TheGreenBow IPSec VPN Client

Configuration Guide

ZyXEL ZyWALL P1
firmware V3.64

WebSite:  http://www.thegreenbow.com
Contact:  support@thegreenbow.com
Table of contents

1 Introduction .................................................................................................................................................... 3
  1.1 Goal of this document ............................................................................................................................... 3
  1.2 VPN Network topology .............................................................................................................................. 3

2 Setup ZyWALL P1 ......................................................................................................................................... 4
  2.1 Gateway Policy 4
  2.2 Network Policy 5
  2.3 VPN configuration overview 6

3 TheGreenBow IPSec VPN Client configuration ............................................................................................ 0
  3.1 VPN client Phase 1 configuration ............................................................................................................. 7
  3.2 VPN client Phase 2 configuration ............................................................................................................. 9
  3.3 Console log 9

4 VPN IPSec Troubleshooting ........................................................................................................................ 11
  4.1 « PAYLOAD MALFORMED » error ........................................................................................................... 11
  4.2 « INVALID COOKIE » error ..................................................................................................................... 11
  4.3 « no keystore » error .................................................................................................................................. 11
  4.4 « received remote ID other than expected » error .................................................................................... 11
  4.5 « NO PROPOSAL CHOSEN » error .......................................................................................................... 12
  4.6 « INVALID ID INFORMATION » error ...................................................................................................... 12
  4.7 I clicked on “Open tunnel”, but nothing happens .................................................................................... 12
  4.8 The VPN tunnel is up but I can’t ping ! ................................................................................................... 12

5 Contacts....................................................................................................................................................... 14
1. Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a ZyXEL ZyWALL P1 with firmware 3.64

1.2 VPN Network topology

This gateway is a personal firewall with very limited LAN capabilities (DHCP for a single IP address for example). Eventhough Zyxel highlights its nomad VPN client features (which connects to a VPN server), it can also be configured as a VPN server usable with a road warrior vpn client like TheGreenBow. In this case both server and client can be nomads.

It can also be configured with a NAT device behind it, hidding a LAN overriding its limited LAN features, but this is not the purpose of this document.

- External IP of the ZyWALL P1: mygateway.dyndns.org (or public IP address)
- IP Subnet behind the ZyWALL P1: 192.168.167.0/255.255.255.0
2 Setup ZyWALL P1

This section describes how to build an IPSec VPN configuration with ZyWALL P1 VPN Gateway. There is no mandatory configuration, all settings may be altered to match your needs (speed vs security)

2.1 Gateway Policy

Create a new gateway policy on the ZyWALL (related to phase 1 on TheGreenBow VPN Client):
We used “Main mode” instead of “Aggressive mode” because of the lack of security with “Aggressive” compared to “Main.” AES algorithm is more efficient than DES or 3DES (faster to cipher data and more secured), but anything can be used.

2.2 Network Policy

Create a new Network policy (related to phase 2 on TheGreenBow VPN client)

VPN - NETWORK POLICY - EDIT
2.3 VPN configuration overview

<table>
<thead>
<tr>
<th>VPN Rules (IKE)</th>
<th>SA Monitor</th>
<th>Global Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[Diagram]</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>VPN Rules</th>
<th>0.0.0.0</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TGB Phase 1</td>
<td>0.0.0.0</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>

| TGB Phase 2 | 192.168.167.0 / 255.255.255.0 | Any |

[Image of VPN configuration diagram]
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 Configuration

You MUST change “Remote Gateway” IP address to match your dyndns name or static public ip address. Click on “P1 Advanced…” to setup IDs.
ID used in this example are DNS type. These type and values must match between vpn client and router even though they are just flags that can contain any value (in the example, the values entered are NOT proper dns names, but match between client and router)
3.2 VPN Client Phase 2 Configuration

The VPN client address must not belong to the remote subnet range (virtual IP address 10.10.10.10).

Phase2 advanced is used to enter alternate dns and/or wins servers addresses from the ones the vpn client is using prior to establish the tunnel.

3.3 Console log

The console screenshot below, shows a successful vpn connection with the P1.
### IPSec VPN Router Configuration

#### Property of TheGreenBow Sistech SA - © Sistech 2001-2006

#### 10/14

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006/12/05</td>
<td><strong>VPN Console ACTIVE</strong></td>
</tr>
<tr>
<td>151513</td>
<td>Default (SA Gateway_policy-P1) SEND phase 1 Main Mode [SA] [MD] [MD] [MD] [MD]</td>
</tr>
<tr>
<td>2006/12/05</td>
<td>Default (SA Gateway_policy-P1) RECVD phase 1 Main Mode [SA] [MD] [MD] [MD] [MD]</td>
</tr>
<tr>
<td>2006/12/05</td>
<td>Default (SA Gateway_policy-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]</td>
</tr>
<tr>
<td>2006/12/05</td>
<td>Default (SA Gateway_policy-P1) RECVD phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]</td>
</tr>
<tr>
<td>2006/12/05</td>
<td>Default (SA Gateway_policy-P1) SEND phase 1 Main Mode [HASH] [ID]</td>
</tr>
<tr>
<td>2006/12/05</td>
<td>Default (SA Gateway_policy-P1) RECVD phase 1 Main Mode [HASH] [ID]</td>
</tr>
<tr>
<td>2006/12/05</td>
<td>Default (SA Gateway_policy-P1) SEND phase 1 Main Mode [HASH] [ID]</td>
</tr>
<tr>
<td>2006/12/05</td>
<td>Default (SA Gateway_policy-P1) RECVD phase 1 Main Mode [HASH] [ID]</td>
</tr>
<tr>
<td>2006/12/05</td>
<td>Default (SA Gateway_policy-P1) SEND phase 1 Main Mode [HASH] [ID]</td>
</tr>
<tr>
<td>2006/12/05</td>
<td>Default (SA Gateway_policy-P1) RECVD phase 1 Main Mode [HASH] [ID]</td>
</tr>
</tbody>
</table>

**VPN version 3.1x**

**Doc.Ref tgbvpn_cg_P1_en**

**Doc.version 1.0 – December.2006**

**VPN version 3.1x**
4 VPN IPSec Troubleshooting

4.1 « 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

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

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

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
4.5 « NO PROPOSAL CHOSEN » error

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:

4.6 « INVALID ID INFORMATION » error

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, UDP port 4500 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