 TheGreenBow IPsec VPN Client
Configuration Guide
Oxyan Access-Net

WebSite: <http://www.thegreenbow.com>

Contact: support@thegreenbow.com

Table of contents

| | | |
|-----|--|---|
| 1 | Introduction | 0 |
| 1.1 | Goal of this document | 0 |
| 1.2 | Network topology | 0 |
| 2 | Access-Net VPN Configuration | 0 |
| 3 | TheGreenBow IPSec VPN Client configuration | 0 |
| 3.1 | VPN Client Phase 1 (IKE) Configuration | 0 |
| 3.2 | VPN Client Phase 2 (IPSec) Configuration | 0 |
| 3.3 | Open the IPSec VPN tunnels | 0 |
| 4 | VPN IPSec Troubleshooting | 0 |
| 4.1 | « PAYLOAD MALFORMED » error | 0 |
| 4.2 | « INVALID COOKIE » error | 0 |
| 4.3 | « no keystate » error | 0 |
| 4.4 | « received remote ID other than expected » error | 0 |
| 4.5 | « NO PROPOSAL CHOSEN » error | 0 |
| 4.6 | « INVALID ID INFORMATION » error | 0 |
| 4.7 | I clicked on "Open tunnel", but nothing happens | 0 |
| 4.8 | The VPN tunnel is up but I can't ping ! | 0 |
| 5 | Contacts | 0 |

1 Introduction

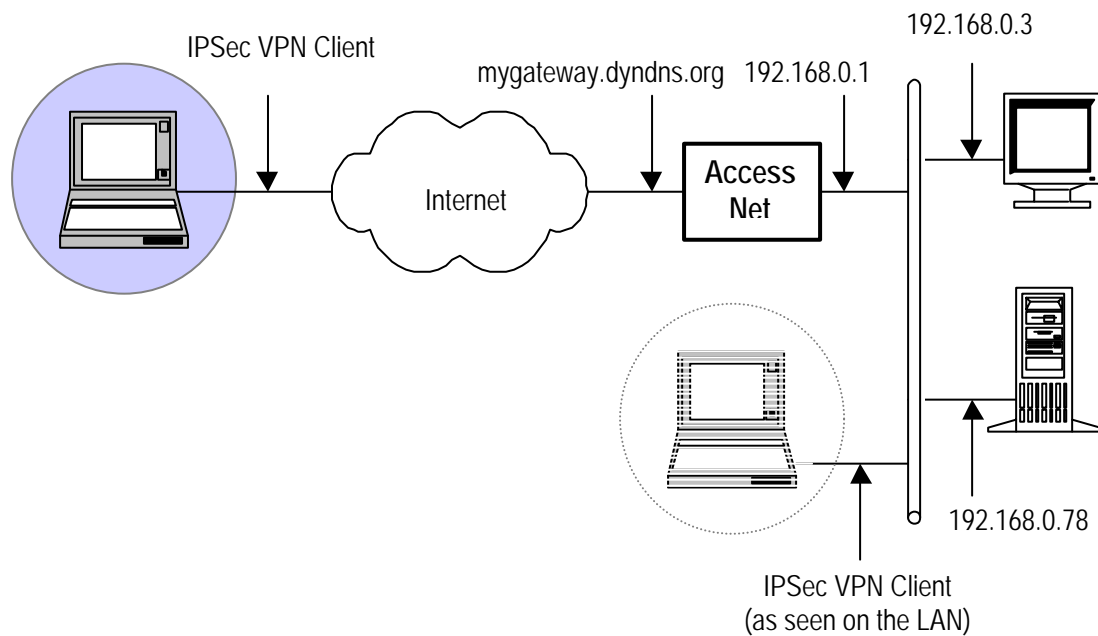
1.1 Goal of this document

This document describes how to configure TheGreenBow VPN Client with an Access-Net VPN platform. Access-Net is a software platform combining in one solutions messaging, agenda, groupware and Internet security tools.

This document has been written with the support of www.oxyan.com.

1.2 Network topology

In our example, we will connect TheGreenBow VPN client to the LAN behind the Access-Net Router. The VPN client is connected to the Internet by a dialup connection from an ISP. The client will have a virtual IP address in the remote LAN. All the addresses in this document are given for example purpose.



2 Access-Net VPN Configuration

Access-Net VPN configuration can be achieved with a web browser. Read Access-Net documentation for more information.

| Connexion IPSEC | |
|---------------------|--|
| Nom de la connexion | Nom de la connexion (nom arbitraire) |
| Activer | <input checked="" type="checkbox"/> |
| Commentaire | Connexion IPSEC entre un ACCESS-Net et un client VPN TheGreenBow |
| type | tunnel |
| left | Adresse IP publique de l'ACCESS-Net |
| right | %any |
| leftsubnet | Adresse IP du LAN local/Masque du LAN local |
| rightsubnet | vhost:%all |
| leftnexthop | %defaultroute |
| rightnexthop | |
| keyexchange | ike |
| auto | add |
| auth | esp |
| authby | secret |
| leftid | |
| rightid | |
| leftrsasigkey | |

| | |
|--|------|
| rightrsasigkey | |
| pfs | yes |
| keylife | 8.0h |
| rekey | yes |
| rekeymargin | 9m |
| keyingtries | 3 |
| ikelifetime | 1h |
| compress | no |
| disablearrivalcheck | yes |
| <input type="button" value="Valider"/> | |

3 TheGreenBow IPsec VPN Client configuration

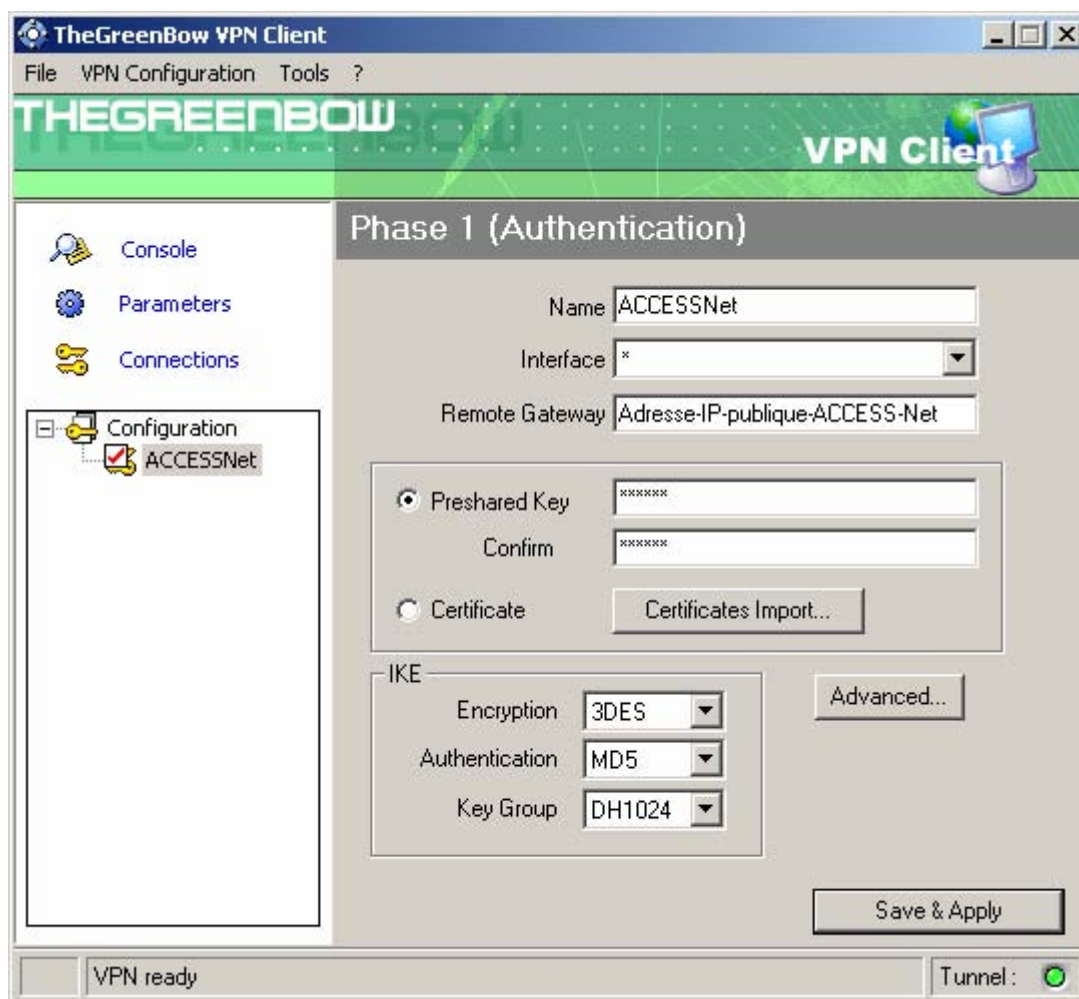
3.1 VPN Client Phase 1 (IKE) Configuration

In the "Interface" field, you can select a star ("*"), if the client host receive a dynamic IP Address from an ISP for example.

The "Remote Address" field value is the Access-Net VPN router public IP address or DNS address.

Keep default value for other field.

By clicking in "Advanced" button, you can setup "Phase 1 Ids" and "Aggressive Mode".



Phase 1 configuration

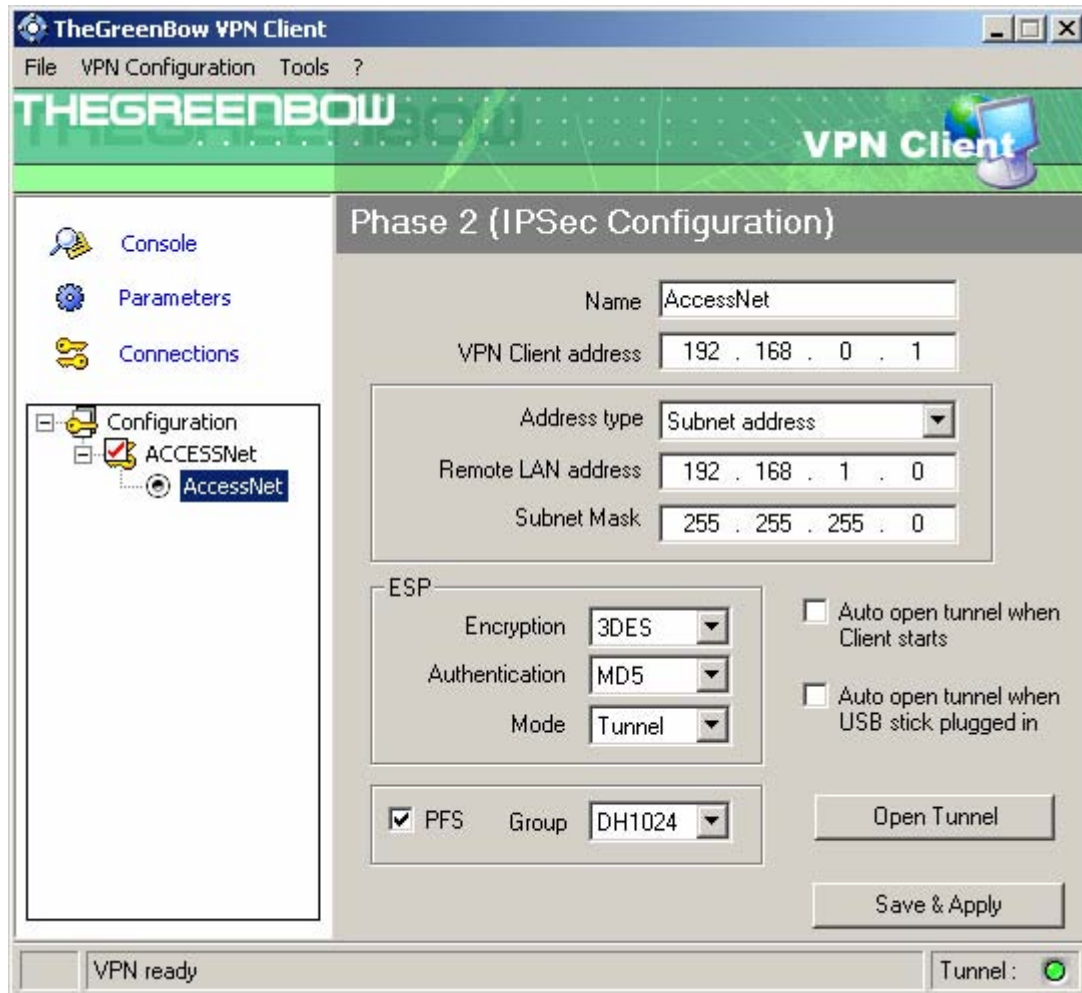
3.2 VPN Client Phase 2 (IPSec) Configuration

In this window, you define IPSec VPN Policy. "VPN Client address" is the virtual IP address of the client inside the LAN. With Access-Net VPN gateway, this address must not belong to the remote LAN.

The "Address Type": Select « Subnet Address ».

The "Remote LAN Address" and "Subnet mask": must be the IP address and the mask of the remote LAN

Keep default value for other field.



Phase2 Configuration

3.3 Open the IPSec VPN tunnels

Once both Oxayan ACCESS-NET VPN 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 & 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.

4 VPN IPSec Troubleshooting

4.1 « PAYLOAD MALFORMED » error

```

114920 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [SA][VID]
114920 Default (SA CnxVpn1-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_rcv: 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 CnxVpn1-P1) SEND phase 1 Main Mode [SA][VID]
115317 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [SA][VID]
115317 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [KEY][NONCE]
115319 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [KEY][NONCE]
115319 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50

```

If you have an « 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

```

120348 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [SA][VID]
120349 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [SA][VID]
120349 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [KEY][NONCE]
120351 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [KEY][NONCE]
120351 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default ike_phase_1_rcv_ID: received remote ID other than expected
support@thegreenbow.fr

```

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

4.5 « NO PROPOSAL CHOSEN » error

```

115911 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [SA][VID]
115913 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [SA][VID]
115913 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [KEY][NONCE]
115915 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [KEY][NONCE]
115915 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default (SA CnxVpn1-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 CnxVpn1-CnxVpn1-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 CnxVpn1-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 CnxVpn1-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 CnxVpn1-P1) SEND phase 1 Main Mode [SA][VID]
122625 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [SA][VID]
122625 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA CnxVpn1-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 CnxVpn1-CnxVpn1-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 CnxVpn1-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).

Check in your VPN router SA monitor if a previous SA is still alive.

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.

| | | |
|--|-------------|--------------------|
|  | Doc.Ref | tgbvpn_cg_Oxyan_en |
| | Doc.version | 2.0 – Nov.2004 |
| | VPN version | 2.5x |

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