TheGreenBow VPN
客户端软件

Juniper SRX 系列
防火墙

— 配置手册

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

目 录

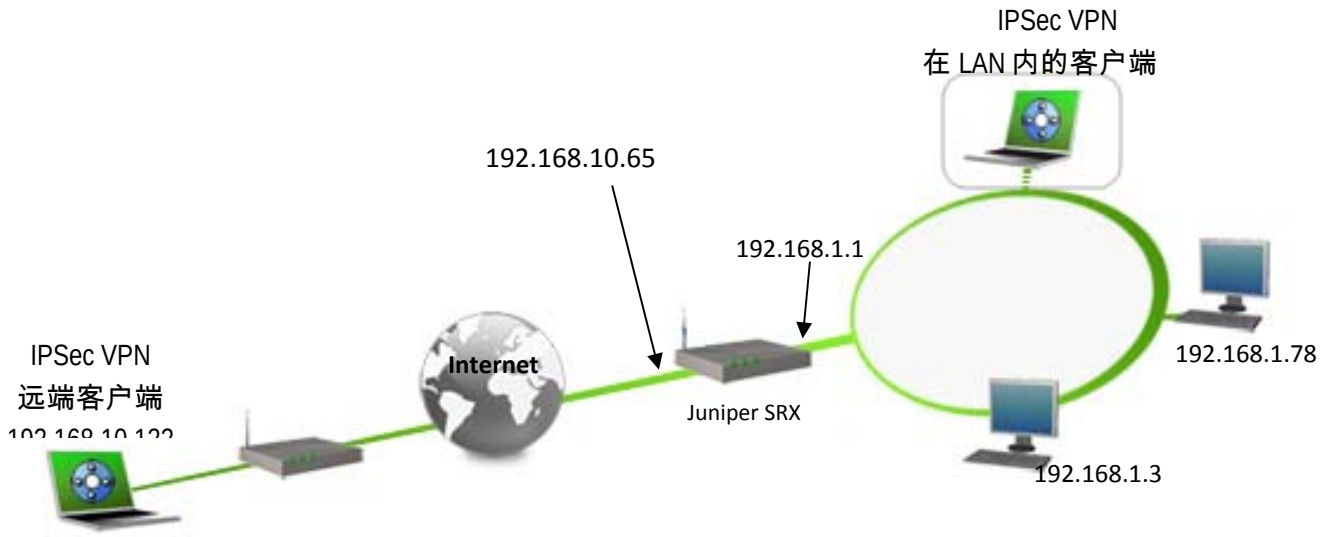
1 介绍

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 Juniper SRX 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 Juniper SRX 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 Juniper SRX系列防火墙

示例中 Juniper SRX 系列防火墙软件版本为 9.6R1.13 版。

1.4 Juniper SRX系列防火墙产品信息

用户需要找到 Juniper SRX 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Juniper SRX系列防火墙的信息可在该网站找到：
http://www.juniper.net/us/en/products-services/security/srx-series/

2 Juniper SRX防火墙VPN配置

这章介绍 Juniper SRX 系列防火墙如何建立 VPN 连接。

通过 console 线以 CLI 方式连接到 SRX100 :

添加第一阶段:

```
root@SRX100# set security ike proposal p1 authentication-method pre-shared-keys
root@SRX100# set security ike proposal p1 dh-group group2
root@SRX100# set security ike proposal p1 authentication-algorithm sha1
root@SRX100# set security ike proposal p1 encryption-algorithm 3des-cbc
root@SRX100# set security ike policy ike-policy-1 mode main
root@SRX100# set security ike policy ike-policy-1 proposals p1
root@SRX100# set security ike policy ike-policy-1 pre-shared-key ascii-text 123456
root@SRX100# set security ike gateway gw1 address 192.168.10.122
root@SRX100# set security ike gateway gw1 external-interface fe-0/0/3.0
root@SRX100# set security ike gateway gw1 ike-policy ike-policy-1
```

添加第二阶段 :

```
root@SRX100# set security ipsec proposal p2 protocol esp
root@SRX100# set security ipsec proposal p2 authentication-algorithm hmac-sha1-96
root@SRX100# set security ipsec proposal p2 encryption-algorithm 3des-cbc
root@SRX100# set security ipsec policy vpn-policy1 proposals p2
root@SRX100# set security ipsec vpn ike-vpn ike gateway gw1
root@SRX100# set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group2
root@SRX100# set security ipsec vpn ike-vpn ike ipsec-policy vpn-policy1
```

添加地址簿：

```
root@SRX100# set security zones security-zone trust address-book
address local_net 192.168.1.0/24
root@SRX100# set security zones security-zone untrust address-book
address remote_net 192.168.10.122/32
```

添加 VPN 策略：

```
root@SRX100# set security policies from-zone trust to-zone untrust
policy vpn1 match source-address local_net destination-address
remote_net application any
root@SRX100# set security policies from-zone trust to-zone untrust
policy vpn1 then permit tunnel ipsec-vpn ike-vpn
root@SRX100# set security policies from-zone untrust to-zone trust
policy vpn2 match source-address remote_net destination-address
local_net application any
root@SRX100# set security policies from-zone untrust to-zone trust
policy vpn2 then permit tunnel ipsec-vpn ike-vpn
```

开启外网口 IKE 服务：

```
root@SRX100# set security zones security-zone untrust interfaces fe-
0/0/3 host-inbound-traffic system-services ike
```

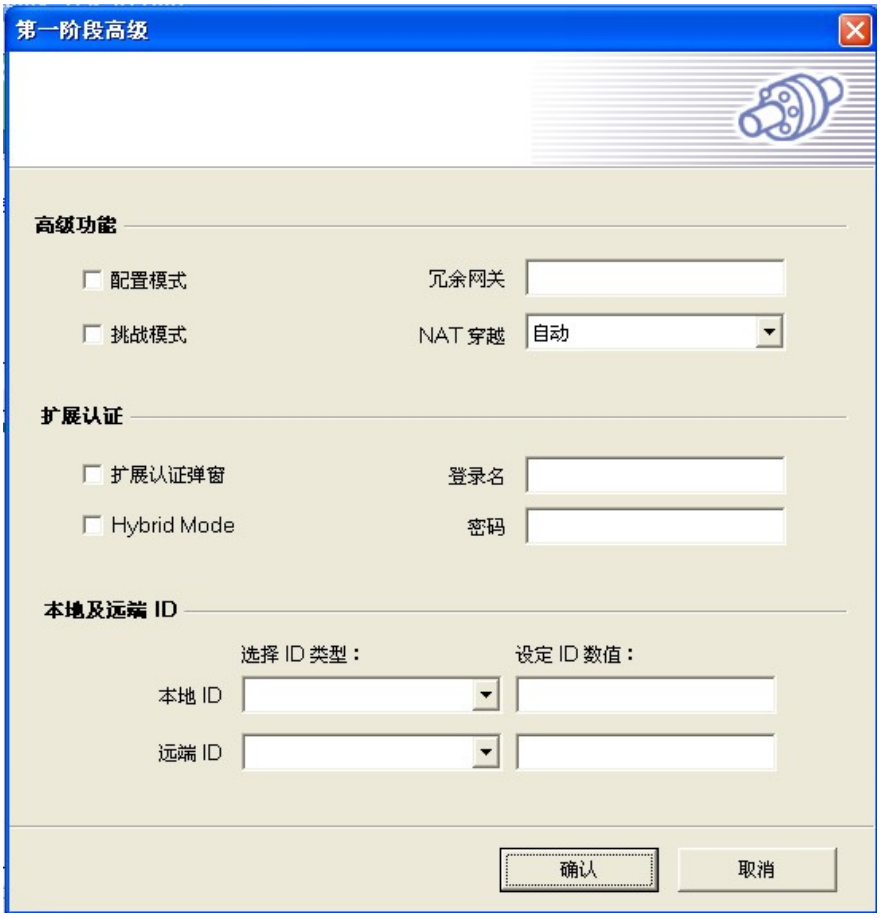
3 VPN客户端设置

这章介绍如何配置 VPN 客户端和 Juniper SRX 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/vpn_down.html

3.1 VPN客户端第一阶段（IKE阶段）设置

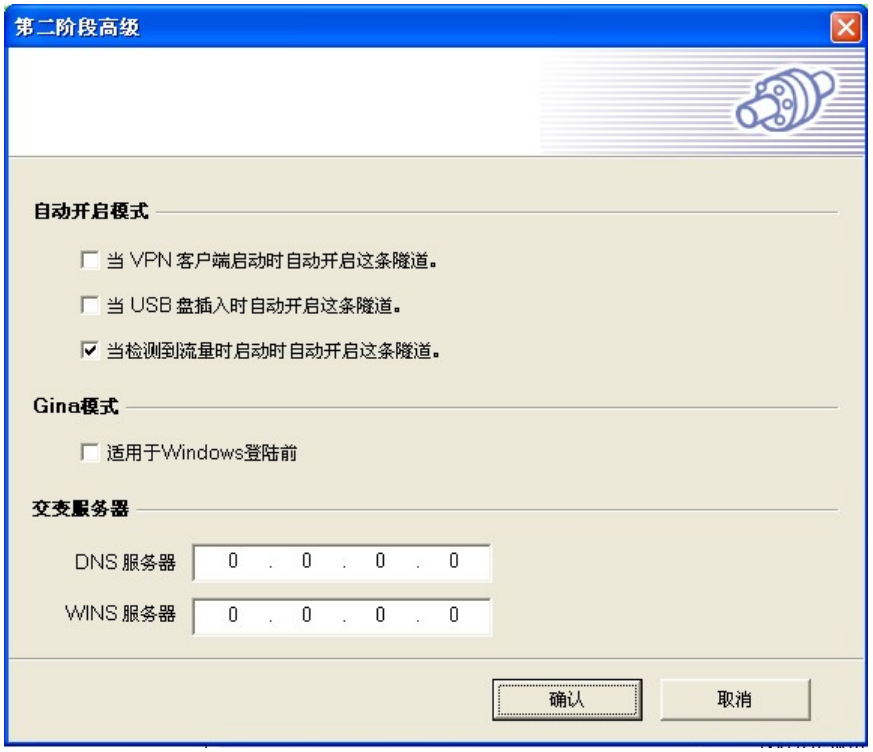
阶段 1 设置


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
自动
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
确认
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



阶段 2（高级设置）

3.3 启用IPSec VPN隧道

当 Juniper SRX 系列防火墙和 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

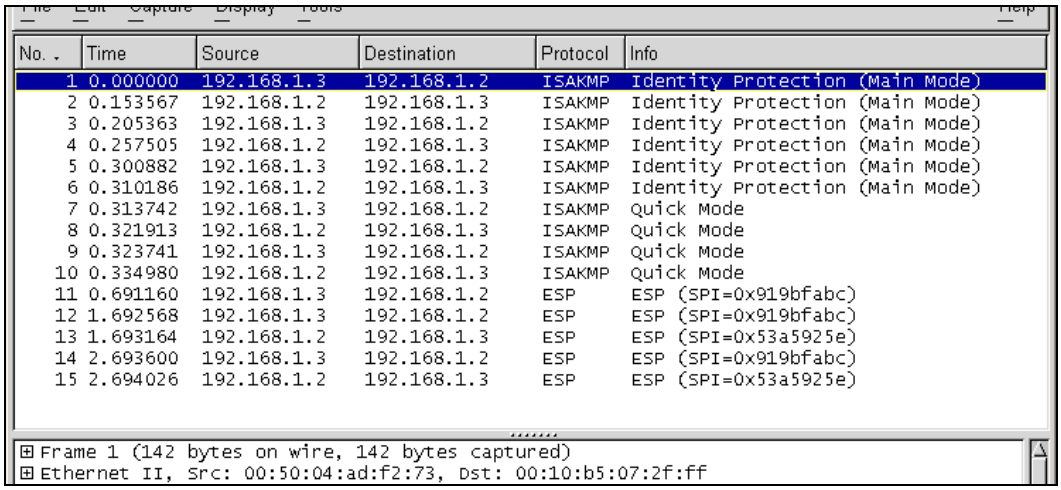
配置一条 IPSec VPN 隧道可能是一项很难的工作。一个疏忽的参数设置就能阻碍 VPN 建立。

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/)。



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。

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