



THEGREENBOW



TheGreenBow VPN

客户端软件与

天融信 NG 系列

防火墙

— 配置手册

WebSite: <http://www.thegreenbow.com/zh>

Contact: support@thegreenbow.com

目 录

1	介绍	3
1.1	手册用途	3
1.2	VPN 网络	3
1.3	天融信 防火墙	3
1.4	天融信 防火墙 产品信息	3
2	天融信 防火墙 VPN 配置	4
3	VPN 客户端设置	6
3.1	VPN 客户端第一阶段 (IKE 阶段) 设置	6
3.2	VPN 客户端第二阶段 (IPSec 阶段) 设置	8
3.3	启用 IPSec VPN 隧道	9
4	故障排除工具	10
4.1	一个好的网络分析工具 : Wireshark	10
5	IPSec VPN 问题分析	11
5.1	« 畸形载荷 » 错误 (阶段 1 建立错误)	11
5.2	« 无效 COOKIE » 错误	11
5.3	« no keystate » 错误	11
5.4	« 接收到的远程 ID 与所期不符 » 错误	11
5.5	« no proposal chosen » 错误	12
5.6	« 无效的 ID 信息 » 错误	12
5.7	“ 我点击 ‘ 打开隧道 ’ , 但是什么都没出现 ”	12
5.8	“ VPN 隧道被激活了 , 但是我 Ping 不通 ”	12
6	联系我们	14

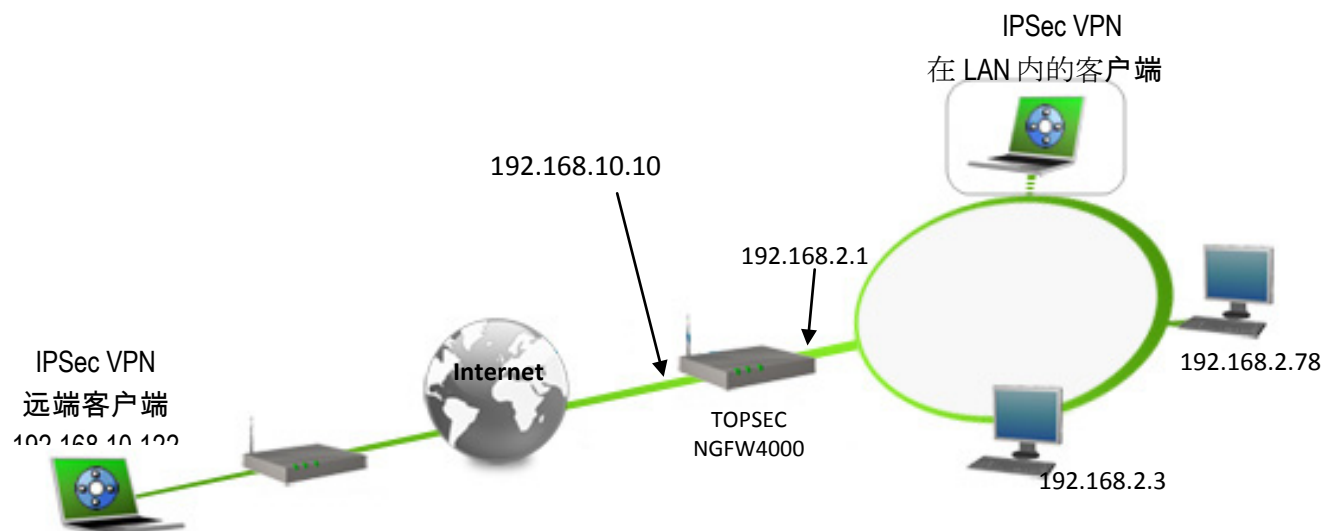
1 介绍

1.1 手册用途

此配置手册旨在介绍如何使用 TheGreenBow VPN 客户端和天融信 NG 系列防火墙建立 VPN 连接。

1.2 VPN 网络

在 VPN 连接示例中，将演示 IPsec VPN 客户端和天融信 NG 系列防火墙建立 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 天融信 防火墙

示例中天融信 TOPSEC NGFW4000 系列防火墙软件版本为 v3.3.005.066.1 版。

1.4 天融信 防火墙 产品信息

用户需要找到天融信 TOPSEC NGFW4000 系列防火墙的所有相关信息。

所有产品信息，用户手册和关于天融信 防火墙的信息可在该网站找到：

<http://www.topsec.com.cn>

2 天融信 防火墙VPN配置

本章介绍天融信 TOPSEC NGFW4000 系列防火墙如何建立 VPN 连接。

一旦连接到 VPN 防火墙，您需要进入“虚拟专网（静态隧道）”界面，点击“添加隧道”按钮进行设置。

设置第一阶段：

设置第二阶段：

添加地址簿：

主机 | 范围 | 子网 | 地址组

主机地址 [添加] [清空]

名称	IP地址	修改	删除
192.168.10.122	192.168.10.122		

主机 | 范围 | 子网 | 地址组

子网 [添加] [清空]

名称	IP地址	掩码地址	除去地址	修改	删除
local_net	192.168.2.0	255.255.255.0			-

虚拟接口绑定：

虚拟接口绑定

虚接口名：

通告IP地址：

绑定接口名：

接口地址：

添加访问控制策略：

访问控制规则 [添加组] [添加策略] [清空策略]

目的区域 策略组 [高级搜索](#) 每页

[1]

ID	控制	源	目的	服务	时间	日志	选项	修改	复制	移动	插入	删除	状态
8051	✓	区域: trust 地址: local_net	区域: untrust 地址: 192.168.10.122										
8044	✓	区域: area_eth0 地址: any	区域: area-3 地址: any	PING HTTP DNS_Transfer									
8052	✓	区域: untrust 地址: 192.168.10.122	区域: trust 地址: local_net										

3 VPN客户端设置

本章介绍如何配置 VPN 客户端和天融信 TOPSEC NGFW4000 系列防火墙建立 VPN 连接。

请通过以下链接下载 TheGreenBow IPsec VPN 客户端软件最新版本：http://www.thegreenbow.com/zh/vpn_down.html

3.1 VPN客户端第一阶段 (IKE阶段) 设置



阶段 1 设置

第一阶段高级

高级功能

配置模式 冗余网关

挑战模式 NAT 穿越

扩展认证

扩展认证弹窗 登录名

Hybrid Mode 密码

本地及远端 ID

选择 ID 类型： 设定 ID 数值：

本地 ID

远端 ID

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



阶段 2 (高级设置)

3.3 启用IPSec VPN隧道

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

- 1、点击“保存和提交”保存并应用已经在 VPN 客户端做过的设置。
- 2、点击“打开隧道”自动启用一条 IPSec VPN 隧道。
- 3、点击“连接”查看已经启动的 VPN 隧道。
- 4、点击“控制台”。若您想获得 IPSec VPN 日志，获取 IPSec VPN 的信息，使用此功能。

4 故障排除工具

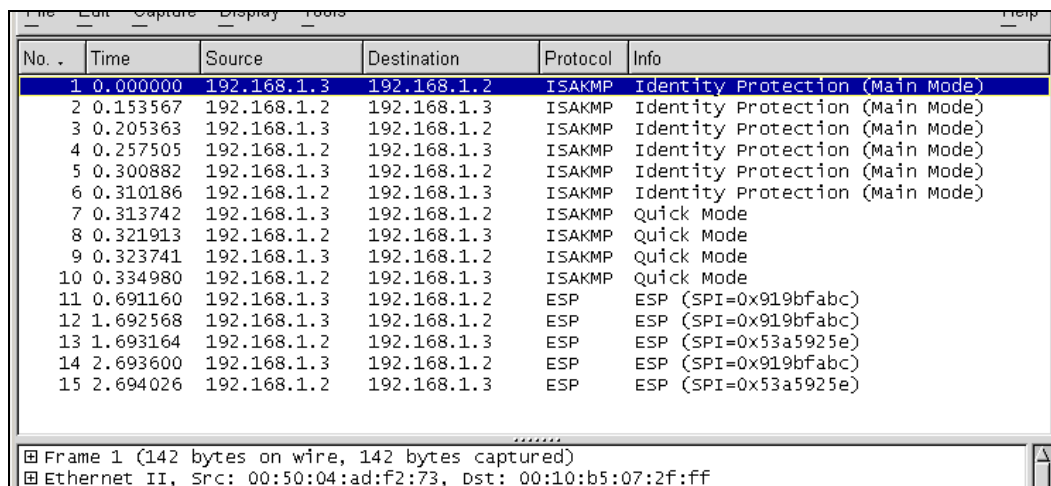
配置一条 IPsec VPN 隧道可能是一项很难的工作。一个疏忽的参数设置就能阻碍 VPN 建立。

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：Wireshark

Wireshark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.wireshark.org>。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(<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 IPsec VPN问题分析

5.1 « 畸形载荷 » 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 « 畸形载荷 » 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 « 无效 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 « 无效 COOKIE » 错误，它表示 VPN 端点 (客户端或点) 的其中一端正在使 SA 而不能再被使用。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“预共享密钥”是否正确或者检查“本地 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 « 接收到的远程ID与所期不符 » 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“远程 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 « 无效的 ID 信息 » 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 « 无效的 ID 信息 » 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。

Doc.Ref	tgvpn_cg_天融信 NG 系列防火墙
Doc.version	1.0 – Jun 2010
VPN version	4.65.003

- ◆ 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Wireshark (<http://www.wireshark.org>)，您可以检查 ping 命令是否到达了这台计算机。

	Doc.Ref	tgvpn_cg_天融信 NG 系列防火墙
	Doc.version	1.0 – Jun 2010
	VPN version	4.65.003

6 联系我们

请登陆TheGreenBow 网站：<http://www.thegreenbow.com/zh/>

联系我们的技术支持：support@thegreenbow.com

联系我们的业务部门：sales@thegreenbow.com