TheGreenBow IPSec VPN Client

Configuration Guide

Symantec
Firewall/VPN 200

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 Symantec VPN/200 Restrictions ......................................................................................................... 0

2 Symantec Firewall/VPN 200 VPN Configuration ............................................................................... 0
   2.1 Symantec User identity ....................................................................................................................... 0
   2.2 Symantec Dynamic key ....................................................................................................................... 0

3 TheGreenBow VPN client configuration ............................................................................................... 0
   3.1 Client Phase 1 (IKE) Configuration .................................................................................................... 0
   3.2 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 configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Symantec VPN/200 router.

1.2 VPN Network topology
In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Symantec VPN/200 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.

In our example, we will configure an IPSec VPN tunnel between a DSL device and a LAN behind a Symantec. Symantec LAN IP network address will be 192.168.0.1/24

1.3 Symantec VPN/200 Restrictions
No known restrictions.
2 Symantec Firewall/VPN 200 VPN Configuration

This section describes the configuration of a Symantec Firewall/VPN 200 gateway in order to open a Client-To-Gateway tunnel with the TheGreenBow IPSec VPN Client. Read Symantec documentation for more details about this VPN gateway.

2.1 Symantec User identity

In the main web configuration page of the Symantec VPN gateway, click on "Client Identity". You have to set:

- the user name: thegreenbow
- a preshared key associated with this user: abcdedghij0123456789. This value must be at least 20 bytes long.

### User Identity

<table>
<thead>
<tr>
<th>Select User</th>
<th>thegreenbow</th>
<th>Select only if Updating or Deleting current Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td></td>
<td>Select User above first unless Adding</td>
</tr>
<tr>
<td>User Name</td>
<td>thegreenbow</td>
<td>Must match Client ID offered by remote VPN client</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>abcdedghij0123456789</td>
<td></td>
</tr>
</tbody>
</table>

### User List

<table>
<thead>
<tr>
<th>Name</th>
<th>Enable?</th>
<th>Pre-Shared Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>thegreenbow</td>
<td>Enabled</td>
<td>abcdedghij0123456789</td>
</tr>
</tbody>
</table>
2.2 Symantec Dynamic key

In order to enable a VPN client to get connected with the VPN gateway, a dynamic key must be configured. The following picture shows settings that can be used:

**IPSec Security Association**

<table>
<thead>
<tr>
<th>Select Security Association</th>
<th>Name: testVPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Port</td>
<td>WAN1</td>
</tr>
<tr>
<td>PPPoE Session</td>
<td>Session 1</td>
</tr>
<tr>
<td>Phase 1 Negotiation</td>
<td></td>
</tr>
<tr>
<td>Encryption and Authentication Method</td>
<td>ESP 3DES SHA1</td>
</tr>
<tr>
<td>SA Lifetime</td>
<td>1000 Minutes</td>
</tr>
<tr>
<td>Data Volume Limit</td>
<td>1000000 KBytes</td>
</tr>
<tr>
<td>Inactivity Timeout</td>
<td>1000 Minutes</td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>Enable</td>
</tr>
</tbody>
</table>

Aggressive mode setting is mandatory. These settings will be reported in the IPSec VPN Client configuration interface.

Phase 1 IDs are configured in “Local Security Gateway” and “Remote Security Gateway”.

**Local Security Gateway**

<table>
<thead>
<tr>
<th>ID Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

**Remote Security Gateway**

<table>
<thead>
<tr>
<th>Gateway Address</th>
<th>ID Type</th>
<th>Distinguished Name</th>
<th>Phase 1 ID</th>
<th>Pre-Shared Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>Distinguished Name</td>
<td>Select Distinguished Name for Client-to-Gateway tunnels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leave Phase 1 ID and Shared Secret blank for Client SA, Remote Client ID must match a User in Client List</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When finished, click on “Add”. A new line will appear in the “Security Association List”.

**Security Association List**

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>Security Gateway</th>
<th>Remote Subnet</th>
<th>Encryption Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>testVPN</td>
<td>0.0.0.0</td>
<td></td>
<td>ESP 3DES SHA1</td>
</tr>
</tbody>
</table>
3 TheGreenBow VPN client configuration

3.1 Client Phase 1 (IKE) Configuration

Note: If the IP address of the VPN Client is automatically assigned, select Interface = " * "

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

"abcdefgij0123456789"
"abcdefgij0123456789"

Give here client identity for phase 1: thegreenbow with KEY_ID type
3.2 Phase 2 (IPSec) Configuration

IP address given in “Local Address” will not be used because Symantec Firewall/VPN 200 gateway does not support virtual IP addresses.

![Phase 2 Configuration](image)

3.3 Open the IPSec VPN tunnels

Once both Symantec Firewall/VPN 200 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 messaging shall be exactly the same with a Symantec Firewall/VPN200 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:

If you still have a « 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").

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

Technical support by email at [support@thegreenbow.com](mailto:support@thegreenbow.com)

Sales contacts at +33 1 43 12 39 37 or by email at [info@thegreenbow.com](mailto:info@thegreenbow.com)