TheGreenBow IPSec VPN Client

Configuration Guide

Ingate Firewall

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

1 Introduction .............................................................................................................................................................0
  1.1 Goal of this document .................................................................................................................................0
  1.2 VPN Network topology ...............................................................................................................................0
  1.3 Ingate Firewall VPN Gateway ..................................................................................................................0
2 Ingate Firewall VPN configuration .......................................................................................................................0
  2.1 Use the Ingate Firewall to create the client certificate ....................................................................................0
  2.2 Extract the pkcs12 files with certificate.exe ....................................................................................................0
3 TheGreenBow IPSec VPN Client configuration ...................................................................................................0
  3.1 VPN Client Phase 1 (IKE) Configuration .........................................................................................................0
  3.2 Certificates Import ............................................................................................................................................0
  3.3 Advanced Configuration ..................................................................................................................................0
  3.4 VPN Client Phase 2 (IPSec) Configuration .....................................................................................................0
  3.5 Open IPSec VPN tunnels ..................................................................................................................................0
4 Tools in case of trouble ..........................................................................................................................................0
  4.1 A good network analyser: ethereal ..................................................................................................................0
5 VPN IPSec Troubleshooting ..................................................................................................................................0
  5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) ...........................................................................0
  5.2 « INVALID COOKIE » error ............................................................................................................................0
  5.3 « no keystate » error .........................................................................................................................................0
  5.4 « received remote ID other than expected » error ..........................................................................................0
  5.5 « NO PROPOSAL CHOSEN » error ................................................................................................................0
  5.6 « INVALID ID INFORMATION » error .............................................................................................................0
  5.7 I clicked on “Open tunnel”, but nothing happens ............................................................................................0
  5.8 The VPN tunnel is up but I can’t ping ! ...........................................................................................................0
6 Contacts ..................................................................................................................................................................0
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with the Ingate Firewall VPN router.

This document has been written with the support of Ingate team: www.ingate.com.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Ingate Firewall 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 Ingate Firewall VPN Gateway

Our tests and VPN configuration have been conducted with Ingate Firewall firmware release version 4.2.1.
2 Ingate Firewall VPN configuration

This section describes how to build an IPSec VPN configuration with your Ingate Firewall VPN router.

Once connected to your VPN gateway, you must select “Security” and “VPN” tabs.

This document assumes that your Ingate Firewall is configured according to the examples available in the product manual here: http://www.ingate.se/files/fwmanual-sv//xx906.html.

This document also assumes that you have downloaded this tool: http://www.thegreenbow.fr/bin/certificate.zip.

2.1 Use the Ingate Firewall to create the client certificate

In order to create a Client Certificate please proceed through the following steps:

- Create an X.509 certificate on the Ingate Firewall
- Export this in p12 format and rename the file to client.p12
- Remove the certificate from the Ingate (The row below “Private certificate” that we just added)
- Export the Firewall’s “Private X509 certificate” in .p12 format and rename it to ingate.p12
- Transfer these files to the client computer

![Screenshot of Ingate Firewall configuring client certificate](image-url)
2.2 Extract the pkcs12 files with certificate.exe

Download and extract the certificate.exe from [www.thegreenbow.fr/bin/certificate.zip](http://www.thegreenbow.fr/bin/certificate.zip)

You can find more information on this tool at [www.thegreenbow.fr/doc/greenbow-x509.pdf](http://www.thegreenbow.fr/doc/greenbow-x509.pdf)

Use certificate.exe to extract ingate.p12 and client.p12 to 4 files each. (clientCert.Pem, rootCA.pem, local.key and DER_ASN1_DN.txt)

The tool "certificate.exe" creates subfolders for the p12 cert files that are extracted with the same filename.
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

Right click on "Configuration" and select "New Phase 1"

- **Name**: Give this connection a suitable name
- **Interface**: Leave as is (*) if no special configuration is needed
- **Remote Gateway**: Enter your Firewall's outside address
- **Certificate**: Select this option to use certificates
- **Preshared key**: Select and type your secret (not used for this example).
3.2 Certificates Import

Select "Certificate" and click on "Certificates Import ...".

- **Root Certificate**
  Select "Browse" for "Root Certificate" and browse to the file in the folder that was created by certificate.exe, in this case \Ingate\clientCert.Pem".

- **User Certificate**
  Select "Browse" for "User Certificate" and browse to the file in the folder that was created by certificate.exe, in this case \client\clientCert.Pem".
  Note that this is NOT the same file as for "Root Certificate".

- **User Private Key**
  Select "Browse" for "User Private Key" and browse to the file in the folder that was created by certificate.exe, in this case \client\local.Key"

3.3 Advanced Configuration

Fill in the following field and click "Ok".

- **Local ID Value:** Open the file \client\DER_ASN1_DN.txt and copy the text and paste it in the "Value" field.
- **Local ID Type:** Select "DER ASN1 DN"
3.4 VPN Client Phase 2 (IPSec) Configuration

Right click on "Phase 1" configuration and select "Add Phase 2"

- **Name**: Give this a suitable name
- **VPN Client Address**: Leave as is (0.0.0.0) if no special type is needed.
- **Address type**: If this tunnel is connected to a subnet (check this in your Ingate under VPN -> IPSec-Tunnels "Local Network" for this tunnel) then you should select "Subnet Address" and enter the exact networks that are located in your Firewall's "Local Network". If this tunnel is connected to a single address (check this in your Ingate under VPN -> IPSec-Tunnels "Local Network" for this tunnel) then you should select "Single Address" and enter the exact networks that are located in your Firewall's "Local Network".
- **ESP Encryption**: Select 3DES or AES 256. **ESP Authentication**: Select SHA or MD5. **ESP Mode**: Tunnel.
- **PFS**: Must be selected. **PFS Group**: Select DH1024 or DH2048.

3.5 Open IPSec VPN tunnels

Once both Ingate Firewall 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. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Microsoft Windows 2000 Server.

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0:00.0000</td>
<td>192.168.1.12</td>
<td>192.168.1.2</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>2</td>
<td>0:00.0007</td>
<td>192.168.1.2</td>
<td>192.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>3</td>
<td>0:00.0015</td>
<td>192.168.1.3</td>
<td>192.168.1.2</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>4</td>
<td>0:00.0025</td>
<td>192.168.1.2</td>
<td>192.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>5</td>
<td>0:00.0035</td>
<td>192.168.1.3</td>
<td>192.168.1.2</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>6</td>
<td>0:00.0045</td>
<td>192.168.1.2</td>
<td>192.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>7</td>
<td>0:00.0055</td>
<td>192.168.1.3</td>
<td>192.168.1.2</td>
<td>ISAKMP</td>
<td>ISAKMP Quick Mode</td>
</tr>
<tr>
<td>8</td>
<td>0:00.0065</td>
<td>192.168.1.2</td>
<td>192.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Quick Mode</td>
</tr>
<tr>
<td>9</td>
<td>0:00.0075</td>
<td>192.168.1.3</td>
<td>192.168.1.2</td>
<td>ISAKMP</td>
<td>ISAKMP Quick Mode</td>
</tr>
<tr>
<td>10</td>
<td>0:00.0085</td>
<td>192.168.1.2</td>
<td>192.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Quick Mode</td>
</tr>
<tr>
<td>11</td>
<td>0:00.0095</td>
<td>192.168.1.3</td>
<td>192.168.1.2</td>
<td>ESP</td>
<td>ESP (SPI=0x8290fabc)</td>
</tr>
<tr>
<td>12</td>
<td>0:00.0105</td>
<td>192.168.1.2</td>
<td>192.168.1.3</td>
<td>ESP</td>
<td>ESP (SPI=0x8290fabc)</td>
</tr>
<tr>
<td>13</td>
<td>0:00.0115</td>
<td>192.168.1.3</td>
<td>192.168.1.2</td>
<td>ESP</td>
<td>ESP (SPI=0x8290fabc)</td>
</tr>
<tr>
<td>14</td>
<td>0:00.0125</td>
<td>192.168.1.2</td>
<td>192.168.1.3</td>
<td>ESP</td>
<td>ESP (SPI=0x8290fabc)</td>
</tr>
<tr>
<td>15</td>
<td>0:00.0135</td>
<td>192.168.1.3</td>
<td>192.168.1.2</td>
<td>ESP</td>
<td>ESP (SPI=0x8290fabc)</td>
</tr>
</tbody>
</table>
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: ethereal

Ethereal 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.ethereal.com/. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.
5  VPN IPSec Troubleshooting

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

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

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

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

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
5.5 « 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:

5.6 « 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).

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 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.
6 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 or by email at info@thegreenbow.com