

## IPSec between uSysCom 3GAT and Microsoft Windows

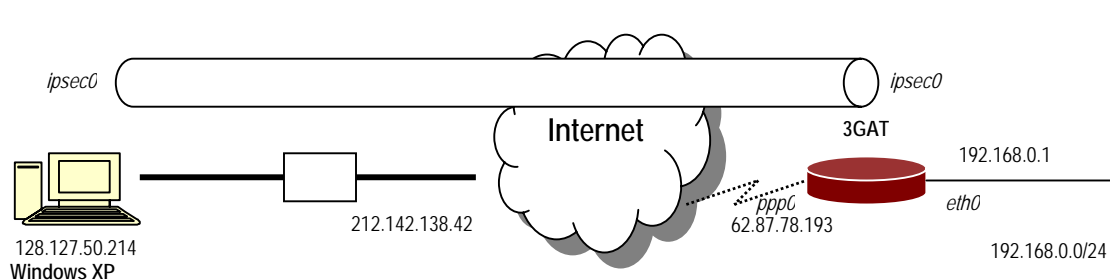
### Scope

This application note describes the main steps in order to set up an IPSec tunnel between uSysCom 3GAT wireless routers and Microsoft Windows.

This document assumes that the reader is familiar with both, IPSec/IKE concepts and the Microsoft Management Console.

### Network architecture

Next figure shows the architecture that is to be described. On one end, a Windows XP-based computer that has SP2 installed. A LAN behind the 3GAT wireless router is on the other end. It is important to note that the Windows XP-based computer has a public address. More accurately, the Windows XP is behind a NAT/Firewall device which translates the public IP address into the Windows XP-based computer private IP address.



The tunnel is defined by the following parameters:

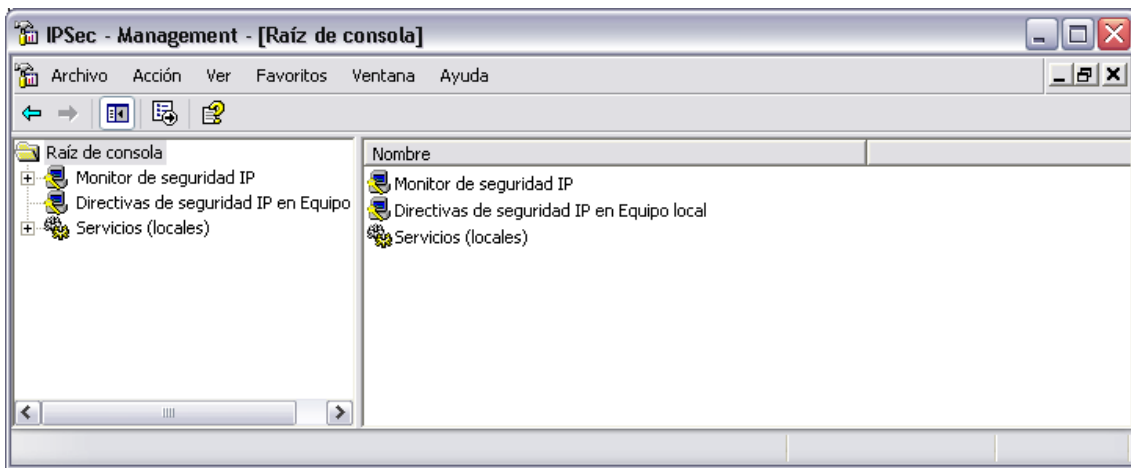
IKE Parameter	Value
Identification	IP Address
Authentication method (Pre-shared key)	"usyscom"
Exchange mode for phase 1	Main mode
Encryption Algorithm	3DES
Authentication algorithm	SHA1
Diffie Hellman	DH2
IKE LifeTime (seconds)	28.800 s

IPSec Parameter	Value
Security Protocol	ESP
Encryption Algorithm	3DES
Authentication algorithm	MD5
IPSec LifeTime (seconds)	3.600 s
PFS Group	None

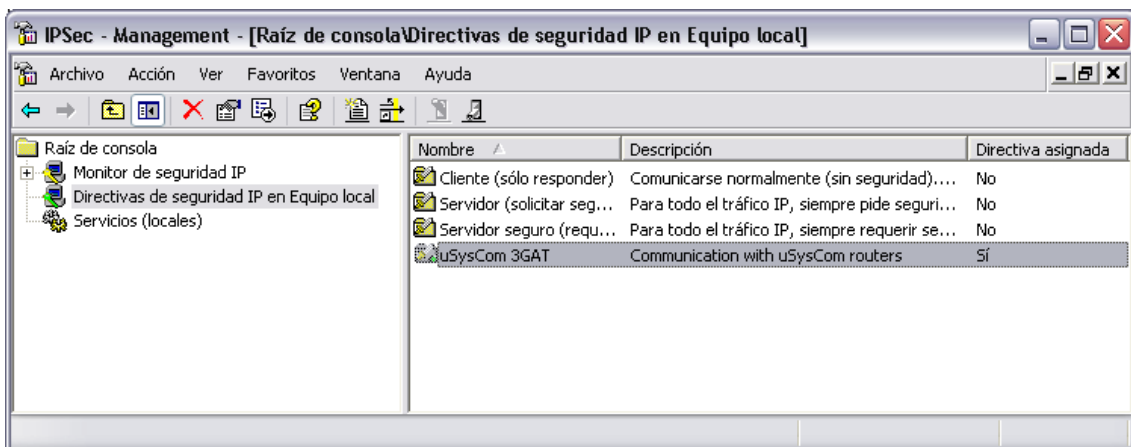
## Windows XP Configuration

All configuration steps will be done using Microsoft Management Console (*mmc*).

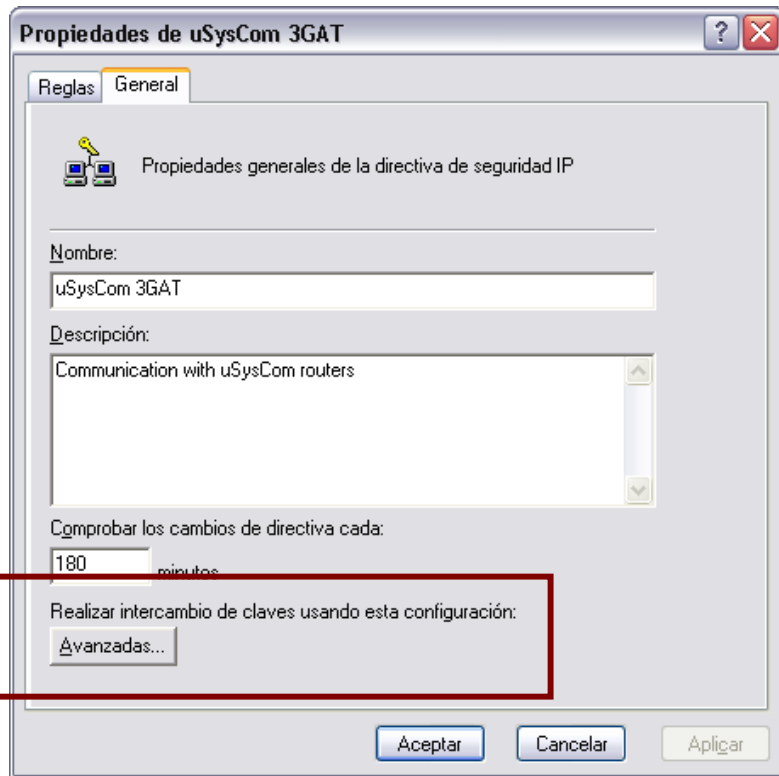
- Start – Run – *mmc*
- Configure a *mmc* that includes the following snap-ins:
  - a. IPSEC Monitoring. This snap-in will be used to know the status of the IPSEC tunnel.
  - b. IPSEC Security policies. This snap-in will allow us to configure the IPsec Tunnel
  - c. Services. This snap-in can be used in order to start/stop/restart the IPSEC related services.



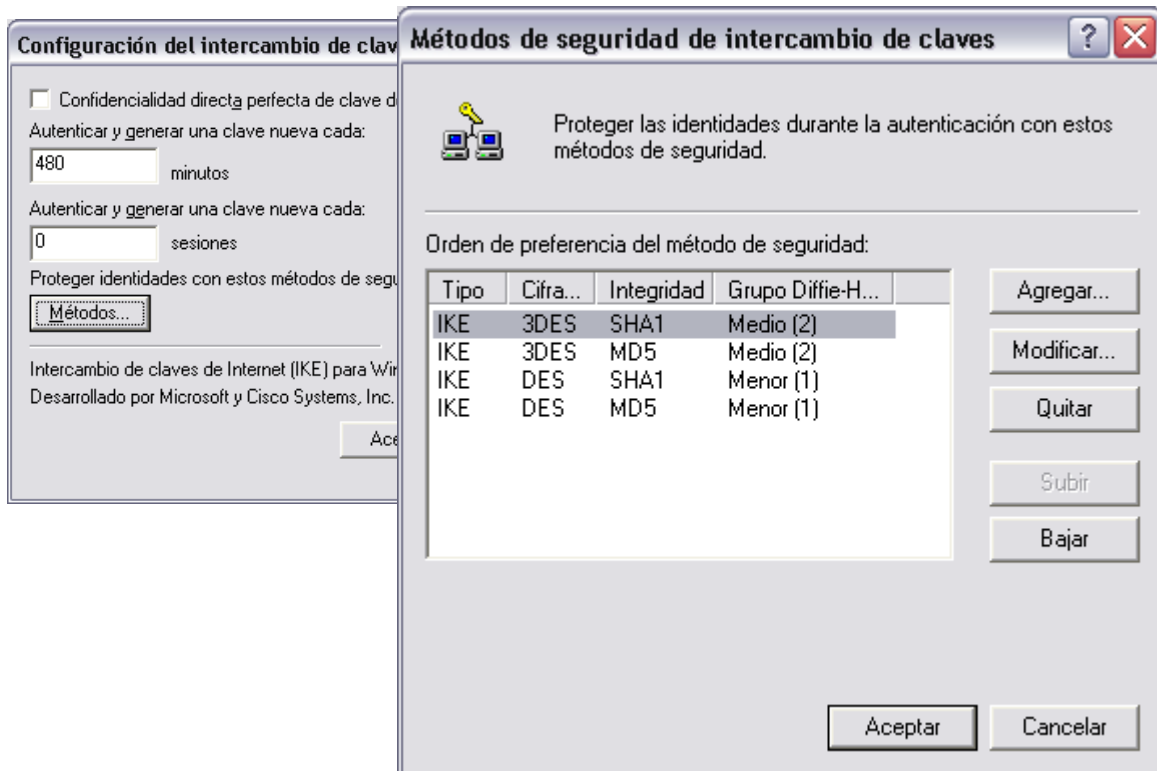
- Create a new IPsec policy for handling the communication with the 3GAT wireless router. It should be noted that when a new IPsec policy is created, it will not be assigned. Don't forget to assign it once it has already be defined.



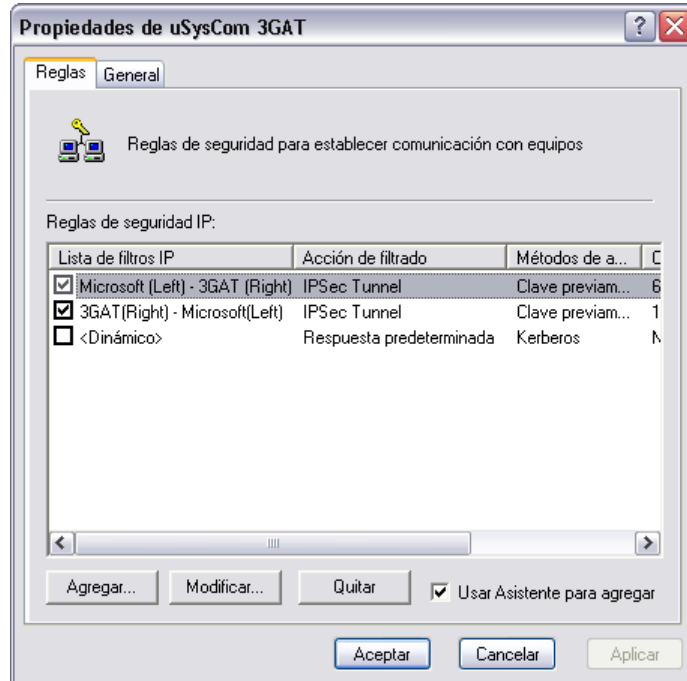
- *uSysCom 3GAT* security policy needs to define two different rules that will indicate how to handle data traffic from the Windows XP-based computer to the 3GAT and from the 3GAT to the Windows XP-based computer. Accessing the general tab – Advanced button, IKE parameters can be modified.



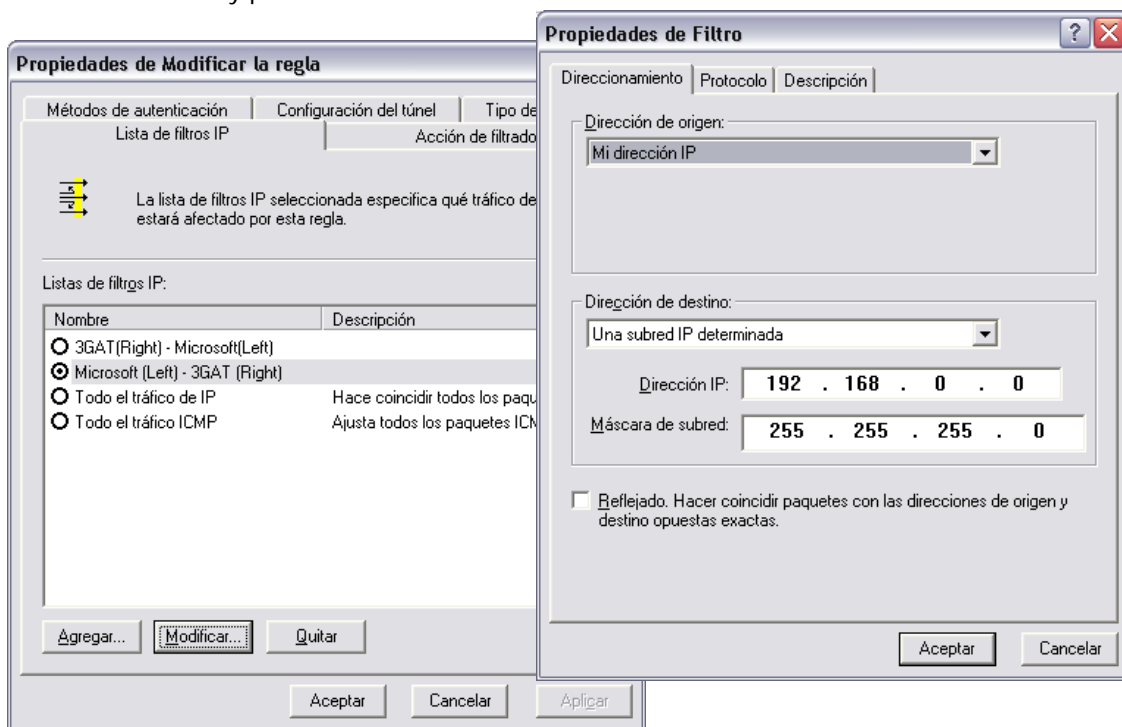
- We need to be sure that the IKE policy is properly configured.



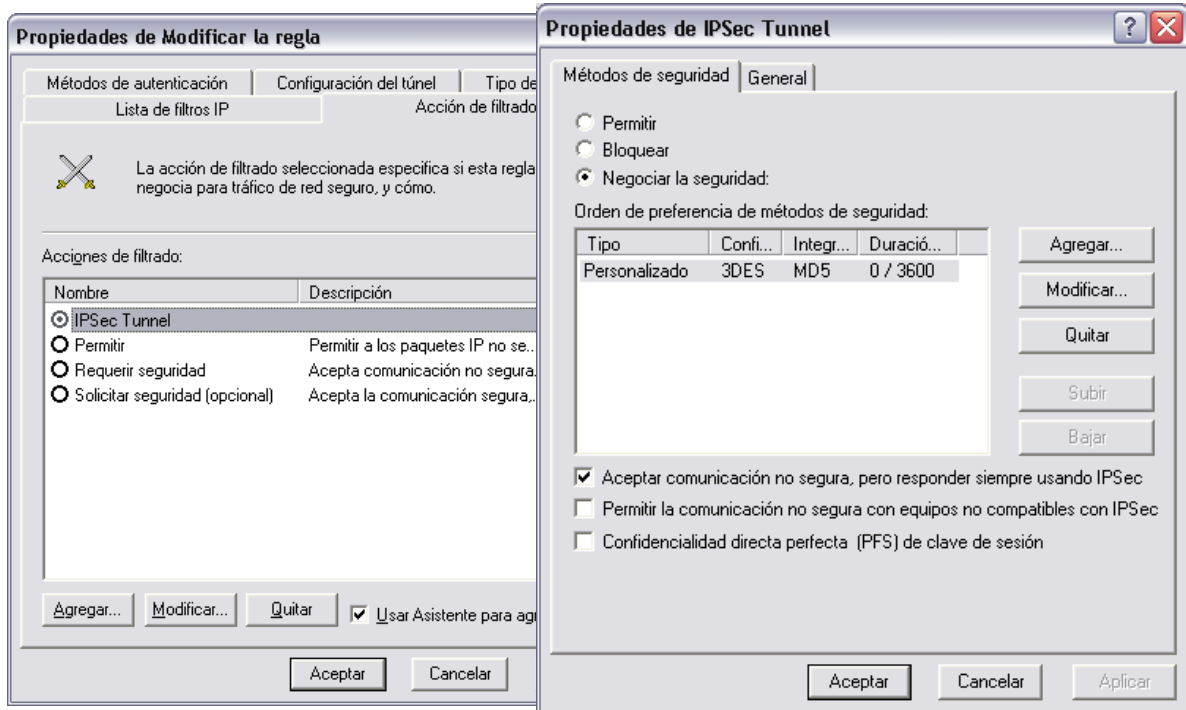
- As indicated above, two different rules are required.



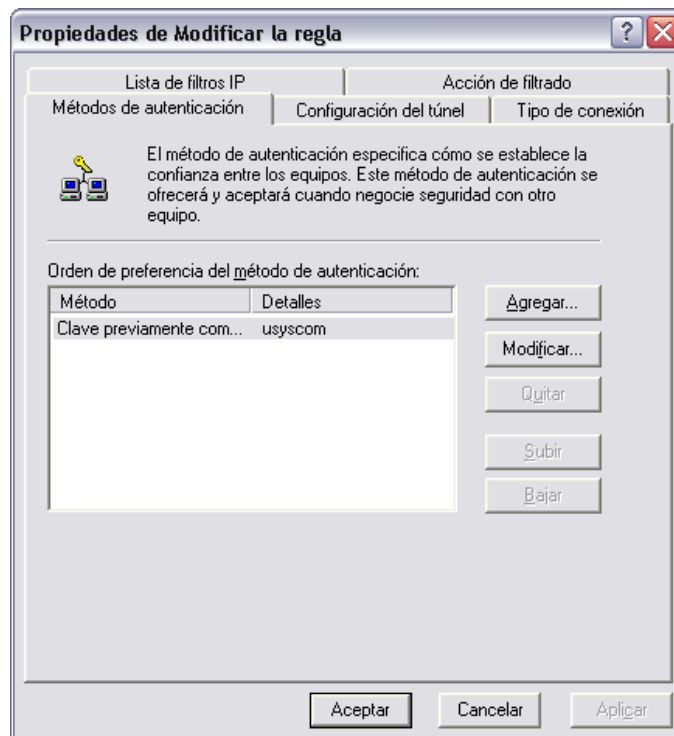
- Every rule defines both, the traffic to be protected and the IPSec tunnel parameters. The security rule for the traffic from *Windows XP to 3GAT* is defined as shown below:
  - First of all we need to define a **IP filter – Microsoft (Left) – 3GAT (Right)**. It will be defined by IP addresses as no special conditions are placed for restricting any protocol.



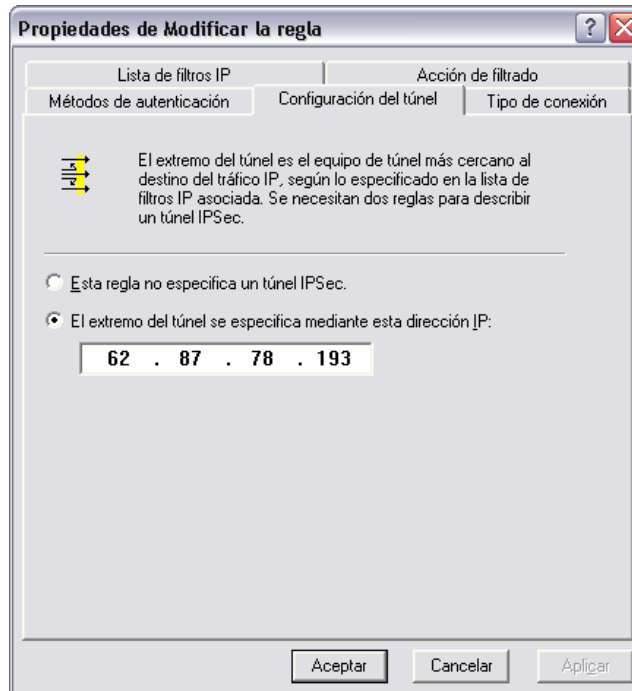
- b. We will define an action for above traffic list. We will call it **IPSec Tunnel**, as it basically define the tunnel policy. It is important to note that ESP protocol has been selected.



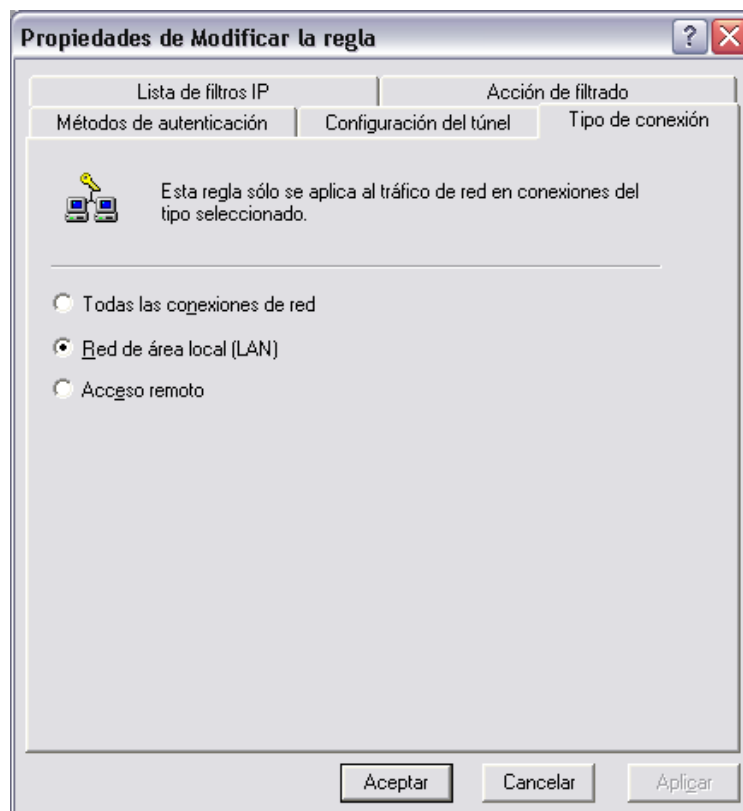
- c. The authentication method used is a pre-shared key of "usyscom", which is defined in the authentication methods tab.



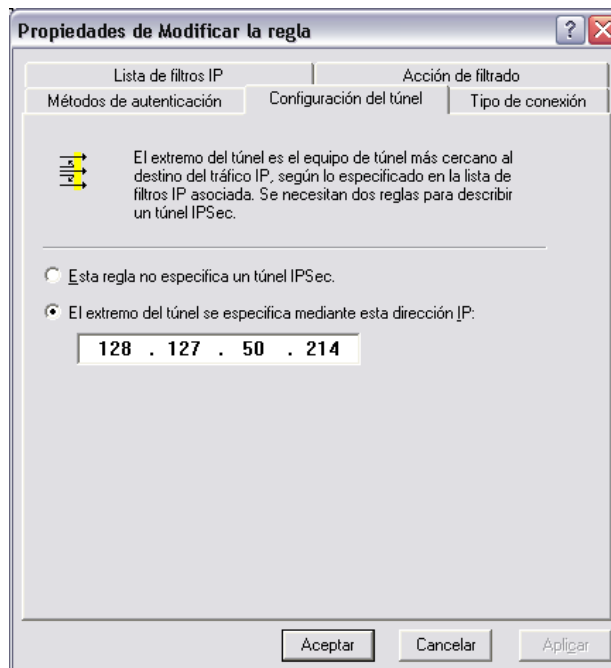
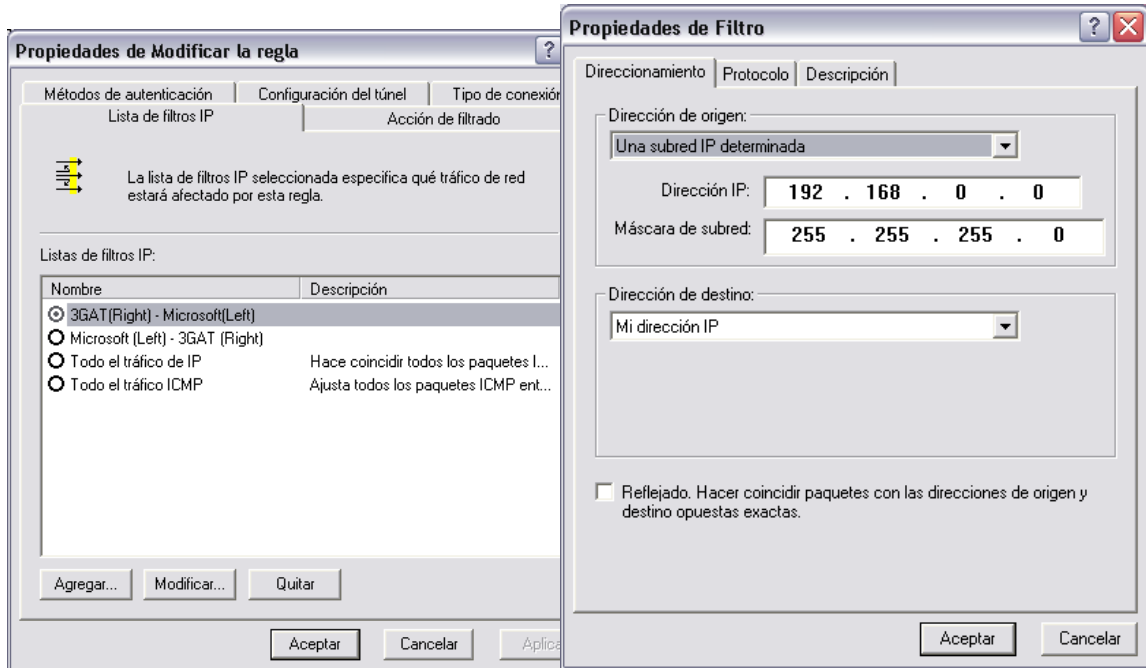
- d. In the tunnel configuration tab, the tunnel end-point is set.



- e. Finally, the type of connection should be set to LAN.



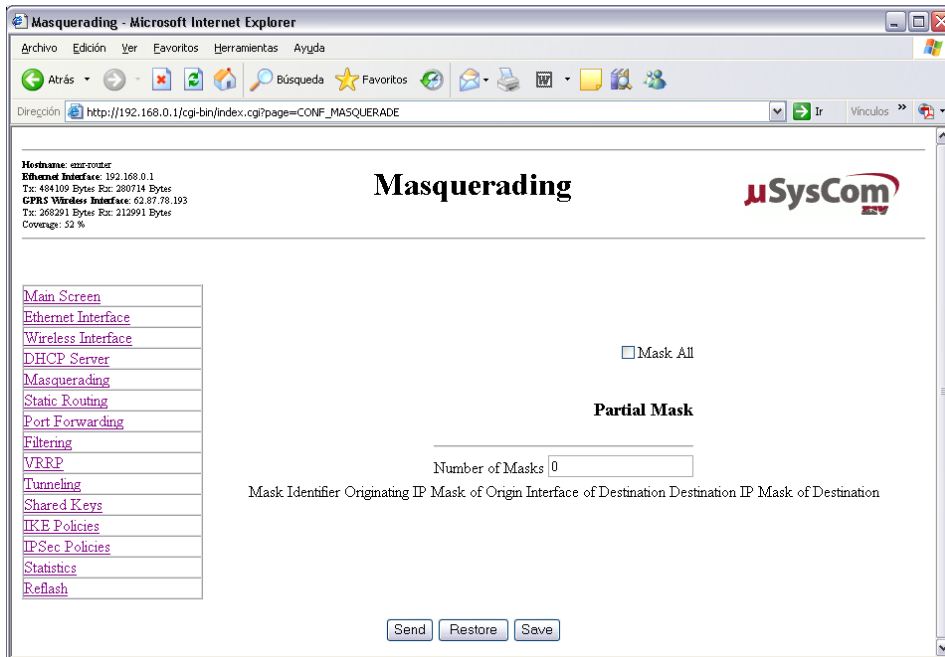
- The security rule for the traffic from *3GAT to Windows XP* is defined in a similar way. The only difference resides in the IP Filter (Traffic list) and the tunnel configuration. Both screenshots are depicted.



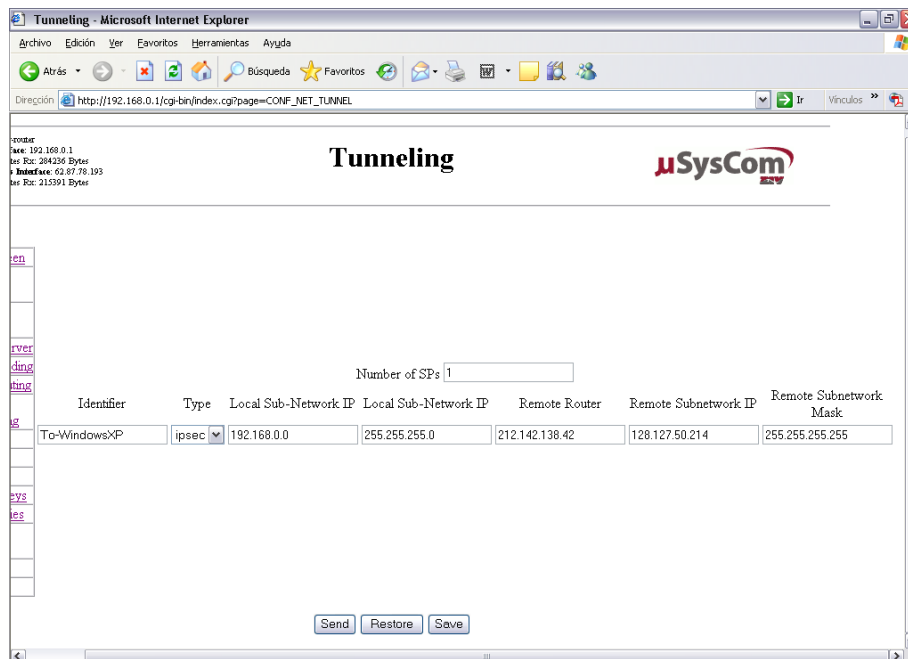
## 3GAT Configuration

This paragraph focuses on the IPSec configuration parameters. For additional info, please refer to the 3GAT SW Configuration Guide.

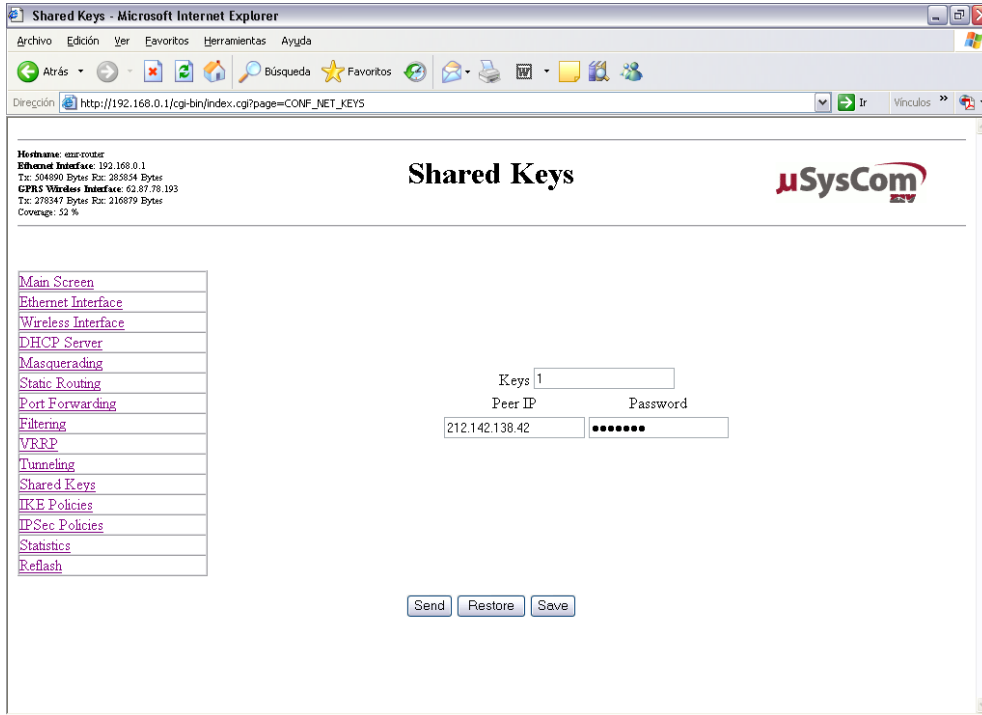
- First of all, it is important to verify that no masquerading rules are active. To do so, uncheck the mask all checkbox.



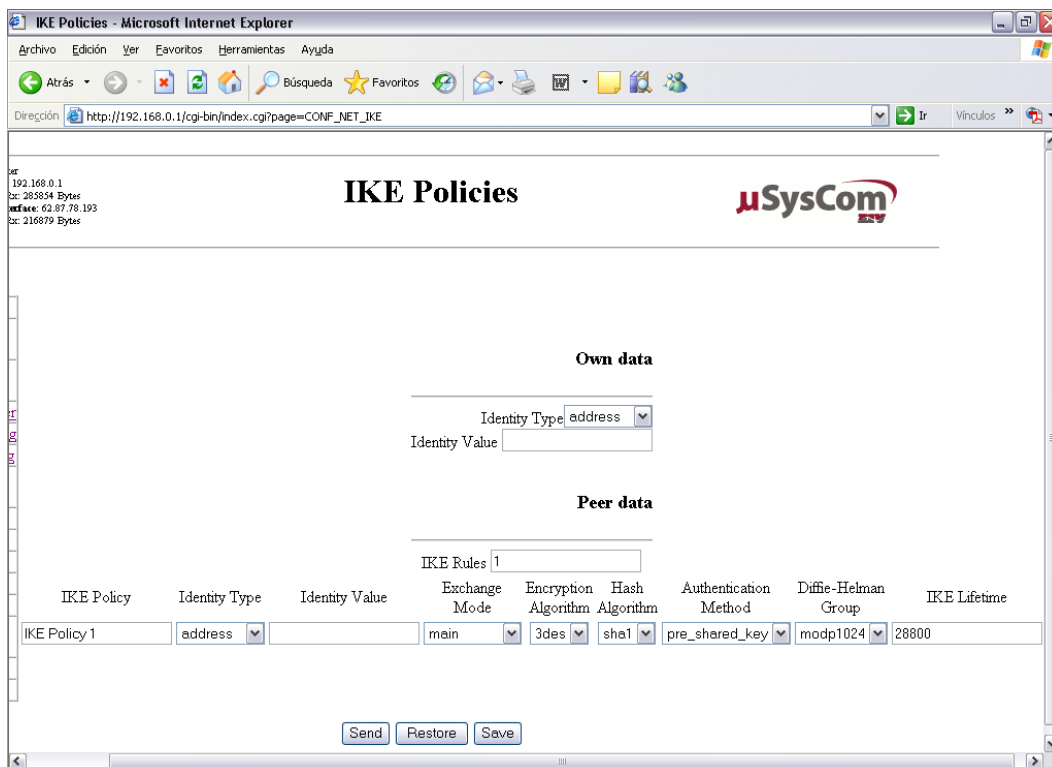
- Tunnel parameters need to be defined:



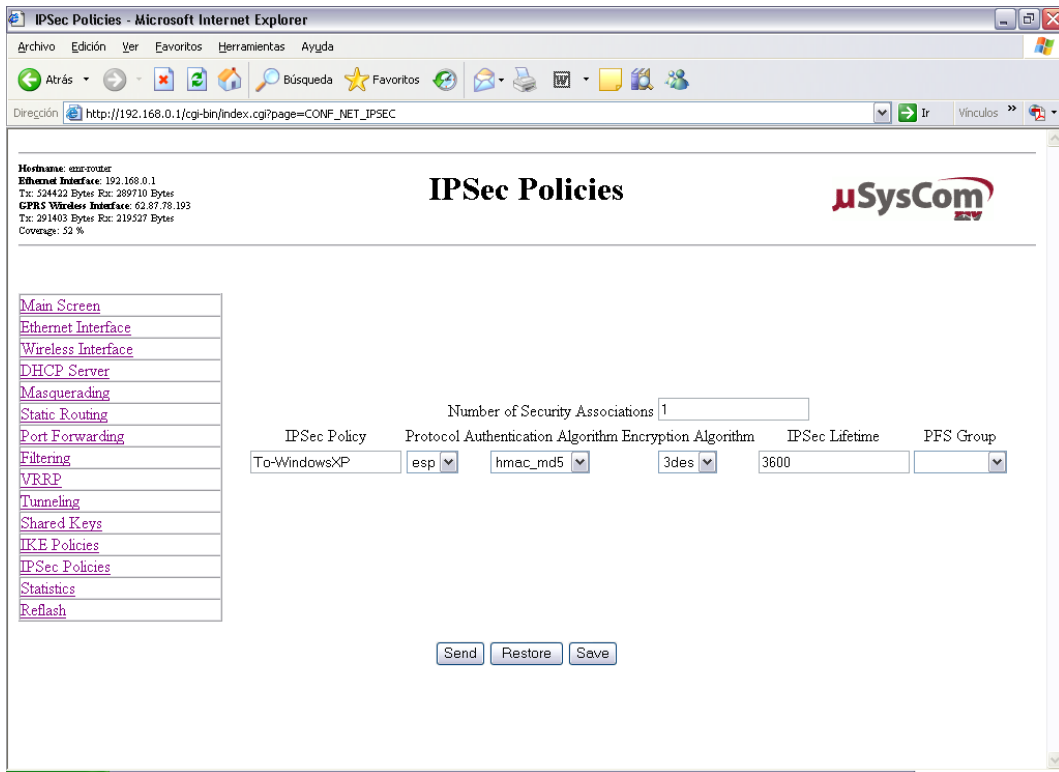
- “usyscom” preshared key is defined for the peer IP 212.142.138.42



- The IKE policy should reflect previously agreed parameters:

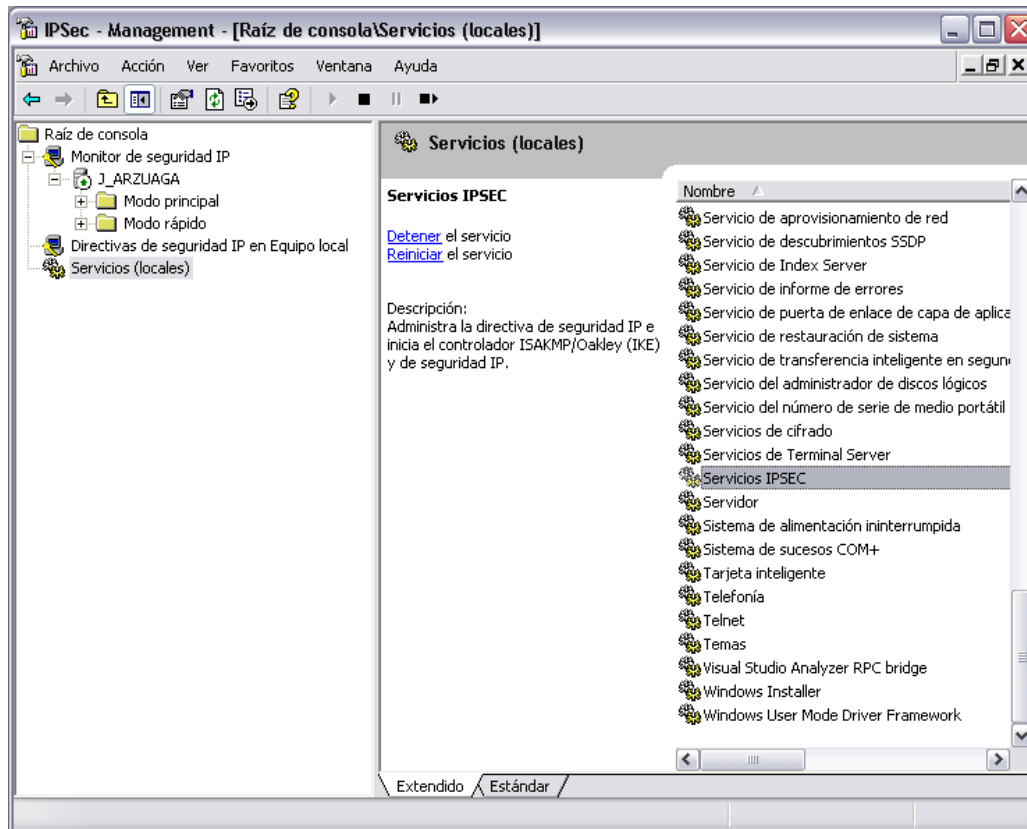


- Finally, IPSec tunnel policy should be configured for ESP protocol, being the authentication and ciphering algorithms MD5 and 3DES respectively.



## IPSec Tunnel / Established

Before testing the connection, be sure that the IPSEC Windows service is up and running.



To initiate the tunnel, send a ping from the Windows XP-based computer to the 192.168.0.1 IP address. Once the IP Security is successfully negotiated, the tunnel is established and the 192.168.0.0/24 subnetwork is accessible.

