first then "RADIUS". There are input fields for "User Name" and "Password".
- IKE Proposal:** Contains several dropdown menus: "Negotiation Mode" (Main), "Encryption Algorithm" (DES), "Authentication Algorithm" (MD5), and "Key Group" (DH1). There is also a text input field for "SA Life Time (Seconds)" set to 28800 and a checkbox for "Enable Multiple Proposals" (unchecked).
- Associated Network Policies:** A table with columns for "#", "Name", "Local Network", and "Remote Network". The table is currently empty.

At the bottom of the interface are "Apply" and "Cancel" buttons.

- Mantener sin marcar la opción de “*Enable Extended Authentication*”
- Definir las opciones de IKE, deberán ser las mismas que en el extremo remoto

Apéndice IV - Definir VPN remota -

▪ Definir políticas de red (I)

VPN - NETWORK POLICY - EDIT

The screenshot displays the 'Property' section of a VPN configuration window. The 'Active' checkbox is checked. The 'Name' field contains 'RedesOficinaCentral' and the 'Protocol' field contains '0'. The 'Nailed-Up' checkbox is unchecked. The 'Allow NetBIOS broadcast Traffic Through IPsec Tunnel' checkbox is unchecked. The 'Check IPsec Tunnel Connectivity' checkbox is unchecked, and the 'Log' checkbox is checked. The 'Ping this Address' field contains '0 . 0 . 0 . 0'. The 'Gateway Policy Information' section shows a 'Gateway Policy' dropdown menu set to 'OficinaRemota'.

- Se marca como activa la política de red que se va a definir
- Se habilita la opción de *“Nailed-Up”* para que se mantenga la VPN levantada
- Si se desea que funcione el “entorno de red” se debe marcar la opción *“Allow NetBIOS...”*

Apéndice IV - Definir VPN remota -

▪ Definir políticas de red (II)

The screenshot displays the configuration interface for a remote VPN. It is divided into three main sections: Local Network, Remote Network, and IPsec Proposal.

Local Network:

- Address Type: Subnet Address
- Starting IP Address: 192 . 168 . 3 . 0
- Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0
- Local Port: Start 0, End 0

Remote Network:

- Address Type: Subnet Address
- Starting IP Address: 192 . 168 . 2 . 0
- Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0
- Remote Port: Start 0, End 0

IPsec Proposal:

- Encapsulation Mode: Tunnel
- Active Protocol: ESP
- Encryption Algorithm: DES
- Authentication Algorithm: SHA1
- SA Life Time (Seconds): 28800
- Perfect Forward Secrecy (PFS): NONE
- Enable Replay Detection
- Enable Multiple Proposals

Buttons: Apply, Cancel

- Se define la red local (que en el otro extremo será remota)
- Se define la red remota (que en el otro extremo será local)
- Se definen los campos de seguridad de IPsec (deben ser los mismos en el extremo remoto de la VPN)