TheGreenBow IPsec VPN Client

Configuration Guide

Strongswan

Website:  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  
1.3 Strongswan Restrictions................................................................................................................. 3  
1.4 Strongswan VPN Gateway ............................................................................................................. 3  
1.5 Strongswan VPN Gateway product info ........................................................................................ 3  
2 Strongswan VPN configuration............................................................................................................... 4  
2.1 Server Certificates.......................................................................................................................... 4  
2.2 Client Certificates........................................................................................................................... 4  
2.3 Create VPN connections in Strongswan......................................................................................... 4  
2.4 ipsec.secrets................................................................................................................................... 5  
3 TheGreenBow IPsec VPN Client configuration ....................................................................................... 6  
3.1 VPN Client - IKE Auth Configuration .............................................................................................. 6  
3.2 VPN Client Phase 2 (Child SA) Configuration ................................................................................. 8  
3.3 Open IPsec VPN tunnels................................................................................................................. 9  
4 Tools in case of trouble......................................................................................................................... 10  
4.1 A good network analyser: Wireshark ........................................................................................... 10  
5 VPN IPsec Troubleshooting.................................................................................................................. 11  
5.1 “NO PROPOSAL CHOSEN” error (wrong IKE Auth)................................................................. 11  
5.2 “AUTHENTICATION FAILED” error............................................................................................ 11  
5.3 “no user certificate available for the connexion” error............................................................... 11  
5.4 “Remote ID rejected” error........................................................................................................... 11  
5.5 “NO PROPOSAL CHOSEN” error (wrong CHILD SA)............................................................ 11  
5.6 “FAILED CP REQUIRED” error..................................................................................................... 12  
5.7 I clicked on “Open tunnel”, but nothing happens................................................................. 12  
5.8 The VPN tunnel is up but I can’t ping ! ..................................................................................... 12  
6 Contacts................................................................................................................................................ 13
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a Strongswan VPN router to establish VPN connections for remote access to corporate network.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPsec VPN Client software to the LAN behind the Strongswan 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 Strongswan Restrictions

No known restrictions

1.4 Strongswan VPN Gateway

Our tests and VPN configuration have been conducted with Strongswan version 5.5.

1.5 Strongswan VPN Gateway product info

It is critical that users find all necessary information about Strongswan VPN Gateway. All product info, User Guide and knowledge base for the Strongswan VPN Gateway can be found on the Strongswan website: https://www.strongswan.org/

<table>
<thead>
<tr>
<th>Strongswan Product page</th>
<th><a href="https://www.strongswan.org/">https://www.strongswan.org/</a></th>
</tr>
</thead>
</table>
2 Strongswan VPN configuration

This section describes how to build an IPsec VPN configuration with your Strongswan VPN router.

2.1 Server Certificates

Once connected to your Strongswan VPN gateway, make sure you have Certificate authority configured and these certificates are ready and copied to concerned folders.

- "server.crt" - Certificate of the strongswan machine. This file needs to be copied to folder "/etc/ipsec.d/cert/
- "server.key" - Certificate private key of the strongswan machine. This file needs to be copied to folder "/etc/ipsec.d/private/
- "ca.crt" - Certificate authority certificate for all certificates. This file needs to be copied to folder "/etc/ipsec.d/ca/

2.2 Client Certificates

- "client1.crt" - User certificate to be imported to VPN Client.
- "client1.key" - User certificate's private key to be imported to VPN Client.
- "ca.crt" - CA certificate of user certificate.

It is also possible to create single file "client1.p12" or "client1.pfx" using above 3 files and import to VPN Client.

2.3 Create VPN connections in Strongswan

Once done, go to terminal command prompt and edit following files. Set the contents as follows.

```
#--------------- Contents of file: /etc/ipsec.conf

conn %default
   ikelifetime=140m
   keylife=50m
   rekeymargin=3m
   rekeyfuzz=0%
   keyingtries=1
   ike= aes256-sha512-modp8192
   esp= aes256-sha512-modp8192

conn cert
   left=192.168.10.21
   leftsubnet=192.168.175.0/24
   leftcert=server.crt
```
leftfirewall=yes
right=%any
righthost=10.80.80.0/24
forceencaps=yes
keyexchange=ikev2
auto=add

#--------------- end of file

- IP "192.168.10.21" is WAN IP of Strongswan gateway, where the IPsec connection request comes in.
- "192.168.175.0/24" is the range of network to be reached by VPN Client tunnel.
- "righthost=10.80.80.1" - Virtual IP address to be assigned for the VPN Client tunnel.

Optional : In case of ESP 50 is blocked in your firewall, it is possible to force NAT-Traversal (UDP 4500) in Strongswan using "forceencaps=yes", thus not using protocol ESP 50. Uncomment the line from ipsec.conf file.

2.4 ipsec.secrets

#--------------- Contents of file: /etc/ipsec.secrets

#/etc/ipsec.secrets - strongSwan IPsec secrets file

: RSA server.key

#--------------- end of file

Once both files are edited, restart IPsec server by executing command : "ipsec restart"
3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a Strongswan VPN router via VPN connections. To download the latest release of TheGreenBow IPsec VPN Client software, please go to www.thegreenbow.com/vpn_down.html.

3.1 VPN Client - IKE Auth Configuration

IKE Auth configuration

Cryptography can be set to AUTO. This will automatically negotiate with the VPN Router.
IKE Auth Certificate configuration

This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Strongswan router user guide or TheGreenBow IPsec VPN Client software User Guide for more details on User Authentication options.
3.2 VPN Client Phase 2 (Child SA) Configuration

Cryptography can be set to AUTO. This will automatically negotiate with the VPN Router.

Virtual IP address and Remote LAN address/subnet will be sent by Strongswan through Mode CP.

Child SA Configuration

Cryptography can be set to AUTO. This will automatically negotiate with the VPN Router.
3.3 Open IPsec VPN tunnels

Once both Strongswan 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/ Select menu "Configuration" and "Save" to take into account all modifications we’ve made on your VPN Client configuration.

2/ Double Click on your Child SA tunnel name or Click "Open" button in Connection panel to open tunnel.

3/ Select menu "Tools" and "Console" if you want to access to the IPsec VPN logs. The following example shows a successful connection between TheGreenBow IPsec VPN Client and a Strongswan VPN router.
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 www.wireshark.org. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (www.wireshark.org/docs/).
5   VPN IPsec Troubleshooting

5.1 “NO PROPOSAL CHOSEN” error (wrong IKE Auth)

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

5.2 “AUTHENTICATION FAILED” error

If you have an “Authentication Failed” error, it means that the certificate or Preshared key is not matching. Check the Gateway if the User certificate or preshare key is valid.

5.3 “no user certificate available for the connexion” error

Check if the certificate is selected or the Token (smartcard) is available on the computer.

5.4 “Remote ID rejected” error

The “Remote ID” value (see “Protocol” tab) does not match what the remote endpoint is expected.

5.5 “NO PROPOSAL CHOSEN” error (wrong CHILD SA)
If you have an “NO PROPOSAL CHOSEN” error, check that the “Child SA” encryption algorithms are the same on each side of the VPN Tunnel.

### 5.6 “FAILED CP REQUIRED” error

20XX0913 16:29:46:780 TIKEV2_Tunnel RECV IKE_AUTH  
[HDR][Idr][CERT][AUTH][N(AUTH_LIFETIME)][N(FAILED_CP_REQUIRED)][N(TS_UNACCEPTABLE)]  
20180913 16:29:46:780 TIKEV2_Tunnel Remote endpoint sends error FAILED_CP_REQUIRED  
20XX0913 16:29:46:780 TIKEV2_Tunnel Remote endpoint is expecting a configuration request from the client

If you have an “FAILED CP REQUIRED” error, then the Gateway is configured to use Mode CP. Go to Traffic selectors and enable "Request configuration from the gateway".

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

20XX1003 11:08:34:031 [VPNCONF] TGBIKE_STARTED received  
20XX1003 11:21:34:379 TIKEV2_vRHEL75 SEND IKE_SA_INIT  
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]  
20XX1003 11:21:39:397 TIKEV2_vRHEL75 SEND IKE_SA_INIT  
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]  
20XX1003 11:21:44:409 TIKEV2_vRHEL75 SEND IKE_SA_INIT  
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]  

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPsec Client uses UDP port 500.  
Check if the remote server is online.

### 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 Child SA 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 and if the protocol 50 is allowed to pass traffic in your firewalls.
- 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 ([www.wireshark.org](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: www.thegreenbow.com

Technical support by email at: support@thegreenbow.com

Sales contacts by email at: sales@thegreenbow.com
Secure, Strong, Simple
TheGreenBow Security Software