TheGreenBow IPSec VPN Client

Configuration Guide

Netscreen NS-5GT

WebSite: http://www.thegreenbow.com
Contact: support@thegreenbow.com

Table of contents

1 Introduction

1.1 Goal of this document

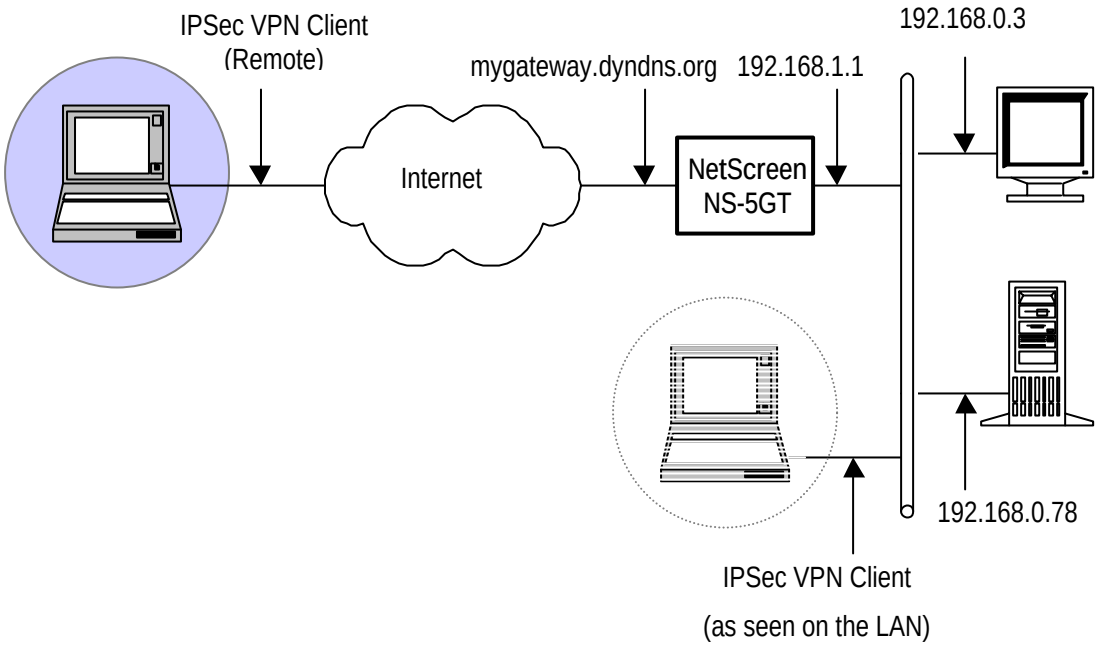
This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a NetScreen NS-5GT VPN router.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the NetScreen NS-5GT 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.

In our example, we will configure a VPN tunnel with the following settings:

- Netscreen WAN IP address will be 195.100.205.115 (mygateway.dyndns.org)
- Netscreen LAN IP network address will be 192.168.1.1/24



1.3 Netscreen NS-5GT Restrictions

Depending on the firmware version, Netscreen NS-5GT VPN router may not support virtual IP address. Please check on Netscreen website for newer firmware.

2 Netscreen NS-5GT VPN Configuration

This section describes the VPN configuration of a Netscreen NS-5GT VPN gateway in order to open IPSec VPN tunnels with the TheGreenBow IPSec VPN Client. Read Netscreen documentation for more details about these VPN gateways (i.e. "Vol. 4 VPNs" in Netscreen's documentation).

2.1 Netscreen Interfaces – Security Zones

Go to Network > Interfaces and edit WAN and LAN interfaces with the appropriate IP addresses values.

Name	IP/Netmask	Zone	Type	Link	Configure	
trust	192.168.1.1/24	Trust	Layer3	up	Edit	
untrust	195.100.205.115/24	Untrust	Layer3	up	Edit	

2.2 Netscreen Address

Go to *Objects* > *Addresses* > *List* > *New*

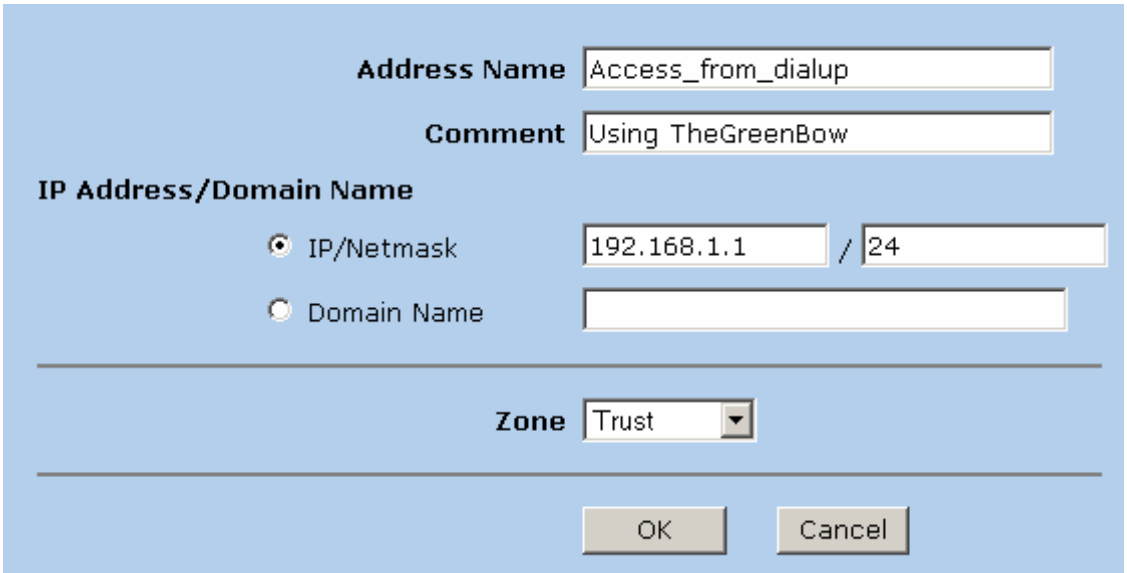
Address Name: Access_from_dialup

IP Address/Domain Name:

IP/Netmask: 192.168.1.1/24

Zone: Trust (LAN interface)

Click on OK when finished.

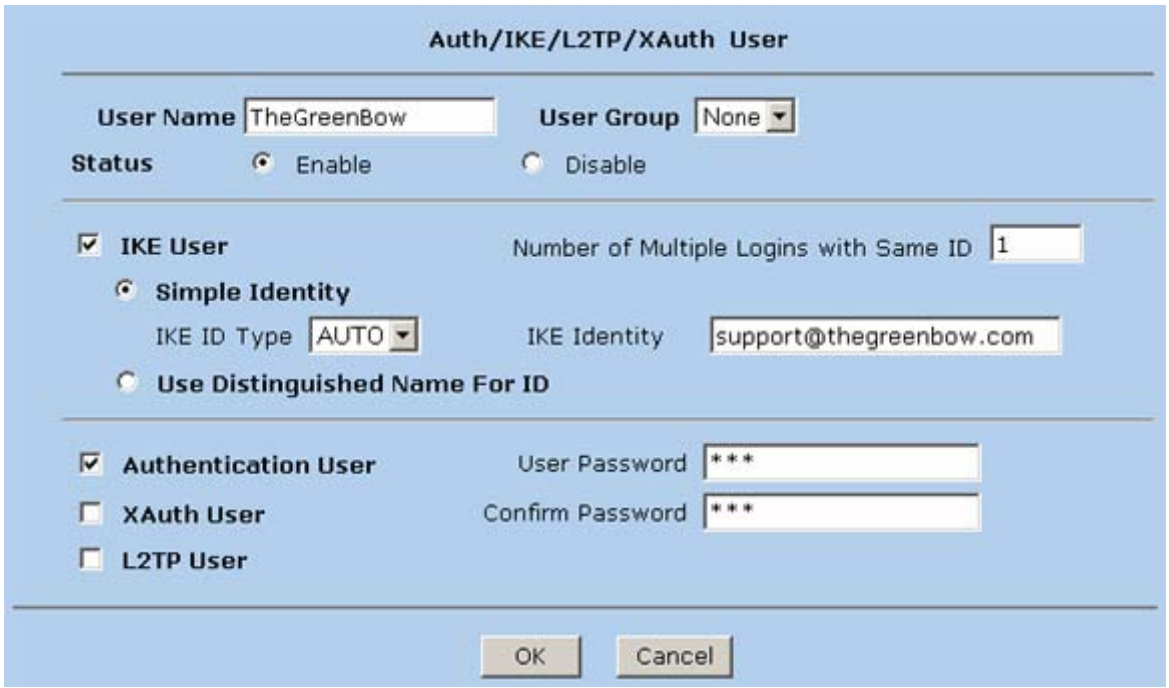


2.3 Netscreen User

Go to *Objects* > *Users* > *Local* > *New* :

User Name:	TheGreenBow
Status:	select "enable"
IKE User:	Select "IKE User"
	Select "Simple Identity"
	Fill in "IKE identity" with support@thegreenbow.com
Authentication User:	give a password

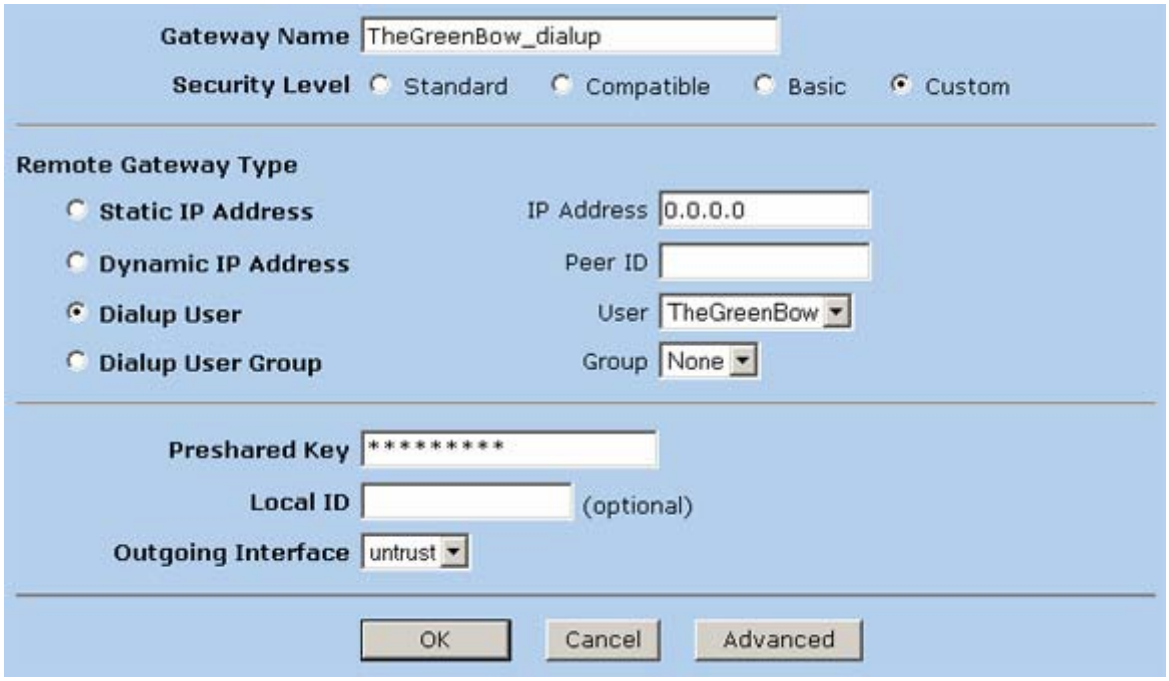
In our example, we will use a basic authentication for the user that will be activated by a prompt. Click on OK when finished.



2.4 Netscreen VPN

Go to *VPN* > *Autokey Advanced* > *Gateway* > *New*:

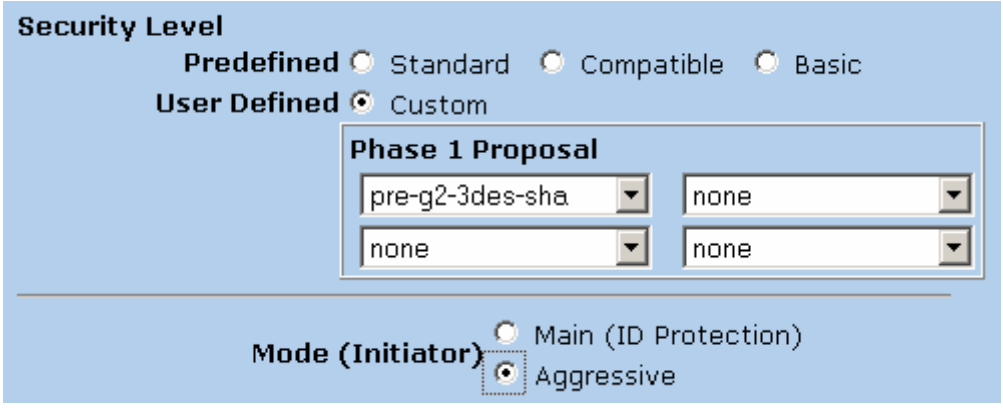
Gateway Name:	"TheGreenBow_dialup"
Security Level:	select "custom"
Remote Gateway Type:	Select "Dialup User"
	Select user "TheGreenBow"
Preshared key:	"123456789"
Outgoing Interface:	"untrust" (WAN interface).



Click then on "Advanced":

Security Level:	select "Custom"
Phase 1 Proposal:	select a "Proposal"
Mode:	select "Agressive"

In our example, we have chosen preshared key (pre), Diffie-Hellman 1024 as key group (g2), 3DES as encryption algorithm and SHA as authentication algorithm.

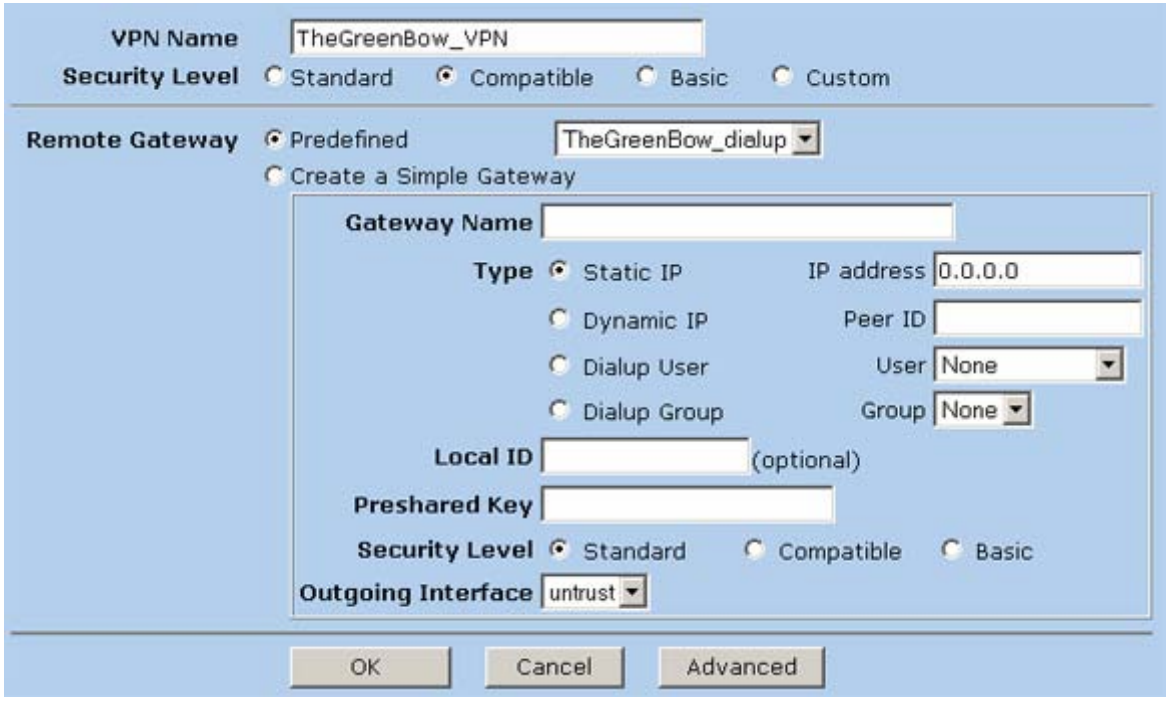


Go to *VPNs* > *AutoKey IKE* > *New*:

VPN Name: "TheGreenBow_VPN"

Security Level: select "Compatible"

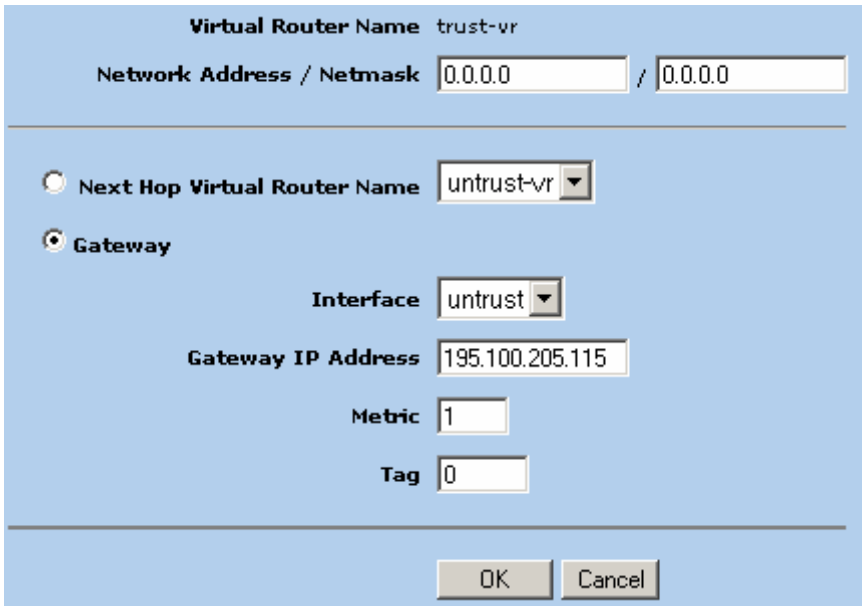
Remote Gateway: select "TheGreenBow_dialup"



2.5 Netscreen Route

Go to *Network* > *Routing* > *Routing Table* > *trust-vr* (LAN virtual route):

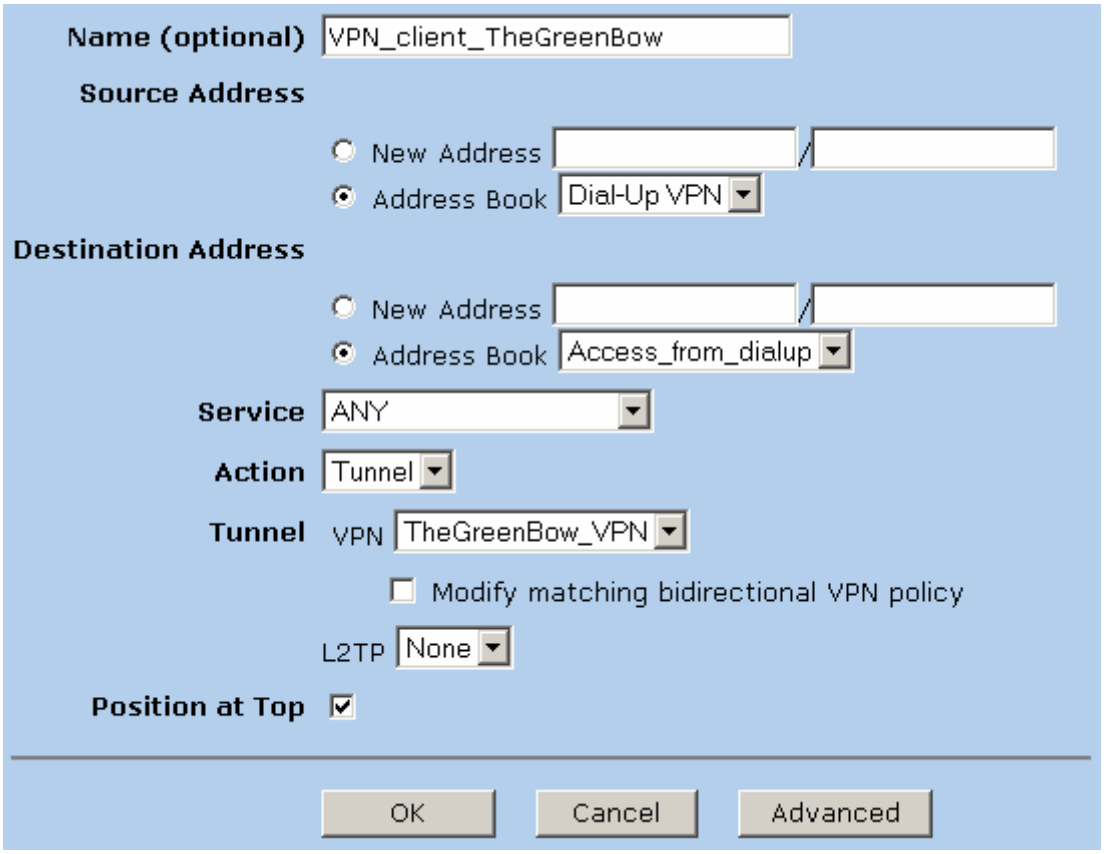
Network Address/Netmask: 0.0.0.0/0
Gateway: checked
Interface: untrust (WAN interface)
Gateway IP Address: 195.100.205.115 (WAN IP address)



2.6 Netscreen Policy

Go to *Policies*. Select From: *Untrust* and To: *Trust*. Click on *New*.

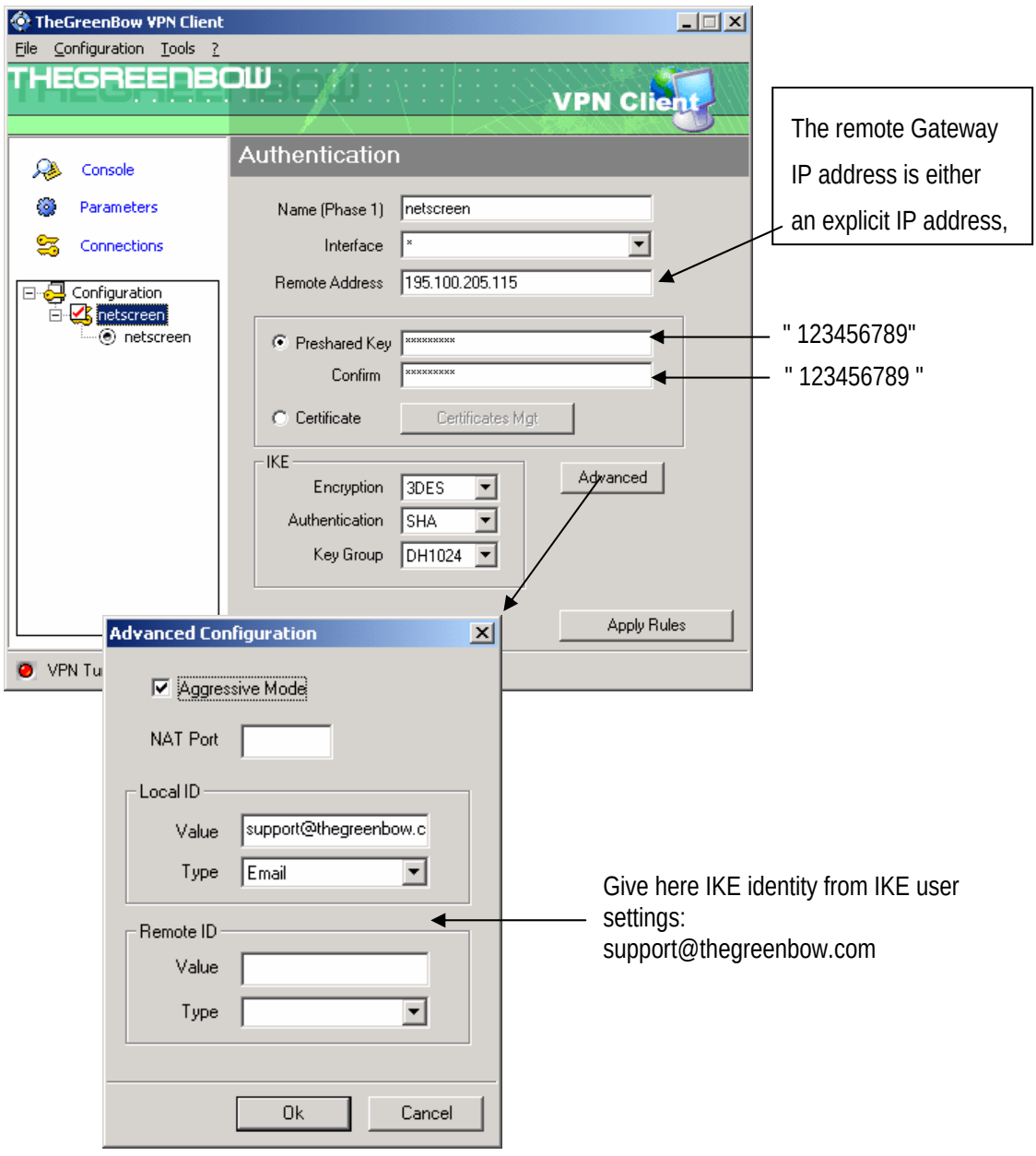
Source Address:	select "Dial-up VPN" in "Address Book"
Destination Address:	select "Access from dialup" in "Address Book"
Service:	select ANY
Action:	select Tunnel
Tunnel VPN:	select TheGreenBow_VPN
Modify matching VPN policy:	clear
Position on Top:	checked



3 TheGreenBow 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 = " * "



3.2 VPN Client Phase 2 (IPSec) Configuration

IP address given in "Local Address" will not be used because Netscreen NS-5GT VPN Gateway does not support virtual IP address.

Phase 2 Configuration

3.3 Establishing IPSec VPN tunnels

Once both Linksys WRV54G 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.

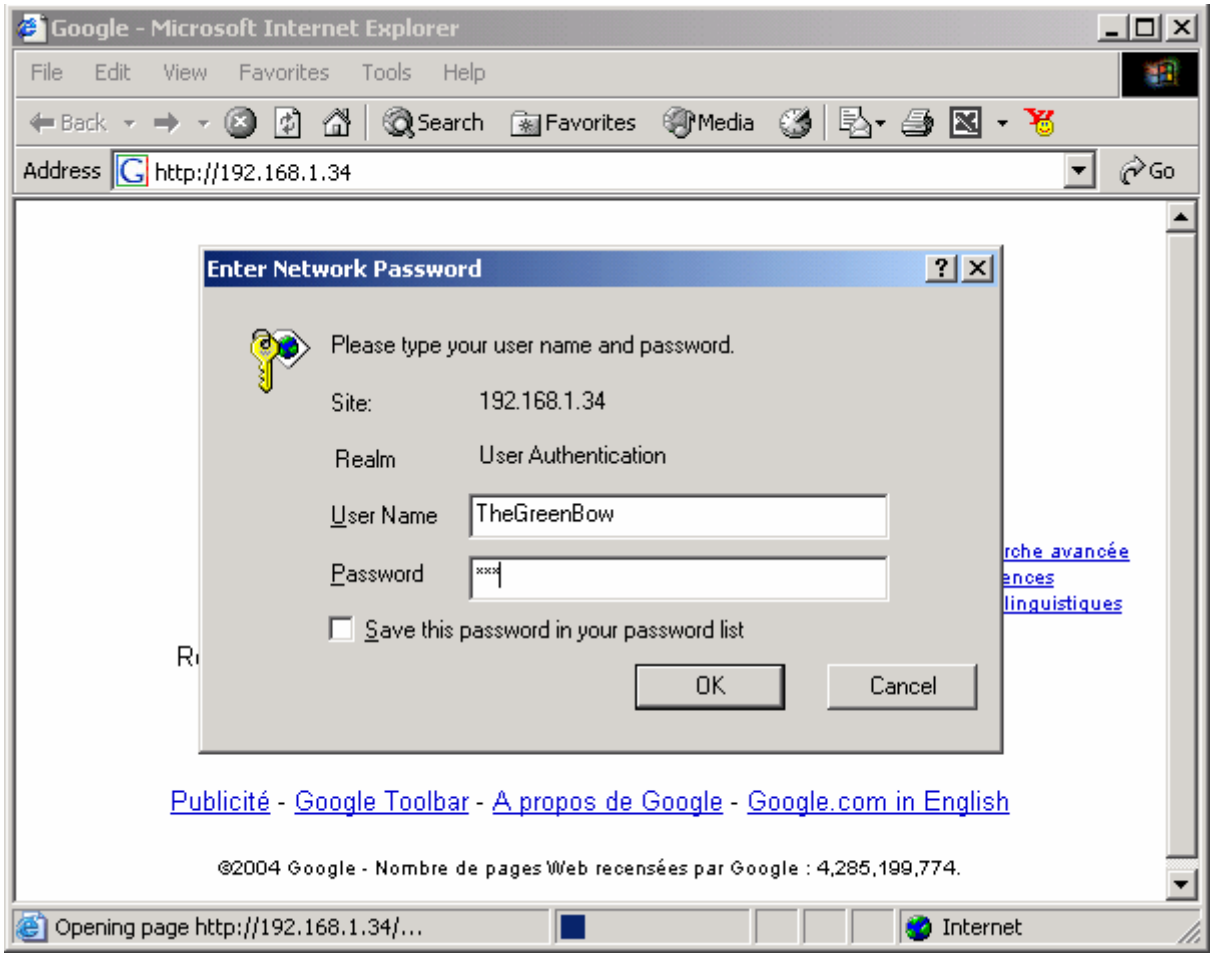
1. Click on " Apply Rules" to take into account all modifications we've made on your VPN Client configuration

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

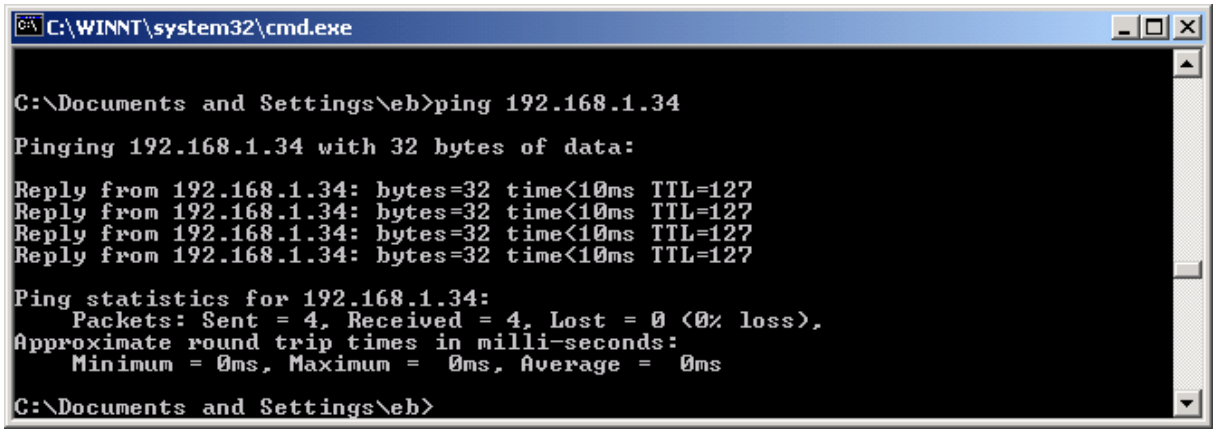
3. Select "Connections" to see opened VPN Tunnels

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

If you want to access a computer into Netscreen LAN, you will have to answer to an authentication prompt:



Once user is authenticated, he can ping and browse the LAN. This authentication is mandatory.



4 VPN IPSec Troubleshooting

Those error samples have been voluntarily produced with a Linksys WRV54G, but logs and messaging shall be exactly the same with a Netscreen NS-5GT VPN Gateway.

4.1 « PAYLOAD MALFORMED » error

```
114920 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification
type PAYLOAD_MALFORMED
114920 Default SEND Informational  [NOTIFY] with PAYLOAD_MALFORMED error
```

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

4.2 « INVALID COOKIE » error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOKIE
115933 Default SEND Informational  [NOTIFY] with INVALID_COOKIE error
```

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

4.3 « no keystate » error

```
115315 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

4.4 « received remote ID other than expected » error

```
120348 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
support@thegreenbow.fr
```

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.

4.5 « NO PROPOSAL CHOSEN » error

```
115911 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915    Default    (SA    WRV54G-WRV54G-P2)    SEND    phase    2    Quick    Mode
[SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational  [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational  [HASH][DEL]
115915 Default WRV54G-P1 deleted
```

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

```
115911 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

4.6 « INVALID ID INFORMATION » error

```
122623 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626    Default    (SA    WRV54G-WRV54G-P2)    SEND    phase    2    Quick    Mode
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational  [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default WRV54G-P1 deleted
```

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type (“Subnet address” and “Single address”). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

4.7 I clicked on “Open tunnel”, but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500 and protocol ESP (protocol 50).

4.8 The VPN tunnel is up but I can’t ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP

- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal for example). You will have an indication that encryption works.
- Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no “Default gateway” setting.
- You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- We recommend you to install ethereal (http://www.ethereal.com) on one of your target computer. You can check that your pings arrive inside the LAN.

5 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