
# TheGreenBow IPSec VPN Client

## Configuration Guide

## Efficient SpeedStream 5861

WebSite: http://www.thegreenbow.com

Contact: support@thegreenbow.com

# Table of contents

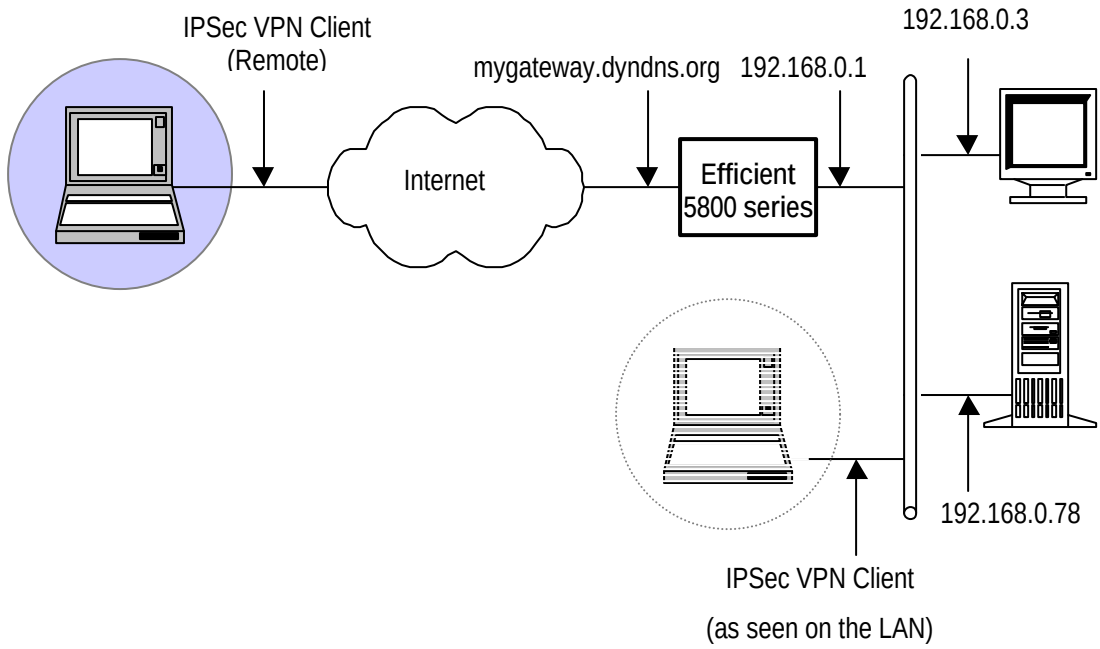
# 1 Introduction

## 1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Linksys WRV54G router.

## 1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Efficient SpeedStream 5800 router. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.



# 2 Efficient SpeedStream 5800 VPN Configuration

This section describes how to build an IPSec VPN configuration with your Efficient Network SpeedStream 5800 VPN router. For more details about how to configure an Efficient Network router, please see the documentation of the router.

Our tests and VPN configurations have been conducted using an Efficient Network SpeedStream 5861 VPN Router.

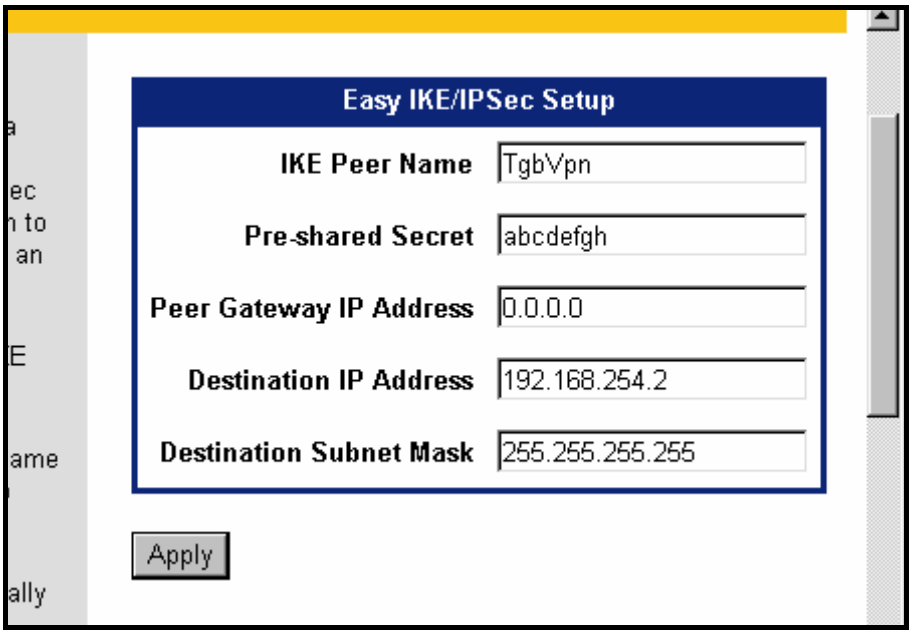
## 2.1 Efficient SpeedStream using the Wizard

Once connected to your VPN gateway, you must open the VPN Configuration of the router, click on the link "IKE/IPSec Configuration" on the home page of the internal WEB server of the router.

Click on "Easy IKE/IPSec Setup" and fill in the following fields:

| Field | Comment |
|---|---|
| IKE Peer Name | Name of the connection (doesn't matter) |
| Pre-shared Secret | Key shared between the VPN Client and the router |
| Peer Gateway IP Address | IP address of the remote host.<br>Since the Client get a dynamic IP address, this value must be set to 0.0.0.0 |
| Destination IP Address | Virtual IP address of the Client in the LAN behind the router.<br>This address must not belong to the LAN behind the router. |
| Destination Subnet Mask | Subnet mask associated with the virtual IP address of the VPN Client.<br>Since the station is unique, this mask must be set to 255.255.255.255. |

Example:




Click on "Apply" for the configuration being recorded.

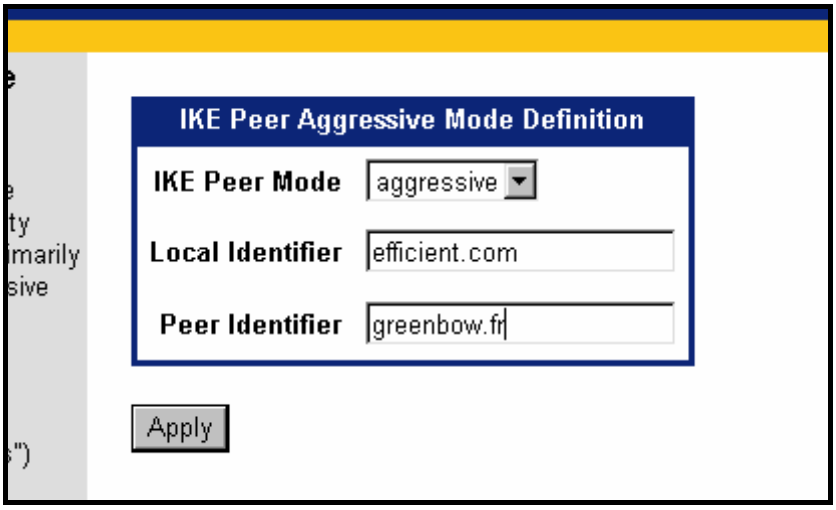
## 2.2 Efficient SpeedStream IKE mode

Since the router doesn't know the IP address of the VPN Client, the Aggressive mode must be configured.

In the section "IKE Peer", click on the link "Modify" located near "Main", and fill in the following fields:

| Field | Comment |
|---|---|
| IKE Peer Mode | Select "aggressive" |
| Local identifier | Identifier of the router (set for the VPN Client) |
| Peer Identifier | Identifier of the VPN Client (set for the router) |

Example:




Click on "Apply" for this configuration being recorded.

Restart the Efficient SpeedStream VPN router for these modifications being taken into account.

## 2.3 Efficient SpeedStream IKE/IPSec router configuration

### 2.3.1 SpeedStream "IKE Peers" Parameters

| Parameter | Comment | Value |
|---|---|---|
| Gateway | IP address of the TheGreenBow VPN Client | 0.0.0.0 |
| Secret | Pre-shared key used for authentication. | efficient |
| Mode | Initialization mode of the VPN connection | Aggressive |
| Local ID | Identifier of the router (set for the VPN Client) | efficient.com |
| Peer ID | Identifier of the VPN Client (set for the router) | thegreenbow.fr |

### 2.3.2 SpeedStream "IKE Proposals" Parameters

| Parameter | Comment | Value |
|---|---|---|
| Message | IP address of the TheGreenBow VPN Client | SHA-1 |
| Session authentication | Authentication mode between the Client and the router | PRE-SHARED |
| Phase 1 encryption | Encryption algorithm for the Phase 1 | 3-DES |
| Diffie-Hellman group | DH Authentication algorithm Group | Group 2 |

### 2.3.3 SpeedStream "IKE IPSec Proposals" Parameters

| Parameter | Comment | Value |
|---|---|---|
| AH authentication scheme | AH authentication algorithm | None |
| ESP authentication scheme | ESP authentication algorithm | SHA-1 |
| ESP encryption scheme | ESP encryption algorithm | DES-CBC |
| Compression scheme | Compression | None |

### 2.3.4 SpeedStream "IKE IPSec Policies" Parameters

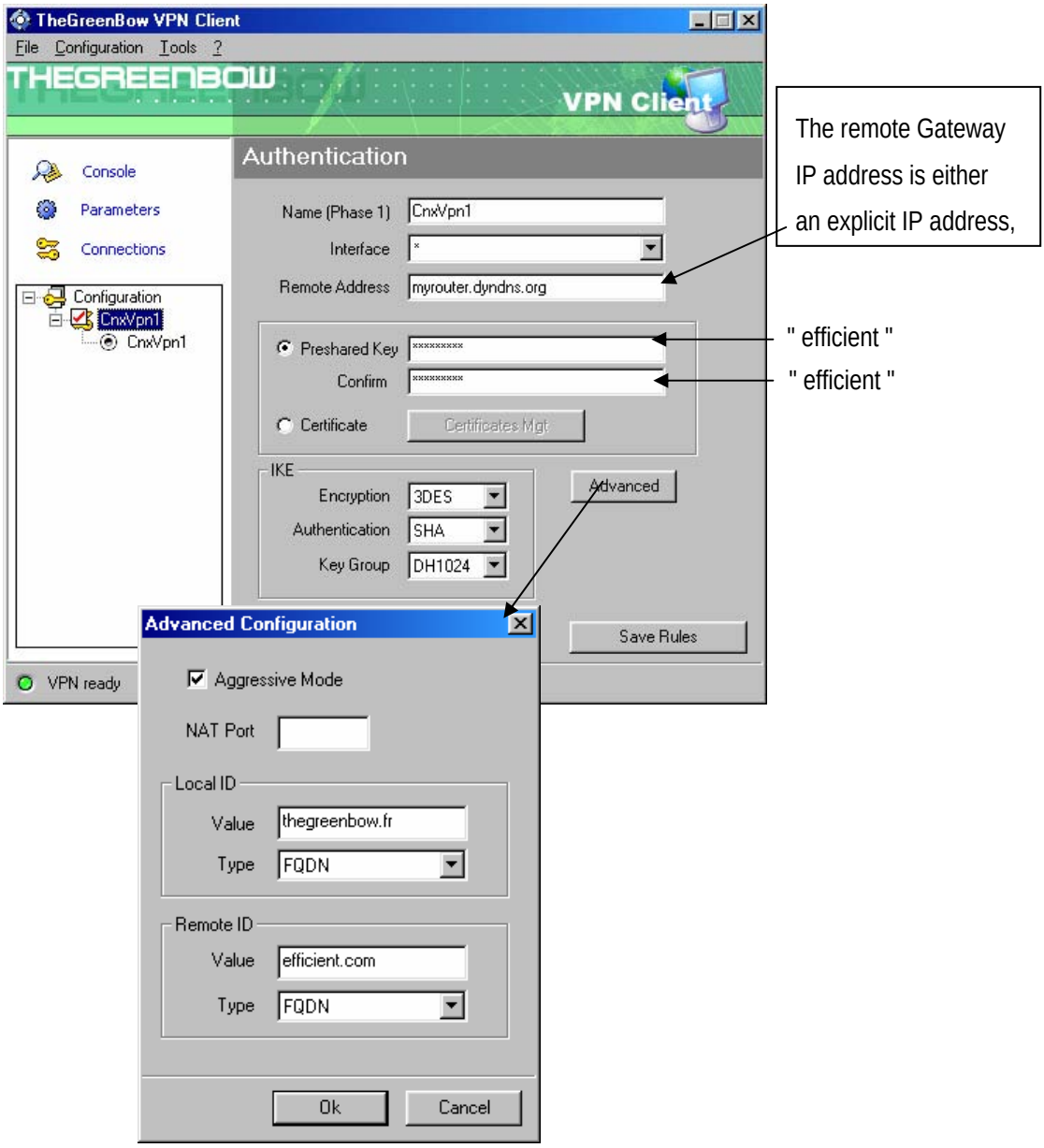
| Parameter | Comment | Value |
|---|---|---|
| Source IP address | Network IP address range the client can reach | 192.168.253.254 |
| Source IP mask | Network IP mask the client can reach | 255.255.255.0 |
| Destination IP address | IP address of the client in the local area network | 192.168.254.2 |
| Destination IP mask | IP mask of the client in the local area network | 255.255.255.255 |

# 3 TheGreenBow IPSec VPN Client configuration

## 3.1 VPN Client Phase 1 (IKE) Configuration

Note: If the IP address of the VPN Client is automatically assigned, select "**Interface**" = " * "

| Phase 1 Configuration | Efficient Section | Efficient Parameter |
|---|---|---|
| Preshared Key (ad Confirm) | IKE Peers | Secret |
| IKE Encryption | IKE Proposals | Phase 1 encryption |
| IKE Authentication | IKE Proposals | Message |
| IKE Key Group | IKE Proposals | Diffie-Hellman group |
| Advanced Aggressive Mode | IKE Peers | Mode |
| Advanced Local ID Value | IKE Peers | Peer ID |
| Advanced Remote ID Value | IKE Peers | Local ID |



## 3.2 TheGreenBow VPN Client Phase 2 (IPSec) Configuration

| Phase 2 Configuration | Efficient Section | Efficient Parameter |
|---|---|---|
| Local Address | IKE IPSec Policies | Destination IP Address |
| Network Address | IKE IPSec Policies | Source IP Address |
| Subnet Mask | IKE IPSec Policies | Source IP Mask |
| ESP Encryption | IKE IPSec Proposals | ESP encryption scheme |
| ESP Authentication | IKE IPSec Proposals | ESP authentication scheme |


Phase 2 Configuration

## 3.3 Open IPSec VPN tunnels

Once both Efficient SpeedStream router and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

1. Click on "Save Rules" to take into account all modifications we've made on your VPN Client configuration

2. Click on "Open Tunnel", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)

3. Select "Connections" to see opened VPN Tunnels

4. Select "Console" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging.

# 4 Contacts

News and updates on TheGreenBow web site : http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts at +33 1 43 12 39 37 ou by email at info@thegreenbow.com