



THEGREENBOW



# TheGreenBow VPN

## 客户端软件与

## Hillstone SA 系列

## 防火墙

## — 配置手册

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

Contact: [support@thegreenbow.com](mailto:support@thegreenbow.com)

## 目录

1	介绍	3
1.1	手册用途	3
1.2	VPN 网络	3
1.3	Hillstone 防火墙	3
1.4	Hillstone 防火墙 产品信息	3
2	Hillstone 防火墙 VPN 配置	4
3	VPN 客户端设置	7
3.1	VPN 客户端第一阶段 ( IKE 阶段 ) 设置	7
3.2	VPN 客户端第二阶段 ( IPSec 阶段 ) 设置	9
3.3	启用 IPSec VPN 隧道	10
4	故障排除工具	11
4.1	一个好的网络分析工具 : Wireshark	11
5	IPSec VPN 问题分析	12
5.1	« 畸形载荷 » 错误 ( 阶段 1 建立错误 )	12
5.2	« 无效 COOKIE » 错误	12
5.3	« no keystate » 错误	12
5.4	« 接收到的远程 ID 与所期不符 » 错误	12
5.5	« no proposal chosen » 错误	13
5.6	« 无效的 ID 信息 » 错误	13
5.7	“ 我点击 ‘ 打开隧道 ’ , 但是什么都没出现 ”	13
5.8	“ VPN 隧道被激活了 , 但是我 Ping 不通 ”	13
6	联系我们	15

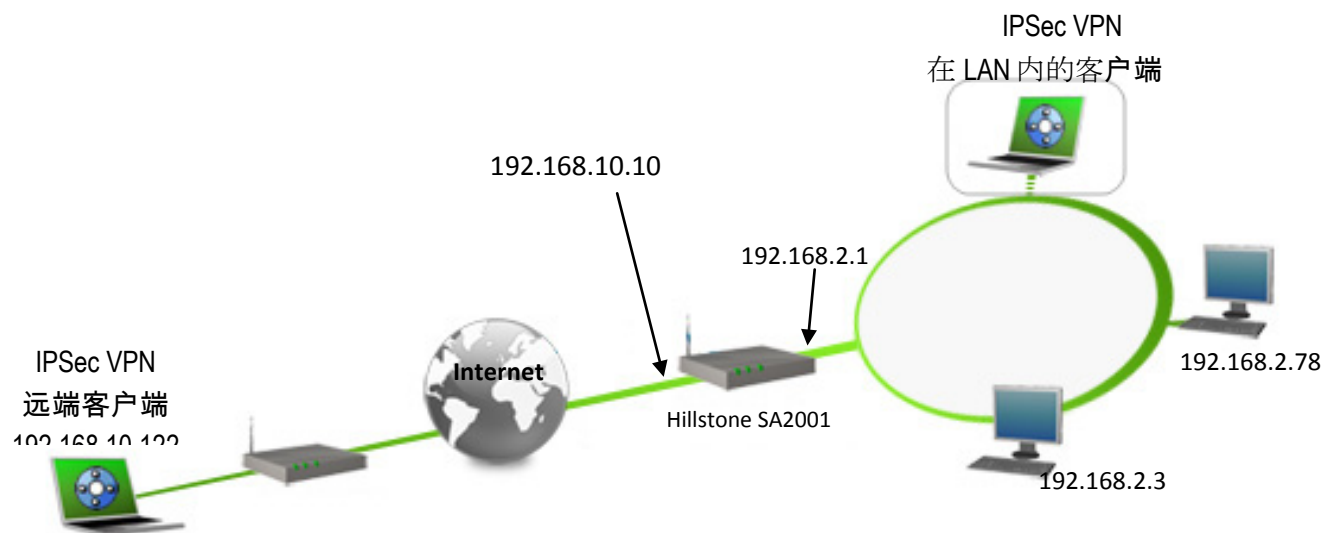
## 1 介绍

### 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 Hillstone SA 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 Hillstone SA 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 Hillstone 防火墙

示例中 Hillstone SA 系列防火墙软件版本为 4.0 R3p4 版。

### 1.4 Hillstone 防火墙 产品信息

用户需要找到 Hillstone SA 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 Hillstone 防火墙的信息可在该网站找到

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

## 2 Hillstone 防火墙VPN配置

本章介绍 Hillstone SA 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“VPN（IPSec VPN）”界面，点击“新建”按钮进行设置。

新建“对端”：

步骤 1：对端

*对端名称	to-greenbow	(1~31字符)
*接口	ethernet0/1	
*模式	<input checked="" type="radio"/> 主模式 <input type="radio"/> 野蛮模式	
*类型	<input checked="" type="radio"/> 静态IP <input type="radio"/> 动态IP <input type="radio"/> 用户组	
*对端IP地址	192.168.10.122	
本地ID	<input checked="" type="radio"/> 无 <input type="radio"/> FQDN <input type="radio"/> U-FQDN <input type="radio"/> ASN1-DN	
对端ID	<input checked="" type="radio"/> 无 <input type="radio"/> FQDN <input type="radio"/> U-FQDN <input type="radio"/> ASN1-DN	
*提议 1	psk-sha-3des-g2	
*预共享密钥	.....	(6~32)

[高级](#)

高级选项：

[高级](#)

连接类型	<input checked="" type="radio"/> 双向 <input type="radio"/> 发起者 <input type="radio"/> 响应者
NAT穿越	<input checked="" type="checkbox"/> 启用
产生路由	<input type="checkbox"/> 启用
对端存活检测(DPD)	<input checked="" type="checkbox"/> 启用
DPD间隔	10 (1~10秒)
DPD重试	3 (1~10)
描述	

点击“隧道”：

**步骤 1：对端**

**步骤 2：隧道**

\*名称 to-greenbow (1~31字符)

\*模式  tunnel  transport

\*提议名称 esp-sha-3des-g2

\*代理ID  自动  手工

[高级](#)

---

DNS 1

WINS 1

启用空闲时间  启用

DF位  Copy  Clear  Set

防重放  关闭  32  64  128  256  512

响应者设置Commit位  启用

自动连接  启用

隧道路由  [多个...](#)

描述  (1~255字符)

添加地址簿：

地址簿列表					总数: 10 每页: 50
名称	描述	关联安全域	成员	关联项	操作
192.168.10.122		所有安全域	192.168.10.122/32		
Any			0.0.0.0/0		-
ipv4.ethernet0/0			192.168.2.1/32		-
ipv4.ethernet0/0_subnet			192.168.2.1/24		-
ipv4.ethernet0/1			192.168.10.10/32		-
ipv4.ethernet0/1_subnet			192.168.10.10/24		-
ipv4.tunnel1			0.0.0.0/32		-
ipv4.tunnel1_subnet			0.0.0.0/0		-
local_net			192.168.2.0/24		

添加 VPN 策略：

Policy from trust to untrust：

**策略高级配置(id=4)**

\*源安全域 trust

\*源地址 local\_net 多个...

---

\*目的安全域 untrust

\*目的地址 192.168.10.122 多个...

---

\*服务簿 Any 多个...

时间表 ----- 多个...

---

角色/用户/用户组 多个...

---

\*行为  允许  拒绝  Web认证  隧道  来自隧道

\*隧道 to-greenbow

---

描述  (1~255)字符

QoS标记  (1~1024)

Profile组

日志  策略拒绝  会话开始  会话结束

Policy from untrust to trust：

**策略高级配置(id=5)**

\*源安全域 untrust

\*源地址 192.168.10.122 多个...

---

\*目的安全域 trust

\*目的地址 local\_net 多个...

---

\*服务簿 Any 多个...

时间表 ----- 多个...

---

角色/用户/用户组 多个...

---

\*行为  允许  拒绝  Web认证  隧道  来自隧道

\*隧道 to-greenbow

---

描述  (1~255)字符

QoS标记  (1~1024)

Profile组

日志  策略拒绝  会话开始  会话结束

### 3 VPN客户端设置

本章介绍如何配置 VPN 客户端和 Hillstone SA 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](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  
  
 挑战模式

冗余网关   
  
 NAT 穿越

---

**扩展认证**

扩展认证弹窗  
  
 Hybrid Mode

登录名   
  
 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 Hillstone 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

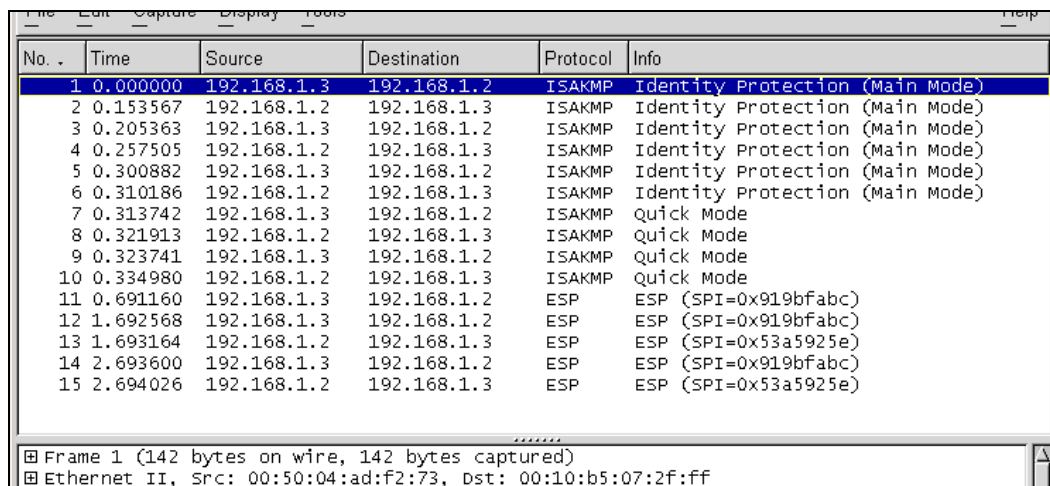
配置一条 IPsec VPN 隧道可能是一项很难的工作。一个疏忽的参数设置就能阻碍 VPN 建立。

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。

- ◆ 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。

<b>THEGREENBOW</b>	Doc.Ref	tgbvpn_cg- Hillstone SA 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](mailto:support@thegreenbow.com)

联系我们的业务部门：[sales@thegreenbow.com](mailto:sales@thegreenbow.com)