TheGreenBow IPSec VPN 客户端

配置向导

DWnet SAFEcon5

网站： http://www.thegreenbow.com http://www.dwnet.com.cn

联系方式： support@thegreenbow.com service@dwnet.com.cn

目 录

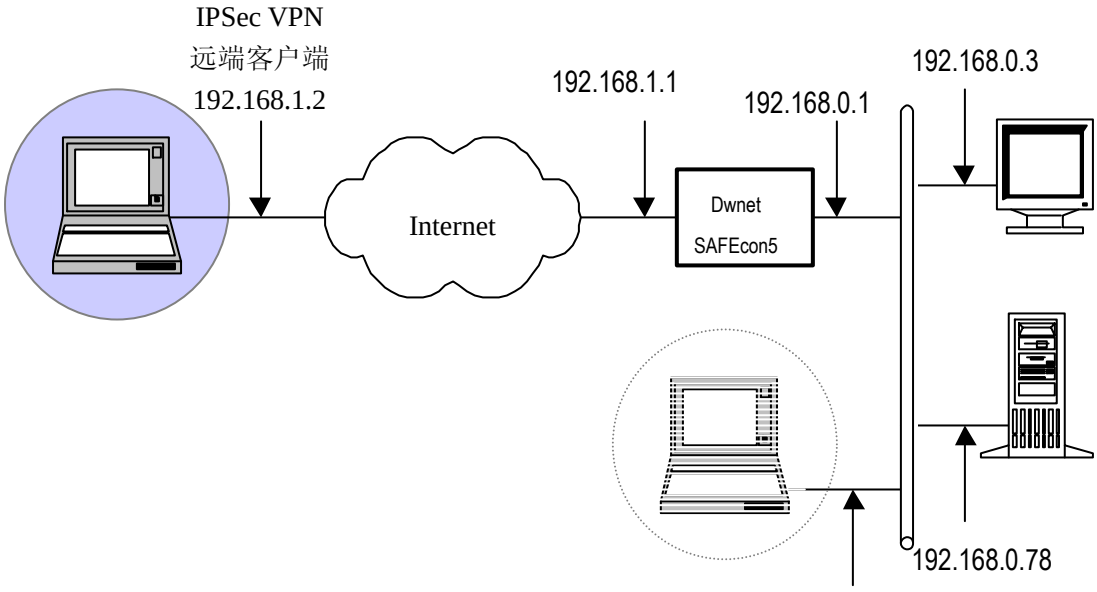
1 介绍

1.1 手册用途

这篇设定向导旨在介绍如何使用 TheGreenbow IPSec VPN 客户端和 DWnet SAFEcon5 VPN 防火墙建立 VPN 连接。

1.2 VPN 网络

在 VPN 连接示例中，将演示 TheGreenbow IPSec VPN 客户端和 DWnet SAFEcon5 VPN 防火墙建立 VPN 连接的过程。VPN 客户端使用 DSL 或者通过局域网上网。文中所有 IP 地址仅为示例使用。



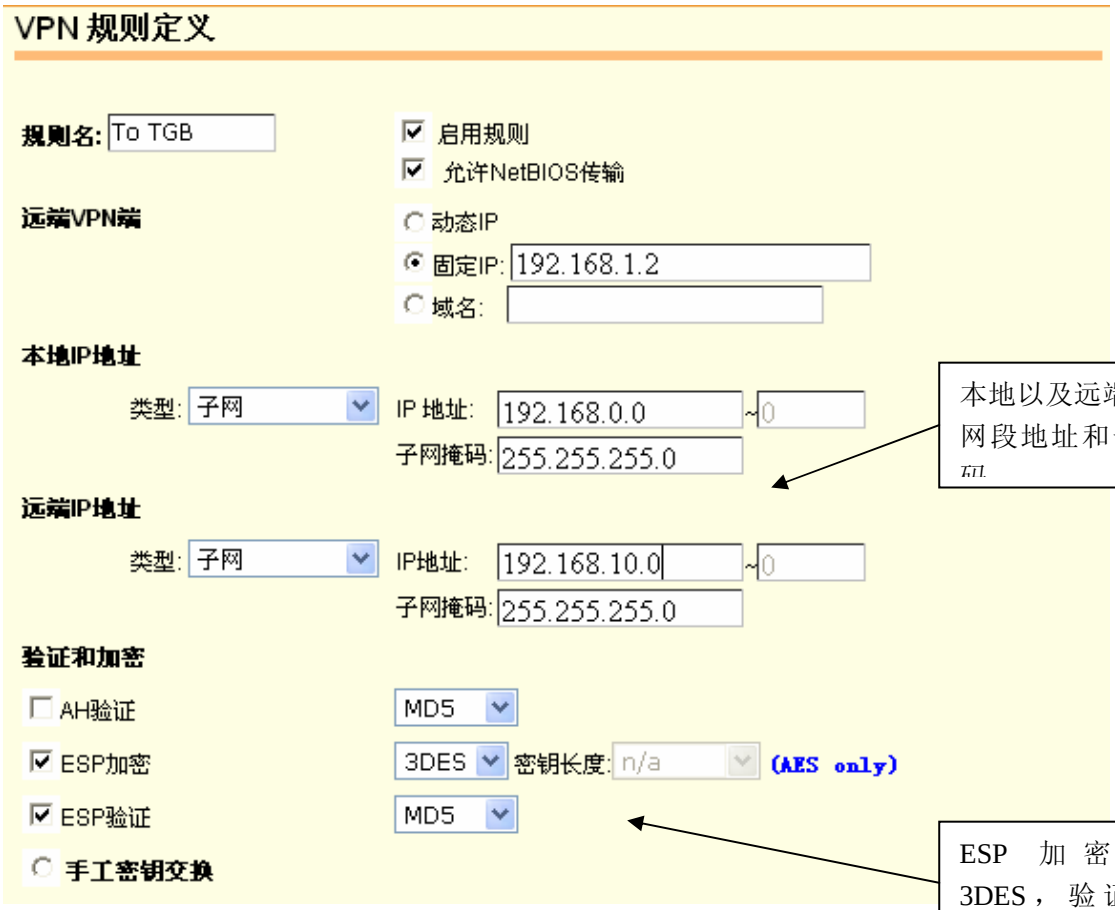
1.3 DWnet SAFEcon5 VPN 防火墙

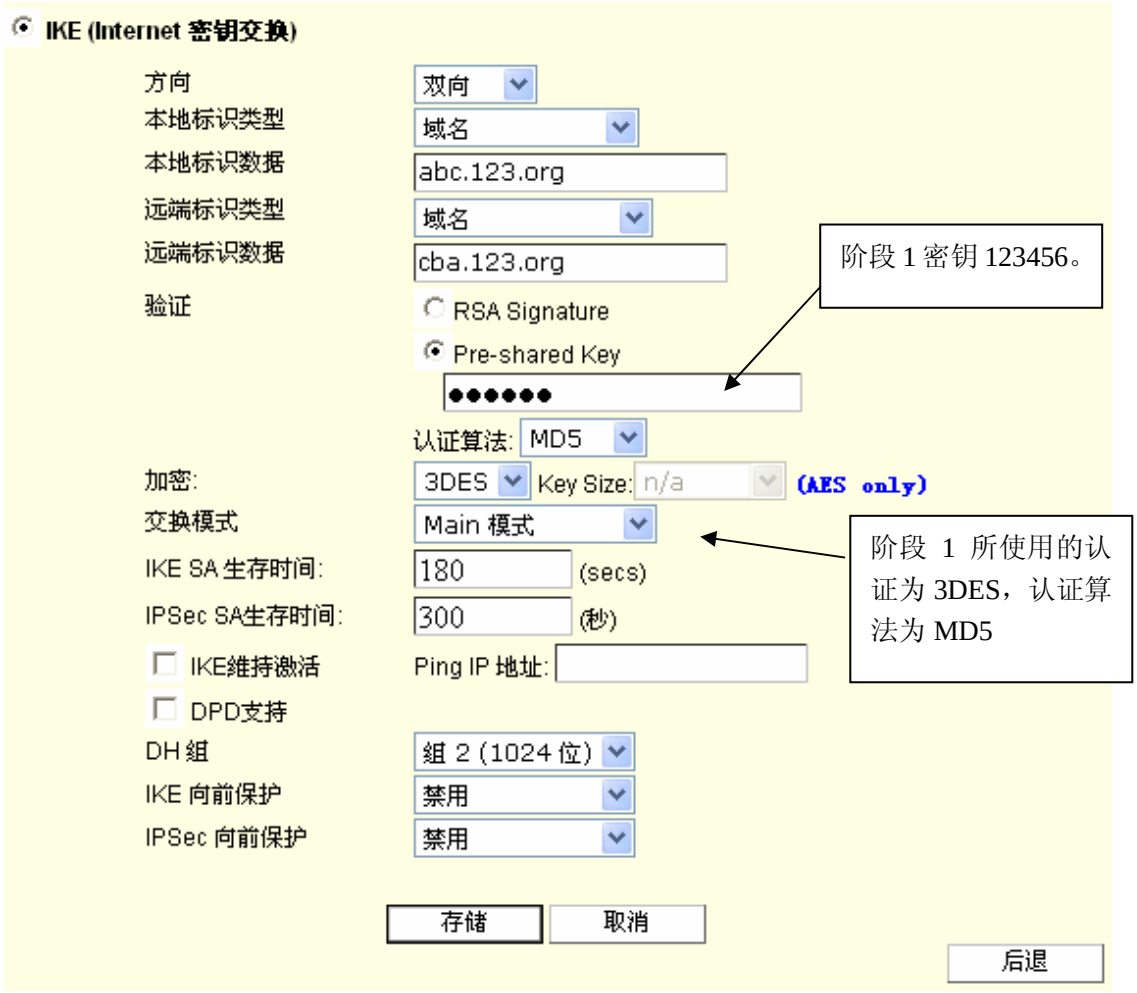
示例中 DWnet SAFEcon5 VPN 防火墙软件版本为 Release A0 Version 18。

2 DWnet SAFEcon5 VPN 防火墙 VPN 配置

这章介绍 SAFEcon5 VPN 防火墙如何建立 VPN 连接。

一但连接到 VPN 防火墙，您需要进入“VPN（IPSec）”界面，点击“添加新规则”按钮进行设置。

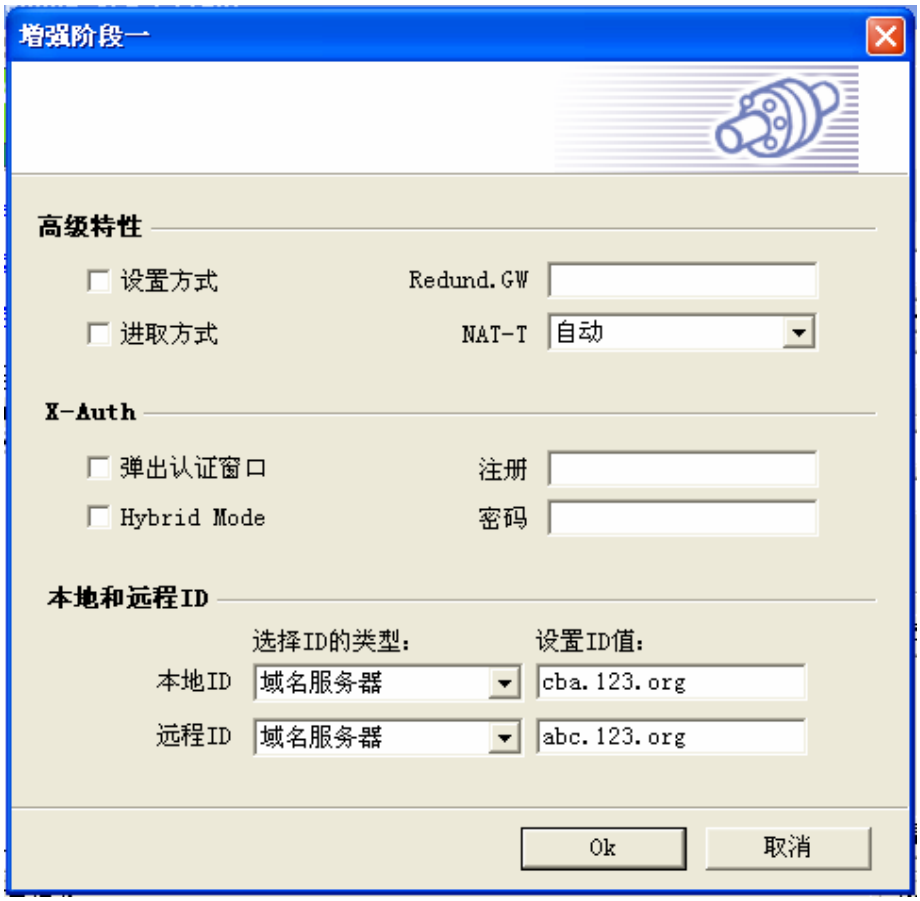



IKE (Internet 密钥交换)
方向
双向
本地标识类型
域名
本地标识数据
abc.123.org
远端标识类型
域名
远端标识数据
cba.123.org
验证
RSA Signature
Pre-shared Key
●●●●●●
认证算法: MD5
加密:
3DES
Key Size:
n/a
(AES only)
交换模式
Main 模式
IKE SA 生存时间:
180
(secs)
IPSec SA生存时间:
300
(秒)
IKE维持激活
Ping IP 地址:
DPD支持
DH 組
組 2 (1024 位)
IKE 向前保护
禁用
IPSec 向前保护
禁用
存储
取消
后退
阶段 1 密钥 123456。
阶段 1 所使用的认证为 3DES，认证算法为 MD5

3 TheGreenbow IPSec VPN 客户端设置

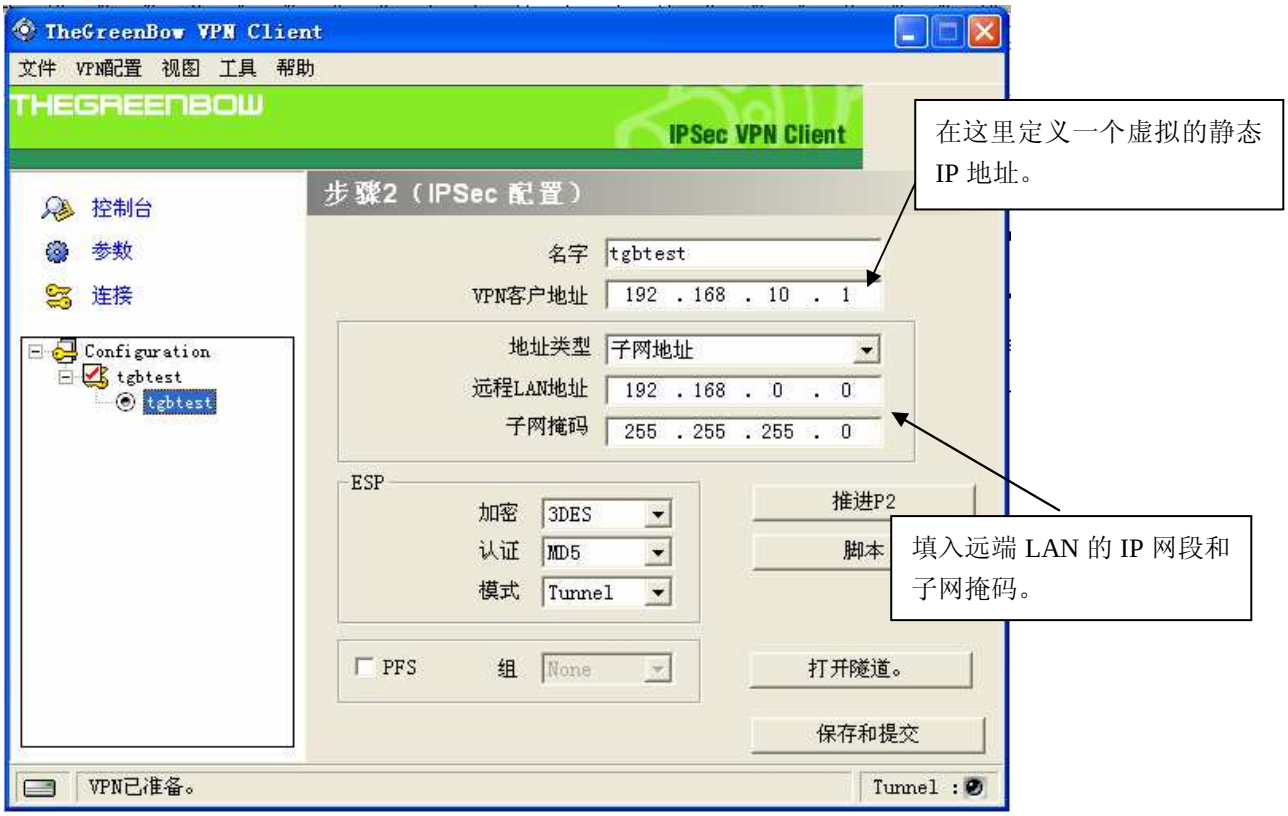
3.1 VPN 客户端第一阶段（IKE 阶段）设置

阶段 1 设置


增强阶段一
高级特性
设置方式
进取方式
Redund.GW
NAT-T
自动
X-Auth
弹出认证窗口
Hybrid Mode
注册
密码
本地和远程ID
选择ID的类型:
设置ID值:
本地ID
域名服务器
cba.123.org
远程ID
域名服务器
abc.123.org
Ok
取消

阶段 1 （高级设置）

3.2 VPN 客户端第二阶段（IPSec 阶段）设置



阶段 2 设置

3.3 启用 IPSec VPN 隧道

当 SAFEcon5 VPN 防火墙和 TheGreenbow IPSec VPN 客户端都设置好以后，准备启用 VPN 隧道。首先，确保防火墙允许 IPSec 数据流通过。

1、 点 "**保存和提交**" 保存并应用已经在 VPN 客户端做过的设置。
2、 点 "**打开隧道**" 自动启用一条 IPSec VPN 隧道。
3、 点 "**连接**" 查看已经启动的 VPN 隧道。
4、 点 "**控制台**" ，如果您想获得 IPSec VPN 日志，获取 IPSec VPN 的信息，使用此功能。下面的图显示了 TheGreenbow IPSec VPN 客户端和 DWnet SAFEcon5 VPN 防火墙成功连接 IPSec VPN 的状态信息。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	192.168.1.1	ISAKMP	Identity Protection (Main Mode)
2	0.002537	192.168.1.1	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
3	0.027169	192.168.1.2	192.168.1.1	ISAKMP	Identity Protection (Main Mode)
4	0.489477	192.168.1.1	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
5	0.517998	192.168.1.2	192.168.1.1	ISAKMP	Identity Protection (Main Mode)
6	1.063896	192.168.1.1	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
7	1.066122	192.168.1.2	192.168.1.1	ISAKMP	Quick Mode
8	1.071811	192.168.1.1	192.168.1.2	ISAKMP	Quick Mode
9	1.072777	192.168.1.2	192.168.1.1	ISAKMP	Quick Mode
10	5.105201	192.168.1.1	192.168.1.2	ISAKMP	Quick Mode
11	5.105683	192.168.1.2	192.168.1.1	ISAKMP	Quick Mode
12	10.105373	192.168.1.1	192.168.1.2	ISAKMP	Quick Mode
13	10.105846	192.168.1.2	192.168.1.1	ISAKMP	Quick Mode
14	15.105090	192.168.1.1	192.168.1.2	ISAKMP	Quick Mode
15	15.105553	192.168.1.2	192.168.1.1	ISAKMP	Quick Mode

```
⊞ Frame 1 (202 bytes on wire, 202 bytes captured)
⊞ Ethernet II, Src: 00:13:8f:b9:7e:df (00:13:8f:b9:7e:df), Dst: 00:c0:02:ed:ed:ee (00:c0:02:ed:ed:ee)
⊞ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)
⊞ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
⊞ Internet Security Association and Key Management Protocol
```

4 故障排除工具

配置一条 IPSec VPN 隧道可能是一项很难的工作。一个疏忽的参数设置就能阻碍 VPN 建立。一些工具可以在 VPN 建立过程中找到产生问题的原因所在。

4.1 一个好的网络分析工具：Ethereal

Ethereal 是可以分析数据包和包流程的免费软件。它显示在网卡上收到的 IP 和 TCP 数据包。这个工具可以在这个链接找到 http://www.ethereal.com/。它可以用在两个设备之间搜集协议交换流程。该软件的详细安装和使用细节，请参看它的说明。

5 IPSec VPN 问题分析

5.1 « PAYLOAD MALFORMED »错误(阶段 1 建立错误)

```
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
```

如果遇到 « PAYLOAD MALFORMED » 错误，有可能是您输入了错误的第一阶段[SA], 检查一下是否 VPN 隧道两端都采用了相同的加密算法。

5.2 « INVALID COOKIE » 错误

```
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
```

如果遇到 « INVALID COOKIE » 错误, 表示两个 VPN 端中其中有一个端点正在使用 SA 不能再被使用。重新建立两个端点的 VPN 连接。

5.3 « no keystate » 错误

```
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
```

检查"**preshared key**" 是否正确或者检查"**local ID**" 是否正确，你应该能够从远端的 VPN 端点的日志上获取更多的信息。

5.4 « received remote ID other than expected » 错误

```
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
```

两端的" **Remote ID** "不匹配。

5.5 « NO PROPOSAL CHOSEN » 错误

```
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
```

出现 « NO PROPOSAL CHOSEN » 错误时，检查两端阶段 2 加密方式和密码是否相同。
如果相同，再检查阶段 1 的认证方式是否相同。

```
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 » 错误

```
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
```

出现 « INVALID ID INFORMATION » 错误时，检查阶段 2 的 ID (本地 IP 地址和网络地址)是否正确并且和远端相对应，同样，还要检查 ID 类型 (“子网掩码” 和 “地址范围”)。

5.7 “我点击‘打开隧道’，但是什么都没出现”

查看 VPN 两端的日志，IKE 请求可能被防火墙阻挡掉了。所有的 IPSec 客户端使用 UDP 500 的端口，ESP 协议。

5.8 “VPN 隧道被激活了，但是我 Ping 不通”

如果 VPN 隧道已经被激活了，但是你仍然 ping 不通对方的网关，请看下面的几点建议：

- 检查阶段 2 的设置：VPN 客户端地址和远端 LAN 地址。通常，VPN 客户端 IP 地址不应该和远端相同。
- 如果 VPN 隧道被激活了，数据包都会以 ESP 协议形式发送。ESP 可能会被防火墙阻挡掉，检查并确认在 VPN 客户端和服务器之间的设备都允许 ESP 协议通过。
- 检查 VPN 服务器上的日志，VPN 数据包有可能被它的防火墙规则阻挡掉了。
- 确认您的 ISP 支持 ESP。
- 如果您还是 ping 不通，抓取 VPN 服务器和 LAN 发出 ping 命令的电脑之间的数据包(例如使用 Ethereal)，您会在这上面发现一些信息
- 检查 VPN 服务器 LAN 内的“默认网关”，远端 LAN 内的一台计算机可能收到了您发出的 ping 请求，但是并没有设置回应。
- 您不能通过计算机名访问到远端 LAN 的计算机，您必须指定它们在 LAN 内的 IP 地址。
- 我们建议您在目标计算机上安装 Ethereal (http://www.ethereal.com) ，您可以检查 ping 命令是否到达了这台计算机。

6 链接

TheGreenbow 新闻和更新网站：http://www.thegreenbow.com
技术支持信箱：support@thegreenbow.com
销售支持信箱：info@thegreenbow.com

DWnet 官方网站： http://www.dwnet.com.cn
技术支持信箱： service@dwnet.com.cn
销售联系方式： +86 0512 67615551