Hillstone Networks

StoneOS 命令行用户手册

VPN 分册

Version 5.5R7

TechDocs | docs.hillstonenet.com

Hillstone Networks

联系信息

公司总部（北京总部）：

地址：北京市海淀区宝盛南路1号院20号楼5层

邮编： 100192

联系我们：http://www.hillstonenet.com.cn/about/contact_Hillstone.html

关于本手册

本手册介绍Hillstone Networks 公司的产品系统的使用方法。

获得更多的文档资料，请访问：https://docs.hillstonenet.com.cn

针对本文档的反馈，请发送邮件到：hs-doc@hillstonenet.com

Hillstone Networks

https://www.hillstonenet.com.cn

TWNO: TW-CUG-UNI-VPN-5.5R7-CN-V1.0-11/12/2020

目 录

关于本手册

手册约定

为方便用户阅读与理解，本手册遵循以下约定：

内容约定

本手册内容约定如下：

- 提示：为用户提供相关参考信息。
- 说明：为用户提供有助于理解内容的说明信息。
- 注意：如果该操作不正确，会导致系统出错。
- 『 』：用该方式表示Hillstone设备WebUI界面上的链接、标签或者按钮。例如，“点击『登录』按钮进入Hillstone设备的主页”。
- < >：用该方式表示WebUI界面上提供的文本信息，包括单选按钮名称、复选框名称、文本框名称、选项名称以及文字描述。例如，“改变MTU值，选中<手动>单选按钮，然后在文本框中输入合适的值”。

CLI约定

本手册在描述CLI时，遵循以下约定：

- 大括弧（{ }）：指明该内容为必要元素。
- 方括弧（[ ]）：指明该内容为可选元素。
- 竖线（|）：分隔可选择的互相排斥的选项。
- 粗体：粗体部分为命令的关键字，是命令行中不可变部分，用户必须逐字输入。
- 斜体：斜体部分为需要用户提供值的参数。
- 命令实例中，需要用户输入部分用粗体标出；需要用户提供值的变量用斜体标出；命令实

例包括不同平台的输出，可能会有些许差别。

- 命令实例中，命令提示符中的主机名称均使用“hostname”。

命令行接口（CLI）

CLI介绍

Hillstone山石网科多核安全网关操作系统StoneOS提供一系列命令以及命令行接口（Command Line Interface），使用户能够对安全网关进行配置和管理。以下各节将介绍StoneOS命令行接口的使用方法及特点。

注意: 使用CLI配置安全网关时，命令本身的关键字不区分大小写，但是，用户输入的内容区分大小写。

命令模式和提示符

StoneOS CLI有不同级别的命令模式，一些命令只有在特定的命令模式下才可使用。例如，只有在相应的配置模式下，才可以输入并执行配置命令，这样也可以防止意外破坏已有的配置。不同的命令模式都有其相应的CLI提示符。

执行模式

用户进入到CLI时的模式是执行模式。执行模式允许用户使用其权限级别允许的所有的设置选项。该模式的提示符如下所示，包含了一个井号（#）：

```
hostname#
```

全局配置模式

全局配置模式允许用户修改安全网关的配置参数。用户在执行模式下，输入`configure`命令，可进入全局配置模式。该模式的提示符如下所示：

```
hostname(config)#
```

子模块配置模式

安全网关的不同模块功能需要在其对应的命令行子模块模式下进行配置。用户在全局配置模式输入特定的命令可以进入相应的子模块配置模式。例如，运行`interface ethernet0/0`命令进入ethernet0/0接口配置模式，此时的提示符变更为：

```
hostname(config-if-eth0/0)#
```

CLI命令模式切换

用户登录到安全网关CLI就进入到CLI的执行模式。用户可以通过不同的命令在各种命令模式之间进行切换。下表列出CLI的模式切换命令：

模式	命令
执行模式到全局配置模式	configure
全局配置模式到子模块配置模式	不同功能使用不同的命令进入各自的命令配置模式。
退回到上一级命令模式	exit
从任何模式退回到执行模式	end

命令行错误信息提示

StoneOS CLI具有命令语法检查功能，只有通过了CLI语法检查的命令能够正确执行。对于不能通过CLI语法检查的命令，StoneOS会输出错误信息提示。常见的错误信息如下表所示：

提示信息	描述
Unrecognized command	StoneOS找不到输入的命令或者关键字。
	输入的参数类型错误。
	输入的参数值越界。
Incomplete command	输入的命令不完整。
Ambiguous command	输入的参数不明确。

命令行的输入

为简化用户的输入操作，用户可以使用命令的缩写形式进行配置，除此之外，StoneOS CLI还提供自动列出命令关键字和自动补齐命令功能。

命令行的缩写形式

命令的缩写形式一般是由命令中的几个独特字符组成。大部分StoneOS命令都有缩写形式。例如，用户可以仅输入`sho int`来查看设备的接口配置信息，而不用输入`show interface`；仅输入`conf`就可进入全局配置模式。

自动列出命令关键字

StoneOS CLI具有输入问号（？）列出命令关键字的功能。具体包括以下两种情况：

- 在一个或一组有效字符后输入问号，CLI将自动列出以这个或该组字母开头的可用命令（包括命令功能的简短介绍）或者该有效字符后可以输入参数值。
- 如果直接输入问号，CLI将列出所在模式下所有的可用命令和命令的简短介绍。

自动补齐命令关键字

StoneOS CLI支持TAB键补齐命令关键字的功能。在部分字符后按TAB键，以该字符开头的命令会被自动补齐。但是，该自动补齐功能仅在只有唯一命令匹配时有效。例如，在执行模式下输入“`conf`”后敲TAB键，系统会自动将命令补齐为“`configure`”。

命令行的编辑

StoneOS命令行的编辑操作简单，主要包括以下几方面：

查看历史命令

StoneOS CLI可记录最近输入的64条命令，用户可以通过上、下键或快捷键Ctrl+P、Ctrl+N来查看上一条或者下一条历史命令。用户可以编辑或是使用任何一条找到的历史命令。

快捷键

StoneOS CLI支持快捷键的使用。下表列出StoneOS支持的快捷键及其功能：

快捷键	功能
Ctrl-A	将光标移至所在行的行首。
Ctrl-B	将光标向回移动一个字符。
Ctrl-D	删除光标所在的字符。
Ctrl-E	将光标移至所在行的行尾。
Ctrl-F	将光标向前移动一个字符。
Ctrl-H	删除光标前一个字符。
Ctrl-K	删除光标后所有字符。
Ctrl-N	显示下一条历史命令。
Ctrl-P	显示上一条历史命令。
Ctrl-T	调换光标所在字母及其前一字母的顺序。
Ctrl-U	删除光标所在行。
Ctrl-W	删除光标前的词。
META-B	将光标移至所在词的词首。
META-D	删除光标后的词。
META-F	将光标移至所在词的词尾。
META-Backspace	删除光标前的词。
META-Ctrl-H	删除光标前的词。

提示: 在没有META键的电脑上，请先按ESC键，再按字母键。例如，META-B的操作过程为先按一下ESC键，然后再按字母B。

过滤CLI输出信息

StoneOS CLI用show命令显示设备的配置信息。用户可以根据需要对show命令的输出信息进行过滤。过滤方法为在show命令后添加一个过滤条件并用竖线（|）把命令和过滤条件隔开。过滤条件有

三种：

- include <过滤条件>：输出符合过滤条件的信息。<过滤条件>中的字母区分字母大小写。
- exclude <过滤条件>：输出过滤条件以外的信息。<过滤条件>中的字母区分大小写。
- begin <过滤条件>：从第一条符合过滤条件的信息开始输出。<过滤条件>中的字母区分大小写。

CLI输出信息过滤的语法格式为：

`hostname#` **`show command`** | {**`include`** | **`exclude`** | **`begin`**} {*`filter-condition`*}

在以上命令行中，第一个竖线（|）是命令的一部分，指明输出信息要按照过滤条件进行过滤。以后的竖线用来分隔命令的不同参数，并不是命令包含的部分。

过滤条件符合正则表达式规范。下表列出正则表达式中常用的字符及其表示的含义：

字符	含义
句点（.）	匹配任意单字符。
星号（*）	一个单字符后紧跟*，匹配0个或多个此单字符。
加号（+）	一个单字符后紧跟+，匹配1个或多个此单字符。
脱字符号（^）	只匹配行首。
美元符号（$）	只匹配行尾。
下划线（_）	匹配逗号（，）、左大括号（{）、右大括号（}）、左圆括号（（）、右圆括号（））、行首、行尾或者空格。
方括号（[]）	指定单个字符的范围。
连字符（-）	分隔范围的终点。

分页显示CLI输出信息

一些命令回显输出信息比较长，可能需要许多页显示，CLI会用提示符“--More--”表示一页的结束。用户可以通过不同的操作指定继续显示信息或者终止显示信息。用户可执行的操作有：

- 显示下一行信息：按回车键。
- 返回到命令行：按“Q”键或者“q”键。
- 继续显示下一页信息：按除回车、“Q”和“q”以外的任意键。

设置终端属性

用户可以通过命令设置所使用终端的宽度和长度。默认情况下，终端宽为80个字符，长为25行。请使用以下命令设置终端的宽度和长度：

- 宽度：**terminal width** *character-number*

  character-number – 指定字符数。范围是64到512个字符。

- 长度：**terminal length** *line-number*

  line-number – 指定行数，终端显示的行数为指定行数减1（但是如果配置行数为1，则显示1行）。范围是0到256行，0的含义为不分屏显示。

终端的设置只对当前连接有效，不会被记录到配置文件。终端断开连接后再次登录时，终端的宽度和长度又会恢复到默认值。

设置连接超时时间

StoneOS CLI可以设置Console、SSH或Telnet连接的超时时间。在全局配置模式下，输入以下命令设置超时时间：

- **console timeout** *timeout-value*

  timeout-value – 指定Console超时时间。范围是0到60分钟，0表示永不超时。默认值为10分钟。

  在全局配置模式使用**no console timeout**命令恢复Console超时时间的默认值。

- **ssh timeout** *timeout-value*

  timeout-value - 指定SSH超时时间。范围是1到60分钟。默认值是10分钟。

  在全局配置模式使用**no ssh timeout**命令恢复SSH超时时间的默认值。

- **telnet timeout** *timeout-value*

  timeout-value - 指定Telnet超时时间。范围是1到60分钟，默认是10分钟。

  在全局配置模式使用**no telnet timeout**命令恢复Telnet超时时间的默认值。

重定向输出

StoneOS允许用户将show命令的输出信息重定向输出到其它的目的地址，包括安全设备的FTP Server和TFTP Server。重定向输出命令的格式为：

show command | redirect *dst-address*

目的地址（*dst-address*）的格式为：

- FTP – `ftp://[username:password@]x.x.x.x[:port]/filename`
- TFTP – `tftp://x.x.x.x/filename`

诊断命令

StoneOS CLI支持`ping`和`traceroute`两个诊断命令。用户可以通过这两个命令查看网络和路由是否连通。

VPN

本章节包含以下内容：

IPSec协议：主要介绍IPSec协议、IPSec VPN的应用、配置IPSecVPN以及相关的配置举例。

SSL VPN：主要介绍了SSL VPN的概念、设备端的配置以及各种客户端的配置和配置举例。

拨号VPN：主要介绍了拨号VPN的概念、应用、配置方法及相关的配置举例。

PnPVPN：主要介绍了PnPVPN的概念、链路冗余的相关内容及PnPVPN服务器端的配置，同时还介绍了相关的配置举例。

GRE协议：主要介绍了GRE相关的概念、配置方法以及相关的配置举例。

L2TP协议：主要介绍了L2TP的相关概念、典型组网、服务器及客户端的配置以及相关的配置举例。

IPSec协议

IPSec协议介绍

IPSec是为实现VPN功能而最普遍使用的协议。IPSec不是一个单独的协议，它给出了应用于IP层上网络数据安全的一整套体系结构。该体系结构包括认证头协议（Authentication Header，简称为AH）、封装安全负载协议（Encapsulating Security Payload，简称为ESP）、密钥管理协议（Internet Key Exchange，简称为IKE）和用于网络认证及加密的一些算法等。IPSec规定了如何在对等体之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

- 认证头协议（AH）：IPsec体系结构中的一种主要协议，它为IP数据包提供无连接完整性的保护与数据源认证，并提供保护以避免重播情况。AH尽可能为IP头和上层协议数据提供足够多的认证。
- IPsec封装安全负载（ESP）：IPsec 体系结构中的一种主要协议。ESP加密需要保护的数据并且在IPsec ESP的数据部分进行数据的完整性校验，以此来保证机密性和完整性。ESP 提供了与AH相同的安全服务并提供了一种保密性（加密）服务，ESP与AH各自提供的认证根本区别在于它们的覆盖范围。
- 密钥管理协议（IKE）：用于协商AH和ESP所使用的密码算法，并将算法所需的必备密钥放到恰当位置。

注意: IPSec VPN支持使用国家商用密码算法配置。详细的国密算法标准，请参阅国家密码管理局颁发的《IPSec VPN技术规范》。

安全联盟（Security Association）

IPSec在两个端点之间提供安全通信，两个端点被称为IPSec ISAKMP网关。安全联盟（简称为SA）是IPSec的基础，也是IPSec的本质。SA是通信对等体间对某些要素的约定，例如使用哪种协议、协议的操作模式、加密算法（DES、3DES、AES-128、AES-192和AES-256）、特定流中保护数据的共享密钥以及SA的生存周期等。

安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。

SA建立方式

建立安全联盟的方式有两种，一种是手工方式（Manual），一种是IKE自动协商（ISAKMP）方式。

手工方式配置比较复杂，创建安全联盟所需的全部信息都必须手工配置，而且IPSec的一些高级特性（例如定时更新密钥）不能被支持，但优点是可以不依赖IKE而单独实现IPSec功能。该方式适用于当与之进行通信的对等体设备数量较少的情况，或是IP地址相对固定的环境中。

IKE自动协商方式相对比较简单，只需要配置好IKE协商安全策略的信息，由IKE自动协商来创建和维护安全联盟。该方式适用于中、大型的动态网络环境中。该方式建立SA的过程分两个阶段。第一阶段，协商创建一个通信信道（ISAKMP SA），并对该信道进行认证，为双方进一步的IKE通信提供机密性、数据完整性以及数据源认证服务；第二阶段，使用已建立的ISAKMP SA建立IPsec SA。分两个阶段来完成这些服务有助于提高密钥交换的速度。

第一阶段SA

第一阶段SA为建立信道而进行的安全联盟。第一阶段协商的步骤是：

1. 参数配置。包括：
    - 认证方法：选择预共享密钥或数字证书认证
    - Diffie-Hellman组的选择
2. 策略协商。包括：
    - 加密算法：选择DES、3DES、AES-128、AES-192或AES-256
    - hash算法：选择MD5、SHA-1或SHA-2
3. DH交换。虽然名为“密钥交换”，但事实上在任何时候，两台通信主机之间都不会交换真正的密钥，它们之间交换的只是一些DH算法生成共享密钥所需要的基本材料信息。DH交换，可以是公开的，也可以受保护。在彼此交换过密钥生成“材料”后，两端主机可以各自生成出完全一样的共享“主密钥”，保护紧接其后的认证过程。
4. 认证 。DH交换需要得到进一步认证，如果认证不成功，通信将无法继续下去。“主密钥”结合在第一步中确定的协商算法，对通信实体和通信信道进行认证。在这一步中，整个待认证的实体载荷，包括实体类型、端口号和协议，均由前一步生成的“主密钥”提供机密性和完整性保证。

第二阶段SA

第二阶段SA为快速SA，为数据传输而建立的安全联盟。这一阶段协商建立IPsec SA，为数据交换提供IPSec服务。第二阶段协商消息受第一阶段SA保护，任何没有第一阶段SA保护的消息将被拒收。
第二阶段协商（快速模式协商）步骤是：

1．策略协商，双方交换保护需求：

- 使用哪种IPSec协议：AH或ESP
- 是否使用hash算法：MD5、SHA-1、SHA-2或NULL
- 是否要求加密，若是，选择加密算法：DES或3DES、AES-128、NULL、AES-192或AES-256
- 是否使用压缩算法：DEFLATE
- 在上述四方面达成一致后，将建立起两个SA，分别用于入站和出站通信。

2．会话密钥“材料”刷新或交换。
在这一步中，将通过DH交换生成加密IP数据包的“会话密钥”。

3．将SA递交给IPSec驱动程序。
在第二阶段协商过程中，如果响应超时，则自动尝试重新进行第二阶段SA协商。

验证算法

AH和ESP都能够对IP报文的完整性进行验证，以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过杂凑函数。杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。一般来说IPSec使用下列验证算法：

- MD5：MD5输入任意长度的消息，产生128bit的消息摘要。
- SHA-1：SHA-1输入长度小于2的64次方比特的消息，产生160bit的消息摘要。SHA-1的摘要长于MD5，因而是更安全的。
- SHA-2：SHA-2一般包含SHA-256、SHA-384和SHA-512三种杂凑函数，能将输入消息对应到更长的消息摘要。SHA-256输入长度小于2的64次方比特的消息，产生256bit的消息摘

要；SHA-384输入长度小于2的128次方比特的消息，产生384bit的消息摘要；SHA-512输入长度小于2的128次方比特的消息，产生512bit的消息摘要。

- SM3：SM3输入长度小于2的64次方比特的消息，产生256bit的消息摘要。

加密算法

ESP能够对IP报文内容进行加密保护，防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。StoneOS实现了三种加密算法：

- DES（Data Encryption Standard）：使用56bit的密钥对每个64bit的明文块进行加密。
- 3DES（Triple DES）：使用三个56bit的DES密钥（共168bit密钥）对明文进行加密。
- AES（Advanced Encryption Standard）：StoneOS实现了128bit、192bit和256bit密钥长度的AES算法。
- SM1: 国家密码管理局编制的一种商用密码分组标准对称算法。分组长度和密钥长度都为128bit。仅国密设备支持该算法。
- SM4: 国家密码管理局编制的一种商用密码分组标准对称算法。分组长度和密钥长度都为128bit。

压缩算法

IPComp（IP Payload Compression，IP有效载荷压缩）是一个减少IP数据报长度的协议，该协议通过支持不同的压缩算法对IP数据报的有效负载进行压缩处理，从而实现通信数据在低带宽条件下的高负载传输。

应用IPComp的关键在于通信的两个端点之间必须首先建立一个IPComp关联（IPCA），此关联中包含了IPComp操作要求的所有信息，例如所使用的压缩算法以及所选择的压缩算法要求的参数等。使用IPComp对IPSec处理的网络数据流进行压缩时，用户可以手工配置创建IPCA，也可以通过动态协商创建IPCA。当使用动态协商方式时，ISAKMP网关提供建立IPCA必须的机制。Hillstone设备的IPSec功能提供以下IPComp压缩算法：

- DEFLATE：使用LZ77算法和Huffman译码，是一种可以在IPComp中实现的自由可用的无损耗压缩算法。

相关资料

StoneOS的IPSec功能遵循RFC中IPSec协议的规定。关于IPSec协议的更多详细信息，请参阅以下RFC文档的相关章节：

- Security Architecture for the Internet Protocol: RFC2401/RFC4301
- ESP：RFC2406/RFC4303
- AH：RFC2402/RFC4302
- 加密算法参考：RFC2410（Null Encryption），RFC2405（DES-CBC），RFC2451（3DES-CBC）以及RFC3602（AES-CBC）
- 验证算法参考：：FIPS180-2（SHA），RFC2404（SHA-1），RFC4868（SHA-2）以及RFC2403（MD5）
- 压缩算法参考：RFC2393（IPComp）以及RFC2394（DEFLATE）

IPSec VPN的应用

StoneOS通过“基于策略的VPN”和“基于路由的VPN”两种方式把配置好的VPN隧道应用到Hill-stone设备上，实现流量的加密解密安全传输。

- 基于策略的VPN：将配置成功的VPN隧道名称引用到策略规则中，使符合条件的流量通过指定的VPN隧道进行传输。
- 基于路由的VPN：将配置成功的VPN隧道与隧道接口绑定；配置静态路由时，将隧道接口指定为下一跳路由。

配置IPSec VPN功能

StoneOS支持两种配置IPSec VPN的方法，分别是：

- 手工密钥VPN
- IKE VPN，支持IKEv1和IKEv2两个版本。

提升IPSec VPN解密性能

该功能仅支持虚拟化产品云•界。当云•界使用的CPU数大于2个vCPU以上时，用户可以根据需要开启IPSec VPN解密性能提升功能。开启后，系统将采用多核解密技术对数据包进行解密，IPSec VPN解密性能将提升，同时设备的吞吐量也将增大。开启IPSec VPN解密性能提升功能，在全局配置模式下使用以下命令：

tunnel-core-unbind

在全局配置模式下，使用**no tunnel-core-unbind**恢复默认配置。

手工密钥VPN

手工密钥VPN的配置包括指定IPSec协议的操作模式、安全参数索引、协议类型、加密算法/验证算法和压缩算法等。

创建手工密钥VPN

创建手工密钥VPN，在全局配置模式下，使用以下命令：

tunnel ipsec *name* **manual**

- *name* – 指定所创建的手工密钥VPN隧道的名称。

执行该命令后，CLI进入到手工密钥VPN配置模式。对手工密钥VPN的所有参数配置都需要在该模式下进行。在全局配置模式下使用以下命令删除指定的手工密钥VPN隧道：

no tunnel ipsec *name* **manual**

指定IPSec协议的操作模式

指定IPSec协议的操作模式，可以是隧道模式或者传输模式，在手工密钥VPN配置模式下使用以下命令：

mode {**transport** | **tunnel**}

- **transport** – 指定IPSec协议的操作模式为传输模式。
- **tunnel** – 指定IPSec协议的操作模式为隧道模式。该模式为系统默认模式。

使用**no mode**命令恢复默认模式。

指定安全参数索引

安全参数索引（Security Parameter Index，简称为SPI）是为唯一标识SA而生成的一个32比特的数值，它在AH和ESP头中传输。SPI的作用是查找对应的VPN隧道进行解密。指定手工密钥VPN隧道的SPI，在手工密钥VPN配置模式下使用以下命令：

spi *spi-number out-spi-number*

- *spi-number* – 指定本端的SPI参数。
- *out-spi-number* – 指定对端的SPI参数。

使用**no spi**命令取消对SPI参数的配置。

在为系统配置安全联盟时，必须分别设置进方向（inbound）和出方向（outbound）两个方向的安全联盟的参数。并且在隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的SPI必须和对端的出方向安全联盟的SPI一样；本端的出方向安全联盟的SPI必须和对端的入方向安全联盟的SPI一样。

指定协议类型

IPSec协议的类型为ESP和AH两种。为手工密钥VPN隧道指定协议类型，在手工密钥VPN配置模式下使用以下命令：

protocol {**esp** | **ah**}

- **esp** – 指定使用ESP协议。该协议为系统默认协议。
- **ah** – 指定使用AH协议。

使用**no protocol**恢复默认协议配置。

指定加密算法

为手工密钥VPN隧道指定加密算法，请在手工密钥VPN配置模式下使用以下命令：

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256** | **null**}

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为系统默认方法。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。

- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。
- **null** – 不使用加密功能。

使用**no encryption**命令恢复默认加密算法。

指定验证算法

为手工密钥VPN隧道指定验证算法，请在手工密钥VPN配置模式下使用以下命令：

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **null**}

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为StoneOS的默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** –指定使用SHA-512验证算法。摘要为512比特。
- **null** – 不使用验证功能。

使用**no hash**命令恢复默认验证算法。

指定压缩算法

默认情况下，手工密钥VPN不使用任何压缩算法。为手工密钥VPN隧道指定压缩算法（DEFLATE算法），请在手工密钥VPN配置模式下使用以下命令：

compression deflate

使用**no compression**命令取消对压缩算法的指定。

指定对端IP地址

配置对端的IP地址，请在手工密钥VPN配置模式下使用以下命令：

peer *ip-address*

- *ip-address* – 指定对端的IP地址。

使用**no peer**命令取消对端IP地址的配置。

配置协议的验证密钥

用户需要为安全隧道两端均配置协议的验证密钥，且本端入方向验证密钥必须与对端出方向的验证密钥相同，而本端出方向的验证密钥必须与对端入方向的验证密钥相同。配置协议验证密钥，请在手工密钥VPN配置模式下使用以下命令：

hash-key inbound *hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* – 配置本端进方向的验证密钥。
- **outbound** *hex-number-string* – 配置本端出方向的验证密钥。

使用**no hash-key**命令取消对验证密钥的配置。

配置协议的加密密钥

用户需要为安全隧道两端均配置协议的加密密钥，且本端入方向加密密钥必须与对端出方向的加密密钥相同，而本端出方向的加密密钥必须与对端入方向的加密密钥相同。配置协议加密密钥，请在手工密钥VPN配置模式下使用以下命令：

encryption-key inbound *hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* – 配置本端进方向的加密密钥。
- **outbound** *hex-number-string* – 配置本端出方向的加密密钥。

使用**no encryption-key**命令取消对加密密钥的配置。

指定出接口

为手工密钥VPN隧道指定出接口，请在手工密钥VPN配置模式下使用以下命令：

- **interface** *interface-name*
- **interface-name** – 指定出接口名称。

使用**no interface**命令取消对出接口的指定。

注意: 非根VSYS中的出接口不可以为VSYS共享接口。

IKEv1 VPN

IKEv1 VPN的配置包括：

- 配置P1提议
- 配置ISAKMP网关
- 配置P2提议
- 配置隧道

配置P1提议

P1提议是IKE安全提议，可应用到ISAKMP网关上，在SA第一阶段使用。对IKE安全提议的配置包括指定认证方式、加密算法、验证算法、DH组和安全联盟的生命周期。

创建P1提议

创建一个P1提议，即IKE安全提议，请在全局配置模式下使用以下命令：

isakmp proposal *p1-name*

- *p1-name* – 指定所创建的P1提议的名称。执行该命令后，CLI进入到P1提议配置模式。用户可以在该模式下对P1提议进行参数配置。

使用**no isakmp proposal** *p1-name*命令删除指定的P1提议。

指定认证方式

此处指定的是IKE身份认证的方式。身份认证用来确认通信双方的身份。方式有预共享密钥认证、数字证书认证和国密数据信封认证。对于预共享密钥认证方式，认证字用来作为一个输入产生密钥，认证字不同是不可能在双方产生相同的密钥的。指定IKE安全提议的身份认证方式，在P1提议配置模式下使用以下命令：

authentication {**pre-share** | **rsa-sig** | **dsa-sig** | **gm-de** }

- **pre-share** – 指定使用预共享密钥认证方式。该方式为默认认证方式。
- **rsa-sig** – 指定使用RSA数字证书认证方式。
- **dsa-sig** – 指定使用DSA数字证书认证方式。此方式对应的验证算法只能为SHA-1。

- **gm-de** – 指定使用国密数据信封认证方式。当认证方式为此选项时，加密算法仅支持使用SM1和SM4，验证算法仅支持使用SHA或SM3。

使用**no authentication**命令恢复默认认证方式。

指定加密算法

指定IKE安全提议的加密算法，在P1提议配置模式下使用以下命令：

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256** | **sm1** | **sm4**}

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为StoneOS系统默认方法。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。
- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。
- **sm1** – 指定使用国家商用密码SM1分组密码算法。密钥长度为128比特。
- **sm4** – 指定使用国家商用密码SM4分组密码算法。密钥长度为128比特。

使用**no encryption**命令恢复默认加密算法。

指定验证算法

指定IKE安全提议的验证算法，在P1提议模式下使用以下命令：

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3**}

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为StoneOS的默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。

- **sha512** – 指定使用SHA-512验证算法。摘要为512比特。
- **sm3** – 指定使用国密SM3验证算法。摘要为256比特。该算法用于密码应用中的数字签名和验证、消息认证码的生成与验证，可满足多种密码应用的安全需求。

使用**no hash**命令恢复默认认证方式。

选择DH组

Diffie-Hellman（DH）是一种建立密钥的方法。DH组决定DH交换中密钥生成“材料”的长度。密钥的牢固性部分决定于DH组的强度。密钥“材料”长度越长，所生成的密钥安全度也就越高，越难被破译。DH组的选择很重要，因为DH组只在第一阶段的SA协商中确定，第二阶段的协商不再重新选择DH组，两个阶段使用的是同一个DH组，因此该DH组的选择将影响所有会话密钥的生成。在协商过程中，两个ISAKMP网关间应选择同一个DH组，即密钥“材料”长度应该相等。若DH组不匹配，将协商失败。

在P1提议选择DH组，在P1提议配置模式下使用以下命令：

group {**1** | **2** | **5** | **14** | **15** |**16**}

- **1** – 选择DH组1。密钥的长度为768比特。
- **2** – 选择DH组2。密钥的长度为1024比特。2为系统默认值。
- **5** – 选择DH组5。密钥的长度为1536比特。
- **14** – 选择DH组14。密钥的长度为2048比特。
- **15** – 选择DH组15。密钥的长度为3072比特。
- **16** – 选择DH组16。密钥的长度为4096比特。

使用**no group**命令恢复默认DH组。

在P2提议中配置PFS时，也可选用如上DH组。

指定安全联盟的生命周期

第一阶段SA有一个默认的生命周期，如果ISAKMP SA生命期时间到，要向对方发送第一阶段SA删除消息，通知对方第一阶段SA已经过期。之后需要重新进行SA协商。指定安全联盟的生命周期，在P1提议配置模式下使用以下命令：

lifetime *time-value*

- *time-value* – 指定SA第一阶段的生命周期长度，单位为秒。默认86400秒。范围是300到86400秒。

使用**no lifetime**命令恢复默认生命周期长度。

配置ISAKMP网关

创建一个ISAKMP网关后，用户可以配置ISAKMP网关的IKE协商模式、ISAKMP网关IP地址及类型、IKE安全提议、预共享密钥、PKI信任域、本地ID、ISAKMP网关ID 、ISAKMP网关连接方式以及是否开启ISAKMP网关的NAT穿越功能等。

创建ISAKMP网关

创建ISAKMP网关，在全局配置模式下，使用以下命令:

isakmp peer *peer-name*

- *peer-name* – 指定ISAKMP网关的名称。

执行该命令后，CLI进入到ISAKMP网关配置模式。用户可以在该模式下对ISAKMP网关进行参数配置。

在全局配置模式下使用**no isakmp peer** *peer-name*命令删除指定的ISAKMP网关。

绑定接口到ISAKMP网关

用户可以绑定某个接口到ISAKMP网关。将接口绑定到ISAKMP网关，在ISAKMP网关配置模式下使用以下命令：

interface *interface-name*

- *interface-name* – 指定被绑定接口的名称。

使用**no interface** *interface-name*命令取消接口绑定。

配置IKE协商模式

IKE的协商模式有两种：主模式（main mode）和野蛮模式（aggressive mode）。IKE野蛮模式不提供身份保护，以下情况只能用野蛮模式：中心设备的IP地址为固定分配的地址，而客户端设备的

IP地址为动态获取的地址。配置IKE协商模式，在ISAKMP网关配置模式下使用以下命令：

mode {**main** | **aggressive**}

- **main** – 指定使用主模式，可提供ID保护功能。该模式为系统的默认模式。
- **aggressive** – 指定使用野蛮模式。

使用**no mode**命令恢复默认协商模式。

配置自定义IKE协商端口

用户可以自定义UDP端口进行IKE协商，并且建立IPSec连接。配置自定义IKE协商端口，在ISAKMP网关配置模式下使用以下命令：

ipsec-over-udp port *port-number*

- *port-number* – 指定UDP端口号。取值范围是1到65535。

使用**no ipsec-over-udp**命令取消自定义的UDP端口配置。

指定对端的IP地址及类型

用户可以为所创建的ISAKMP网关指定对端的IP地址和IP地址的类型（静态或者动态）。指定对端的IP地址，请在ISAKMP网关配置模式下使用以下命令：

type {**dynamic** | **static**}

- **dynamic** – 指定对端的IP地址为动态IP地址。
- **static** – 指定对端的IP地址为静态IP地址。该选项为系统的默认选项。

使用**no type**命令恢复对端IP地址的默认类型。

peer *ip-address*

- *ip-address* - 指定对端的IP地址或主机名称。该IP地址只有当对端的IP地址类型是静态的时候才有效。

使用**no peer**命令取消对端IP地址或主机名称的指定。

接受对端ID

使所创建的ISAKMP网关接受任意的对端ID，不对对端进行ID检查，在ISAKMP网关配置模式下使用以下命令：

accept-all-peer-id

使用**no accept-all-peer-id**关闭该功能。

指定P1提议

为ISAKMP网关指定P1提议，在ISAKMP网关配置模式下使用以下命令：

isakmp-proposal p1-proposal1 [p1-proposal2] [p1-proposal3] [p1-proposal4]

- **p1-proposal1** – 指定P1提议的名称。用户最多可以为ISAKMP网关指定4个P1提议供对端选择使用。

使用**no isakmp-proposal**取消对P1提议的指定。

配置预共享密钥

如果使用预共享密钥认证方式，用户就需要指定预共享密钥。为ISAKMP网关指定预共享密钥，在ISAKMP网关配置模式下使用以下命令：

pre-share *string*

- *string* – 指定预共享密钥的内容。

使用**no pre-share**取消对预共享密钥的指定。

配置PKI信任域

如果使用数字证书认证方式，用户就需要指定数字证书的PKI信任域。为ISAKMP网关指定PKI信任域，在ISAKMP网关配置模式下使用以下命令：

trust-domain *string*

- *string* – 指定PKI信任域。

使用**no trust-domain**取消对PKI信任域的指定。

提示: 关于如何配置PKI信任域，请参阅《用户认证》的“PKI配置”部分。

配置对端证书的信任域

对端证书一般用于协商中数据加密以及认证，需由发起VPN连接的一端先导入对端证书。该命令仅适用于国密1.0版本。配置对端证书所在的信任域，请在ISAKMP网关配置模式下使用以下命令：

remote-trust-domain *string*

- *string* – 指定对端证书所在的信任域。

使用**no remote-trust-domain**命令删除对端证书的信任域配置。

配置加密证书的信任域

加密证书一般用于协商中数据加密。该命令仅适用于国密1.1版本，需为系统指定双证书。配置加密证书所在的信任域，请在ISAKMP网关配置模式下使用以下命令：

trust-domain-enc *string*

- string – 指定加密证书所在的信任域。

使用**no trust-domain-enc**命令删除加密证书的信任域配置。

配置协商协议标准

协商协议标准分为国际标准IKEv1和国密标准。默认情况下，系统使用国际标准IKEv1为协商协议标准。指定协商协议的标准，请在ISAKMP网关配置模式下使用以下命令：

protocol-standard {**ikev1** | **guomi**[**v1.0** | **v1.1**]}

- **ikev1** – 指定使用国际标准IKEv1为协商协议标准。
- **guomi**[**v1.0** | **v1.1**] – 指定使用国密标准为协商协议标准。v1.0为国密1.0版本；v1.1为国密1.1版本。如指定版本号v1.0或v1.1，进行协商的两端设备必须是相同的版本号才能协商成功，否则协商失败。如不指定版本号，那么发起端国密协议版本号为国密v1.0或v1.1都可协商。

使用**no protocol-standard**命令取消协商协议标准的配置。

配置本端ID

配置本端的ID，请在ISAKMP网关配置模式下使用以下命令：

local-id {**fqdn** *string* | **asn1dn** [*string*] | **u-fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn** *string* – 指定使用FQDN类型的ID。string为ID的具体内容。
- **asn1dn** [*string*] – 指定使用Asn1dn类型的ID，该类型只可应用于使用证书的情况。string为ID的具体内容。用户可以不指定ID的具体内容，在此种情况下，系统将从证书中获取ID。
- **u-fqdn** *string* – 指定使用U-FQDN类型的ID，即电子邮件地址类型，例如user-1@hillstonenet.com。
- **key-id** *string* - 指定使用Key ID类型的ID。该类型仅应用于XAUTH功能。
- **ip** *ip-address* - 指定使用IP地址类型的ID。ip-address为ID的具体内容。

使用no local-id命令取消对本端ID的配置。

配置对端ID

配置对端的ID，请在ISAKMP网关配置模式下使用以下命令：

peer-id {**fqdn** | **asn1dn** | **u-fqdn** | **key-id** | **ip** } *string*

- **fqdn** – 指定使用FQDN类型的ID。string为ID的具体内容。
- **asn1dn** – 指定使用Asn1dn类型的ID，该类型只可应用于使用证书的情况。string为ID的具体内容。
- **u-fqdn string** – 指定使用U-FQDN类型的ID，即电子邮件地址类型，例如user-1@hillstonenet.com。
- **key-id** - 指定使用Key ID类型的ID。该类型仅应用于XAUTH功能。
- **ip** - 指定使用IP地址类型的ID。

使用**no peer-id**命令取消对对端ID的配置。

指定连接类型

创建的ISAKMP网关可以是发起端、响应端或者既是发起端也是响应端。指定ISAKMP网关的连接类型，在ISAKMP网关配置模式下使用以下命令：

connection-type {**bidirectional** | **initiator-only** | **responder-only**}

- **bidirectional** – 指定该ISAKMP网关既是发起端也是响应端。该选项为系统的默认选项。
- **initiator-only** – 指定该ISAKMP网关仅是发起端。
- **responder-only** – 指定该ISAKMP网关仅是响应端。

使用**no connection-type**命令恢复默认连接方式。

开启NAT穿越功能

在IPSec或者IKE组建的VPN隧道中，若存在NAT网关设备，且NAT网关设备对VPN数据进行了NAT转换，则必须开启IPSec或者IKE的NAT穿越功能。默认情况下，NAT穿越功能是关闭的。开启NAT穿越功能，在ISAKMP网关配置模式下，使用以下命令：

nat-traversal

使用**no nat-traversal**命令关闭NAT穿越功能。

配置DPD功能

DPD（Dead Peer Detection）为安全隧道对端状态探测功能。该功能开启后，如果接收端长时间收不到对端的报文，便触发DPD查询，主动向对端发送请求报文，对ISAKMP网关是否存在进行检测。默认情况下，DPD功能是关闭的。配置DPD功能，在ISAKMP网关配置模式下使用以下命令：

dpd [**interval** *seconds*] [**retry** *times*]

- **interval seconds** – 指定向对端发送查询请求的时间间隔。间隔范围是0到10秒。默认值是0，表示不开启DPD功能。
- **retry times** – 指定向对端发送查询请求的次数。向对端发送查询请求后，如果本端在指定的时间间隔内收不到对端的报文，系统会在再次发送查询请求，如此反复，直到完成该参数指定的次数。在指定次数查询完成后如果仍然收不到对端的报文，则判断对端ISAKMP网关已经死掉。查询请求的次数范围是1到20次，默认是3次。

使用**no dpd**命令恢复默认的DPD配置。

指定描述信息

为所配置的ISAKMP网关指定描述信息，请在ISAKMP网关配置模式下使用以下命令：

description *string*

- *string* – ISAKMP网关的描述信息。

使用**no description**命令删除ISAKMP网关的描述信息。

配置P2提议

P2提议使用在SA第二阶段。对P2提议的配置包括指定协议类型、加密算法、验证算法、压缩算法和生命周期。

创建P2提议

创建P2提议，即IPSec安全提议，请在全局配置模式下使用以下命令：

ipsec proposal *p2-name*

- *p2-name* – 指定所创建的P2提议的名称。执行该命令后，CLI进入到P2提议配置模式。对P2提议各项参数的配置都要在该模式下进行。

使用**no ipsec proposal** *p2-name*命令删除指定的IPSec proposal。

指定协议类型

P2提议可使用的协议类型有AH以及ESP。为P2提议指定协议类型，在P2提议配置模式下使用以下命令：

protocol {**esp** | **ah**}

- **esp** – 指定使用ESP协议。该协议为系统默认协议。
- **ah** – 指定使用AH协议。

使用**no protocol**命令恢复默认协议配置。

指定加密算法

用户可以为P2提议指定至少一种最多四种加密算法。为P2提议指定加密算法，在P2提议配置模式下使用以下命令：

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256** | **sm1** | **sm4** | **null**} [**3des** | **des** | **aes** | **aes-192** | **aes-256** | **sm1** | **sm4** | **null**] [**3des** | **des** | **aes** | **aes-192** | **aes-256** | **sm1** | **sm4** | **null**]……

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为StoneOS系统默认方法。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。
- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。
- **sm1** – 指定使用国家商用密码SM1分组密码算法。密钥长度为128比特。
- **sm4** – 指定使用国家商用密码SM4分组密码算法。密钥长度为128比特。
- **null** – 不使用加密功能。

使用**no encryption**命令恢复默认加密算法。

指定验证算法

用户可以为P2提议指定至少一种最多三种验证算法。为P2提议指定验证算法，在P2提议配置模式下使用以下命令：

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**} [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**] [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**]

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为StoneOS的默认算法。

- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** –指定使用SHA-512验证算法。摘要为512比特。
- **sm3** – 指定使用国密SM3验证算法。摘要为256比特。
- **null** – 不使用验证功能。

使用**no hash**命令恢复默认验证算法。

指定压缩算法

默认情况下，P2提议不使用任何压缩算法。为P2提议指定压缩算法（DEFLATE算法），请在P2提议配置模式下使用以下命令：

compression deflate

使用**no compression**命令取消对压缩算法的指定。

配置PFS功能

PFS（Perfect Forward Security）功能决定新密钥的生成方式，而不是新密钥的生成时间。PFS保证无论在哪一阶段，一个密钥只能使用一次，而且，生成密钥的“材料”也只能使用一次。某个“材料”在生成了一个密钥后就被弃，绝不用来再生成任何其它密钥。这样可以确保一旦单个密钥泄密，最多只可能影响用该密钥加密的数据，而不会危及整个通信。PFS功能是由DH算法做保障的。配置P2提议的PFS功能，在P2提议配置模式下使用以下命令：

group {**nopfs** | **1** | **2** | **5** | **14** | **15** |**16**}

- **nopfs** – 不使用PFS功能。该选项为系统的默认选项。
- **1** – 选择DH组1。密钥的长度为768比特。
- **2** – 选择DH组2。密钥的长度为1024比特。
- **5** – 选择DH组5。密钥的长度为1536比特。
- **14** – 选择DH组14。密钥的长度为2048比特。

- **15** – 选择DH组15。密钥的长度为3072比特。
- **16** – 选择DH组16。密钥的长度为4096比特。

使用**no group**命令恢复默配置。

指定生命周期

Hillstone设备有两种衡量生命周期的方法，分别是按时间和按流量。当SA的流量或者时间达到特定值时，SA就会过期，需要重新进行协商。指定P2提议的生命周期，在P2提议配置模式，使用以下命令：

lifetime *seconds*

- *seconds* – 指定时间类型生命周期的时间长度，单位为秒。默认值是28800秒。

lifesize *kilobytes*

- *kilobytes* – 指定流量类型周期的流量值，单位为字节。默认值是0，意义为没有周期流量限制。

使用以上两个命令no的形式恢复默认配置。即

no lifetime

no lifesize

配置隧道

通过IKE配置IPSec隧道，用户需要配置的选项有指定协议类型、ISAKMP网关、IKE安全提议、ID号、是否分片以及防重放等。

创建IKE隧道

创建IKE隧道，在全局配置模式下，使用以下命令：

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* - 指定所创建的IKE隧道的名称。

执行该命令后，CLI进入到IKE隧道配置模式。对IKE隧道的所有参数配置都需要在该模式下进行。

在全局配置模式下使用**no tunnel ipsec** *tunnel-name* **auto**删除指定的IKE隧道。

指定 IPSec协议的操作模式

为IKE隧道指定操作模式，可以是隧道模式或者传输模式，在IKE隧道配置模式下使用以下命令：

mode {**transport** | **tunnel**}

- **transport** – 指定IPSec协议的操作模式为传输模式。
- **tunnel** – 指定IPSec协议的操作模式为隧道模式。该模式为系统默认模式。

使用**no mode**命令恢复默认模式。

指定ISAKMP网关

为IKE隧道指定ISAKMP网关，请在IKE隧道配置模式下使用以下命令：

isakmp-peer *peer-name*

- *peer-name* – 指定ISAKMP网关的名称。

使用**no isakmp-peer**取消对ISAKMP网关的指定。

指定P2提议

为IKE隧道指定P2提议，请在IKE隧道配置模式下使用以下命令：

ipsec-proposal *p2-name*

- *p2-name* – 指定P2提议的名称。

使用**no ipsec-proposal**取消对P2提议的指定。

指定第二阶段ID

为IKE IPSec隧道指定第二阶段ID，请在IKE隧道配置模式下使用以下命令：

id {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}

- **auto** – 自动指定第二阶段ID。此参数为系统默认配置。
- **local** *ip-address/mask* – 指定本端第二阶段local ID。

- **remote** *ip-address/mask* – 指定本端第二阶段remote ID。
- **service** *service-name* – 指定服务名称。

用户可配置最多64个第二阶段ID用于协商建立多个IKE隧道。

使用**no id** {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}命令恢复系统默认配置。

配置IPsec VPN流量分流与限流

流量分流功能根据第二阶段ID的配置，在IKE隧道入口对进入IKE隧道的流量进行分流。如果流量的源IP地址、目的IP地址、以及流量的类型(service)匹配某一个第二阶段ID的配置，则该流量进入相应的IKE隧道进行封装发送。如果没有匹配的第二阶段ID，则该流量被丢弃。

流量限流功能根据第二阶段ID的配置，在IKE隧道出口对解封装后的流量进行限流。如果解封装后流量的源IP地址、目的IP地址、以及流量的类型(service)匹配某一个第二阶段ID的配置，则该流量被接收设备继续处理；如果流量无法匹配任何一个第二阶段ID的配置，则该流量被丢弃。

开启流量分流与限流功能，在IKE隧道配置模式，使用如下命令：

check-id

在IKE隧道配置模式下，使用该命令no的形式关闭流量分流与限流功能。

启用接受对端ID功能

默认情况下，该功能为禁用状态。开启该功能后，如果安全设备作为接收端，它将接受对端的ID为它的IKE协商第二阶段ID，并返回该ID给对端。如果用户配置了多个第二阶段ID，需要关闭此功能。在IKE隧道配置模式下，使用以下命令开启接受对端ID的功能：

accept-all-proxy-id

在IKE隧道配置模式下，使用该命令no的形式关闭接受对端ID功能：

no accept-all-proxy-id

配置自动连接功能

设备提供了两种触发建立SA的方式：自动方式和流量触发方式。

- 自动方式是指设备每60秒检查一次SA的状态，如果SA未建立则自动发起协商请求；
- 流量触发方式是指当有数据流量需要通过隧道进行传输时，该隧道才发起协商请求。

默认情况下，使用流量触发方式。欲使用自动方式，请在IKE隧道配置模式下使用以下命令：

```
auto-connect
```

使用**no auto-connect**命令恢复系统的默认设置。

注意: 自动连接功能仅在对端IP地址为静态类型且本端可以作为发起端时有效。

配置分片功能

用户可以指定是否允许转发设备将包进行分片处理。为IKE隧道配置分片功能，请在IKE隧道配置模式下使用以下命令：

```
df-bit {copy | clear | set}
```

- **copy** – 直接从发包端拷贝IP包的DF选项。该选项为系统默认选项。
- **clear** – 允许转发设备对包做分片处理。
- **set** – 不允许转发设备对包做分片处理。

使用**no df-bit**恢复系统的默认设置。

配置防重放功能

防重放（anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。默认情况下，防重放功能是关闭的。为IKE IPSec隧道配置防重放功能，请在IKE IPSec隧道配置模式下使用以下命令：

```
anti-replay {32 | 64 | 128 | 256 | 512}
```

- **32** – 指定防重放的窗口为32。
- **64** – 指定防重放的窗口为64。
- **128** – 指定防重放的窗口为128。

- **256** – 指定防重放的窗口为256。
- **512** – 指定防重放的窗口为512。

在网络状况较差时，例如存在严重乱序现象等，请选择较大的窗口。

使用**no anti-replay**命令关闭防重放功能。

配置VPN监控及冗余备份功能

Hillstone设备能够监测指定的VPN隧道是否连通，并且能够实现两条或者多条VPN隧道的备份或者分流。该功能仅对基于路由的VPN以及基于策略的VPN均有效。具体实现包括以下两种环境：

- 为同一个远程对端配置备份VPN隧道，并且在任意时刻只有一个隧道处于活动状态。最初，主VPN隧道处于活动状态，如果监测到该主隧道中断，Hillstone设备会通过备份隧道重新传输信息流；
- 为同一个远程对端配置了两个或者多个VPN隧道，所有隧道都同时处于活动状态，并且通过等价多径路由（ECMP）实现负载均衡。如果监测到隧道中断，Hillstone设备会通过其它隧道重新传输信息流。

VPN监控功能支持通过Ping报文对目标隧道进行监测。默认情况下，该功能是关闭的。配置VPN监控功能，请在IKE IPSec隧道配置模式下使用以下命令：

vpn-track [*A.B.C.D*] [**src-ip** *A.B.C.D*] [**interval** *time-value*] [**threshold** *value*]

- *A.B.C.D* – 指定监测目标的IP地址。当对端设备为Hillstone设备时，如果不指定该参数，系统默认为对端IP地址。此IP地址不能为“0.0.0.0”和“255.255.255.255”。
- **src-ip** *A.B.C.D* – 指定发送Ping监测报文的源IP地址。当对端设备为Hillstone设备时，如果不指定该参数，系统默认为出接口IP地址。此IP地址不能为“0.0.0.0”和“255.255.255.255”。
- **interval** *time-value* – 指定发送Ping监测报文的时间间隔，单位为秒。范围是1到255秒。默认值是10秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标隧道中断。取值范围是1到255。默认值是10。

使用**no vpn-track**命令取消VPN监控功能的配置。

默认情况下，如果是基于路由的VPN，VPN监控功能一旦监测到中断的VPN隧道，会立即通知路由模块中断的VPN隧道信息并进行隧道路由的更新处理；如果是基于策略的VPN，VPN监控功能一旦监测到中断的VPN隧道，会立即通知策略模块中断的VPN隧道信息并进行隧道策略的更新处理。用户可以通过命令禁用VPN监控失败通知功能，使其不对监测失败的隧道信息进行通知。禁用或者启用VPN监控失败通知功能，在IKE IPSec隧道配置模式下，使用以下命令：

track-event-notify {**disable** | **enable**}

- **disable** – 禁用。
- **enable** – 启用。默认状态下，系统启用该功能。

VPN监控功能包括active和dead两种状态。用户可以使用相应的show命令在CLI的任何模式下查看VPN监控功能的状态以及配置信息：

- 查看VPN监控功能的状态：**show ipsec sa** {*id*}
- 查看VPN监控功能的配置情况：**show tunnel ipsec** {**manual** | **auto**} {*tunnel-name*}

例如：

```
查看VPN监控功能状态
hostname(config)# show ipsec sa 5
VPN Name: vpn1
Outbound
Gateway: 1.1.1.2
......
VPN track status: alive
Inbound
Gateway: 1.1.1.2
......
VPN track status: alive
查看VPN监控功能配置
hostname(config)# show tunnel ipsec auto vpn1
```

```
Name: vpn1

mode: tunnel

......

vpn-track: enable

tracknotify: enable

vpntrack destination 1.1.1.1

vpntrack source ip: 2.2.2.2

vpntrack interval: 3

vpntrack threshold: 3
```

提示: 关于VPN监控及冗余备份的具体实例，请参阅VPN监控及冗余备份的具体实例一节。

设置Commit位

用户可以配置使响应方设置Commit位，从而防止出现丢包和时间差现象。但是，设置Commit位可能导致响应速度变慢。设置Commit位，请在IKE IPSec隧道配置模式下使用以下命令：

响应方设置Commit位：**`responder-set-commit`**

响应方不设置Commit位：**`no responder-set-commit`**

指定描述信息

为所配置的IKE隧道指定描述信息，请在IKE IPSec隧道配置模式下使用以下命令：

`description` *`string`*

- *`string`* – IKE隧道的描述信息。

使用**`no description`**命令删除IKE隧道的描述信息。

配置自动生成路由功能

对于IKEv1 VPN，当指定对端的IP地址类型为static或dynamic时，配置自动生成路由功能后，每创建一个IPSec SA，设备会将目的地址为对端的local ID、下一跳为隧道接口的路由条目添加到自己的路由表。删除一个IPSec SA后，相应的路由条目也会被删除。

默认情况下，设备的自动生成路由功能是关闭的。开启此功能，请在ISAKMP配置模式下，使用以下命令：

generate-route

使用**no generate-route**命令关闭自动生成路由功能。

IKEv2 VPN

IKEv2 VPN的配置包括：

- 配置P1提议
- 配置IKEv2对等体
- 配置P2提议
- 配置隧道

配置P1提议

P1提议是IKEv2安全提议，用于保存IKE_SA_INIT交换中所使用的安全参数，包括加密算法、完整性验证算法、PRF（pseudo-random function）算法和DH组。一个完整的IKEv2安全提议中至少应该包含一组安全参数，即一个加密算法、一个完整性验证算法、一个PRF算法和一个DH组。

创建P1提议

创建一个P1提议，即IKEv2安全提议，请在全局配置模式下使用以下命令：

ikev2 proposoal *p1-name*

- *p1-name* – 指定所创建的P1提议的名称。执行该命令后，CLI进入到P1提议配置模式。用户可以在该模式下对P1提议进行参数配置。

使用**no ikev2 proposoal** *p1-name*命令删除指定的P1提议。

指定验证算法

StoneOS支持以下验证算法：MD5、SHA-1以及SHA-2（包括SHA-256、SHA-384和SHA-512）。用户可指定至少一种最多四种验证算法。指定IKEv2安全提议的验证算法，在P1提议模式下使用以下命令：

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为StoneOS的默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** – 指定使用SHA-512验证算法。摘要为512比特。

使用**no hash**命令恢复默认认证方式。

指定PRF算法

StoneOS支持以下PRF算法：MD5、SHA-1以及SHA-2（包括SHA-256、SHA-384和SHA-512）。用户可指定至少一种最多四种PRF算法。指定IKEv2安全提议的PRF算法，在P1提议模式下使用以下命令：

prf {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

- **md5** – 指定使用MD5算法。摘要为128比特。
- **sha** – 指定使用SHA-1算法。摘要为160比特。该算法为StoneOS的默认算法。
- **sha256** – 指定使用SHA-256算法。摘要为256比特。
- **sha384** – 指定使用SHA-384算法。摘要为384比特。
- **sha512** – 指定使用SHA-512算法。摘要为512比特。

使用**no prf**命令恢复默认认证方式。

指定加密算法

StoneOS提供以下四种加密算法：3DES、128bit AES、192bit AES以及256bit AES。用户可指定至少一种最多四种加密算法。指定IKEv2安全提议的加密算法，在P1提议配置模式下使用以下命令：

encryption {**3des** | **aes** | **aes-192** | **aes-256**}

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为StoneOS系统默认方法。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。
- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。

使用**no encryption**命令恢复默认加密算法。

选择DH组

Diffie-Hellman（DH）是一种建立密钥的方法。DH组决定DH交换中密钥生成“材料”的长度。密钥的牢固性部分决定于DH组的强度。指定IKEv2安全提议的DH组，在P1提议配置模式下使用以下命令：

group {**1** | **2** | **5**}

- **1** – 选择DH组1。密钥的长度为768比特。
- **2** – 选择DH组2。密钥的长度为1024比特。DH组2为StoneOS系统默认选择。
- **5** – 选择DH组5。密钥的长度为1536比特。

使用**no group**命令取消已指定的DH组。

指定的生命周期

IKEv2 SA的生命周期不需要协商，由各自的配置决定，重协商总是由生命周期较小的一方发起，可尽量避免两端同时发起重协商造成冗余SA的生成，导致两端SA状态不一致。指定本端IKEv2 SA的生命周期，在P1提议配置模式下使用以下命令：

lifetime *time-value*

- *time-value* – 指定IKEv2 SA的生命周期长度，单位为秒。默认28800秒。范围是180到86400秒。

使用**no lifetime**命令恢复默认生命周期长度。

配置IKEv2对等体

创建一个IKEv2对等体后，用户可以配置对等体的IKE协商模式、对等体的IP地址、IKE安全提议、本地ID等。

创建IKEv2对等体

创建IKEv2对等体，在全局配置模式下，使用以下命令:

ikev2 peer *peer-name*

- *peer-name* – 指定对等体的名称。

执行该命令后，CLI进入到IKEv2对等体配置模式。用户可以在该模式下对IKEv2对等体进行参数配置。

在全局配置模式下使用**no ikev2 peer** *peer-name*命令删除指定的IKEv2对等体。

绑定接口到对等体

用户可以绑定某个接口到IKEv2对等体。将接口绑定到IKEv2对等体，在IKEv2对等体配置模式下使用以下命令：

interface *interface-name*

- *interface-name* – 指定被绑定接口的名称。

使用**no interface**命令取消接口绑定。

指定对端的IP地址

用户可以为所创建的IKEv2指定对端的IP地址。指定对端的IP地址，在IKEv2对等体配置模式下使用以下命令：

match-peer *ip-address*

- *ip-address* - 指定对端的IP地址。

使用**no match-peer**命令取消对端IP地址。

配置认证方式

StoneOS支持预共享密钥认证方式，且该认证方式为默认认证方式。为IKEv2对等体指定预共享密钥认证方式，在IKEv2对等体配置模式下使用以下命令：

auth psk

指定P1提议

为IKEv2对等体指定P1提议，在IKEv2对等体配置模式下使用以下命令：

ikev2-proposal *p1-name*

- *p1-name* – 指定P1提议的名称。

使用**no ikev2-proposal** *p1-name*取消对P1提议的指定。

配置本端ID

配置本端的ID，请在IKEv2对等体配置模式下使用以下命令：

local-id {**fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn***string* – 指定使用FQDN类型的ID。string为ID的具体内容。
- **key-id***string* - 指定使用Key ID类型的ID。string为ID的具体内容。
- **ip***ip-address* - 指定使用IP地址类型的ID。ip-address为ID的具体内容。

使用**no local-id**命令取消对本端ID的配置。

指定连接类型

创建的IKEv2对等体可以是发起端、响应端或者既是发起端也是响应端。指定IKEv2对等体的连接类型，在IKEv2对等体配置模式下使用以下命令：

connection-type {**bidirectional** | **initiator-only** | **responder-only**}

- **bidirectional** – 指定该ISAKMP网关既是发起端也是响应端。该选项为系统的默认选项。
- **initiator-only** – 指定该ISAKMP网关仅是发起端。
- **responder-only** – 指定该ISAKMP网关仅是响应端。

使用**no connection-type**命令恢复默认连接方式。

创建IKEv2 Profile

IKEv2 profile用来保存非协商的IKEv2 SA的参数，例如对端的身份信息、预共享密钥、被保护数据流量的信息。IKEv2 profile在发起端和响应端都需要配置。创建IKEv2 Profile，在IKEv2对等体配置模式下使用以下命令：

ikev2-profile *profile-name*

- *profile-name* – 指定该IKEv2 profile的名称。

执行该命令后，CLI进入到IKEv2 profile配置模式。用户可以在该模式下对非协商的IKEv2 SA的参数进行配置。

在全局配置模式下使用**no ikev2-profile** *profile-name*命令删除指定的IKEv2 profile。

配置对端ID

配置对端的ID，请在IKEv2 profile配置模式下使用以下命令：

remote id {**fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn** *string* – 指定使用FQDN类型的ID。string为ID的具体内容。
- **key-id** *string* - 指定使用Key ID类型的ID。string为ID的具体内容。
- **ip** *ip-address* - 指定使用IP地址类型的ID。ip-address为ID的具体内容。

使用**no remote id**命令取消对对端ID的配置。

配置预共享密钥

两端的预共享密钥的值相同时，IKEv2隧道才能建立。配置预共享密钥，在IKEv2 profile配置模式下使用以下命令：

remote key *key-value*

- *key-value* – 指定预共享密钥的值。

使用**no remote key**命令删除所指定的预共享密钥。。

指定被保护的数据流量信息

使用traffic-selector参数指定被保护的数据流量的信息。本端的源地址和对端目的地址在同一网段，并且本端的目的地址和对端的源地址在同一网段，IKEv2隧道才能建立。目前仅支持在一个profile下使用traffic-selector参数指定一个源地址和一个目的地址。

traffic-selector {**src** | **dst**} **subnet** *ip/mask*

- **src** – 指定本端的外发数据流量的源地址。
- **dst** – 指定本端的接受数据流量的目的地址。
- **subnet** *ip/mask* – 输入IP地址及子网掩码。

使用**no traffic-selector** {**src** | **dst**} **subnet** *ip/mask*命令删除所配置的信息。

配置P2提议

P2提议是IPSec安全提议，用于保存IPsec需要使用的安全协议、加密/认证算法等，为协商IPSec SA提供各种安全参数。对P2提议的配置包括指定协议类型、加密算法、验证算法、压缩算法和生命周期。

创建P2提议，即IPSec安全提议，请在全局配置模式下使用以下命令：

ikev2 ipsec proposal *p2-name*

- *p2-name* – 指定所创建的P2提议的名称。执行该命令后，CLI进入到P2提议配置模式。对P2提议各项参数的配置都要在该模式下进行。

使用**no ikev2 ipsec proposal** *p2-name*命令删除指定的IPSec安全提议。

指定协议类型

P2提议可使用的协议类型有ESP。为P2提议指定协议类型，在P2提议配置模式下使用以下命令：

protocol esp

- **esp** – 指定使用ESP协议。该协议为系统默认协议。

指定验证算法

用户可以为P2提议指定至少一种最多四种验证算法。为P2提议指定验证算法，在P2提议配置模式下使用以下命令：

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **null**}

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为StoneOS的默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **Sha512** –指定使用SHA-512验证算法。摘要为512比特。
- **null** – 不使用验证功能。

使用**no hash**命令恢复默认验证算法。

指定加密算法

用户可以为P2提议指定至少一种最多四种加密算法。为P2提议指定加密算法，在P2提议配置模式下使用以下命令：

encryption {**3des**| **des** | **aes-192** | **aes-256** | **null** }

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为StoneOS系统默认方法。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。
- **null** – 不使用加密功能。

使用**no encryption**命令恢复默认加密算法。

配置PFS功能

PFS（Perfect Forward Security）功能决定新密钥的生成方式，而不是新密钥的生成时间。PFS保证无论在哪一阶段，一个密钥只能使用一次，而且，生成密钥的“材料”也只能使用一次。某个“材料”在生成了一个密钥后就被弃，绝不用来再生成任何其它密钥。这样可以确保一旦单个密钥泄密，最多只可能影响用该密钥加密的数据，而不会危及整个通信。PFS功能是由DH算法做保障的。配置P2提议的PFS功能，在P2提议配置模式下使用以下命令：

group {**nopfs** | **1** | **2** | **5**}

- **nopfs** – 不使用PFS功能。该选项为系统的默认选项。
- **1** – 选择DH组1。密钥的长度为768比特。
- **2** – 选择DH组2。密钥的长度为1024比特。
- **5** – 选择DH组5。密钥的长度为1536比特。

使用**no group**命令恢复默配置。

指定生命周期

Hillstone设备按时间衡量生命周期。当IPSec SA的时间达到特定值时，SA就会过期，需要重新进行协商。指定P2提议的生命周期，在P配置模式，使用以下命令：

lifetime *seconds*

- *seconds* – 指定时间类型生命周期的时间长度，单位为秒。默认值是28800秒。范围是180到86400秒。

使用以**no lifetime**命令恢复默认配置。

配置隧道

通过IKEv2配置IPSec隧道，用户需要配置的选项有指定操作模式、IKEv2对等体、IKEv2安全提议、以及自动连接。

创建IKEv2隧道

创建IKEv2隧道，在全局配置模式下，使用以下命令：

tunnel ipsec *tunnel-name* **ikev2**

- **tunnel-name** - 指定所创建的IKEv2隧道的名称。

执行该命令后，CLI进入到IKEv2隧道配置模式。对IKEv2隧道的所有参数配置都需要在该模式下进行。

在全局配置模式下使用**no tunnel ipsec** *tunnel-name* **ikev2**删除指定的IKEv2隧道。

指定 IKEv2隧道的操作模式

StoneOS支持IKEv2隧道的操作模式为隧道模式。该模式为系统默认模式。

指定IKEv2对等体

为IKEv2隧道指定IKEv2对等体，请在IKEv2隧道配置模式下使用以下命令：

ikev2-peer *peer-name*

- *peer-name* – 指定IKEv2对等体的名称。

使用**no ikev2-peer**取消对IKEv2对等体的指定。

指定P2提议

为IKEv2隧道指定P2提议，请在IKEv2隧道配置模式下使用以下命令：

ipsec-proposal p2-name1 [**p2-name2**] [**p2-name3**]

- **p2-name** – 指定P2提议的名称。用户最多可以为IKEv2隧道指定3个P2提议供对端选择使用。

使用**no ipsec-proposal**取消对P2提议的指定。

配置自动连接功能

设备支持自动方式触发建立SA。自动方式是指设备每60秒检查一次SA的状态，如果SA未建立则自动发起协商请求。自动连接功能默认不开启。使用自动方式，请在IKE隧道配置模式下使用以下命令：

auto-connect

注意: 自动连接功能仅在本端可以作为发起端时有效。

XAUTH

XAUTH是对IKE协议的扩展和增强，允许设备结合已配置的认证服务器（RADIUS和本地AAA服务器）对试图访问IPSec VPN网络的用户进行身份认证，目前大量应用在移动终端上。远程用户发起VPN连接请求后，设备上的XAUTH服务器会中断VPN协商过程并要求用户输入有效的用户名和密码进行认证，认证成功后会继续VPN协商过程并为合法的客户端分配IP地址，否则会中断VPN连接。

提示: 有关认证服务器配置的更多信息，请参考《用户认证》的“认证、授权与计费”部分。

XAUTH的配置包括：

- 启用XAUTH服务器
- 配置XAUTH地址池
- 绑定地址池到XAUTH服务器
- 配置IP用户绑定和IP角色绑定规则
- 配置推送到客户端的WINS服务器或DNS服务器

启用XAUTH服务器

XAUTH服务器在设备上默认是禁用的。启用XAUTH服务器，在ISAKMP网关配置模式下，使用以下命令：

```
xauth server
```

在ISAKMP网关配置模式下，使用该命令no的形式禁用XAUTH服务器：

```
no xauth server
```

配置XAUTH地址池

XAUTH通过地址池为客户端分配IP地址。当客户端连接XAUTH服务端成功后，设备端会从地址池里取出一个IP地址与其它相关参数（如DNS服务器地址、WINS服务器地址等）一起分配给客户端。创建XAUTH地址池，在全局配置模式下，使用以下命令：

```
xauth pool pool-name
```

- *pool-name* - 指定XAUTH地址池名称并进入XAUTH地址池配置模式。如果指定的名称已存在，系统会直接进入XAUTH地址池配置模式。

在XAUTH地址池配置模式下，使用该命令no的形式删除指定的XAUTH地址池：

no xauth pool p*ool-name*

指定XAUTH地址池中允许分配的IP地址范围，在XAUTH地址池配置模式下，使用以下命令：

address *start-ip end-ip* **netmask** *mask*

- *start-ip* - 指定XAUTH地址池的起始IP地址。
- *end-ip* - 指定XAUTH地址池的结束IP地址。
- *mask* - 指定网络掩码

在XAUTH地址池配置模式下，使用该命令no的形式删除指定的IP地址范围：

no address

保留地址池中的IP地址为XAUTH地址池中的部分IP地址，当XAUTH服务器从地址池里取出IP地址分配给客户端时，可以保留已经被占用的部分IP地址，不进行分配。

指定XAUTH保留地址池，在XAUTH地址池配置模式下，使用以下命令：

exclude-address *start-ip end-ip*

- *start-ip* - 指定XAUTH保留地址池的起始IP地址。
- *end-ip* - 指定XAUTH保留地址池的结束IP地址。

在XAUTH地址池配置模式下，使用该命令no的形式删除指定的保留地址池IP范围：

no exclude-address

绑定地址池到XAUTH服务器

XAUTH地址池只有在绑定到XAUTH服务器后才会生效。将指定的XAUTH地址池绑定到XAUTH服务器，在ISAKMP网关配置模式下，使用以下命令：

xauth pool-name *pool-name*

- *pool-name* - 指定绑定的地址池名称。

在ISAKMP网关配置模式下，使用该命令no的形式取消地址池绑定：

no xauth pool-name

配置IP用户绑定和IP角色绑定规则

XAUTH服务器通过创建和执行IP地址绑定规则来满足客户端的固定IP地址需求。IP地址绑定规则包括IP用户绑定规则和IP角色绑定规则。IP用户绑定规则将客户端用户与已配置地址池中的某个固定IP地址绑定，当客户端连接成功后，设备端会将绑定的IP地址分配给客户端；IP角色绑定规则是将角色与已配置地址池中的某一IP地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个IP地址分配给客户端。

当XAUTH通过地址池给客户端分配IP地址时，系统会按照一定的顺序对客户端的IP地址绑定规则进行检查，决定如何为客户端分配IP地址：

1. 检查是否已为客户端用户配置 IP用户绑定规则，如果是，则将绑定的 IP地址分配给客户端；否则，需要进一步检查。注意，如果此 IP用户绑定规则中的 IP地址已被占用，则该用户无法登录。
2. 检查是否已为客户端用户配置 IP角色绑定规则，如果是，则从绑定的地址范围中取出一个IP地址分配给客户端；否则，在未绑定的IP地址范围中取出一个IP地址分配给客户端。注意，如果绑定的地址范围中的地址都已经被分配，则该用户无法登录。

注意: IP用户绑定规则中的IP地址和IP角色绑定规则中的IP地址不能重叠。

配置IP用户绑定规则，在XAUTH地址池配置模式下使用以下命令：

ip-binding user *user-name* **ip** *ip-address*

- **user** *user-name* - 指定客户端用户名。
- **ip** *ip-address* - 指定绑定的IP地址。此地址必须为地址池中可以分配的地址。

在XAUTH地址池配置模式下，使用该命令no的形式取消对特定用户IP用户绑定规则的配置：

no ip-binding user *user-name*

配置IP角色绑定规则，在XAUTH地址池配置模式下使用以下命令：

ip-binding role *role-name* **ip-range** *start-ip end-ip*

- **role** *role-name* - 指定角色名称。
- **ip-range** *start-ip end-ip* - 指定绑定的IP范围的起始IP地址start-ip和结束IP地址end-ip。此地址范围必须为地址池中可以分配的地址范围。

在XAUTH地址池配置模式下使用该命令no的形式取消对特定角色的IP角色绑定规则的配置：

no ip-binding role *role-name*

修改IP角色绑定规则排列顺序

一个用户可以绑定到一个或者多个角色，不同角色可以配置不同的IP角色绑定规则。对于绑定到多个角色且多个角色有相应的IP角色绑定规则的用户，设备会对IP角色绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。默认情况下，系统会将新创建的规则放到所有规则的末尾，管理员可以移动已有的IP角色绑定规则从而改变规则的排列顺序。改变规则的排列顺序，在XAUTH地址池配置模式下使用以下命令：

move *role-name1* {**before** *role-name2* | **after***role-name2*| **top** | **bottom**}

- *role -name1* – 指定被移动的IP角色绑定规则的角色名称。
- **before** *role-name2* – 将IP角色绑定规则移动到某个IP角色绑定规则(角色名称为role-name2的规则)之前。
- **after** *role-name2* – 将IP角色绑定规则移动到某个IP角色绑定规则(角色名称为role-name2的规则)之后。
- **top** – 将IP角色绑定规则移动到所有IP角色绑定规则之首。
- **bottom** – 将IP角色绑定规则移动到所有IP角色绑定规则的末尾。

配置推送到客户端的WINS/DNS服务器

配置DNS服务器，在XAUTH地址池配置模式下使用以下命令：

dns *address1* [*address2*]

- *address1* - 指定DNS服务器IP地址。用户最多可配置2个DNS服务器。

在XAUTH地址池配置模式下，使用该命令no的形式取消对DNS服务器的指定：

no dns

配置WINS服务器，在XAUTH地址池配置模式下使用以下命令：

wins *address1* [*address2*]

- *address1* - 指定WINS服务器IP地址。用户最多可配置2个WINS服务器。

在XAUTH地址池配置模式下，使用该命令no的形式取消对WINS服务器的指定：

no wins

强制断开客户端XAUTH连接

XAUTH服务端可以通过命令强制断开某个客户端与设备端的连接。强制断开客户端XAUTH连接，在执行模式使用以下命令：

exec xauth *isakmp-peer-name* **kickout** *user-name*

- *isakmp-peer-name* - 指定ISAKMP对端的名称。
- *user-name* - 指定被强制断开连接的用户名称。

配置非根VSYS隧道配额

配置非根VSYS的IPSec隧道资源配额，在VSYS Profile配置模式下使用以下命令：

tunnel-ipsec max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num*– 指定非根VSYS中IPSec隧道数的最大配额（*max-num* **reserve**）和预留配额（**reserve** *reserve-num*）。最大配额和预留配额根据不同平台取值范围不同。预留配额不能超过最大配额。最大配额取值范围为0至max (capacity*2/max-vsys-num, capacity/10)，默认值为(capacity*2/max-vsys-num, capacity/10)；预留配额的最小值为0。

在VSYS Profile配置模式下使用该命令no的形式删除配额：

notunnel-ipsec max *max-num* **reserve** *reserve-num*

显示IPSec配置信息

用户可以使用相应的show命令在CLI的任何模式下查看IPSec功能的配置信息。

- 查看IKEv1 P1提议的配置信息：**show isakmp proposal** [**p1-name**]
- 查看IKEv2 P1提议的配置信息：**show ikev2 proposal** [*p1-name*]
- 查看IKEv1 ISAKMP网关的配置信息：**show isakmp peer** [*peer-name*]
- 查看IKEv2对等体的配置信息：**show ikev2 peer** [*peer-name*]
- 查看IKEv2对等体中IKEv2 profile的配置信息：**show ikev2 peer** [*peer-name*] **profile** [*profile-name*]
- 查看IKEv1 P2提议的配置信息：**show ipsec proposal** [*proposal-name*]
- 查看手工密钥VPN隧道的配置信息：**show tunnel ipsec manual** [*tunnel-name*]
- 查看IKEv1 隧道的配置信息：**show tunnel ipsec auto** [*tunnel-name*]
- 查看IKEv2隧道的配置信息：**show tunnel ipsec ikev2** [*tunnel-name*]
- 查看IKEv1安全联盟的配置信息：**show isakmp sa** [*dsp_ip*]
- 查看IKEv2安全联盟的配置信息：**show ikev2 ike-sa**
- 查看基于IKEv1的IPSec安全联盟的配置信息：**show ipsec sa** [*id* | **active** | **inactive**]
- 查看基于IKEv2的IPSec安全联盟的配置信息：**show ikev2 ipsec-sa** [*sa-id*]
- 查看XAUTH地址池信息：**show xauth pool** [*pool-name*]
- 查看接入的XAUTH用户信息：**show xauth client** *isakmp-peer-name* [**user** *user-name*]

配置举例

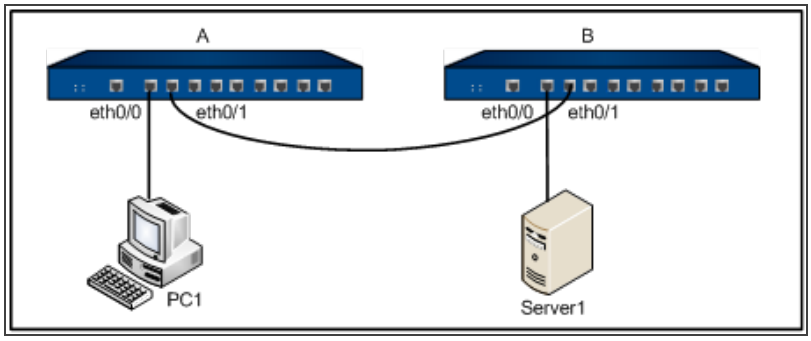
本节介绍通过手工密钥VPN和IKE VPN两种方式建立安全联盟的具体实例、VPN监控及冗余备份的具体实例以及XAUTH的配置实例。

手工密钥VPN

手工密钥VPN隧道要求安全联盟的所有相关配置都由用户手动一一指定。请看以下实例。

组网需求

在HillstoneHillstone设备A和HillstoneHillstone设备B之间建立一个安全隧道，PC1作HillstoneHillstone设备A端的主机，IP地址为188.1.1.2，网关为188.1.1.1；server1作为HillstoneHillstone设备B端的服务器，IP地址为10.110.88.210，网关是10.110.88.220。要求对PC1代表的子网（188.1.1.0/24）与Server1代表的子网（10.110.88.0/24）之间的数据流进行安全保护（通过基于策略的VPN方式实现VPN的应用）。安全协议采用ESP协议，加密算法采用3DES，验证算法采用SHA1，压缩算法采用DEFLATE。下图为该需求的组网图。



配置步骤

第一步：配置Hillstone设备接口。

```
Hillstone设备A
  hostname(config)# interface ethernet0/0
  hostname(config-if-eth0/0)# zone trust
  hostname(config-if-eth0/0)# ip address 188.1.1.1/24
  hostname(config-if-eth0/0)# exit
  hostname(config)# interface ethernet0/1
  hostname(config-if-eth0/1)# zone untrust
  hostname(config-if-eth0/1)# ip address 192.168.1.2/24
  hostname(config-if-eth0/1)# exitip address 10.1.1.1/24
  Hillstone设备B
  hostname(config-if-eth0/0)# zone trust
  hostname(config-if-eth0/0)# ip address 10.110.88.220/24
```

```
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/0
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 192.168.1.3/24
hostname(config-if-eth0/1)# exitip route 172.16.10.0/24 tunnel1 10
```

第二步：配置路由。

```
Hillstone设备A
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.110.88.0/24 192.168.1.3
hostname(config-vrouter)# exit
Hillstone设备B
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 188.1.1.0/24 192.168.1.2
hostname(config-vrouter)# exit
```

第三步：手动配置名为VPN1的隧道。

```
Hillstone设备A
hostname(config)# tunnel ipsec vpn1 manual
hostname(config-tunnel-ipsec-manual)# interface ethernet0/1
hostname(config-tunnel-ipsec-manual)# protocol esp
hostname(config-tunnel-ipsec-manual)# peer 192.168.1.3
hostname(config-tunnel-ipsec-manual)# hash sha
hostname(config-tunnel-ipsec-manual)# hash-key inbound 1234 out-
bound 5678
hostname(config-tunnel-ipsec-manual)# encryption 3des
hostname(config-tunnel-ipsec-manual)# encryption-key inbound 00ff
```

```
outbound 123a
hostname(config-tunnel-ipsec-manual)# compression deflate
hostname(config-tunnel-ipsec-manual)# spi 6001 6002
hostname(config-tunnel-ipsec-manual)# exit
Hillstone设备B
hostname(config)# tunnel ipsec vpn1 manual
hostname(config-tunnel-ipsec-manual)# interface ethernet0/1
hostname(config-tunnel-ipsec-manual)# protocol esp
hostname(config-tunnel-ipsec-manual)# peer 192.168.1.2
hostname(config-tunnel-ipsec-manual)# hash sha
hostname(config-tunnel-ipsec-manual)# hash-key inbound 5678 out-
bound 1234
hostname(config-tunnel-ipsec-manual)# encryption 3des
hostname(config-tunnel-ipsec-manual)# encryption-key inbound 123a
outbound 00ff
hostname(config-tunnel-ipsec-manual)# compression deflate
hostname(config-tunnel-ipsec-manual)# spi 6002 6001
hostname(config-tunnel-ipsec-manual)# exit
```

第四步：配置Hillstone设备策略规则。

```
Hillstone设备A
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action fromtunnel vpn1
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
Hillstone设备B
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn1
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

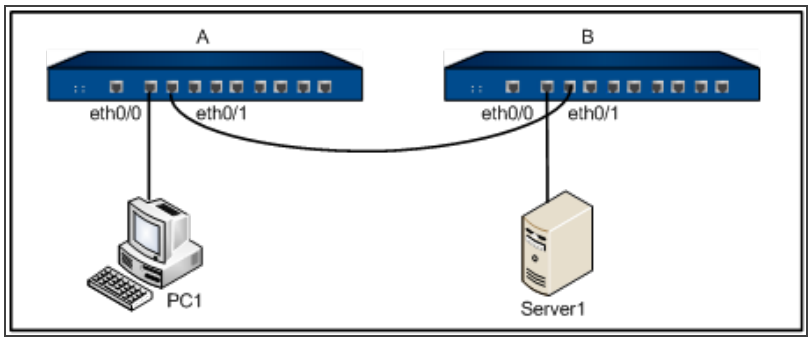
完成以上配置后，Hillstone设备A和Hillstone设备B之间的安全隧道便建立成功了。子网（188.1.1.0/24）与server1代表的子网（10.110.88.0/24）之间的数据流将会被加密传输。

IKE VPN

本节介绍通过IKE方式创建安全联盟的实例。

组网需求

在HillstoneHillstone设备A和HillstoneHillstone设备B之间建立一个安全隧道，PC1作为Hillstone Hillstone设备A端的主机，IP地址为10.1.1.1，网关为10.1.1.2；Server1作为Hillstone Hillstone设备B端的服务器，IP地址为192.168.1.1，网关是192.168.1.2。要求对PC1代表的子网（10.1.1.0/24）与server1代表的子网（192.168.1.0/24）之间的数据流进行安全保护（通过基于路由的VPN方式实现VPN的应用）。安全协议采用ESP协议，加密算法采用3DES，验证算法采用SHA1，压缩算法采用DEFLATE。组网图请参考下图：



配置步骤

第一步：配置Hillstone设备接口。

```
Hillstone设备A
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
```

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
Hillstone设备B
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
```

第二步：配置Hillstone设备策略规则。

```
Hillstone设备A
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
Hillstone设备B
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

第三步：配置路由。

```
Hillstone设备A
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.1.0/24 tunnel1
hostname(config-vrouter)# exit
Hillstone设备B
```

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.1.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

第四步：配置P1提议。

```
Hillstone设备A
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
Hillstone设备B
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

第五步：配置ISAKMP网关。

```
Hillstone设备A
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.2
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# exit
```

```
Hillstone设备B
hostname(config)# isakmp peer west
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.1
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# exit
```

第六步：配置P2提议。

```
Hillstone设备A
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# compression deflate
hostname(config-ipsec-proposal)# exit
Hillstone设备B
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# compression deflate
hostname(config-ipsec-proposal)# exit
```

第七步：配置名为VPN的隧道。

```
Hillstone设备A
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
```

```
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 10.1.1.0/24 remote
192.168.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
Hillstone设备B
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 192.168.1.0/24 remote
10.1.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
```

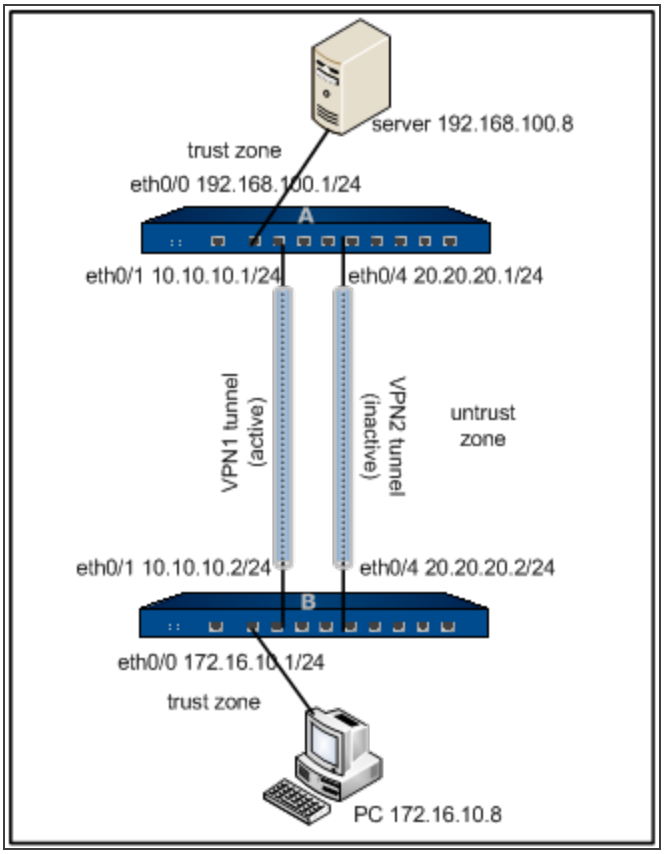
完成以上配置后，Hillstone设备A和Hillstone设备B之间的安全隧道便建立成功了。子网（10.1.1.0/24）与Server1代表的子网（192.168.1.0/24）之间的数据流将会被加密传输。

基于路由的VPN监控及冗余备份功能配置举例

该节介绍基于路由的VPN监控及冗余备份功能配置实例。

组网需求

在Hillstone设备A和Hillstone设备B之间配置IKE VPN隧道VPN1 tunnel和VPN2 tunnel，server作为Hillstone设备A端的服务器，IP地址为192.168.100.8，网关是192.168.100.1；PC作为Hillstone设备B端的主机，IP地址为172.16.10.8，网关为172.16.10.1。要求实现VPN1 tunnel和VPN2 tunnel的VPN监控，并当主隧道（VPN1 tunnel）链路发生故障时，流量转向备份隧道（VPN2 tunnel）；主隧道恢复正常时，流量切换回主隧道。组网图参见下图：



配置步骤

第一步：配置Hillstone设备A：

```
配置接口：
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.100.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
```

```
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.1/24
hostname(config-if-eth0/4)# exit
配置P1提议
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
配置ISAKMP网关：
hostname(config)# isakmp peer gwa-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.2
hostname(config-isakmp-peer)# pre-share
U8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwa-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.2
hostname(config-isakmp-peer)# pre-share i39jn-
nNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
配置P2提议：
hostname(config)# ipsec proposal p2
```

```
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

配置VPN隧道：

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold
9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold
9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

创建隧道接口并绑定VPN隧道：

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)#
hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel
hostname(config-if-tun1)# exit
hostname(config)# interface tunnel2
```

```
hostname(config-if-tun2)# zone untrust
hostname(config-if-tun2)# ip address 10.2.2.1/24
hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel
hostname(config-if-tun2)# exit
```

配置路由：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)#
hostname(config-vrouter)# ip route 172.16.10.0/24 tunnel2 20
hostname(config-vrouter)# exit
```

配置策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
```

```
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

第二步：配置Hillstone设备B：

配置接口：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 172.16.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.2/24
hostname(config-if-eth0/4)# exit
```

配置P1提议

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

配置ISAKMP网关：

```
hostname(config)# isakmp peer gwb-peer-1
```

```
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.1
hostname(config-isakmp-peer)# pre-share
U8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwb-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.1
hostname(config-isakmp-peer)# pre-share i39jn-
nNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
```

配置P2提议：

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

配置VPN隧道：

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold
9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# auto-connect
```

```
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold
9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

创建隧道接口并绑定VPN隧道：

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 10.1.1.2/24
hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel
hostname(config-if-tun1)# exit
hostname(config)# interface tunnel2
hostname(config-if-tun2)# zone untrust
hostname(config-if-tun2)# ip address 10.2.2.2/24
hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel
hostname(config-if-tun2)# exit
```

配置路由：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel1 1
hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel2 2
hostname(config-vrouter)# exit
```

配置策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

由于本例中VPN终端设备都是Hillstone设备，因此可使用缺省源和目标地址进行VPN监控。

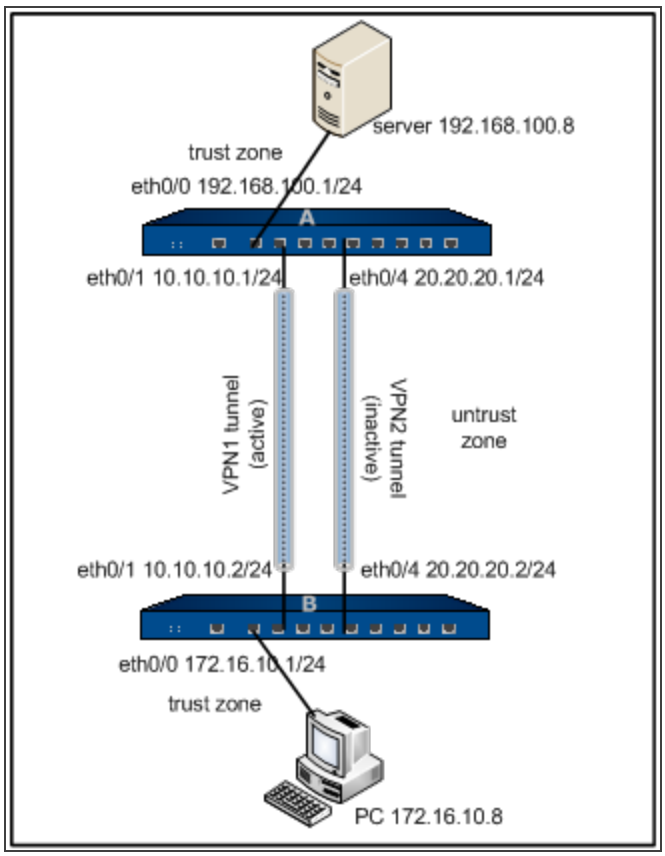
基于策略的VPN监控及冗余备份功能配置举例

该节介绍基于策略的VPN监控及冗余备份功能配置实例。

组网需求

在Hillstone设备A和Hillstone设备B之间配置IKE VPN隧道VPN1 tunnel和VPN2 tunnel，server作为Hillstone设备A端的服务器，IP地址为192.168.100.8，网关是192.168.100.1；PC作为Hillstone

设备B端的主机，IP地址为172.16.10.8，网关为172.16.10.1。要求实现VPN1 tunnel和VPN2 tunnel的VPN监控，并当主隧道（VPN1 tunnel）链路发生故障时，流量转向备份隧道（VPN2 tunnel）；主隧道恢复正常时，流量切换回主隧道。组网图参见下图：



配置步骤

第一步：配置Hillstone设备A：

```
配置接口：
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.100.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.1/24
```

```
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.1/24
hostname(config-if-eth0/4)# exit
```

配置路由：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 172.16.10.0/24 20.20.20.2
hostname(config-vrouter)# exit
```

配置P1提议

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

配置ISAKMP网关：

```
hostname(config)# isakmp peer gwa-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.2
hostname(config-isakmp-peer)# pre-
shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwa-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
```

```
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.2
hostname(config-isakmp-peer)# pre-share i39jn-
nNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
```

配置P2提议：

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

配置VPN隧道：

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold
5
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold
5
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)#auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

配置策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn2-tunnel
hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# rule id 5
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

第二步：配置Hillstone设备B：

```
配置接口：
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 172.16.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.2/24
hostname(config-if-eth0/4)# exit
配置路由：
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.100.0/24 20.20.20.1
hostname(config-vrouter)# exit
```

配置P1提议

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

配置ISAKMP网关：

```
hostname(config)# isakmp peer gwb-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.1
hostname(config-isakmp-peer)# pre-
shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwb-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.1
hostname(config-isakmp-peer)# pre-sharei39jn-
nNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
```

配置P2提议：

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
```

```
hostname(config-ipsec-proposal)# exit
```

配置VPN隧道：

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1threshold 5
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold
5
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)#auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

配置策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# src-ip 192.168.100.8/24
```

```
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 5
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

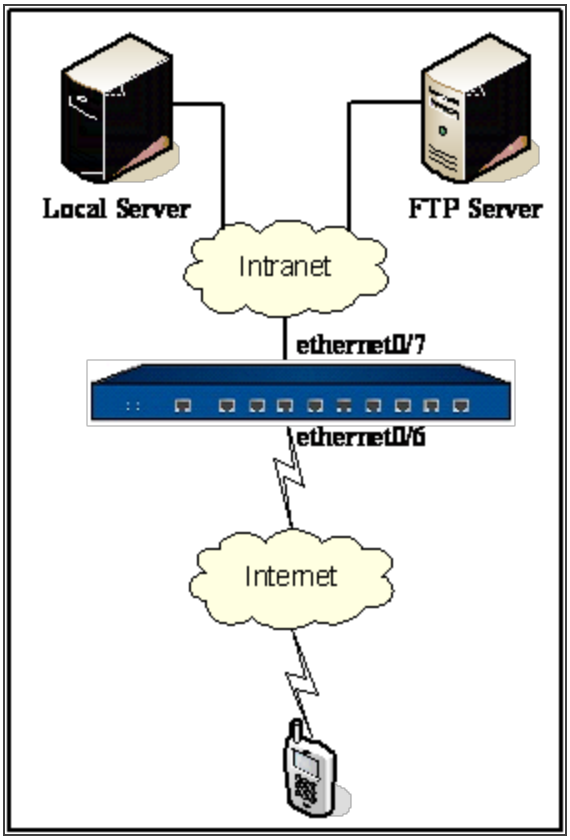
由于本例中VPN终端设备都是Hillstone设备，因此可使用缺省源和目标地址进行VPN监控。

XAUTH

本节介绍典型的XAUTH配置实例。

组网需求

Hillstone设备上启用了XAUTH服务器，使用本地AAA服务器认证用户。要求当用户试图通过手机终端创建VPN连接并访问内网的FTP服务器时，XAUTH服务器通过预共享秘钥方式对用户身份进行验证，并允许通过验证的用户访问内网资源。组网图请参考下图。



配置步骤

第一步：配置接口、安全域和策略：

```
接口配置：

hostname(config)# interface ethernet0/6

hostname(config-if-eth0/7)# zone trust

hostname(config-if-eth0/7)# ip address 6.6.6.6 255.255.255.0
```

```
hostname(config-if-eth0/7)# manage ping
hostname(config-if-eth0/7)# manage ssh
hostname(config-if-eth0/7)# manage http
hostname(config-if-eth0/7)# exit
hostname(config)# interface ethernet0/7
hostname(config-if-eth0/6)# zone untrust
hostname(config-if-eth0/6)# ip address 7.7.7.7 255.255.255.0
hostname(config-if-eth0/6)# exit
hostname(config)# rule top
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

第二步：配置AAA服务器：

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user xauth
hostname(config-user)# password test
hostname(config-user)# ike-id key-id xauth
hostname(config-user)# end
hostname(config)#
```

第三步：配置XAUTH地址池

```
hostname(config)# xauth pool pool
hostname(config-xauth-pool)# address 9.9.9.9 9.9.9.99 netmask
255.255.255.0
```

```
hostname(config-xauth-pool)# exit
hostname(config)#
```

第四步：配置ISAKMP网关：

```
hostname(config)# isakmp peer xauth
hostname(config-isakmp-peer)# mode aggresive
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# psk-sha-aes128-g2
hostname(config-isakmp-peer)# pre-share XhF44BilJO3b/2HFl5lVqX-
niqeMByq
hostname(config-isakmp-peer)# aaa-server local
hostname(config-isakmp-peer)# local-id key-id xauth
hostname(config-isakmp-peer)# xauth pool-name pool
hostname(config-isakmp-peer)# xauth server
hostname(config-isakmp-peer)# interfaceethernet0/7
hostname(config-isakmp-peer)# exit
hostname(config)#
```

第五步：创建IKE隧道和隧道接口：

```
hostname(config)# tunnel ipsec xauth auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer xauth
hostname(config-tunnel-ipsec-auto)# esp-sha-aes128-g0
hostname(config-tunnel-ipsec-auto)# accept-all-proxy-id
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel22
hostname(config-if-tun22)# zone trust
hostname(config-if-tun22)# ip address 9.9.9.1 255.255.255.0
hostname(config-if-tun22)# manage telnet
```

```
hostname(config-if-tun22)# manage ssh
hostname(config-if-tun22)# manage ping
hostname(config-if-tun22)# manage http
hostname(config-if-tun22)# manage https
hostname(config-if-tun22)# manage snmp
hostname(config-if-tun22)# tunnel ipsec xauth
hostname(config-if-tun22)# exit
hostname(config)#
```

完成上述配置后，手机用户可以利用安卓或iOS系统中自带的VPN客户端完成认证（用户名xauth，密码test，IPSec标示符/群组名称xauth）并访问内网资源。

HA Peer模式支持IPsec VPN

HA Peer模式支持IPsec VPN。具体使用请参考如下功能举例。

本节介绍如何在非对称路由环境中将Peer工作模式结合IPsec VPN功能。在配置之前，确认搭建成HA Peer组网模式的两台Hillstone设备采用完全相同的硬件平台、固件版本和相同的许可证。

配置完成后，两台设备均会开启Peer工作模式以及IPsec VPN功能。PC访问Server的流量的流量经由设备A并由设备A上配置的IPsec VPN功能进行安全保护，Server的回包流量经由设备B并由设备B的配置IPsec VPN功能进行安全保护。其中一台设备或设备所在上下链路出现故障，将由另外一台设备接管相应的流量转发功能及IPsec VPN功能。组网图请参见下图：

配置步骤

第一步：配置HA Peer工作模式。

```
Hillstone设备A
  hostname(config)# ha link interface eth0/4
  hostname(config)# ha link ip 1.1.1.1/24
  hostname(config)# ha group 0
  hostname(config-ha-group)# priority 50
  hostname(config-ha-group)# exit
```

```
hostname(config)# ha group 1
hostname(config-ha-group)# priority 100
hostname(config-ha-group)# exit
Hillstone设备B
hostname(config)# ha link interface eth0/4
hostname(config)# ha link ip 1.1.1.2/24
hostname(config)# ha group 0
hostname(config-ha-group)# priority 100
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# exit
```

第二步：配置VFI接口并添加相应路由及NAT规则。

```
Hillstone设备A
hostname(config)# interface eth0/1:1
hostname(con-if-eth0/1:1)# zone untrust
hostname(con-if-eth0/1:1)# ip address192.168.10.1/24
hostname(con-if-eth0/1:1)# exit
hostname(config)# interface eth0/0:1
hostname(con-if-eth0/2:1)# zone trust
hostname(con-if-eth0/2:1)# ip address192.168.20.1/24
hostname(con-if-eth0/2:1)# exit
```

第三步：配置IPsec VPN。

```
Hillstone设备A
hostname(M0D1)(config)# isakmp peer peer1
hostname(M0D1)(config-isakmp-peer)# interface ethernet0/1
```

```
hostname(M0D1)(config-isakmp-peer)# peer 192.168.1.2
hostname(M0D1)(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(M0D1)(config-isakmp-peer)# pre-share hillstone
hostname(M0D1)(config-isakmp-peer)# exit
hostname(M0D1)(config)# isakmp peer peer2
hostname(M0D1)(config-isakmp-peer)# interface ethernet0/1:1
hostname(M0D1)(config-isakmp-peer)# peer 192.168.10.2
hostname(M0D1)(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(M0D1)(config-isakmp-peer)#  pre-share hillstone
hostname(M0D1)(config-isakmp-peer)# exit
hostname(M0D1)(config)# tunnel ipsec vpn1 auto
hostname(M0D1)(config-tunnel-ipsec-auto)# isakmp-peer peer1
hostname(M0D1)(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-
des-g2
hostname(M0D1)(config-tunnel-ipsec-auto)# exit
hostname(M0D1)(config)# tunnel ipsec vpn2 auto
hostname(M0D1)(config-tunnel-ipsec-auto)# isakmp-peer peer2
hostname(M0D1)(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-
des-g2
hostname(M0D1)(config-tunnel-ipsec-auto)# exit
hostname(M0D1)(config)# int tunnel1
hostname(M0D1)(config-if-tun1)# zone vpn
hostname(M0D1)(config-if-tun1)# tunnel ipsec vpn1
hostname(M0D1)(config-if-tun1)# exit
hostname(M0D1)(config)# int tunnel1:1
hostname(M0D1)(config-if-tun1)# zone vpn
hostname(M0D1)(config-if-tun1)# tunnel ipsec vpn2
```

```
hostname(M0D1)(config-if-tun1)# exit
Hillstone设备C
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# peer 192.168.1.1
hostname(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(config-isakmp-peer)# pre-share hillstone
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer peer2
hostname(config-isakmp-peer)# interface ethernet0/2
hostname(config-isakmp-peer)# peer 192.168.10.1
hostname(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(config-isakmp-peer)# pre-share hillstone
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn1 auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer peer1
hostname(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2 auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer peer2
hostname(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# int tunnel1
hostname(config-if-tun1)# zone vpn
hostname(config-if-tun1)# tunnel ipsecvpn1
hostname(config-if-tun1)# exit
```

```
hostname(config)# int tunnel2
hostname(config-if-tun1)# zone vpn
hostname(config-if-tun1)# tunnel ipsec vpn2
hostname(config-if-tun1)# exit
```

第四步：配置VPN相关的策略和路由。

Hillstone设备A

```
hostname(M0D1)(config)# ip vrouter trust-vr
hostname(M0D1)(config-vrouter)# ip route192.168.1.2/24 tunnel1
hostname(M0D1)(config-vrouter)# ip route 192.168.10.2/24 tunnel1:1
hostname(M0D1)(config-vrouter)# ip route 172.16.20.0/24
192.168.2.2
hostname(M0D1)(config-vrouter)# ip route 172.16.20.0/24
192.168.20.2
hostname(M0D1)(config-vrouter)# exit
hostname(M0D1)(config)# rule id 1 from any to any service any per-
mit
```

Hillstone设备C

```
hostname(config)# ip vrouter trust-vr
hostname(config)# ip route 172.16.20.0/24 tunnel1 20
hostname(config)# ip route 172.16.20.0/24 tunnel2 10
hostname(config)# exit
hostname(config)# rule id 1 from any to any service any permit
```

SSL VPN

SSL VPN介绍

为解决远程用户安全访问私网数据的问题，Hillstone设备提供基于SSL的远程登录解决方案SSL VPN。SSL VPN功能可以通过简单易用的方法实现信息的远程连通。

StoneOS的SSL VPN功能包含设备端和客户端两部分。配置了SSL VPN功能的Hillstone设备作为设备端，具有以下功能：

- 接受客户端连接；
- 为客户端分配IP地址、DNS服务器地址和WINS服务器地址；
- 进行客户端用户的认证与授权；
- 进行客户端主机的安全检测；
- 对IPSec数据进行加密与转发。

Hillstone设备SSL VPN的客户端工具为Hillstone Secure Connect。用户可以通过浏览器下载该客户端，然后将其安装到PC，连接设备端成功后，用户就可以通过SSL VPN功能安全的传输数据信息。

不同型号的Hillstone设备默认情况下支持的同时在线最大VPN客户端数不同，如果想增加支持的客户端数，请向代理商购买相应的许可证。

SSL VPN设备端配置

Hillstone设备的SSL VPN功能配置包括以下各部分：

- 地址池配置
- 资源列表配置
- UDP端口号配置
- SSL VPN实例配置
- 绑定SSL VPN实例到隧道接口
- 配置客户端USB Key证书认证

- 配置短信口令认证功能
- 配置主机验证功能
- 配置主机安全检测功能
- 配置最优路径检测功能
- 强制断开客户端SSL VPN连接
- 允许本地用户修改密码

地址池配置

SSL VPN设备端通过地址池给客户端分配IP地址。当客户端连接SSL VPN设备端成功后，设备端会从地址池里取出一个IP地址与其它相关参数（如DNS服务器地址与WINS服务器地址等）一起分配给客户端。在全局配置模式，使用以下命令创建SSL VPN地址池：

scvpn pool *pool-name*

- *pool-name* – 指定地址池的名称。

执行该命令后，系统创建指定名称的地址池，并且进入SSL VPN地址池配置模式；如果指定的名称已存在，则直接进入SSL VPN地址池配置模式。在全局配置模式下，使用该命令no的形式删除指定的SSL VPN地址池：

no scvpn pool *pool-name*

在SSL VPN地址池配置模式下可进行如下配置：

- 配置地址池地址范围和网络掩码
- 配置保留地址池
- 配置IP地址绑定规则
- 配置DNS服务器
- 配置WINS服务器

配置地址池地址范围

为地址池配置地址范围和网络掩码，在SSL VPN地址池配置模式下使用以下命令：

address *start-ip end-ip* **netmask** *A.B.C.D*

- *start-ip* – 指定IP范围的起始IP地址。
- *end-ip* – 指定IP范围的结束IP地址。
- **netmask** *A.B.C.D* – 指定地址池IP范围的网络掩码。

在SSL VPN地址池配置模式下使用该命令no的形式删除配置的IP地址范围：

no address

配置保留地址池

保留地址池中的IP地址为地址池中的部分IP地址，当SSL VPN设备端从地址池里取出IP地址分配给客户端时，需要保留已经被占用的部分IP地址（如网关、FTP服务器等），不进行分配。配置保留地址池，在SSL VPN地址池配置模式下使用以下命令：

exclude address *start-ip end-ip*

- *start-ip* – 指定保留地址池的起始IP地址。
- *end-ip* – 指定保留地址池的结束IP地址。

在SSL VPN地址池配置模式下使用该命令no的形式取消保留地址池的配置：

no exclude

配置IP地址绑定规则

Hillstone设备SSL VPN通过创建和执行IP地址绑定规则来满足客户端的固定IP地址需求。IP地址绑定规则包括IP用户绑定规则和IP角色绑定规则。IP用户绑定规则将客户端用户与已配置地址池中的某个固定IP地址绑定，当客户端连接成功后，设备端会将绑定的IP地址分配给客户端；IP角色绑定规则是将角色与已配置地址池中的某一IP地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个IP地址分配给客户端。

当SSL VPN设备端通过地址池给客户端分配IP地址时，系统会按照一定的顺序对客户端的IP地址绑定规则进行检查，决定如何为客户端分配IP地址：

1. 检查是否已为客户端用户配置IP用户绑定规则，如果是，则将绑定的IP地址分配给客户端；否则，需要进一步检查。注意，如果此IP用户绑定规则中的IP地址已被占用，则该用户无法登录。

2. 检查是否已为客户端用户配置IP角色绑定规则，如果是，则从绑定的地址范围中取出一个IP地址分配给客户端；否则，在未绑定的IP地址范围中取出一个IP地址分配给客户端。注意，如果绑定的地址范围中的地址都已经被分配，则该用户无法登录。

注意: IP用户绑定规则中的IP地址和IP角色绑定规则中的IP地址不能重叠。

配置IP用户绑定规则

配置IP用户绑定规则，在SSL VPN地址池配置模式下使用以下命令：

ip-binding user *user-name* **ip** *ip-address*

- **user** *user-name* – 指定客户端用户名。
- **ip** *ip-address* – 指定绑定的IP地址。此地址必须为地址池中可以分配的地址。

在SSL VPN地址池配置模式下使用该命令no的形式取消对特定用户IP用户绑定规则的配置：

no ip-binding user *user-name*

配置IP角色绑定规则

配置IP角色绑定规则，在SSL VPN地址池配置模式下使用以下命令：

ip-binding role *role-name* **ip-range** *start-ip end-ip*

- **role** *role -name* – 指定角色名称。
- **ip-range** *start-ip end-ip* – 指定绑定的IP范围的起始IP地址**start-ip**和结束IP地址**end-ip**。此地址范围必须为地址池中可以分配的地址范围。

在SSL VPN地址池配置模式下使用该命令no的形式取消对特定角色的IP角色绑定规则的配置：

no ip-binding role *role-name*

修改IP角色绑定规则排列顺序

一个用户可以绑定到一个或者多个角色，不同角色可以配置不同的IP角色绑定规则。对于绑定到多个角色且多个角色有相应的IP角色绑定规则的用户，Hillstone设备会对IP角色绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。默认情况下，系统会将新创建的规则

放到所有规则的末尾，管理员可以移动已有的IP角色绑定规则从而改变规则的排列顺序。改变规则的排列顺序，在SSL VPN地址池配置模式下使用以下命令：

move *role-name1* {**before** *role-name2* | **after** *role-name2*| **top** | **bottom**}

- *role -name1* – 指定被移动的IP角色绑定规则的角色名称。
- **before** *role-name2* – 将IP角色绑定规则移动到某个IP角色绑定规则(角色名称为role-name2的规则)之前。
- **after** *role-name2* – 将IP角色绑定规则移动到某个IP角色绑定规则(角色名称为role-name2的规则)之后。
- **top** – 将IP角色绑定规则移动到所有IP角色绑定规则之首。
- **bottom** – 将IP角色绑定规则移动到所有IP角色绑定规则的末尾。

配置DNS服务器

配置DNS服务器，在SSL VPN地址池配置模式下使用以下命令：

dns *address1* [*address2*] [*address3*] [*address4*]

- *address1* – 指定DNS服务器IP地址。用户最多可配置4个DNS服务器。

在SSL VPN地址池配置模式下使用该命令no的形式取消对DNS服务器的指定：

no dns

配置WINS服务器

配置WINS服务器，在SSL VPN地址池配置模式下使用以下命令：

wins *address1* [*address2*]

- *address1* – 指定WINS服务器IP地址。用户最多可配置两个WINS服务器。

在SSL VPN地址池配置模式下使用该命令no的形式取消对WINS服务器的指定：

no wins

显示SSL VPN地址池信息

显示SSL VPN地址池信息，在任何模式下使用以下命令：

show scvpn pool [*pool-name*]

- *pool-name* – 指定SSL VPN地址池名称以显示指定的地址池信息。如果不指定该参数值，系统将显示所有已配置的SSL VPN地址池信息。

以下是显示SSL VPN地址池具体信息的命令示例：

```
hostname(config)# show scvpn pool pool_test1
Name: pool_test1
Address range: 3.3.3.1 - 3.3.3.10 （地址池IP地址范围）
Exclude range: 3.3.3.1 - 3.3.3.2 （保留地址池地址范围）
Netmask: 255.255.255.0 （地址池网络掩码）
Wins server: （WINS服务器信息）
wins1: 10.1.1.1
Dns server:  （DNS服务器信息）
dns1: 10.10.209.1
IP Binding User: （IP用户绑定信息）
test 3.3.3.8
IP Binding Role: （IP角色绑定信息）
role1 3.3.3.3 3.3.3.7
```

显示SSL VPN地址池统计信息，在任何模式下使用以下命令：

show scvpn pool *pool-name* **statistics**

- *pool-name* – 指定SSL VPN地址池名称以显示指定的地址池统计信息。

以下是显示SSL VPN地址池统计信息的命令示例：

```
hostname(config)# show scvpn pool pool_test1 statistics
Total Ip Num 10 （地址池中IP地址总数）
Exclude Ip Num 2 （保留IP地址个数）
Fixed Ip Num 6 （绑定IP地址个数）
Used Ip Num 2 （已分配IP地址个数）
```

```
Fixed Used Ip Num 0 （已分配绑定IP地址个数）
Free Ip Num 6 （可用地址个数）
```

资源列表配置

资源列表是指系统中配置的用户可便捷访问的资源，其中每个资源又包含多个资源条目。资源条目的展现形式为“资源条目名称+对应的URL“。SSL VPN用户登录认证通过后，认证服务器将该用户所属的用户组信息发送给SSL VPN服务器，然后服务器会根据配置的SSL VPN实例中用户组和资源的绑定关系，把该用户可访问的内网资源列表发送给SSL VPN客户端，客户端对接收到的资源列表信息进行分析并展示在用户系统自带的IE浏览器弹出的页面中，用户可以通过点击URL链接直接访问内网资源。需要注意的是，该资源列表页面只在认证通过后显示一次。如果登录的用户不属于任何用户组，认证成功后浏览器不会弹出资源列表页面。

配置SSL VPN资源，在全局配置模式下，使用以下命令：

scvpn resource-list *list-name*

- *list-name* –指定资源的名称。取值范围是1到31个字符。

执行该命令后，系统进入SSL VPN资源列表配置模式，用户可以继续为该新建资源配置资源条目。在全局配置模式下，使用该命令no的形式删除指定的资源：

no resource-list *list-name*

提示:

- 配置的资源数目不能超过48。
- SSL VPN的资源列表功能仅适用于Windows的SSL VPN客户端。

添加资源条目

每个资源中可以添加的资源条目数量为0~48。所有资源中包含的资源条目的总数不能超过48条。在SSL VPN资源列表配置模式下，为新建资源添加资源条目：

name *name* **url** *url-string*

- *name* –指定资源条目的名称。取值范围是1到63个字符。
- *url-string* –指定资源条目所对应的URL。取值范围是1到255个字符。

在SSL VPN资源列表配置模式下，使用以下命令删除指定的资源条目：

no name *name*

查看资源列表

用户可以在任何模式下，使用以下命令查看资源列表的配置信息：

show scvpn resource-list [*list-name*]

- *list-name* –指定要查看的资源的名称。取值范围是1到31个字符。如果不指定该参数，则显示所有资源的配置信息。

UDP端口号配置

配置SSL VPN连接采用的UDP端口号，在全局配置模式下，使用以下命令：

scvpn-udp-port *port-number*

- *port-number* –指定UDP端口号。默认值是4433。取值范围是1到65535。

执行该命令后，所有配置的SSL VPN实例均采用此UDP端口号进行数据连接。

在全局配置模式下使用该命令no的形式恢复默认UDP端口号：

no scvpn-udp-port

配置空闲时间

空闲时间指客户端与设备端在无流量状态下能够保持连接状态的最长时间，超出空闲时间后，设备端将断开与客户端的连接。

默认情况下，空闲时间为30分钟。配置设备的空闲时间，请在SCVPN隧道配置模式下，使用以下命令：

idle-time *time*

- *time*– 指定设备的空闲时间，单位为分钟，取值范围是1到1500分钟。

使用**no idle-time**命令删除设备的空闲时间。

SSL VPN实例配置

创建SSL VPN实例，在全局配置模式下，使用以下命令：

tunnel scvpn *instance-name*

- *instance-name* – 指定SSL VPN实例的名称。

执行该命令后，系统创建指定名称的SSL VPN实例，并且进入SSL VPN实例配置模式；如果指定的名称已存在，则直接进入SSL VPN实例配置模式。在全局配置模式下，使用该命令no的形式删除指定的SSL VPN实例：

no tunnel scvpn *instance-name*

在SSL VPN实例配置模式下，用户可以进行如下配置：

- 指定地址池
- 指定设备端接口
- 指定SSL协议
- 指定PKI信任域
- 指定隧道密码
- 指定AAA服务器
- 指定HTTPS端口号
- 配置防重放功能
- 配置分片功能
- 配置空闲时间
- 配置用户同名登录功能
- 配置URL重定向功能
- 配置SSL VPN隧道路由
- 启用/禁用清除SSL VPN桌面版客户端缓存数据功能
- 在HA Peer模式中使用SSL VPN

- 绑定L2TP VPN实例
- 绑定资源

指定地址池

为SSL VPN实例指定SSL VPN地址池，在SSL VPN实例配置模式下，使用以下命令：

pool *pool-name*

- *pool-name* – 指定已配置的SSL VPN地址池名称。

在SSL VPN实例配置模式下使用该命令no的形式取消地址池的指定：

no pool

指定设备端接口

客户端通过HTTPS协议访问设备端接口。指定设备端SSL VPN接口，在SSL VPN实例配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定设备端接口的名称。

在SSL VPN实例配置模式下使用该命令no的形式取消设备端接口的配置：

no interface *interface-name*

指定SSL协议

为SSL VPN指定SSL协议，在SSL VPN实例配置模式下，使用以下命令：

ssl-protocol {**sslv3** | **tlsv1** | **tlsv1.2** | **gmsslv1.0** | **any**}

- **sslv3** – 指定使用SSLv3协议。
- **tlsv1** – 指定使用TLSv1协议。
- **tlsv1.2** – 指定使用TLSv1.2协议。
- **gmsslv1.0** – 指定使用国密GMSSLv1.0协议。当协议为此选项时，PKI信任域和加密信任域必须选择配置含有SM2类型密钥的信任域，加密算法建议优先选择SM4，Hash算法建议优先选择SM3.

- **any** – 指定使用SSLv2、SSLv3、TLSv1、TLSv1.1或者TLSv1.2任何一种协议。此为系统默认设置。

在SSL VPN实例配置模式下使用该命令no的形式恢复SSL协议的默认值：

no ssl-protocol

如果设备端指定的SSL协议类型为tlsv1.2或者any，在SSL VPN客户端进行数字证书认证前，需要用户将要导入到浏览器中的软证书或者USB Key中的.pfx格式证书进行处理，使得证书能够支持tlsv1.2协议，以便用户在使用“用户名/密码+数字证书”或者“数字证书”认证方式进行认证时，能够连接成功。处理证书前，请先准备一台安装了OpenSSL1.0.1版本及以上的PC（Windows或Linux系统均可）。以文件名称为oldcert.pfx的证书为例，处理步骤如下：

1. 在OpenSSL软件界面中，输入以下命令将.pfx格式的证书转换为.pem格式的证书。
   `openssl pkcs12 -in oldcert.pfx -out cert.pem`
2. 继续输入下面的命令将.pem格式的证书转换为支持tlsv1.2的.pfx格式证书。`openssl pkcs12 -export -in cert.pem -out newcert.pfx -CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"`
3. 将新生成的.pfx格式证书导入到浏览器或者USB Key。

上述操作完成后，请使用1.4.6.1239及以上版本的SSL VPN客户端进行登录。当配置使用国密标准的SSL VPN功能时，PC端需安装支持国密标准的SSL VPN客户端（当前支持国密标准的Windows客户端版本为1.4.7.1252），并且使用“国密SSL”相关登录模式进行登录。

指定PKI信任域

此处指定的PKI信任域用于HTTPS访问认证。为SSL VPN指定PKI信任域，在SSL VPN实例配置模式下，使用以下命令：

trust-domain *trust-domain-name*

- *trust-domain-name* – 指定系统中已配置的PKI信任域的名称。默认信任域为trust_domain_default。

在SSL VPN实例配置模式下使用该命令no的形式恢复信任域的默认配置：

no trust-domain

提示: 关于如何创建PKI信任域，请参阅《用户认证》的“PKI配置”部分。

指定加密信任域

此处为SSL VPN指定加密信任域，加密信任域用于国密SSL协商。在SSL VPN实例配置模式下，使用以下命令：

trust-domain-enc *enc-cert*

- *enc-cert* – 指定系统预定义的用于国密SSL协商的加密信任域的名称。

在SSL VPN实例配置模式下使用该命令no的形式删除加密信任域的配置：

no trust-domain-enc

指定隧道密码

隧道密码包括加密算法和验证算法。为SSL VPN指定隧道密码，在SSL VPN实例配置模式下，使用以下命令：

tunnel-cipher encryption {**null** | **des** | **3des** | **aes** | **aes192** | **aes256** | **sm4**} **hash** {**null** | **md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3**} [**compression defl**]

- **null** | **des** | **3des** | **aes** | **aes192** | **aes256** | **sm4** – 指定加密算法。默认加密算法为3des。null表示不使用加密功能。关于加密算法的详细描述，请参阅“加密算法”。
- **null** | **md5** | **sha** | **sha256** | **sha384** | **sha512**| **sm3** – 指定验证算法。默认验证算法为sha。null表示不使用验证功能。关于验证算法的详细描述，请参阅“验证算法”。
- **compression defl** – 指定DEFLATE压缩算法。默认无压缩算法。关于压缩算法的详细描述，请参阅“压缩算法”。

在SSL VPN实例配置模式下使用该命令no的形式恢复加密算法和验证算法的默认值并取消压缩算法的配置：

no tunnel-cipher

指定AAA服务器

此处指定的AAA服务器为进行客户端用户身份认证的AAA服务器。指定AAA服务器，在SSL VPN实例配置模式下，使用以下命令：

aaa-server *aaa-server-name* [**domain** *domain-name*] [**keep-domain-name**]

- aaa-server-name – 指定AAA服务器的名称。
- **domain** *domain-name* – 为AAA服务器指定域名以区分不同的AAA服务器。
- **keep-domain-name** – 指定该参数后， 用于身份认证的用户名将验证域名。

在SSL VPN实例配置模式下使用该命令no的形式取消对AAA服务器的指定：

no aaa-server *aaa-server-name* [**domain** *domain-name*]

指定HTTPS端口号

HTTPS端口号用于客户端访问设备端时使用。指定HTTPS端口号，在SSL VPN实例配置模式下，使用以下命令：

https-port *port-number*

- *port-number* – 指定HTTPS端口号。默认值是4433。取值范围是1到65535。为避免与WebUI使用的HTTPS端口号相冲突，建议用户不要把HTTPS端口号设置为443。绑定到同一个接口的SSL VPN实例需配置不同的HTTPS端口号。

在SSL VPN实例配置模式下使用该命令no的形式恢复默认HTTPS端口号：

no https-port

配置SSL VPN隧道路由

SSL VPN隧道路由是指通过SSL VPN隧道到指定网段/域名的路由。SSL VPN客户端接收到指定网段后，生成到达指定网段的路由条目；接收到指定域名后，根据域名解析结果，生成到达域名所在地址的路由条目。

指定网段

使用网段方式配置SSL VPN隧道路由，在SSL VPN实例配置模式下，使用以下命令：

split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

- *ip-address/netmask* – 指定目的地址和掩码。
- **metric** *metric-number* – 指定路由的度量值。默认值是35。取值范围是1到9999。

用户可以配置多条该命令添加多条路由。

在SSL VPN实例配置模式下使用该命令no的形式删除指定的路由：

no split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

指定域名

使用域名方式配置SSL VPN隧道路由后，系统将域名下发给客户端。客户端根据域名解析结果，生成到达域名所在地址的路由条目。指定域名，在SSL VPN实例配置模式下，使用以下命令：

domain-route {**disable** | **enable** | **max-entries** *value* | *url*]

- **disable** – 不下发域名到客户端。此为系统默认设置。
- **enable** – 下发域名到客户端。
- **max-entries** *value* – 指定客户端可以根据域名解析后地址所生成的最大路由条目数。默认值是1000，取值范围是1到10000。
- *url* – 指定域名。每次可添加一个，支持最多64个域名。每个域名的字符串长度不得超过63个字符。域名末尾不能为“.”，不支持通配符，且不支持过于宽泛的URL，比如：“.-com”、“com”。

在SSL VPN实例配置模式下使用该命令no的形式删除指定的路由：

no domain-route *url*

配置防重放功能

防重放（anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。配置防重放功能，在SSL VPN实例配置模式下，使用以下命令：

anti-replay {**32** | **64** | **128** | **256** | **512**}

- **32** – 指定防重放的窗口为32。该数值为系统的默认数值。
- **64** – 指定防重放的窗口为64。

- **128** – 指定防重放的窗口为128。
- **256** – 指定防重放的窗口为256。
- **512** – 指定防重放的窗口为512。

在网络状况较差时，例如存在严重乱序现象等，请选择较大的窗口。

在SSL VPN实例配置模式下使用该命令no的形式恢复默认防重放窗口：

no anti-replay

配置分片功能

用户可以指定是否允许转发设备将包进行分片处理。配置分片功能，在SSL VPN实例配置模式下，使用以下命令：

df-bit {**copy** | **clear** | **set**}

- **copy** – 直接从发包端拷贝IP包的DF选项。该选项为系统默认选项。
- **clear** – 允许转发设备对包做分片处理。
- **set** – 不允许转发设备对包做分片处理。

在SSL VPN实例配置模式下使用该命令no的形式恢复系统的默认设置：

no df-bit

配置空闲时间

空闲时间指客户端与设备端在无流量状态下能够保持连接状态的最长时间，超出空闲时间后，设备端将断开与客户端的连接。配置空闲时间，在SSL VPN实例配置模式下，使用以下命令：

idle-time *time-value*

- *time-value* – 指定空闲时间，单位为分钟。默认值是30分钟。取值范围是15到1500分钟。

在SSL VPN实例配置模式下使用该命令no的形式恢复空闲时间的默认值：

no idle-time

配置用户同名登录功能

用户同名登录功能指允许同一个用户在多个地点同时登录认证。开启用户同名登录功能，在SSL VPN实例配置模式下，使用以下命令：

allow-multi-logon

执行该命令后，开启用户同名登录功能，并且不对同一用户名的登录次数做限制。用户可以在SSL VPN实例配置模式下通过使用以下命令指定用户同名登录次数：

allow-multi-logon number *number*

- *number* – 指定用户同名登录次数。范围是1到99999999。

在SSL VPN实例配置模式下使用以下命令no的形式关闭用户同名登录功能：

no allow-multi-logon

配置URL重定向功能

URL重定向功能是指在SSL VPN设备端配置重定向的URL，客户端认证成功后将自动跳转到指定URL的页面。默认情况下，URL重定向功能是关闭的。配置URL重定向功能，在SSL VPN实例配置模式下，使用以下命令：

redirect-url *url* **title-en** *name* **title-zh** *name*

- *url* – 指定认证成功后，客户端自动跳转页面的URL，取值范围为1到255字节。系统支持HTTP（http://）和HTTPS（https://）两种类型的URL。
- **title-en** *name* – 指定重定向URL的英文描述，范围为1到31字节。当客户端PC为英文操作系统时，该名称会在客户端菜单项中显示。
- **title-zh** *name* – 指定重定向URL的中文描述，范围为1到63字节。当客户端PC为中文操作系统时，该名称会在客户端菜单项中显示。建议选用支持中文输入的超级终端，当超级终端不支持中文输入时，请通过WebUI配置该参数。

在SSL VPN实例配置模式下使用该命令no的形式取消URL重定向功能：

no redirect-url

URL内容格式

根据重定向页面类型的不同，StoneOS支持内容符合下列格式的URL输入，以HTTP类型URL为例：

- UTF-8编码格式的页面：输入“URL”+“username=$USER&password=$PWD”。比如，“http://www.abc.com/oa/login.do?username=$USER&password=$PWD”
- GB2312编码格式的页面：输入“URL”+“username=$GBUSER&password=$PWD”。比如，“http://www.abc.com/oa/login.do?username=$GBUSER&password=$PWD”
- 其它页面：直接输入URL。比如，http://www.abc.com

注意: 关于URL重定向功能的具体实例，请参阅“URL重定向配置举例”。

配置SSL VPN隧道路由

SSL VPN隧道路由是指通过SSL VPN隧道到指定网段的路由。SSL VPN客户端通过设备下发的路由可以访问到指定的网段。配置SSL VPN隧道路由，在SSL VPN实例配置模式下，使用以下命令：

split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

- *ip-address/netmask* – 指定目的地址和掩码。
- **metric** *metric-number* – 指定路由的度量值。默认值是35。取值范围是1到9999。
- 用户可以配置多条该命令添加多条路由。

在SSL VPN实例配置模式下使用该命令no的形式删除指定的路由：

no split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

启用/禁用清除SSL VPN桌面版客户端主机缓存数据功能

为了保证用户SSL VPN桌面版客户端主机的隐私数据安全性，用户可以在SSL VPN桌面版客户端断开后，启用清除桌面版客户端主机缓存数据功能，清除浏览器缓存、临时文件等隐私数据。启用/禁用清除桌面版客户端主机缓存数据功能，在SSL VPN实例配置模式下，使用以下命令：

- 启用：**host-cache-clear enable**
- 禁用：**host-cache-clear disable**

在HA Peer模式中使用SSL VPN

在HA Peer模式的网络环境中，分别在两台设备上配置正确有效的SSL VPN。当一台主设备或者其上下链路出现故障时，SSL VPN客户端可以重新连接到另外一台主设备。用户需要指定重连地址列表。SSL VPN客户端将根据重连地址列表中地址的优先级进行重连。若重连失败，将会循环尝试列表中的地址，直到连接成功。用户可最多指定四个重连地址。四个重连地址按配置先后顺序进行优先级排列。先配置的重连地址具有较高优先级。配置重连地址列表，在SSL VPN实例配置模式下，使用如下命令：

cluster { **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]]

- **ip** *A.B.C.D* | **domain** *url* – 指定用于SSL VPN连接的服务器IP地址或者域名。
- **port** *port-number* – 指定用于SSL VPN连接的端口号。默认值是4433。

使用**no cluster**命令清除以上配置。

在使用此功能时，需要注意以下事项：

- 当SSL VPN客户端选择<自动重连>选项且用户通过client-auto-connect count命令在服务器端设置自动重连次数为unlimited时，SSL VPN客户端将连接之前指定的连接地址，不会连接重连地址列表中的地址；当用户通过命令设置自动重连次数为X次时，SSL VPN客户端将在X次连续重连失败后，使用重连地址列表中的地址进行重连。
- 当SSL VPN客户端不选择<自动重连>选项时，无论服务器端的配置如何，SSL VPN客户端将直接使用地址重连列表中的地址进行重连。
- 当使用支持此功能的系统固件时，如果服务器端没有配置重连地址列表，低于1.4.4.1207版本的SSL VPN客户端可正常连接SSL VPN服务器端。StoneOS会提示用户存在新版本的SSL VPN客户端。如果服务器端配置重连地址列表，当低于1.4.4.1207版本的SSL VPN客户端连接SSL VPN服务器端时，StoneOS会提示用户进行升级。用户需要手动卸载旧版本的SSL VPN客户端，然后登陆SSL VPN的Web登陆界面进行SSL VPN客户端的下载与安装。新版本的SSL VPN客户端可与不支持此功能的系统固件兼容。

绑定L2TP VPN实例

在使用iOS的SSL VPN客户端与SSL VPN服务器进行连接时，需要为SSL VPN实例绑定L2TP VPN实例且此实例需引用IPSec隧道。进行绑定配置，在SSL VPN实例配置模式下，使用以下命令：

client-bind-lns *tunnel-name*

- *tunnel-name* – 指定系统中已配置的L2TP VPN实例。此实例需要引用IPSec隧道。使用该命令no的形式取消绑定配置：**no client-bind-lns**
- 对于绑定的L2TP VPN实例和引用的IPSec隧道，需要满足如下条件：
  - IPSec隧道的认证方式需要使用预共享密钥认证。
  - L2TP实例的隧道密码（通过secret secret-string指定）需要与IPSec隧道的预共享密钥一致。
  - L2TP实例与SSL VPN实例指定的AAA服务器需要一致。
  - L2TP实例的地址池需要正确配置，设备根据L2TP实例的地址池为iOS的SSL VPN客户端下发相关地址。

绑定资源

配置资源和用户组的绑定关系后，SSL VPN客户端才能在用户认证成功后将其可访问的资源列表显示在IE浏览器的页面中。一个用户组可以绑定多个资源，一个资源也可以绑定多个用户组。一个SSL VPN实例中最多可以配置32个绑定条目。

配置资源和用户组的绑定条目，在SSL VPN实例配置模式下，使用以下命令：

bind resource-list *list-name* **user-group** *aaa-server-name group-name*

- *list-name* –指定资源的名称。取值范围是1到31个字符。
- *aaa-server-name* –指定用户组所属的认证服务器的名称。目前仅支持本地认证服务器和RADIUS认证服务器。
- *group-name* –指定用户组的名称。

在SSL VPN实例配置模式下，使用以下命令可以取消指定的资源和用户组的绑定关系：

no bind resource-list *list-name* **user-group** *aaa-server-name group-name*

绑定SSL VPN实例到隧道接口

配置好的SSL VPN实例需要绑定到隧道接口，才能够生效。绑定SSL VPN实例到隧道接口，在隧道接口配置模式下，使用以下命令：

tunnel scvpn *instance-name*

- *instance-name* – 指定系统中已配置的SSL VPN实例的名称。

在隧道接口配置模式下使用该命令no的形式取消隧道接口与SSL VPN实例的绑定：

no tunnel scvpn *instance-name*

配置客户端USB Key证书认证

Hillstone设备支持客户端USB Key证书认证。只要用户持有的USB Key支持标准的Windows SDK（Certificate Store Functions），并且存储合法的证书，就能通过认证进而实现网络连通的目的。

USB Key证书认证功能支持以下两种认证方式：

- 用户名/密码 + USB Key：SSL VPN用户需要持有存储正确数字证书的USB Key，并且在登录时输入正确的用户名、密码和USB Key用户口令，才能通过认证；
- 只用USB Key：SSL VPN用户需要持有存储正确数字证书的USB Key，并且在登录时输入正确的USB Key用户口令，即可通过认证，无需输入用户名和密码。

注意: 当认证方式为“只用USB Key”时，

- 系统可以根据USB Key数字证书中的证书名称（证书CN字段）或者组织机构（证书OU字段）为认证成功的用户映射相应的角色。关于如何进行证书名称或者组织机构的角色映射，请参阅《系统管理》“配置角色映射规则”部分。
- 系统不支持允许本地用户修改密码。
- 系统不支持配置短信口令认证功能。
- 如果移除USB Key，客户端不会自动重连。

实现USB Key证书认证功能，用户需在设备端配置以下功能：

- 开启USB Key证书认证功能
- 导入USB Key证书相应CA证书到信任域
- 配置USB Key证书相应CA证书的信任域

开启USB Key证书认证功能

默认情况下，设备端的USB Key证书认证功能为关闭状态，用户可以在SSL VPN实例配置模式下使用以下命令开启USB Key证书认证功能：

client-cert-authentication [**usbkey-only**]

- **usbkey-only** – 指定USB Key证书认证方式为“只用USB Key”。如不指定该参数，认证方式为“用户名/密码 + USB Key”。

在SSL VPN实例配置模式下使用该命令no的形式关闭USB Key证书认证功能：

no client-cert-authentication [**usbkey-only**]

导入USB Key证书相应CA证书到信任域

用户可以通过多种方式（FTP、TFTP和USB）实现CA证书到信任域的导入。在执行模式下使用以下命令：

import pki *trust-domain-name* **cacert from** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- *trust-domain-name* – 指定PKI信任域的名称。
- **ftp server ip-address** [**user** *user-name* **password** *password*] – 指定FTP服务器的IP地址以及访问服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。
- **tftp server** *ip-address* – 指定TFTP服务器的IP地址。
- **usb0 | usb1** – 指定通过USB方式从usb0或者usb1插槽所对应的U盘根目录导入CA证书。
- *file-name* – 指定要导入的CA证书的文件名。

配置USB Key证书相应CA证书的信任域

设备端开启客户端USB Key证书认证功能后，还需要指定用户证书相应的CA（Certification Authority）的信任域。客户端所提交的证书匹配到其中任意一个信任域的CA证书，都会认证成功。在SSL VPN实例配置模式下，使用以下命令：

client-auth-trust-domain *trust-domain*

- *trust-domain* – 指定CA证书所在的PKI信任域，该信任域需已经创建。

如果需要配置多个信任域，需重复使用本命令。系统最多可以支持10个信任域。

在SSL VPN实例配置模式下使用该命令no的形式取消对PKI信任域的指定：

no client-auth-trust-domain *trust-domain*

提示: 关于如何创建PKI信任域，请参阅《用户认证》的“PKI配置”部分。

配置短信口令认证功能

短信口令认证功能是指SSL VPN用户使用用户名和密码登录时，收到登录请求的Hillstone设备通过短信猫或短信网关自动向该用户的手机号码发送一条包含随机认证码的短信，用户输入收到的认证码后，才可以通过认证，进而访问内网资源。

注意: Hillstone设备的部分平台支持短信口令认证功能。

短信猫认证

Hillstone设备采用外置GSM短信猫或CDMA短信猫。配置短信口令认证功能前，请准备一张手机SIM卡和一个GSM短信猫或CDMA短信猫，并将短信猫正确连接到网关设备上。连接短信猫和Hillstone设备，首先，将SIM卡正确插入短信猫内；然后，通过USB数据线将短信猫与Hillstone设备的USB接口连接起来。我们推荐用户使用以下两种型号的短信猫：

型号	类型	芯片	接口
华腾通宇GSM MODEM	GSM	WAVECOM	USB接口

型号	类型	芯片	接口
金笛GSM MODEM	GSM	WAVECOM	USB接口
金笛CDMA MODEM	CDMA	WAVECOM	USB接口

短信口令认证功能的设备端配置包括：

- 开启/关闭短信口令认证功能
- 设置短信认证手机号码
- 配置短信认证码有效时间
- 配置短信最大发送数量
- 发送测试短信

开启/关闭短信口令认证功能

默认情况下，系统的短信口令认证功能为关闭状态。开启/关闭短信口令认证功能，在SSL VPN实例配置模式下，使用以下命令：

- 开启：**`sms-auth enable`**
- 关闭：**`sms-auth disable`**

设置短信认证手机号码

SSL VPN本地用户和AD用户均可使用短信口令认证功能。管理员可以为每个本地用户和AD用户设置一个手机号码。开启短信口令认证功能后，系统会向已指定的登录用户手机号码发送认证码短信。

为本地用户设置手机号码，在用户配置模式下，使用以下命令：

`phone` *`phone-number`*

- *`phone-number`* – 指定本地用户手机号码。

在用户配置模式下使用该命令no的形式取消用户手机号码的指定：

`no phone`

为AD用户设置手机号码，需要在AD服务器的“mobile”属性中配置手机号码。

配置短信认证码有效时间

每条短信认证码都有一个有效时间，如果用户在有效时间内没有输入短信认证码也没有重新申请认证码，SSL VPN设备端将自动断开连接。配置短信认证码有效时间，在SSL VPN实例配置模式下，使用以下命令：

sms-auth expiration *expiration*

- *expiration* – 指定短信认证码有效时间。默认为10分钟，范围为1-10分钟。

在SSL VPN实例配置模式下使用该命令no的形式恢复系统默认有效时间：

no sms-auth expiration

配置短信最大发送数量

管理员可以配置短信猫每小时或者每天最多发送的短信数量。对超出数量限制的短信，系统将自动丢弃并记录日志信息。配置短信最大发送数量，在全局配置模式下，使用以下命令：

sms modem {**num-per-hour** | **num-per-day**} *number*

- {**num-per-hour** | **num-per-day**} *number* – 指定短信猫每小时（**num-per-hour**）或者每天（**num-per-day**）最多发送的短信数量。范围为1-1000条。

在全局配置模式下使用该命令no的形式不限制短信最大发送数量：

no sms modem {**num-per-hour** | **num-per-day**}

发送测试短信

为验证设备能否正常发送短信，管理员可以向指定手机号码发送测试短信。发送测试短信，在任意模式下，使用以下命令：

exec sms send test-message to *phone-number*

- *phone-number* – 指定接收测试短信的手机号码。

如果测试短信发送成功，指定手机号码会收到系统发送的测试短信；如果测试短信发送失败，系统会记录日志并描述失败原因。

显示短信猫配置信息

在任意模式下，使用以下命令查看短信猫的配置信息，包括存在状态和短信最大发送数量：

show sms modem

短信网关认证

Hillstone安全设备可通过运营商的短信网关或者其代理服务器向用户发送短消息。配置该功能前，用户需先向运营商索要短信网关的地址、发送短消息的设备ID等相关信息。

短信网关认证的配置包括：

1. 创建Service Provider（SP）实例，并根据需要，配置SP实例。
2. 绑定SP实例到已创建的SSL VPN隧道，开启短信口令认证功能。

创建SP实例名称

创建SP实例，在全局配置模式下，使用以下命令：

sms service-provider *sp-name* [**protocol sgip** | **ums**]

- *sp-name* - 指定SP实例的名称，取值范围为1至31个字符。
- **protocol sgip | ums** - 指定SP实例运行的短信网关协议。sgip表示联通的SGIP协议，ums表示使用联通企业信息平台。

执行该命令后，系统创建指定名称的SP实例，并且进入SP实例配置模式；如果指定的名称已存在，则直接进入SP实例配置模式。对于每种协议类型的SP实例，系统最多允许配置8个SP实例。

在全局配置模式下，使用该命令no的形式删除指定的SP实例：

no sms service-provider *instance-name* [**protocol sgip**]

在SP实例配置模式下，用户可以进行如下配置：

- 设置发送认证短信的号码
- 指定设备ID
- 指定短信网关的地址
- 指定VRouter

- 指定用户名和登录密码
- 指定短信最大发送数量

设置发送认证短信的号码

开启短信口令认证功能后，系统会向已指定的用户手机号码发送认证码短信。在SP实例配置模式下，使用以下命令设置手机号码：

source-number *phone-number*

- *phone-number* – 指定用户的手机号码，取值范围为1至21个字符。

在SP实例配置模式下使用该命令no的形式取消用户手机号码的指定：

no source-number

指定设备ID

配置短信网关前，用户需向运营商索取允许发送短信的设备ID。在SP实例配置模式下，使用以下命令在设备端指定ID：

device-code *code-number*

- *code-number* - 指定设备的ID，取值范围为1至4294967295。

在SP实例配置模式下使用该命令no的形式取消ID号码的指定：

no device-code

指定短信网关的地址和端口号

指定短信网关的地址和端口号，在SP实例配置模式下，使用以下命令：

gateway {**host** *hostname* | **ip** *ip-address*} [**port** *port-number*]

- **host** *hostname* - 指定短信网关的主机名称，名称范围为1至31个字符。
- **ip** *ip-address* - 指定短信网关的IP地址。
- **port** *port-number* - 指定短信网关的端口号。当协议类型指定为“SGIP”时，默认端口号为8801；当协议类型指定为“UMS”时，默认端口号为9600。

多次执行此命令，最新一次执行的命令生效。

在SP实例配置模式下使用该命令no的形式删除短信网关的地址和端口号：

no gateway {**host** *hostname* | **ip** *ip-address*}

指定VRouter

系统有一个默认VRouter，即trust-vr，同时系统支持多VR。指定SP所属的VRouter，在SP实例配置模式下，使用以下命令：

vrouter {**trust-vr** | *vr-name*}

- **trust-vr** - 指定SP所属VR为默认VR。
- *vr-name* – 指定已创建的VR名称。

在SP实例配置模式下使用该命令no的形式恢复为默认VR：

no vrouter {**trust-vr** | *vr-name*}

指定用户名和密码

指定登录短信网关的用户名称及密码，在SP实例配置模式下，使用以下命令：

user *username***password** *password*

- *username* –指定登录短信网关的用户名称，名称范围是1至64个字符。
- *password* – 指定登录密码，取值范围为1至64个字符。

在SP实例配置模式下使用该命令no的形式取消用户名和密码的指定：

no user *username***password** *password*

配置短信最大发送数量

管理员可以配置短信网关每小时或者每天最多发送的短信数量。对超出数量限制的短信，系统将自动丢弃并记录日志信息。配置短信最大发送数量，在SP实例配置模式下，使用以下命令：

{**num-per-hour** | **num-per-day**} *number*

- *number* – 指定短信网关每小时（**num-per-hour**）或者每天（**num-per-day**）最多发送的短信数量。范围为0-65535条。

在SP实例配置模式下使用该命令no的形式取消短信最大发送数量的指定：

no {**num-per-hour** | **num-per-day**}

指定UMS协议类型

指定UMS协议类型，在SP实例配置模式下，使用以下命令：

protocol {**http** | **https**}

- **http** – 指定UMS协议类型为HTTP。
- **https** – 指定UMS协议类型为HTTPS。

在SP实例配置模式下使用该命令no的形式恢复默认UMS协议类型HTTPS：

no protocol

指定企业编码

当SP实例使用UMS协议类型时，用户可以指定在UMS平台上注册的企业编码，在SP实例配置模式下，使用以下命令：

spcode *spcode-number*

- *spcode-number* - 指定企业编码，取值范围为1至31位数字。

在SP实例配置模式下使用该命令no的形式取消企业编码的指定：

no spcode

发送测试短信

为验证设备能否正常发送短信，管理员可以向指定手机号码发送测试短信。发送测试短信，在任意模式下，使用以下命令：

exec sms sp sp-name *tunnel-name* **send test-message to** *phone-number*

- *phone-number* – 指定接收测试短信的手机号码。
- *tunnel-name* – 指定绑定该SP实例的隧道的名称。

如果测试短信发送成功，指定手机号码会收到系统发送的测试短信；如果测试短信发送失败，系统会记录日志并描述失败原因。

开启/关闭短信网关认证功能

配置好的SP实例需要绑定到SSL VPN隧道才能生效。默认情况下，系统的短信网关认证功能为关闭状态。在SSL VPN实例配置模式下，使用以下命令开启短信网关认证功能：

sms-auth enable *sp-name*

- *sp-name* – 指定SP实例的名称，该名称须是已创建的SP实例名称。取值范围为1至31个字符。

在SSL VPN实例配置模式下，使用该命令no的形式关闭该功能：

sms-auth disable *sp-name*

指定发送方名称

用户可以指定短信发送方名称以显示在短信内容中，在SSL VPN实例配置模式下，使用以下命令：

sms-auth sms-sender-name *sender-name*

- *sender-name* – 指定发送方名称。取值范围是1到63字符。

在SSL VPN实例配置模式下，使用该命令no的形式删除发送方名称的指定：

no sms-auth sms-sender-name

注意:

由于UMS企业信息平台限制，当使用短信网关认证时，发送方名称将会显示在UMS企业信息平台注册的名称。

显示短信网关配置信息

在任意模式下，使用以下命令查看短信网关的配置信息：

show sms service-provider [*sp-name*]

- *sp-name* – 指定已创建的SP实例。如不指定，则默认显示所有已创建的SP实例的配置信息。

显示短信统计信息

在任意模式下，使用以下命令查看短信网关发送短信成功或失败的计数信息：

show tunnel scvpn *scvpn-name***smsp-statistice** [*clear*]

- *scvpn-name* – 指定已创建的SSL VPN实例名称。
- **clear** – 清除所有的计数信息。

配置主机验证功能

主机验证功能是指SSL VPN实例对运行SSL VPN客户端的主机进行验证。用户在PC上通过SSL VPN客户端登录时，客户端先收集主机的主板序列号、硬盘序列号、CPU ID和BIOS序列号，然后客户端对这些信息进行MD5运算，生成一个32位的字符串，即主机ID。之后，客户端将主机ID以及用户名密码信息发送到SSL VPN设备端进行验证。SSL VPN设备端根据候选表和绑定表中记录表项以及主机验证配置进行验证。候选表和绑定表描述如下：

- 候选表：客户端首次登录时，SSL VPN设备端会记录用户名与主机ID的对应关系，并加入候选表中。
- 绑定表：绑定表中包含允许验证通过的主机ID与用户名对应关系的表项。用户可以通过手工操作或首次登录自动批准方式把候选表中的表项移入绑定表中。客户端登录时，SSL VPN设备端会先检查绑定表中是否有该主机ID与用户名的对应关系表项，如果有，则通过主机验证，继续进行用户名密码验证；如果没有，则直接中断SSL通讯过程。

开启主机验证功能

默认情况下，设备端的主机验证功能处于关闭状态。在SSL VPN实例配置模式下，使用以下命令开启主机验证功能：

user-host-verify [**allow-multi-host**] [**allow-shared-host**] [**auto-approved-first-bind**]

- **user-host-verify** – 开启主机验证功能。默认情况下，仅允许一个用户通过一台主机登录，即用户名和主机一一对应。
- **allow-multi-host** – 允许一个用户通过多台主机登录。
- **allow-shared-host** – 允许多个用户通过一台主机登录。

- **auto-approved-first-bind** – 用户首次登录时自动把用户名和主机ID的对应关系加入绑定表。

在SSL VPN实例配置模式下使用该命令no的形式关闭主机验证功能：

no user-host-verify

批准候选表项

批准候选表项是把候选表中的主机ID与用户名的对应关系表项移到绑定表中。在任意模式下，使用以下命令批准指定的候选表项：

exec scvpn *instance-name* **approve-binding user** *user-name* **host** *host-id*

- **scvpn** *instance-name* – 指定SSL VPN实例的名称。
- **user** *user-name* – 指定候选表项对应的用户名称。
- **host** *host-id* – 指定候选表项对应的主机ID。

配置超级用户

超级用户不受主机验证功能限制，可以通过任意主机登录。在任意模式下使用以下命令配置候选表或者绑定表中的用户为超级用户：

exec scvpn *instance-name* **no-host-binding-check user** *user-name*

- **scvpn** *instance-name* – 指定SSL VPN实例的名称。
- **user** *user-name* – 指定超级用户的用户名称。

使用以下命令取消超级用户配置：

exec scvpn *instance-name***host-binding-checkuser** *user-name*

配置共享主机

通过共享主机登录的用户不受主机验证功能限制。在任意模式下使用以下命令配置候选表或者绑定表中的主机为共享主机：

exec scvpn *instance-name* **no-user-binding-check host** *host-id*

- **scvpn** *instance-name* – 指定SSL VPN实例的名称。
- **host** *host-id* – 指定共享主机的主机ID。该主机ID需要为候选表或者绑定表中的主机ID。

使用以下命令取消共享主机配置：

no exec scvpn *instance-name* **no-user-binding-check host** *host-id*

增加/减少预批准主机数

当允许一个用户通过多台主机登录且设置了用户首次登录自动批准用户名和主机ID的绑定关系时，默认情况下，仅自动批准用户和首次登录主机ID的绑定关系表项，即仅批准一个主机ID，以后登录的主机ID进入候选表。在任意模式下，使用以下命令增加/减少预批准主机数：

exec scvpn *instance-name* **increase-host-binding user** *user-name number*

- **scvpn** *instance-name* – 指定SSL VPN实例的名称。
- **user** *user-name* – 指定用户名称。
- *number* – 指定增加的预批准主机数。取值范围为1到32。系统将在原预批准主机数的基础上进行增加。单个用户的预批准主机数的总数范围为0到100。

exec scvpn *instance-name* **decrease-host-binding user** *user-name number*

- **scvpn** *instance-name* – 指定SSL VPN实例的名称。
- **user** *user-name* – 指定用户名称。
- *number* – 指定减少的预批准主机数。取值范围为1到32。系统将在原预批准主机数的基础上进行减少。单个用户的预批准主机数的总数范围为0到100。

清除绑定表

在任意模式下，使用以下命令清除绑定表或指定的绑定表项：

exec scvpn *instance-name* **clear-binding** [{**user** *user-name* [**host** *host-id*] | **host** *host-id* }]

- **scvpn** *instance-name* – 指定SSL VPN实例的名称。
- **user** *user-name* – 指定用户名称。如果不指定Host ID，则删除指定用户的所有绑定表项。
- **host** *host-id* – 指定主机ID。

导出/导入绑定表

用户可以通过FTP、TFTP或USB方式实现绑定表的导出或导入。在执行模式下使用以下命令导出绑定表：

export scvpn user-host-binding to {**ftp server** ip-address [**user** user-name **password** password] | **tftp server** ip-address | **usb0** | **usb1**} [**file-name**]

- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – 指定通过FTP方式导出绑定表。**user** *user-name* **password** *password*指定FTP服务器的IP地址以及访问服务器使用的用户名和密码，当不指定用户名和密码时表示采用匿名登录方式。
- **tftp server** *ip-address* – 指定通过TFTP方式导出绑定表。*ip-address* 指定TFTP服务器的IP地址。
- **usb0 | usb1** – 指定将绑定表导出到U盘根目录。
- *file-name* – 指定导出的绑定表的文件名称。默认名称为scvpn_bind_file。

在执行模式下，使用以下命令导入绑定表：

import scvpn user-host-binding from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} [*file-name*]

- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – 指定通过FTP方式导入绑定表。**user** *user-name* **password** *password*指定FTP服务器的IP地址以及访问服务器使用的用户名和密码，不指定用户名和密码时表示采用匿名登录方式。
- **tftp server** *ip-address* – 指定通过TFTP方式导入绑定表。*ip-address* 指定TFTP服务器的IP地址。

- **usb0 | usb1** – 指定从U盘根目录导入绑定表。
- *file-name* – 指定要导入的文件名。

配置主机安全检测功能

主机安全检测功能是指SSL VPN实例对运行SSL VPN客户端主机的安全状况进行检测，通过检查客户端主机的操作系统、IE版本以及特定软件的安装情况等因素来评估客户端主机的安全级别，并根据不同安全级别为客户端分配不同的资源访问权限，保证SSL VPN接入的安全性。

主机安全检测内容

Hillstone设备主机安全检测功能对客户端主机的详细检查内容，请参见下表：

检查项目	详细描述
操作系统配置	• 操作系统版本（如Windows 2000、Windows 2003、Windows XP、Windows Vista等） • 操作系统补丁包版本（如Service Pack 1等） • Windows特定补丁包是否安装（如KB958215等）
	• Windows安全中心和自动升级是否打开 • 防病毒软件是否必须安装，实时监控和病毒特征库在线升级是否打开 • 防间谍软件是否必须安装，实时监控和特征库在线升级是否打开 • 个人防火墙是否必须安装和实时保护是否打开
其他配置	IE版本和安全级别是否达到指定标准
	指定进程是否正在运行
	指定服务是否已经安装
	指定服务是否正在运行
	指定注册表条目是否存在
	指定文件是否存在于操作系统中

基于角色的访问控制和主机安全检测流程

基于角色的访问控制是指用户的权限不是由用户名而是由用户在系统中的角色决定的，一个登录于某系统的用户，可以通过它所对应角色的权限来决定其可以访问的系统资源。在权限管理中，角色作为中间桥梁把用户和权限联系起来。

Hillstone设备SSL VPN在主机安全检测流程中实现了基于角色的访问控制，在安全检测策略规则中引入初级角色和次级角色的概念。初级角色主要用于用户从设备端获取对应的安全检测Profile（包含主机安全检测的内容以及安全级别，可通过WebUI进行配置）以及决定检测成功用户的实际访问权限；次级角色决定检测失败用户的实际访问权限。关于角色配置与安全检测结果之间的关系，请参见本章配置主机安全检测策略规则中的表7：主机安全检测策略规则配置和检测结果以及权限授予对应列表。

主机安全检测流程如下：

1. 客户端发起连接请求并成功认证。
2. 设备端下发安全检测Profile到客户端。
3. 客户端根据安全检测Profile对主机系统进行相应的安全检测。
4. 客户端将最终检测结果返回给设备端。
5. 如果安全检测成功，设备端根据配置的安全检测策略规则中的初级角色授予用户实际访问权限；如果安全检测失败，设备端断开检测失败客户端的连接并给出提示或者根据配置的安全检测策略规则中的次级角色授予用户实际访问权限。

另外，Hillstone设备主机安全检测功能还支持动态的访问权限控制。一方面，当设备端的安全状况发生变化时，设备端会主动下发Profile给客户端，并要求客户端重新进行安全检测；另一方面，客户端可以周期性地进行安全检查，比如可以定时地检查客户端主机的防病毒软件是否开启，如果用户在使用过程中关闭了防病毒软件，系统可能会因此在用户的访问过程中改变该用户所属的角色，重新为该用户分配相应的权限。

配置主机安全检测Profile

主机安全检测Profile指定主机安全检查的内容以及安全级别。用户可以通过WebUI和CLI指定安全检测Profile名称，但是Profile的内容需要通过WebUI进行配置。指定主机安全检测Profile，在全局配置模式下使用以下命令：

scvpn host-check-profile *hostcheck-profile-name*

- *hostcheck-profile-name* – 指定主机安全检测Profile的名称。执行该命令后，系统创建指定名称的主机安全检测Profile。

在全局配置模式下，使用**no scvpn host-check-profile** *hostcheck-profile-name*删除指定的主机安全检测Profile。

通过WebUI配置主机安全检测Profile

用户可以通过WebUI配置主机安全检测Profile，指定主机安全检测内容。通过WebUI配置主机安全检测Profile，按照以下步骤进行配置：

1. 访问页面“配置 > 网络 > SSL VPN”，在页面右侧辅助栏的<任务>区选择『主机检测』链接进入主机检测配置页面。
2. 在该页面点击『新建』按钮，弹出<主机检测配置>对话框。
3. 依次填写或者选择各项。配置选项具体描述如下：

基本配置

- **名称：**指定主机检测Profile名称。
- **OS版本：**指定是否检测客户端主机的操作系统版本。从下拉菜单中选择合适的检测类型，包括：
  - 不检测 - 不对客户端主机操作系统版本进行检测。
  - 必须匹配 - 客户端主机操作系统版本必须和指定操作系统版本一致。分别在后面的下拉菜单中选择操作系统版本和操作系统补丁包版本。
  - 至少 - 客户端主机操作系统版本必须高于指定操作系统版本或者和指定操作系统版本一致。分别在后面的下拉菜单中选择操作系统版本和操作系统补丁包版本。
- **补丁包x：**指定客户端主机必须安装的特定Windows补丁包，在文本框中输入补丁包名称。用户最多可以为每条主机检测Profile指定5个补丁包。
- **最低IE版本：**指定检测客户端主机Internet zone的IE版本必须高于指定版本或者和指定版本一致。选中所需选项的单选按钮。

- 最低IE安全级别：指定检测客户端主机的IE安全级别必须高于指定级别或者和指定级别一致。选中所需选项的单选按钮

高级配置

- **安全中心：**指定检测客户端主机的Windows安全中心是否开启。选中<必须启用>复选框指定客户端主机必须开启Windows安全中心。

- **自动更新：**指定检测客户端主机的Windows自动升级功能是否开启。选中<必须启用>复选框指定客户端主机必须开启Windows自动升级功能。

- **防病毒软件：**指定检测客户端主机的反病毒软件是否安装，实时监控和病毒特征库更新是否打开。选项包括：
    - 安装软件 - 选中该复选框指定客户端主机必须安装防病毒软件。
    - 实时监控 - 选中该复选框指定客户端主机必须开启防病毒软件实时监控功能。
    - 病毒特更新 - 选中该复选框指定客户端主机必须开启防病毒软件病毒特征库在线升级功能。
- **防间谍软件：**指定检测客户端主机的防间谍软件是否安装，实时监控和特征库更新是否打开。选项包括：
    - 安装软件 - 选中该复选框指定客户端主机必须安装防间谍软件。
    - 实时监控 - 选中该复选框指定客户端主机必须开启防间谍软件实时监控功能。
    - 特征库更新 - 选中该复选框指定客户端主机必须开启防间谍软件特征库在线升级功能。
- **防火墙：**指定检测客户端主机的个人防火墙是否安装，实时监控是否打开。选项包括：
    - 安装软件 - 选中该复选框指定客户端主机必须安装个人防火墙。
    - 实时监控 - 选中该复选框指定客户端主机必须开启个人防火墙实时监控功能。

- **注册表键值x：**指定检测客户端主机的特定注册表条目是否存在。用户最多可以为每条主机检测Profile指定5个注册表条目名称。从下拉菜单中选择合适的检测类型，包括：
    - 不检测 - 不检测特定注册表条目是否存在。
    - 存在 - 客户端主机中包含指定注册表条目。在文本框中输入注册表条目名称。
    - 不存在 - 指定注册表条目在客户端主机中不存在。在文本框中输入注册表条目名称。
- **文件路径名称x：**指定检测客户端主机的特定文件是否存在。用户最多可以为每条主机检测Profile指定5个文件路径名称。从下拉菜单中选择合适的检测类型，包括：
    - 不检测 - 不检测特定文件是否存在。
    - 存在 - 客户端主机操作系统中包含指定文件。在文本框中输入文件路径名称。
    - 不存在 - 指定文件在客户端主机操作系统中不存在。在文本框中输入文件路径名称。
- **运行进程名称x：**指定检测客户端主机的特定进程是否正在运行。用户最多可以为每条主机检测Profile指定5个进程名称。从下拉菜单中选择合适的检测类型，包括：
    - 不检测 - 不对特定进程的运行情况进行检测。
    - 存在 - 指定进程在客户端主机中正在运行。在文本框中输入进程名称。
    - 不存在 - 指定进程在客户端主机中没有运行。在文本框中输入进程名称。
- **安装服务名称x：**指定检测客户端主机的特定服务是否已经安装。用户最多可以为每条主机检测Profile指定5个服务名称。从下拉菜单中选择合适的检测类型，包括：

- 不检测 - 不对特定服务的安装情况进行检测。
- 存在 - 指定服务在客户端主机中已经安装。在文本框中输入服务名称。
- 不存在 - 指定服务在客户端主机中没有安装。在文本框中输入服务名称。

• **运行服务名称x：**指定检测客户端主机的特定服务是否正在运行。用户最多可以为每条主机检测Profile指定5个服务名称。从下拉菜单中选择合适的检测类型，包括：

- 不检测 - 不对特定服务的运行情况进行检测。
- 存在 - 指定服务在客户端主机中正在运行。在文本框中输入服务名称。
- 不存在 - 指定服务在客户端主机中没有运行。在文本框中输入服务名称。

4. 配置完成，点击『确定』或者『应用』按钮保存所做配置。

配置主机安全检测策略规则

主机安全检测Profile配置完成后，只有把它引用到主机安全检测策略规则中，配置的安全检测功能才能对用户生效。配置主机安全检测策略规则，请在SSL VPN实例配置模式下使用以下命令：

host-check [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name*] [**periodic-check** *period-time*]

• **role** *role-name* – 指定用户的初级角色，该初级角色为AAA服务器中已配置的用户角色。如果配置该参数，该主机安全检测Profile对该指定角色有效；如果不配置此参数，该主机安全检测Profile将作为缺省Profile并对所有未指定Profile的用户生效。

• **profile** *profile-name* – 指定绑定的主机安全检测Profile名称。

• **guest-role** *guestrole-name* – 指定用户的次级角色。当客户端的主机安全检测失败时，如果配置该参数，用户将获得该次级角色拥有的访问权限；如果不配置该参数，系统将断开该客户端连接。

• **periodic-check** *period-time* – 指定该用户的自动检测周期。单位为分钟，取值范围为5到1440分钟，默认值为30分钟。

可以配置多条该命令添加多个安全检测策略规则。当一个用户可匹配多个安全检测策略规则时，设备端会按照查找到的第一条相匹配的规则进行处理；另外，一个用户可以绑定到一个或者多个角

色，当一个用户绑定到多个角色且多个角色均配置安全检测策略规则时，设备端会按照查找到的第一条相匹配的规则进行处理。

在SSL VPN实例配置模式下，使用**no host-check** [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name*] [**periodic-check** *period-time*]取消主机安全检测策略规则的配置。

- **role** *role-name* – 删除指定初级角色相关的安全检测Profile。若未指定初级角色和次级角色，将删除缺省主机安全检测Profile。
- **guest-role** *guestrole-name* – 在指定初级角色的前提下，删除所指定的次级角色。
- **periodic-check** *period-time* – 在指初级定角色的前提下，将指定角色所对应的自动检测周期恢复为默认值30分钟。

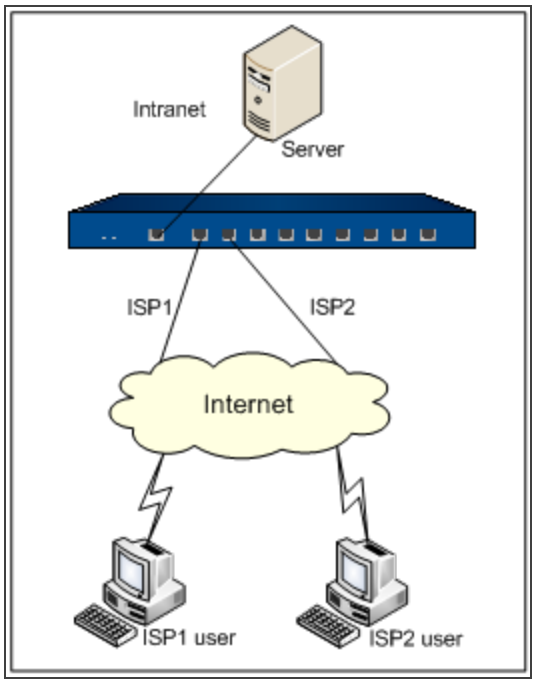
根据上述主机安全检测策略规则CLI描述，表20-3列出主机安全检测策略规则配置情况、检测结果和权限授予之间的详细对应关系：

策略规则配置	检测结果	
	通过检测	未通过检测
初级角色：配置 profile：配置 次级角色：配置	获得初级角色对应访问权限	获得次级角色对应访问权限
初级角色：配置 profile：配置 次级角色：未配置	获得初级角色对应访问权限	断开连接并给出提示
初级角色：未配置 profile：配置 次级角色：配置	正常连接	获得次级角色对应访问权限
初级角色：未配置 profile：配置 次级角色：未配置	正常连接	断开连接并给出提示

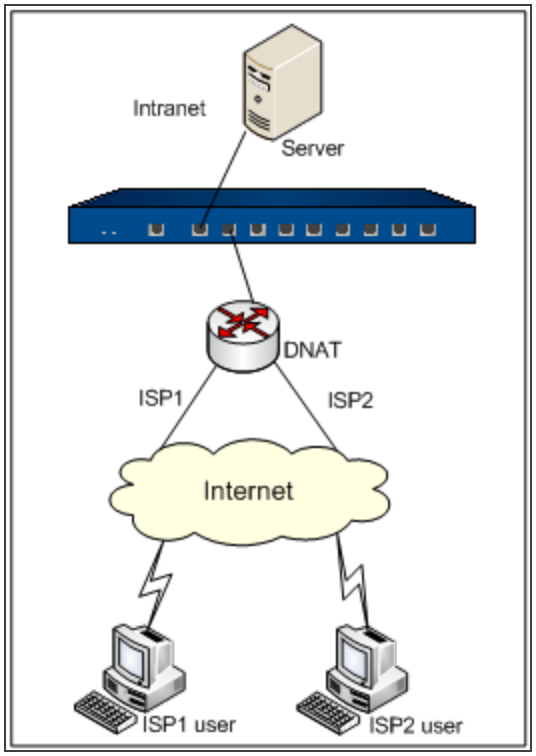
配置最优路径检测功能

目前，大规模VPN网络往往都是跨ISP（Internet Service Provider，互联网服务提供商）的，但是不同ISP间通信时带宽小、延迟大，严重影响了VPN的应用效果。针对此问题，Hillstone设备SSL VPN支持最优路径检测功能，该功能能够使不同ISP线路接入的客户端自动选择最快线路连接到SSL VPN设备端，从而提高访问总部资源时的速度。

Hillstone设备SSL VPN最优路径检测功能的网络环境实现包括以下两种：



如上图所示，SSL VPN客户端直接访问设备端出接口地址。SSL VPN设备端首先需要申请多条不同的ISP上网线路连接到Internet，并启用相应数目的设备端接口作为SSL VPN通道出接口。当客户端使用不同的ISP上网线路访问总部资源时，如果开启了设备端检测最优通道功能，设备端Hillstone设备会通过客户端的源接入地址判断其ISP类型，根据判断，将所有的SSL VPN出接口IP地址按照优先级重新排序并下发给客户端，由客户端选择连接的最优通道；否则，客户端通过发送UDP探测包自动判断最优链路，并选择连接的最优通道。



如上图所示，SSL VPN客户端通过DNAT设备访问SSL VPN设备端，该DNAT设备会将客户端的访问地址映射到SSL VPN设备端的出接口地址。这种方式下，DNAT设备外网端口通过多条不同的ISP上网线路连接到Internet，用户需要将DNAT设备的外网接口地址配置为设备端地址簿中的地址条目，当客户端使用不同的ISP上网线路访问DNAT设备外网接口地址时，如果开启了设备端检测最优通道功能，设备端Hillstone设备会通过客户端的源接入地址判断其ISP类型，根据判断，将所有的DNAT外网接口IP地址按照优先级重新排序并下发给客户端，由客户端选择连接的最优通道；否则，客户端通过发送UDP探测包自动判断最优链路，并选择连接的最优通道。

启用设备端接口作为SSL VPN通道出接口，在SSL VPN实例配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定设备端接口的名称。

多次执行该命令启用多个接口，系统允许最多开启两个接口。在SSL VPN实例配置模式下使用该命令no的形式取消指定设备端接口的配置：

no interface *interface-name*

配置自动检测最优通道功能，在SSL VPN实例配置模式下，使用以下命令：

link-select [**server-detect**] [*A.B.C.D* [**https-port** *port-number*]] [**A.B.C.D** [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]]

- **server-detect** – 开启设备端检测最优通道功能，默认情况下由客户端检测最优通道。
- *A.B.C.D* – 指定DNAT设备外网接口IP。系统允许最多配置四个IP地址。
- **https-port** *port-number* –指定DNAT设备外网接口HTTPS端口号。默认值是4433。取值范围是1到65535。为避免与WebUI使用的HTTPS端口号相冲突，建议用户不要把HTTPS端口号设置为443。

在SSL VPN实例配置模式下使用**no link-select**命令取消自动检测最优通道功能的配置。

另外，SSL VPN最优路径检测的应用还提供多链路冗余的功能，当任意一条链路不通时，数据均会自动切换到另外的链路，从而保证客户端连接的稳定性（切换过程中流量可能会中断）。

强制断开客户端SSL VPN连接

设备端可以通过命令强制断开某个客户端与设备端的连接。强制断开客户端SSL VPN连接，在执行模式使用以下命令：

exec scvpn *instance-name* **kickout** *user-name*

- *instance-name* – 指定SSL VPN实例的名称。
- *user-name* – 指定被强制断开连接的用户名称。

允许本地用户修改密码

Hillstone设备支持本地用户成功通过SSL VPN认证后，在客户端修改自己的用户密码。默认情况下，该功能为关闭状态。在本地AAA服务器配置模式下，使用以下命令开启或关闭允许本地用户修改登录密码功能：

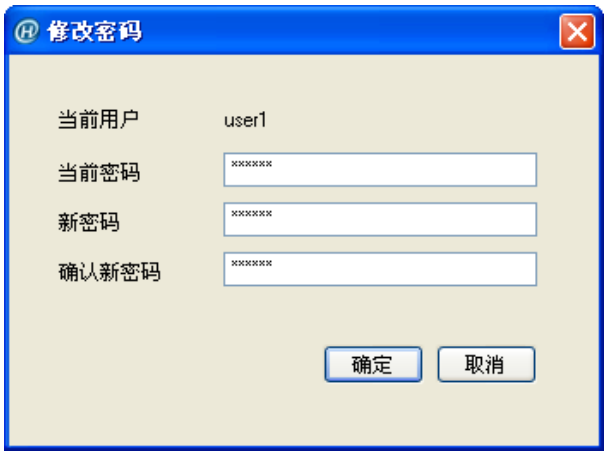
- 开启：**allow-pwd-change**
- 关闭：**no allow-pwd-change**

提示: SSL VPN客户端1.2.0.1106（Hillstone Secure Connect 1.2.0.1106）及后续版本支持允许本地用户修改密码功能。为避免出错，建议用户使用最新版本的SSL VPN客户端。

开启该功能并成功通过SSL VPN认证后，本地用户可通过以下步骤修改登录密码：

1. 右键单击系统任务栏通知区域的Hillstone Secure Connect绿色图标，系统弹出客户端菜单，如下图所示：

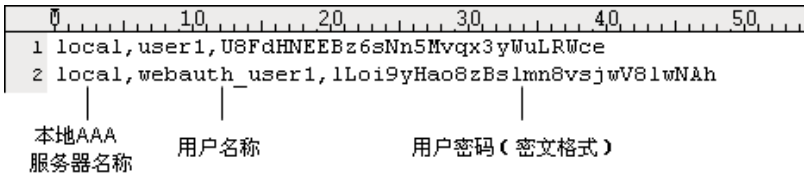
2. 点击<修改密码>，系统弹出<修改密码>对话框。在<当前密码>文本框中输入正确的旧密码，在<新密码>文本框中输入新密码并在<确认新密码>处再次输入相同的新密码。如下图所示：



3. 点击『确定』按钮，系统显示提示信息“修改密码成功”。

导出和导入密码文件

为防止恢复配置时误将密码信息重置，用户可以将密码信息以文件格式从设备端导出或者导入。导出或者导入的密码文件为CSV格式，下图为密码文件及参数描述示例：



导入密码信息的原则是：

- 如果密码文件中的用户信息和系统中的用户信息一致，按照密码文件的信息恢复所有本地用户的密码；
- 如果密码文件中的用户信息比系统中的用户信息少，只恢复密码文件中已有用户的信息，系统中其它用户的信息不变；
- 如果密码文件中的用户信息比系统中的用户信息多，只恢复系统中已有用户的信息，密码文件中其它用户的信息删除。

注意:

- 若需直接用Excel打开密码文件，请将密码文件的扩展名改成“.csv”。
- 导入密码文件后，配置立即生效。
- 导入密码文件后，系统会在CLI中提示导入成功的用户数目。

导出密码文件

导出密码文件，在执行模式下使用以下命令：

export aaa user-password to {**tftp server** *ip-address* | **ftp server** *ip-address* [**user** *user-name* **password** *password*]} [*file-name*]

- *ip-address* – 指定FTP或者TFTP服务器的IP地址。
- **user** *user-name* **password** *password* – 指定FTP服务器的用户名和密码。
- *file-name* – 指定导出的密码文件名称。

导入密码文件

导入密码文件，在执行模式下使用以下命令：

import aaa user-password from {**tftp server** *ip-address* | **ftp server ip-address** [**user** *user-name* **password** *password*]} *file-name*

- *ip-address* – 指定FTP或者TFTP服务器的IP地址。
- **user** *user-name* **password** *password* – 指定FTP服务器的用户名和密码。
- *file-name* – 指定导入的密码文件名称。

定制登录页面

Hillstone设备支持用户自行定制SSL VPN认证登录页面。默认情况下，配置SSL VPN认证功能后，其认证登录页面分别如下图所示：

定制登录页面

用户可以通过改变登录页面上的背景图片自行定制登录页面。引入登录页面背景图片到系统，请在执行模式下使用以下命令：

import customize scvpn from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – 指定从FTP服务器获取图片，并指定FTP服务器的IP地址以及访问服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。

- **tftp server** *ip-address* – 指定从TFTP服务器获取图片，并指定TFTP服务器的IP地址。

- **usb0 | usb1** – 指定通过USB方式从USB0或者USB1插槽所对应的U盘根目录获取图片。

- *file-name* – 指定图片名称。其文件名必须为“Login_box_bg_en.gif”（用于英文登录页面）或“Login_box_bg_cn.gif”（用于中文登录页面）。所有图片的分辨率必须为624px * 376px，并且只有将它们压缩到zip包后才能上载。

恢复默认图片，在任何配置模式下，使用以下命令：

exec customize scvpn [language {**en** | **zh_cn**}] **default**

- **language** {**en** | **zh_cn**} – 指定将英文（en）或者中文（zh_cn）认证登录页面恢复为默认图片。

通过Radius认证服务器限定用户的访问范围

当用户使用Radius认证方式时，系统可限定已认证用户的访问范围。对于已认证的用户，系统从Radius服务器上获取此用户的授权区域信息（即可访问的目的地址范围）。根据该授权区域，系统为此用户动态创建从其源地址到授权区域的安全策略；对于未通过认证的用户，系统拒绝将其接入网络。当用户注销登录、登陆超时、或被系统管理员强制登出后，对应的安全策略将被自动删除。

在任何模式下，使用以下命令查看用户的授权区域信息：

show auth-user username *user-name*

- *user-name* – 指定要查看的用户的用户名。

配置Radius服务器

用户需要在Radius服务器的字典文件中增如下自定义属性：

属性名称	属性类型	描述
Hillstone-user-policy-dst-ip-begin	ipaddr	授权区域的起始IP地址。请输入

属性名称	属性类型	描述
		IPv4地址。
Hillstone-user-policy-dst-ip-end	ipaddr	授权区域的终止IP地址。请输入IPv4地址。

添加自定义属性后，为Radius服务器中的用户赋予相应的属性值。完成赋值后，重启Radius服务。当用户使用SSL VPN客户端成功认证后，系统将根据此用户在Radius服务器中配置的属性值限定其可访问的网络资源。如果没有为此用户设定授权区域，用户将不受访问限制。

配置客户端升级URL

客户端通过配置的URL进行新版本检查及下载升级。系统默认已经存在指向官方升级服务器的URL，且此URL不可删除。客户端会通过此官方升级服务器的URL进行新版本检查以及下载升级。当用户需要使用内网服务器进行客户端新版本的检查以及下载升级时，可配置新的升级URL后，且新配置URL生效。配置升级URL，在全局配置模式下执行以下命令：

scvpn-update-url *ip-address*

- *ip-address* – 如果需要使用内网服务器进行客户端新版本的检查以及下载升级，则输入内网服务器URL。用户需要自行在此服务器部署客户端新版本。

在全局配置模式下，使用该命令no的形式恢复默认的官方升级服务器的URL：

no scvpn-update-url

注意: 当客户端版本为1.4.4.1199或更低版本且StoneOS版本为5.5R1或更高版本，推荐卸载旧版客户端并重新登陆Web下载安装。

显示SSL VPN信息

用户可以通过show命令查看系统SSL VPN信息。

- 显示SSL VPN实例信息：

show tunnel scvpn [*scvpn-instance-name*]

- 显示通过浏览器访问SSL VPN的HTTP会话信息：

show scvpn session *scvpn-instance-name* [**user** *user-name*]

- 显示指定SSL VPN实例当前在线的客户端信息：

show scvpn client *scvpn-instance-name* [**user** *user-name*]

- 显示所有SSL VPN实例当前在线的客户端信息：

show auth-user scvpn [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]

- 显示主机验证绑定表：

show scvpn user-host-binding *scvpn-instance-name* {**host** [*host-id*] | **user** [*user-name*]}

SSL VPN客户端 for Windows

针对Windows操作系统的SSL VPN客户端程序为Hillstone Secure Connect。Hillstone Secure Connect可在以下操作系统中运行：Windows 2000/2003/2008/XP/Vista/Windows 7/Windows 8/Windows 8.1/Windows10/Windows2012。通过客户端与设备端的连接，即可实现数据的加密通信。该客户端的主要作用包括：

- 从所在PC获得接口和路由信息；
- 显示与连接状态、数据流统计数据以及接口和路由信息；
- 显示应用程序日志信息；
- 调用客户端更新程序进行客户端更新；
- 解析从服务器端接收到的资源列表信息。

本节主要介绍SSL VPN客户端的下载、安装和启动。根据设备端配置的认证方式的不同，客户端的下载、安装和启动方法将不同。SSL VPN设备端支持以下三种认证方式：

- 用户名/密码
- 用户名/密码 + 数字证书（包括USB Key证书和软证书）
- 只用数字证书（包括USB Key证书和软证书）

客户端的下载与安装

初次使用SSL VPN客户端时，用户需要下载和安装客户端程序Hillstone Secure Connect。本节将根据设备端的三种认证方式，分别介绍对应的客户端下载和安装方法。对于“用户名/密码 + 数字证书”认证方式，数字证书可以是厂商提供的USB Key证书或管理员所提供的软证书。

下载与安装（用户名/密码）

当设备端配置“用户名/密码”认证方式时，请按照以下步骤下载和安装客户端程序Hillstone Secure Connect：

1. 在浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端SSL VPN实例中指定的接口的IP地址（interface interface-name命令）和HTTPS（https-port port-number命令）端口号。
2. 浏览器转到登录页面，输入用户名和密码，并点击『登录』按钮。

   - 如果设备端采用本地认证服务器进行用户认证，此处的用户名和密码为Hillstone设备中配置的用户及其相应的密码；
   - 如果设备端采用“RADIUS认证+通过RSA Server进行RSA SecurID Token认证”相结合的方式，并且是首次登录，此处输入的用户名应为RADIUS服务器中的用户名称，密码为该用户绑定的实时Token动态口令。输入完成并点击『登录』按钮后，浏览器将转到PIN码设置页面，用户需要在该页面设置PIN码，为4至8位数字。PIN码设置成功后，系统会提示使用新密码重新登录，点击<重新登录>，浏览器返回登录页面，输入正确的用户名和新密码，并点击『登录』按钮。此处的新密码为“PIN码+实时Token动态口令”，例如，如果PIN码设置为54321，实时Token动态口令为808771，则新密码为54321808771；
   - 如果设备端采用“RADIUS认证+通过RSA Server进行RSA SecurID Token认证”相结合的方式，但不是首次登录，此处输入的用户名为RADIUS服务器中的用户名称，密码为首次重新登录时输入的新密码“PIN码+实时Token动态口令”。

提示: 用户可以自行定制此登录页面，即改变登录页面上的背景图片。关于如何自行定制登录页面，请参阅“定制登录页面”。

3. 如果设备端开启短信口令认证功能，浏览器将转到短信口令认证对话框，如下图所示。输入短信认证码，并点击『认证』按钮。如果用户在1分钟内没收到认证码短信，可以重新申请

认证码。

提示:

- 通过用户名和密码验证后，用户最多可以输入3次认证码。如果连续3次输入错误，设备端将自动断开连接。
- 用户最多能重新申请3次认证码，新认证码短信发送的时间间隔为1分钟。重新申请认证码后，旧认证码信息失效，用户必须输入最新认证码才能认证成功。

4. 成功登录后，如果使用IE浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox等浏览器，请点击『下载』按钮下载客户端程序scvpn.exe，下载完成，双击scvpn.exe，按照安装向导提示进行安装。

成功安装Hillstone Secure Connect后，将有一个虚拟网卡安装到PC上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

下载与安装（用户名/密码 + USB Key证书）

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于USB Key证书，请按照以下步骤下载和安装客户端程序Hillstone Secure Connect：

1. 将USB Key插入PC的USB接口。

2. 在浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端SSL VPN实例中指定的接口的IP地址（**interface** *interface-name*命令）和HTTPS（**https-port** *port-number*命令）端口号。

3. 浏览器弹出<选择数字证书>对话框，如图所示。选中需要的数字证书，点击『确定』按钮。继续在弹出的<请输入PIN码>对话框（如图所示）中输入UKey的PIN码，并点击『确定』按钮。

提示: Hillstone UKey的正常使用需要有配套的驱动程序和管理员软件，具体信息请参阅《Hillstone UKey使用指南》。

4．浏览器转到登录页面。输入用户名和密码，并点击『登录』按钮。此处的用户名和密码为Hillstone设备中配置的用户及其相应的密码。

5．如果设备端开启短信口令认证功能，浏览器将转到短信口令认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在1分钟内没收到认证码短信，可以重新申请认证码。

6．成功登录后，如果使用IE浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox等浏览器，请点击『下载』按钮下载客户端程序scvpn.exe，下载完成，双击scvpn.exe，按照安装向导提示进行安装。

成功安装Hillstone Secure Connect后，将有一个虚拟网卡安装到PC上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

下载与安装（用户名/密码 + 软证书）

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于软证书，请按照以下步骤下载和安装客户端程序Hillstone Secure Connect：

1．手动导入管理员所提供的软证书。

2．在浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端SSL VPN实例中指定的接口的IP地址（**interface** *interface-name*命令）和HTTPS（**https-port** *port-number*命令）端口号。

3．浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。

4．浏览器转到登录页面。输入用户名和密码，并点击『登录』按钮。此处的用户名和密码为Hillstone设备中配置的用户及其相应的密码。

5．如果设备端开启短信口令认证功能，浏览器将转到短信口令认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在1分钟内没收到认证码短信，可以重新申请认证码。

6．成功登录后，如果使用IE浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox等浏览器，请点击『下载』按钮下载客户端程序scvpn.exe，下载完成，双击scvpn.exe，按照安装向导提示进行安装。

成功安装Hillstone Secure Connect后，将有一个虚拟网卡安装到PC上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

下载与安装（只用USB Key证书）

当设备端配置“只用数字证书”认证方式时，对于USB Key证书，请按照以下步骤下载和安装客户端程序Hillstone Secure Connect：

1. 将USB Key插入PC的USB接口。

2. 在浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端SSL VPN实例中指定的接口的IP地址（**interface** *interface-name*命令）和HTTPS（**https-port** *port-number*命令）端口号。

3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。继续在弹出的<请输入用户口令>对话框中输入UKey的用户口令（默认为“1111”），并点击『确定』按钮。

4. 成功登录后，如果使用IE浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox等浏览器，请点击『下载』按钮下载客户端程序scvpn.exe，下载完成，双击scvpn.exe，按照安装向导提示进行安装。

成功安装Hillstone Secure Connect后，将有一个虚拟网卡安装到PC上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

下载与安装（只用软证书）

当设备端配置“只用数字证书”认证方式时，对于软证书，请按照以下步骤下载和安装客户端程序Hillstone Secure Connect：

1. 手动导入管理员所提供的软证书。

2. 在浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端SSL VPN实例中指定的接口的IP地址（**interface** *interface-name*命令）和HTTPS（**https-port** *port-number*命令）端口号。

3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。

4. 成功登录后，如果使用IE浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox等浏览器，请点击『下载』按钮下载客户端程序scvpn.exe，下载完成，双击scvpn.exe，按照安装向导提示进行安装。

成功安装Hillstone Secure Connect后，将有一个虚拟网卡安装到PC上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

客户端的启动

PC上安装SSL VPN客户端程序Hillstone Secure Connect后，用户有两种方法可以启动客户端：

- Web方式启动
- 直接启动

Web方式启动

本节将根据设备端的三种认证方式，分别介绍对应的客户端Web启动方法。对于“用户名/密码 + 数字证书”认证方式，数字证书可以是厂商提供的USB Key证书或管理员所提供的软证书。

Web方式启动（用户名/密码）

当设备端配置“用户名/密码”认证方式时，请按照以下步骤通过Web启动客户端，完成客户端与设备端的连接：

1. 在IE浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。

2. 浏览器转到登录页面（如图所示）。输入用户名和密码，并点击『登录』按钮。
如果设备端采用本地认证服务器进行用户认证，此处的用户名和密码为Hillstone设备中配置的用户及其相应的密码；
如果设备端采用“RADIUS认证+通过RSA Server进行RSA SecurID Token认证”相结合的方式，并且是首次登录，此处输入的用户名应为RADIUS服务器中的用户名称，密码为该用户绑定的实时Token动态口令。输入完成并点击『登录』按钮后，浏览器将转到PIN码设置页面，用户需要在该页面设置PIN码，为4至8位数字。PIN码设置成功后，系统会提示使用新密码重新登录，点击<重新登录>，浏览器返回登录页面，输入正确的用户名和新密码，并点击『登录』按钮。此处的新密码为“PIN码+实时Token动态口令”，例如，如果PIN码设置为54321，实时Token动态口令为808771，则新密码为54321808771；
如果设备端采用“RADIUS认证+通过RSA Server进行RSA SecurID Token认证”相结合的方式，但不是首次登录，此处输入的用户名为RADIUS服务器中的用户名称，密码为首次重新登录时输入的新密码“PIN码+实时Token动态口令”。

3. 如果设备端开启短信口令认证功能，浏览器将转到短信认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在1分钟内没收到认证码短信，可以重新申请认证码。

完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

Web方式启动（用户名/密码 + USB Key证书）

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于USB Key证书，请按照以下步骤通过Web启动客户端，完成客户端与设备端的连接：

1. 将USB Key插入PC的USB接口。

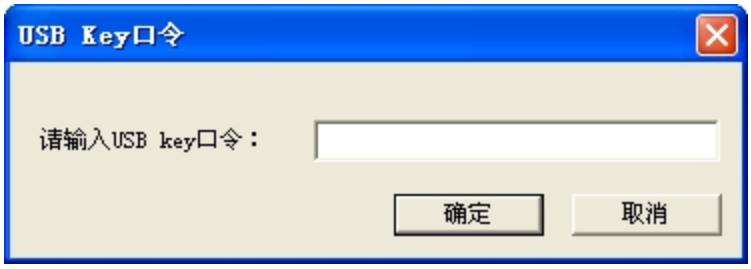
2. 在IE浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。

3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。继续在弹出的<请输入用户口令>对话框中输入UKey的用户口令（默认为“1111”），并点击『确定』按钮。

4. 浏览器转到登录页面。输入用户名和密码，并点击『登录』按钮。此处的用户名和密码为Hillstone设备中配置的用户及其相应的密码。

5. 如果设备端开启短信口令认证功能，浏览器将转到短信认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在1分钟内没收到认证码短信，可以重新申请认证码。

6. 浏览器弹出<USB Key口令>对话框，如下图所示。输入UKey的用户口令（默认为“1111”），并点击『确定』按钮。



完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

Web方式启动（用户名/密码 + 软证书）

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于软证书，请按照以下步骤通过Web启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。
2. 在IE浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。
4. 浏览器转到登录页面。输入用户名和密码，并点击『登录』按钮。此处的用户名和密码为Hillstone设备中配置的用户及其相应的密码。
5. 如果设备端开启短信口令认证功能，浏览器将转到短信认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在1分钟内没收到认证码短信，可以重新申请认证码。

完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

Web方式启动（只用USB Key证书）

当设备端配置“只用数字证书”认证方式时，对于USB Key证书，请按照以下步骤通过Web启动客户端，完成客户端与设备端的连接：

1. 将USB Key插入PC的USB接口。
2. 在IE浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。继续在弹出的<请输入用户口令>对话框中输入UKey的用户口令（默认为“1111”），并点击『确定』按钮。
4. 浏览器会弹出<USB Key口令>对话框。输入UKey的用户口令（默认为“1111”），并点击『确定』按钮。

完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

Web方式启动（只用软证书）

当设备端配置“只用数字证书”认证方式时，对于软证书，请按照以下步骤通过Web启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。
2. 在IE浏览器的地址栏输入以下URL访问设备端：https://IP-Address:Port-Number。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。

完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

直接启动

本节将根据设备端的三种认证方式以及SSL协议类型，分别介绍对应的通过启动文件直接启动客户端的方法。

基于TLS/SSL协议的启动方式

对于“用户名/密码 + 数字证书”（TLS/SSL）认证方式，数字证书可以是厂商提供的USB Key证书或管理员所提供的软证书。

基于TLS/SSL协议的启动方式如下：

- 用户名/密码
- 用户名/密码 + USB Key证书
- 用户名/密码 + 软证书
- 只用USB Key证书
- 只用软证书

使用“用户名/密码”方式

当设备端配置“用户名/密码”认证方式时，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

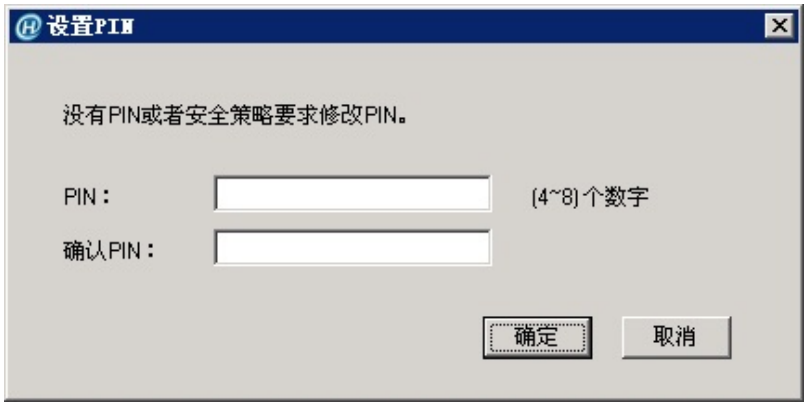
1．双击桌面的Hillstone Secure Connect快捷方式，或者点击“开始菜单”中的“所有程序→Hillstone Secure Connect→Hillstone Secure Connect”，系统弹出登录对话框。

2．点击对话框中的“模式”按钮，系统弹出<登录模式>对话框，如下图所示。在“TLS/SSL”部分，选中“用户名/密码”单选按钮，点击“确定”按钮。

3．系统弹出“用户名/密码”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。

如果设备端采用本地认证服务器进行用户认证，此处的用户名和密码为Hillstone设备中配置的用户及其相应的密码；

如果设备端采用“RADIUS认证+通过RSA Server进行RSA SecurID Token认证”相结合的方式，并且是首次登录，此处输入的用户名应为RADIUS服务器中的用户名称，密码为该用户绑定的实时Token动态口令。输入完成并点击『登录』按钮后，浏览器将转到PIN码设置对话框（如下图所示）。



用户需要在该对话框设置PIN码，为4至8位数字。PIN码设置成功后，系统会提示使用新密码重新登录（如下图所示）。

点击“确定”按钮返回登录对话框，输入新密码，并点击『登录』按钮。此处的新密码为“PIN码+实时Token动态口令”，例如，如果PIN码设置为54321，实时Token动态口令为808771，则新密码为54321808771；

如果设备端采用“RADIUS认证+通过RSA Server进行RSA SecurID Token认证”相结合的方式，但不是首次登录，此处输入的用户名为RADIUS服务器中的用户名称，密码为首次重新登录时输入的新密码“PIN码+实时Token动态口令”。

最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见

Secure Connect设置部分）。如不选择，请依次填写以下各项。

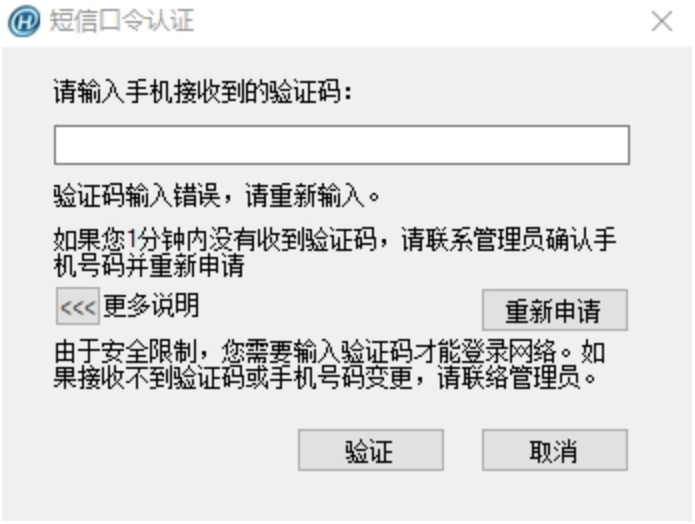
服务器：填写设备端的IP地址。

端口：填写设备端的HTTPS端口号。

用户名：填写客户端用户名。

密码：填写与用户名相对应的密码。如果用户在1分钟内连续3次输入错误密码登录SCVPN客户端，在接下来的2分钟内系统将禁止该用户再次登录。

如果设备端开启短信口令认证功能，系统将弹出<短信口令认证>对话框，如下图所示。在该对话框中输入认证码，并点击“验证”按钮。如果用户在1分钟内没收到认证码短信，可以重新申请认证码。



连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

使用“用户名/密码 + USB Key证书” 方式

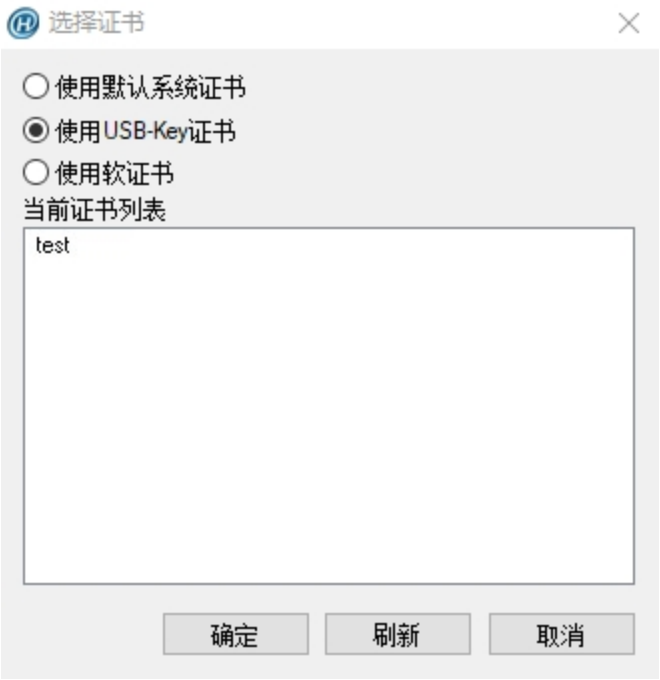
当设备端配置“用户名/密码 + 数字证书”认证方式时，对于USB Key证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将USB Key插入PC的USB接口。

2. 双击桌面的Hillstone Secure Connect快捷方式，或者点击“开始菜单”中的“所有程序→Hillstone Secure Connect→Hillstone Secure Connect”，系统弹出登录对话框。

3. 点击“模式”按钮，系统弹出<登录模式>对话框。首先，在“TLS/SSL”部分，选中<用户名/密码 + 数字证书>单选按钮；如需要，点击“选择证书”按钮，在弹出的<选择证书>对话

框中选择“使用USB Key证书”（如下图所示）。如果当前证书列表中没有显示USB Key证书，请点击“刷新”按钮。客户端会将选中的USB Key证书传送至设备端，设备端对收到的USB Key证书进行认证；最后，点击“确定”按钮。



使用默认系统证书：选中该复选框，客户端自动选择默认系统证书传送至设备端进行认证。Hillstone设备采用Hillstone UKey证书作为默认系统证书。该选项为系统默认选项。

使用USB Key证书：选中该单选按钮，客户端自动选择厂商所提供的USB Key证书传送至设备端进行认证。

使用软证书：选中该单选按钮，客户端自动选择管理员所提供的软证书传送至设备端进行认证。

当前证书列表：显示系统中已有的证书，用户可以通过该列表选择所需证书进行认证。

提示: 用户可以通过USB Key批量部署工具将第三方USB Key证书设置为默认系统证书。关于USB Key批量部署工具的详细信息，请参阅“USB Key批量部署”。

4. 系统弹出“用户名/密码 + USB Key证书”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。

最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见Secure Connect设置部分）。如不选择，请依次填写以下各项。

端口：填写设备端的HTTPS端口号。

用户名：填写客户端用户名。

密码：填写与用户名相对应的密码。

PIN码：填写USB Key对应的用户口令（默认为“1111”）。一个USB Key对应一个用户口令。

5. 如果设备端开启短信口令认证功能，系统将弹出<短信口令认证>对话框。在该对话框中输入认证码，并点击“验证”按钮。如果用户在1分钟内没收到认证码短信，可以重新申请认证码。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

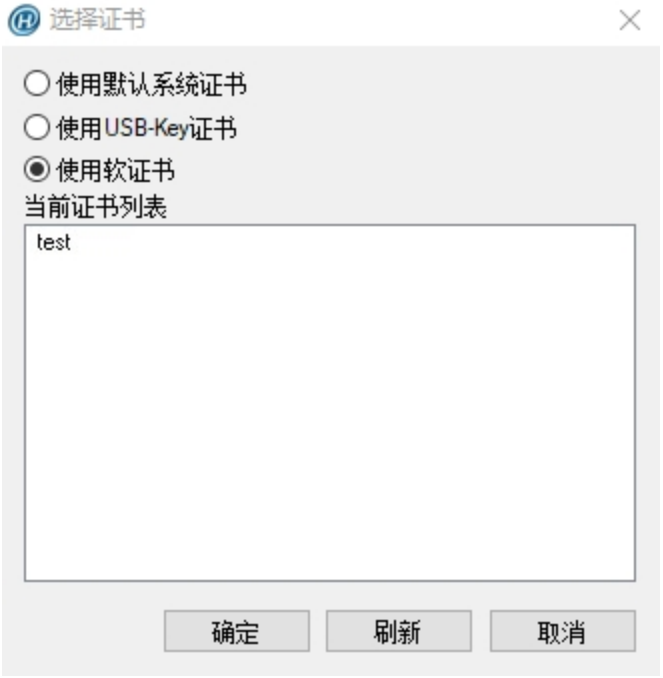
使用“用户名/密码 + 软证书”方式

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于软证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接。

1．手动导入管理员所提供的软证书。

2．双击桌面的Hillstone Secure Connect快捷方式，或者点击“开始菜单”中的“所有程序→Hillstone Secure Connect→Hillstone Secure Connect”，系统弹出登录对话框。

3．点击“模式”按钮，系统弹出<登录模式>对话框。首先，在“TLS/SSL”部分，选中<用户名/密码 + 数字证书>单选按钮；如需要，点击“选择证书”按钮，在弹出的<选择证书>对话框中选择软证书（如下图所示）。如果当前证书列表中没有显示软证书，请点击“刷新”按钮。客户端会将选中的软证书传送至设备端，设备端对收到的软证书进行认证；最后，点击“确定”按钮。



4．系统弹出“用户名/密码 + 软证书”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。

最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见Secure Connect设置部分）。如不选择，请依次填写以下各项。

服务器：填写设备端的IP地址。

端口：填写设备端的HTTPS端口号。

用户名：填写客户端用户名

密码：填写与用户名相对应的密码。

5. 如果设备端开启短信口令认证功能，系统将弹出<短信口令认证>对话框。在该对话框中输入认证码，并点击“验证”按钮。如果用户在1分钟内没收到认证码短信，可以重新申请认证码。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

使用“只用USB Key证书”方式

当设备端配置“只用数字证书”认证方式时，对于USB Key证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将USB Key插入PC的USB接口。

2. 双击桌面的Hillstone Secure Connect快捷方式，或者点击“开始菜单”中的“所有程序→Hillstone Secure Connect→Hillstone Secure Connect”，系统弹出登录对话框。

3．点击“模式”按钮，系统弹出<登录模式>对话框。首先，选中<只用数字证书>单选按钮；如需要，点击“选择证书”按钮，在弹出的<选择证书>对话框中选择USB Key证书。如果当前证书列表中没有显示USB Key证书，请点击“刷新”按钮。客户端会将选中的USB Key证书传送至设备端，设备端对收到的USB Key证书进行认证；最后，点击“确定”按钮。

4．系统弹出“只用数字证书”登录模式客户端程序登录对话框（如下图所示）依次填写登录对话框中的各项，然后点击“登录”按钮。

最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见 Secure Connect 设置部分）。如不选择，请依次填写以下各项。

服务器：填写设备端的IP地址。

端口：填写设备端的HTTPS端口号。

PIN码：填写USB Key对应的用户口令（默认为“1111”）。一个USB Key对应一个用户口令。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

使用“只用软证书”方式

当设备端配置“只用数字证书”认证方式时，对于软证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。

2. 双击桌面的Hillstone Secure Connect快捷方式，或者点击“开始菜单”中的“所有程序→Hillstone Secure Connect→Hillstone Secure Connect”，系统弹出登录对话框。

3. 点击“模式”按钮，系统弹出<登录模式>对话框。首先，选中<只用数字证书>单选按钮；如需要，点击“选择证书”按钮，在弹出的<选择证书>对话框中选择软证书。如果当前证书列表中没有显示软证书，请点击“刷新”按钮。客户端会将选中的软证书传送至设备端，设备端对收到的软证书进行认证；最后，点击“确定”按钮。

4. 系统弹出“只用数字证书”登录模式客户端。依次填写登录对话框中的各项。

最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见Secure Connect设置部分）。如不选择，请依次填写以下各项，然后点击『登录』按钮。

服务器：填写设备端的IP地址。

端口：填写设备端的HTTPS端口号。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

基于国密SSL协议的启动方式

基于国密SSL协议的启动方式如下：

- 用户名/密码
- 用户名/密码 + 数字证书
- 只用数字证书

使用“用户名/密码”方式

请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 双击桌面的Hillstone Secure Connect快捷方式，或者点击“开始菜单”中的“所有程序→Hillstone Secure Connect→Hillstone Secure Connect”，系统弹出登录对话框。

2. 点击对话框中的“模式”按钮，系统弹出<登录模式>对话框，如下图所示。在“国密SSL”部分，选中“用户名/密码”单选按钮，点击“确定”按钮。

3. 系统弹出“用户名/密码”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。

最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见Secure Connect设置部分）。如不选择，请依次填写以下各项。

服务器：填写设备端的IP地址。

端口：填写设备端的HTTPS端口号。

用户名：填写客户端用户名。

密码：填写与用户名相对应的密码。如果用户在1分钟内连续3次输入错误密码登录SCVPN客户端，在接下来的2分钟内系统将禁止该用户再次登录。

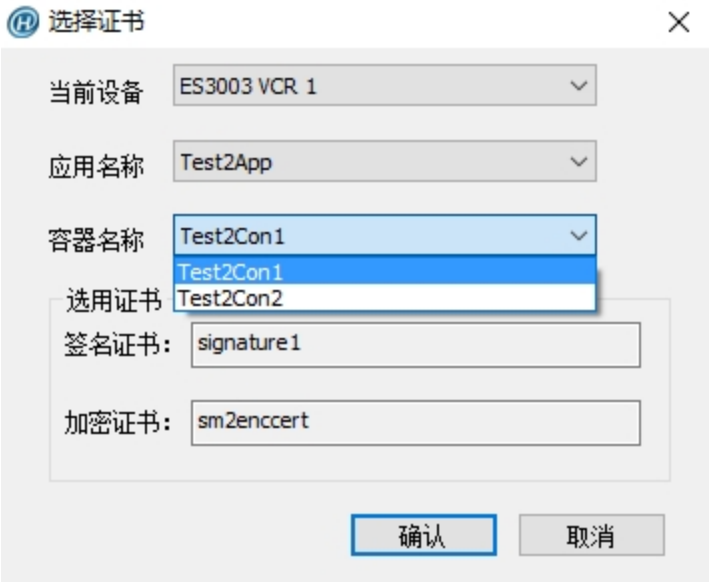
连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

使用“用户名/密码+数字证书”方式

当设备端配置“用户名/密码 + 数字证书”认证方式时，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将USB Token插入PC的USB接口。

2. 双击桌面的Hillstone Secure Connect快捷方式，或者点击“开始菜单”中的“所有程序→Hillstone Secure Connect→Hillstone Secure Connect”，系统弹出登录对话框。
点击“模式”按钮，系统弹出<登录模式>对话框。首先，在“国密SSL”部分，选中<用户名/密码 + 数字证书>单选按钮；如需要，点击“选择国密证书”按钮，在弹出的<选择证书>对话框中选择证书相关信息（如下图所示），最后，点击“确定”按钮。



当前设备：在下拉菜单中选择当前USB Token设备名称。

应用名称：应用是包含容器、设备认证密钥以及文件的一种结构。在下拉菜单选择指定的应用名称。

容器名称： 容器是USB Token设备中用于保存密钥所划分的唯一性存储空间。用来存储加密密钥对、与加密密钥对所对应的加密证书、签名密钥对、与签名密钥对所对应的签名证书。在下拉菜单选择指定的容器名称。

签名证书：显示指定容器内的SM2签名证书名称。

加密证书：显示指定容器内的SM2加密证书名称。

3. 系统弹出“用户名/密码 + 数字证书”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。

最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见Secure Connect设置部分）。如不选择，请依次填写以下各项。

服务器：填写设备端的IP地址。

端口：填写设备端的HTTPS端口号。

用户名：填写客户端用户名。

密码：填写与用户名相对应的密码。

PIN码：填写USB Token对应的用户口令。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

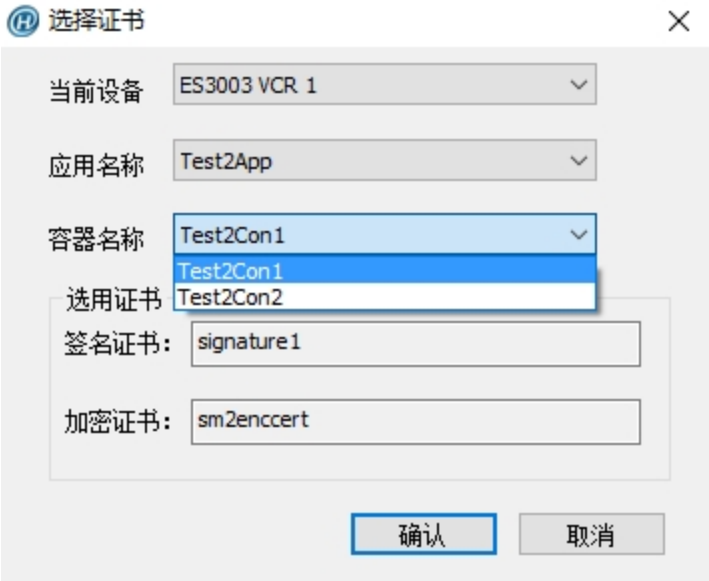
使用“只用数字证书”方式

当设备端配置“只用数字证书”认证方式时，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将USB Token插入PC的USB接口。

2. 双击桌面的Hillstone Secure Connect快捷方式，或者点击“开始菜单”中的“所有程序→Hillstone Secure Connect→Hillstone Secure Connect”，系统弹出登录对话框。
点击“模式”按钮，系统弹出<登录模式>对话框。首先，在“国密SSL”部分，选中<只用数字证书>单选按钮；如需要，点击“选择国密证书”按钮，在弹出的<选择证书>对话框中选择

证书相关信息（如下图所示），最后，点击“确定”按钮。



当前设备：在下拉菜单中选择当前USB Token设备名称。

应用名称：应用是包含容器、设备认证密钥以及文件的一种结构。在下拉菜单选择指定的应用名称。

容器名称：容器是USB Token设备中用于保存密钥所划分的唯一性存储空间。用来存储加密密钥对、与加密密钥对所对应的加密证书、签名密钥对、与签名密钥对所对应的签名证书。在下拉菜单选择指定的容器名称。

签名证书：显示指定容器内的SM2签名证书名称。

加密证书：显示指定容器内的SM2加密证书名称。

3. 系统弹出“只用数字证书”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。

最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见Secure Connect设置部分）。如不选择，请依次填写以下各项。

服务器：填写设备端的IP地址。

端口：填写设备端的HTTPS端口号。

PIN码：填写USB Token对应的用户口令。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标 。此时就可以通过SSL VPN实现加密通信。

通过计划任务启动并自动连接

SSL VPN客户端支持在用户登录系统前完成启动及连接。用户需要对SSL VPN客户端进行配置并创建计划任务。当通过计划任务启动并自动连接时，登录模式只支持“用户名/密码”认证方式。

通过SSL VPN客户端对自动连接进行相关的配置。

1. 双击桌面的Hillstone Secure Connect快捷方式，或者点击“开始菜单”中的“所有程序→Hillstone Secure Connect→Hillstone Secure Connect”，系统弹出登录对话框。
2. 右键单击系统通知栏区域的Hillstone Secure Connect图标。
3. 在左侧选项列表中选择登录信息。

    - **最近访问**：输入信息作为登录信息条目标识。用户可选择不填写。如果不填写，则在点击『应用』后，客户端根据服务器信息，端口信息，以及用户名称自动生成。生成后，用户可对其进行修改。

- **服务器**：填写设备端 的域名或IP地址。
- **端口**：填写设备端SCVPN实例的HTTPS端口号。
- **用户名**：填写需要连接的用户的用户名。
- **密码**：填写与用户名相对应的密码。
- **登录模式**：选择"密码"登录模式。当通过计划任务启动并自动连接时，登录模式只支持此种模式。
- **记住密码**：选中<记住密码>复选框使用记住密码功能。
- **最优通道**：选中该复选框开启最优路径检测功能。关于最优路径检测功能的详细信息，请参见《05-VPN》手册中的配置最优路径检测功能章节。

4. 点击『应用』，客户端保存此登录信息条目。

5. 在左侧选项列表中选择设置。在右侧配置区域选择<自动登录>。在登录用户下拉菜单中，选择登录信息条目。

6. 点击『应用』，保存配置。

通过创建计划，SCVPN客户端可以在指定的时间内完成启动。以Windows 7为例，介绍创建计划任务过程。

1. 点击开始菜单中的<控制面板>。在控制面板中依次进入”系统和安全→管理工具→计划任务”，系统弹出<任务计划程序>对话框。

2. 在<任务计划程序>对话框中，点击<创建基本任务>。系统弹出<创建基本任务向导>对话框。

3. 在<创建基本任务>页面，输入任务名称和描述。完成后点击『下一步』。

4. 在<触发器>，选择<计算机启动时>。

5. 在<操作>页面，选择<启动程序>。完成后点击『下一步』。

6. 在<启动程序>页面，点击『浏览』并选择SCVPN客户端执行程序SecureConnect.exe。默认路径为C:\Program Files (x86)\Hillstone\Hillstone Secure Connect\bin。

7. 在<添加参数>文本框中输入如下参数。

   - -l “C:\Users\Administrator\AppData\Roaming\Hillstone\Hillstone Secure Connect\ SecurecConfig.xml”
   - 参数中的C:\Users\Administrator\AppData\Roaming\Hillstone\Hillstone Secure Connect\ SecurecConfig.xml为用户Administrator的SCVPN客户端配置文件的默认路径。若当前为其他登录用户，请输入与当前用户匹配的路径。

8. 完成上述操作后后点击『下一步』。
9. 在<完成>页面，选择<当点击”完成”时，打开此任务属性的对话框>复选框。选择后点击『完成』。
10. 在弹出对话框中，选择<不管用户是否登录都要运行>单选框。选择后点击『完成』。系统弹出对话框要求指定运行此程序的用户及其密码。输入具有管理员权限的用户名及密码。
11. 点击『确认』完成配置。

完成上述配置后，SCVPN客户端即可在用户登录系统前完成启动及连接。

USB Key批量部署

Hillstone设备采用Hillstone UKey证书作为默认系统证书。使用默认系统证书进行认证时，客户端会自动选择默认系统证书传送至设备端，设备端对收到的数字证书进行认证，整个认证过程对用户来说是透明的，不需要用户手动进行证书选择。针对用户使用第三方USB Key进行SSL VPN客户端认证的情况，Hillstone提供USB Key批量部署工具SelectUSBKey。通过SelectUSBKey，用户能够将第三方USB Key证书设置为默认系统证书，从而简化认证时的操作过程。

通过SelectUSBKey将第三方USB Key证书设置为默认系统证书，用户首先要将USB Key的CSP Name信息以注册表文件的格式导出，然后将文件中的信息添加进客户端PC注册表。

请按照以下步骤导出USB Key的CSP Name信息：

1. 在PC中安装第三方USB Key驱动程序。
2. 插入第三方USB Key。

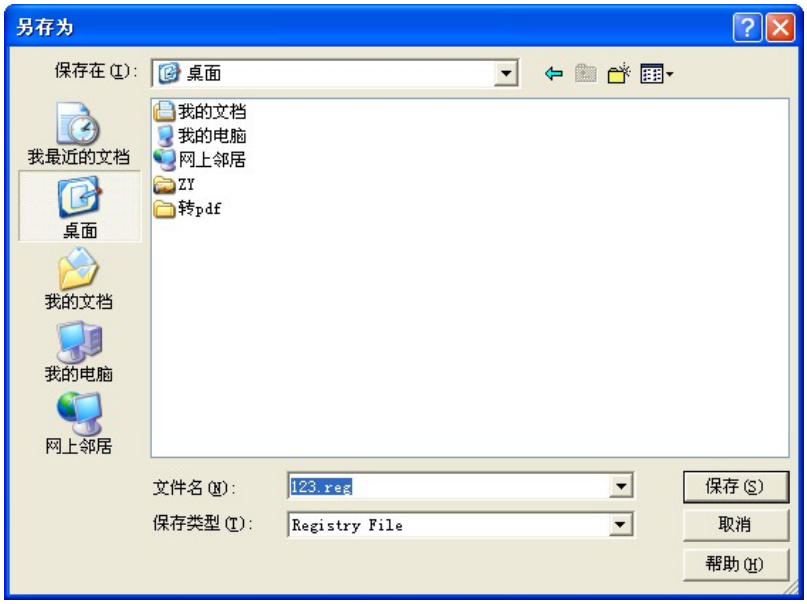
3. 双击SelectUSBKey.exe，系统弹出<Select Default Certificate>对话框。如下图所示：

Export：将USB Key的CSP Name以注册表文件（.reg）格式导出到本地目录。

Update：刷新证书列表。

Close：关闭对话框。

4. 在<Certificate List>中选中所需证书，点击『Export』按钮，将USB Key的CSP Name信息以注册表文件（.reg）格式导出到本地目录。如下图所示:



导出USB Key的CSP Name信息后，用户将信息文件存放在客户端PC目录中并双击该文件，将文件中的信息添加进客户端PC注册表。添加完成后，当用户通过该USB Key进行SSL VPN客户端认证时，客户端会自动选择USB Key中的数字证书传送至设备端，不需要用户手动选择证书。

客户端GUI

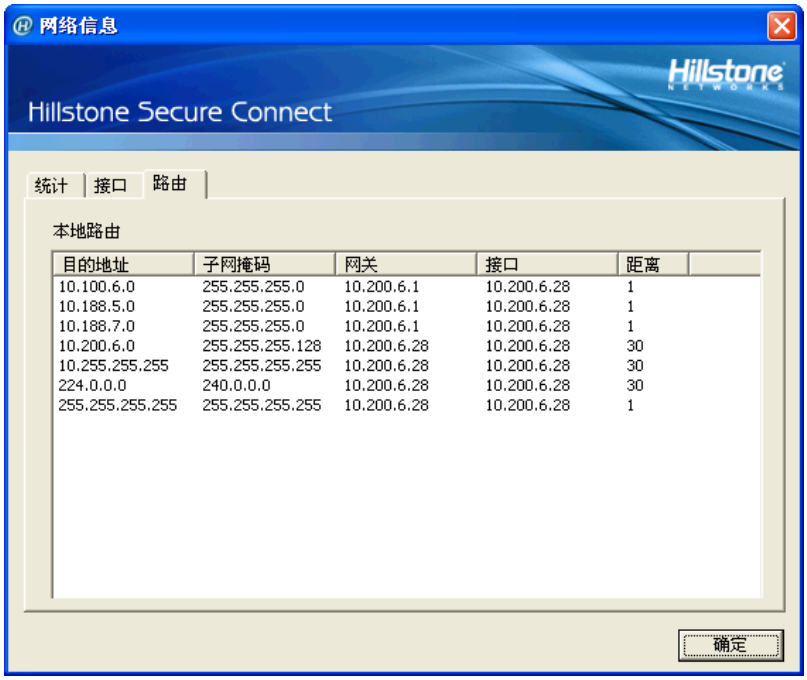
单机系统任务栏通知区域的Hillstone Secure Connect绿色的图标，系统弹出<网络信息>对话框。<网络信息>对话框显示统计信息、接口信息以及路由信息。下图为统计信息对话框：

地址信息:显示IP地址信息。	
服务器	显示客户端连接到的设备端的IP地址。
客户端	示当前客户端的IP地址。
加密信息:显示SSL VPN使用的加密与验证算法以及SSL版本信息。	
密码组合	依次显示SSL VPN使用的加密算法和验证算法。
版本	显示SSL PN使用的SSL协议版本。
连接状态:	
状态	显示客户端与设备端的当前连接状态。可能出现的状态包括：正在连接、已

地址信息:显示IP地址信息。	
	经连接、正在断开和断开。
IP压缩	
算法	显示客户端所使用的数据压缩算法。
隧道数据包数	
发送	显示通过SSL VPN隧道发送的数据包数。
接收	显示通过SSL VPN隧道接收的数据包数。
隧道数据字节数	
发送	显示通过SSL VPN隧道发送的数据字节数。
接收	显示通过SSL VPN隧道接收的数据字节数。
连接时间	
持续	显示客户端与设备端保持连接的时间。
压缩率	
发送	显示通过压缩算法处理后的发送数据长度百分比。
接收	显示通过压缩算法处理后的接收数据长度百分比。

点击<网络信息>对话框左上方的『接口』标签，系统将显示接口信息。如下图所示：

选项	说明
接口名称	显示SSL VPN客户端传送加密信息的接口的名称。
接口类型	显示SSL VPN客户端传送加密信息的接口的类型。
接口状态	显示SSL VPN客户端传送加密信息的接口的状态。
物理地址	显示SSL VPN客户端传送加密信息的接口的MAC地址。
IP地址类型	显示SSL VPN客户端传送加密信息的接口IP地址的类型。
网络地址	显示SSL VPN客户端传送加密信息的接口的IP地址（由设备端自动分配）。
子网掩码	显示SSL VPN客户端传送加密信息的接口的网络掩码。
默认网关	显示SSL VPN客户端传送加密信息的接口的默认网关地址。
DNS服务器地址	显示客户端使用的DNS服务器地址。
WINS地址	显示客户端使用的WINS服务器地址。



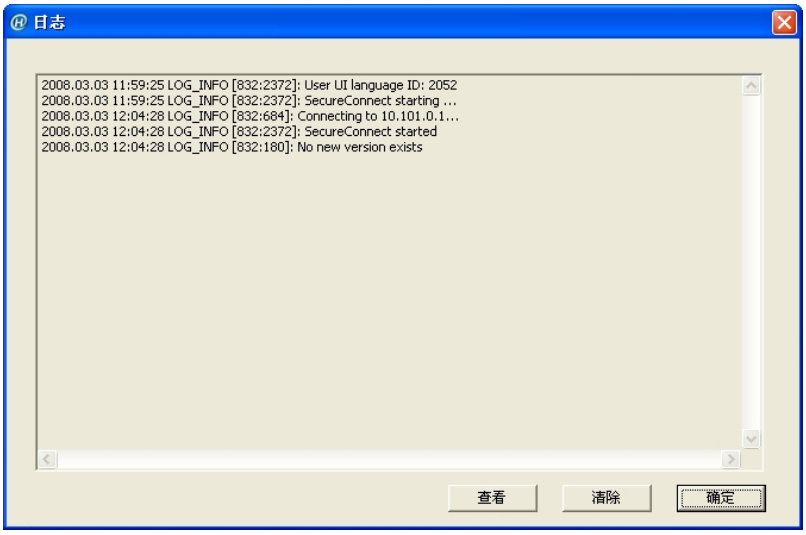
选项	说明
本地路由	显示通过虚拟网卡实现数据加密传输的路由条目信息。

客户端菜单

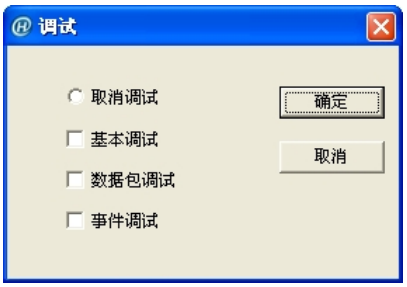
单击系统任务栏通知区域的Hillstone Secure Connect绿色的图标，系统弹出客户端菜单，如下图所示：

菜单项的作用如下：

- 网络信息：弹出<网络信息>对话框查看相关信息。
- 日志：弹出<日志>对话框显示Hillstone Secure Connect日志信息。如下图所示：



- 该对话框显示基本的日志信息，查看所有详细日志信息，点击对话框下方的『查看』按钮。点击『清除』按钮清除对话框的日志信息。点击『确定』按钮关闭<日志>对话框。
- 调试：弹出<调试>对话框，对客户端程序的调试功能进行配置。对话框如下图所示

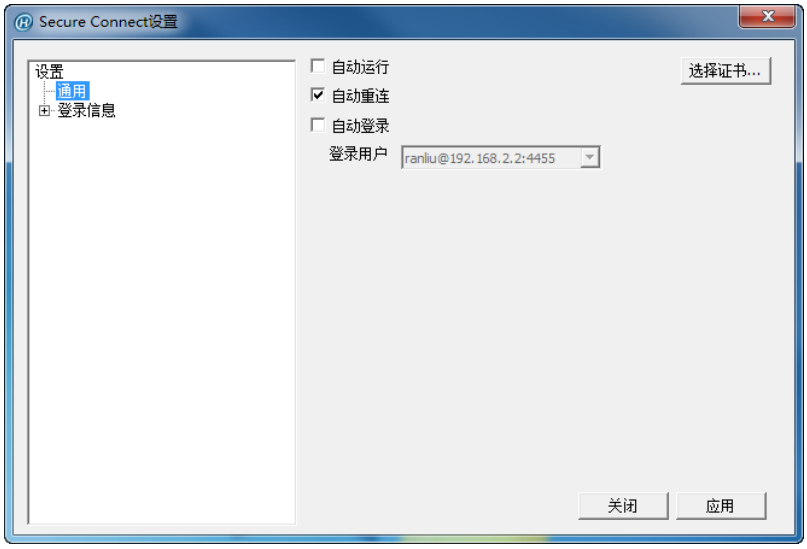


- 关于：弹出<关于Hillstone Secure Connect>对话框，显示Hillstone Secure Connect的版本、版权等相关信息。如下图所示：

- 连接：当客户端处于断开状态时，点击该选项弹出<登录>对话框，进行连接。
- 断开：当客户端处于连接状态时，点击该选项使客户端断开与设备端的连接。
- 选项：弹出<Secure Connect设置>对话框。通过该对话框，用户可以设置客户端的登录信息、自动运行和自动登录等。具体介绍请参见Secure Connect设置部分
- 退出：退出Hillstone Secure Connect客户端程序。

Secure Connect设置

点击客户端菜单中的<选项>，系统将弹出<Secure Connect设置>对话框。如下图所示：



通过该对话框，用户可以：

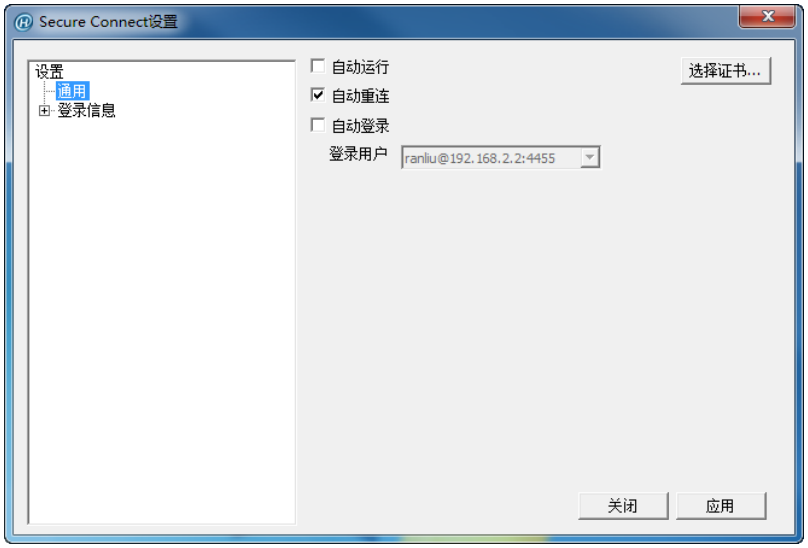
- 设置通用选项
- 添加登录信息条目
- 修改登录信息条目
- 删除登录信息条目

设置通用选项

在<Secure Connect设置>对话框，选中左侧导航栏中的<通用>节点，右方将显示可配置的通用选项，包括“自动运行”和“自动登录”：

- 自动运行：选中该选项，SSL VPN客户端将在PC系统启动时自动启动。
- 自动重连：选中该选项，SSL VPN客户端将在VPN连接中断时进行自动重连。
- 自动登录：选中该选项，SSL VPN将在PC系统启动时使用指定的用户名自动登录。从<登录用户>下拉菜单中选择自动登录用户名称。
- 选择证书：选中该选项，系统弹出<选择证书>对话框，用户可以通过该对话框选择USB Key认证证书，详细描述信息请参阅“直接启动”。该选项适用于设备端已开启USB Key证书

认证功能。



添加登录信息条目

为方便用户登录，用户可以配置登录信息条目。配置的登录信息条目将显示在<登录>对话框的<最近访问>下拉菜单中，供用户登录时选择。

按照以下步骤添加登录信息条目：

1. 选中<Secure Connect设置>对话框左侧导航栏的<登录信息>节点，右方将显示登录信息配置选项。参见下图：
2. 依次填写各选项。

    - **最近访问：**为所创建登录信息条目指定名称作为登录信息条目的标识。如果不指定该项，客户端会根据所填写的服务器、端口和用户信息自动生成该标识。
    - **服务器：**填写服务器端的IP地址。
    - **端口：**填写服务器端的HTTPS端口。
    - **用户：**填写用户名。
    - **登录模式：**在下拉菜单中选择登录模式，<密码>、<密码 + PIN>或<PIN>。<密码>表示使用“用户名/密码”认证方式，选中<记住密码>复选框使用记住密码功能，并在<密码>文本框中输入该用户对应的登录密码；<密码 + PIN>表示使用“用户名/密码 + USB Key”认证方式，选中<记住密码>复选框使用记住密码功能，并在

<密码>文本框中输入该用户对应的登录密码，选中<记住PIN码>复选框使用记住PIN码功能，然后在<PIN码>文本框中输入UKey对应的用户口令；<PIN>表示使用“只用USB Key”认证方式，选中<记住PIN码>复选框使用记住PIN码功能，然后在<PIN码>文本框中输入UKey对应的用户口令。

- **最优通道：**选中该复选框开启最优路径检测功能。关于最优路径检测功能的详细信息，请参见配置最优路径检测功能。

3. 填写完毕，点击对话框下方的『应用』按钮。

编辑登录信息条目

按照以下步骤对登录信息条目进行修改：

1. 选中<Secure Connect设置>对话框左侧导航栏的<登录信息>节点下需要修改的登录条目，右方将显示相应的登录信息配置选项。

2. 根据需要进行修改，然后点击对话框下方的『应用』按钮。
修改登录信息条目时，登录信息条目标识（即<最近访问>文本框中的字符串）不会随着其他信息的更改而变动。客户端通过对登录信息条目标识的比较来辨别登录信息条目的增加或修改：

- 如果修改了登录信息条目标识，则作为新增登录信息条目处理；
- 如果没有修改登录信息条目标识，则作为修改登录信息条目处理。

删除登录信息条目

用户可以使用以下两种方法删除登录信息条目：

- 选中左侧导航栏的登录信息条目标识，点击右键菜单的<删除用户>。
- 选中左侧导航栏的登录信息条目标识，点击右下方的『删除』按钮。

客户端的卸载

从PC上卸载Hillstone Secure Connect，从“开始菜单”点击“所有程序→Hillstone Secure Connect Uninstall”。

SSL VPN客户端 for Android

支持Android系统的SSL VPN客户端工具为Hillstone Secure Connect，可在Android 4.0以上系统环境中运行。Hillstone Secure Connect主要作用包括：

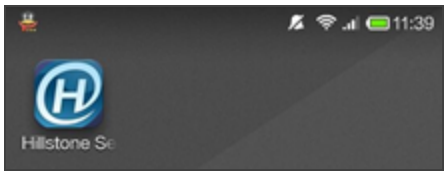
- 从所在Android系统中获得接口信息；
- 显示与设备端连接状态、数据流统计以及接口和路由信息；
- 显示应用程序日志信息。

下载与安装

下载和安装Hillstone Secue Connect，参照如下步骤：

1. 访问客户端下载页面：http://www.hillstonenet.com.cn/product/technology/VPN.html。
2. 在右侧边栏，用手机扫描Android客户端二维码。
3. 通过二维码扫描结果打开下载链接并下载安装文件Hillstone-Secure-Connect-Versione_Number.apk到手机。
4. 下载完成后，在手机存储器中找到该安装文件。
5. 点击该安装文件。弹出程序安装界面。
6. 阅读权限需求。
7. 点击“安装”按钮。

安装成功后会在Android系统中出现程序图标，如下图所示：



启动与登录

启动与登录客户端，按照以下步骤进行操作：

1. 点击Android系统桌面上的Hillstone Secure Connect图标，进入登录界面。

2. 依次填写对话框中的各项，然后点击“登入”按钮：

   - **请选择**：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见VPN连接配置管理部分）。如不选择，请依次填写以下各项。
   - **服务器**：填写设备端的IP地址或域名。
   - **端口**：填写设备端的HTTPS端口号。
   - **用户名**：填写登录用户名。
   - **密码**：填写与用户名相对应的密码。

3. 如果设备端开启短信口令认证功能，系统将弹出短信验证界面, 如下图所示。在该对话框中输入认证码，并点击“提交“按钮。如果用户在1分钟内没收到认证码短信，可以重新申请认

证码。

4. 连接成功后，Android系统通知栏显示钥匙形图标（ ），此时就可以实现客户端与设备端之间的加密通信。

GUI

客户端与设备端连接成功后，会自动进入功能界面。功能界面包括如下五个界面：连接状态、VPN连接配置管理、连接日志、系统配置和关于我们。

连接状态

点击客户端界面下方的<状态>标签，可进入<连接状态>界面。<连接状态>界面显示统计信息及路由信息。

- **连接时长**：显示版客户端与设备端保持连接的时间。
- **接收字节**：显示通过SSL VPN隧道接收的数据字节数。
- **发送字节**：显示通过SSL VPN隧道发送的数据字节数。
- **服务器地址**：显示客户端连接到的设备端的IP地址或域名。
- **端口**：显示客户端连接到的设备端的端口。
- **用户名**：显示客户端连接到的设备端的用户名。

- **服务器私有地址**：显示客户端连接到的设备端的接口的IP地址。
- **客户端私有地址**：显示客户端传送加密信息的接口的IP地址（由设备端自动分配）。
- **掩码地址**：显示客户端传送加密信息的接口的网络掩码。
- **DNS地址**：显示客户端使用的DNS服务器地址。
- **路由信息**：显示通过虚拟网卡实现数据加密传输的路由条目信息。
- **断开连接**：点击该按钮可以断开当前VPN连接。

VPN连接配置管理

点击客户端界面下方的<VPN>标签，可进入<VPN连接配置管理>界面。用户在此页面可执行以下操作：添加登录信息条目、编辑登录信息条目、删除登录信息条目、修改设备端登录密码、断开与设备端的连接，以及登入设备端。

添加登录信息条目

为方便用户登录，用户可以添加登录信息条目。添加的登录信息条目将显示在登录界面的请选择”下拉菜单中，供用户登录时选择。

按照以下步骤添加登录信息条目：

1. 点击<VPN连接配置管理>界面右上角的添加按钮( )，弹出<新建连接配置>对话框。

2. 依次填写各选项：

   - **连接名称**：为所创建登录信息条目指定名称。该名称作为登录信息条目的标识。
   - **服务器地址**：填写服务器端的IP地址或域名。
   - **端口**：填写服务器端的HTTPS端口。
   - **用户名**：填写登录用户名。

3. 编辑完毕，点击对话框下方的“确认”按钮保存配置。此登录信息条目将显示在登录界面的“请选择”下拉菜单中。

编辑登录信息条目

按照以下步骤编辑登录信息条目：

1. 点击列表中的某一个登录信息条目，登录信息条目下方显示多个按钮。
2. 点击“编辑”按钮，弹出<编辑VPN连接配置>对话框。
3. 在对话框中编辑各选项设置。
4. 编辑完毕，点击对话框下方的“确认”按钮保存配置。

删除登录信息条目

按照以下步骤删除登录信息条目：

1. 点击列表中的某一个登录信息条目，登录信息条目下方显示多个按钮。
2. 点击“删除”按钮，弹出提示框对删除操作进行确认。
3. 3点击提示框下方的“确认”按钮，删除此登录信息条目。

修改设备端登录密码

当设备端允许用户通过客户端修改登录密码时，可按照以下步骤修改：

1. 点击列表中的某一个登录信息条目，登录信息条目下方显示多个按钮。
2. 点击“修改密码”按钮，在弹出对话框中修改密码。
3. 点击提示框下方的“确认”按钮保存配置。

断开与设备端的连接/登入设备端

按照以下步骤断开与设备端的连接/登入设备端：

1. 点击VPN连接列表中的某一个登录信息条目，登录信息条目下方显示多个按钮。
2. 点击“断开连接”/“登入”按钮，弹出提示框对断开/登入连接操作进行确认。
3. 点击提示框下方的“确认”按钮，断开与设备端的连接/登入设备端。

连接日志

点击客户端界面下方的<日志>标签，可进入<连接日志>界面。该界面显示基本的日志信息。

系统配置

点击客户端界面下方的<配置>标签，可进入<系统配置>界面。通过该界面用户可以修改系统配置、登录配置和退出应用程序。

- **自动重连**：开启该选项，客户端将在断开连接时自动重新连接设备端。
- **显示通知**：开启该选项，客户端将在Android系统通知栏中显示客户端的图标。
- **允许休眠**：开启该选项，客户端在Android系统进入休眠状态时保持稳定连接。关闭该选项，客户端在Android系统进入休眠状态时可能断开连接且无法长时间保持连接。
- **自动登入**：选中该选项，客户端将在启动时自动登入上次连接的VPN。
- **记住密码**：选中该选项，客户端将记住用户的登录密码并自动填写登录密码。
- **退出**：退出客户端。

关于我们

点击客户端界面下方的<关于>标签，可进入<关于我们>界面。该界面显示客户端的版本、版权等相关信息。

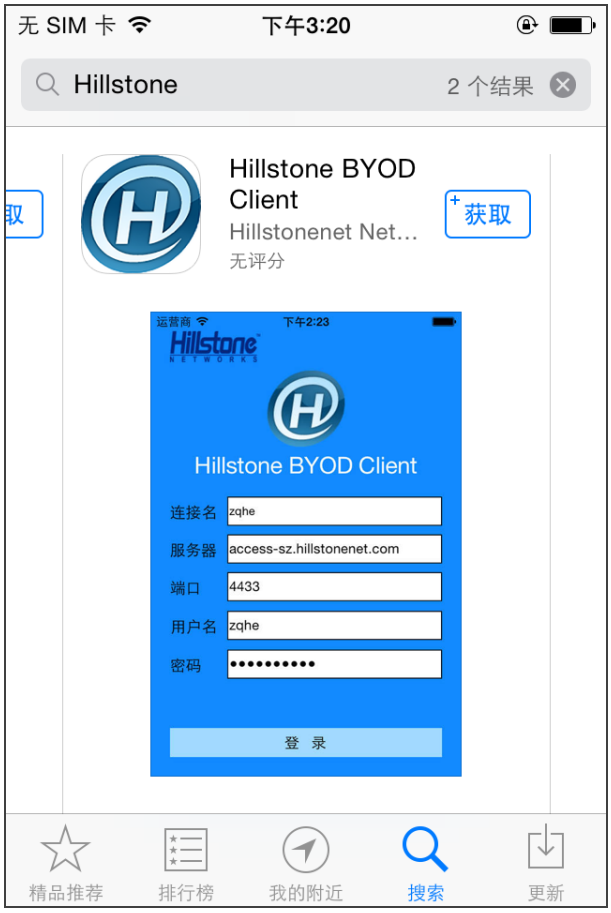
SSL VPN客户端 for iOS

支持iOS系统的SSL VPN客户端工具为Hillstone BYOD Client，可在iOS 6.0以上系统环境中运行。Hillstone BYOD Client的主要作用包括：

- 简化与设备端建立VPN的过程；
- 显示与设备端连接状态；
- 显示日志信息。

安装与建立连接

为使用客户端，用户需要从App Store搜索应用Hillstone BYOD Client并完成应用的安装。



应用安装完成后，需要使用Hillstone BYOD Client与设备端建立连接。对于首次登录，需要安装VPN配置文件。

注意: 卸载此应用后，再次安装后的登录也为首次登录；如果这5个登录参数中任何一个变化后进行登录，也为首次登录。

按照以下步骤与设备端建立连接：

1. 点击iOS系统桌面上的HBC图标，系统进入HBC的登录界面。
2. 依次填写对话框中的各项创建VPN连接实例，然后点击“登录”按钮。
   - **名称**：输入连接名称标示此VPN连接实例。
   - **服务器地址**：填写设备端的IP地址或域名。
   - **端口号**：填写设备端的HTTPS端口号。

- **用户名**：填写登录用户名。
- **密码**：填写与用户名相对应的密码。

3. 登录成功后，客户端与设备端成功建立连接。弹出Safari浏览器安装VPN配置文件。

4. 在<安装描述文件>对话框中，点击“安装”按钮。

5. 点击“安装”按钮后，弹出如下对话框。点击“现在安装”按钮。

6. 在<输入密码>页面中，输入iOS锁屏密码。密码输入正确后，iOS开始执行安装。

7. 完成安装后，在<已安装描述文件>对话框中，点击“完成”按钮。

此次安装的VPN配置文件根据第二步中的五个参数。如果此五个参数中的任意一个参数值发生变化，则被视为新的VPN连接实例。用户需要为新的VPN连接实例安装VPN配置文件。重新安装VPN配置文件，参照连接部分中的“导入连接配置”开关。

建立VPN连接

完成客户端与设备端的连接以及安装VPN配置文件后，用户可按照如下步骤建立客户端与设备端之间的VPN连接：

1. 打开iOS设置功能，点击“通用>VPN”。在<选择配置>列表中，选中需要连接的VPN名称，即在VPN配置中设置的连接名。

2. 打开VPN开关。iOS进行VPN连接。

3. 当iOS显示VPN连接成功且客户端在<连接状态>界面显示“当前已经连接”，表明客户端与设备端成功建立VPN连接。

注意: 如果不是首次登录，将不会进行VPN配置文件的安装。只需要登录客户端与设备端进行连接，并在iOS系统中完成VPN的连接，即可对客户端与设备端之间传输的数据进行加密。

GUI

客户端与设备端成功建立VPN连接后，进入客户端主界面。客户端包括如下三个界面：连接状态、日志、和关于我们。

连接

点击客户端界面下方的<连接>标签，可进入<连接状态>界面。<连接状态>界面显示当前连接状态。用户可在<连接状态>界面进行如下配置：

- 记住密码：开启此功能，将保存本次登录的密码。如果不开启，则下次登录需要输入密码。
- 断开连接/重新登录：断开客户端与设备端的连接，并断开VPN连接。点击“重新登录“进行连接。如果用户只在iOS系统中的“设置 > 通用 > VPN”中关闭VPN连接，将只会断开VPN连接，而不会断开客户端与设备端的连接，如需使用VPN加密通信，只需要打开VPN连接的开关。
- 导入连接配置：如果客户端可与设备端连接成功，但iOS VPN连接失败；或出现其他异常导致VPN无法连接成功，则需要重新部署VPN配置。打开“导入连接配置“开关，再次登录HBC，HBC将重新部署VPN配置。

日志

点击客户端界面下方的“日志”标签，可进入<连接日志>界面。该界面显示基本的日志信息。

关于我们

点击客户端界面下方的“关于”标签，可进入<关于我们>界面。该界面显示相关的版本、版权等相关信息。

SSL VPN

SSL VPN介绍

为解决远程用户安全访问私网数据的问题，Hillstone设备提供基于SSL的远程登录解决方案SSL VPN。SSL VPN功能可以通过简单易用的方法实现信息的远程连通。

StoneOS的SSL VPN功能包含设备端和客户端两部分。配置了SSL VPN功能的Hillstone设备作为设备端，具有以下功能：

- 接受客户端连接；
- 为客户端分配IP地址、DNS服务器地址和WINS服务器地址；
- 进行客户端用户的认证与授权；
- 进行客户端主机的安全检测；
- 对IPSec数据进行加密与转发。

Hillstone设备SSL VPN的客户端工具为Hillstone Secure Connect。用户可以通过浏览器下载该客户端，然后将其安装到PC，连接设备端成功后，用户就可以通过SSL VPN功能安全的传输数据信息。

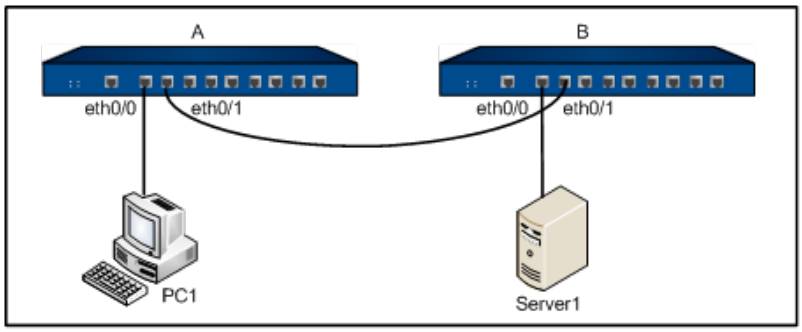
不同型号的Hillstone设备默认情况下支持的同时在线最大VPN客户端数不同，如果想增加支持的客户端数，请向代理商购买相应的许可证。

SSL VPN配置举例

该节介绍SSL VPN配置实例。分别针对用户名密码方式认证和USB Key认证方式进行进行举例。

组网需求

外网PC1（IP：6.6.6.5/24）通过Hillstone设备设备访问内网服务器Server1（IP：10.160.65.52/21），要求使用SSL VPN对数据进行加密。组网图参见下图：



- 需求一：使用用户名密码方式对用户进行认证。
- 需求二：使用USB Key方式对用户进行认证。

需求一配置步骤

第一步：创建本地用户：

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
hostname(config-user)# password 123456
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#exit
```

第二步：配置SSL VPN地址池：

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address 20.1.1.120.1.1.100 netmask
255.255.255.0
hostname(config-pool-scvpn)# dns 20.1.1.1
hostname(config-pool-scvpn)# wins 20.1.1.2
hostname(config-pool-scvpn)# exit
hostname(config)#
```

第三步：配置SSL VPN实例。系统默认添加split-tunnel-route 0.0.0.0/0的路由条目，如需限定远程用户访问范围，请使用no split-tunnel-route 0.0.0.0/0命令。

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/5
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.160.64.0/21
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

第四步：创建隧道接口并把SSL VPN实例绑定到此接口（隧道接口的IP地址必须与SSL VPN地址池的IP地址在同一网段）：

```
hostname(config)# zone VPN
hostname(config-zone-VPN)#
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# ip address 20.1.1.101/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

第五步：配置从VPN安全域到trust安全域的策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

第六步:在PC1的浏览器中输入https://6.6.6.1:4433，在弹出的登录页面输入用户名密码，分别是“user1”和“123456”。认证通过后下载并安装Hillstone Secure Connect。

第七步:通过Web方式或客户端方式登录SSL VPN设备端成功后，PC1便可通过SSL VPN安全地访问trust安全域中的资源。

需求二配置步骤

为了增加安全性，在需求一的基础上开启USB Key证书认证功能：只有当用户的USB Key支持标准的Windows SDK （Certificate Store Functions），并且存储的证书合法时，用户才可以登录设备。本例以用户持有Hillstone UKey为例。

准备工作

使用USB Key认证，用户需要做以下准备工作：

- 准备数字证书和相应的CA证书。
- 准备Hillstone UKey和配套光盘。
- 使用Hillstone UKey管理员软件导入数字证书到USB Key。

配置步骤

第一步：配置设备端：

```
#创建PKI信任域stone，并指定该信任域的证书获得方式为terminal
hostname(config)# pki trust-domain stone
hostname(config-trust-domain)# enrollment terminal
hostname(config-trust-domain)# exit
hostname(config)#
#开启SSL VPN实例SSL1的USB Key证书认证功能，并指定CA证书的信任域
```

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# client-cert-auth
hostname(config-tunnel-scvpn)# client-auth-trust-domain stone
hostname(config-tunnel-scvpn)# exit
hostname(config)#
#导入CA证书文件到CA证书的信任域
hostname(config)# exit
hostname# import pki stone cacert from tftp server 192.168.1.2
certnew.cer
```

第二步：客户端操作，步骤如下：

1. 在客户端PC安装Hillstone UKey驱动程序。

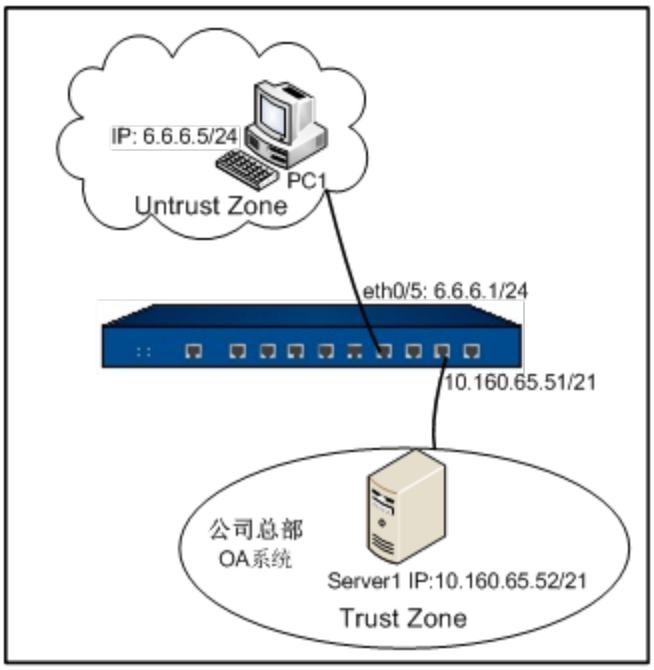
2. 插入USB Key。

3. 打开SSL VPN客户端，按下图所示依次填写登录信息（密码为“123456”；PIN码为USB Key的用户口令，默认为1111）。填写完毕，点击『登录』按钮，进行连接。

URL重定向配置举例

某公司总部有一套OA系统，并且选用一台Hillstone设备作为SSL VPN设备端。现要求通过配置，实现客户端在登录SSL VPN的同时成功登录OA系统。

该实例通过配置URL重定向功能实现上述需求。组网图参见下图。



配置步骤

第一步：创建本地用户：

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user test
hostname(config-user)# password test
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

第二步：配置SSL VPN地址池：

```
hostname(config)# scvpn pool pool1
```

```
hostname(config-pool-scvpn)# address 20.1.1.120.1.1.255 netmask
255.255.255.0
hostname(config-pool-scvpn)# dns 20.1.1.1
hostname(config-pool-scvpn)# wins 20.1.1.2
hostname(config-pool-scvpn)# exit
hostname(config)#
```

第三步：配置SSL VPN实例，并在实例中配置URL重定向功能。系统默认添加split-tunnel-route 0.0.0.0/0的路由条目，如需限定远程用户访问范围，请使用no split-tunnel-route 0.0.0.0/0命令。

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/5
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# redirect-url
http://192.10.5.201/oa/login.do?username=$USER&password=$PWD
title-en OA title-zh 中文OA系统
hostname(config-tunnel-scvpn)# split-tunnel-route 10.160.64.0/21
hostname(config-tunnel-scvpn)# split-tunnel-route 192.10.5.0/24
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

第四步：创建隧道接口并把SSL VPN实例绑定到此接口（隧道接口的IP地址必须与SSL VPN地址池的IP地址在同一网段）：

```
hostname(config)# zone VPN
hostname(config-zone-VPN)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# ip address 20.1.1.1/24
```

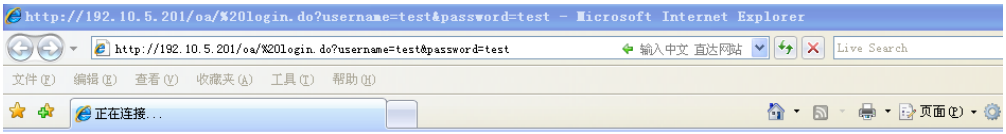
```
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

第五步：配置从VPN安全域到trust安全域的策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

第六步：在PC1的浏览器中输入https://6.6.6.1:4433，在弹出的登录页面输入用户名密码，分别是“test”和“test”。认证通过后下载并安装Hillstone Secure Connect。

第七步：通过Web方式或客户端方式登录SSL VPN设备端成功后，客户端自动跳转到OA系统认证页面并成功登录；同时，客户端菜单中增加“中文OA系统”菜单项，参见图下图：



当OA系统认证页面关闭后，用户可以点击“中文OA系统”菜单项，再次打开OA系统认证页面。

主机安全检测配置举例

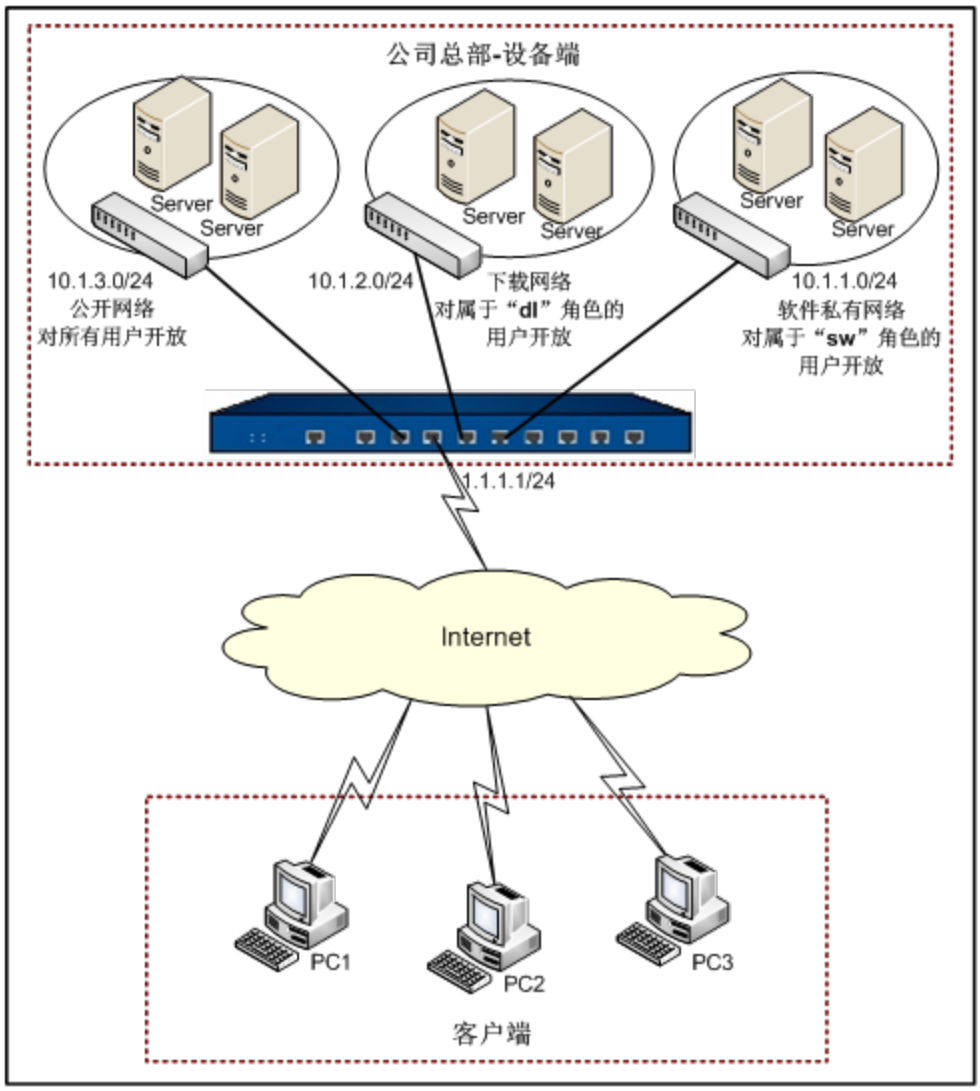
该节介绍SSL VPN主机安全检测配置实例。

组网需求

外网PC通过Hillstone设备设备访问公司总部资源，需要组建SSL VPN网络并配置主机安全检测功能，以达到以下目的：

- 客户端PC通过SSL VPN访问公司总部资源；
- 公司总部的软件私有网络网段（IP：10.1.1.0/24）的资源只允许属于角色“sw”的用户访问；总部下载网络网段（IP：10.1.2.0/24）的资源只允许属于角色“dl”的用户访问；总部公开网络网段（IP：10.1.3.0/24）的资源允许所有的用户访问；
- 对访问总部资源的客户端PC进行主机安全检测，并根据检测结果授予相应的资源访问权限。

组网图参见下图：



配置步骤

第一步：创建本地用户：

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user pc1
hostname(config-user)# password xxxfcvg236
hostname(config-user)# exit
hostname(config-aaa-server)# user pc2
```

```
hostname(config-user)# password xcabuv112
hostname(config-user)# exit
hostname(config-aaa-server)# user pc3
hostname(config-user)# password xacfomg763
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

第二步：配置角色映射规则：

```
hostname(config)# role sw
hostname(config)# role dl
hostname(config)# role-mapping-rule rule1
hostname(config-role-mapping)# match user pc1 role sw
hostname(config-role-mapping)# match user pc1 role dl
hostname(config-role-mapping)# match user pc2 role dl
hostname(config-role-mapping)# exit
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# role-mapping-rule rule1
hostname(config)#
```

第三步：配置设备端接口：

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第四步：配置主机安全检测Profile（请通过WebUI配置相应的Profile文件）：

```
hostname(config)# scvpn host-check-profile dl-security-check
```

```
hostname(config-profile_scvpn)# exit
hostname(config)# scvpn host-check-profile sw-security-check
hostname(config-profile_scvpn)# exit
hostname(config)#
```

通过WebUI配置主机安全检测Profile，指定主机安全检测内容如下：

1. 从页面左侧导航树选择并点击“配置⑥网络⑥SSL VPN”，进入SSL VPN页面。
2. 从页面右侧辅助栏的<任务>区选择『主机检测』链接，进入SSL VPN的主机检测页面。
3. 点击主机检测规则列表左上角的『新建』按钮，弹出<主机检测配置>对话框。在『基本配置』标签页，进行如下配置：
    - 名称：dl-security-check
    - OS版本：依次从下拉菜单中选择“至少”、“Win2003”、“无”
    - 补丁包1：KB958215
    - 最低IE版本：IE6.0
    - 最低IE安全级别：高
4. 在『高级配置』标签页，进行如下配置：
    - 安全中心：勾选“必须启用”
    - 防病毒软件：依次勾选“安装软件”、“实时监控”、“病毒库更新”
    - 防间谍软件：依次勾选“安装软件”、“实时监控”、“特征库更新”
    - 防火墙：依次勾选“安装软件”、“实时监控”
5. 点击『确定』按钮，保存所做配置并返回上一级对话框/页面。
6. 点击主机检测规则列表左上角的『新建』按钮，弹出<主机检测配置>对话框。在『基本配置』标签页，进行如下配置：
    - 名称：sw-security-check
    - OS版本：依次从下拉菜单中选择“必须匹配”、“WinXP”、“SP3”

- 补丁包1：KB921883
- 最低IE版本：IE7.0
- 最低IE安全级别：高

7．在『高级配置』标签页，进行如下配置：

- 安全中心：勾选“必须启用”
- 自动更新：勾选“必须启用”
- 防病毒软件：依次勾选“安装软件”、“实时监控”、“病毒库更新”
- 防间谍软件：依次勾选“安装软件”、“实时监控”、“特征库更新”
- 防火墙：依次勾选“安装软件”、“实时监控”
- 文件路径名称：在<文件1>下拉菜单中选择“存在”并在文本框中输入“C:\Program Files\McAfee\VirusScan\Enterprise.exe”

8．点击『确定』按钮，保存所做配置并返回上一级对话框/页面。

第五步：配置SSL VPN地址池：

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address11.1.1.10 11.1.1.100 netmask
255.255.255.0
hostname(config-pool-scvpn)# dns 10.1.1.1
hostname(config-pool-scvpn)# wins 10.1.1.2
hostname(config-pool-scvpn)# exit
hostname(config)#
```

第六步：配置SSL VPN实例。系统默认添加split-tunnel-route 0.0.0.0/0的路由条目，如需限定远程用户访问范围，请使用no split-tunnel-route 0.0.0.0/0命令。

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
```

```
hostname(config-tunnel-scvpn)# interface ethernet0/1
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.1.0/24 metric 10
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.2.0/24 metric 5
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.3.0/24 metric 3
hostname(config-tunnel-scvpn)# host-check role sw profile sw-security-check guest-role dl
hostname(config-tunnel-scvpn)# host-check profile dl-security-check periodic-check 50
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

第七步：创建隧道接口并把SSL VPN实例绑定到此接口（隧道接口的IP地址必须与SSL VPN地址池的IP地址在同一网段）：

```
hostname(config)# zone VPN
hostname(config-zone-VPN)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# ip address11.1.1.1/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

第八步：配置策略规则：

```
hostname(config)# address sw
hostname(config-addr)# ip 10.1.1.0/24
```

```
hostname(config-addr)# exit
hostname(config)# address dl
hostname(config-addr)# ip 10.1.2.0/24
hostname(config-addr)# exit
hostname(config)# address public
hostname(config-addr)# ip 10.1.3.0/24
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr sw
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role sw
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr dl
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role dl
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr public
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

客户端PC发起SSL VPN连接请求并通过认证后，设备端会根据配置的安全检测策略规则对客户端进行安全检测，并根据检测结果授予客户端用户相应的资源访问权限。本示例的主机安全检测策略规则配置以及资源访问权限授予之间的对应关系，请参见下表：

用户	策略规则配置	检测结果	
		未通过检测	通过检测
PC1	初级角色：sw profile：sw-security-check 次级角色：dl 自动检测周期：默认30分钟 CLI：**host-check role sw profile sw-security-check guest-role dl**	可以访问软件私有网络并且每隔30分钟自动进行安全检测	可以访问下载网络并且每隔30分钟自动进行安全检测
PC2	初级角色：未配置（根据default角色“dl”授予权限） profile：dl-security-check 次级角色：未配置 自动检测周期：50分钟 CLI：**host-check profile dl-security-check periodic-check 50**	可以访问下载网络并且每隔50分钟自动进行安全检测	断开连接
PC3	初级角色：未配置 profile：dl-security-check 次级角色：未配置 自动检测周期：50分钟 CLI：**host-check**	可以访问公开网络并且每隔50分钟自动进行安全检测	断开连接

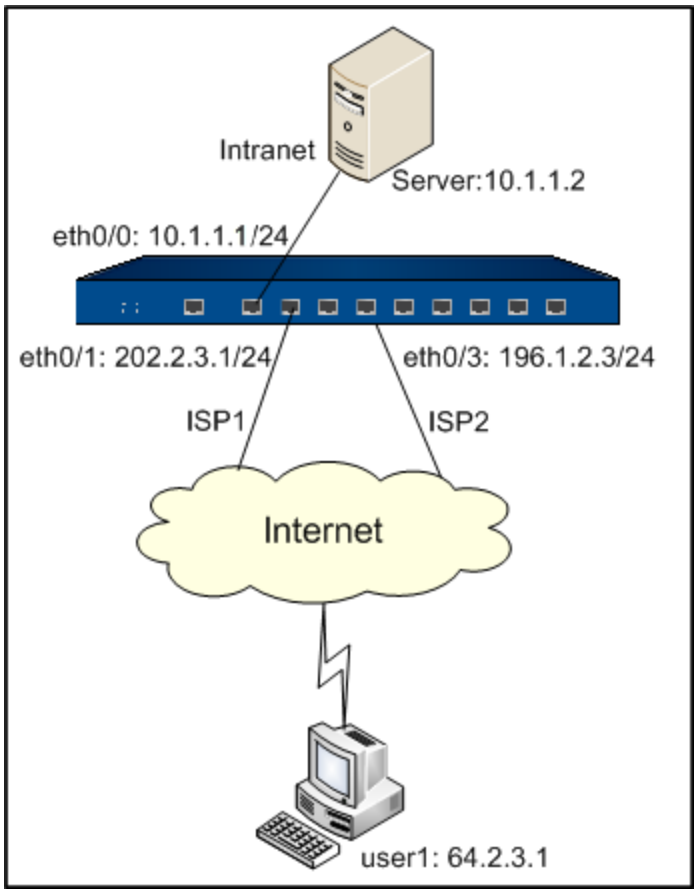
用户	策略规则配置	检测结果	
		未通过检测	通过检测
	profile dl-security-check periodic-check 50		

最优路径检测配置举例

该节介绍SSL VPN最优路径检测配置实例。

组网需求一

某公司总部选用一台Hillstone设备作为SSL VPN设备端，并通过两条不同的上网线路ISP1（接口ethernet0/1，IP：202.2.3.1/24）和ISP2（接口ethernet0/3，IP：196.1.2.3/24）接入Internet。现要求通过配置，实现客户端PC（IP：64.2.3.1）通过最优路径检测功能访问公司总部Server（IP：10.1.1.2）。组网图参见下图：



该需求有两种配置方式，分别是：

- 设备端作最优通道判断
- 客户端判断最优通道

设备端作最优通道判断

第一步：创建本地用户：

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user user1
hostname(config-user)# password drgrhrgerg231
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

第二步：配置设备端接口：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.0/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.2.3.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone untrust
hostname(config-if-eth0/3)# ip address 196.1.2.3/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

第三步：配置SSL VPN地址池：

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address 11.1.1.10 11.1.1.100 netmask
255.255.255.0
hostname(config-pool-scvpn)# dns 10.1.1.1
hostname(config-pool-scvpn)# wins 10.1.1.2
hostname(config-pool-scvpn)# exit
hostname(config)#
```

第四步：配置SSL VPN实例（在SSL VPN实例中配置最优路径检测功能）。系统默认添加split-tunnel-route 0.0.0.0/0的路由条目，如需限定远程用户访问范围，请使用no split-tunnel-route 0.0.0.0/0命令。

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/1
hostname(config-tunnel-scvpn)# interface ethernet0/3
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.1.0/24 met-
ric 10
hostname(config-tunnel-scvpn)# link-select server-detect
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

第五步：创建隧道接口并把SSL VPN实例绑定到此接口（隧道接口的IP地址必须与SSL VPN地址池的IP地址在同一网段）：

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 11.1.1.1/24
hostname(config-if-tun1)# tunnel scvpn ssl1
```

```
hostname(config-if-tun1)# exit
hostname(config)#
```

第六步：配置策略规则：

```
hostname(config)# address dst
hostname(config-addr)# ip 10.1.1.0/24
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

第七步：配置ISP信息：

```
hostname(config)# isp-network isp1
hostname(config-isp)# subnet 202.2.3.0/24
hostname(config-isp)# subnet 64.2.3.0/24
hostname(config-isp)# exit
hostname(config)#
```

当客户端PC通过ISP2向设备端发起连接请求时，设备端判断客户端PC的IP地址与SSL VPN出接口ethernet0/1的IP地址同属于ISP1，根据判断，将带有优先级的出接口IP地址下发给客户端，最终，客户端PC将选择通过ISP1访问公司总部Server。

客户端判断最优通道

此种情况下的配置与设备端作最优通道判断中的配置基本相似，不同在于：

第四步：配置SSL VPN实例（在SSL VPN实例中配置最优路径检测功能）：

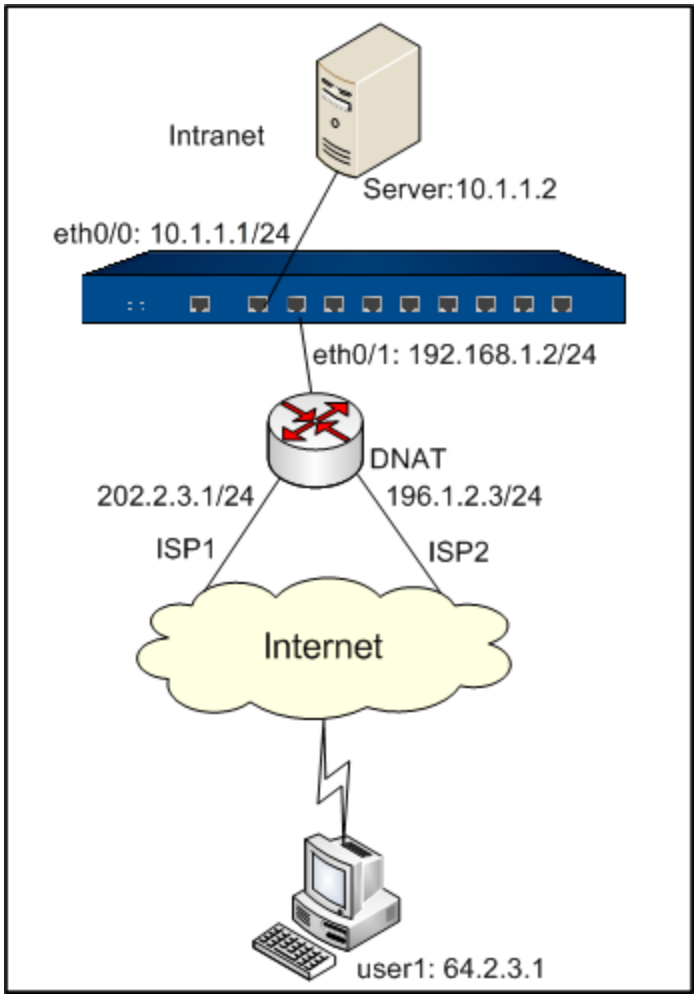
```
hostname(config)# tunnel scvpn ssl1

……

hostname(config-tunnel-scvpn)# link-select

……
```

第七步：无（不需配置）

当客户端PC通过ISP2向公司总部发起连接请求时，设备端会将SSL VPN出接口ethernet0/1和ethernet0/3的IP地址下发给客户端，客户端通过发送UDP探测包自动判断最优通道。

组网需求二

某公司总部选用一台Hillstone设备作为SSL VPN设备端，并通过一台DNAT设备经由两条不同的上网线路ISP1（IP：202.2.3.1/24）和ISP2（IP：196.1.2.3/24）接入Internet。现要求通过配置，实现客户端PC（IP：64.2.3.1）通过最优路径检测功能访问公司总部Server（IP：10.1.1.2）。组网图参见下图：



该需求有两种配置方式，分别是：

- 设备端作最优通道判断
- 客户端判断最优通道

设备端作最优通道判断

第一步：创建本地用户：

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user user1
hostname(config-user)# password drgrhrgerg231
hostname(config-user)# exit
hostname(config-aaa-server)# exit
```

```
hostname(config)#
```

第二步：配置设备端接口：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.0/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 192.168.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第三步：配置SSL VPN地址池：

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address 11.1.1.10 11.1.1.100 netmask
255.255.255.0
hostname(config-pool-scvpn)# dns 10.1.1.1
hostname(config-pool-scvpn)# wins 10.1.1.2
hostname(config-pool-scvpn)# exit
hostname(config)#
```

第四步：配置SSL VPN实例（在SSL VPN实例中配置最优路径检测功能）。系统默认添加split-tunnel-route 0.0.0.0/0的路由条目，如需限定远程用户访问范围，请使用no split-tunnel-route 0.0.0.0/0命令。

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/1
```

```
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route10.1.1.0/24 met-
ric 10
hostname(config-tunnel-scvpn)# link-select server-detect 202.2.3.1
https-port 2234 196.1.2.3 https-port 3367
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

第五步：创建隧道接口并把SSL VPN实例绑定到此接口（隧道接口的IP地址必须与SSL VPN地址池的IP地址在同一网段）：

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 11.1.1.1/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

第六步：配置策略规则（从dmz到trust安全域的策略）：

```
hostname(config)# address dst
hostname(config-addr)# ip 10.1.1.0/24
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone dmz
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
```

```
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

第七步：配置ISP信息：

```
hostname(config)# isp-network isp1
hostname(config-isp)# subnet 202.2.3.0/24
hostname(config-isp)# subnet 64.2.3.0/24
hostname(config-isp)# exit
hostname(config)#
```

当客户端PC通过ISP2向DNAT设备发起连接请求时，DNAT设备会将客户端的访问地址196.1.2.3:3367映射到SSL VPN设备端的出接口地址192.168.1.2:4433。此时，设备端判断客户端PC的IP地址与DNAT外网接口IP地址202.2.3.1/24同属于ISP1，根据判断，将带有优先级的DNAT外网接口IP地址下发给客户端，最终，客户端PC将选择通过ISP1访问公司总部Server。

客户端判断最优通道

此种情况下的配置与设备端作最优通道判断中的配置基本相似，不同在于：

第四步：配置SSL VPN实例（在SSL VPN实例中配置最优路径检测功能）：

```
hostname(config)# tunnel scvpn ssl1
……
hostname(config-tunnel-scvpn)# link-select 202.2.3.1 https-port
2234 196.1.2.3 https-port 3367
……
```

第九步:无（不需配置）

当客户端PC通过ISP2向公司总部发起连接请求时，DNAT设备会将客户端的访问地址196.1.2.3:3367映射到SSL VPN设备端的出接口地址192.168.1.2:4433。设备端会将DNAT外网接口IP地址下发给客户端，客户端通过发送UDP探测包自动判断最优通道。

拨号VPN

拨号VPN介绍

拨号VPN指，在中心设备上仅配置一个VPN隧道，之后允许多个远程拨号端通过VPN隧道访问中心设备。远程拨号端需配置与中心设备VPN隧道对应的IKE VPN，进行数据保护。同时，中心设备通过预共享密钥或者证书认证方式，认证拨号端的身份，从而建立与拨号端的VPN隧道。

拨号VPN的应用

StoneOS通过“基于策略的VPN”和“基于路由的VPN”两种方式把配置好的VPN隧道应用到Hillstone设备上，实现流量的加密解密安全传输。

- 基于策略的VPN：将配置成功的VPN隧道名称引用到策略规则中，使符合条件的流量通过指定的VPN隧道进行传输。此方式只支持分支机构访问中心，不支持中心访问分支机构以及Hub-and-spoke。
- 基于路由的VPN：将配置成功的VPN隧道与隧道接口绑定；配置静态路由时，将隧道接口指定为下一跳路由。

中心设备配置

拨号VPN的中心设备配置包括：

- 配置P1提议
- 配置ISAKMP网关
- 配置P2提议
- 配置隧道
- 配置拨号端用户信息

配置P1提议

P1提议是IKE安全提议，可应用到ISAKMP网关上，在SA第一阶段使用。对IKE安全提议的配置包括指定认证方式、加密算法、验证算法、DH组和安全联盟的生命周期。

创建P1提议

创建一个P1提议，即IKE安全提议，请在全局配置模式下使用以下命令：

isakmp proposal *p1-name*

- *p1-name* – 指定所创建的P1提议的名称。执行该命令后，CLI进入到P1提议配置模式。用户可以在该模式下对P1提议进行参数配置。

使用**no isakmp proposal** *p1-name*命令删除指定的P1提议。

指定认证方式

此处指定的是IKE身份认证的方式。身份认证用来确认通信双方的身份。方式有两种：预共享密钥认证和数字证书认证。对于预共享密钥认证方式，认证字用来作为一个输入产生密钥，认证字不同是不可能在双方产生相同的密钥的。指定IKE安全提议的身份认证方式，在P1提议配置模式下使用以下命令：

authentication {**pre-share** | **rsa-sig** | **dsa-sig**}

- **pre-share** – 指定使用预共享密钥认证方式。该方式为默认认证方式。
- **rsa-sig** – 指定使用RSA数字证书认证方式。
- **dsa-sig** – 指定使用DSA数字证书认证方式。此方式对应的验证算法只能为SHA-1。

使用**no authentication**命令恢复默认认证方式。

指定加密算法

StoneOS提供以下五种加密算法：3DES、DES、128bit AES、192bit AES以及256bit AES。指定IKE安全提议的加密算法，在P1提议配置模式下使用以下命令：

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256**}

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为StoneOS系统默认方法。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。

- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。

使用**no encryption**命令恢复默认加密算法。

指定验证算法

StoneOS支持以下验证算法：MD5、SHA-1和SHA-2（包括SHA-256、SHA-384和SHA-512）。指定IKE安全提议的验证算法，在P1提议模式下使用以下命令：

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为StoneOS的默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** – 指定使用SHA-512验证算法。摘要为512比特。

使用**no hash**命令恢复默认认证方式。

选择DH组

Diffie-Hellman（DH）是一种建立密钥的方法。DH组决定DH交换中密钥生成“材料”的长度。密钥的牢固性部分决定于DH组的强度。密钥“材料”长度越长，所生成的密钥安全度也就越高，越难被破译。DH组的选择很重要，因为DH组只在第一阶段的SA协商中确定，第二阶段的协商不再重新选择DH组，两个阶段使用的是同一个DH组，因此该DH组的选择将影响所有会话密钥的生成。在协商过程中，两个ISAKMP网关间应选择同一个DH组，即密钥“材料”长度应该相等。若DH组不匹配，将协商失败。

选择DH组，在P1提议配置模式下使用以下命令：

group {**1** | **2** | **5** | **14** | **15** |**16**}

- **1** – 选择DH组1。密钥的长度为768比特。
- **2** – 选择DH组2。密钥的长度为1024比特。2为系统默认值。

- **5** – 选择DH组5。密钥的长度为1536比特。
- **14** – 选择DH组14。密钥的长度为2048比特。
- **15** – 选择DH组15。密钥的长度为3072比特。
- **16** – 选择DH组16。密钥的长度为4096比特。

使用**no group**命令恢复默认DH组。

指定安全联盟的生命周期

第一阶段SA有一个默认的生命周期，如果ISAKMP SA生命期时间到，要向对方发送第一阶段SA删除消息，通知对方第一阶段SA已经过期。之后需要重新进行SA协商。指定安全联盟的生命周期，在P1提议配置模式下使用以下命令：

lifetime *time-value*

- *time-value* – 指定SA第一阶段的生命周期长度，单位为秒。默认86400秒。范围是300到86400秒。

使用**no lifetime**命令恢复默认生命周期长度。

配置ISAKMP网关

创建一个ISAKMP网关后，用户可以指定ISAKMP网关的认证服务器、IKE协商模式、ISAKMP网关IP地址及类型、IKE安全提议、预共享密钥、PKI信任域、本地ID、ISAKMP网关ID 、ISAKMP网关连接方式以及是否开启ISAKMP网关的NAT穿越功能等。

创建ISAKMP网关

创建ISAKMP网关，在全局配置模式下，使用以下命令:

isakmp peer *peer-name*

- *peer-name* – 指定ISAKMP网关的名称。

执行该命令后，CLI进入到ISAKMP网关配置模式。用户可以在该模式下对ISAKMP网关进行参数配置。

在全局配置模式下使用**no isakmp peer** *peer-name*命令删除指定的ISAKMP网关。

指定ISAKMP网关的认证服务器

此处指定的认证服务器用来对拨号端的设备进行身份认证。指定ISAKMP网关的认证服务器，在ISAKMP网关配置模式下，使用以下命令：

aaa-server *server-name*

- *server-name* – 指定认证服务器的名称。支持“local”、Radius、AD、LDAP和TACACS+认证服务器。

在ISAKMP网关配置模式下使用该命令no的形式取消认证服务器的指定：

no aaa-server

绑定接口到ISAKMP网关

用户可以绑定某个接口到ISAKMP网关。将接口绑定到ISAKMP网关，在ISAKMP网关配置模式下使用以下命令：

interface *interface-name*

- *interface-name* – 指定被绑定接口的名称。

使用**no interface**命令取消接口绑定。

配置IKE协商模式

IKE的协商模式有两种：主模式（main mode）和野蛮模式（aggressive mode）。IKE野蛮模式不提供身份保护，以下情况推荐使用野蛮模式：中心设备的IP地址为固定分配的地址，而客户端设备的IP地址为动态获取的地址。配置IKE协商模式，在ISAKMP网关配置模式下使用以下命令：

mode {**main** | **aggressive**}

- **main** – 指定使用主模式，可提供ID保护功能。该模式为系统的默认模式。
- **aggressive** – 指定使用野蛮模式。

使用**no mode**命令恢复默认协商模式。

指定对端类型

用户可以为所创建的ISAKMP网关指定对端的类型。指定对端的类型，请在ISAKMP网关配置模式下使用以下命令：

type usergroup

在ISAKMP网关配置模式下使用该命令no的形式恢复默认配置：

no type

指定P1提议

为ISAKMP网关指定P1提议，在ISAKMP网关配置模式下使用以下命令：

isakmp-proposal p1-proposal1[p1-proposal2] [p1-proposal3] [p1-proposal4]

- **p1-proposal1** – 指定P1提议的名称。用户最多可以为ISAKMP网关指定4个P1提议供对端选择使用。

使用**no isakmp-proposal**取消对P1提议的指定。

配置预共享密钥

如果使用预共享密钥认证方式，用户就需要指定预共享密钥。为ISAKMP网关指定预共享密钥，在ISAKMP网关配置模式下使用以下命令：

pre-share *string*

- *string* – 指定预共享密钥的内容。

使用**no pre-share**取消对预共享密钥的指定。

配置PKI信任域

如果使用数字证书认证方式，用户就需要指定数字证书的PKI信任域。为ISAKMP网关指定PKI信任域，在ISAKMP网关配置模式下使用以下命令：

trust-domain *string*

- *string* – 指定PKI信任域。

使用**no trust-domain**取消对PKI信任域的指定。

提示: 关于如何配置PKI信任域，请参阅《用户认证》的“PKI配置”部分。

配置本端ID

配置本端的ID，请在ISAKMP网关配置模式下使用以下命令：

local-id {**fqdn** *string* | **asn1dn** [*string*] | **u-fqdn***string* }

- **fqdn** *string* – 指定使用FQDN类型的ID。string为ID的具体内容。
- **asn1dn** [*string*] – 指定使用Asn1dn类型的ID，该类型只可应用于使用证书的情况。string为ID的具体内容。用户可以不指定ID的具体内容，在此种情况下，系统将从证书中获取ID。
- **u-fqdn** *string* – 指定使用U-FQDN类型的ID，即电子邮件地址类型，例如user-1@hillstonenet.com。

使用**no local-id**命令取消对本端ID的配置。

指定连接类型

创建的ISAKMP网关可以是发起端、响应端或者既是发起端也是响应端。指定ISAKMP网关的连接类型，在ISAKMP网关配置模式下使用以下命令：

connection-type {**bidirectional** | **initiator-only** | **responder-only**}

- **bidirectional** – 指定该ISAKMP网关既是发起端也是响应端。该选项为系统的默认选项。
- **initiator-only** – 指定该ISAKMP网关仅是发起端。
- **responder-only** – 指定该ISAKMP网关仅是响应端。

由于拨号VPN只能做响应端，因此此处只能配置**bidirectional**或者**responder-only**。

使用**no connection-type**命令恢复默认连接方式。

开启NAT穿越功能

在IPSec或者IKE组建的VPN隧道中，若存在NAT网关设备，且NAT网关设备对VPN数据进行了NAT转换，则必须开启IPSec或者IKE的NAT穿越功能。默认情况下，NAT穿越功能是关闭的。开启NAT穿越功能，在ISAKMP网关配置模式下，使用以下命令：

nat-traversal

使用**no nat-traversal**命令关闭NAT穿越功能。

配置DPD功能

DPD（Dead Peer Detection）为安全隧道对端状态探测功能。该功能开启后，如果接收端长时间收不到对端的报文，便触发DPD查询，主动向对端发送请求报文，对ISAKMP网关是否存在进行检测。默认情况下，DPD功能是关闭的。配置DPD功能，在ISAKMP网关配置模式下使用以下命令：

dpd [**interval** *seconds*] [**retry** *times*]

- **interval** *seconds* – 指定向对端发送查询请求的时间间隔。间隔范围是0到10秒。默认值是0，表示不开启DPD功能。
- **retry** *times* – 指定向对端发送查询请求的次数。向对端发送查询请求后，如果本端在指定的时间间隔内收不到对端的报文，系统会在再次发送查询请求，如此反复，直到完成该参数指定的次数。在指定次数查询完成后如果仍然收不到对端的报文，则判断对端ISAKMP网关已经死掉。查询请求的次数范围是1到20次，默认是3次。

使用**no dpd**命令恢复默认的DPD配置。

指定描述信息

为所配置的ISAKMP网关指定描述信息，请在ISAKMP网关配置模式下使用以下命令：

description *string*

- *string* – ISAKMP网关的描述信息。

使用**no description**命令删除ISAKMP网关的描述信息。

配置P2提议

P2提议使用在SA第二阶段。对P2提议的配置包括指定协议类型、加密算法、验证算法、压缩算法和生命周期。

创建P2提议

创建P2提议，即IPSec安全提议，请在全局配置模式下使用以下命令：

ipsec proposal *p2-name*

- *p2-name* – 指定所创建的P2提议的名称。执行该命令后，CLI进入到P2提议配置模式。对P2提议各项参数的配置都要在该模式下进行。

使用**no ipsec proposal** *p2-name*命令删除指定的IPSec proposal。

指定协议类型

P2提议可使用的协议类型有AH以及ESP。为P2提议指定协议类型，在P2提议配置模式下使用以下命令：

protocol {**esp** | **ah**}

- **esp** – 指定使用ESP协议。该协议为系统默认协议。
- **ah** – 指定使用AH协议。

使用**no protocol**命令恢复默认协议配置。

指定加密算法

用户可以为P2提议指定至少一种最多四种加密算法。为P2提议指定加密算法，在P2提议配置模式下使用以下命令：

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256** | **null**} [**3des** | **des** | **aes** | **aes-192** | **aes-256** | **null**] [**3des** | **des** | **aes** | **aes-192** | **aes-256** | **null**]……

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为StoneOS系统默认方法。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。
- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。
- **null** – 不使用加密功能。

使用**no encryption**命令恢复默认加密算法。

指定验证算法

用户可以为P2提议指定至少一种最多三种验证算法。为P2提议指定验证算法，在P2提议配置模式下使用以下命令：

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**} [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **null**] [**md5** | **sha** | **sha256** | **sha384** | **sha512** |**null**]

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为StoneOS的默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** –指定使用SHA-512验证算法。摘要为512比特。
- **null** – 不使用验证功能。

使用**no hash**命令恢复默认验证算法。

配置PFS功能

PFS（Perfect Forward Security）功能决定新密钥的生成方式，而不是新密钥的生成时间。PFS保证无论在哪一阶段，一个密钥只能使用一次，而且，生成密钥的“材料”也只能使用一次。某个“材料”在生成了一个密钥后就被弃，绝不用来再生成任何其它密钥。这样可以确保一旦单个密钥泄密，最多只可能影响用该密钥加密的数据，而不会危及整个通信。PFS功能是由DH算法做保障的。配置P2提议的PFS功能，在P2提议配置模式下使用以下命令：

group {**nopfs** | **1** | **2** | **5** | **14** | **15** |**16**}

- **nopfs** – 不使用PFS功能。该选项为系统的默认选项。
- **1** – 选择DH组1。密钥的长度为768比特。
- **2** – 选择DH组2。密钥的长度为1024比特。
- **5** – 选择DH组5。密钥的长度为1536比特。

- **14** – 选择DH组14。密钥的长度为2048比特。
- **15** – 选择DH组15。密钥的长度为3072比特。
- **16** – 选择DH组16。密钥的长度为4096比特。

使用**no group**命令恢复默配置。

指定生命周期

Hillstone设备有两种衡量生命周期的方法，分别是按时间和按流量。当SA的流量或者时间达到特定值时，SA就会过期，需要重新进行协商。指定P2提议的生命周期，在P2提议配置模式，使用以下命令：

lifetime *seconds*

- *seconds* – 指定时间类型生命周期的时间长度，单位为秒。默认值是28800秒。

lifesize *kilobytes*

- *kilobytes* – 指定流量类型周期的流量值，单位为字节。默认值是0，意义为没有周期流量限制。

使用以上两个命令no的形式恢复默认配置。即

no lifetime

no lifesize

配置隧道

通过IKE配置IPSec隧道，用户需要配置的选项有指定协议类型、ISAKMP网关、IKE安全提议、ID号、是否分片以及防重放等。

创建IKE隧道

创建IKE隧道，在全局配置模式下，使用以下命令：

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* - 指定所创建的IKE隧道的名称。

执行该命令后，CLI进入到IKE隧道配置模式。对IKE隧道的所有参数配置都需要在该模式下进行。

在全局配置模式下使用**no tunnel ipsec** *tunnel-name* **auto**删除指定的IKE隧道。

指定 IPSec协议的操作模式

为IKE隧道指定操作模式（隧道模式），在IKE隧道配置模式下使用以下命令：

mode tunnel

使用**no mode**命令恢复默认模式。

指定ISAKMP网关

为IKE隧道指定ISAKMP网关，请在IKE隧道配置模式下使用以下命令：

isakmp-peer *peer-name*

• *peer-name* – 指定ISAKMP网关的名称。

使用**no isakmp-peer**取消对ISAKMP网关的指定。

指定P2提议

为IKE隧道指定P2提议，请在IKE隧道配置模式下使用以下命令：

ipsec-proposal *p2-name*

- *p2-name* – 指定P2提议的名称。

使用**no ipsec-proposal**取消对P2提议的指定。

指定第二阶段ID

为IKE IPSec隧道指定第二阶段ID，请在IKE隧道配置模式下使用以下命令：

id {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask***service** *service-name*}

- **auto** – 自动指定第二阶段ID。此参数为系统默认配置。
- **local** *ip-address/mask* – 指定本端第二阶段local ID。
- **remote** *ip-address/mask* – 指定本端第二阶段remote ID。
- **service** *service-name* – 指定服务名称。

当中心设备端配置了多个第二阶段ID时，中心设备能够与拨号端协商并创建多个IPSec SA，即创建多个IKE隧道。配置了自动生成路由功能后（参见配置自动生成路由功能），每创建一个IPSec SA，中心设备会将目的地址为拨号端的local ID、下一跳为拨号端网关接口（出接口）的IP地址的路由条目添加到自己的路由表。删除一个IPSec SA后，相应的路由条目也会被删除。

使用**no id** {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}命令恢复系统默认配置。

配置ID为包含关系时生成IPSec SA

当中心设备配置的第二阶段的remote ID包含拨号端的第二阶段的local ID时，配置该功能后，中心设备和远程拨号端之间可成功协商生成IPSec SA。配置ID为包含关系时生成IPSec SA，请在IKE隧道配置模式下使用以下命令：

dialup-control-id

使用**no dialup-control-id**恢复默认配置。

配置IPSec分流限流功能

中心设备可以和一个远程拨号端协商生成多个IPSec SA，并在IKE隧道出接口对封装的数据包进行限流，在IKE隧道入接口对封装的数据包进行分流。如果数据包的源IP地址、目的IP地址和服务类型匹配某个第二阶段ID的配置，那么该数据包会被中心设备接收并继续处理，否则该数据包会被丢弃。配置IPSec分流限流功能，请在IKE隧道配置模式下使用以下命令：

check-id

使用**no check-id**恢复默认配置。

配置自动连接功能

设备提供两种触发建立SA的方式：自动方式和流量触发方式。

- 自动方式：设备每60秒检查一次SA的状态，如果SA未建立则自动发起协商请求；
- 流量触发方式：当有数据流量需要通过隧道进行传输时，该隧道才发起协商请求。

默认情况下，系统使用流量触发方式。使用自动方式，在IKE隧道配置模式下使用以下命令：

auto-connect

使用**no auto-connect**命令恢复系统的默认设置。

注意: 自动连接功能仅在对端IP地址为静态类型且本端可以作为发起端时有效。

配置分片功能

用户可以指定是否允许转发设备将包进行分片处理。为IKE隧道配置分片功能，请在IKE隧道配置模式下使用以下命令：

df-bit {**copy** | **clear** | **set**}

- **copy** – 直接从发包端拷贝IP包的DF选项。该选项为系统默认选项。
- **clear** – 允许转发设备对包做分片处理。
- **set** – 不允许转发设备对包做分片处理。

使用**no df-bit**恢复系统的默认设置。

配置防重放功能

防重放（anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。默认情况下，防重放功能是关闭的。为IKE IPSec隧道配置防重放功能，请在IKE IPSec隧道配置模式下使用以下命令：

anti-replay {**32** | **64** | **128** | **256** | **512**}

- **32** – 指定防重放的窗口为32。
- **64** – 指定防重放的窗口为64。
- **128** – 指定防重放的窗口为128。
- **256** – 指定防重放的窗口为256。
- **512** – 指定防重放的窗口为512。

在网络状况较差时，例如存在严重乱序现象等，请选择较大的窗口。

使用**no anti-replay**命令关闭防重放功能。

设置Commit位

用户可以配置使响应方设置Commit位，从而防止出现丢包和时间差现象。但是，设置Commit位可能导致响应速度变慢。设置Commit位，请在IKE IPSec隧道配置模式下使用以下命令：

响应方设置Commit位：**responder-set-commit**

响应方不设置Commit位：**no responder-set-commit**

配置空闲时间

空闲时间指隧道在无流量状态下能够保持连接状态的最长时间，超出空闲时间后，SA将会被清除。配置空闲时间，在IKE IPSec隧道配置模式下，使用以下命令：

idle-time *time-value*

- *time-value* – 指定空闲时间，单位为秒。取值范围是120到3000秒。

在IKE IPSec隧道配置模式下使用该命令no的形式关闭空闲时间功能：

no idle-time

指定描述信息

为所配置的IKE隧道指定描述信息，请在IKE IPSec隧道配置模式下使用以下命令：

description *string*

- *string* – IKE隧道的描述信息。

使用**no description**命令删除IKE隧道的描述信息。

配置自动生成路由功能

对于基于路由的拨号VPN或者PnPVPN，其中心设备通常会连接多个分支机构（拨号VPN的拨号端或者PnPVPN的客户端），并且这些分支机构的IP地址会经常发生变动，因此，当中心设备访问分支机构时，手工配置路由会给管理员带来很多不便。Hillstone设备支持自动生成路由功能，该功能允许设备自动添加从中心设备到分支机构的路由条目，从而避免了手工配置路由所带来的问题。

默认情况下，设备的自动生成路由功能是关闭的。开启此功能，请在ISAKMP配置模式下，使用以下命令：

generate-route

对于拨号VPN，执行此命令后，自动生成路由条目的目的地址为拨号端的第二阶段local ID，下一跳IP地址为对端的IP地址。关于如何配置第二阶段ID，请参阅“指定第二阶段ID”。

对于PnPVPN，执行此命令后，自动生成路由条目的目的地址为客户端DHCP地址池的起始IP地址和客户端DHCP地址池的网络掩码的逻辑“与”运算结果（dhcp-pool-addr-start & dhcp-pool-net-mask）。下一跳IP地址为对端的IP地址。关于如何配置客户端DHCP地址池及其网络掩码，请参阅“通过CLI配置PnPVPN服务器端”。

使用**no generate-route**命令关闭自动生成路由功能。

注意:

- 对于拨号VPN，当拨号端的第二阶段local ID指定为0.0.0.0/0时，强烈建议用户不要开启自动生成路由功能。
- 当分支机构访问中心设备时，用户可以使用no reverse-route命令取消隧道接口的逆向路由功能，使所有反向数据原路返回。

配置拨号端用户信息

中心设备需要创建拨号端的用户信息，包括用户帐号以及生成拨号端用户预共享密钥。

创建拨号端用户帐号

在全局配置模式下，使用以下命令：

user *user-name* **aaa-server local**

- *user-name* – 指定用户名称。

执行该命令后，系统进入用户配置模式，在该模式下，指定用户的IKE ID，命令如下：

ike_id {**fqdn** *string* | **asn1dn** *string*}

- **fqdn** *string* – 指定使用FQDN类型的IKE ID。string为ID的具体内容。
- **asn1dn** *string* – 指定使用Asn1dn类型的ID，该类型只可应用于使用证书的情况。string为ID的具体内容。

在用户配置模式下使用该命令no的形式取消IKE ID的配置：

```
no ike_id
```

生成拨号端用户预共享密钥

根据拨号端用户的用户名以及IKE ID，中心设备可生成相应的预共享密钥。在执行模式下，使用以下命令：

exec generate-user-key rootkey *pre-share-key* **userid** *string*

- *pre-share-key* – 指定设备端的预共享密钥。
- *string* – 指定用户名称相对应的IKE ID。

拨号端配置

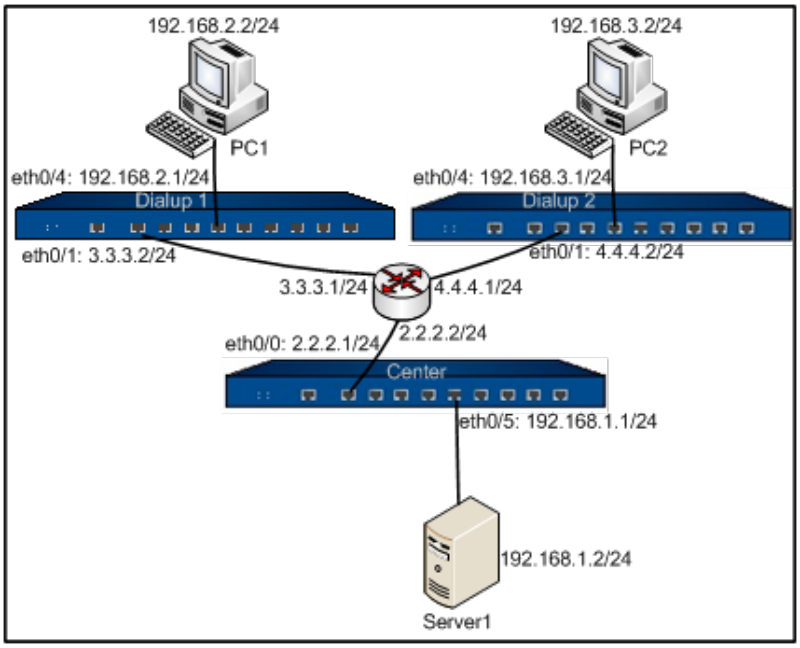
拨号端需要配置与中心端相对应的P1提议、P2提议、ISAKMP网关以及隧道。配置命令与中心设备的配置基本相同。但是，在配置拨号端ISAKMP网关的本地ID时，如果使用的是预共享密钥，指定的预共享密钥为中心设备生成的相应的预共享密钥。

拨号VPN举例

该节介绍一个拨号VPN的实例。

组网需求

两个拨号端设备（User1和User2）与中心设备（2.2.2.1/24）组成拨号VPN，实现与拨号端设备相连的PC（PC1和PC2）能够安全访问被中心设备保护的服务器（Server1）资源。组网图参见下图：



中心设备配置

第一步：接口配置：

```
hostname(config)# zone vpnzone
hostname(config-zone-vpnzone)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone vpnzone
hostname(config-if-eth0/0)# ip address 2.2.2.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/5
hostname(config-if-eth0/5)# zone trust
hostname(config-if-eth0/5)# ip address 192.168.1.1/24
hostname(config-if-eth0/5)# exit
hostname(config)#exitlocal-id fqdn hillstone2
```

第二步：配置拨号端用户帐号及预共享密钥信息：

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
hostname(config-user)# ike_id fqdn hillstone1
hostname(config-user)# exit
hostname(config-aaa-server)# user user2
hostname(config-user)# ike_id fqdn hillstone2
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)# exit
hostname# exec generate-user-key rootkey 123456 userid hill-
stone1
userkey: 3zPNDY6MmI8Wejk5fa3jhPU39p8=
hostname# exec generate-user-key rootkey 123456 userid hill-
stone2
userkey: tAFW+48HcAr15+NcISm6TZJZzGU=
hostname# configure
hostname(config)#
```

第三步：配置IKE VPN：

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# aaa-server local
hostname(config-isakmp-peer)# interface ethernet0/0
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
```

```
hostname(config-isakmp-peer)# pre-share 123456
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer test
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# id local192.168.1.2/24 remote
0.0.0.0/0 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

第四步：配置策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone vpnzone
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone vpnzone
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action fromtunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

拨号端1配置

第一步：接口配置：

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 3.3.3.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/5)# zone trust
hostname(config-if-eth0/5)# ip address 192.168.2.1/24
hostname(config-if-eth0/5)# exit
hostname(config)#
```

第二步：配置IKE VPN：

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# peer 2.2.2.1
```

```
hostname(config-isakmp-peer)# pre-share 3zPNDY6MmI8We-
jk5fa3jhPU39p8=
hostname(config-isakmp-peer)# local-id fqdn hillstone1
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer test
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# id local 192.168.2.2/24 remote
192.168.1.2/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

第三步：配置策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action fromtunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

拨号端2配置

第一步：接口配置：

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 4.4.4.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/5)# zone trust
hostname(config-if-eth0/5)# ip address 192.168.3.1/24
hostname(config-if-eth0/5)# exit
hostname(config)#
```

第二步：配置IKE VPN：

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)#
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# peer 2.2.2.1
hostname(config-isakmp-peer)# pre-share
```

```
tAFW+48HcAr15+NcISm6TZJZzGU=
hostname(config-isakmp-peer)#
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer test
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# id local 192.168.3.2/24 remote
192.168.1.2/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

第三步：配置策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zonetrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action fromtunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

PnPVPN

PnPVPN简介

IPSec VPN配置复杂，维护成本高，对网管人员技术要求高，针对该问题，Hillstone为企业用户提供了一种简单易用的VPN技术——PnPVPN，即即插即用VPN。PnPVPN由两部分组成，分别是PnPVPN Server和PnPVPN Client，各自功能描述如下：

- PnPVPN Server：通常放置于企业总部，由总部IT工程师负责维护，客户端的大多数配置由服务器端下发。PnPVPN Server通常由Hillstone设备充当，一台Hillstone设备可充当多个PnPVPN Server。
- PnPVPN Client：通常放置于企业分支机构（如办事处），可由总部工程师远程维护，只需要做简单配置（如客户端ID、密码和服务器端IP地址），和Server端协商成功后即可从Server端获取配置信息（如DNS、WINS、DHCP地址池等）。PnPVPN Client通常由Hillstone下一代防火墙低端产品充当。

注意: Hillstone设备既可以充当PnPVPN Server，又可以充当PnPVPN Client。当充当Server时，不同平台支持的VPN实例数和每个实例所支持的客户端数有所不同。

PnPVPN工作流程

PnPVPN的工作流程如下：

1. 客户端发起连接请求，并传送自己的ID以及密码到服务器端。
2. 服务器端收到请求后，验证客户端传送的ID和密码，验证通过即下发预配置的DHCP地址池、DHCP掩码、DHCP网关、WINS、DNS和隧道路由等信息到客户端。
3. 客户端把收到的信息下发到相应的功能模块。
4. 客户端PC自动获取IP地址、IP地址掩码和网关地址等网络参数，并正常接入VPN网络。

PnPVPN链路冗余

PnPVPN服务器端支持一个PnPVPN客户端拨入两条VPN链路并自动生成到客户端的路由、为客户端配置VPN监控。服务器端需要配置两个ISAKMP网关和两个隧道接口，两个VPN隧道分别引用不同的ISAKMP网关，并绑定到两个不同的隧道接口。

客户端支持通过VPN双链路拨入服务器端、VPN监控和冗余选路。PnP客户端的两个VPN隧道在和服务器端协商时，会根据服务器端的隧道路由配置分别生成不同优先级的路由，优先级高的隧道作为主链路，优先级低的隧道作为备份链路，从而实现冗余选路。主VPN隧道会首先处于active状态，如果客户端监测到该主隧道中断，客户端设备会通过备份隧道重新传输数据；当监测到主隧道恢复正常后，客户端设备会重新启用主隧道传输数据。

PnPVPN服务器端配置

PnPVPN配置包括服务器端配置和客户端配置。服务器端可通过CLI和WebUI两种方式进行配置。

通过CLI配置PnPVPN服务器端

PnPVPN服务器端配置基于IPSec VPN命令行，此外，还有特有的命令行，本节仅介绍PnPVPN特有命令行。使用以下特有命令并不能完成服务器端的配置，完整配置请参见PnPVPN配置举例部分。

配置用户网络参数

客户端与服务器端VPN协商成功后，服务器端需要下发给用户端网络参数信息，包括DNS服务器地址、WINS服务器地址、隧道路由、DHCP地址池及其掩码和网关地址。这些网络参数需要在相应的用户配置模式下进行配置。DNS、WINS和隧道路由也可以在IKE隧道配置模式下配置，但用户配置模式下的配置优先级高于IKE隧道配置模式，即当用户配置模式和IKE隧道配置模式同时配置了DNS、WINS或隧道路由，服务器使用用户配置模式下的配置下发给客户端。

进入本地用户配置模式，使用以下命令：

aaa-server *aaa-server-name* **type local** （进入本地AAA认证服务器配置模式）

user *user-name*

- *user-name* – 指定用户名称。

通过以下命令完成用户网络参数的配置，其中DHCP地址池、DHCP网络掩码和网关为必配网络参数。

dns *A.B.C.D* [*A.B.C.D*] [*A.B.C.D*] [*A.B.C.D*]

- *A.B.C.D* – 配置DNS服务器的IP地址，可同时指定1个主DNS服务器和最多3个备份服务器。使用no dns命令取消配置。

wins *A.B.C.D* [*A.B.C.D*]

- *A.B.C.D* – 配置WINS服务器的IP地址，可同时指定一个主WINS服务器和一个备份WINS服务器。使用no wins命令取消配置。

split-tunnel-route *A.B.C.D/Mask*

- *A.B.C.D/Mask* – 配置隧道路由。A.B.C.D为IP地址前缀，Mask为子网掩码的位数。最多可设置128条隧道路由。使用no split-tunnel-route A.B.C.D/Mask命令取消配置。

dhcp-pool-address *start-ipaddr end-ipaddr*

- *start-ipaddr end-ipaddr* – 配置DHCP地址池的起始IP地址和终止IP地址。使用no dhcp-pool-address命令取消配置。

dhcp-pool-netmask *A.B.C.D*

- *A.B.C.D* – 配置DHCP地址池的网络掩码。使用**no dhcp-pool-netmask**命令取消配置。

dhcp-pool-gateway *A.B.C.D*

- *A.B.C.D* – 配置DHCP地址池的网关地址。该地址用来作为PnPVPN客户端内网接口的IP地址，并被设置为PC的网关地址，PC的IP地址由以上设置的DHCP地址池的网段以及网络掩码确定，所以网关地址应该和DHCP地址池在同一个网段。使用no dhcp-pool-gateway命令取消配置。

配置隧道网络参数

当所有或大部分客户端使用统一的DNS、WINS或隧道路由时，可以在IKE隧道配置模式下配置DNS、WINS或隧道路由以减少用户配置模式下的工作量。使用以下命令进入IKE隧道配置模式：

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* – 指定IKE隧道名称。

通过以下命令完成DNS、WINS或隧道路由的配置：

dns *A.B.C.D* [*A.B.C.D*] [*A.B.C.D*] [*A.B.C.D*]

- *A.B.C.D* – 配置DNS服务器的IP地址，可同时指定1个主DNS服务器和最多3个备份服务器。使用**no dns**命令取消配置。

wins *A.B.C.D* [*A.B.C.D*]

- *A.B.C.D* – 配置WINS服务器的IP地址，可同时指定一个主WINS服务器和一个备份WINS服务器。使用**no wins**命令取消配置。

split-tunnel-route *A.B.C.D/Mask*

- *A.B.C.D/Mask* – 配置隧道路由。A.B.C.D为IP地址前缀，Mask为子网掩码的位数。最多可设置128条隧道路由。使用no split-tunnel-route A.B.C.D/Mask命令取消配置。

配置ISAKMP网关对端通配符

当PnPVPN Server通过Radius服务器进行认证时，需要配置ISAKMP网关对端的通配符。Hillstone设备在收到客户端的VPN连接建立请求时，根据客户端的用户名与ISAKMP网关对端通配符的匹配结果，确定与客户端接入的PnPVPN Server（一台Hillstone设备可同时充当多个PnPVPN的Server），进而确定对用户进行认证的Radius服务器。

在ISAKMP网关配置模式下使用以下命令配置ISAKMP网关对端通配符：

peer-id fqdn wildcard *string*

- **fqdn** – 指定使用FQDN类型的通配符。
- **wildcard** *string* – 指定通配符ID，通常为客户端的域名。如abc.com。

使用**no peer-id**命令取消通配符配置。

配置PnPVPN客户端的隧道接口

为了使分支机构的多个子网网段可以访问服务器端，StoneOS支持在PnPVPN服务器端为客户端的隧道接口指定IP地址，并启用SNAT规则。如果PnPVPN客户端是由Hillstone SR系列安全路由器充当，那么需要SR系列产品的版本支持该功能。

注意: 该功能工作时，PnPVPN服务器端将无法访问客户端。

进入本地用户配置模式，使用以下命令：

aaa-server *aaa-server-name* **type local** （进入本地AAA认证服务器配置模式）

user *user-name*

- *user-name* – 指定用户名称。

在本地用户配置模式下，使用以下命令配置PnPVPN客户端的隧道接口：

tunnel-ip-address *A.B.C.D* [**snat**]

- *A.B.C.D* – 指定客户端隧道接口的IP地址，该地址不能与客户端已存在的IP地址冲突。
- **snat** – 启用SNAT规则。默认情况下，系统不开启隧道接口的SNAT规则。

在本地用户配置模式下，使用该命令no的形式取消配置PnPVPN客户端的隧道接口：

no tunnel-ip-address

通过WebUI配置服务器端

通过WebUI配置服务器端，用户需要在以下模块进行配置：

- 用户配置
- IKE VPN配置
- 隧道接口配置
- 路由配置
- 策略配置

注意: 注意：PnPVPN支持两种认证服务器：Local和Radius。以下配置列出使用本地服务器进行认证的情况，关于Radius服务器认证配置请参阅相应的Radius服务器使用手册。

用户配置

请按照以下步骤进行用户配置：

1. 从工具栏的<对象用户>下拉菜单选择『本地用户』，弹出<本地用户>对话框。

2. 在<本地服务器>下拉菜单中选择需要的本地服务器名称，然后点击对话框左上角的『新建』下拉菜单，选择<用户>，弹出<用户配置>对话框。

3. 在<名称>对话框中输入用户名称。

4. 设置用户密码。在<密码>文本框输入密码，并在<重新输入密码>文本框再次输入密码进行确认。

5. 指定用户IKE ID。从<IKE标识>部分选中<FQDN>单选按钮，并在<IKE标识>文本框中输入ID。PnPVPN Client将使用该ID进行登录认证。

6. 点击<PnPVPN配置>，展开具体配置选项，包括DHCP相关选项、DNS、WINS以及隧道路由。当该用户不使用隧道下已经配置的DNS、WINS和隧道路由选项或者新建隧道页面未配置这些选项时，这些选项必须在本页面完成配置。

7. 根据需要对该页面的其它选项进行配置。

8. 配置完成，点击『确定』按钮保存所做配置。

IKE VPN配置

IKE VPN配置包括P1提议配置、P2提议配置、对端配置以及隧道配置。

按照以下步骤配置P1提议：

1. 从页面左侧导航树选择并点击“配置 > 网络 > IPSec VPN”，进入IPSec VPN页面。点击『P1提议』标签，进入P1提议标签页。

2. 点击P1提议列表左上方的『新建』按钮，弹出<阶段1提议配置>对话框。

3. 指定P1提议名称。在<提议名称>文本框输入P1提议名称。

4. 指定认证方式。选中“pre-share”单选按钮。

5. 指定DH组。选中“Group2”单选按钮。

6. 根据需要对该页面的其它选项进行配置或保持其默认值。

7. 配置完成，点击『确定』按钮保存所做配置。

按照以下步骤配置P2提议：

1. 从页面左侧导航树选择并点击“配置⑥网络⑥IPSec VPN”，进入IPSec VPN页面。点击『P2提议』标签，进入P2提议标签页。

2. 点击P2提议列表左上方的『新建』按钮，弹出<阶段2提议配置>对话框。

3. 指定P2提议名称。在<提议名称>文本框输入P2提议名称。

4. 选择使用的协议、验证算法、加密算法和PFS组。

5. 根据需要对该页面的其它选项进行配置或保持其默认值。

6. 配置完成，点击『确定』按钮保存所做配置。

按照以下步骤配置对端：

1. 从页面左侧导航树选择并点击“配置⑥网络⑥IPSec VPN”，进入IPSec VPN页面。点击『VPN对端列表』标签，进入VPN对端列表标签页。

2. 点击列表左上方的『新建』按钮，弹出<VPN对端配置>对话框。

3. 指定对端名称。在<对端名称>文本框输入对端名称。

4. 指定外网接口。从<接口>下拉菜单中选择需要的接口。

5. 指定模式和类型。选中<野蛮模式>和<用户组>单选按钮。

6. 指定认证服务器。从<AAA服务器>下拉菜单选择使用的认证服务器。

7. 指定P1提议。从<提议1>下拉菜单中选择需要的P1提议。

8. 指定预共享密钥。在<预共享密钥>文本框输入相应的预共享密钥。

9. 根据需要对该页面的其它选项进行配置或保持其默认值。

10. 点击『生成』按钮，弹出<生成用户密钥>对话框。输入用户ID和预共享密钥，点击『生成』按钮，生成的密钥将显示在<创建结果>文本框中。PnPVPN Client将使用该密钥作为密码进行登录认证。点击『关闭』按钮返回对端配置页面。

11. 点击『确定』按钮保存所做配置。

注意: 当选用Radius服务器进行认证时，必须配置对端通配符。

按照以下步骤配置隧道：

1. 从页面左侧导航树选择并点击“配置⑥网络⑥IPSec VPN”，进入IPSec VPN页面。点击『IPSec VPN』标签，进入IPSec VPN标签页。

2. 点击IKE VPN列表左上方的『新建』按钮，弹出<IKE VPN配置>对话框。

3. 在<步骤1：对端>部分，点击<对端名称>的『导入』按钮，然后从下拉菜单中选择需要的对端。用户也可以直接在该页面新建对端（ISAKMP网关）。

4. 点击<步骤2：隧道>，展开隧道具体配置选项。

5. 指定隧道名称。在<名称>文本框输入隧道名称。

6. 指定模式。选中<tunnel>单选按钮。

7. 指定提议。从<p2提议>下拉菜单选择需要的提议。

8. 点击『高级配置』标签进行高级选项配置。

9. 配置DNS和WINS服务器。通过该隧道接入的用户将使用此处指定的DNS和WINS。

10. 设置隧道路由。

11. 根据需要对该页面的其它选项进行配置或保持其默认值。

12. 点击『确定』按钮保存所做配置。

dns *A.B.C.D [A.B.C.D] [A.B.C.D] [A.B.C.D] A.B.C.D* – 配置DNS服务器的IP地址，可同时指定1个主DNS服务器和最多3个备份服务器。使用**no dns**命令取消配置。 **wins** *A.B.C.D [A.B.C.D] A.B.C.D* – 配置WINS服务器的IP地址，可同时指定一个主WINS服务器和一个备份WINS服务器。使用**no wins**命令取消配置。 **split-tunnel-route**

A.B.C.D/Mask A.B.C.D/Mask – 配置隧道路由。A.B.C.D为IP地址前缀，Mask为子网掩码的位数。最多可设置128条隧道路由。使用**no split-tunnel-route** *A.B.C.D/Mask*命令取消配置。

注意: 用户配置部分指定的DNS、WINS和隧道路由优先级高于此处配置。

隧道接口配置

请按照以下步骤进行隧道接口配置：

1. 点击“配置 > 网络 > 网络连接”，进入网络连接页面。
2. 点击接口列表左上方的『新建』下拉菜单，选择并点击<隧道接口>，弹出<接口配置>对话框。
3. 指定隧道接口名称。在<名称>部分的<tunnel>文本框输入编号。
4. 指定隧道接口所属安全域类型。在<安全域类型>部分选中<三层安全域>单选按钮。
5. 指定隧道接口所属安全域。从<安全域>下拉菜单选择需要的安全域。
6. 绑定隧道。在<隧道绑定配置>部分选中<IPSec VPN>单选按钮，然后从<VPN名称>下拉菜单选择VPN隧道名称。无需配置网关地址。
7. 点击『确定』按钮保存所做配置。

路由配置

为实现服务器端网络的主机能够访问客户端网络，用户需要添加静态路由条目。按照以下步骤配置路由：

1. 访问“配置⑥网络⑥路由”，进入目的路由页面。
2. 点击目的路由列表左上方的『新建』按钮，弹出<目的路由配置>对话框。
3. 配置目的IP。在<目的地>和<子网掩码>文本框中分别输入客户端网络内网IP前缀和子网掩码。

4. 配置下一跳。在<下一跳>部分选中<接口>单选按钮，然后从<接口>下拉菜单中选择VPN隧道绑定的隧道接口，并在<网关>文本框中填写设备端外网接口的IP地址。

5. 根据需要对该页面的其它选项进行配置或保持其默认值。

6. 点击『确定』按钮保存所做配置。

策略配置

根据网络拓扑情况，配置相应的访问策略（点击“配置 > 安全 >策略”，进入策略页面）。

配置PnPVPN客户端

PnPVPN客户端仅支持WebUI方式配置。按照以下步骤通过WebUI配置PnPVPN客户端：

1. 从页面左侧导航树选择并点击“配置⑥网络⑥IPSec VPN”，进入IPSec VPN页面。

2. 从页面右侧辅助栏的<任务>区选择『PnPVPN客户端』链接，弹出<PnPVPN配置>对话框。

3. 依次填写或者选择各项。配置选项具体描述如下：

   - 服务器地址1：指定服务器端IP地址。该选项为必选项。
   - 服务器地址2：指定服务器端IP地址。服务器地址1和服务器地址2可以相同，也可以不同。该选项为可选项。
   - ID：指定服务器端分配给用户端的IKE ID。
   - 密码：指定服务器端分配给用户端的密码。
   - 重新输入密码：再次输入密码以确认。
   - 自动保存：选中<启用>复选框，系统自动保存连接建立后PnPVPN服务器端下发给客户端的DHCP和WINS信息。
   - VPN出接口1：VPN出接口1是接入Internet的接口，从下拉菜单中选择需要的接口名称。该选项为必选项。
   - VPN出接口2：VPN出接口2是接入Internet的接口，从下拉菜单中选择需要的接口名称。出接口1和出接口2可以相同，也可以不同。该选项为可选项。

- VPN入接口：VPN入接口是内部PC或者各种应用服务器在PnPVPN客户端上的接入口。选中所需接口类型的单选按钮。当选择<接口>时需要在后面的<接口>下拉菜单中选择接口名称；当客户端有多个内网口连接PnPVPN的时候，选择<bgroup接口>，并需要在后面的<bgroup接口>部分指定该bgroup接口包含的可用接口成员。指定接口成员，在左侧的<可用成员>列表中选中需要指定的接口名称，点击右箭头按钮将其添加到右侧<服务成员>列表中；删除已指定的接口，在右侧的<服务成员>列表中选中需要删除的接口名称，点击左箭头按钮将其删除。

4. 配置完成，点击『确定』按钮保存所做配置并返回IPSec VPN页面。

PnPVPN配置举例

该节介绍PnPVPN配置实例。

组网需求

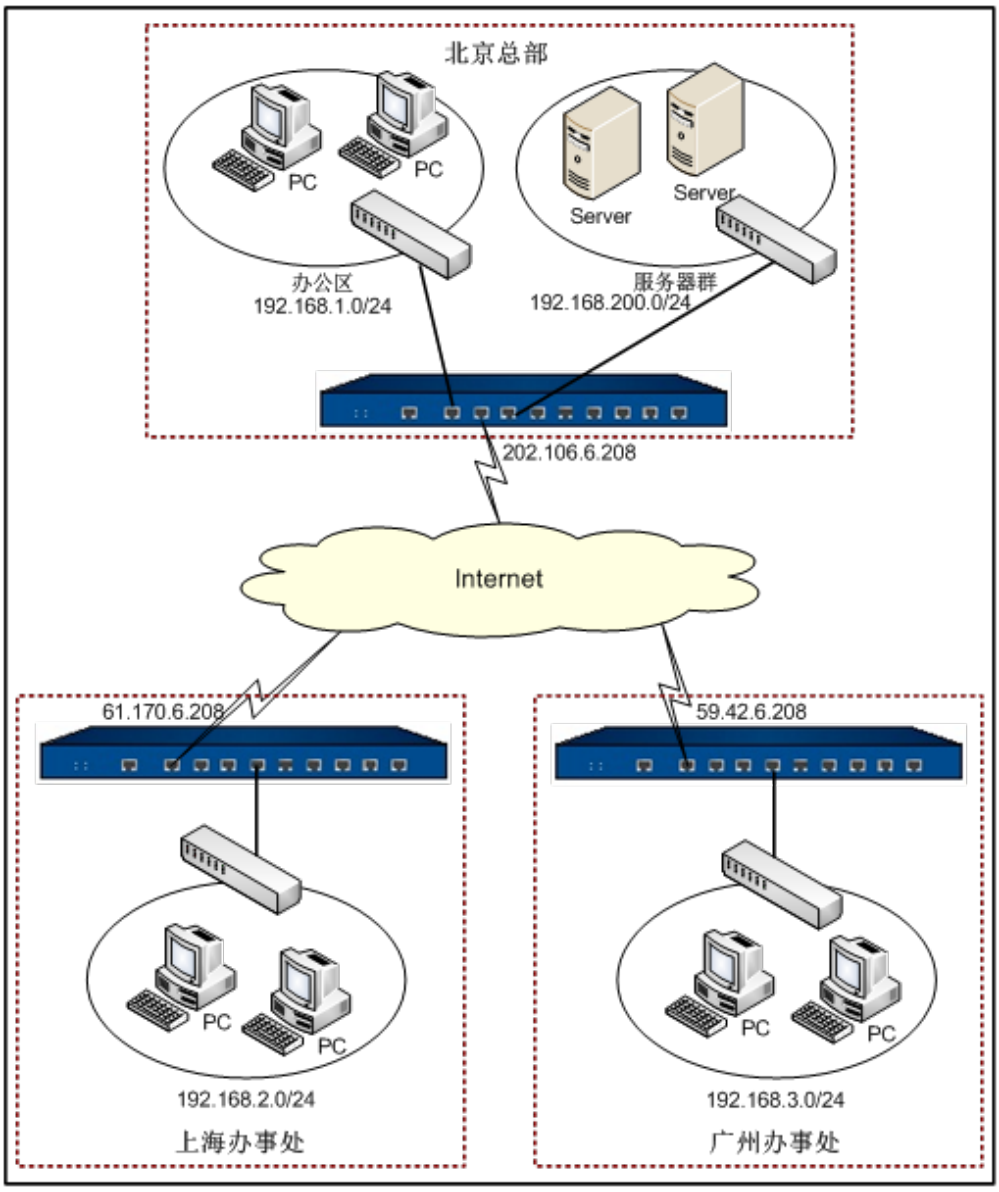
某公司总部位于北京，在上海和广州设有办事处，三地均可成功接入Internet。由于业务需求，需要组建VPN网络，达到以下目的：

- 广州和上海办事处的员工通过VPN访问总部数据库；
- 公司员工（包括总部和两办事处三地）之间可以通过VPN共享资源。

通过配置PnPVPN可实现以上需求，并且简单实用。组网图如图所示。配置方式如下：

- 公司总部选用一台Hillstone设备作为PnPVPN Server，采用本地认证方式；
- 上海和广州办事处各部署一台Hillstone设备，作为PnPVPN Client，接入总部VPN网络。

- 通过策略和路由配置实现允许公司员工之间的资源共享。



根据上图，具体网络环境描述如下：

- 总部局域网网段为192.168.1.0/24，通过接口ethernet0/0接入网络，属于trust安全域；
- 总部服务器群网段为192.168.200.0/24，通过接口ethernet0/2接入网络，属于trust安全域；
- 总部Hillstone设备通过接口ethernet0/1（IP地址为202.106.6.208）接入Internet，属于untrust安全域。

- 上海办事处设备接入Internet的接口IP地址为61.170.6.208，广州办事处设备接入Internet的IP地址为59.42.6.208。
- PnPVPN Server将分配192.168.2.0/24网段到上海办事处，192.168.3.0/24网段到广州办事处。

配置步骤

配置步骤分服务器端配置和客户端配置。

服务器端配置

第一步：配置本地AAA认证服务器：

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# exit
hostname(config)#
```

第二步：为上海办事处配置网络参数：

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# password shanghaiuser
hostname(config-user)# ike-id fqdn shanghai
hostname(config-user)# dhcp-pool-address 192.168.2.1
192.168.2.100
hostname(config-user)# dhcp-pool-netmask 255.255.255.0
hostname(config-user)# dhcp-pool-gateway 192.168.2.101
hostname(config-user)# split-tunnel-route 192.168.200.0/24
hostname(config-user)# split-tunnel-route 192.168.1.0/24
hostname(config-user)# split-tunnel-route 192.168.3.0/24
hostname(config-user)# exit
hostname(config-aaa-server)# exit
```

```
hostname(config)#
```

第三步：为广州办事处配置网络参数：

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user guangzhou
hostname(config-user)# password guangzhouuser
hostname(config-user)# ike-id fqdn guangzhou
hostname(config-user)# dhcp-pool-address 192.168.3.1
192.168.3.100
hostname(config-user)# dhcp-pool-netmask 255.255.255.0
hostname(config-user)# dhcp-pool-gateway 192.168.3.101
hostname(config-user)# split-tunnel-route 192.168.200.0/24
hostname(config-user)# split-tunnel-route 192.168.1.0/24
hostname(config-user)# split-tunnel-route 192.168.2.0/24
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

第四步：配置PnPVPN Server：

```
hostname(config)# isakmp proposal test1
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal test2
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer test1
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# interface ethernet0/1
```

```
hostname(config-isakmp-peer)# aaa-server test
hostname(config-isakmp-peer)# isakmp-proposal test1
hostname(config-isakmp-peer)# pre-share 123456
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec test auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal test2
hostname(config-tunnel-ipsec-auto)# isakmp-peer test1
hostname(config-tunnel-ipsec-auto)# mode tunnel
hostname(config-tunnel-ipsec-auto)# id auto
hostname(config-tunnel-ipsec-auto)# dns 192.168.200.1
192.168.200.11
hostname(config-tunnel-ipsec-auto)# wins 192.168.200.2
192.168.200.12
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

第五步：生成客户端密钥：

```
hostname(config)# exec generate-user-key rootkey 123456 userid
shanghai
userkey: kyZAKmLWCc5Nz75fseDiM2r+4Vg=
hostname(config)# exec generate-user-key rootkey 123456 userid
guangzhou
userkey: SdqhY4+dPThTtpipW2hs2OMB5Ps=
```

第六步：配置隧道接口和策略规则：

```
hostname(config)# zone VPN
hostname(config-zone-VPN)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
```

```
hostname(config-if-tun1)# tunnel ipsec test
hostname(config-if-tun1)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone VPN
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone VPN
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# exit
hostname(config)#
```

第七步：配置路由：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.2.0/24 tunnel1
61.170.6.208
hostname(config-vrouter)# ip route 192.168.3.0/24 tunnel1
59.42.6.208
hostname(config)#
```

客户端配置

上海办事处设备配置如下：

1. 登录设备WebUI，从页面左侧导航树选择并点击“配置⑥网络⑥IPSec VPN”，进入IPSec VPN页面。
2. 从页面右侧辅助栏的<任务>区选择『PnPVPN客户端』链接，弹出<PnPVPN配置>对话框。在该对话框做以下配置：
    - 服务器地址：202.106.6.208
    - ID：shanghai
    - 密码：kyZAKmLWCc5Nz75fseDiM2r+4Vg=
    - 重新输入密码：kyZAKmLWCc5Nz75fseDiM2r+4Vg=
    - 自动保存：选中复选框
    - VPN出接口：ethernet0/0
    - VPN入接口：ethernet0/3
3. 点击『确定』按钮保存所做配置并发起链接。

广州办事处设备配置如下：

1．登录设备WebUI，从页面左侧导航树选择并点击“配置⑥网络⑥IPSec VPN”，进入IPSec VPN页面。

2．从页面右侧辅助栏的<任务>区选择『PnPVPN客户端』链接，弹出<PnPVPN配置>对话框。在该对话框做以下配置：

- 服务器地址：202.106.6.208
- ID：guangzhou
- 密码：SdqhY4+dPThTtpipW2hs2OMB5Ps=
- 重新输入密码：SdqhY4+dPThTtpipW2hs2OMB5Ps=
- 自动保存：选中复选框
- VPN出接口：ethernet0/0
- VPN入接口：ethernet0/3

3．点击『确定』按钮保存所做配置并发起链接

GRE协议

GRE协议介绍

GRE（Generic Routing Encapsulation）是通用封装路由，是定义了在任意一种网络层协议上封装任意一个其它网络层协议的协议。StoneOS支持GRE over IPSec功能，实现路由协议信息的安全传输。

GRE配置

StoneOS的GRE配置包括：

- 配置GRE隧道
- 绑定GRE隧道到隧道接口

配置GRE隧道

GRE隧道配置需要在GRE隧道配置模式下进行。进入GRE隧道配置模式，在全局配置模式下，使用以下命令：

tunnel gre *gre-tunnel-name*

- *gre-tunnel-name* – 指定将要创建的GRE隧道的名称。执行该命令后，系统创建指定名称的GRE隧道，并且进入GRE隧道配置模式；如果指定的名称已存在，则直接进入GRE隧道配置模式。

使用以上命令no的形式删除指定的GRE隧道：

no tunnel gre *gre-tunnel-name*

进入GRE隧道配置模式后，用户需要为GRE隧道配置以下参数：

- 指定源接口/地址
- 指定目的地址
- 指定出接口

- 指定IPSec VPN隧道（可选）
- 指定验证秘钥（可选）

指定源地址

为GRE隧道指定源地址，在GRE隧道配置模式下，使用以下命令：

source {**interface** *interface-name* | *ip-address* }

- **interface** *interface-name* – 指定接口的IP地址为GRE隧道的源地址。通过interface-name参数指定接口名称。
- *ip-address* – 为GRE隧道指定源地址。

在GRE隧道配置模式下使用该命令no的形式取消源地址的配置：

no source

指定目的地址

为GRE隧道指定目的地址，在GRE隧道配置模式下，使用以下命令：

destination *ip-address*

- *ip-address* – 为GRE隧道指定目的地址。

在GRE隧道配置模式下，使用下命令no的形式取消目的地址的配置：

no destination

指定出接口

为GRE隧道指定出接口，在GRE隧道配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定出接口的名称。

在GRE隧道配置模式下使用该命令no的形式取消出接口配置：

no interface

指定IPSec VPN隧道

使用GRE over IPSec功能时，用户需要通过该命令指定IPSec VPN隧道对数据进行IPSec封装。指定IPSec VPN隧道，在GRE隧道配置模式下，使用以下命令：

next-tunnel ipsec *tunnel-name*

- *tunnel-name* – 指定IPSec VPN隧道的名称。

在GRE隧道配置模式下使用该命令no的形式取消IPSec VPN隧道的指定：

no next-tunnel

指定验证秘钥

通过指定验证秘钥，对进入GRE隧道的数据包进行封装与验证。当数据包携带的秘钥与接收端配置的验证秘钥相同时，数据包将会被解密。如果不相同，数据包将会被丢弃。指定验证秘钥，在GRE隧道配置模式下，使用以下命令：

key *key-value*

- *key-value* – 指定验证秘钥。取值范围为0到4294967295。

在GRE隧道配置模式下使用该命令no的形式取消验证秘钥的指定：

no key

绑定GRE隧道到隧道接口

配置完成的GRE隧道需要绑定到隧道接口上才能够生效。绑定GRE隧道到隧道接口，在隧道接口配置模式下，使用以下命令：

tunnel gre *gre-tunnel-name* [**gw** *ip-address*]

- *gre-tunnel-name* – 指定将要绑定的GRE隧道的名称。该隧道为系统中已创建的GRE隧道。
- *gw ip-address* – 当配置多个隧道到隧道接口时，需要配置该参数。该参数指定GRE隧道的下一跳IP地址，为对端隧道接口的IP地址。系统默认值为0.0.0.0。

在隧道接口配置模式下，使用该命令no的形式取消GRE隧道的绑定：

no tunnel gre *gre-tunnel-name*

提示: 关于隧道接口的静态路由配置，请参阅《路由》的“配置静态路由”部分。

显示GRE隧道配置信息

用户可以在任何模式下使用以下命令查看GRE隧道配置信息：

show tunnel gre [*gre-tunnel-name*]

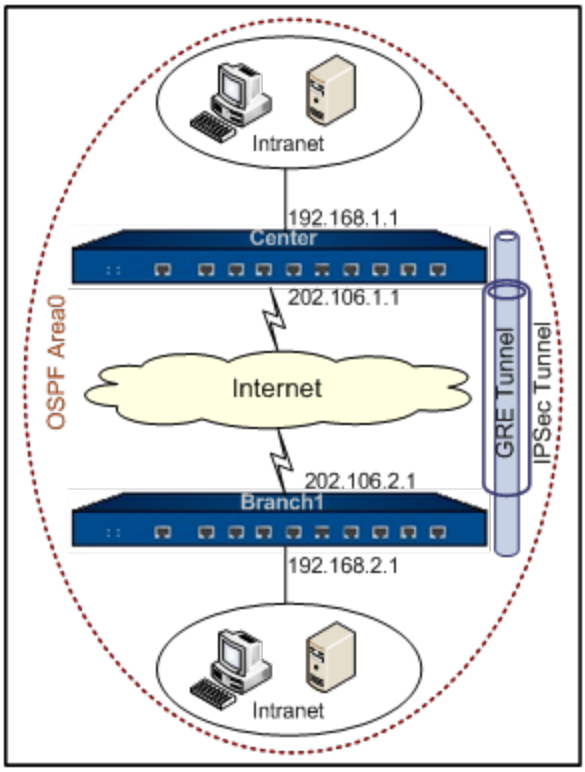
- *gre-tunnel-name* – 显示指定名称的GRE隧道配置信息。

GRE配置举例

本节介绍通过Hillstone设备实现GRE over IPSec with OSPF的配置实例。

需求描述

中心（Center）与分支（Branch1）跨越Internet互联，且中心与分支之间使用OSPF动态路由协议。通过配置GRE over IPSec功能实现中心与分支之间信息的安全传输。下图为该需求组网图：



配置步骤

以下分别介绍中心设备Center和分支设备Branch1的配置。

中心配置

对于IPSec VPN和OSPF配置，该文档仅列出必要配置。

第一步：接口配置：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.106.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#exit
```

第二步：IPSec VPN配置：

```
hostname(config)# isakmp proposal branch1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal branch1
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer branch1
hostname(config-isakmp-peer)# interface ethernet0/0
hostname(config-isakmp-peer)# peer 202.106.2.1
hostname(config-isakmp-peer)# pre-share 111111
hostname(config-isakmp-peer)# isakmp branch1
```

```
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec branch1 auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer branch1
hostname(config-tunnel-ipsec-auto)# ipsec-proposal branch1
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

第三步：GRE隧道配置：

```
hostname(config)# tunnel gre center-branch1
hostname(config-tunnel-gre)# source 202.106.1.1
hostname(config-tunnel-gre)# destination 202.106.2.1
hostname(config-tunnel-gre)# interface ethernet0/0
hostname(config-tunnel-gre)# next-tunnel ipsec branch1
hostname(config-tunnel-gre)# exit
hostname(config)#
```

第四步：绑定GRE隧道到隧道接口：

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ip address 172.16.1.1/24
hostname(config-if-tun1)# tunnel gre center-branch1 gw 172.16.1.2
hostname(config-if-tun1)# exit
hostname(config)#
```

第五步：OSPF配置：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 172.16.1.1
hostname(config-router)# network 172.16.1.1/24 area 0
hostname(config-router)# network 192.168.1.1/24 area 0
hostname(config-router)# exit
hostname(config-vrouter)# exit
hostname(config)#
```

第六步：策略配置：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# exit
hostname(config)#
```

分支配置

第一步：接口配置：

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.106.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第二步：IPSec VPN配置：

```
hostname(config)# isakmp proposal center
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal center
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer center
hostname(config-isakmp-peer)# interface ethernet0/0
hostname(config-isakmp-peer)# peer 202.106.1.1
hostname(config-isakmp-peer)# pre-share 111111
hostname(config-isakmp-peer)# isakmp center
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec center auto
```

```
hostname(config-tunnel-ipsec-auto)# isakmp-peer center
hostname(config-tunnel-ipsec-auto)# ipsec-proposal center
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

第三步：GRE隧道配置：

```
hostname(config)# tunnel gre branch1
hostname(config-tunnel-gre)# source 202.106.2.1
hostname(config-tunnel-gre)# destination 202.106.1.1
hostname(config-tunnel-gre)# interface ethernet0/0
hostname(config-tunnel-gre)# next-tunnel ipsec center
hostname(config-tunnel-gre)# exit
hostname(config)#
```

第四步：绑定GRE隧道到隧道接口：

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ip address 172.16.1.2/24
hostname(config-if-tun1)# tunnel gre branch1 gw 172.16.1.1
hostname(config-if-tun1)# exit
hostname(config)#
```

第五步：OSPF配置：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 172.16.1.2
hostname(config-router)# network 172.16.1.2/24 area 0
hostname(config-router)# network 192.168.2.1/24 area 0
hostname(config-router)# exit
```

```
hostname(config-vrouter)# exit
hostname(config)#
```

第六步：策略配置：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)#
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

L2TP协议

介绍

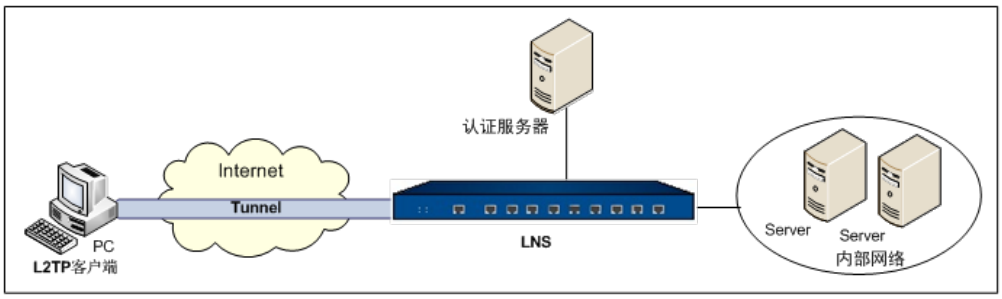
L2TP（Layer Two Tunneling Protocol，第二层隧道协议）是虚拟专用拨号网络（VPDN）技术的一种。L2TP可以让拨号用户从L2TP客户端或者L2TP访问集中器端（LAC）发起VPN连接，通过点对点协议（PPP）连接到L2TP 网络服务器（LNS）。连接成功后，LNS会向合法用户分配IP地址，并允许其访问私网。

Hillstone设备在L2TP协议隧道组网中充当LNS的角色，它接受来自L2TP客户端或LAC的连接，进行用户认证与授权，为合法用户分配IP地址、DNS服务器地址和WINS服务器地址。

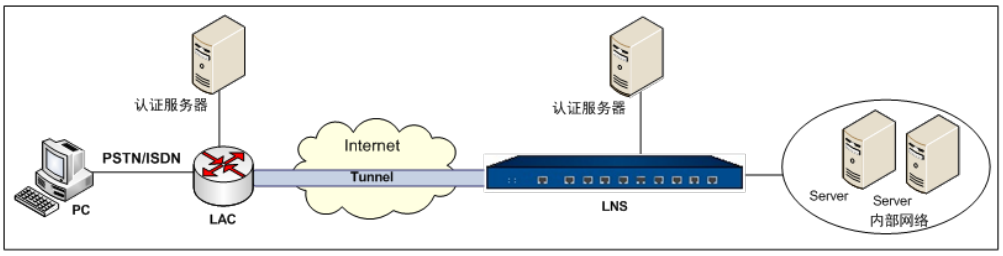
说明：关于L2TP协议的更多详细信息，请参阅RFC2661。

典型的L2TP隧道组网

以下为两种典型的L2TP隧道组网模式：



上图为L2TP客户端直接向LNS发出连接请求并建立隧道的组网模式。任何一台装有Windows 2000/2003/XP/Vista或Linux操作系统的计算机都可以充当L2TP客户端。



上图为远程拨号用户通过PSTN/ISDN拨入LAC后，由LAC向LNS发起VPN连接并建立隧道的组网模式。LAC是为远程拨号用户提供接入服务的设备。它位于远程拨号用户和LNS之间，负责它们之间的

数据转发。LAC与远程拨号用户的连接使用PPP协议或采用本地连接，与LNS端的连接需要利用L2TP协议在它们之间建立隧道。

L2TP over IPSec

L2TP协议不对隧道传输中的数据进行加密，因此在传输过程中无法保证数据的安全。用户可以将L2TP协议和IPSec协议结合使用，利用IPsec协议对数据进行加密的优势，保证L2TP隧道传输中的数据安全。

配置L2TP over IPSec，请按照以下步骤进行：

1. 配置L2TP 客户端，并确保客户端启用IPSec数据加密。客户端的配置方法，请参阅相应操作系统的使用手册。Windows XP操作系统的L2TP客户端配置，可参阅本章的L2TP over IPSec配置举例。
2. 配置IPSec VPN。具体操作，请参阅“IPSec协议”。
3. 配置L2TP实例，并引用已创建的IPSec隧道。
4. 配置策略规则。

使用Windows操作系统的L2TP客户端时，应注意以下事项：

- Windows操作系统的L2TP客户端仅支持主模式的IKE协商。因此用户需要将LNS端的IKE协商模式配置为主模式，同时需要配置accept-all-peer-id命令使ISAKMP网关接受任意的对端ID。配置后，LNS端将不对其IPSec VPN对端的IP地址进行认证。其他操作系统的L2TP客户端是否支持野蛮模式，请参阅其使用手册。
- Windows操作系统的IPSec协议操作模式仅支持传输模式（transport），因此用户需要将LNS端的IPSec协议操作模式配置为传输模式。

LNS端配置

LNS端的配置包括：

- 地址池配置
- L2TP实例配置
- 绑定已配置的L2TP 实例到隧道接口

- 强制断开L2TP连接
- 隧道重启

地址池配置

LNS通过地址池给用户分配IP地址。当用户连接LNS成功后，LNS会从地址池里取出一个IP地址与其它相关参数（如DNS服务器地址与WINS服务器地址等）一起分配给用户。在全局配置模式，使用以下命令创建L2TP地址池：

l2tp pool *pool-name*

- *pool-name* – 指定地址池的名称。

执行该命令后，系统创建指定名称的地址池，并且进入L2TP地址池配置模式；如果指定的名称已存在，则直接进入L2TP地址池配置模式。在全局配置模式下，使用该命令no的形式删除指定的L2TP地址池：

no l2tp pool *pool-name*

在L2TP地址池配置模式下可进行如下配置：

- 配置地址池地址范围
- 配置保留地址池
- 配置IP地址绑定规则

配置地址池地址范围

为地址池配置地址范围，在L2TP地址池配置模式下使用以下命令：

address *start-ip end-ip*

- *start-ip* – 指定IP范围的起始IP地址。
- *end-ip* – 指定IP范围的结束IP地址。

用户可以为一个地址池最多指定60000个IP地址。

在L2TP地址池配置模式下，使用该命令no的形式删除配置的IP地址范围：

no address

配置保留地址池

保留地址池中的IP地址为地址池中的部分IP地址，当LNS从地址池里取出IP地址分配给用户时，需要保留已经被占用的部分IP地址（如网关、FTP服务器等），不进行分配。配置保留地址池，在L2TP地址池配置模式下使用以下命令：

exclude-address *start-ip end-ip*

- *start-ip* – 指定保留地址池的起始IP地址。
- *end-ip* – 指定保留地址池的终止IP地址。

在L2TP地址池配置模式下，使用该命令no的形式取消保留地址池的配置：

no exclude *address*

配置IP地址绑定规则

L2TP通过创建和执行IP地址绑定规则来满足客户端的固定IP地址需求。IP地址绑定规则包括静态IP地址绑定规则和角色-IP地址绑定规则。静态IP地址绑定规则将客户端用户与已配置地址池中的某个固定IP地址绑定，当客户端连接成功后，系统会将绑定的IP地址分配给客户端；角色-IP地址绑定规则是将角色与已配置地址池中的某一IP地址范围绑定，当此客户端连接成功后，系统会从绑定的地址范围中取出一个IP地址分配给客户端。

当LNS通过地址池给客户端分配IP地址时，系统会按照一定的顺序对客户端的IP地址绑定规则进行检查，决定如何为客户端分配IP地址：

1. 检查是否已为客户端用户配置静态IP地址绑定规则，如果是，则将绑定的IP地址分配给客户端；否则，需要进一步检查。注意，如果此静态IP地址绑定规则中的IP地址已被占用，则该用户无法登录。
2. 检查是否已为客户端用户配置角色-IP地址绑定规则，如果是，则从绑定的地址范围中取出一个IP地址分配给客户端；否则，该用户无法登录。

注意: 静态IP地址绑定规则中的IP地址和角色-IP地址绑定规则中的IP地址不能重叠。

配置静态IP地址绑定规则

配置静态IP地址绑定规则，在L2TP地址池配置模式下使用以下命令：

ip-binding user *user-name ip-address*

- **user** *user-name* – 指定客户端用户名。
- *ip-address* – 指定绑定的IP地址。此地址必须为地址池中可以分配的地址。

在L2TP地址池配置模式下，使用该命令no的形式取消对特定用户静态IP地址绑定规则的配置：

no ip-binding user *user-name*

配置角色-IP地址绑定规则

配置角色-IP地址绑定规则，在L2TP地址池配置模式下使用以下命令：

ip-binding role *role-name* **ip-range** *start-ip end-ip*

- **role** *role-name* – 指定角色名称。
- **ip-range** *start-ip end-ip* – 指定绑定的IP范围的起始IP地址start-ip和结束IP地址end-ip。此地址范围必须为地址池中可以分配的地址范围。

在L2TP地址池配置模式下，使用该命令no的形式取消对特定角色的角色-IP地址绑定规则的配置：

no ip-binding role *role-name*

修改角色-IP地址绑定规则排列顺序

一个用户可以绑定到一个或者多个角色，不同角色可以配置不同的角色-IP地址绑定规则。对于绑定到多个角色且多个角色有相应的角色-IP地址绑定规则的用户，Hillstone设备会对角色-IP地址绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。默认情况下，系统会将新创建的规则放到所有规则的末尾，管理员可以移动已有的角色-IP地址绑定规则从而改变规则的排列顺序。改变规则的排列顺序，在L2TP地址池配置模式下使用以下命令：

move *role-name1* {**before** *role-name2* | **after** *role-name2*| **top** | **bottom**}

- *role -name1* – 指定被移动的角色-IP地址绑定规则的角色名称。
- **before** *role-name2* – 将角色-IP地址绑定规则移动到某个角色-IP地址绑定规则(角色名称为role-name2的规则)之前。

- **after** *role-name2* – 将角色-IP地址绑定规则移动到某个角色-IP地址绑定规则(角色名称为role-name2的规则)之后。
- **top** – 将角色-IP地址绑定规则移动到所有角色-IP地址绑定规则之首。
- **bottom** – 将角色-IP地址绑定规则移动到所有角色-IP地址绑定规则的末尾。

L2TP 实例配置

创建L2TP实例，在全局配置模式下，使用以下命令：

tunnel l2tp *tunnel-name*

- *tunnel-name* – 指定L2TP实例的名称。

执行该命令后，系统创建指定名称的L2TP实例，并且进入L2TP实例配置模式；如果指定的名称已存在，则直接进入L2TP实例配置模式。在全局配置模式下，使用该命令no的形式删除指定的L2TP实例：

no tunnel l2tp *tunnel-name*

在L2TP实例配置模式下，用户可以进行如下配置：

- 指定分配IP方式
- 指定地址池
- 配置DNS服务器
- 配置WINS服务器
- 指定隧道出接口
- 指定AAA服务器
- 指定PPP认证的协议
- 指定Hello报文间隔
- 启用隧道认证
- 指定隧道密码

- 指定LNS本端名称
- 启用AVP数据隐含
- 指定隧道接受窗口大小
- 配置用户同名登录功能
- 允许或禁止用户指定IP地址
- 指定控制报文重传次数
- 引用IPSec隧道
- 配置LCP强制协商

指定分配IP方式

LNS通过地址池或本地AAA认证服务器给用户分配IP地址和DNS服务器地址。默认情况下，LNS通过地址池分配IP地址。

为L2TP实例指定分配IP地址方式，在L2TP实例配置模式下，使用以下命令：

```
assign-client-ip from { pool | aaa-server }
```

- **pool** – 指定地址池为用户分配IP地址和DNS服务器地址。
- **aaa-server** – 指定本地AAA认证服务器为用户分配IP地址和DNS服务器地址。

注意: 所指定的本地AAA认证服务器类型必须是Radius类型。

指定地址池

为L2TP实例指定L2TP地址池，在L2TP实例配置模式下，使用以下命令：

```
pool pool-name
```

- *pool-name* – 指定已配置的L2TP地址池名称。

在L2TP实例配置模式下，使用该命令no的形式取消地址池的指定：

```
no pool
```

配置DNS服务器

指定DNS服务器的地址，在L2TP地址池配置模式下使用以下命令：

dns *address1* [*address2*]

- *address1* – 指定DNS服务器IP地址。用户最多可配置2个DNS服务器。

在L2TP地址池配置模式下，使用该命令no的形式取消对DNS服务器的指定：

no dns

配置WINS服务器

指定WINS服务器的地址，在L2TP地址池配置模式下使用以下命令：

wins *address1* [*address2*]

- *address1* – 指定WINS服务器IP地址。用户最多可配置2个WINS服务器。

在L2TP地址池配置模式下，使用该命令no的形式取消对WINS服务器的指定：

no wins

指定隧道出接口

指定隧道出接口，在L2TP实例配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定出接口的名称。

在L2TP实例配置模式下，使用该命令no的形式取消出接口的配置：

no interface

指定AAA服务器

此处指定的AAA服务器为LNS进行L2TP用户身份认证的AAA服务器。指定AAA服务器，在L2TP实例配置模式下，使用以下命令：

aaa-server *aaa-server-name* [**domain** *domain-name* [*keep-domain-name*]]

- *aaa-server-name* – 指定AAA服务器的名称。
- *domain domain-name* – 为AAA服务器指定域名以区分不同的AAA服务器。
- *keep-domain-name* – 指定该参数后， 用于身份认证的用户名将验证域名。

在L2TP实例配置模式下，使用该命令no的形式取消对AAA服务器的指定：

no aaa-server *aaa-server-name* [**domain** *domain-name*]

指定PPP认证的协议

LNS与客户端或LAC建立连接时，在PPP协商的过程中可以对用户使用PAP和CHAP协议进行身份验证。指定PPP认证的协议，在L2TP实例配置模式下，使用以下命令：

ppp-auth {**pap** | **chap** | **any**}

- **pap** – 指定PPP认证方式为密码认证协议PAP。
- **chap** – 指定PPP认证方式为质询握手认证协议CHAP。此选项为默认选项。
- **any** – 指定该参数后，系统首选认证方式为CHAP，如果认证不支持CHAP协议时，则使用PAP协议进行认证。

在L2TP实例配置模式下，使用该命令no的形式恢复默认配置：

no ppp-auth

指定LCP Echo报文发送间隔

在PPP协商过程中LNS会定期发送LCP Echo报文判断链路的连通性。指定LCP Echo报文发送的时间间隔，在L2TP实例配置模式下，使用以下命令：

ppp-lcp-echo interval *time*

- *time* – 指定LCP Echo报文发送的时间间隔。单位为秒。范围是0到1000秒，0秒表示不发送LCP Echo报文。默认值是30秒。

在L2TP实例配置模式下，使用该命令no的形式恢复时间间隔的默认值：

no ppp-lcp-echo interval

指定Hello报文间隔

L2TP 使用Hello 报文来检测隧道是否连通。LNS定时向L2TP客户端或LAC发送Hello 报文，若在一段时间内未收到应答，该隧道连接将被断开。指定Hello报文发送的时间间隔，在L2TP实例配置模式下，使用以下命令：

keepalive *time*

- *time* – 指定Hello报文发送的时间间隔。单位为秒。范围是60到1800秒。默认值是60秒。

在L2TP实例配置模式下，使用该命令no的形式恢复时间间隔的默认值：

no keepalive

启用隧道认证

在隧道建立连接前，用户可启用隧道认证功能以保证连接的安全。隧道认证可由LNS或LAC任何一端发起，只有两端均通过隧道认证，即隧道密码一致时，方可建立隧道。默认情况下，隧道验证功能是关闭状态。在L2TP实例配置模式下，使用以下命令启用该功能：

tunnel-authentication

在L2TP实例配置模式下，使用该命令no的形式禁用隧道认证：

no tunnel-authentication

指定隧道密码

指定LNS端隧道认证的密码，在L2TP实例配置模式下，使用以下命令：

secret *secret-string* [**peer-name** *name*]

- *secret-string* – 指定隧道密码。范围为1至31个字符。
- **peer-name** *name* – 指定LAC端设备的主机名称。如果多个LAC与LNS建立连接，用户可通过配置该项参数为不同的LAC端设备指定不同的隧道密码。如果没有指定该参数，系统对多个LAC端均使用相同的隧道密码。

在L2TP实例配置模式下，使用该命令no的形式取消指定隧道密码：**no secret** *secret-string* [**peer-name** *name*]

指定LNS本端名称

用户可以在LNS端指定本端隧道的名称，在L2TP实例配置模式下，使用以下命令：

local-name *name*

- *name* – 指定LNS端隧道的名称。范围为1至31个字符。默认值为“LNS”。

在L2TP实例配置模式下，使用该命令no的形式恢复默认值：

no local-name

启用AVP数据隐含

L2TP协议使用AVP（attribute value pair，属性值对）来传递和协商L2TP 的一些参数、属性等。在默认情况下，AVP 是采用明文形式传输的。为了保证数据安全，用户可以通过隧道密码加解密这些数据，将这些AVP 隐藏起来传输。在L2TP实例配置模式下，使用以下命令启用或禁用AVP数据隐含功能：

- 启用AVP数据隐含：**avp-hidden**
- 禁用AVP数据隐含（默认配置）：**no avp-hidden**

注意: 启用AVP数据隐含功能需要配置隧道密码。

指定隧道接受窗口大小

传送数据时，用户可以指定隧道传输数据的窗口大小。在L2TP实例配置模式下，使用以下命令：

tunnel-receive-window *window-size*

- *window-size* – 指定窗口大小。单位为包，默认值为8包，取值范围为4至800包。

在L2TP实例配置模式下，使用该命令no的形式恢复默认值：

no tunnel-receive-window

配置用户同名登录功能

用户同名登录功能指允许同一个用户在多个地点同时登录认证。默认情况下，此功能为开启状态。在L2TP实例配置模式下，使用以下命令启用或禁用用户同名登录功能：

- 启用用户同名登录：**allow-multi-logon**
- 禁用用户同名登录：**no allow-multi-logon**

允许或禁止客户端指定IP地址

默认情况下，客户端的IP地址由LNS从地址池中取出并自动分配。启用该功能后，用户可以指定IP地址，但该IP地址必须属于已指定的地址池范围之内且与用户的用户名和角色一致。如果指定的IP地址已被占用，则系统禁止该用户登录。在L2TP实例配置模式下，使用以下命令允许或禁止指定IP地址：

- 允许客户端指定IP地址（默认配置）：**accept-client-ip**
- 禁止客户端指定IP地址：**no accept-client-ip**

指定控制报文重传次数

L2TP协议使用两种类型的报文：控制报文和数据报文。控制报文负责创建、维护及清除L2TP隧道，数据报文负责传输数据。数据报文的传输是不可靠传输，若数据丢失，则不进行数据重传。控制报文的传输是可靠传输，如果在指定的重传次数内未收到对端的响应，则系统认为隧道连接已经断开。控制报文重传间隔从1秒开始，按照2的倍数增长，如1秒、2秒、4秒、8秒、16秒等。指定控制报文重传次数，在L2TP实例配置模式下，使用以下命令：

transmit-retry *times*

- *times* – 指定控制报文重传次数。范围是1至10次。默认值为5次。

在L2TP实例配置模式下，使用该命令no的形式恢复控制报文重传次数的默认值：

no transmit-retry

引用IPSec隧道

用户在配置L2TP over IPSec时，需要将IPSec隧道与L2TP隧道结合用来加密数据。在L2TP实例配置模式下，使用以下命令在L2TP实例中引用IPSec隧道：

next-tunnel ipsec *tunnel-name*

- *tunnel-name* – 指定已创建的IPSec VPN的隧道名称。

在L2TP实例配置模式下，使用该命令no的形式取消引用IPSec隧道：

no next-tunnel ipsec

配置LCP强制协商

远程拨号用户拨入LAC后，由LAC向LNS发起L2TP VPN连接并建立隧道。当LNS再次对用户进行验证时，可配置LNS是否与L2TP客户端进行LCP（Link Control Protocol，链路控制协议）强制协商。

默认情况下，LNS不与L2TP客户端进行LCP强制协商，而是根据ICCN（Incoming-Call-Connected）报文中Proxy Authen Type AVP所指定的认证方式对L2TP客户端进行认证。系统支持PAP与CHAP认证两种类型。

用户可配置LNS与L2TP客户端进行LCP强制协商，在L2TP实例配置模式下，使用如下命令：

ppp-lcp-force

关闭强制协商，使用**no ppp-lcp-force**命令。

在远程用户直接向LNS发起L2TP VPN连接并建立隧道的场景下，ICCN（Incoming-Call-Connected）报文中不会携带Proxy Authen Type AVP，无论用户是否开启和关闭LCP强制协商，LNS都将于L2TP客户端进行LCP强制协商。

绑定L2TP实例到隧道接口

配置好的L2TP实例需要绑定到隧道接口，才能够生效。每一个隧道接口只能绑定一个L2TP实例。当一个L2TP实例只绑定一个隧道接口并且没有为此L2TP隧道（绑定L2TP实例的隧道）指定域名时，所有拨入此LNS的客户端将被划分到此隧道对应的VR中。

用户也可将多个隧道接口绑定到一个L2TP实例并为每一个L2TP隧道指定不同的域名。当客户端发起L2TP VPN连接并完成用户认证后，系统将根据客户端用户的域名，将客户端接入到指定了相同域名的隧道中。当隧道接口属于不同的VR时，LNS可通过认证服务器将内网资源地址重复分配给每个L2TP隧道中的客户端。绑定L2TP实例到隧道接口，在隧道接口配置模式下，使用以下命令：

tunnel l2tp *tunnel-name* [**bind-to-domain** *domain-name*]

- *tunnel-name* – 指定系统中已配置的L2TP实例的名称。
- **bind-to-domain** *domain-name* – 为L2TP隧道绑定域名（即domain name）。绑定域名后，如果登陆用户的用户名不存在域名，拨号将失败。如果没有为L2TP实例绑定域名，LNS进行认证时将忽略登录用户的域名。

在隧道接口配置模式下使用该命令no的形式取消隧道接口与L2TP实例的绑定以及指定的域名：

no tunnel l2tp *tunnel-name*

在隧道接口配置模式下使用如下命令取消指定的域名：

no tunnel l2tp *tunnel-name* **bind-to-domain** *domain-name*

强制断开L2TP连接

用户可以通过命令强制断开某个用户与LNS的连接。强制断开连接，在执行模式下使用以下命令：

exec l2tp *tunnel-name* **kickout user** *user-name*

- tunnel-name – 指定L2TP实例的名称。
- user-name – 指定被强制断开连接的用户名。

隧道重启

隧道重启后，所有与该隧道的连接将被清除。在任何模式下，使用以下命令重启隧道：

clear l2tp t*unnel-name*

- *tunnel-name* – 指定L2TP实例的名称。

显示L2TP信息

用户可以通过show命令查看系统L2TP信息。

- 显示L2TP实例信息：

show tunnel l2tp [*l2tp-tunnel-name*]

- 显示已创建的L2TP隧道的状态信息：

show l2tp tunnel *l2tp-tunnel-name*

- 显示L2TP实例当前在线的客户端信息：

show l2tp client {*tunnel-name l2tp-tunnel-name* [**user** *user-name*]|
tunnel-id *ID*}

- 显示L2TP地址池的配置信息：

show l2tp pool [*pool-name*]

- 显示L2TP地址池的统计信息：

show l2tp pool *pool-name* **statistics**

- 显示所有L2TP实例当前在线的客户端信息：

show auth-user l2tp [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]

L2TP客户端配置

如果采用L2TP客户端和Hillstone设备（LNS）之间建立L2TP隧道的组网模式，用户需要对L2TP客户端进行配置。关于Windows 2000/2003/XP/Vista操作系统的L2TP信息，请参阅Windows 2000/2003/XP/Vista操作系统相关文档。

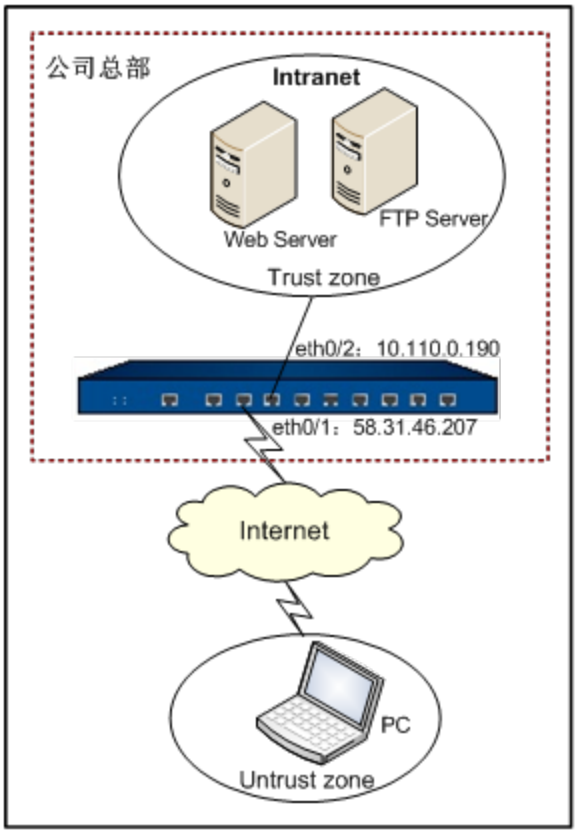
注意: 使用Windows操作系统的L2TP客户端拨号连接LNS时，请确保系统中未安装Hillstone Secure Defender。

L2TP配置举例

本节介绍L2TP的配置实例。

组网需求

某员工需要通过L2TP VPN 远程访问公司总部的内网资源，组网图如下：



配置步骤

该组网的配置分为LNS配置和L2TP客户端配置。

LNS配置

第一步：配置Hillstone设备的接口：

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 58.31.46.207/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 10.110.0.190/24
```

```
hostname(config-if-eth0/2)# exit
hostname(config)#
```

第二步：配置本地AAA认证服务器：

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# password 123456
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

第三步：配置LNS地址池，并指定地址池IP范围：

```
hostname(config)# l2tp pool pool1
hostname(config-l2tp-pool)# address 10.232.241.2 10.232.244.254
hostname(config-l2tp-pool)# exit
hostname(config)#
```

第四步：配置L2TP实例：

```
hostname(config)# tunnel l2tp test
hostname(config-tunnel-l2tp)# pool pool1
hostname(config-tunnel-l2tp)# dns 202.106.0.20 10.188.7.10
hostname(config-tunnel-l2tp)# interface ethernet0/1
hostname(config-tunnel-l2tp)# ppp-auth any
hostname(config-tunnel-l2tp)# keepalive 1800
hostname(config-tunnel-l2tp)# aaa-server local
hostname(config-tunnel-l2tp)# exit
hostname(config)#
```

第五步：创建隧道接口并绑定L2TP实例“test”到该接口：

```
hostname(config)# interface tunnel1
```

```
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 10.232.241.1 255.255.248.0
hostname(config-if-tun1)# manage ping
hostname(config-if-tun1)# tunnel l2tp test
hostname(config-if-tun1)# exit
hostname(config)#
```

第六步：配置策略规则：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

客户端配置

本部分以配置Windows XP操作系统的L2TP客户端程序为例，说明配置步骤：

1. 创建L2TP拨号连接。
2. 配置已创建的拨号连接，修改相关属性。
3. 修改注册表禁用IPSec加密。

创建L2TP拨号连接

按照以下步骤创建Windows XP操作系统的L2TP拨号连接：

1. 点击“开始菜单→控制面板→网络和Internet 连接”。
2. 选择“创建一个到您的工作位置的网络连接”，系统弹出新建连接向导对话框。
3. 选择“虚拟专用网络连接”的单选按钮，并点击“下一步”。
4. 在“公司名”文本框中指定此连接的名称“L2TP”；并点击“下一步”。
5. 选择“不拨此初始连接”的单选按钮，并点击“下一步”。
6. 在“主机名或IP地址”文本框中输入LNS的IP 地址“58.31.46.207”，点击“下一步”。
7. 根据连接向导，完成L2TP客户端其它配置。

配置L2TP拨号连接

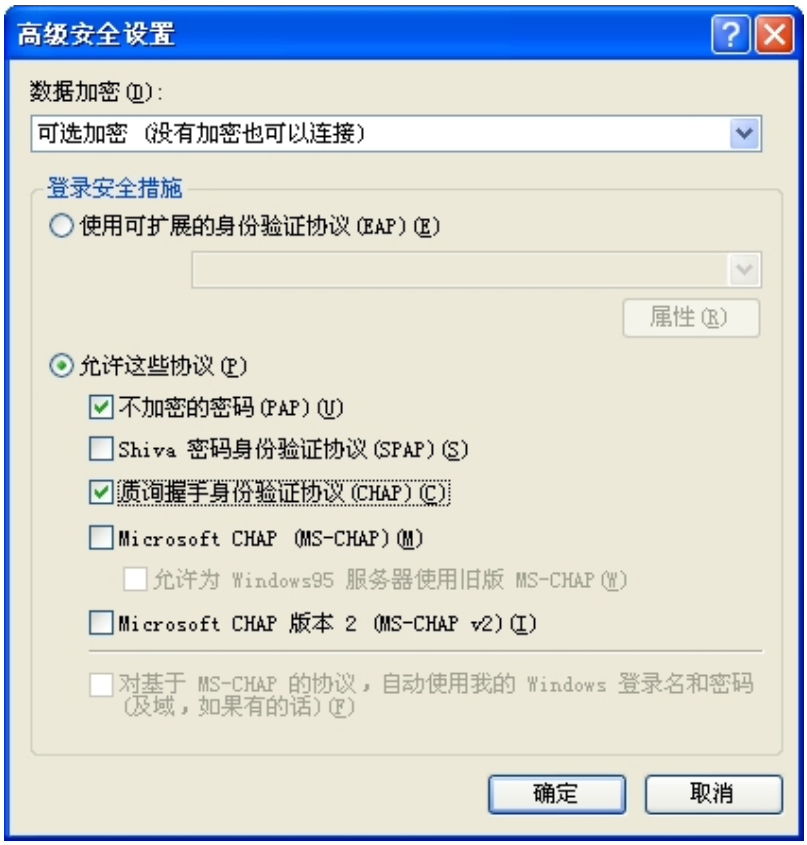
按照以下步骤修改已创建的拨号连接的属性：

1. 打开“网上邻居”，双击网络连接中已创建的拨号连接名称“L2TP”，打开连接L2TP对话框。如下图所示：

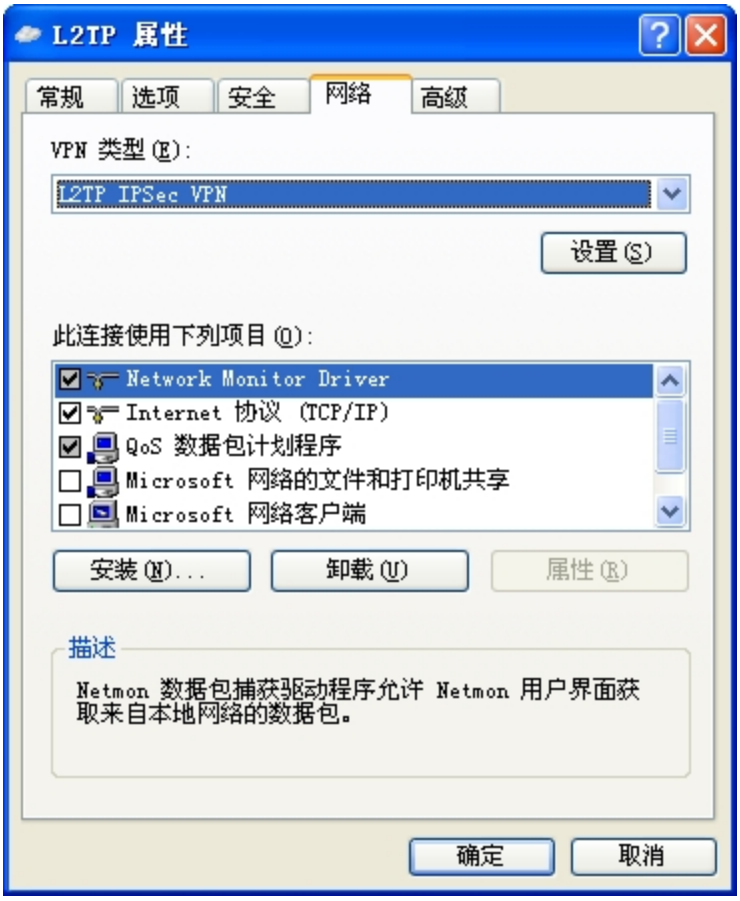
2. 点击“属性”，打开L2TP属性对话框。

3. 点击L2TP属性的“安全”标签，选择“高级（自定义设置）”单选按钮，并点击其后的“设置”，弹出高级安全设置对话框。

4. 在“数据加密”下拉菜单中选择“可选加密（没有加密也可以连接）”，在“登录安全措施”框内选择“允许这些协议”的单选按钮，并勾选“不加密的密码（PAP）”和“质询握手身份验证协议（CHAP）”前的复选框。点击“确定”。如下图所示：



5. 点击L2TP属性对话框的“网络”标签，在“VPN类型”下拉菜单中选择“L2TP IPSec VPN”，勾选“此连接使用下列项目”栏内的“Internet 协议（TCP/IP）”。如下图所示：



6. 点击“确定”，保存所做的修改。

修改注册表

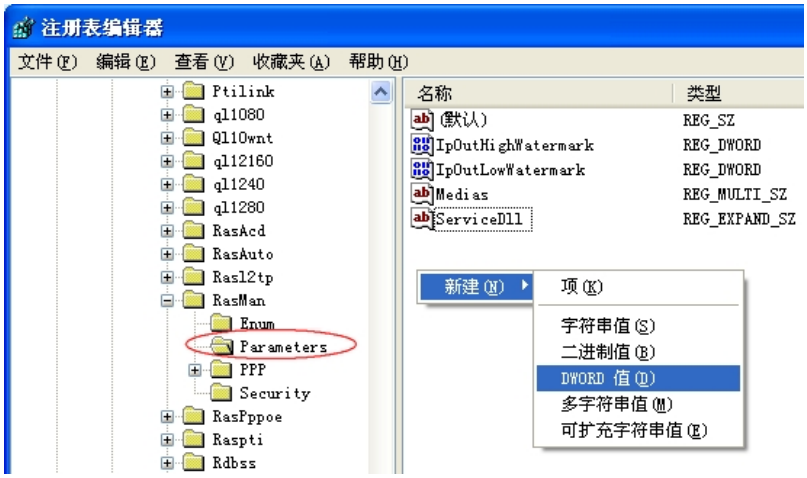
默认情况下，Windows XP操作系统对L2TP连接启用IPSec加密。用户可以通过修改Windows XP的注册表来禁用这种默认行为。如果没有禁用IPSec加密，L2TP客户端在拨号过程中会被自动断开连接。

按照以下步骤修改注册表：

1. 点击“开始菜单→运行”，在运行对话框中输入“Regedt32”，弹出注册表编辑器窗口。

2. 在左侧注册表项目中逐级点击HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\Parameters。

3．为Parameters参数添加DWORD值。单击Parameters项，然后在注册表编辑器右侧空白处单击鼠标右键，弹出右键菜单。选择“新建→DWORD值”，如下图所示。指定该值名称为“ProhibitIPSec”、数据类型为“REG_DWORD”、值为“1”。点击“确定”，保存所做的修改。



4．退出注册表编辑器，重新启动计算机以使改动生效。

使用客户端连接LNS

完成LNS和客户端的配置后，用户可以使用已配置的客户端对LNS发起VPN连接并建立隧道。

使用客户端连接LNS，用户需要打开“网上邻居”，双击网络连接中已创建的拨号连接“L2TP”，在弹出的连接对话框中输入用户名“shanghai”和密码“123456”，然后点击“连接”。如下图所示：

拨号连接成功后，该名在上海的员工就可以通过L2TP协议安全地访问公司的Web服务器和FTP服务器。

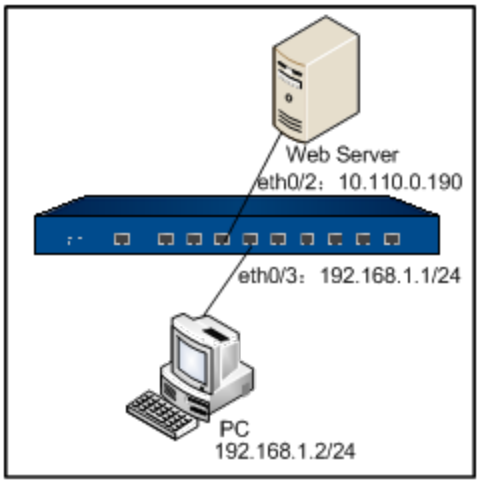
在MS-DOS方式下输入“ipconfig”，系统返回一个LNS地址池中的地址“10.232.241.2 15”，即LNS分配给他的PC的IP地址。

L2TP over IPSec配置举例

本节介绍L2TP over IPSec的配置实例。

组网需求

某员工需要通过L2TP VPN访问公司的Web资源，PC与LNS之间的数据通过IPSec协议加密后传输。组网图如下：



配置步骤

该组网的配置分为LNS配置和L2TP客户端配置。

LNS配置

第一步：配置Hillstone设备的接口：

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 10.110.0.190/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone untrust
hostname(config-if-eth0/3)# ip address 192.168.1.1/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

第二步：配置IPSec VPN：

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# hash sha
```

```
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/3
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# accept-all-peer-id
hostname(config-isakmp-peer)# mode main
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# aaa-server local
hostname(config)# tunnel ipsec vpn1 auto
hostname(config-tunnel-ipsec-auto)# mode transport
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# accept-all-proxy-id
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

第三步：配置本地AAA认证服务器：

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# password 123456
hostname(config-user)# exit
```

```
hostname(config-aaa-server)# exit
hostname(config)#
```

第四步：配置LNS地址池，并指定地址池IP范围：

```
hostname(config)# l2tp pool pool2
hostname(config-l2tp-pool)# address 10.10.10.2 10.10.10.100
hostname(config-l2tp-pool)# exit
hostname(config)#
```

第五步：配置L2TP实例，并引用IPSec隧道：

```
hostname(config)# tunnel l2tp l2tp1
hostname(config-tunnel-l2tp)# pool pool2
hostname(config-tunnel-l2tp)# dns 202.106.0.20
hostname(config-tunnel-l2tp)# interface ethernet0/3
hostname(config-tunnel-l2tp)# next-tunnel ipsec vpn1
hostname(config-tunnel-l2tp)# ppp-auth chap
hostname(config-tunnel-l2tp)# keepalive 1800
hostname(config-tunnel-l2tp)# aaa-server test
hostname(config-tunnel-l2tp)# exit
hostname(config)#
```

第六步：创建隧道接口并绑定L2TP实例“l2tp1”到该接口：

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone dmz
hostname(config-if-tun1)# ip address 10.10.10.1/24
hostname(config-if-tun1)# manage ping
hostname(config-if-tun1)# tunnel l2tp l2tp1
hostname(config-if-tun1)# exit
hostname(config)#
```

第七步：配置策略规则：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone dmz
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

客户端配置

本部分以配置Windows XP操作系统的L2TP客户端程序为例，说明配置步骤：

1. 创建L2TP拨号连接。
2. 配置已创建的拨号连接，修改相关属性。
3. 启用IPSec加密。

创建L2TP拨号连接

按照以下步骤创建Windows XP操作系统的L2TP拨号连接：

1. 点击“开始菜单→控制面板→网络和Internet 连接”。
2. 选择“创建一个到您的工作位置的网络连接”，系统弹出新建连接向导对话框。
3. 选择“虚拟专用网络连接”的单选按钮，并点击“下一步”。
4. 在“公司名”文本框中指定此连接的名称“L2TP over IPSec”；并点击“下一步”。

5. 选择“不拨此初始连接”的单选按钮，并点击“下一步”。

6. 在“主机名或IP地址”文本框中输入LNS的IP 地址“192.168.1.1”，点击“下一步”。

7. 根据连接向导，完成L2TP客户端其它配置。

配置L2TP拨号连接

按照以下步骤修改已创建的拨号连接的属性：

1. 打开“网上邻居”，双击网络连接中已创建的拨号连接名称“L2TP over IPSec”，打开连接L2TP over IPSec对话框。

2. 点击“属性”，打开属性对话框。

3. 点击标签页，进行属性的详细配置，配置如下：

   - “安全”标签页的配置：

   - 选择“高级（自定义设置）”单选按钮，并点击其后的“设置”，弹出高级安全设置对话框。在“数据加密”下拉菜单中选择“可选加密（没有加密也可以连接）”，在“登录安全措施”框内选择“允许这些协议”的单选按钮，并勾选“不加密的密码（PAP）”和“质询握手身份验证协议（CHAP）”前的复选框。点击“确定”。

   - 选择“IPSec设置”，在弹出的对话框中勾选“使用预共享的密钥作身份验证”并输入密钥“hello1”。点击“确定”。

   - “网络”标签页的配置：在“VPN类型”下拉菜单中选择“L2TP IPSec VPN”，并勾选“此连接使用下列项目”栏内的“Internet 协议（TCP/IP）”。

4. 点击“确定”按钮，保存配置并关闭属性对话框。

启用IPSec加密

默认情况下，Windows XP操作系统对L2TP连接启用IPSec加密。如果禁用了IPSec加密，用户也可以通过修改注册表来重新启用这种默认行为。

按照以下步骤修改注册表：

1．点击“开始菜单→运行”，在运行对话框中输入“Regedt32”，弹出注册表编辑器窗口。

2．在左侧注册表项目中逐级点击HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\Parameters。

3．为Parameters参数添加DWORD值。单击Parameters项，然后在注册表编辑器右侧空白处单击鼠标右键，弹出右键菜单。选择“新建→DWORD值”。指定该值名称为“ProhibitIPSec”、数据类型为“REG_DWORD”、值为“0”。点击“确定”，保存所做的修改。

4．退出注册表编辑器，重新启动计算机以使改动生效。

使用客户端连接LNS

完成LNS和客户端的配置后，用户可以使用已配置的客户端对LNS发起VPN连接并建立隧道。使用客户端连接LNS，用户需要打开“网上邻居”，双击网络连接中已创建的拨号连接“L2TP over IPSec”，在弹出的连接对话框中输入用户名“shanghai”和密码“123456”，然后点击“连接”。拨号连接成功后，该员工就可以通过L2TP协议安全地访问公司的Web资源。