TheGreenBow IPSec VPN Client

Configuration Guide

Symantec Gateway Security v3.0x

WebSite: http://www.thegreenbow.com
Contact: support@thegreenbow.com

Configuration Guide written by:

Writer:	Symantec
Company:	www.symantec.com

Table of contents

1 Disclaimer 3

2 Introduction 4
2.1 Goal of this document 4
2.2 VPN Network topology 4
2.3 Symantec Gateway Security v3.0x Restrictions 4
2.4 Symantec Gateway Security v3.0x VPN Gateway 4
2.5 Symantec Gateway Security v3.0x VPN Gateway product info 4

3 Symantec Gateway Security v3.0x VPN configuration 5

4 TheGreenBow IPSec VPN Client configuration 6
4.1 VPN Client Phase 1 (IKE) Configuration 6
4.2 VPN Client Phase 2 (IPSec) Configuration 7
4.3 Open IPSec VPN tunnels 7

5 Tools in case of trouble 9
5.1 A good network analyser: Wireshark 9

6 VPN IPSec Troubleshooting 10
6.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) 10
6.2 « INVALID COOKIE » error 10
6.3 « no keystate » error 10
6.4 « received remote ID other than expected » error 10
6.5 « NO PROPOSAL CHOSEN » error 11
6.6 « INVALID ID INFORMATION » error 11
6.7 I clicked on “Open tunnel”, but nothing happens. 11
6.8 The VPN tunnel is up but I can’t ping ! 11

7 Contacts 13

1 Disclaimer

These instructions are provided for your convenience only. Remember that TheGreenBow has NO legal right on the set of instructions to configure the Symantec Appliance listed in this document. This document is basically a copy of a Symantec web page called: "How to connect a tunnel to a Symantec Gateway Security v3.0.1 appliance using TheGreenBow VPN" that you can google easily here: http://www.google.com/search?q=How+to+connect+a+tunnel+to+a+Symantec+Gateway+Security+v3.0.1+appliance+using+TheGreenBow+VPN.

Certification of the Symantec Gateway Security v3.0x appliance has NOT been processed by TheGreenBow. However, we assume Symantec did certify it with TheGreenBow IPSec VPN Client before issuing their HowTo webpage. In any case, if you detect any errors in this Configuration Guide (HowTo), we apologize to you in advance and would like you to post a request to our techsupport so we can take the appropriate action.

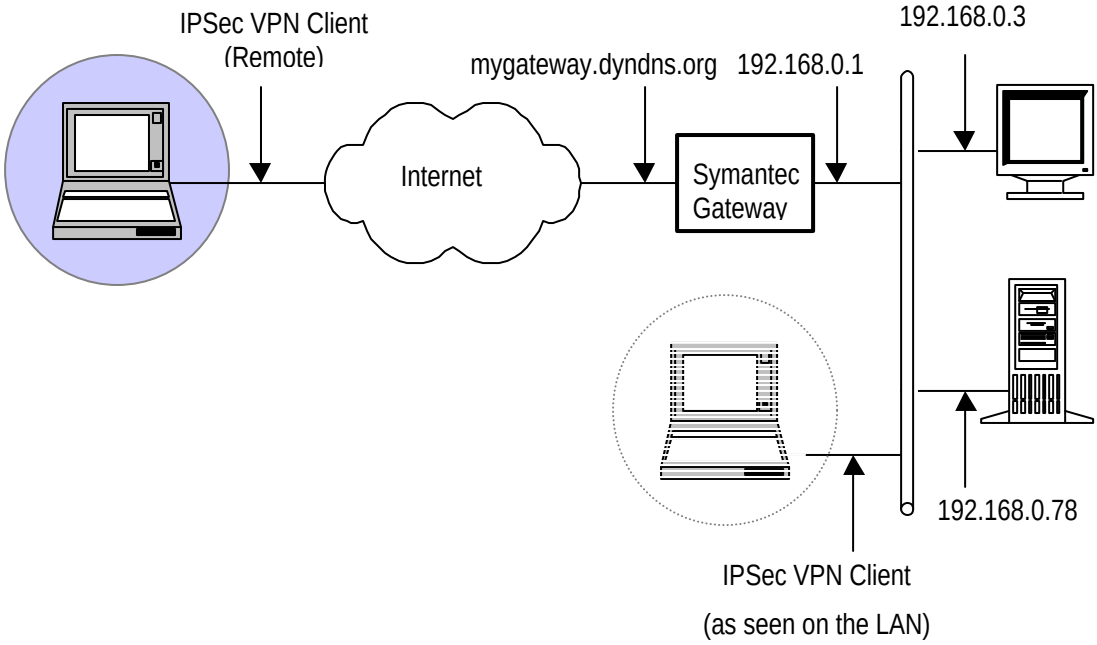
2 Introduction

2.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Symantec Gateway Security v3.0x VPN router.

2.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Symantec Gateway Security v3.0x 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.



2.3 Symantec Gateway Security v3.0x Restrictions

No known restriction.

2.4 Symantec Gateway Security v3.0x VPN Gateway

Tests and VPN configuration have been conducted with Symantec Gateway Security firmware release v3.0 and v3.0.1.

2.5 Symantec Gateway Security v3.0x VPN Gateway product info

It is critical that users find all necessary information about Symantec Gateway Security v3.0x VPN Gateway. All product info, User Guide and knowledge base for the Symantec Gateway Security v3.0x VPN Gateway can be found on the Symantec Gateway Security v3.0x website: www.symantec.com.

Symantec SGS Product page	http://www.symantec.com/avcenter/security/Content/Product/Product_SGS.html

3 Symantec Gateway Security v3.0x VPN configuration

This section describes how to build an IPSec VPN configuration with your Symantec Gateway Security v3.0x VPN router.

Once connected to your Symantec Gateway Security v3.0x VPN gateway, you must select “VPN” in the left pane of the SGM.

On the ‘Tunnels’ tab, double-click your Client VPN tunnel.

In the ‘Tunnel Properties’, click the check mark button beside the ‘Remote Endpoint user group’.

In the ‘User Group Properties’, on the ‘VPN Authentication’ tab, check to make sure that:

- ‘Authentication Scheme’ is set to (none)
- ‘Enforce Client Compliance’ is set to ‘Ignore’

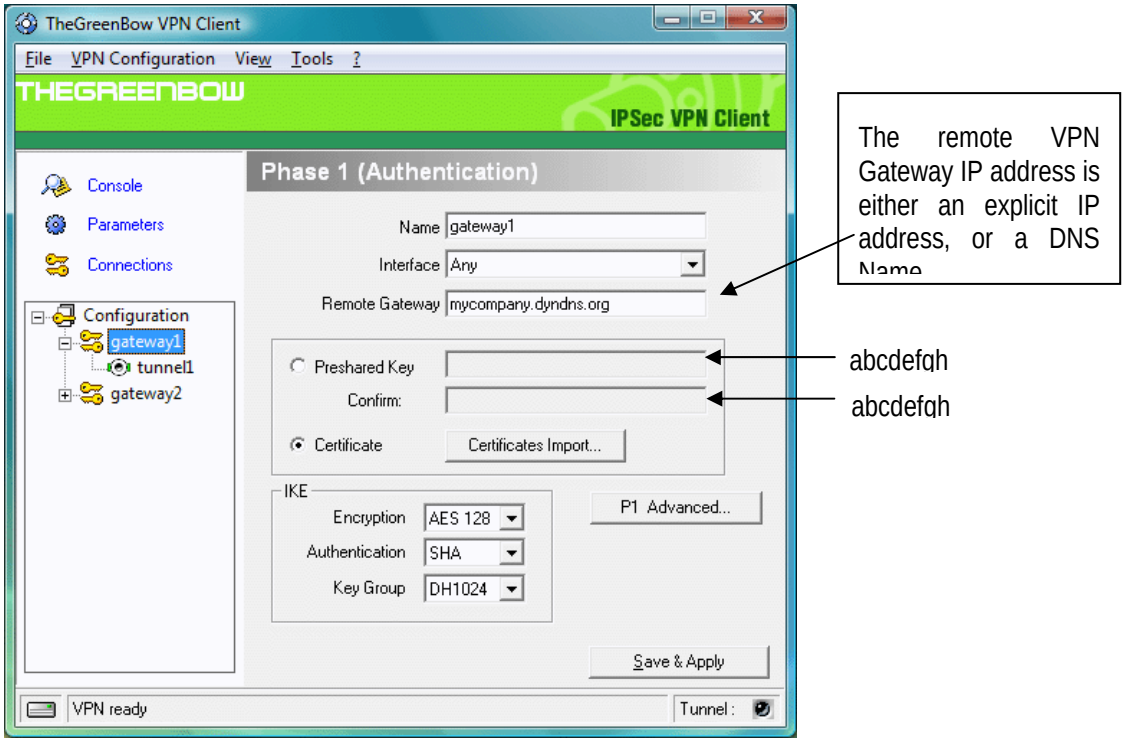
If either the ‘Authentication Scheme’ or ‘Enforce Client Compliance’ is set differently, disable those options or create another user group for use with TheGreenBow IPSec VPN Client.

4 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Symantec Gateway Security v3.0x VPN router.

To download the latest release of TheGreenBow IPSec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html.

4.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 configuration

Phase1 Authentication settings must be as followed:

- Encryption: 3DES
- Authentication: SHA
- Key Group: DH1024

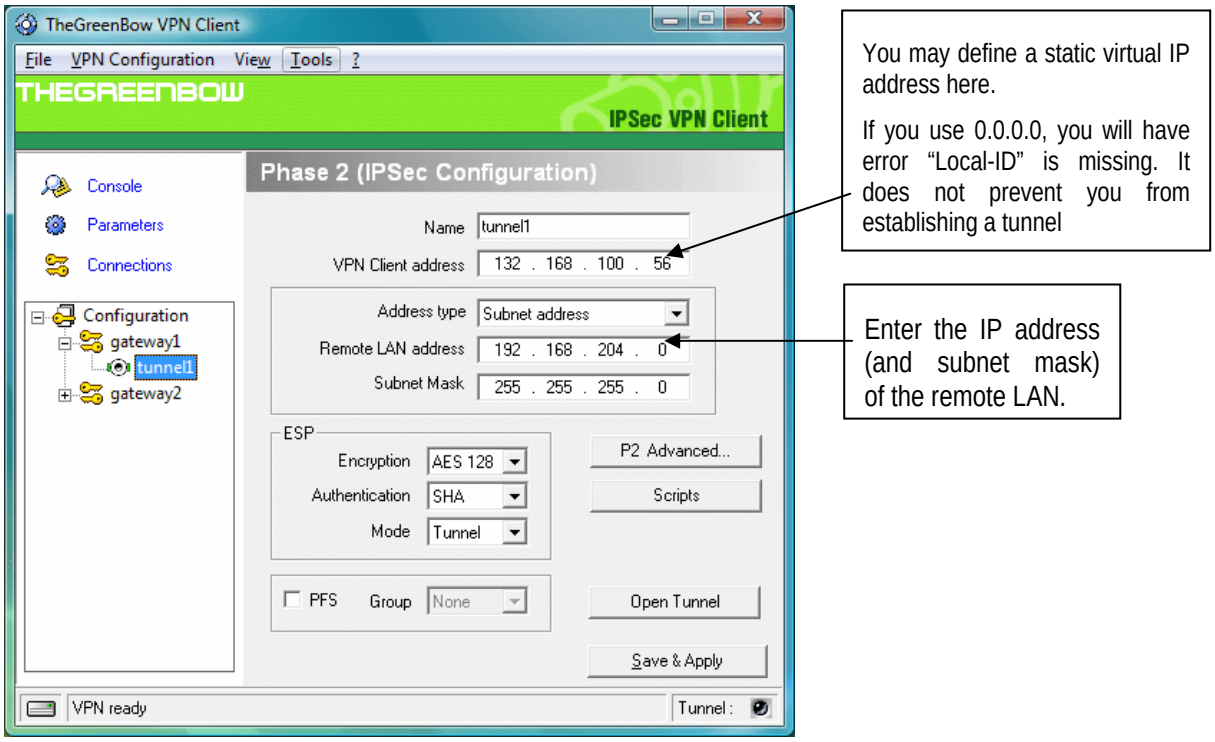
Click P1 Advanced. In the NAT-T drop down box, select Disabled. Check Aggressive Mode.

In the Local ID dropdown box, choose KEY ID. In the text box next to the Local ID dropdown box, type the username.

If your Security Gateway Network Entity has a custom phase 1 ID, then in the Remote ID dropdown box, choose KEY ID. In the text box next to the Remote ID dropdown box, type the custom Phase 1 ID.

You may use either Preshared, Certificates, USB Tokens or X-Auth for User Authentication with the Symantec Gateway Security v3.0x router. This configuration is one example of can be accomplished in term of User Authentication. You may want to refer to either the Symantec Gateway Security v3.0x router user guide or TheGreenBow IPSec VPN Client User Guide for more details on User Authentication options.

4.2 VPN Client Phase 2 (IPSec) Configuration



Phase 2 Configuration

In the lower left pane, right-click the gateway name that was added, then select Add Phase 2. In the right pane, enter the following parameters:

- Name: <A name for the network>
- VPN Client address: 0.0.0.0
- Address Type: Subnet address
- Remote LAN address: <The internal subnet>
- Subnet mask: <The internal subnet mask>
- Encryption: 3DES
- Authentication: SHA
- Mode: Tunnel
- PFS: Checked
- Group: DH1024

Click P2 Advanced. Enter the IP addresses of your internal DNS and/or WINS servers, if any, then click OK.

Repeat Phase1 & Phase2 steps for any other internal networks that you want to connect to.

In the upper left pane, click Parameters. In the right pane, in the Check interval (sec.) text box under Dead Peer Detection (DPD), type: 28800

Click Save & Apply, then close the TheGreenBow VPN configuration dialog box.

4.3 Open IPSec VPN tunnels

Once both Symantec Gateway Security v3.0x 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. 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

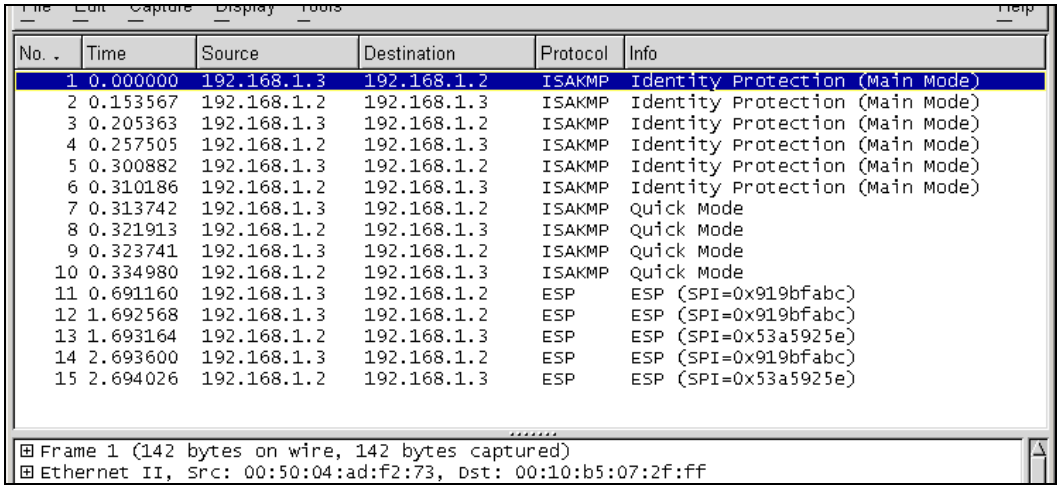
4. Select "Console" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Symantec Gateway Security v3.0x VPN router.

5 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.

5.1 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 http://www.wireshark.org. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (http://www.wireshark.org/docs/).



6 VPN IPSec Troubleshooting

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

```
114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification
type PAYLOAD_MALFORMED
114920 Default SEND Informational  [NOTIFY] with 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.

6.2 « INVALID COOKIE » error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOKIE
115933 Default SEND Informational  [NOTIFY] with 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.

6.3 « no keystate » error

```
115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

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.

6.4 « received remote ID other than expected » error

```
120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
support@thegreenbow.fr
```

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

6.5 « NO PROPOSAL CHOSEN » error

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915    Default    (SA    CNXVPN1-CNXVPN1-P2)    SEND    phase    2    Quick    Mode
[SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational  [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational  [HASH][DEL]
115915 Default CNXVPN1-P1 deleted
```

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:

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

6.6 « INVALID ID INFORMATION » error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626    Default    (SA    CNXVPN1-CNXVPN1-P2)    SEND    phase    2    Quick    Mode
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational  [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

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).

6.7 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).

6.8 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 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 (http://www.wireshark.org) on one of your target computer. You can check that your pings arrive inside the LAN.

7 Contacts

News and updates on TheGreenBow web site: http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com