TheGreenBow IPSec VPN Client

Configuration Guide

Fortinet FortiWifi-60B

FortiOS 4.0.0 - Build 0092

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

Configuration Guide written by:

Writer:	Benjamin Neuhoff
Company:	www.neuhoff.ch

Table of contents

1 Introduction 3
1.1 Goal of this document 3
1.2 VPN Network topology 3
1.3 FortiWifi-60B VPN Gateway 3
1.4 FortiWifi-60B VPN Gateway product info 3
2 FortiWifi-60B VPN configuration 4
2.1 IPsec 4
Create Phase 1 4
Create Phase 2 4
2.2 Firewall 5
Create IPsec Firewall Policy 5
3 TheGreenBow IPSec VPN Client configuration 6
3.1 VPN Client Phase 1 (IKE) Configuration 6
3.2 VPN Client Phase 2 (IPSec) Configuration 7
3.3 Open IPSec VPN tunnels 7
4 Tools in case of trouble 8
4.1 A good network analyser: Wireshark 8
5 VPN IPSec Troubleshooting 9
5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) 9
5.2 « INVALID COOKIE » error 9
5.3 « no keystate » error 9
5.4 « received remote ID other than expected » error 9
5.5 « NO PROPOSAL CHOSEN » error 10
5.6 « INVALID ID INFORMATION » error 10
5.7 I clicked on “Open tunnel”, but nothing happens. 10
5.8 The VPN tunnel is up but I can’t ping ! 10
6 Contacts 12

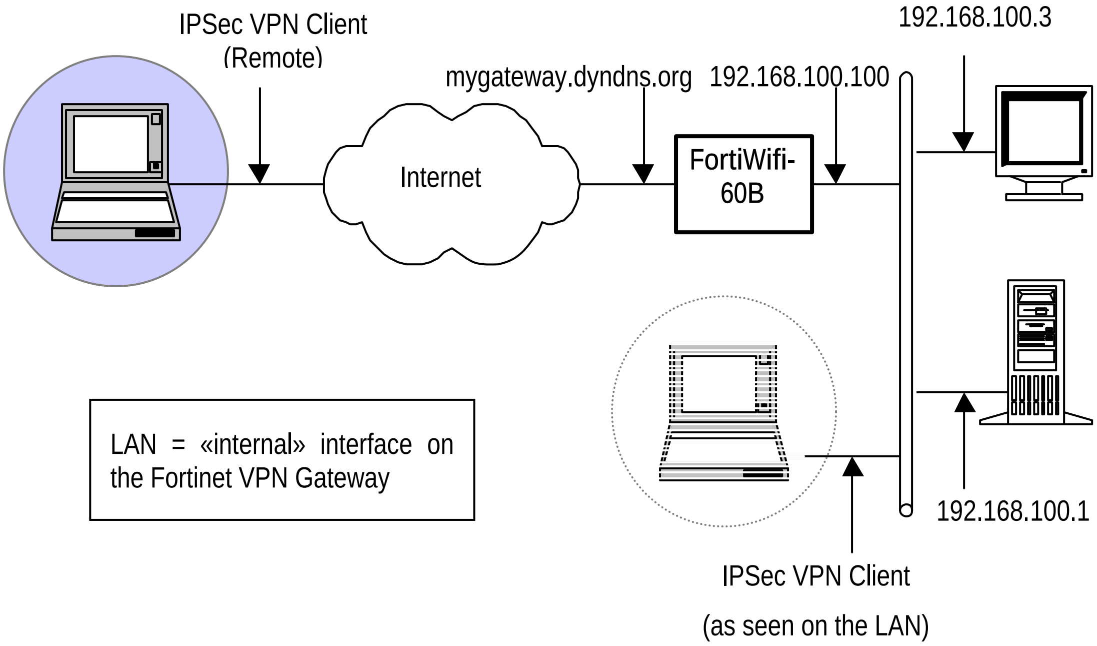
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Fortinet FortiWifi-60B VPN router using a pre-shared key for the authentication. The guide can probably applied for any FortiGate / FortiWifi VPN Router running the same FortiOS as mentioned in section in section 1.3 below.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN (192.168.100.0/255.255.255.0) behind the FortiWifi-60B 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 FortiWifi-60B VPN Gateway

The test and VPN configuration have been conducted with a Fortinet FortiWifi-60B and the following firmware releases:

- FortiOS 4.0.0 - Build 0092
- FortiOS 3.0.0 - MR7 Patch 3 Build 0737

1.4 FortiWifi-60B VPN Gateway product info

It is critical that users find all necessary information about the FortiWifi-60B VPN Gateway. All product info, User Guide and knowledge base for the FortiWifi-60B VPN Gateway can be found on the FortiWifi-60B website: http://kc.forticare.com/.

FortiWifi-60B Product page	http://www.fortinet.com/products/fortiwifi/60B.html
FortiWifi-60B User Guide	http://docs.forticare.com/fgt.html
FortiWifi-60B FAQ/Knowledge Base	http://kc.forticare.com/

2 FortiWifi-60B VPN configuration

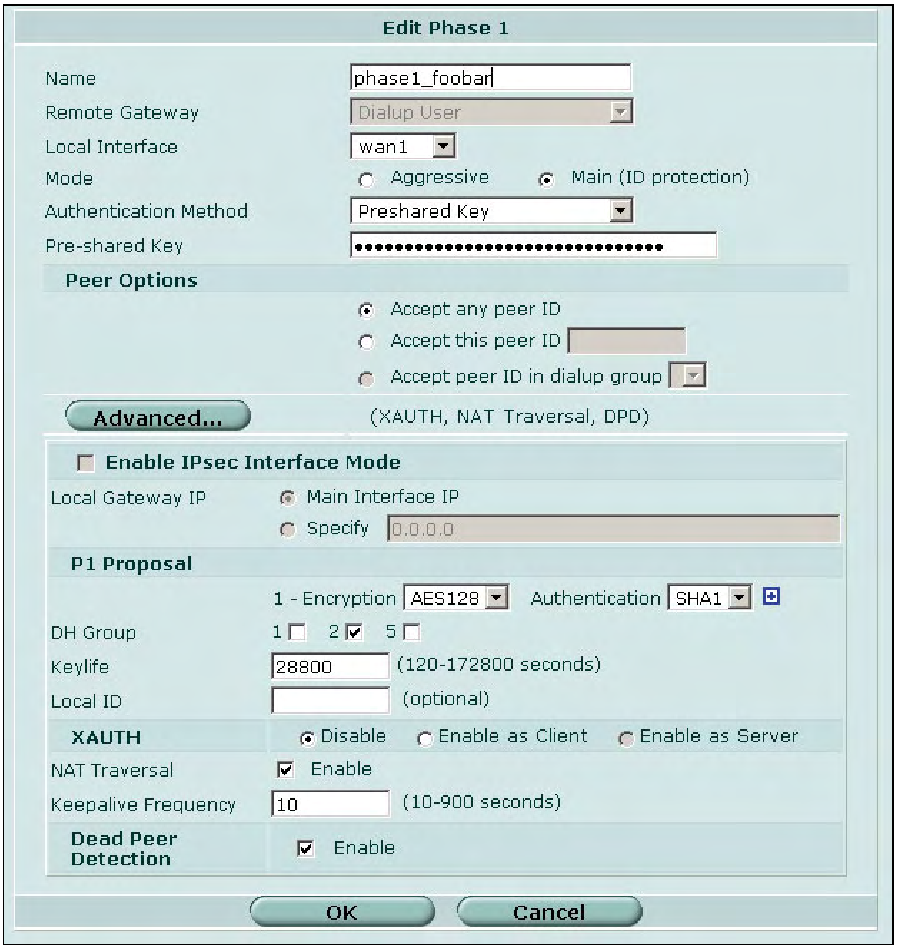
This section describes how to build an IPSec VPN configuration with your FortiWifi-60B VPN router using a pre-shared key for the authentication. For that you need to define the IPsec parameters as well as to create a corresponding firewall policy.

2.1 IPsec

- Once connected to your VPN gateway go to “VPN” -> “IPsec”

Create Phase 1

- Click on “Create Phase 1”
- Click on “Advanced…” to see the form below
- Fill in the proposals shown below and click “OK”. They will also be used in the client settings.
- Have the Pre-shared Key saved somewhere



Edit Phase 1

Name: phase1_foobar
Remote Gateway: Dialup User
Local Interface: wan1
Mode: ○ Aggressive ● Main (ID protection)
Authentication Method: Preshared Key
Pre-shared Key: ••••••••••••••••••••••••••••••••

Peer Options
● Accept any peer ID
○ Accept this peer ID
○ Accept peer ID in dialup group

(XAUTH, NAT Traversal, DPD)

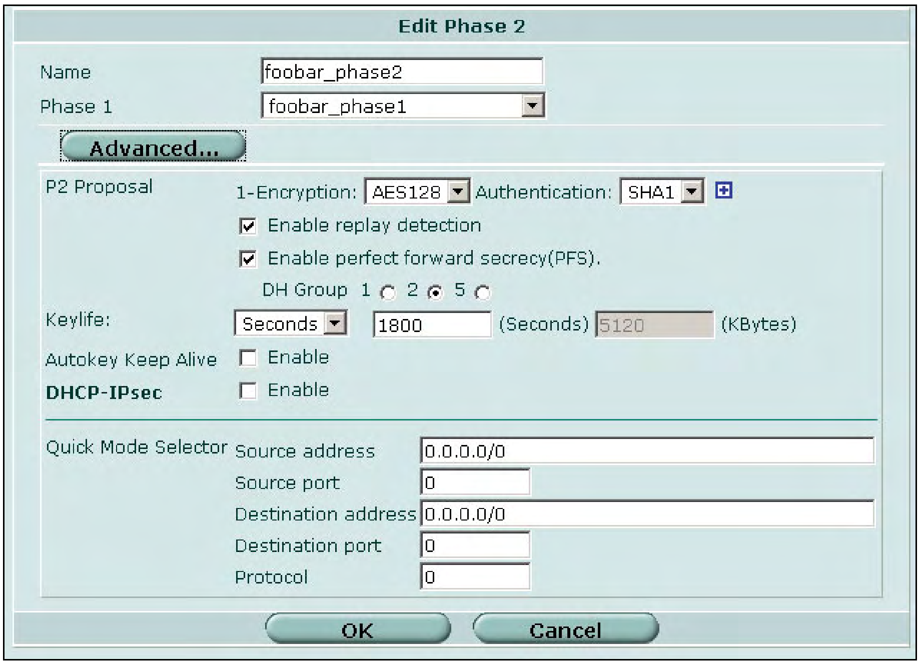
□ Enable IPsec Interface Mode
Local Gateway IP: ● Main Interface IP ○ Specify 0.0.0.0

P1 Proposal
1 - Encryption AES128 Authentication SHA1
DH Group: 1 □ 2 ☑ 5 □
Keylife: 28800 (120-172800 seconds)
Local ID: (optional)

XAUTH: ● Disable ○ Enable as Client ○ Enable as Server
NAT Traversal: ☑ Enable
Keepalive Frequency: 10 (10-900 seconds)
Dead Peer Detection: ☑ Enable

Create Phase 2

- Click on “Create Phase 2”
- Click on “Advanced…” to see the form below
- Fill in the proposals shown below and click “OK”



Edit Phase 2

Name: foobar_phase2

Phase 1: foobar_phase1

P2 Proposal: 1-Encryption: AES128 Authentication: SHA1

☑ Enable replay detection

☑ Enable perfect forward secrecy(PFS).

DH Group 1 ○ 2 ● 5 ○

Keylife: Seconds 1800 (Seconds) 5120 (KBytes)

Autokey Keep Alive ☐ Enable

DHCP-IPsec ☐ Enable

Quick Mode Selector

Source address: 0.0.0.0/0

Source port: 0

Destination address: 0.0.0.0/0

Destination port: 0

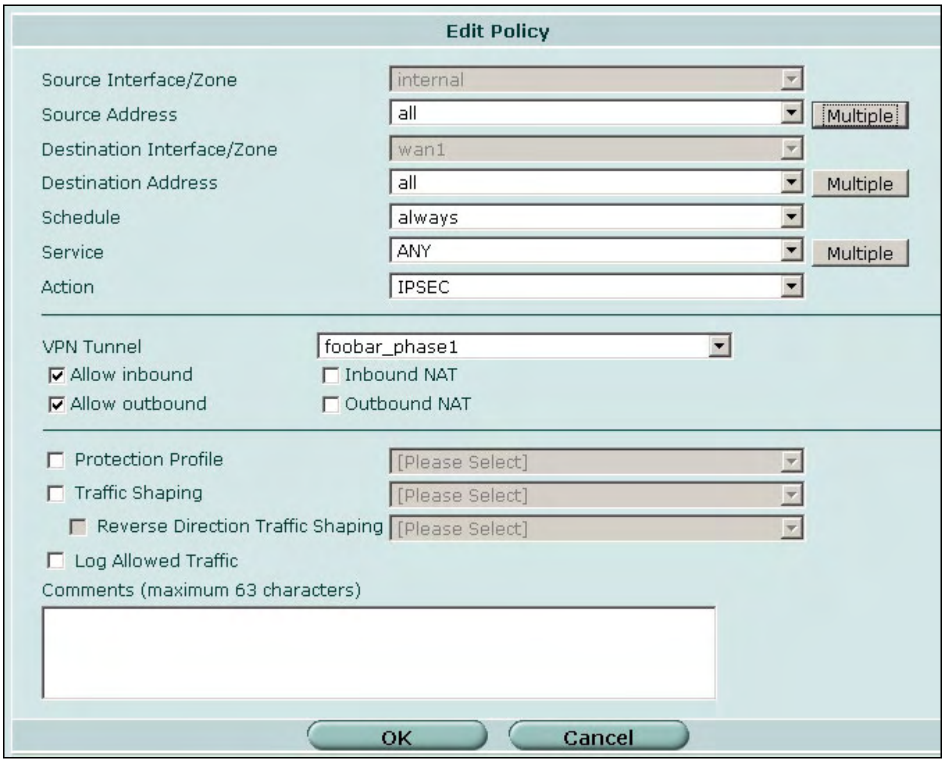
Protocol: 0

2.2 Firewall

Go to “Firewall”- > “Policy”

Create IPsec Firewall Policy

- Click on “Create New”
- Fill in the settings shown below and click “OK”



Edit Policy

Source Interface/Zone: internal

Source Address: all

Destination Interface/Zone: wan1

Destination Address: all

Schedule: always

Service: ANY

Action: IPSEC

VPN Tunnel: foobar_phase1

☑ Allow inbound ☐ Inbound NAT

☑ Allow outbound ☐ Outbound NAT

☐ Protection Profile [Please Select]

☐ Traffic Shaping [Please Select]

☐ Reverse Direction Traffic Shaping [Please Select]

☐ Log Allowed Traffic

Comments (maximum 63 characters)

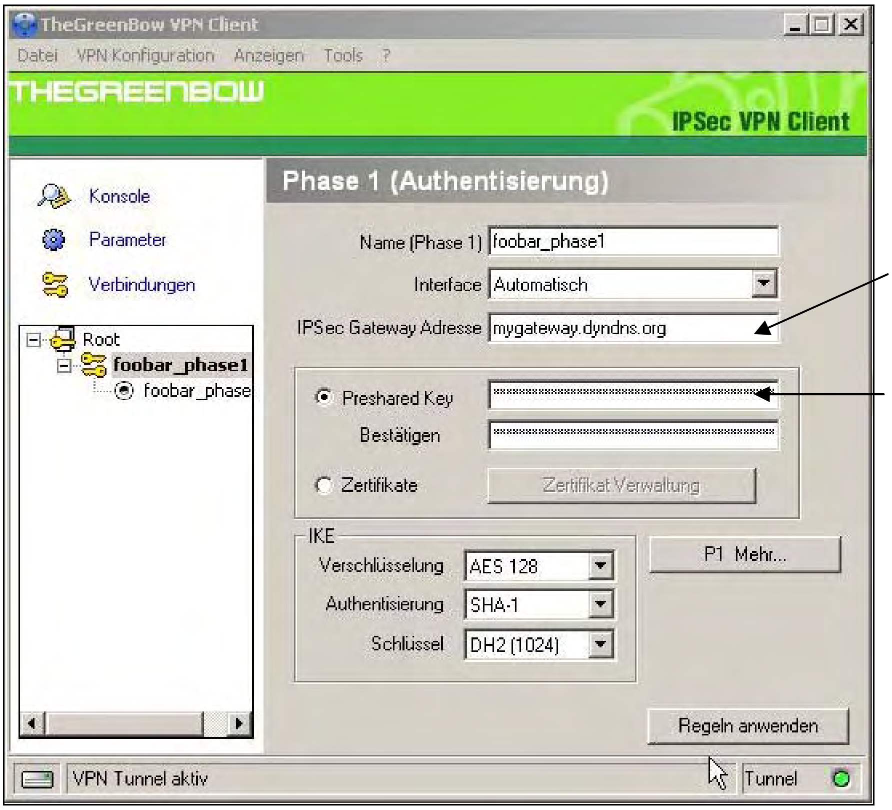
- Logout. You are done with the VPN gateway configuration.

3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a FortiWifi-60B VPN router.

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

3.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 (Authentisierung)

Name (Phase 1) foobar_phase1

Interface Automatisch

IPSec Gateway Adresse mygateway.dyndns.org

● Preshared Key **

Bestätigen **

○ Zertifikate

IKE

Verschlüsselung AES 128

Authentisierung SHA-1

Schlüssel DH2 (1024)

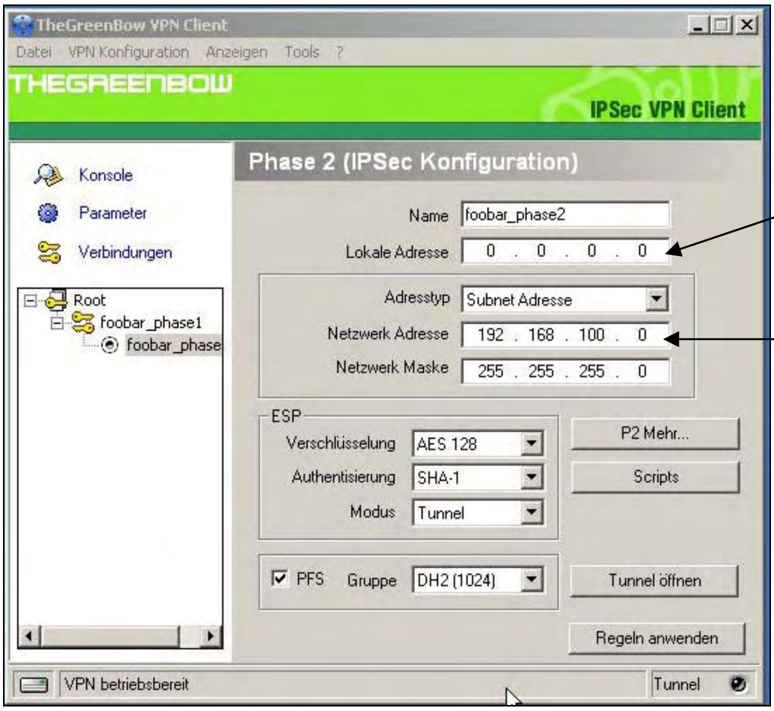
The remote VPN Gateway IP address is either an explicit IP address, or a DNS Name

As defined in section 2.1 on page 4

Phase 1 configuration

You may use either Preshared, Certificates, USB Tokens or X-Auth combined with RADIUS Server for User Authentication with the FortiWifi-60B router. This configuration is one example of can be accomplished in term of User Authentication. You may want to refer to either the FortiWifi-60B router user guide or TheGreenBow IPSec VPN Client User Guide for more details on User Authentication options.

3.2 VPN Client Phase 2 (IPSec) Configuration



Phase 2 (IPSec Konfiguration)

Name foobar_phase2

Lokale Adresse 0 . 0 . 0 . 0

Adresstyp Subnet Adresse

Netzwerk Adresse 192 . 168 . 100 . 0

Netzwerk Maske 255 . 255 . 255 . 0

ESP

Verschlüsselung AES 128

Authentisierung SHA-1

Modus Tunnel

☑ PFS Gruppe DH2 (1024)

You may define a static virtual IP address here.

If you use 0.0.0.0, you will have error "Local-ID" is missing. It does not prevent you from establishing a tunnel

Enter the IP address (and subnet mask) of the remote LAN. (by default called "internal" on the Fortinet VPN gateway

Phase 2 Configuration

3.3 Open IPSec VPN tunnels

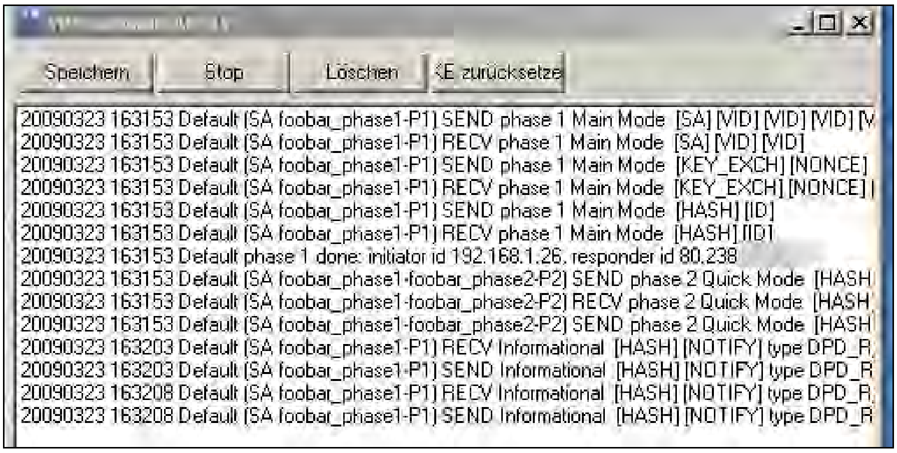
Once both FortiWifi-60B router and TheGreenBow IPSec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

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 FortiWifi-60B VPN router.



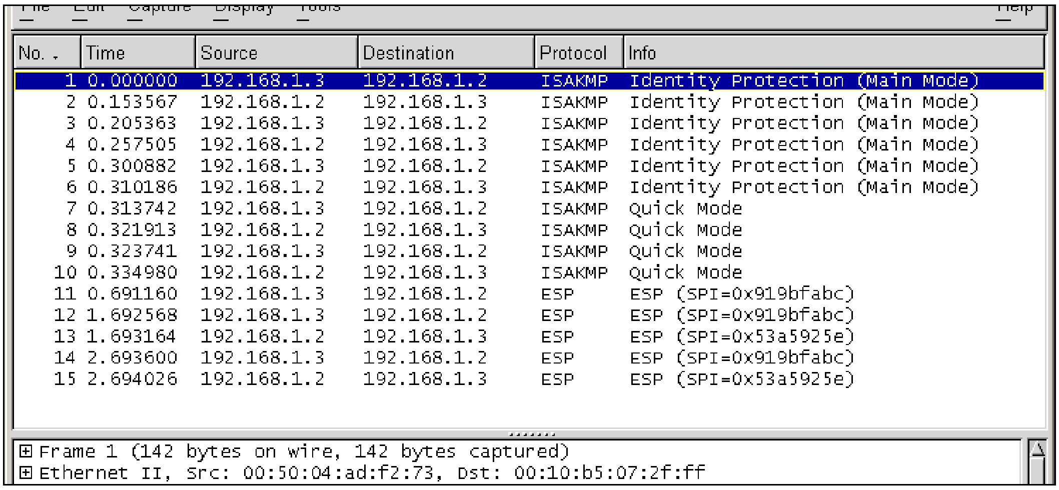
```
20090323 163153 Default (SA foobar_phase1-P1) SEND phase 1 Main Mode  [SA] [VID] [VID] [VID] [V
20090323 163153 Default (SA foobar_phase1-P1) RECV phase 1 Main Mode  [SA] [VID] [VID]
20090323 163153 Default (SA foobar_phase1-P1) SEND phase 1 Main Mode  [KEY_EXCH] [NONCE]
20090323 163153 Default (SA foobar_phase1-P1) RECV phase 1 Main Mode  [KEY_EXCH] [NONCE] [
20090323 163153 Default (SA foobar_phase1-P1) SEND phase 1 Main Mode  [HASH] [ID]
20090323 163153 Default (SA foobar_phase1-P1) RECV phase 1 Main Mode  [HASH] [ID]
20090323 163153 Default phase 1 done: initiator id 192.168.1.26, responder id 80.238
20090323 163153 Default (SA foobar_phase1-foobar_phase2-P2) SEND phase 2 Quick Mode  [HASH
20090323 163153 Default (SA foobar_phase1-foobar_phase2-P2) RECV phase 2 Quick Mode  [HASH
20090323 163153 Default (SA foobar_phase1-foobar_phase2-P2) SEND phase 2 Quick Mode  [HASH
20090323 163203 Default (SA foobar_phase1-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R
20090323 163203 Default (SA foobar_phase1-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R
20090323 163208 Default (SA foobar_phase1-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R
20090323 163208 Default (SA foobar_phase1-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R
```

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 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/).



```
No. .  Time      Source        Destination   Protocol Info
    1 0.000000  192.168.1.3   192.168.1.2   ISAKMP   Identity Protection (Main Mode)
    2 0.153567  192.168.1.2   192.168.1.3   ISAKMP   Identity Protection (Main Mode)
    3 0.205363  192.168.1.3   192.168.1.2   ISAKMP   Identity Protection (Main Mode)
    4 0.257505  192.168.1.2   192.168.1.3   ISAKMP   Identity Protection (Main Mode)
    5 0.300882  192.168.1.3   192.168.1.2   ISAKMP   Identity Protection (Main Mode)
    6 0.310186  192.168.1.2   192.168.1.3   ISAKMP   Identity Protection (Main Mode)
    7 0.313742  192.168.1.3   192.168.1.2   ISAKMP   Quick Mode
    8 0.321913  192.168.1.2   192.168.1.3   ISAKMP   Quick Mode
    9 0.323741  192.168.1.3   192.168.1.2   ISAKMP   Quick Mode
   10 0.334980  192.168.1.2   192.168.1.3   ISAKMP   Quick Mode
   11 0.691160  192.168.1.3   192.168.1.2   ESP      ESP (SPI=0x919bfabc)
   12 1.692568  192.168.1.3   192.168.1.2   ESP      ESP (SPI=0x919bfabc)
   13 1.693164  192.168.1.2   192.168.1.3   ESP      ESP (SPI=0x53a5925e)
   14 2.693600  192.168.1.3   192.168.1.2   ESP      ESP (SPI=0x919bfabc)
   15 2.694026  192.168.1.2   192.168.1.3   ESP      ESP (SPI=0x53a5925e)

⊞ Frame 1 (142 bytes on wire, 142 bytes captured)
⊞ Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff
```

5 VPN IPSec Troubleshooting

5.1 « 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.

5.2 « 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.

5.3 « 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.

5.4 « 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.

5.5 « 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
```

5.6 « 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).

5.7 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).

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 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.

6 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