TheGreenBow IPSec VPN Client
Configuration Guide
Micronet SP881

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 Micronet SP881 VPN Configuration ........................................................................... 0
  2.1 Micronet SP881 create new IPSec VPN tunnel ....................................................... 0
  2.2 Micronet SP881 Authentication method .................................................................... 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 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 IPSec VPN Client with a Micronet SP881 Broadband VPN Firewall.

1.2 Network topology

In our example, we will connect TheGreenBow VPN client to the LAN behind the Micronet Router. The VPN client is connected to the Internet by a dialup/DSL 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 Micronet SP881 VPN Configuration

Micronet firmware release version used during tests was 2.50.
Micronet SP881 configuration can be achieved with a web browser. Read Micronet SP881 documentation for more information.

2.1 Micronet SP881 create new IPSec VPN tunnel

First, select "VPN" and click on "IPSec Autokey" link in the Micronet VPN configuration interface. Select a connection and click on "Modify", or if you want to add a new configuration click on "New Entry".

Enter a "Name" for the VPN Tunnel.
Specify your local Network. This is the network which TheGreenbow VPN Clients should be allowed to connect to.
And select "Remote Client".
2.2 Micronet SP881 Authentication method

Select “Preshare” for Authentication method and choose a “Preshared key”.

Select algorithms you want to use. For IPSec Algorithm don’t forget to select “Data Encryption + Authentication”.

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Preshare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encapsulation</td>
<td></td>
</tr>
<tr>
<td>ISAKMP Algorithm</td>
<td>3DES</td>
</tr>
<tr>
<td>ENC Algorithm</td>
<td>MD5</td>
</tr>
<tr>
<td>AUTH Algorithm</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>GROUP 2</td>
</tr>
<tr>
<td>IPSec Algorithm</td>
<td>Data Encryption + Authentication</td>
</tr>
<tr>
<td>ENC Algorithm</td>
<td>3DES</td>
</tr>
<tr>
<td>AUTH Algorithm</td>
<td>SHA1</td>
</tr>
<tr>
<td>Authentication Only</td>
<td></td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td></td>
</tr>
</tbody>
</table>

Leave the other fields empty and click “Ok”

<table>
<thead>
<tr>
<th>IPSec Lifetime</th>
<th>20000</th>
<th>Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep alive IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggressive mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>My ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GRE/IPSec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GRE Local IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GRE Remote IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schedule</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

The VPN configuration of Micronet SP881 router is completed.
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.

"Remote Address" field value is the Micronet router public IP address or DNS address.
By clicking in "Advanced" button, you can setup Phase 1 IDs and Aggressive Mode.

The remote Gateway IP address is either an explicit IP address, or a DNS Name.

Phase 1 configuration
3.2 VPN Client Phase 2 (IPSec) Configuration

In this window, you define IPSec Policy. "Local Address" is the virtual IP address of the client inside the LAN. This address must not belong to the remote LAN.

You may define a static virtual IP address here.
For use with Micronet routers, do NOT specify an IP address belonging to the remote LAN's

Enter the IP address (and subnet mask)

3.3 Open IPSec VPN tunnels

Once both MicroNet SP881 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 "Apply Rules" 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

Those error samples have been voluntarily produced with a Linksys WRV54G, but logs and IPSec messaging shall be exactly the same with a MicroNet SP881 VPN Gateway.

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 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 or by email at info@thegreenbow.com