TheGreenBow IPSec VPN Client

Configuration Guide

Planet CS-1000

WebSite: [http://www.thegreenbow.com](http://www.thegreenbow.com)

Contact: [support@thegreenbow.com](mailto:support@thegreenbow.com)
# Table of contents

1 Introduction .................................................................................................................................................... 3  
1.1 Goal of this document ............................................................................................................................... 3  
1.2 VPN Network topology .............................................................................................................................. 3  
2 Setup Planet CS-1000 .................................................................................................................................. 4  
2.1 IPSec AutoKey .......................................................................................................................................... 4  
2.2 Trunk Policy .............................................................................................................................................. 6  
3 TheGreenBow IPSec VPN Client configuration ............................................................................................ 7  
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 keystate » 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 ....................................................................................................................................................... 13
1. Introduction

1.1 Goal of this document
This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Planet CS-1000 Multi-Homing Security Gateway.

1.2 VPN Network topology

- Planet CS-1000 External IP: mygateway.dyndns.org (or static public IP address)
- Planet CS-1000 Internal IP: 10.254.254.248
- Subnet behind Planet CS-1000: 10.254.254.0 / 255.255.255.0
- VPN client virtual IP (phase 2): 10.10.10.10
2 Setup Planet CS-1000

This section describes how to build an IPSec VPN configuration with Planet CS-1000 VPN Gateway.
There is no mandatory configuration, all settings may be altered to match your needs (speed vs security).
We need to setup an IPSec AutoKey, and a Trunk Policy

2.1 IPSec AutoKey

Create a new IPSec Autokey policy on the CS-1000.
We used “Main mode” instead of “Aggressive mode” because of the lack of security with “Aggressive” compared to “Main”. In aggressive mode, keys are exchanged in clear.

AES algorithm is more efficient than DES or 3DES (faster to cipher data and more secured), but anything else can be used.

If lifetimes are modified, it is recommended to tune ipsec and ike lifetimes accordingly on the vpn client (default values). This is found in Vpn configuration/Parameters.

IDs fields are left blank in our example, security can be increased by entering local and remote IDs with IP address or FQDN (DNS) string type.
2.2 Trunk policy

Create a New Entry Trunk, which in fact, is TheGreenBow vpn client's phase 2.

This is a traffic policy that needs to be linked to a tunnel definition. In our case there is only the greenbow tunnel available. Phase 2 distant subnet on the vpn client must match the “Source Subnet/Mask” field on the newly created entry trunk.
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 if local and remote IDs were previously defined on the CS-1000.
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's screenshot below, shows a successful main mode vpn connection with the Planet CS-1000.
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 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