Greenbow VPN Client with Teldat VPN Server

Configuration Highlights

INDEX

1. The Simulation Scenario

In order to validate the correct operation of the Greenbow VPN Client with the Teldat VPN Server, the following simulation scenario has been implemented:

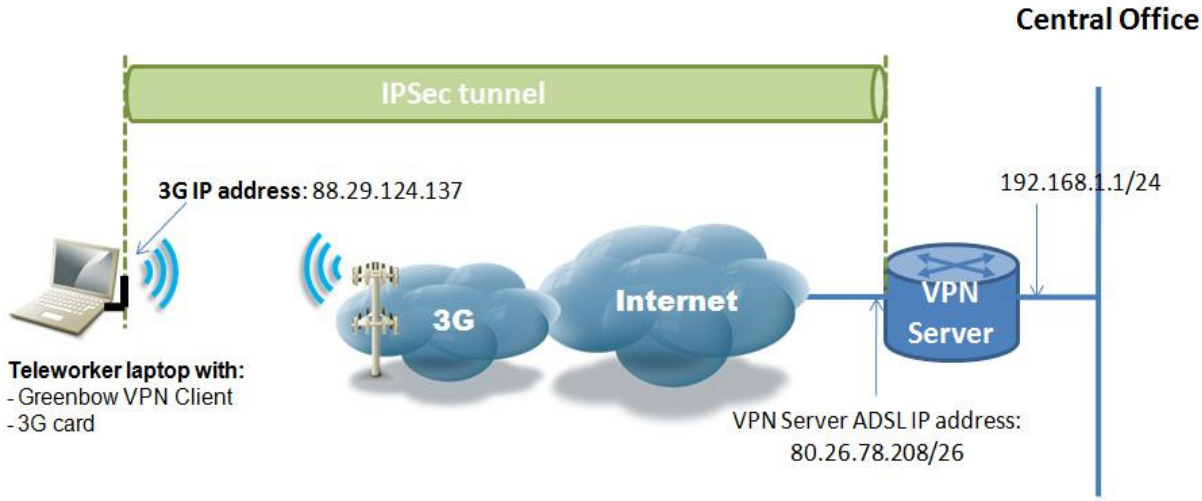

Figure 1. Simulation network diagram

The Greenbow VPN Client is installed in the Teleworker laptop, which can access the Internet through a 3G card installed in it. The IP address obtained from the 3G provider is 88.29.124.137 and the Greenbow software version is the following:

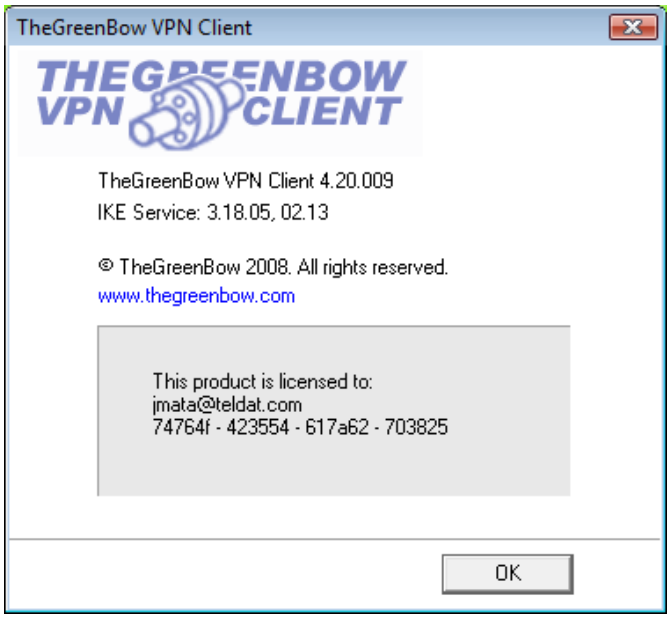

Figure 2. Greenbow VPN Client product version

The VPN Server can be any Teldat router with the IPSec software license activated.

2. Greenbow VPN Client configuration

The Teldat VPN server is connected to an ADSL line in the public IP address 80.26.78.208, as depicted in Figure 1. This IP address is set as the Remote Gateway IP address in the Greenbow VPN client Phase one configuration, as shown in Figure 3.
The secret code used for this simulation is ***teldat***. The IKE encryption parameters are the ones shown in Figure 3.

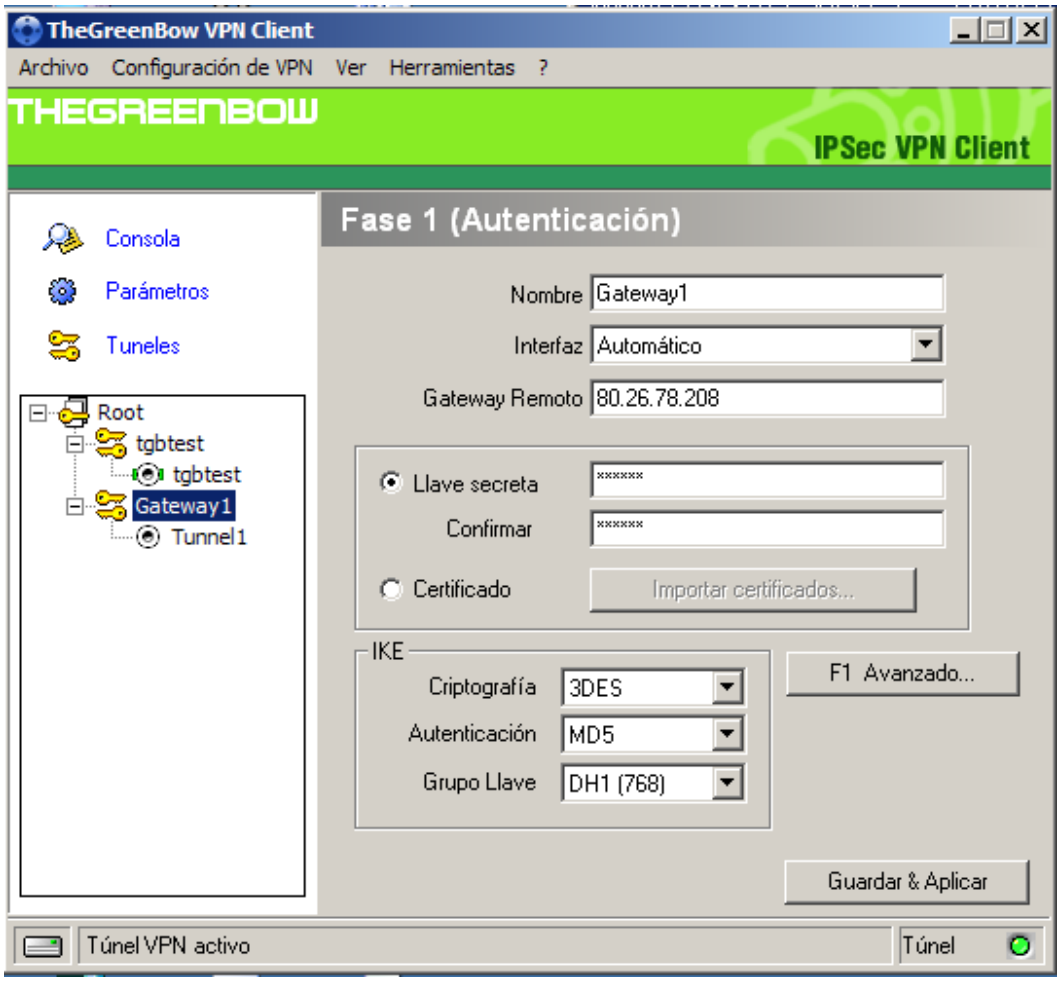

Figure 3. Greenbow Phase 1 configuration

In the Phase two configuration (Figure 4) we need to configure the IP address assigned to the teleworker laptop 3G interface (88.29.124.137 in Figure 1), since it will be the source IP address of the Greenbow IPSec packets received into the VPN Server.
In this example, the Greenbow VPN access is granted to a single private host in the Central Office, the one at 192.168.1.1. In this simulation scenario, this IP address is actually the one assigned to the VPN Server Ethernet port.
In a more realistic scenario, the host at 192.168.1.1 could be located anywhere in the Central Office LAN network. Once the VPN tunnel has been established, the Greenbow

VPN Client will be able to contact its host as long as the VPN Server has IP connectivity to it.

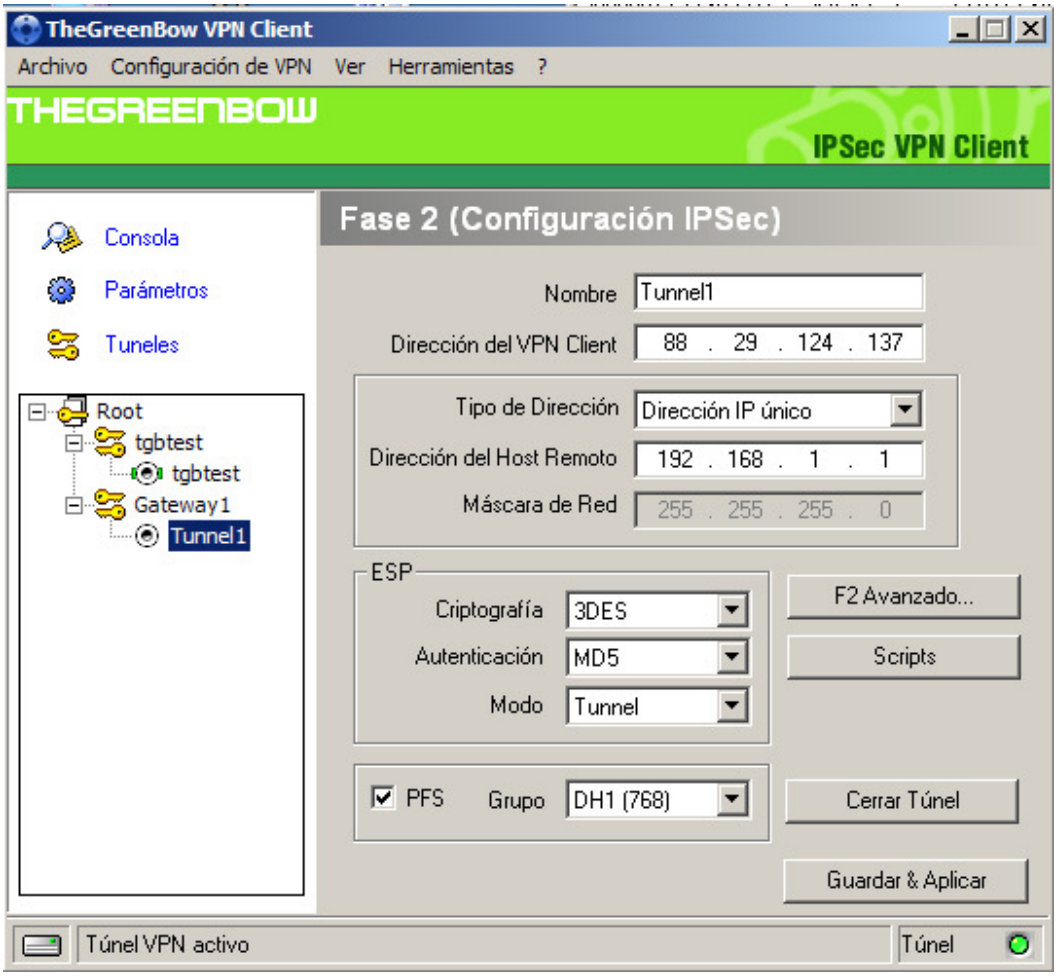

Figure 4. Greenbow Phase 2 configuration

3. Teldat VPN Server configuration

3.1 Basic router configuration

First of all, we can customize the Teldat VPN Server router, giving it a hostname and defining the communication interfaces. The following parameters are hence configured:

1. The router hostname can be any character string (*VPN_Server* in this example).
2. The router user login and password for an authenticated console access.
3. The ADSL interface configuration.
4. The IP addresses, the default route to the ADSL and the NAPT configuration.

3.2 IPSec configuration

First of all, the VPN Client IP address (88.29.124.137) is set as the destination address in an extended Access List of the VPN Server. Teldat extended access-lists are the ones which identifier is set to the integer value in the interval from 100 to 1999. The VPN Server uses this Access List to build the Security Policy DataBase (SPD) of the IPSec tunnel with the Greenbow VPN Client. The SPD is negotiated during the VPN Phase-two negotiation.

Then, we can access the Teldat IPSec configuration section where we will set:

1. The Phase one encryption parameters are set in the ISAKMP template (**`template 1`** commands in the text configuration below). The command **`template 1 udp-encapsulation`** forces the IPSec packets to be encapsulated in UDP so they can traverse Firewalls and NAPT without having the IPSec modified.
2. The Phase two encryption parameters are set in the Dynamic template (i.e. **`template 2`** commands in the text configuration below). The IP addresses of the VPN tunnel edges are also set in the Dynamic template.
3. We assign the Access List to the Dynamic template.
4. We configure the preshared key for the Greenbow VPN Client to ***teldat***, as it is set in the Greebow Phase one configuration.

The complete VPN Server test configuration will be as follows:

```
; Showing System Configuration ...
; Router XX IPSec Y ZZ Version VVVVV

no configuration

add device atm-subinterface atm0/0 1
set hostname VPN_Server
user PTadmin password teldatcli
feature access-lists
; -- Access Lists user configuration --
   access-list 100
;
      entry 1 default
      entry 1 permit
      entry 1 destination address 88.29.124.137 255.255.255.255
;
   exit
;
exit
;
network atm0/0
; -- ATM interface configuration --
   aal-connection 1 pvc 8 32
;
```

```
   pvc 8 32 default
;
exit
;
network atm0/0.1
; -- ATM subinterface configuration --
   aal-connection-requested 1 default
;
exit
;
protocol ip
; -- Internet protocol user configuration --
   address ethernet0/0 192.168.1.1 255.255.255.0
   address atm0/0.1 80.26.78.208 255.255.255.192
;
;
   route 0.0.0.0 0.0.0.0 80.26.78.208 1
;
   rule 1 default
   rule 1 local-ip 80.26.78.208
   rule 1 napt translation
;
   classless
;
   ipsec
; -- IPSec user configuration --
      enable
      assign-access-list 100
;
      template 1 default
      template 1 isakmp tdes md5
      template 1 udp-encapsulation
;
      template 2 default
      template 2 dynamic esp tdes md5
      template 2 source-address 80.26.78.208
      template 2 destination-address 88.29.124.137
      template 2 life type both
;
      map-template 100 2
      key preshared ip 88.29.124.137 plain teldat
   exit
;
exit
;
; --- end ---
```

Teldat VPN Server text configuration