TheGreenBow IPSec VPN Client

Configuration Guide

Zyxel Zywall USG 300

WebSite: http://www.thegreenbow.com

Contact: support@thegreenbow.com

Table of contents

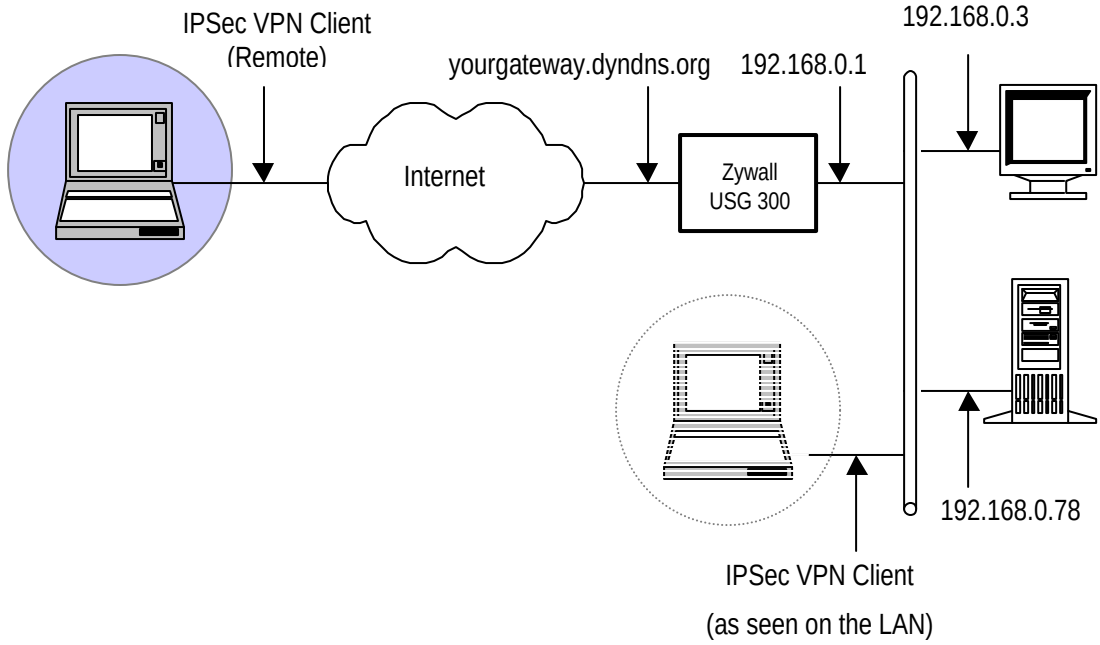
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Zyxel Zywall USG 300 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 Zyxel Zywall USG 300 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.



1.3 Zyxel Zywall USG 300 Restrictions

No known restrictions.

1.4 Zyxel Zywall USG 300 VPN Gateway

Our tests and VPN configuration have been conducted with Zyxel Zywall USG 300 firmware release 2.01(AQE.2).

1.5 Zyxel Zywall USG 300 VPN Gateway product info

It is critical that users find all necessary information about Zyxel Zywall USG 300 VPN Gateway. All product info, User Guide and knowledge base for the Zyxel Zywall USG 300 VPN Gateway can be found on the Zyxel Zywall USG 300 website: www.zyxel.com

Zywall USG 300 Product page	http://us.zyxel.com/web/product_family_detail.php?PC1indexflag=20040908175941&CategoryGroupNo=PDCA2007126
Zywall USG 300 User Guide	http://dl01.zyxel.com/DownloadLibary_ShortName/ZyWALL_USG_300/user_guide/ZyWALL%20USG%20300_1.00_Ed2.pdf
Zywall USG 300 FAQ/K. Base	http://us.zyxel.com/web/support_knowledgebase.php

2 Zyxel Zywall USG 300 VPN configuration

This section describes how to build an IPSec VPN configuration with your Zyxel Zywall USG 300 VPN router.

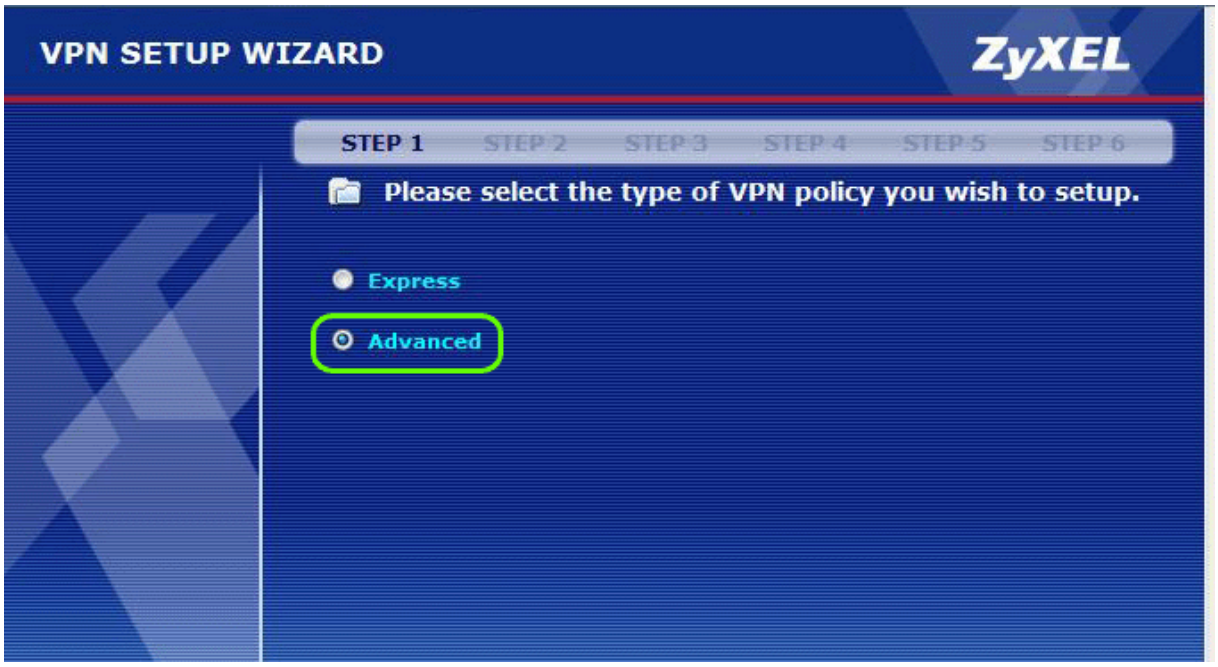
Once connected to your Zyxel Zywall USG 300 VPN gateway, the home page will show Main Menu.

2.1 VPN Setup

Use the Wizard to create a new VPN. Click on the upper right, Wizard icon: 

Launch the VPN Wizard and click 'VPN SETUP'.

Select 'Advanced' and click 'Next'.

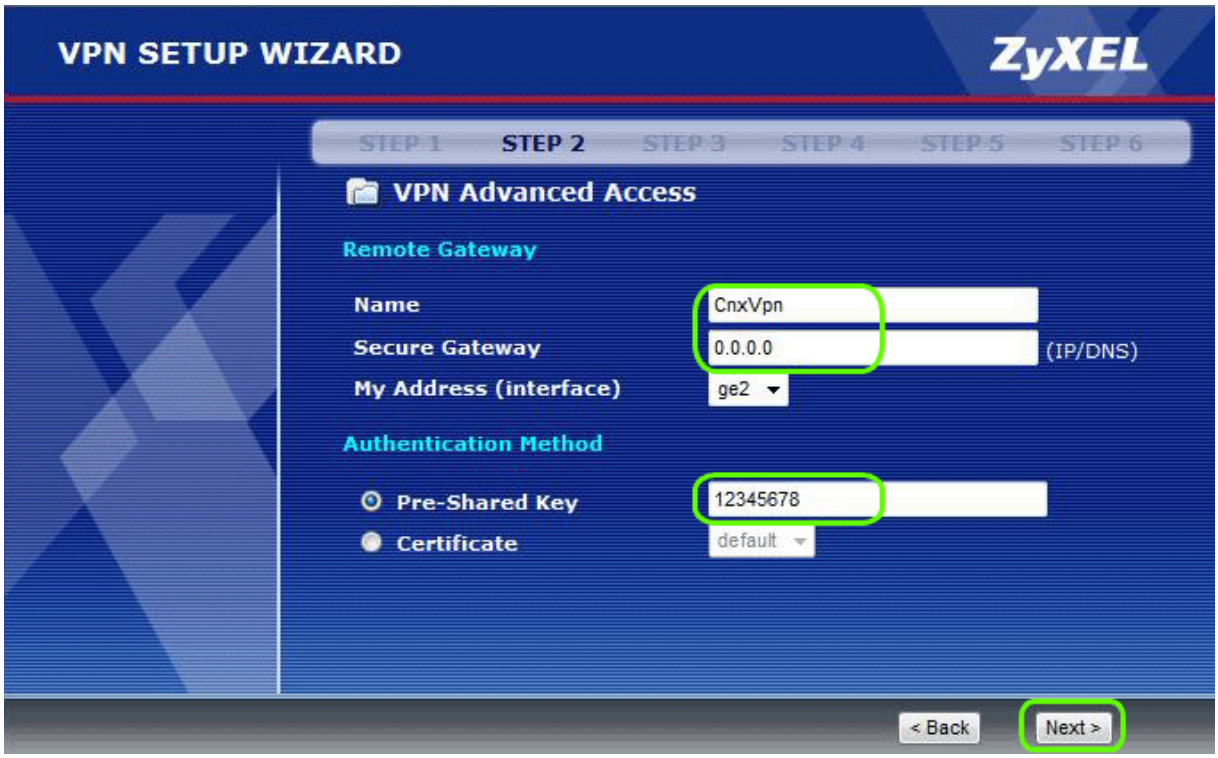


Enter a ‘Name’ for the VPN tunnel, and leave ‘Secure Gateway’ to 0.0.0.0

‘My Address (Interface)’ is the WAN interface (VPN incoming interface)

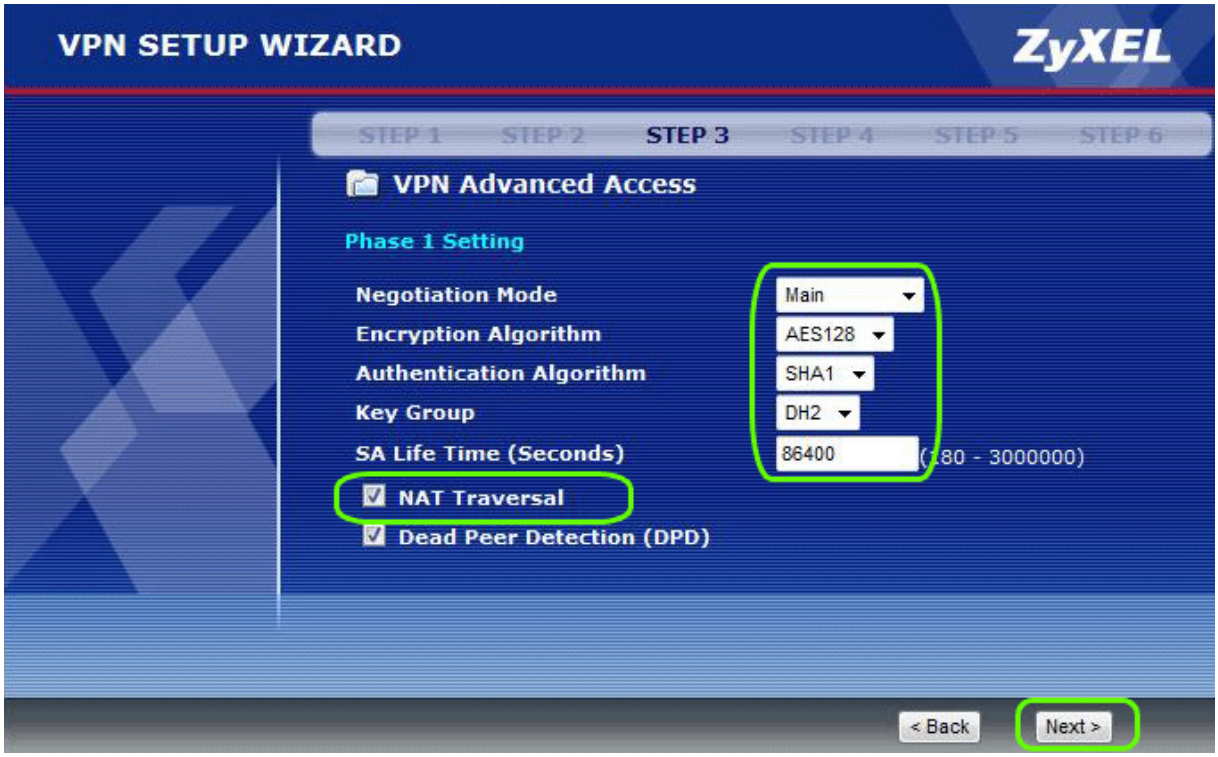
Enter the ‘Pre-Shared Key’ (example : 12345678).

Then click ‘Next’.

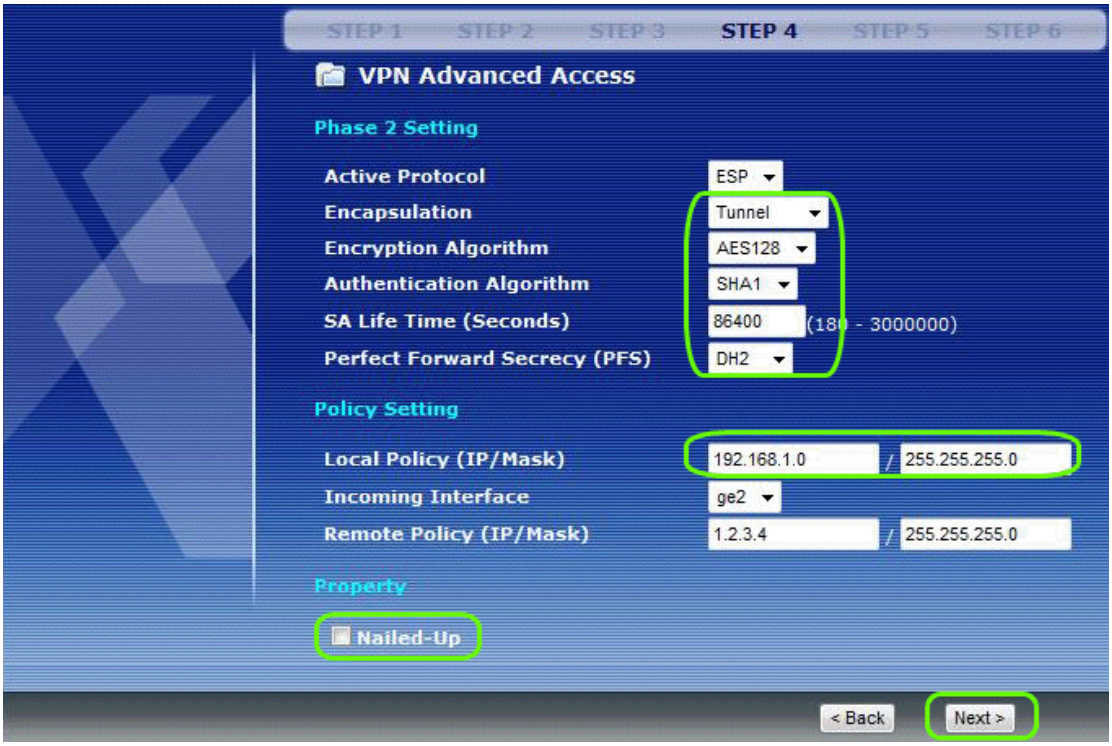


Then, you configure the ESP algorithms under Phase1 settings, as shown below.

Turn ‘NAT Traversal’ ON, only when either side is behind a NAT router. Click ‘Next’. You can keep ‘Dead Peer Detection’ slected as TheGreenBow IPSec VPN Client support DPD aka ‘Dead Peer Detection’.

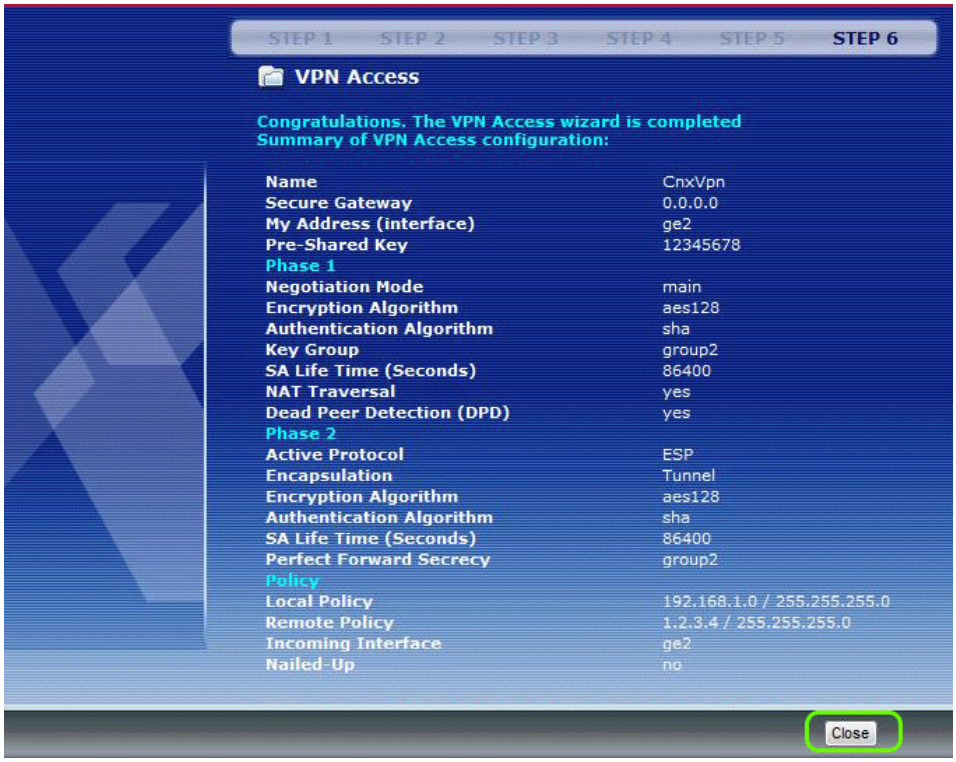


Fill in ‘Remote Policy’ 1.2.3.4 even temporarily as in this Wizard you're unable to fill what is ultimately 0.0.0.0. Also make sure that Nailed-Up checkbox is unchecked, we'll make a Dynamic VPN.



Check all your VPN configuration in the next ‘VPN Access’ screen, and click on ‘Save’ to save the VPN configuration.

Click ‘Close’ in below screen and the VPN Wizard is completed.



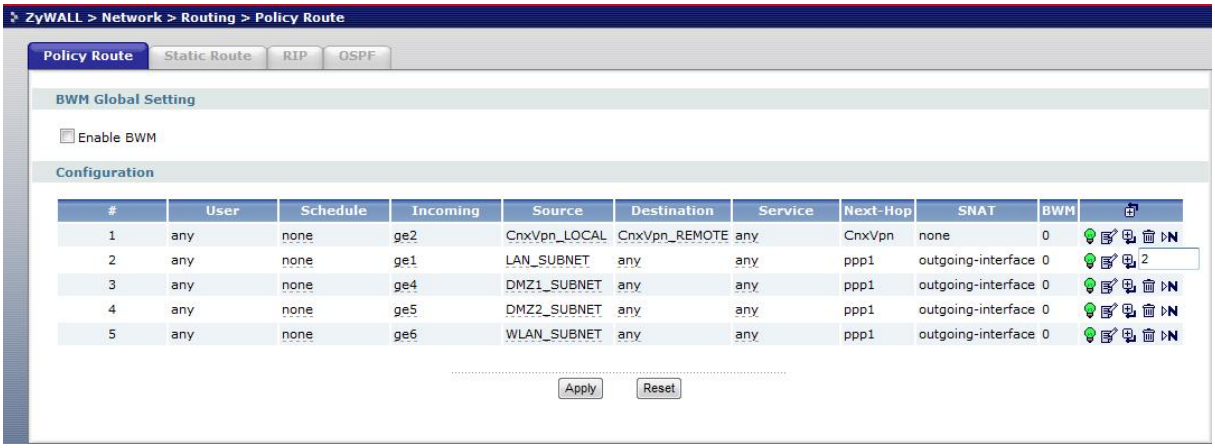
2.2 Policy Route setup

By default, the VPN Wizard created a Policy Route, which is in the first line in the routing table. It will slow down the LAN. This means that ALL traffic from the LAN will be sent through the tunnel.

Therefore, this rule should be moved to 2nd position, (or at least under the "standard" LAN_SUBNET line).

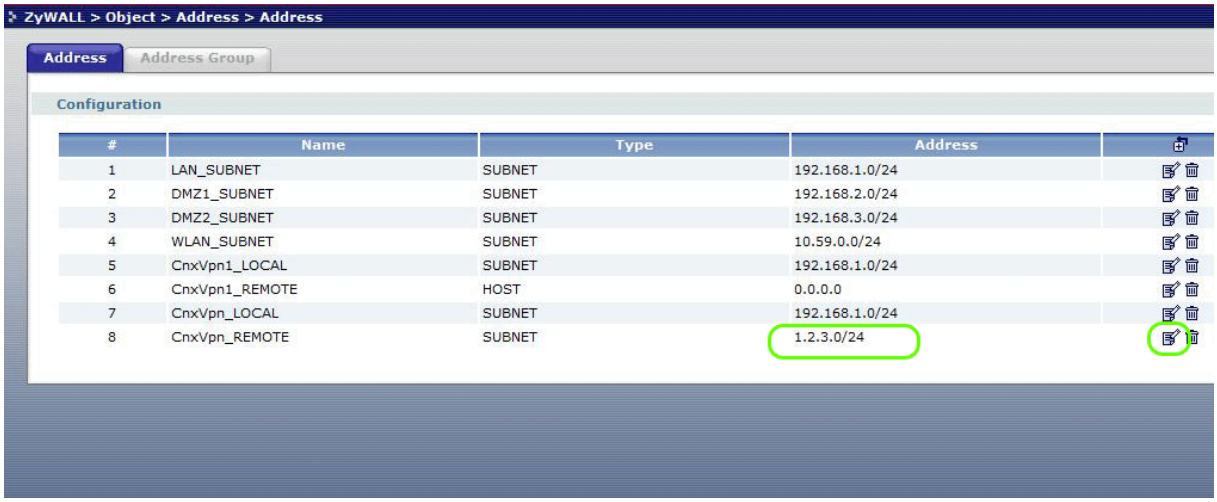
To change the order of Policy Route, click on the 'N' symbol of the first line and type '2'. Press 'ENTER' key to complete.

Then, you can see the Policy Route displayed in second line.

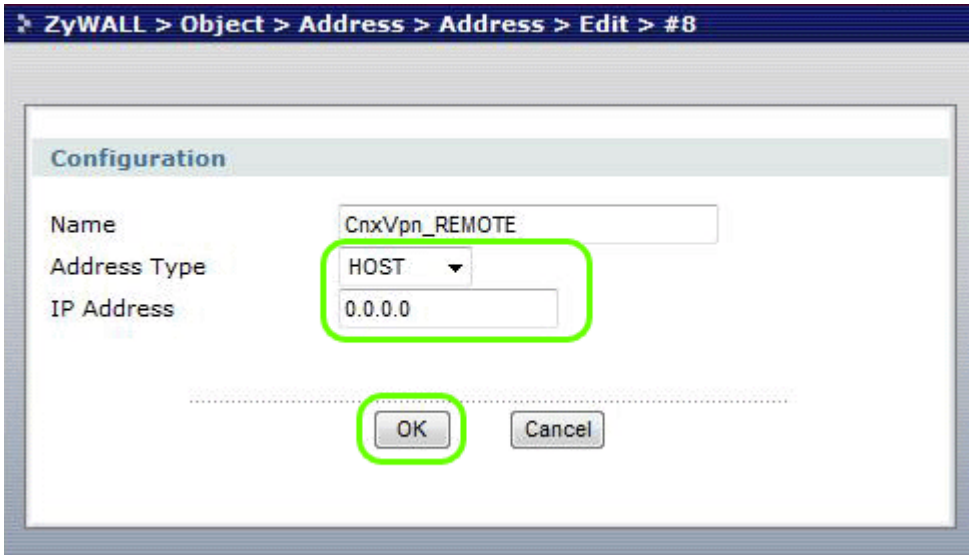


2.3 Dynamic VPN

Now, we have to change Remote IP address to 0.0.0.0 from 1.2.3.4 (Dynamic VPN). In the left side menu, click 'Object' and then select the 'Address' tab. Click the 'Edit' icon as indicated below:



Change ‘Address Type’ to ‘Host’ and then change the IP address to 0.0.0.0 and click ‘OK’:



Logoff from Zywall USG 300. The VPN configuration of the Zywall USG 300 is now ready.

The required VPN rules, Objects and Address (Policy) Routes have been automatically created in the Zywall USG 300 VPN Gateway.

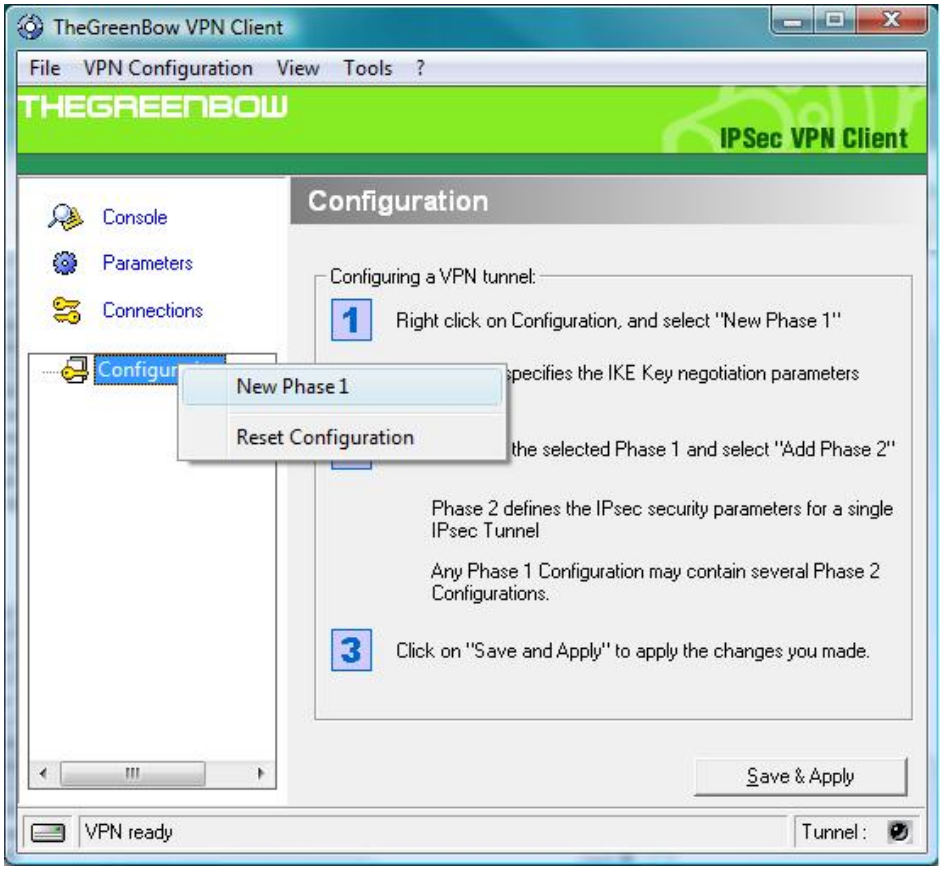
3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Zyxel Zywall USG 300 VPN router.

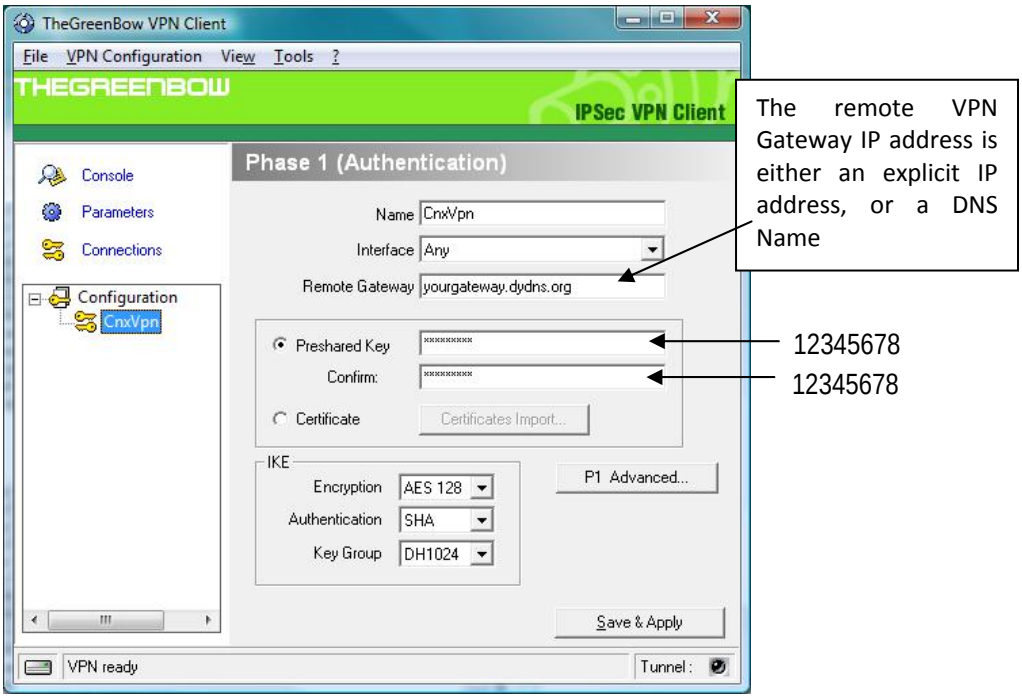
To download the latest release of TheGreenBow IPSec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html.

3.1 VPN Client Phase 1 (IKE) Configuration

Click right mouse button on Configuration and select New Phase 1.



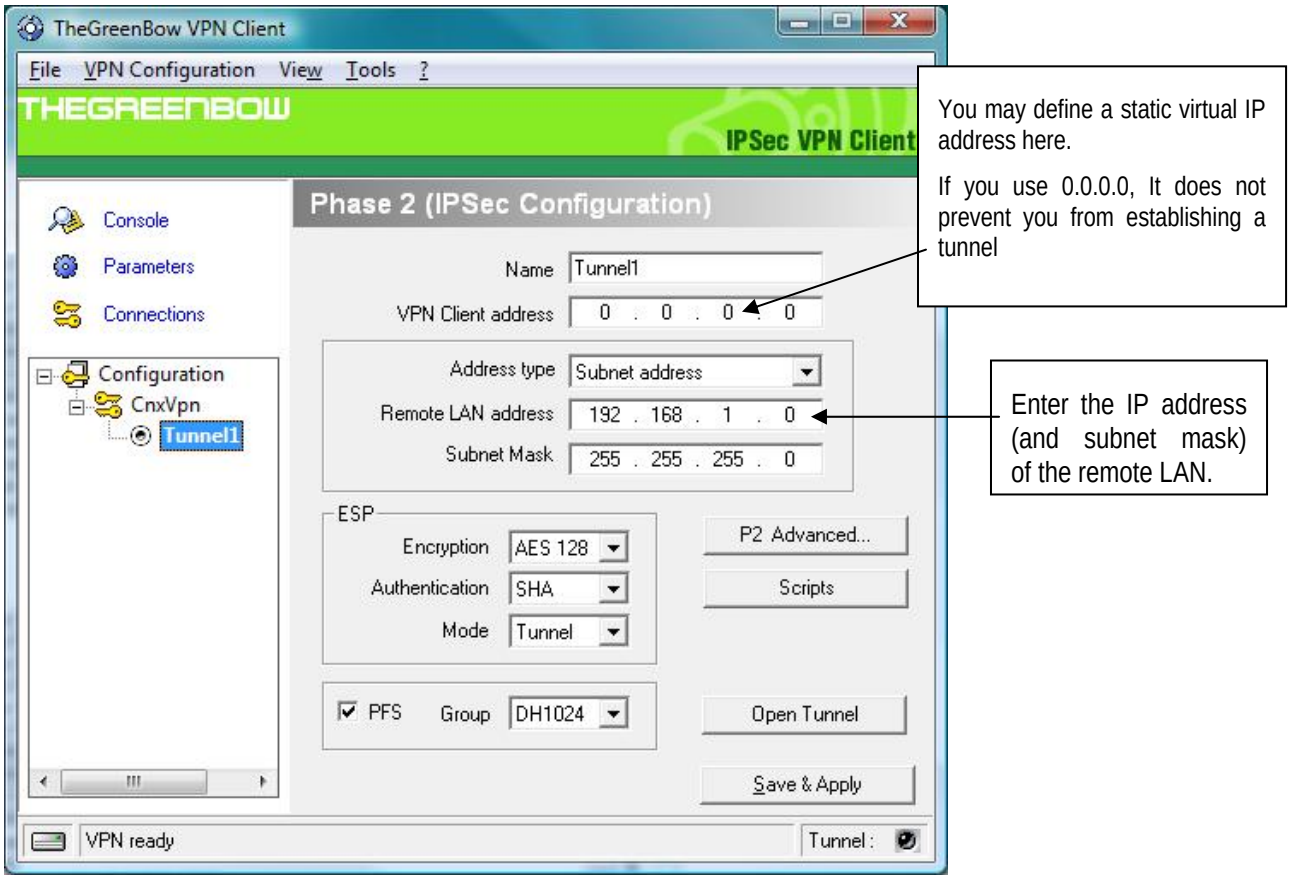
Fill up the configuration as shown below.



Phase 1 configuration

You may use either Preshared, Certificates, USB Tokens or X-Auth for User Authentication with the Zyxel Zywall USG 300 router. This configuration is one example of can be accomplished in term of User Authentication. You may want to refer to either the Zyxel Zywall USG 300 router user guide or TheGreenBow IPSec VPN Client User Guide for more details on User Authentication options.

3.2 VPN Client Phase 2 (IPSec) Configuration



Phase 2 Configuration

3.3 Open IPSec VPN tunnels

Once both Zyxel Zywall USG 300 router and TheGreenBow IPSec VPN Client software 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 & Apply" 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. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Zyxel Zywall USG 300 VPN router.

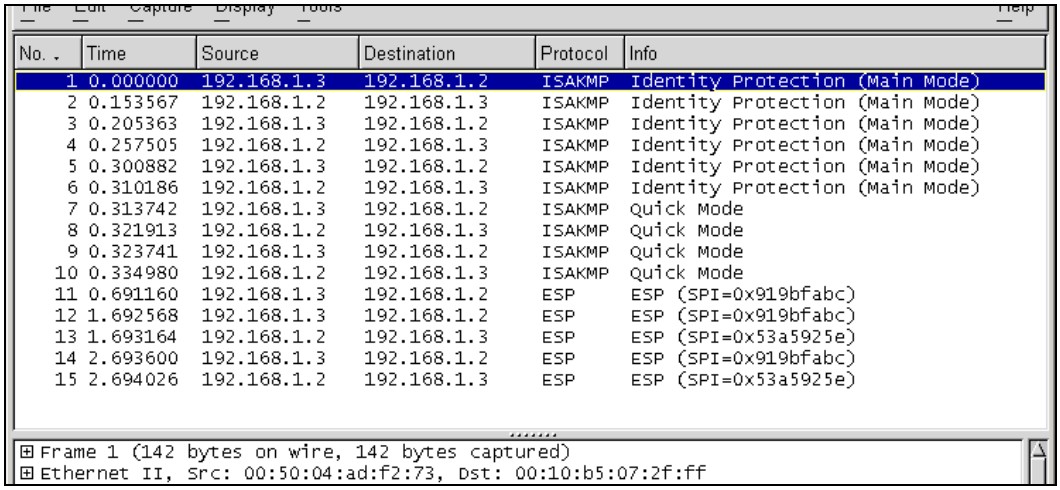
```
[VPNCONF] TGBIKESTART received
20080424 100334 Default (SA CnxVpn-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID] [VID]
20080424 100334 Default (SA CnxVpn-P1) RECV phase 1 Main Mode [SA] [VID] [VID]
20080424 100335 Default (SA CnxVpn-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE]
20080424 100335 Default (SA CnxVpn-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE]
20080424 100335 Default (SA CnxVpn-P1) SEND phase 1 Main Mode [HASH] [ID] [NOTIFY]
20080424 100335 Default (SA CnxVpn-P1) RECV phase 1 Main Mode [HASH] [ID]
20080424 100335 Default phase 1 done: initiator id 192.168.205.152, responder id 77.197.53.56
20080424 100335 Default (SA CnxVpn-Tunnel1-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080424 100335 Default (SA CnxVpn-Tunnel1-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080424 100335 Default (SA CnxVpn-Tunnel1-P2) SEND phase 2 Quick Mode [HASH]
```

4 Tools in case of trouble

Configuring an IPSec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

4.1 A good network analyser: Wireshark

Wireshark is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website http://www.wireshark.org. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (http://www.wireshark.org/docs/).



5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

```
114920 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA CNXVPN-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.

5.2 « 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.

5.3 « no keystate » error

```
115315 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN-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.

5.4 « received remote ID other than expected » error

```
120348 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN-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.

5.5 « NO PROPOSAL CHOSEN » error

```
115911 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN-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    CNXVPN-CNXVPN-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 CNXVPN-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 CNXVPN-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

5.6 « INVALID ID INFORMATION » error

```
122623 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN-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    CNXVPN-CNXVPN-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 CNXVPN-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).

5.7 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).

5.8 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 Wireshark 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 Wireshark (http://www.wireshark.org) on one of your target computer. You can check that your pings arrive inside the LAN.

6 Contacts

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

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com