

Hillstone 山石网科多核安全网关

基础配置手册

version 5.0

www.hillstonenet.com.cn

目录	2
关于本手册 5	5
手册内容	5
手册约定	5
内容约定	5
第1章 设备管理1	L
设备管理介绍1	L
终端 Console 登录1	L
WebUI 方式登录1	L
恢复出厂设置	2
通过 CLI 方式	2
通过 WebUI 方式	2
通过 CLR 按键方式	ł
StoneOS版本升级	ł
通过网络迅速升级 StoneOS(TFTP)4	ł
通过 WebUI 方式升级 StoneOS	5
许可证安装	3
通过 CLI 方式安装	3
通过 WebUI 方式安装	3
第2章基础上网配置10)
基础上网配置介绍10)
接口配置10)
路由配置11	Ĺ
策略配置13	3
源 NAT 配置	3
第3章常用功能配置15	5
常用配置介绍15	5
PPPoE 配置15	5
DHCP 配置17	7
IP-MAC 绑定配置18	3
端到端 IPsec VPN 配置20)

SCVPN 配置	27
DNAT 配置	
一对一 IP 映射	35
一对一端口映射	
一对多映射(包含服务器负载均衡)	
第4章 链路负载均衡	42
链路负载均衡介绍	
基于目的路由的负载均衡	43
基于源路由的负载均衡	
智能链路负载均衡	45
第 5 章 QoS 配置	47
QoS 介绍	
IP QoS 配置	47
应用 QoS 配置	
混合 QoS 配置	
QoS 白名单配置	53
第 6 章 网络行为控制	54
URL 过滤 (有 URL 许可证)	54
配置自定义 URL 库	58
URL 过滤 (无 URL 许可证)	59
网页关键字过滤	60
网络聊天控制	64
第 7 章 VPN 高级配置	67
基于 USB Key 的 SCVPN 配置	67
新建 PKI 信任域	67
配置 SCVPN	72
制作 USB Key	73
使用 USB Key 方式登录 SCVPN	75
PnPVPN	77
用户配置	78
IKE VPN 配置	80
隧道接口配置	
策略配置	85
PnPVPN 客户端配置	86
第8章 高可靠性	

高可靠性介绍	 	38
高可靠性配置	 	39

关于本手册

手册内容

本手册为 Hillstone 山石网科多核安全网关的基础配置手册,对 Hillstone 山石网科多核安全 网关的主要功能模块配置进行介绍,帮助用户快速掌握安全网关的 WebUI 配置。适用于 StoneOS 5.0 以及以上版本。具体内容包括:

- ◆ 第1章:设备管理。介绍登录方式、StoneOS升级以及许可证安装等。
- ◆ 第2章:基础上网配置。介绍接口、路由、策略等基本上网配置。
- ◆ 第3章:常用功能配置。介绍 PPPoE 拨号、动态地址分配 DHCP、DNAT 等配置。
- ◆ 第4章:链路负载均衡。介绍基于目的路由、源路由、策略路由的流量负载配置等。
- ◆ 第5章: QoS配置。介绍 QoS 功能及配置。
- ◆ 第6章:网络行为控制配置。介绍 URL 过滤、网页关键字以及网络聊天控制配置。
- ◆ 第7章: VPN 高级配置。介绍基于 USB Key 的 SCVPN 配置以及 PnPVPN 配置。
- ◆ 第8章:高可靠性。介绍高可靠性(HA)的配置。

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"。



第1章 设备管理

设备管理介绍

为方便管理员管理与配置,安全网关支持本地(Console 口)与远程(Telnet、SSH、HTTP 以及 HTTPS)两种环境配置方法,可以通过 CLI 和 WebUI 两种方式进行配置。

终端 Console 登录

通过 Console 口,用户可登录安全网关设备的 CLI,从而使用命令行对设备进行配置。在计算机上运行终端仿真程序(系统的超级终端、SecureCRT等)建立与安全网关的连接。按照表1配置终端参数:

表1:配置终端参数

参数	数值
波特率	9600 bit/s
数据位	8
奇偶校验	无
停止位	1

WebUI 方式登录

WebUI 是最方便、直观、简单的配置方式,WebUI 同时支持 http 和 https 两种访问方式。 安全网关的 ethernet0/0 接口配有默认 IP 地址 192.168.1.1/24,初次使用安全网关时,用户可 以通过该接口访问安全网关的 WebUI 页面。

请按照以下步骤:

- 1. 将管理 PC 的 IP 地址设置为与 192.168.1.1/24 同网段的 IP 地址 ,并且用网线将管理 PC 与安全网关的 ethernet0/0 接口进行连接。
- 2. 在管理 PC 的 Web 浏览器中输入地址 "http://192.168.1.1"并按回车键。出现登录页 面如下图所示。



恢复出厂设置

Hillstone 山石网科提供三种方法恢复设备的出厂配置,分别是:

- ◆ 命令行:通过 CLI 使用命令进行恢复
- ◆ WebUI:通过 WebUI 清除配置以恢复出厂配置
- ◆ 物理方法:使用设备的 CLR 按键进行恢复

通过 CLI 方式

通过 CLI 使用命令恢复出厂设置,请按照以下步骤进行操作:

- 1. 在执行模式下,使用 unset all 命令。
- 2. 根据提示,选择是否保存当前配置:y/n。
- 3. 选择是否重启设备: y/n。
- 4. 系统重启后即出厂配置恢复完毕。

```
SG-6000# unset all
Remove all the configuration(back to factory default), are you sure? [y]/n: y
removing configuration...
```

System reboot, are you sure? [y]/n: y

通过 WebUI 方式

通过 WebUI 恢复出厂配置,请按照以下步骤进行操作:



1. 通过 WebUI 方式登录 StoneOS 从工具栏的 <系统管理 > 下拉菜单选择 『配置备份还原』。

如下图所示:

StoneOS									系统管理	∎▼ 対象!	用户→ 工具→
配置			定制 刷新		手动刷新	*			配置	备份还原	天 0 小时 7 分 6
🟠 主页		● 系统信息							配置	文件管理	
网络		序列号: 主机 2 称:	0802025110002122	伯場	软件版本:	Ver	sion 5.0 SG6000-M-5.0	R4.bin 2014/04/04 11:29:4	设备	管理	CPU
 网络连接 MAT 	i	王10.44%。 硬件平台: 系統时间:	SR-320 Aug/4/2014 Mon_01:41:08	編編	IPS特征库: URI库:	<u>1.0</u>	194 2014-06-13 16:15 19 2014-02-25 11:09:	5:07 54	日期	和时间 证	内存
罕 路由 船 IPsec VP	n .	HA状态:	Standalone	编辑	应用特征库:	3.0	<u>140326</u> (标准版) 2014-	03-26 13:53	HA		储卡
SSL VPN	. I	● 流量监控							短信	口令认证参数	_
🚳 L2TP VPI	N	整机流里							连接	HSM	25.
● 月戸识别 ↓↓ 802.1X									SNN	IP	能 议;
📒 链路负载地	均衡	z -							系统	工具	;总数:

2. 在弹出的 < 系统配置备份还原向导 > 对话框,选择 < 恢复出厂配置 > 单选按钮,并点击『下

_						
系统翻譯	皆备份还原向导					8
欢迎(可以 1 选	使用系统配置备份还原向导。 备份当前的系统配置信息。 择要执行的操作: ● 恢复系统配置 ● 备份当前配置 ● 恢复出厂配置 意:配置需重启生效。	通过该向导,	可以将系统商	2 置还原到已保	存的配置或出	─ 鼠 置,也
				上一步	下一步	取消

选择是否重启设备。为使配置生效,用户需重新启动设备。选择<是,立即重新启动设备>
 单选按钮,并点击『完成』按钮。





4. 所有配置将会被清除,然后设备将自动重启。

通过 CLR 按键方式

使用 CLR 按键恢复出厂配置,请按照以下步骤进行操作:

- 1. 关闭安全网关的电源。
- 2. 用针状物按住 CLR 按键的同时打开安全网关的电源。
- 保持按住状态直到指示灯 STA 和 ALM 均变为红色常亮,释放 CLR 按键。此时系统开始恢复出厂配置。
- 4. 出厂配置恢复完毕,系统将会自动重新启动。

StoneOS 版本升级

通过网络迅速升级 StoneOS(TFTP)

Sysloader 可以从 TFTP 服务器获取 StoneOS,从而保证用户能够通过网络迅速升级 StoneOS。请按照以下步骤进行操作:

1. 给设备上电根据提示按 ESC 键并且进入 Sysloader。参照以下操作提示:

```
HILLSTONE NETWORKS
Hillstone Bootloader 1.3.2 Aug 14 2008-19:09:37
DRAM: 2048 MB
BOOTROM: 512 KB
```



2. 从 Sysloader 的操作选择菜单选择通过 TFTP 升级 StoneOS。参照以下操作提示:

Sysloader 1.2.13 Aug 14 2008 - 16:53:42								
1	Load firmware via TFTP							
2	Load firmware via FTP							
3	Load firmware from USB disks (not available)							
4	Select backup firmware as active							
5	Show on-board firmware							
6	Reset							
Please	select: 1 在此处键入"1"并敲回车键							

3. 确保设备与控制主机的连通性,并将需升级的 StoneOS 拷贝到指定目录下。

3CDaemon	
文件 查看 帮助	
TFTP 服务器	启动时间 位置 字节 状态
设置 ITTE 服务器 GO	Nov 12, 2012 10:22:40 本地 0 TFTP 服务器已关闭 Nov 12, 2012 10:22:31 本地 0 正在监听 TFTP 请求于 IP 地址: 192.168.1.2, 端口 69 3CDaemon 设置 工 普通设置 工
TFTF 服务器已经停止(点击这里启 初服务) 纪录至 Iftpd log (点击这里停止 纪录)	引入文件请求时创建目录名? 「 允许覆盖现有文件? 上传/下载目录: C:\Users\YISHAW [~] 1\AppDate\Local\Temp [*]
選び、 調試停止(点击这里启动调试) ごで 清除列表	每数据包超时秒数 (2-15): 5 最大重;武次数 (5-20): 10 内部结构传输间隔 (0-1500): 0
FTF 服务器 Sysleg 服务器 TFTP 客户机	3CDaemon 确定 取消 应用 (A)

4. 依次配置 Sysloader 的 IP 地址、TFTP 服务器的 IP 地址、网关 IP 地址以及 StoneOS 名

称。参照以下操作提示:

Local ip address	[]]: 10 . 2 . 2 . 10 / 16 输入 Sysloader 的 IP 地址并敲回车键							
Server ip address	[]]: 10.2.2.3 输入 TFTP 服务器的 IP 地址并敲回车键							
Gateway ip address	[]]: 10.2.2.1 如果 Sysloader 与 TFTP 服务器的 IP 地址不							
属于同一个网段,输入网关的 IP 地址并敲回车键;否则直接敲回车键									
File name : StoneOS	-3.5R2	输入 StoneOS 名称并敲回车键 , 系统开始通过 TFTP 获取							
StoneOS									



5. 保存 StoneOS。参照以下操作提示:

```
File total length 10482508
Checking the image...
Verified OK
Save this image? [y]/n: y 键入字母 "y" 或者敲回车键,保存获得的 StoneOS
Saving ......
Set StoneOS-3.5R2 as active boot image
```

6. 重启。系统将使用新的 StoneOS 启动。参照以下操作提示:

```
      Please reset board to boot this image

      1
      Load firmware via TFTP

      2
      Load firmware via FTP

      3
      Load firmware from USB disks (not available)

      4
      Select backup firmware as active

      5
      Show on-board firmware

      6
      Reset

      Please select:
      6 在此处键入 "6" 并敲回车键,系统开始重启
```

设备的 Flash 中最多可以储存两个 StoneOS。如果 Flash 中已经保存了两个 StoneOS,请

根据提示对储存的 StoneOS 进行删除。

通过 WebUI 方式升级 StoneOS

1. 通过 WebUI 方式登录 StoneOS,从工具栏的<系统管理>下拉菜单选择 『版本升级』。如

下图所示:

St	oneOS								系统管理	里▼ 対象用.	户▪ 工具▪
â i	<u>配置</u> 回	 系统信息 	定制 刷新		手动刷新	~			配置 配置	备份还原 文件管理	0 小时 34 分 33
● エス ● 网络连接 ● NAT ■ 路由 ● IPsec VPN ● SSL VPN ● SSL VPN ● L2TP VPN ● 用户识别 ■ 802.1X	● 网络连接 NAT ■ 路由 ■ IPsec VPN	序列号: 主机名称: 硬件平台: 系统时间: HA状态:	0802025110002122 SR-300 SR-320 Aug/4/2014 Mon 02:08:33 Standalone	<u>編辑</u> <u>編辑</u> 編辑	软件版本: 病毒特征库: IPS特征库: URL库: 应用特征库:	Versi 2.0.1 1.0.1 1.0.1 3.0.1	ion 5.0 SG6000-M-5.0R4. (<u>40624</u> 20140624 23:08 (<u>94</u> 2014-06-13 16:15:0) (9 2014-02-25 11:09:54 (标准版) 2014-03-	bin 2014/04/04 11:29:4/ :31 7 -26 13:53	设备 日期 HA	管理 和时间 证	CPU 內存 法会话 諸卡
	SSL VPN L2TP VPN 用户识别 802.1X	 ● 流量监控 >>>> >>> >> > >> >>							坦la 连接 SNM	山令认业参数 HSM IP	数:
云服务	磁路负载均衡 运识别	z			没有数据				系统版本	江具 升级 24小时IPS項 0个▶	总数:

2. 在弹出的<版本升级向导>对话框,选择<升级到最新的软件版本>单选按钮,并点击『下

一步』按钮。



版本升级向导	6	3
此向导帮助您升级或者还原系	系统软件 版本	
◉ 升级到最新的软件版本]	
当前版本:	SG6000-M-5.0R4.bin	
◎ 还原为已保存的软件版	本	
已备份版本:	SG6000-M-5.0R3P5.bin	
注意:配置完成后,需要重	启设备以使配置生效。	
	上一步下一步取消	

3. 在 < 选择备份软件版本 > 下拉菜单中选择一个软件版本做为备份 , 然后点击 < 上传新的软件

文件>后的『浏览』按钮并在本地 PC 选择新的软件版本文件。

资中最多可保存两个系: ,另一个将被删除。	统固件。升级新	版本的同时,可以	【选择一个软件	卡版本作为 备
选择备份软件版本:				
SG6000-5.0R1.bin	Y			
一任新的软件文件・				
		浏览		

点击『下一步』。根据需要,选择<是,立即重新启动设备>单选按钮,并点击『完成』按
 钮。为使配置生效,用户需重新启动设备。



版本升级向导		٢
是否重新启动设备,以使配置生效?		
◎ 是,立即重新启动设备		
◎ 否,暂不重新启动设备		
	上一步	í

注意:如果选择暂不重新启动设备,将会在下次重新启动设备后加载新版本 StoneOS。

许可证安装

通过 CLI 方式安装

通过 CLI 使用命令安装许可证,请按照以下步骤进行操作:

1. 登录 StoneOS,在执行模式下,使用 exec license install license-string 命

令(license-string - 要安装的许可证字符串。输入"license:"后的字符串)。如下

图所示:

SG-6000# exec license in SG-6000# exec license install license:MBvPXiU8nWYoITvsovRJSSEqJABvQNeJIFdUQZRtbmwLpRWeJVTyMp1ga6pICcjEnyUjI71hDdOZ1KUdMskhlbdMI70YvS L2DwPKqchcyYreajADsBbb+wIGda08BFZ6rxy5E+cnelYjytdxMI08iP0y+Te3EtGnqKuZfL19BMLtYZQYPFp7CoZfSMONoYL19vuPpZwJL1DGrVKP1eHBWWRI9xZCIFoQmL F13ssrwjjN30xgXVbtMyQOw+C808CNERxPYNmOdKspmVWgzoaX4bAFAqLdkrYLFmnqAQ9biJ9gZhqCnWDu+3CVo8Dx7mpMy+4BAmS2g2IJ5NcCMPE2KQ== 2014-08-04 03:16:51, Event WARNING@MGMT: license plat140804110416 installation succeeded

Info: Successfully install the license

SG-6000#

2. 根据系统提示重启后即完成许可证安装。

通过 WebUI 方式安装

通过 WebUI 安装许可证,请按照以下步骤进行操作:

1. 通过 WebUI 方式登录 StoneOS , 从工具栏的 <系统管理 > 下拉菜单选择 『许可证』。如下 图所示:



St	oneOS								系统管理•) 対象用月	□• 工具•
	配置 -		定制 刷新) Ŧá	カ刷新 🎽				配置备份还原	1 小时 44 分 58
âì	页	● 系统信息							配置文件管理	
网络	网络连接	序列号: 主机名称: 硬件平台:	0802025110002122 SG-6000 SR-320	编辑	软件版本: 病毒特征库: IPS排征库:	Version 5.0 SG600 2.0.140624 20140 1.0.194 2014-06-)0-M-5.0R4.bin 2014/04/04)624 23:08:31 13 16:15:07	11:29:4:	设备管理 日期和时间	CPU 内存
	NAT 路由 IPsec VPN	系统时间: HA状态:	Aug/4/2014 Mon 03:18:58 Standalone	<u>编辑</u> 编辑	URL库: 应用特征库:	1.0.19 2014-02-2 3.0.140326 (标准崩	5 11:09:54 ĝ) 2014-03-26 13:53		<mark>许可证</mark> HA	会话 《储卡
9	SSL VPN	 流量监控 						_	担信口令认证参数	
G	L2TP VPN	整机流量							连接HSM	
後 日	用户识别 802.1X								SNMP	数:
E	链路负载均衡	z -							系统工具 版本升级	i总数:
云服务	【 云识别	¥ _			没有数据				24小时IPS政 0个 •	」 击总数:

- 2. 在弹出的 < 许可证 > 对话框中,许可证列表可查看当前系统许可证的类型和有效时间。
- 3. 在 < 许可证安装 > 处,用户可根据需要,选择手动输入许可证请求或选择上传本地文件。
 - 上传许可证文件:选中<上传许可证文件>单选按钮(许可证为纯文本.txt 文件),点 击『浏览』按钮,并且选中许可证文件;
 - **手动输入**:选中<手动输入>单选按钮,然后将许可证字符串内容(包含"license:" 及之后内容)输入到对应的文本框。

印证列表				
客户	类型	有效时间	其它信息	
hillstone	1 平台试用	350天		
hillstone	TO URL	2013-11-02	Hillstone Networks	
hillstone	S IPS	2013-11-02	Hillstone Networks	
hillstone	◎ 功能试用	365天		
hillstone	5 防病毒	2013-11-02	Kaspersky	
hillstone	っ应用特征库	2013-11-02	Hillstone Networks	
 许可证申请 客户: 地址: 邮编: 联系人: 电话: 电子邮件: 		许可证安装 ◎ 上传许可证 将许可证字符 中	文件 • 手动输入 守串输入到该文本框 •	

4. 点击『确定』按钮保存所做配置,并且重启设备完成许可证的安装。



第2章 基础上网配置

基础上网配置介绍

为使设备实现正常上网,基本配置包括接口、路由、策略以及源 NAT 的配置。

接口配置

接口配置,请按照以下步骤进行操作:

 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->网络->网络连接", 进入网络连接页面。

Sto	oneOS									系统管理▼
	配置 -		网络连接							
企 主!	页	安全	≥域-接口视图 ➤							
网络			🛛 新建 🚽 🦻 滑除							
	网络连接		安全域名称	类型	虚拟路由器/交换机		接口数	策略数	防病毒	入侵防御
- 6	NAT 1. 点击网络i	连接	trust	L3	trust-vr		7	5		
	路由		untrust	L3	trust-vr		2	5	test	
95	IPsec VPN		dmz	L3	trust-vr		0	3		
-	SSI VDN		l2-trust	L2	vswitch1		3	1		
a			l2-untrust	L2	vswitch1		1	0		
	LZIP VPIN		I2-dmz	L2	vswitch1		0	0		
C	用尸识别		VPNHub	L3	trust-vr		0	0		
146	802.1X		HA	L3	trust-vr		2	0		
E B	链路负载均衡		vnn	13	trust-vr		0	0		•
云服务		14 4	□ 第 1 页,总页数1 ▶ ▶	🕹 🛛 每页显示	条月数 20 ¥					泉示9个表项中的1-9
<u> </u>	云识别	•	新建 • 2/编辑 简册除	地宏接口	2					1000 1000 100
±0			接口名称 3 点击编辑	状态	IP/ 擔码	MAC		安全博		接入用户/IP教
2±	54mb		aggregate1	0.0.0	0.0.0.0/0	001c.542	3.38ca	12-trust		0
	東略		aggregate2	Q Q Q Q	0.0.0.0/0	001c.5423	3.38cb	trust		0
	两弯过滤	7	ethernet0/0	* * * *	192.168.1.1/24	001c.5423	3.38c0	untrust		0
	人侵防御		ethernet0/0.2	4244	0.0.0/0	001c.5423	3.38c0	trust		0
	攻击防护		2、选择相应接口 ethernet0/1	Q. Q. Q. Q.	0.0.0.0/0	001c.5423	3.38c1	NULL		0
A	ARP防护		ethernet0/2	Q Q Q Q	0.0.0/0	001c.5423	3.38c2	HA		0
协制			ethernet0/3	Q. Q. Q. Q.	0.0.0/0	001c.5423	3.38c3	HA		0
17.01	大田舎田		ethernet0/4	હે છે. છે. છે.	0.0.0/0	001c.5423	3.38c4	NULL		0
Č	流生自理		ethernet0/5	Q. Q. Q. Q.	0.0.0/0	001c.5423	3.38c5	trust		0
- <u></u>	尝诂限制		ethernet0/6		0.0.0/0	001c.5423	3.38c6	l2-untrust		24
<u></u>	URL过源		ethernet0/7		0.0.0/0	001c.5423	3.38c7	l2-trust		1
<u>I</u>	网页关键字		ethernet0/8		0.0.0/0	001c.5423	3.38c8	l2-trust		0
<u> </u>	Web外发信息		ethernet0/9	Q. Q. Q. Q.	0.0.0/0	001c.5423	3.38c9	NULL		0
C.	邮件过滤		loopback1		2.2.2/24	0000.000	0.0800	trust		0
<u>S</u>	网络聊天		tunnel1		10.10.10.1/24	0000.000	0.0800	trust		0
=	应用行为控制		tunnel2		0.0.0/0	0000.000	0.0000	trust		0
1	全局黑名单		tunnel3		3.3.3.1/24	0000.000	0.0000	trust		0
			vswitchif1		10.88.16.250/24	001c.5423	3.38d6	untrust		0

- 2. 从接口列表中选中需要编辑的接口,双击或者点击列表右上方的『编辑』按钮。
- 3. 在弹出的<接口配置>对话框对接口进行编辑:
 - **绑定安全域**:指定接口的安全域类型。三层接口选择三层安全域,二层接口选择二层安全域;
 - 安全域:选择安全域名称。一般情况下,内网选择trust或l2-trust;外网选择untrust 或l2-untrust。



- IP 配置:为接口配置 IP 地址相关信息。
- 管理方式:指定接口的管理方式。在<管理方式>部分选中需要的管理方式的复选框。

接口配置		8
常规 属性 高级	RIP	
名称: etherne	et0/0	
描述:	(0~63)字符	
绑定安全域: 💿 三层的	安全域 💿 二层安全域 💿 无绑定 安全域类型,三层接口选择三层安全域 💿 无绑定 全域,二层接口选择三层安全域	
安全域: untrust	────────────────────────────────────	
IP配置		
类型: ● 静态I	IP 〇 自动获取IP 〇 PPPoE 三层接口配置ip地址	
IP地址: 192.16	8.1.1	
网络掩码: 255.25	5.255.0	
□ 启用DNS代理		
高级选项 DHC	CP DDNS	
管理方式		
🕑 Telnet 🕑 SSH 🛛 🖉	Ping @ HTTP @ HTTPS @ SNMP 开启接口相应管理方式	
路由		
逆向路由: 🛛 启用	○ 关闭 ● 自动	
		确定取消

提示:如果外网接口使用 PPPoE 拨号方式接入,关于接口的配置请参阅 PPPoE 配置。

路由配置

路由配置,请按照以下步骤进行操作:

- 1. 通过 WebUI 方式登录 StoneOS,从页面左侧导航树选择并点击"配置->网络->路由", 进入路由页面。
- 2. 点击『目的路由』标签,进入目的路由页面。
- 3. 从<虚拟路由器>下拉菜单选择一个 VR,新建的路由将属于该 VR,默认为"trust-vr"。
- 点击目的路由列表左上角的『新建』按钮, 弹出<目的路由配置>对话框, 在该对话框对目 的路由进行编辑:
 - 目的地:指定路由条目的目的 IP。
 - 子网掩码:指定路由条目的目的 IP 对应的子网掩码。
 - 下一跳:指定下一跳类型,选中<网关>或<接口>单选按钮。若选择<网关>,需在<
 网关>文本框中输入网关 IP 地址。若选择<接口>,需在<接口>下拉菜单中选择接口
 名称。如果该接口为 tunnel 的时候,需要在可选栏输入 tunnel 对端的网关地址。如:下一跳网关指定为 122.193.30.97(由运营商提供网关地址)。
 - 优先权: 该参数取值越小, 优先级越高, 而在有多条路由选择的时候, 优先级高的路由



会被优先使用。取值范围是1到255,默认值为1。当优先级为255时,该路由无效。

• 路由权值:路由权值决定负载均衡中流量转发的比重。范围是1到255,默认值是1。

目的路由配置		0	1
目的地: 子网掩码: 下一跳:	0.0.0.0 0 ● 网关 ● 当前系统虚拟路由器	目的地、子网掩码全0表示所 有网段 ② 接口 ③ 其他系统虚拟路由器	
网关: 优先权: 路由权值: 描述:	10.88.16.1 1 1	<mark>指定下一跳,一般是运营商给定网关</mark> (1~255),缺省值:1 (1~255),缺省值:1 (0~63)字符	
		确定取消	

5. 用户可以根据需要,在<描述>文本框中指定目的路由的描述信息。

6. 点击『确定』按钮,完成新建目的路由。

Sto	neOS									系统管理・	I ž
	配置 -	目的路由 源路	油 源接口路由	ISP信息 ISP路	由策略路由	就近探测路由	RIP				
🔒 🗎	হ	虚拟路由器: 1	trust-vr 🕶 IP:		/ 下一跳:		下一跳接	□: Any	~		
		协议: Any	▼ 描述:		搜索	清空					
P398	网络连接	♦ \$63₽	编辑 箭 黑泽								
6	NAT		TD / 检23	下	下一號按口	林政	份生却	应用	欧山坦街	構造	
-	路由	17.765	0.0.0/0	10.88.16.1	vswitchif1	100° 6K 	1	152.1E	ar 四 汉 直 1	20,02	
93	IPsec VPN		1.1.1/32	10.88.16.130	vswitchif1	静态	1	0	1		
- -	SSL VPN		1.10.1.0/24		vswitchif1	直连	0	0	1		
G.	L 2TP VPN		1.10.1.1/32		vswitchif1	主机	0	0	1		
1 🍒	田山田町	A A	2.2.2.0/24		loopback1	直连	0	0	1		
1.9	用/Fictori 902.1X	A A	2.2.2/32		loopback1	主机	0	0	1		
voin CCE	802.18	<u> </u>	3.3.3.0/24		tunnel3	直连	0	0	1		
48	链路页载均衡	E 4	3.3.3.1/32		tunnel3	主机	0	0	1		
云服务		<u> </u>	10.10.10.0/24		tunnel1	自连	0	0	1		
A	云识别		10.10.10.1/32		tunnel1	王机	0	0	1		
			10.88 16 250/22		vswitchif1	自注	0	0	1		
安全			101.101.101.0/24	10.88.16.251	vswitchif1	主い	1	0	1		
23	策略		192.168.0.0/16	10.88.16.125	vswitchif1	静态	1	0	1		
藏	病毒过滤					1110					
	入侵防御										
	攻击防护										
a	ARP防护										
15.4.1											
控制											
	流里管理										
10 Ko	会话限制										
<u>A</u>	URL过滤										
100	网页关键字										
1	Web外发信息										
	邮件过滤										
S	网络聊天										
	应用行为控制										
8	全局黑名单										
в											
	监控 +										*
	日志 +	◎ ● 第 1 引	〕,总页数1 🕨 🕅 🛛 🧔	每页显示条目数	20 🗡				显示14个	、表项中的1	- 14



策略配置

策略配置,请按照以下步骤进行操作:

- 1. 通过 WebUI 方式登录 StoneOS,从页面左侧导航树选择并点击"配置->安全->策略", 进入策略页面。
- 点击列表左上角的『新建』按钮,弹出<策略配置>对话框,在该对话框对策略规则进行编辑。基本选项包含策略的源/目的安全域和源/目的地址的选择,以及服务、时间表、用户、 行为和策略描述的指定。

策略配置					8
基本配置 高级控制					
名称:			(0~95))字符	
当满足下列条件时					
^{復安全域} trust 内网安全域 ✓	至	目的安全域: untrust	外网安全域	~	
逆柳叶 :		目的地址:			
Any 内网ip地址 多个	到	Any	外网ip地址	多个	
服务簿: Anv 要要访问的服务 么个	1	时间表:	×	经本	
ony 加入的 max y m)	酒田户:		31	
)	200107		多个	
行为: ①					
● 拒绝	Web 认证只能	能工作在trust	VГ°		
◎ 安全连接	WEB认证	✓ local		¥	
策略描述:			(0~255)字符	
				御定 1	取消
					horf I

3. 配置完成后,点击『确定』按钮保存所做配置并返回策略页面。

源 NAT 配置

源 NAT 配置,请按照以下步骤进行操作:

- 1. 通过 WebUI 方式登录 StoneOS,从页面左侧导航树选择并点击"配置->网络->NAT",进入源 NAT 页面。
- 2. 点击源 NAT 列表中的『新建』按钮, 弹出<新建源 NAT>对话框。在该对话框对源 NAT



规则进行编辑。

源NAT配置					•
基本配置 更多	記置				
──当IP地址符合以T	「条件时 ――				
虚拟路由器:	trust-vr				~
源地址:	地址条目	Y Any	源地址一般是内网地	址	*
目的地址:	地址条目	Y Any	目的地址一般是外网	地址	~
出流里:	出接口	~	vswitchif1	出接口选择外网	利接口
服务:	Any	放行所有服务			~
将地址转换为一					
转换为:	◉ 出接口IP	○ 指定	EIP 〇 不朝	专换	
模式:	动态端口	转换为接口ip或者	音其他指定ip		
Sticky:	🗌 启用				
启用sticky后,每—	个源IP产生的	的所有会话将被映	射到同一个固定的IP地	址∘	
描述:				(0~63)字符	
				确定	取消

3. 配置完成后,点击『确定』按钮保存所做配置。



第3章 常用功能配置

常用配置介绍

本章介绍 Hillstone 山石网科多核安全网关的一些常用功能配置,包括 PPPoE、DHCP、IP-MAC 绑定、端到端 IPsec VPN、SCVPN、DNAT 等配置。

PPPoE 配置

PPPoE 配置,请按照以下步骤进行操作:

- 1. 通过 WebUI 方式登录 StoneOS "从页面左侧导航树选择并点击"配置->网络->网络连接", 进入网络连接页面。
- 2. 从接口列表中选中需要编辑的接口,双击或者点击列表右上方的『编辑』按钮。
- 3. 在弹出的<接口配置>对话框对接口进行编辑。

接口配置			8
常规 属性	高级 RIP		
名称:	ethernet0/3		-
描述:		(0~63)字符	
绑定安全域:	◎ 三层安全域	◎ 二层安全域 ◎ 无绑定	
安全域:	untrust	接口为三层安全域,且未配置IP地址	
IP面置			
类型:	◎ 静态IP ◎ 自动	获取IP	
用户名:		(1~31)字符	-
密码:		(1~31)字符	=
重新输入密码:		(1~31)字符	
挂断前空闲间隔:	30	(0~10000)分钟	
重拨间隔:	0	(0~10000)秒	
PPPoE服务器	是供的网关信息设置为默认网	关路由	
高级选项	DDNS		
管理方式			
Telnet SS	SH 🔲 Ping 🔲 HTTP	HTTPS SNMP	
路由			
		确定取测	肖

- 4. 点击『确定』按钮保存所做配置并返回网络连接页面。
- 5. 从页面右侧辅助栏的<任务>区选择『PPPoE 列表』链接, 弹出<PPPoE 列表>对话框。
- 6. 点击页面左上角的『新建』按钮 , 弹出 < PPPoE 配置 > 对话框。在该对话框进行配置。



PPPoE 歹	山表			•
	PPPoE配置		8	
	接口: PPPoE名称:	v	(未配置IP的三层接口) (1~31)字符	A
	用户名:		(1~31)字符	
	密码: 重新输入密码:		(1~31)字符	
	挂断前空闲间隔:	30	<mark>(0~10000)</mark> 分钟	
	重拨间隔:	0	(0~10000)秒	
	访问集中器:		(1~31)字符	
	认证:	● 任意 ○ CHAP ○ P.	AP	
	网络掩码:	255.255.255.255		
	路由距离:	1	(1~255)	
	路由权值:	1	(1~255)	
	服务:		(1~31)字符	
	静态IP:			~
4			确定取消	► 注闭

7. 配置完成点击 『确定』 按钮并返回 PPPoE 列表对话框。 选中需要连接/断开的 PPPoE 实例, 然后点击页面左上角的 『连接』 按钮。



PPPoE	PPPoE列表					۲
•	🗌 新建 📃 😼 编辑	前殿	🗳 连接 🗳 斷开			
	PPPoE名称	状态	接口	用户名	MAC地址	
V	abc	%	ethernet0/6	hillstone	0000.0000.0000	*
						÷
•					Þ	
					关闭	

DHCP 配置

DHCP 配置,请按照以下步骤进行操作:

- 1. 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->网络->网络连接", 进入网络连接页面。
- 2. 从页面右侧辅助栏的<任务>区选择『DHCP 列表』链接, 弹出<DHCP 列表>对话框。在 该对话框对 DHCP 进行编辑:
 - 接口:选择应用 DHCP 服务器功能的接口。
 - 类型:选中<DHCP服务器>单选按钮。
 - 基本配置: 在<基本配置>标签页对 DHCP 的基本属性进行配置。



DH	ICP列表				8
	DHCP配置			8	
•	接口: 类型: 基本配置 常规 网络摘码: DNS1: DNS2:	▼ J DHCP服务器 留地址 地址绑定 选 192.168.1.1 255.255.255.0	F <mark>启DHCP服务的接口</mark> DHCP中继代理 页 高級配置 网段以192.168.1.0/24为例	-	*
	地址池地址 起始IP: □ 起始IP	终止IP:	R置DHCP地址池,井点击添加 终止IP ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	•	
			确定即消		

3. 配置完成点击『确定』按钮并返回 DHCP 列表对话框。并且将用户 pc 或者交换机连接在 相应端口,即可获取 IP 地址。

DHCP列表						8
1 新建	🚽 编辑 🗂 删除					
□ 接口		类型	服务器	地址池	接入IP个数	
🔽 ether	met0/0	DHCP服务器	-	ethernet0/0_addrpool	0	^
						-
•						•
DHCP服务	器详情接入IP					
网关:	192.168.1.1					-
网络掩码:	255.255.255.0					
租约:	3600					
自动配置:	null					E
域名:						
DNS:						
WINS:						
SMTP服务器:						
DODORAS.						-
					í	Ð

IP-MAC 绑定配置

IP-MAC 绑定配置,请按照以下步骤进行操作:

1. 通过 WebUI 方式登录 StoneOS 从页面左侧导航树选择并点击"配置->安全->ARP 防护", 进入 ARP 防护页面。

- 从静态 IP-MAC 绑定条目列表中选中需要绑定的 IP-MAC 条目,双击或者点击列表上方的 『编辑』按钮,弹出<IP-MAC 绑定>对话框。
- 3. 在<IP-MAC 绑定>对话框中,选中<IP-MAC 绑定>复选框开启 IP-MAC 绑定,并点击 『确 定』按钮保存配置。

IP-MAC绑定				8		
MAC:	40f0.2f50.17	40f0.2f50.17f8				
IP:	192.168.1.1	192.168.1.1				
端口:	🗌 启用	ethernet0/3	×			
IP-MAC绑定:						
VLAN ID:	无		Y			
虚拟路由器:	trust-vr		*			
描述:						
ARP认证:	☑ 启用					
			确定	取消		

- 4. 默认情况下,安全网关的 ARP 学习功能是开启的, IP-MAC 绑定成功后,还需要关闭接口的 ARP 学习功能。
- 从页面左侧导航树选择并点击"配置->网络->网络连接",进入网络连接页面,从接口列表 中选中需要编辑的接口,双击或者点击列表右上方的『编辑』按钮。
- 在弹出的<接口配置>对话框中,点击『属性』标签,在<参数>部分取消选中ARP 学习后 的『启用』复选框开启接口的ARP 学习功能。

接口配置				8
常规属性。	高级 RIP			
工作模式				
双工: 《	● 自动 ○ 全双:	I ◎半双工		
速率: (ම 自动 ◎ 10M	© 100M	© 1000M	
Combo类型:	自动 💙			
参数				
最大传输单元 (MTU):	1500	(1280~1600)字节		
ARP学习:	自用 把勾去掉			
ARP超时:	1200	(5~65535)秒		
Keep-alive IP:				
MAC克隆:		恢复缺省MAC		
应用				
□ 将接口的	所有流量	镜像,对其流里进行分析。		
				确定取消

端到端 IPsec VPN 配置

在 Hillstone 安全网关 A 和 Hillstone 安全网关 B 之间建立一个安全隧道 ,PC1 作为 Hillstone 安全网关 A 端的主机 , PC2 作为 Hillstone 安全网关 B 端的主机 , 两端的公网 IP 都是固定的情况 下 , 配置端到端的 IPsec VPN , 拓补图如下 :

使用 IKE VPN 即自动协商方式配置 IPsec VPN, 配置包括:

- ◆ 配置 P1 提议
- ◆ 配置 VPN 对端
- ◆ 配置 P2 提议
- ◆ 配置隧道
- ◆ 绑定接口到隧道
- ◆ 配置隧道路由和策略

具体配置。请按照以下步骤进行操作:

- 1. 配置 P1 提议。通过 WebUI 方式登录 StoneOS,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。
- 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。在该对话框进行编辑:
 - 提议名称:指定或者显示 P1 提议的名称。
 - 认证:指定 IKE 身份认证的方式。
 - 验证算法:为 P1 提议指定验证算法。选中所需验证算法的单选按钮。
 - 加密算法:为 P1 提议指定加密算法。
 - DH 组:为 P1 提议选择 DH 组。
 - 生存时间:指定 SA 第一阶段的生命周期长度,单位为秒。默认 86400 秒。

阶段1提议配置		8
提议名称:	P1 (1~31)字符	
认证:	● pre-share ○ RSA-Signature ○ DSA-Signature	
验证算法:	○ MD5 ● SHA ○ SHA-256 ○ SHA-384 ○ SHA-512	
加密算法:	● 3DES ○ DES ○ AES ○ AES-192 ○ AES-256	
DH组:	○ Group1	
生存时间:	86400 (300~86400)秒,缺省值:(86400)	
	确定 取消	

- 3. 配置 VPN 对端。在 IPsec VPN 页面,点击『VPN 对端列表』标签,进入 VPN 对端列表 标签页。
- 点击 VPN 对端列表左上方的『新建』按钮, 弹出<VPN 对端配置>对话框。在该对话框对 VPN 对端进行基本配置。

IKE VPN配置		۲
步 骤1: 对端		
基本配置 高级		
对端名称:	1	
接口:	ethernet0/2 * 选择公网接口	
模式:	 ● 主模式 ● 野蛮模式 	
类型:	 ● 静态IP ◎ 动态IP ◎ 用户组 	
对端地址:	11.11.11.11 填写对端公网IP	
本地ID:	● 无 ◎ FQDN ◎ U-FQDN ◎ ASN1-DN ◎ KEY-ID	
对端ID:	● 无 ◎ FQDN ◎ U-FQDN ◎ ASN1-DN ◎ KEY-ID	
提议1:	p1	
预共享密钥:	••••••	
步骤2:隧道		
e:	确定 取消	
	前还有其他 NAT 设备 , 需在 < 高级配置 > 标签下配置 NAT 穿越功能。	

5. 配置 P2 提议。在 IPsec VPN 页面,点击 『P2 提议』标签,进入 P2 提议标签页。

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。在该对话框进行 P2 提议配置。

阶段2提议配置					
提议名称:	p2 (1~31)字符 自定义提议名称				
协议:					
验证算法1:	© MD5 © SHA © SHA-256 © SHA-384				
验证算法 <mark>2</mark> :	● 元 ◎ MD5 ◎ SHA ◎ SHA-256 ◎ SHA-384 ◎ SHA-512 ◎ NULL				
验证算法 <mark>3</mark> :	◎ 元 ◎ MD5 ◎ SHA ◎ SHA-256 ◎ SHA-384 ◎ SHA-512 ◎ NULL				
加密算法1:	③ 3DES ◎ DES ◎ AES ◎ AES-192 ◎ AES-256 ◎ NULL				
加密算法 <mark>2:</mark>	● 元 ◎ 3DES ◎ DES ◎ AES ◎ AES-192 ◎ AES-256 ◎ NULL				
加密算法3:	● 元 ◎ 3DES ◎ DES ◎ AES ◎ AES-192 ◎ AES-256 ◎ NULL				
加密算法4:	● 元 ◎ 3DES ◎ DES ◎ AES ◎ AES-192 ◎ AES-256 ◎ NULL				
压缩:	None Deflate				
PFS组:	◎ Group1 ◎ Group2 ◎ Group5 ◎ No PFS				
生存时间:	28800 (180~86400)秒,缺省值:(28800)				
启用生存大小:	□ 启用				
两端配置保持一致					
	福宁即省				

- 7. 配置隧道。在 IPsec VPN 页面,点击 IKE VPN 列表左上方的『新建』按钮,弹出<IKE VPN 配置>对话框。
- 在<步骤 1:对端>部分配置各选项。点击后面的『导入』按钮,并在<对端名称>下拉菜 单选择已配置的 VPN 对端名称,导入系统中已配置的 VPN 对端参数。
- 9. 点击<步骤2:隧道>,配置隧道相关选项。

IKE VPN配置			8
步骤 1: 对端			
步骤2:隧道			
基本配置	高级配置		
名称:	11		
模式:	tunnel	◎ transport <mark>默认为隧道模式</mark>	
p2 提议:	p2	▼ 选择自建提议p2	
代理ID:	◎ 自动	◎ 手工	
			确定取消

注意:隧道配置完成后,需要流量触发 VPN 连接。如果需要自动连接,请在<高级配置>标签 下配置自动连接功能。

10. 绑定接口到隧道。从主页面左侧导航树选择并点击"配置->网络->网络连接",进入网络连接页面。点击接口列表左上角的『新建』按钮,从下拉菜单中选择并点击<隧道接口>, 系统弹出<接口配置>对话框。在该对话框绑定接口到隧道。

接口配置				۲
常规 属性 高级 RIP				
管理方式 「Telnet 「SSH 」 Ping 「HTT	P HTTPS SNMP			*
路由 逆向路由: ② 启用 ③ 关键] (1) (1) 自动			
隧道绑定配置 隧道类型: ◎ IPSec VPN ◎ SS	L VPN			
VPN名称: 11 × 网关:	选择之前建立的隧	道名称		
	添加			
1 删除				
VPN名称	类型	网关		=
11	ipsec		^	
			T	
•		4		
				*
			确定	

11. 配置隧道路由和策略。从页面左侧导航树选择并点击"配置->网络->路由",进入目的路由页面。点击目的路由列表左上角的『新建』按钮,弹出<目的路由配置>对话框,在该对话框对目的路由进行编辑。

目的路由配置		⊗
目的地: 子网掩码:	192.168.1.0 255.255.255.0	配置对端网段
下一跳:	◎ 网关	◎ 接口
	◎ 当前系统虚拟路由器	◎ 其他系统虚拟路由器
接口:	tunnel1 💌	
优先权:	1	(1~255),缺省值:1
路由权值:	1	(1~255),缺省值:1
描述:		(0~63)字符
		确定 取消
优先权: 路由权值: 描述:		 (1~255),缺省值:1 (1~255),缺省值:1 (0~63)字符 确定 取消

12. 从页面左侧导航树选择并点击"配置->安全->策略",进入策略页面。点击列表左上角的『新建』按钮,弹出<策略配置>对话框,在该对话框对策略规则进行编辑。

Hillstone 山石网科基础配置手册

策略配置			8
基本配置 高级控制			
名称:		(0)~95)字符
——当满足下列条件时————————————————————————————————————	口所属安全域	内网接口所属于	安全域
源安全域: -		目的安全域:	
Any	▲ 到	Any	×
源地址: Anv	<u>ک</u>	目的地址: Anv	▼
服务簿:		时间表:	
Any 🎽 🎯	<u>}</u>		▼ 多个
应用簿: Any		源用户:	
¥ 3/	ř		多个
——做如下控制————————————————————————————————————	可以先配置	Any测试 , 如需细	化再进行后续配置
117/0 ¹¹ ⁽¹ 万分代) (17/0 ¹¹)	许		
◎ 拒绝	Web 认证只能	:工作在trust-vr∘	
◎ 安全连接	WEBilit	▼ local	×
策略描述:		(0)	~255)字符
			确定取消

- 13. 配置完成后,安全网关B也按照步骤1-12进行配置。
- 14. 完成以上配置后,安全网关 A 和安全网关 B 之间的安全隧道便建立成功了。从 IPsec VPN 页面右侧辅助栏的<任务>区选择『ISAKMP SA』/『IPsec SA』/链接,查看 VPN 监控结果。

ISAKMP SA IPSe	ec SA 拔号用户				
,删除					
Cookie	状态	对端	端口	算法	生存时间
c6f90153498ec	d8fb: established	221.224.30.141	500	pre-share md5/des	86393

ISA	MP SA	IPSec SA	拨号用户									
ti HK	余											
	ID	VPN名称	方向	对端	端口	算法	SPI	CPI	生存期(秒)	生存期 <mark>(</mark> …	状态	
	1	ipsec	outbound	221.224	500	esp:des/ -	3a71e2df	0	28767	0	Active	^
	1	ipsec	inbound	221.224	500	esp:des/	44709dc0	0	28767	0	Active	

SCVPN 配置

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

SCVPN 配置,请按照以下步骤进行操作:

- 1. 通过 WebUI 方式登录 StoneOS,从页面左侧导航树选择并点击"配置->网络-> SSL VPN",进入 SCVPN 页面。
- 2. 点击 SCVPN 列表左上角的『新建』按钮或者从页面右侧辅助栏的<任务>区选择『新建 SSL VPN』链接, 弹出<SSL VPN 配置>对话框。
- 3. 阅读 < 欢迎页 > 内容,并在 < SSL VPN 名称 > 文本框中指定 SCVPN 名称。

SSL VPN配置

4. 点击『下一步』按钮进入<接入用户>配置页面。在该页面配置用于客户端用户身份认证的 AAA 服务器。

SSL VPN配置	8						
欢迎页	选择用于用户认证的AAA服务器						
接入用户	青添加用户认证所需的AAA服务器,列表中AAA服务器上的用户均可进行登录。						
接入接口/隧道接口	SSL VPN配置只支持认证,不支持计费,即使选择了支持计费功能的AAA服务器。						
策略/隧道路由配置	AAA服务器: local v 域名: (1~31)字符 添加 AAA服务器 域 删除 local						
	高級配置						

5. 点击『下一步』按钮进入<接入接口/隧道接口>配置页面。在该页面配置设备端接口、隧

道接口和地址池。

SSL VPN配置		e e e e e e e e e e e e e e e e e e e
欢迎页 接入用户 接入接口/隧道接口 策略/隧道路由電器	接入接口 出接口1: 出接口2: 服务端口: 客户端访问VPN服务	ethemet0/0 ▼ 无 ▼ 4433 (1~65535) VPN服务TCP端口。 器的外网接口。一般電置一个出接口即可,配置最优路径检测时需要配置两个出接口。
	 隧道接口和地址池 隧道接口 隧道接口: 所属安全域: IP地址: 网络掩码: 	tunnel20 VPNHub 10.1.1.1 255.255.255.0
	地址池 地址池: 起始IP: 终止IP: 网络掩码:	pool1 ▼ 函置 10.1.1.2 10.1.1.254 255.255.255.0
		高级配置 上一步 下一步 取消

注意:隧道接口地址和地址池必须在同一网段,且地址池地址段中不能包含隧道接口地址。

在<接入接口/隧道接口>配置页面<隧道接口>下拉菜单中选择系统中已配置的隧道接口;
 或者选中下拉菜单中的<新建>选项,在弹出的<接口配置>对话框中新建隧道接口;还可以在下拉菜单中选中系统中已配置的隧道接口,然后点击『配置』按钮,在弹出的<接口配置>对话框中编辑该隧道接口。

接口配置		8
常规 属性	高级 RIP	
名称:	tunnel1	-
绑定安全域:	 ◎ 三层安全域 ○ 二层安全域 ○ 无绑定 	
安全域: IP配置	VPNHub Y	
类型:	 ● 静态IP ● 自动获取IP ● PPPoE 	
IP地址:	10.1.1.1	E
网络掩码:	255.255.255.0	
🔲 启用DNS代理		
高级选项	DHCP DDNS	
管理方式		
Telnet S	SH Ping HTTP HTTPS SNMP	
隧道绑定配置		
隧道类型:	IPSec VPN	
VPN名称:	×	
网关:		-
	确定职	消

 在<接入接口/隧道接口>配置页面<地址池>下拉菜单中选择系统中已配置的地址池;或者, 选中下拉菜单中的<新建>选项,在弹出的<地址池配置>对话框中新建地址池;还可以在 下拉菜单中选中系统中已配置的地址池,然后点击『配置』按钮,在弹出的<地址池配置> 对话框中编辑该地址池。

地址池配置				8
基本配置 IP用户	期定 IP角色绑定			
地址池名称:	pool1	(1~31)字符		Â
起始IP:	10.1.1.2	T I		
终止IP:	10.1.1.254	1		
保留起始IP:	10.1.1.20	-		
保留终止IP:	10.1.1.30			
网络掩码:	255.255.255.0	-		=
DNS1:	10.1.1.2	_		
DNS2:				
DNS3:				
DNS4:				
WINS1:	10.1.1.3			
			确定	取消

8. 点击 『下一步』 按钮进入 < 策略/ 隧道路由配置 > 页面。 在该页面配置策略规则和隧道路由。

SSL VPN配置					C
欢迎页 接入用户	 ●策略 ✓ 系统自动创建如下部 	荷略			
接入接口/隧道接口	源安全域 VPNHub	目的安全域 Any	地址 Any-Any	服务 时间 Any Any	表 行为 分许
泉朝/歷起樹口稱直	隧道路由 IP: 192 168 20 0	网络掩码:	度 <u></u> 置值:	(1,.0000)	35 tu
	IP IP Image: 192.168.2 0.0.0.0	0.0	网络掩码 255.255.255.0 0.0.0.0	(1~9999) 度里值 1 1	
					•
				-	_
			高級暫定	置上一步	完成 取消

注意:系统会自动创建一条源安全域是 VPNHub,目的安全域是 Any 的策略;隧道路由即为 远程拨入用户需要访问的内网资源网段。

9. 如需要,点击页面右下方的『高级配置』按钮,进行 SCVPN 高级参数配置,包括参数配


置、客户端/USB Key 配置、主机检测/绑定配置、短信口令认证配置和最优路径检测配置。

参数配置保持默认即可。

SSL VP	N配置		0
欢	迎页	安全套件	
接	入用户	SSL版本: O	◉ 任意
接	入接口/隧道接口	信任域: tr	trust_domain_defai 💙
策	略/隧道路由配置	加密算法: 31	3DES Y
参	教配置	Hash算法: Si	SHA-1 Y
客	户端/USB Key	压缩算法: ●	◉无 ◎ Deflate
È	机检测/绑定	客户端连接	
短	信口令认证	空闲时间: 3	30 (15~1500)分钟
最	优路径检测	允许同名登录: ▼	☑ 启用
		登录数: 0	0 (0~9999999), 0:任意
		防重放: 〇	◎ 32 💿 64 💿 128 💿 256 💿 512
		DF位: 〇	 ○ 设置 ● 拷贝 ○ 清除
		数据端口(UDP): 4	4433 (1~65535)

10. 建立登录用户。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。

本地用户								8
● 新建 🔹	■ 湯 編 辑 〔	前明除 🧼	IP/MAC绑定	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	■号出 ▼	搜索用户 👂		
オ 用户		▼ 红色:	已过期。橘色:-	—周内过期。黄色:—	·月内过期。			
用户组		📃 用户	Ŗ	目户组		账户到期日	IP-MAC	
								-
		14 4 1 空	• 五, 尚石;	铁1				主币
			1,00,2003	8X • P P 🥪			7.	1422420



11. 选中<新建>下拉菜单中的『用户』按钮,弹出<用户配置>对话框。在『基本配置』标

签页,进行用户名称和密码的配置。

本地用户					۲
● 新建 💌 🚦	编辑 🍈 删除 丨 🄇	》IP/MAC绑定 🛛 🔽 导入 🔽 🗐 导出 🗌	・ 捜索用户 ♀		
本地服务器: local	用户配置		8		
■□所有用户	其木砂罟 PnPV	PN两?罟		户到期日	
	名称:	test 用户名称	(1~63)字符		Î
	密码:		(0~31)字符		
	重新输入密码:		0		
	国家代码(可选)+手机 号码:	请输入手机号	(0,6~15)字符		
	描述:		(0~127)字符		
	组:		选择		
	IKE标识:	None FQDN ASN1DN KEY	(-ID		
	账户到期日:	□ 启用			
	如果启用了短信认证功	能,短信认证码将发送到用户设置的电话号码			
		福元	E 取消		-
	▲ ▲ 第	; 1 页,总页数1 🕨 🕅 🗇 每页显示条	目数 20 👻	显示1个表项中的1.	- 1
		确定重置			

- 12. **Web 方式 (用户名/密码) 启动 SCVPN**。在 IE 浏览器的地址栏输入以下 URL 访问 设备端:https://IP-Address:Port-Number (默认为 4433)。
- 13. 浏览器转到登录页面,输入用户名和密码,并点击『登录』按钮。

Hillstone	Hillstone Secure Connect			
	用户名: hillstone 密码: ●●●●●●● 登录			



14. 下载并启动 SCVPN 客户端 (用户名/密码)。使用 Web 方式登录后,下载并安装客户

端程序 Hillstone Secure Connect。



- 15. 完成安装后,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)。 选中<用户名/密码>单选按钮,点击『确定』按钮。
- 在弹出的"用户名/密码"登录模式客户端程序登录对话框 旅次填写服务器地址、端口号、
 用户名以及密码,然后点击『登录』按钮。

⑦ 登录	
Hillstone Secure	Hillstone 山石岡科 Connect
最近访问: 服务器: 端口: 用户名:	test@61.161.171.138:4433 ▼ 61.161.171.138 4433 test
密码:	••••••

DNAT 配置

目的地址映射主要用于将内网的服务器对外进行发布(如 HTTP 服务, FTP 服务, 数据库服务等), 使外网用户能够通过外网地址访问需要发布的服务。



常用的 DNAT 映射有一对一 IP 映射,一对一端口映射,多对多端口映射,一对多映射。

一对一 IP 映射

配置举例:将公网地址 60.0.0.1 映射到内网地址 192.168.1.100

请按照以下步骤进行配置:

1. 创建两个地址簿(内网地址和外网地址)。从工具栏的<对象用户>下拉菜单选择『地址簿』,

配置地址簿	i			8
名称:	60.0.0.1/32			(1~31)字符
成员:	IP/掩码	✓ 60.0.0.1 /	32	
	类型	成员		添加
				刪除
				-
描述:				(0~255)字符
				· · · · · · · · · · · · · · · · · · ·
				14月7日 - 4以月

弹出<地址簿>对话框。点击『新建』按钮,弹出<配置地址簿>对话框。

配置地址簿				8
名称: [成员:]	192.168.1.100/32 IP/掩码	P地址 / 网络摘	<u>д</u>	(1~31)字符
	处型 P地址	成员 192.168.1.100/32	*	添加

3. 新建目的 NAT IP 映射规则。从页面左侧导航树选择并点击"配置->网络->NAT",进入源 NAT 页面。点击『目的 NAT』标签,进入目的 NAT 页面。点击目的 NAT 列表中的『新建』 按钮,并在弹出的下拉菜单中选择『IP 映射』,弹出<IP 映射配置>对话框。

注意:针对此配置举例,掩码必须填写 32。

^{2.} 同步骤1,创建内网地址簿。



IP映射配置				8
当IP地址符合以下	条件时			
虚拟路由器:	trust-vr			~
HA组(可选):				_
目的地址:	地址条目	Y Any		*
		选择公网地址簿		
映射到地址:	地址条目	Y Any		~
描述:		选择内网地址簿	<mark>(0~63)</mark> 字符	
			确定	取消

 查看接口所在安全域。点击目的 NAT 列表中的『新建』按钮,并在弹出的下拉菜单中选择 『IP 映射』,弹出<IP 映射配置>对话框。从页面左侧导航树选择并点击"配置->网络->网 络连接",进入网络连接页面,在接口列表查看接口所在安全域。

新建 🔹 📝 编辑	计 🛗 删除			
接口名称	状态	获取类型	IP/掩码	安全域
ethernet0/0	જુ 🔍 જુ. જુ.	静态	192.168.1.1/24	trust
ethernet0/1	🤞 🔮 🍕 🖗	静态	60.0.0.1/28	untrust

创建 untrust -> trust 的策略规则。从页面左侧导航树选择并点击"配置->安全->策略",
 进入策略页面。点击列表左上角的『新建』按钮,弹出<策略配置>对话框,在该对话框对策略规则进行编辑。



Hillstone 山石网科基础配置手册

策略配置	8
基本配置 高级控制	
名称:	(0~95)字符
──当满足下列条件时 源安全域: 选择公网接口所属安全域	目的安全域: 选择内网接口所属安全域
Any 判 酒かけ:	Any T
Any Y 多个 到	Any Y 多个…
服务簿: Any ¥ 多个	时间表: 选择公网地址簿 ▼ 多个
应用簿:	源用户: 多个…
做如下控制	
行为: 💿 允许	
◎ 拒绝 Web 认证只能	工作在trust-vr。
◎ 安全连接 WEB认证	
策略描述:	(0~255)字符
	确定 取消

一对一端口映射

配置举例:将公网地址 60.0.0.1 的 TCP 8080 端口映射到内网地址 192.168.1.100 的 80 端口。

请按照以下步骤进行配置:

- 1. 创建两个地址簿 (内网地址和外网地址)。请参阅一对一 IP 映射步骤 1-2。
- 根据所需映射的公网地址端口(8080),创建服务。从工具栏的<对象用户>下拉菜单选择 『服务簿』,弹出<服务簿>对话框。选中<新建>下拉菜单中的『服务』按钮,弹出<服务 配置>对话框。



服务配置				8
名称:	TCP-8080 配	置服务名称		(1~95) 字符
描述:				(0~255)字符
成员:	添加成员	选择正确的协议		
	类型:		◎ ICMP ◎ 其它	
	目的端口:	最小: 8080>	最大: 8080 百	置正确端口
	源端口:	最小:>	最大:	
	🔲 协议	目的端口	源端口	添加
	П ТСР	8080-8080	-	
				•
			确	定即消

 新建目的 NAT 端口映射规则。从页面左侧导航树选择并点击"配置->网络->NAT",进入 源 NAT 页面。点击『目的 NAT』标签,进入目的 NAT 页面。点击目的 NAT 列表中的『新 建』按钮,并在弹出的下拉菜单中选择『端口映射』,弹出<端口映射配置>对话框。



Hillstone 山石网科基础配置手册

端口映射配置				8
──当IP地址符合以下	「条件时			
虚拟路由器:	trust-vr			~
HA组(可选):	0	选择公网均	也址簿	
目的地址:	地址条目	Y Any		~
服务:	Any 选择服	务部		~
		选择内网	地址簿	
映射到地址:	地址条目	Y Any		¥
映射到端口:	配置内	内网只用端口	(1~65535)	_
描述:			(0~63)字符	
			确定	取消
			确定	取消

4. 查看接口所在安全域。请参阅一对一 IP 映射步骤 4-5。



Hillstone 山石网科基础配置手册

策略配置	8
基本配置 高级控制	
名称:	(0~95)字符
当满足下列条件时	*********************
源安全域: 选择外网接口所属安全域	目的安全域:远洋内网接口所属安全域
Any Y	到 Any
源地址· Any	目的1月11日 到 Any ▼ 多个…
服务簿: 选服务薄	时间表: 选择公网地址簿
Any Y 多个	▼ 多个…
应用簿:	源用户:
	· · · · · · · · · · · · · · · · · · ·
御如下控制 会社	
11/0. ④ 允许	
◎ 拒绝 Web 认证	只能工作在trust-vr。
◎ 安全连接 WEB认证	V local
策略描述:	(0~255)字符
	确定 取消

一对多映射(包含服务器负载均衡)

配置举例:将公网地址 60.0.0.1 的 tcp 80 端口映射到内网地址 192.168.1.1 和 192.168.1.3 的 80 端口,多台服务器进行负载均衡。

请按照以下步骤进行配置:

- 1. 创建两个地址簿 (内网地址和外网地址)。请参阅一对一 IP 映射步骤 1-2。
- 2. 根据所需映射的公网地址端口(80), 创建服务。请参阅一对一端口映射步骤2。
- 3. 目的 NAT 高级配置。从页面左侧导航树选择并点击"配置->网络->NAT",进入源 NAT 页面。点击『目的 NAT』标签,进入目的 NAT 页面。点击目的 NAT 列表中的『新建』按钮,并在弹出的下拉菜单中选择『高级配置』,弹出<目的 NAT 配置>对话框。



目的NAT配置					8
基本配置 更多配置	2 L				
当IP地址符合以下条	件时				
虚拟路由器: tru	ust-vr		此处一般为Any		~
源地址: 地	址条目	Ƴ Any			¥
目的地址: 地	址条目	✓ Any			¥
服务: Ar	іу		选择公网服务器地	址簿	~
将地址转换为					
志力作: 💿	转换 💿	不转换	选择内网服务器地	址簿	
转换为IP: 地	址条目	Ƴ Any			~
将服务端口转换为一					
转换端口:	启用 端口值:	此处	不启用,表示选择的	的服务薄端口保	時不表
			(1~65535)		
负载均衡:	启用 开启	后,流量	将会均衡到不同的内网朋	服务器。	
描述:	如需服务器	负责均	衡, <mark>此处必须</mark> 启用	(0~63)字符	
				确定	取消
		L TD nd			

4. 查看接口所在安全域。请参阅一对一 IP 映射步骤 4-5。



Hillstone 山石网科基础配置手册

策略配置		8
基本配置 高级控制		
名称:		(0~95)字符
——当满足下列条件时————————————————————————————————————	544	进择内网络口底层实全域
[2017] 源地址:	目的地址:	
Any ¥ 多个…	到 Any	▼ 多个
服务簿:	时间表:	选择公网地址簿
Any Y 多个…)) (Eq. c),	▼ 多个
^{应用簿:} 选择需要映射的包含多	个端口的服务 ^{遇用户:}	多个
做如下控制		
行为: 💿 允许		
◎ 拒绝	Web 认证只能工作在trust-v	/Г •
◎ 安全连接	WEB认证 💙 local	Y
策略描述:		(0~255)字符
		确定 取消

第4章 链路负载均衡

链路负载均衡介绍

对于多 ISP 链路用户,链路负载均衡功能可以通过动态链路探测技术将流量合理分发到不同链路,从而达到充分利用各条链路资源的目的。可以对内网的流量根据源地址、目的地址或者服务进行流量的负载分摊,以便保证流量的负载分担。

在配置源地址,目的地址的负载均衡后,可以实现冗余,当某一条路由失效时,可以保证正常的流量转发。

在配置链路负载均衡之前,先确保设备的接口、SNAT 和策略都已配置完成。

1. 接口的 IP 地址和掩码配置完成 (掩码位数需要跟运营商确认)



接口名称	状态	IP/摘码	MAC	安全域	接入用户/IP数	流入带
bgroup1	Q. Q. Q. Q.	0.0.0/0	001c.541b.4d91	NULL e0/0和e0/1作为公网口	0	0
ethernet0/0		1.1.1.1/24	001c.541b.4d80	untrust	0	1.34
ethernet0/0.2		11.1.1/24	001c.541b.4d80	trust	0	0
ethernet0/0.3		11.1.2.200/24	001c.541b.4d80	trust	0	0
ethernet0/1		2.2.2.2/24	001c.541b.4d81	untrust	0	0
ethernet0/2		0.0.0/0	001c.541b.4d82	l2-trust	4	1.53

2. SNAT 规则配置完成,使内网的流量可以分别 NAT 成对应公网出口地址池的地址,能够访

问 Internet。

3	源N	AT (目的NAT 服务器	t态							
	ł	新建	📝 编辑 🎁 刪除	루 优先级 🛍 优先级	辦序 虚拟器	由器: trust-vr 🔹					
		ID	源地址 (原始)	目的地址(原始)	服务	出接口 / 下一跳虚拟路由器	转换为	模式	HA组	志	Track
		1	Any	Any	Any	ethernet0/0	出接口IP	动态端口	0	关闭	
		2	Any	Any	Any	ethernet0/1 配置两条对应的s	出接口IP	动态端口	0	关闭	
	-	- 源N	- 源NAT 日 ● 新建 □ ID □ 1 □ 2	滾NAT 目的NAT 服务器 ● 新建 ● 编辑 ● m除 ● 10 泵地址(泵始) □ 1 Any □ 2 Any	褒NAT 目的NAT 服务器状态 ● 新建 2/编辑 1 mm/k 2 优先级 ①优先级 ● ID 泵地址(原始) 目的地址(原始) ● 1 Any Any ● 2 Any Any	褒NAT 目的NAT 服务器状态 ● 新建 ● 編唱 ● 优先级 ● ●	夏NAT 目的NAT 服务器状态 ● 新建 ● 编辑 ● 优先级 ● 优先级 ■ 此优先级排序 虚拟路由器: trust-vr ▼ ID 夏地址(原始) 目的地址(原始) 服务 出接口 / 下一跳虚拟路由器 □ 1 Any Any ethernet0/0 □ 2 Any Any Any ethernet0/1	源NAT 目的NAT 服务器状态 ● 新建 ● 第先 ● 优先级指序 虚拟路由器: Trust-vr ● 新建 ● 第他址(原始) 服务 出接口 / 下一跳虚拟路由器 转换为 ● 1 Any Any Any ethernet0/0 出接口 IP ● 2 Any Any Any ethernet0/1 配置两条对应的snatt	夏NAT 目的NAT 服务器状态 ● 新建 ● 编辑 ● 优先级 ● 化 ●<	褒NAT 目的NAT 服务器状态 ● 新建 ● 续编辑 ● 优先级 ● 优先级 ● 优先级 ● 优先级 ● 优先级 ● 化 ● ● ● ● ● ● ● <th>寮NAT B的NAT 服务器状态 ● 新建 ● 第 Cttstyle Instruction Instruction ● 新建 ● 第 Cttstyle Instruction Instruction Instruction Instruction ● ID 寮地址(寮始) 目的地址(寮始) 服务 出接口 / 下一號虛拟路由器 转換为 模式 HA 日志 ● I Any Any Any ethernet0/0 出接口 IP 动态端口 0 关闭 ● 2 Any Any Any ethernet0/1 Immonstruction 0 关闭</th>	寮NAT B的NAT 服务器状态 ● 新建 ● 第 Cttstyle Instruction Instruction ● 新建 ● 第 Cttstyle Instruction Instruction Instruction Instruction ● ID 寮地址(寮始) 目的地址(寮始) 服务 出接口 / 下一號虛拟路由器 转換为 模式 HA 日志 ● I Any Any Any ethernet0/0 出接口 IP 动态端口 0 关闭 ● 2 Any Any Any ethernet0/1 Immonstruction 0 关闭

3. 策略规则配置完成。允许流量通过设备。

配置	-	•	倚略												
🏠 主页	^	源安全	域: An	y	¥		目的梦	安域: Any	Y	•					
网络		•	新建] 🚽 編	辑 🚺	刪除	🕑 启用	∂禁用 【	自克隆 🛛 🥏 🗇	洗级 👘 优先	級排序				
🔵 网络连接			ID	名称	状态	有	源安全…	目的安	源地址	目的地址	角色/用户/用	服务	特征	行为	命中数
🧔 NAT			12		0	분	dmz	trust	Any(地址条目	Any(地址条目	test(角色)	Any		0	0
罕 路由			6		0	분	untrust	trust	Any(地址条目	Any(地址条目		Any		3	0
🚰 IPsec VPN			11		0	분	Any	Any	Any(地址条目	Any(地址条目		DNS		ø	0
횦 SSL VPN			10		0	분	Any	Any	Any(地址条目	Any(地址条目	UNKNOWN(角	Any			0
🚳 L2TP VPN			9		0	분	Any	Any	Any(地址条目	Any(地址条目		Any		Ø	0
\delta 用户识别			3		0	분	Any	Any	Any(地址条目	Any(地址条目		Any		8	0
🦂 802.1X	_		1		0	분	Any	Any	Any(地址条目	Any(地址条目		Any		Ø	0
🗄 链路负载均衡	=		2		0	是	Any	Any	Any(地址条目	Any(地址条目		DNS		3	0
	- 1		4		0	是	Any	Any	Any(地址条目	Any(地址条目	yyan@local(Any			0
本版方 二次回			7		0	분	Any	Any	Any(地址条目	Any(地址条目		Any	上线通…	3	0
👊 玄洪別			8		0	是	l2-trust	l2-unt	Any(地址条目	Any(地址条目		Any		3	451
安全			5		0	분	Any	Any	Any(地址条目	Any(地址条目		Any		0	339
🏾 🍏 策略		-						お開いた	计运动等略						
🎕 病毒过滤								的专用心	如何的束帽						

基于目的路由的负载均衡

配置举例:ethernet0/1口接入10M带宽的运营商A链路,ethernet0/2接入20M带宽的运营商B链路;实现所有访问公网的流量按1:2的比例分别从ethernet0/1口和ethernet0/2口转发出去。即当设备总共转发3数值的流量时,ethernet0/1转发1数值;ethernet0/2口转发2数值。

请按照以下步骤进行配置:

通过 WebUI 方式登录 StoneOS,从页面左侧导航树选择并点击"配置->网络->路由",
 进入路由页面。点击『目的路由』标签,进入目的路由页面。点击目的路由列表左上角的



▲ 主页	配置 ī	-	目的路由 虚拟路由器:	源路由 源接口路由 IS trust-vr ▼ IP:		策略路由	
网络			1曲人工。	位余			
	网络连接		制新建	▶ 编辑 懂 删除			
<u></u>	NAT		□ 状态	IP/掩码		下一跳接口	
-	路由 IPsec VPN		目的路由配置				8
۹	SSL VPN		E 654h	0.0.0	1		
6	L2TP VPN			0.0.0.0	目的地址和掩码	位全为0	
6	用户识别		子网掩码:	0			
18	802.1X		下一跳:	 ● 网关 	0 1	妾口	
E	链路负载均衡			○ 当前系统虚拟路由器	⊖ ‡	其他系统虚拟路由器	
云服务			网关:	2.2.2.1	公网网关		
<u> </u>	云识别		优先权:	1	(1~255),缺省值:	:1	
安全			路由权值:	1	(1~255),缺省值	:1 流量分摊的比重	
<u> </u>	策略		描述:		(0~63)字符		
藏	病毒过滤				. ,,,,,		
	人侵防御						
	攻击防护 ARP防护					确定	取消

『新建』按钮, 弹出<目的路由配置>对话框, 在该对话框对目的路由进行编辑。

2. 再创建一条路由权值为2的路由条目,方法同步骤1。

配置	-	目的	路由	源路由 源接口路由	ISP信息 ISP路由	策略路由	就近探测路由	RIP			
🏠 主页		虚拟路	油器:	trust-vr 🗸	P: /	下一跳:		下一跳接口	: Any	▼ 协议: A	ny 🗸
网络		描述:		#	紫 清空						
🌍 网络连接		•	新建	▶编辑 箇册除	保证有两条默认路由					表示1日和2日的流量	按1:2分摊
🔞 NAT			状态	IP/ 掩码	下一跳	下一跳接口	协议	优先权	度里	路由权值	描述
🚆 路由			٨	0.0.0/0	2.2.2.1	ethernet0/1	静态	1	0	1	
🗿 IPsec VPN			۸	0.0.0/0	3.3.3.1	ethernet0/2	静态	1	0	2	
N SSL VPN			۵	1.1.1.0/24		ethernet0/0	直连	0	0	1	
I 2TP VPN			۵	1.1.1.1/32		ethernet0/0	主机	0	0	1	

完成配置后,即可实现流量从 ethernet 0/1 转发和从 ethernet 0/2 转发的比是 10:20
 即流量的 1:2 负载均衡。具体比例可根据出口带宽的大小以及实际使用率确定。

基于源路由的负载均衡

配置举例: 负载均衡来自 192.168.1.1/24 网段的流量。

请按照以下步骤进行配置:

 通过 WebUI 方式登录 StoneOS,从页面左侧导航树选择并点击"配置->网络->路由", 进入路由页面。点击『源路由』标签,进入源路由页面。点击源路由列表左上角的『新建』 按钮,弹出<源路由配置>对话框,在该对话框对源路由进行编辑。



	配置	- 目的路由 孫路由 孫接口路由 ISP信息 ISP路由 新路路由	就近探测路由 RIP
<u> </u>	È页	▲ 虚拟路由器: trust-vr ▼ IP: / 下一跳:	下——
网络		投索 清空	
	🔋 网络连接	● 新建 ● 編辑 🎬 删除	
	💫 NAT		协议优先权
		源路由配置	
6	SSL VPN	VE 10. 100 100 10	
6	L2TP VPN	源IP: 192.108.1.0 需要负载均衡的网段	
(💈 用户识别		
ų,	🔒 802.1X		
E	🚪 链路负载均衡	○ 当前系统虚拟路田器 ○ 其他系统虚拟路田	.23
云服	<u>ች</u>	网关: 2.2.2.1 公网网关	
	🛛 云识别	优先权: 1 (1~255),缺省值:1	
安全		路由权值: 1 (1~255),缺省值:1 流量分摊的	北例
6	🗑 策略	描述: (0~63)字符	
X	▲ 病毒过滤		
	◎ 八侵防御		
	♥ 火西防州	确定	取消
A	AIXEN]		

2. 再创建一条网关为 3.3.3.1、路由权值为 2 的路由条目, 方法同步骤 1。

配置	-	目的路由	源路由 源接口路由 I	SP信息 ISP路	油策略路由	就近探测路由	RIP			
🏠 主页	~	虚拟路由器:	trust-vr 💙 IP:		/ 下—跳:		下—跳接口:	Any 👻 🗄	锚述:	
网络		搜索	清空							
🔵 网络连接		●新建	🦻 🍺 编辑 🏾 🎁 删除	两条源路由配置				表示源地	址的路由按比例负	受载均衡
🚳 NAT		■ 状态	IP/掩码	下一跳	下一跳接口	协议	优先权	度里	路由权值	描述
🚃 路由		A 1	192.168.1.0/24	2.2.2.1	ethernet0/1	静态	1	0	1	
IPsec VPN		A 1	192.168.1.0/24	3.3.3.1	ethernet0/2	静态	1	0	2	
SSL VPN										

3. 完成配置后,即可实现来自 192.168.1.1/24 网段的流量从 e0/1 转发和从 e0/2 转发的

比是1:2,具体比例可根据出口带宽的大小以及实际使用率确定。

智能链路负载均衡

当内网用户向外网目标地址首次发起访问时,系统对匹配到默认路由的流量在符合条件的链路 上进行探测,对响应相对快速的接口生成静态路由,后续报文将直接按照路由转发不再探测;如果 生成的静态路由在一定时间内不被命中,则自动老化。

请按照以下步骤进行配置:

- 通过 WebUI 方式登录 StoneOS,从页面左侧导航树选择并点击"配置->网络->链路负载 均衡",进入链路负载均衡页面。
- 2. 点击『出站负载均衡』标签,进入出站负载均衡页面。
- 3. 在页面左上角点击『出站就近探测接口』, 弹出<出站就近探测接口>配置对话框。
- 4. 选择需要启用出站就近探测的接口(即启用出站负载均衡功能的接口)。并点击『确定』按



钮。

	配置		● 出站负载均衡 ● 入站负载均衡	
🏠 主页	ī	~	出站就近探测:出站就近探测接口	
网络			就近探测路由:	
	网络连接		下一跳接口: ALL 💙 虚拟路由器: trust-vr 💙	
	NAT		状态 IP/ 撞码 下一跳 下一跳接口	
	路由 IPsec VPN		出站就近探测接口	
- -	SSL VPN		请选择需要就近探测的接口: 2 全选	
6	L2TP VPN		自用接口 按照需要启用相应的接口 · · · · · · · · · · · · · · · · · · ·	
6	用户识别		ethernet0/0.2 ethernet0/0.3	
18	802.1X		ethernet0/1	
	链路负载均衡		ethemete/1 redundant2 vewitchif1	
云服务				
<u> </u>	云识别			
安全				
<u> </u>	策略			
熾	病毒过滤			
di 🕹	入侵防御			
(攻击防护			
ARP	ARP防护		确定	

- 5. 在页面右侧辅助栏的<任务>区对就近探测路由进行配置:
 - 老化时间:指定就近探测路由的老化时间,单位为分钟。取值范围是1到1440分钟, 默认值为10分钟。如果在老化时间结束后仍没有流量匹配该路由,系统认为该路由已 经老化失效,并从路由表中删除;
 - 子网掩码:指定就近探测路由的掩码。安全网关支持两种格式: A.B.C.D 和 num。
 A.B.C.D 的取值范围是 255.0.0.0 到 255.255.255.255 默认值为 255.255.255.0;
 num 的取值范围是 8 到 32, 默认值为 24。

出版	栽り摘 () 入站负载均	衡								任务	帮助
出站就近探测:	出站就近探测接口									就近探测器	路由设置
就近探测路由:									파 팬들만드 많 속 수 시고보기	老化时间:	
下一跳接口:	ALL	*	虚拟路由器:	trust-vr	v				能宜和江始田老化时间	10	分钟
状态	IP/撞码	下一跳		下一跳接口		协议	优先权	度里	路由权值	(1~144	0),缺省值:10
									^		
										子网掩码:	
									的宣称匹给田的电的	255.255.2	255.0
										保存	恢复默认



第5章 QoS 配置

QoS 介绍

QoS (Quality of Service)即"服务质量"。它是指网络为特定流量提供更高优先服务的同时 控制抖动和延迟的能力,并且能够降低数据传输丢包率。当网络过载或拥塞时,QoS 能够确保重要 业务流量的正常传输。QoS 是网络中管理数据流的可用带宽、延迟、抖动以及分组丢失的技术集合。 所有的 QoS 机制的目的就是影响这些特征中的至少一个,某些情况下甚至是全部。

IP QoS 配置

IP QoS 配置,请按照以下步骤进行操作:

- 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->控制->流量管理",
 进入 QoS 配置页面。
- 2. 点击『IP QoS』标签,页面将出现 IP QoS 列表。
- 3. 点击 IP QoS 列表上方的『新建』按钮, 弹出 < IP QoS > 对话框。
- 4. 在『基本配置』标签页,进行 IP QoS 规则的基本配置。

IP QoS		8
基本配置高		
规则名称:	· · · · · · · · · · · · · · · · · · ·	
限流对象:	接口 × · · · · · · · · · · · · · · · · · ·	
IP:	IP范围 ▼ 起始IP 终止IP 添加	
	输入IP范围或地址条目并点击添加	
	可选中后删除条	
上行带宽:	毎IP ▼ 预留带宽 最大带宽 时间表 ▼ 添加	
	冊除	
下行带宽:	毎IP ▼ 預留带宽 最大带宽 时间表 ▼ 添加	
	冊修	
	确定	取消



上行带宽:	每IP	~	预留带宽	最大带宽	时间表	~	添加
	每IP			配置可じ体田	设置策略在物	铈定	时间生效
	共享	245-4	又无风甘宁地北	的最大带宽			刪除
选择限制对象) IP或所有IP共享	均每	四十	前则面具已地址 能使用这份带宽				

5. 在『高级配置』标签页,可根据需要,配置如下功能:

• 配置弹性 QoS。可设置最大弹性带宽,当接口存在闲置带宽时可暂时突破 QoS 的闲置 以避免资源浪费,必须在主页开启全局弹性 QoS 时才能生效。用户可选择为上行流量 或下行流量配置该功能。

启用 - 选中该复选框开启弹性 QoS 功能。

最大弹性带宽 - 开启弹性 QoS 功能后,该选项用来指定最大弹性带宽,即带宽上涨的 最大限制,单位为 Kbps。默认值是 IP 配置带宽的 100 倍。取值范围是 64 到 1000000。;

• 配置细粒度控制。为 IP QoS 规则嵌套应用 QoS 规则,系统将为不同 IP 按照指定的应用 QoS 规则分配应用带宽,实现 IP QoS 的细粒度控制。用户可选择为上行流量或下行流量配置该功能。点击『嵌套应用 QoS 规则』链接,弹出<嵌套应用 QoS 配置>对话框,配置方式与配置应用 QoS 规则的方式相同。用户可在嵌套应用 QoS 规则列表中点击『编辑』或『删除』按钮,进行相应的编辑或删除操作

注意:使用应用 QoS 需要打开相应安全域的应用识别以及安装应用特征库许可证。

配置举例:配置 192.168.1.2 至 192.168.1.200 范围内 IP 在 ethernet0/2 每 IP 上下行预 留带宽 200K,最大带宽 1M,如下图所示:



IP QoS						8
基本配置高	级配置					
规则名称:	qos	(14	~ 31) 字符			
限流对象:	接口	ethernet0	/2 🗡 所	属安全域为trust		
IP:	IP范围	·起始IP		终止IP		添加
	192.168.1.2:	192.168.1.2	00		(删除
上行带宽:	每IP Y 预留	带宽	最大带宽	时间表	~	添加
	每IP:预留市克。	200KDps	大帝贲 1000	IKDPS	(删除
下行带宽:	每IP × 预留	带宽	最大带宽	时间表	~	添加
	每IP:预留带宽。	200Kbps 最	大带宽 1000	Kbps		删除
					确定	取消

应用 QoS 配置

应用 QoS 配置,请按照以下步骤进行操作:

- 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->控制->流量管理",
 进入 QoS 配置页面。
- 2. 点击应用 QoS 列表上方的『新建』按钮, 弹出 < 应用 QoS > 对话框。
- 3. 在『基本配置』标签页,进行应用 QoS 规则的基本配置。



应用QoS		8
基本配置高级	我 <mark>教育了</mark> 一个人,我们就是这些人,我们就是这些人,我们就是这些人,我们就是这些人,我们就是这些人,我们就是我们的人,我们就是我们的人,我们就是我们的人,我们就是我们的人,我们就是我们的人,我们就是我们的人,我们就是我们的人,我们就	
规则名称:	设定规则名称 (1~31)字符	
限流对象:	接口 >	
匹配条件:	应用 🖌 添加	
	选择相应的应用并添加	
	更多	
上行带宽:	最小带宽 ▼ 32~10000000 Kbps 时间表 ▼ 添加	
	设置上行最小保证带宽或最大带宽	
	高級	
下行带宽:	最大带宽 ▼ 32~10000000 Kbps 时间表 ▼ 添加	
	设置下行最大带宽 删除	
	高级	
	确定	

 在『高级配置』标签页,可根据需要,配置细粒度控制。在<嵌套 QoS 类型>下拉菜单中 选择 IP QoS,然后点击『嵌套 IP QoS 规则』链接,弹出<嵌套 IP QoS 配置>对话框, 配置方式与 IP QoS 配置相同。



嵌套IP QoS配置	1				8		
规则名称:			设置规则 (1~31)字	名称 将			
IP:	IP范围	▼ 起台	Р	终止IP	添加		
	配置IP范	范围或地址条	目并点击	添加	删除		
最大带宽:	32-100,00	0,000 Kbps	时间表	~	添加		
	配置相应应用分配给当前IP的最大带宽						
 在相同时间(置的最大带宽值) 	内,嵌套IP(重。	QoS规则中配置	的最大带宽的	值必须小于其所属	的应用QoS配		
				确定	取消		

注意:使用应用 QoS 需要打开相应安全域的应用识别以及安装应用特征库许可证。

配置举例:限制 P2P 软件及 P2P 流媒体在 ethernet0/2 接口上行最大流量为 10M , 如下图 所示:



应用QoS		8
基本配置 高级		
规则名称:	qos (1~31)字符	
限流对象:	接口 v ethernet0/2 v 所属安全域为trus	t
匹配条件:	应用	▼ 添加
	应用:P2P软件	删除
	应用:P2P流媒体	更多
上行带宽:	最大带宽 ▼ 32~1000000 Kbps 时间表	
	最大带宽:10000Kbps	删除
		高级
下行带宽:	最大带宽 ▼ 32~1000000 Kbps 时间表	▼ 添加
		冊條
		高级
		确定取消

混合 QoS 配置

Hillstone 山石网科安全网关中的 QoS 除了有针对 IP 和应用外,还可以针对地址条目,角色, QoS 标签, IP 优先权以及 DSCP 等多项条件进行混合 QoS 配置以达到更精确的带宽管理。

混合 QoS 配置,请按照以下步骤进行操作:

- 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->控制->流量管理",
 进入 QoS 配置页面。
- 2. 点击应用 QoS 列表上方的『新建』按钮, 弹出<应用 QoS>对话框。
- 在『基本配置』标签页,点击<匹配条件>右侧『更多』按钮,弹出<高级配置>对话框, 可添加多项匹配条件。可针对策略标签,IP优先权,IP范围,地址条目等进行控制。



高级配置			8
1000 000 000 000 000 000 000 000 000 00	如不能超过	过10条,流量控制只需匹配其中一条即可。	
QoS标签	~	11024 添	加
入接口	•		
QoS标签		明	除
DSCP	Ξ		
IP优先权			
CoS			
IP范围			
地址条目	-	确定	则消

QoS 白名单配置

QoS 功能支持配置 IP 地址白名单。配置后,系统将对指定的流量不进行 QoS 控制。

配置 IP 地址白名单,请按照以下步骤进行操作:

- 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->控制->流量管理",
 进入 QoS 配置页面。
- 2. 在『应用 QoS』标签下的<白名单>处指定不受 QoS 规则流量限制的 IP。可以选择指定 IP 范围或地址簿条目:
 - IP 范围: 在文本框中输入起始 IP 地址和终止 IP 地址;
 - 地址条目:在组合框中输入或选择地址簿中的地址条目。

🛛 🔴 QoS酉沿					
限流对象: 1	接口 ~	ethernet0/2	🔪 所属的	安全域为 tru	st
应用QoS	IP QoS				
白名单:	地址条目	✓ test-3.3.3.0			*
时间表:			~	添加	
				删除	



第6章 网络行为控制

配置网络行为控制功能中的 URL 过滤、bypass 域名以及应用行为控制等与网络域名有关的功能时需要现在设备上上进行 DNS 配置,并且尽量保证设备使用的 DNS 与内部电脑的 DNS 一致。 DNS 配置 , , 请按照以下步骤进行操作 :

- 1. 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->网络->网络连接", 进入网络连接页面。
- 2. 从页面右侧辅助栏的<任务>区选择『DNS 列表』链接, 弹出<DNS 列表>对话框。
- 选中『服务器和代理』标签,在<DNS 服务器>部分点击『新建』按钮,弹出<DNS 服务器配置>对话框。

DNS列表				8
服务器和代理	解析配置	餐存 NBT缓存		
DNS服务器				
●新建	🛗 刪除			
■ 服务器I	р	虚拟路由器	类型	
8.8.8.8		trust-vr	手工配置	
	DNS服务器配置		8	
	服务器IP:		填写DNS地址	×
DNS代理	虚拟路由器:	trust-vr 👻		下启用DNS代理
新建「「」「「」「」		确定	取消	
				^
				~
				关闭

URL 过滤(有 URL 许可证)

URL 过滤配置,请按照以下步骤进行操作:

1. 通过 WebUI 方式登录 StoneOS 从页面左侧导航树选择并点击"配置->控制->URL 过滤", 进入 URL 过滤页面。



RL过滤规则配置		1 情言抑励之我	
名称:	test	(1~31)字符	
——当满足以下条件8	J		
目的安全域:		2.选择外网接口所属	安全
用户:	trust	西罟	
叶词丰,	untrust	Hem	
ロルロ北方・	dmz	配置	
做如下控制	I2-trust		
	l2-untrust		
URL类别	l2-dmz		_
1 新建	VPNHub		
URL类别	test	□记录日志	
恶意代码	tap1		
挂马隐患			
钓鱼欺诈			
远程代理			
广告			~
色情			
列表外的所有URI	.: 🗌 阻止访问	🔄 记录日志	
		确定 取消	

2. 点击『新建』按钮, 弹出<URL 过滤规则配置>对话框。

 指定规则的用户,该用户可以为地址簿地址条目、IP 地址、IP 地址范围、角色、用户或用 户组。系统默认用户为 Any,即对任意用户都有效,如果要修改,则先删除 any 用户。点 击后面的『配置』按钮,在弹出的<用户配置>对话框中对用户进行修改。



URL过滤规则配置		8	
名称: test	(1~31)字符		
目的安全域: untrust	Y		
用户: Any	置頌	1.点击配置	
时间表:	置。		
做如下控制			0
			~
配置类型: ④ 源地址	○用户		
添加值			
用户类型: 地址簿 🖌			
地址簿: Any	~		添加
用户	AA	A服务器	删除
Any		^	3 卢夫删除
2.选中any条目			CONTRACTOR OF
		~	
		确定	取消

 配置实际所需要限制的内网 IP 用户,注意掩码 32 表示单个主机 IP,如需整个网段则填写 相应的网络掩码。在<用户类型>下拉菜单选中"IP",需要在<IP 地址>文本框输入 IP 地 址和网络掩码。



用户配	置						۵
配置类	≷型: 5加值—	 ● 源地址 1.洗择IP 	○用户				
用户	唑型:	IP 🗸			4.	添加	
IP地	址:	192.168.1.2	/ 32 ×			添加	
甩	沪	2.主机ip地址	3.掩码32代表单台主体AA服务器	R S		删除	
					^		
				5.确定	×		
				确定		取消	

5. 在<做如下控制>部分配置规则的控制内容(URL 类别和 URL 关键字类别)和控制动作(阻止访问和记录日志)。(可选)



URL过滤规则配置					
名称: ┌────────────────────────────────────	test			(1~31)字符	
目的安全域:	untrust		~		
用户:	192.168.1.	2/32		配置	
时间表:				配置	
做如下控制					
URL类别U	RL关键字类	:别			
1 新建	◙编辑				
URL类别		□阻止访	ÌO	□记录日志	
恶意代码		V			
挂马隐患	1.勾选相				\sim
钓鱼欺诈	应光刑				2.记录日志
远程代理	MAX #				(可选)
广告					~
色情					
列表外的所有URL:	四阻	上访问		记录日志	
				3.确定	
				确定	取消

 完成上述配置,即可实现阻止内网 192.168.1.2 这个 IP 访问"恶意代码"和"挂马隐患" 这两类网站。

配置自定义 URL 库

用户可以根据需要自定义 URL 类别。与预定义 URL 类别相同,自定义 URL 库能够为 URL 过 滤功能配置、网页关键字过滤功能配置和 Web 外发信息控制功能配置提供 URL 类别。

新建 URL 类别,请按照以下步骤进行操作:

1. 从页面左侧导航树选择并点击"配置->控制->URL 过滤/网页关键字/Web 外发信息",进

入功能页面。

- 2. 从页面右侧辅助栏的<任务>区选择『自定义 URL 库』链接, 弹出<自定义 URL 库>对话框。
- 点击『新建』按钮, 弹出<URL 类别>对话框。输入自定义 URL 类别名称和需要过滤的域名。



URL类别		8
类别名称: ABC	定义类别名称	
URL http:// www.sina.com.cn ×	(1~255)字符	添加
URL 输入需要过滤的域名		编辑
www.baidu.com		▲開除
		×
	确定	取消

4. 点击『确定』按钮,保存所做配置。即可在配置 URL 过滤时找到自定义的 URL 类别,选择控制动作。

URL 过滤(无 URL 许可证)

URL 过滤配置,请按照以下步骤进行操作:

- 1. 新建 URL 过滤规则,步骤请参阅 URL 过滤(有 URL 许可证)步骤 1-4。
- 在<URL 过滤规则配置>对话框中的<做如下控制>部分点击<HTTP 控制>,添加要阻止 的网站,*号表示通配符,这样该网站的子域名也会一起被禁止,如果是仅需阻止单个域名, 则填写该域名全称,也可以在用户访问该网站的时记录日志。(可选)



——做如下控制	il]			
FTP控制				÷
HTTP控制				
GET 🗸	*.baidu.com	阻止 丫	记录日志 💙	添加
类型	域名	动作	日志	编辑
1.行为GET	2.填写域名或IP	3.选择阻止	4.记录日志 (可选)	5.添加 删除
НТТР阻止了	下载			ŧ
			6.确定	
			确定	取消

3. 完成上述配置,即实现了阻止内网 192.168.1.2 这个 IP 地址访问带 baidu.com 的所有 网站。

网页关键字过滤

新建网页关键字规则,请按照以下步骤进行操作:

- 1. 从页面左侧导航树选择并点击"配置->控制->网页关键字",进入网页关键字页面。
- 2. 点击『新建』按钮, 弹出<网页关键字规则配置>对话框。



网页关键字规则配置	1.填写规则名称	6
名称:	test	(1~31)字符
目的安全域:		▼ 2.选择外网接口安全域
用户: 时间表:	trust untrust dmz	配置
 做如下控制 ● 新建 关键字类别 	I2-trust I2-untrust I2-dmz VPNHub	□记录日志
	test tap1	^
		~
关键字控制范围:	<u>所有网站</u>	
		确定取消

3. 指定规则的用户,该用户可以为地址簿地址条目、IP 地址、IP 地址范围、角色、用户或用 户组。系统默认用户为 Any,即对任意用户都有效,如果要修改,则先删除 any 用户。点 击后面的『配置』按钮,在弹出的<用户配置>对话框中对用户进行修改。



网页关键字规则配置			6	3	
名称: 当港兄以下冬件P	test	(1~)	31)字符		
目的安全域:	untrust	v			
用户:	Any		配置 1.点	击配置用户	
时间表:			配置		
(時前下15年) 用户配置					0
配置类型: ● 源	间地址	○用户			
添加值					
用户类型:	地址簿 🗸				
地址簿:	Any	~			添加
用户			AAA服务器		刪除
Any			-	~	3.点击删除
2.选中该用户	条目				
				~	
				确定	取消

配置实际所需要限制的内网 IP 用户,注意掩码 32 表示单个主机 IP,如需整个网段则填写相应的网络掩码。在<用户类型>下拉菜单选中"IP",需要在<IP 地址>文本框输入 IP 地址和网络掩码。



用戶	可問問				8
霄	置类型:	◉ 源地址	○用户		
	一添加值-	1.选择IP			
L	用户类型:	IP 👻			4.添加
	IP地址:	192.168.1.2	/ 32	×	添加
	用户	2.填写主机ip	3.掩码32代表	AAA服务器	删除
			单台主机	5 卢志	
					定取消

在<做如下控制>部分配置规则的控制内容(网页关键字类别)和控制动作(阻止访问、记录日志和记录内容)。点击『新建』按钮,弹出<关键字类别配置>对话框。

关键字类别配置	1.填写名称	6	3
类别名称:	www	× (1~31)字符	
● 新建	1 前期除		
■ 关键字	 2.点击新建	类型 信任值	
		^	

 点击『新建』按钮, 弹出<关键字类别>对话框进行新建关键字类别。并点击『确定』按钮 保存所做配置并返回上一级对话框/页面。

关键字类别配置				8
类别名称:	www 1.关键字名称	(1~31)字符	2.匹配规则	
关键字:	赌博	(1~31)字符	完全匹配 Y ?	
信任值:	100	(1~100) ?		
如果关键字1信/ 相应的控制动作	任值*匹配次数++关键	字n信任值*匹配次数:	>=100,贝触发	取消
1 新建	🖬 刪除		3.点击添加	
■ 关键字	:	类型	信任值	

7. 在<做如下控制>部分配置规则的控制内容。



网页关键字规则配置		8
名称: ────当满足以下条件时	test	(1~31)字符
目的安全域:	untrust	*
用户:	192.168.1.2/32	配置
时间表:		西置
——做如下控制——		
1 新建	2/编辑	
关键字类别	□ 阻止访问	□记录日志
www		
	1.勾选阻止访问	2.记录日志 (可选)
		~
关键字控制范围:	所有网站	
		3.点击确定
		确定取消

 完成上述配置,即实现了阻止内网 192.168.1.2 这个 ip 地址访问带有"赌博"关键字的 网页。

网络聊天控制

网络聊天功能可以通过聊天软件的账号控制用户使用 MSN、QQ 和雅虎通聊天的行为,并记录上下线日志。

以 QQ 为例,网络聊天控制配置,请按照以下步骤进行操作:

1. 确认设备已经安装了最新的应用特征库。



Sto	neOS								系统管理-
	配置		定制 刷新	手动場	新				系统
🙆 È	5	● 系统信息							
网络 ● ● ●	网络连接 虚拟系统 NAT 路由	序列号: 主机名称: 硬件平台: 系统时间: HA状态:	1504913110001329 SG-6000 SG-6000-G2120 Aug/2/2014 Sat 03:57:38 Standalone	编辑 编辑 编辑	软件版本: 病毒特征库: IPS特征库: URL库: 应用特征库:	Version 5. 2.0.14073 <u>1.0.194</u> 24 1.0.19 20 <u>3.0.14072</u> 渔伊成	0 SG6000-M-5.0R3P5.bin 2 0 20140730 22:51:55 014-06-13 16:15:07 14-02-25 11:09:54 11 (Profession) 2014-07-21 田純印度版大为最新版	014/04/02 15:17:37	<u>升级</u> 升级 升级 升级 升级
	IPSec VPN SSL VPN L2TP VPN Web认证 802.1X 链路负载均衡	 涼里监控 整机流量 Z – 			沿方部行	#16/1/22	1111⊞+Hac+>3+echnok		详擅
安全 《 》 》	策略 病毒过滤 入侵防御 攻击防护 ARPI5拍	Y			10.06H.XX				
物制	UN MUL	00:00	00:15		00:30	00	:45 01	:00	01:15

- 开启内外安全域的应用识别功能。从页面左侧导航树选择并点击"配置->网络->网络连接",
 进入网络连接页面。
- 3. 从安全域列表中选中安全域,然后双击或者点击列表左上方的『编辑』按钮。
- 在弹出的<安全域配置>对话框的<高级属性>部分,选中<应用识别>复选框开启安全域
 的应用识别功能。

安全域配置		8
安全域名称: 类型:	untrust 〇 二层安全域	^
虚拟路由器: 接口选择:	trust-vr ▼ 可绑定接口 ● ethernet0/1 ● ethernet0/4 ● ethernet0/5 ● ethernet0/6 ● ethernet0/7 ● tunnel1 ● tunnel10 ● tunnel128 ●	
——高级属性—— 应用识别:		
WAN安全域: NBT缓存:		~
-	确定	取消



 新建网络聊天规则。从页面左侧导航树选择并点击"配置->控制->网络聊天",进入网络聊 天页面。点击『新建』按钮,弹出<网络聊天规则配置>对话框。

网络	聊天规则配置		1.持定规则复数
Ę	名称: - 当满足以下条件时	QQ	1.4号规则名称 (1~31)字符
E	目的安全域:	untrust 🗸	2.选择目的安全域
月	月户:	Any	西: 置
B	村间表:	3.配置用户I	P 配置
	- 做如下控制		
	MSN QQ	雅虎通	
	账号:		4.填写需控制的账号 添加 添加
	账号	□ 阻止使用	
	123456		
			5.选择控制行为
	列表外的所有OOM	· 문:	
			6.列表外其它账号行为控制
			确定 取消

如果想要阻止所有的 qq 账号都无法登录,则可以勾选<列表外的所有 QQ 账号>部分的<
 阻止使用>复选框,或者直接通过设备的策略规则进行对 qq 应用的阻止。



第7章 VPN 高级配置

基于 USB Key 的 SCVPN 配置

本节介绍基于 USB-KEY 的 SSL VPN 配置,其他 SSL VPN 配置请参阅 SCVPN 配置。

基于 UEB Key 的 SCVPN 配置包括:

- ◆ 新建 PKI 信任域
- ◆ 配置 SCVPN
- ◆ 制作 USB Key
- ◆ 使用 USB Key 方式登录 SCVPN

新建 PKI 信任域

新建 PKI 信任域,请按照以下步骤进行配置:

- 1. 从工具栏的<对象用户>下拉菜单选择『PKI』, 弹出<PKI 管理>对话框。点击『信任域』 标签, 进入信任域标签页。
- 2. 点击信任域列表左上方的『新建』按钮, 弹出 < PKI 配置 > 对话框。
- 在<信任域>文本框输入信任域的名称并选择证书获取方法,然后点击『下一步』按钮。选择<手动输入>方法获取证书,点击后进入<CA证书>页面,在该页面导入 CA证书(点击 『浏览』按钮选择证书,然后点击『导入』按钮)。获取证书方法包括以下两种:
 - 手动输入:使用终端(剪切和粘贴)的获得方法;
 - 自签名证书:使用自签名的获得方法。


PKI配置		8
PKI配置 基本 信任域: 证书获取方法:	1.输入信任域名称 test × (1~31)字符 ● 手动输入 2.选择手动输入 ● 自签名证书	
	取消 应用 下一步	

4. 导入需要使用的 CA 证书。







5. 导入成功后可看到 CA 证书相关信息。



PKI配置		0
—— 基本 —————		٦
信任域:	test	
CA证书		٦
主题:	/DC=com/DC=zlzhang/CN=hillstone	
颁发者:	/DC=com/DC=zlzhang/CN=hillstone	
序列号:	20:eb:bd:e9:be:bf:c0:8a:41:40:28:40:df:16:79:ef	
指纹(SHA-1):	8D:51:0A:38:2F:7C:C3:D9:9B:4E:0F:80:74:F5:01:0C:CC:B3:41:9B	
有效期:	从 2011-01-11 01:53:18 GMT 到 2016-01-11 02:02:10 GMT	
	取消 上一步 下一步	

6. 点击『下一步』按钮,从<密钥对>下拉菜单为信任域指定密钥对,其他信息可选填。



Hillstone 山石网科基础配置手册

PKI配置		8
基本		
信任域: 密钥对:	test Default-Key	选择相应密钥对
名称:		(1~63)字符
国家(地区):	CN	(1~2)字符,缺省值:CN
位置:		(1~127)字符
州/省:		(1~127)字符
机构:		(1~63)字符
机构单元:		(1~63)字符
即谐	1	由语
取消	上一步 应用	申请 下一步

7. 点击『下一步』, 在新页面配置 CRL 相关选项。



	\ \	
- CRL(业书吊销列表	.)	
检查:	不检查	
自动刷新:	每小时	
URL1:	http:// 🗸	(1~248)字符
URL2:	http:// 🗸	(1~248)字符
URL3:	http:// 🗸	(1~248)字符

配置 SCVPN

请按照以下步骤进行操作:

- 配置 SCVPN 名称、用户身份认证的 AAA 服务器、设备端接口、隧道接口、地址池以及策 略规则和隧道路由,请参阅 <u>SCVPN 配置</u>步骤 1-9。
- 2. 在 < 客户端 > 页面,进行客户端和客户端证书认证配置:
 - USB Key 证书认证:选中<启用>复选框开启客户端证书认证功能。该功能支持"用户 名/密码 + USB Key"和"只用 USB Key"两种认证方式;
 - 信任域:在<信任域>下拉菜单中选中之前创建的信任域。



SSL	VPN配置					8
	欢迎页 接入用户 接入接口/隧道接口 策略/隧道路由配置 参数配置	客户端配置 重定向URL: 英文标题: 中文标题: 客户端证书认证		(1~255)字符 (1~31)字符 (1~63)字符		
	客户端 主机检测/绑定 短信口令认证 最优路径检测	数字证书认证: USB KEY下载网址: 信任域: CN匹雷: 客户端证书的主题CN字 OU匹雷: 客户端证书的主题OU字	 ✓ 启用 ● 用户名/密码 +数字证 test ✓ 段必须包含该字符串 段必须包含该字符串 	 田 (0~63)字符 1.选择新建信任域 主题名字检查: (0~31)字符 (0~31)字符 	○ 只用数字证书□ 启用	2 占土沃加
		☐ 信任域 ☐ test	≥题名字检查	CN匹配	OU匹戳	
				简单配置	上一步	 · · · · · · · · · · · · · · ·

制作 USB Key

请按照以下步骤进行配置:

1. 格式化 USB Key , 打开 "Hillstone 初始化工具", 插入 USB Key , 系统将进行自动格式化。



挑量初始化工具	
─ 初始化参数 ────────────────────────────────────	Hillstone
管理员口令:	1111
管理员口令重试次数:	15
用户口令:	1111
用户口令重试次数:	15
	格式化成功.

2. 导入认证证书,打开"Hillstone ukey admin 管理工具",点击<数字证书>标签,然后 点击<导入证书>按钮,输入保护口令(默认为 hillstone)。



A Hillstone UKey Adm	
关于(A)	
选择一个 UKey 安全设备 Hillstone UKey HID 0	▼刷新
设备信息 修改口令 数字证书 访	置网址
	A
•	
导入证书	退出
查看证书	刪除密钥容器

使用 USB Key 方式登录 SCVPN

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. 在 IE 浏览器的地址栏输入以下 URL 访问设备端:https://IP-Address:Port-Number。
- 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。在弹出的
 <请输入用户口令>对话框(如下图所示)中输入 UKey 的用户口令(默认为"1111"),并
 点击『确定』按钮。



请输入用户口令	
读卡器 Hillstone UKey	VKey 名字 Hillstone
, 请输入用户口令 🛛 🕌	***
原口令密码强度:弱	
确定	

 浏览器转到登录页面(如下图所示),输入用户名和密码,并点击『登录』按钮。此处的用 户名和密码为安全网关中配置的用户及其相应的密码。

Hillstone	Hillstone Secure Connect
	用户名: hillstone 密码: ●●●●●●● 登录

- 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。
- 安装成功后,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)。选中<用户
 名/密码>单选按钮,点击『确定』按钮。



⑦ 登录模式
◎ 用户名/密码
◎ 用户名/密码 + USB key
◎ 只用USB key
选择证书 确定 取消

 系统弹出"用户名/密码"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。

@ 登录	×
Hillstone Secur	Hillstone 山石岡科 re Connect
最近访问:	test@61.161.171.138:4433 ▼
服分器: 端口: 田白夕·	4433 test
·□/·□· 密码: PIN 码:	•••••
	模式 登录 取消

PnPVPN

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)。

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
- ◆ 策略配置
- ◆ PnPVPN 客户端配置

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。
- 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。

用户配置			8
基本配置 PnP V	PN配置		
名称:	pnp		(1~63)字符
密码:	•••••	1.自主的设定,后面基本不使	<mark>用</mark> (0~31)字符
重新输入密码:	•••••		
国家代码(可选)+手机 号码:	请输入手机号	2	(0,6~15)字符
描述:			(0~127)字符
组:			选择
IKE标识:	O None	● FQDN ○ ASN1DN ○ KEY-	·ID
IKE标识:	pnpuser1		(1~255)字符
账户到期日:	🔲 启用	- 2.必须填写IKE标识,设定的 <i>)</i>	为分支的标识
如果启用了短信认证功	能,短信认证	冯将发送到用户设置的电话号码	
		确定	取消

3. 按照上图完成配置后,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。



用户配置		8
基本配置 PnP	VPN配置	
DHCP起始地址:	192.168.3.2	
DHCP结束地址:	192.168.3.200	此处是为客户端
DHCP网络掩码:	255.255.255.0	配置的DHCP地 址池和NAT
DHCP网关:	192.168.3.1	
DNS 1:	8.8.8.8	+
WINS 1:		+
隧道IP(可选):		□ 启用源NAT
		7/2
		确定 取消

4. 根据需要对该页面的其它选项进行配置。

5. 配置完成,点击『确定』按钮保存所做配置。然后需要重新编辑该用户,进入<PnPVPN 配置>,用于指定客户端的 VPN 路由。如果有多个分支客户端可重复上述步骤。



扁辑用户					8
基本配置 PnP	VPN配置 重新编	扁缉该用户	,为客户端酉	C置VPN路E	ŧ
隧道路由:	多个			选择	
DHCP起始地址:	192.168.3.2				
DHCP结束地址:	192.168.3.200				
DHCP网络掩码:	255.255.255.0				
DHCP网关:	192.168.3.1				
DNS 1:	8.8.8.8				
WINS 1:				+	
隧道IP(可选):				□ 启用:	原NAT
			ā	角定 一	取消
配置隧道路由					8
IP地址/网络掩码:	192.168.2.0	/ 24		●新増	
IP地址/网络摘得	<u>д</u>	操作			
192.168.1.0/2	4	Ť			-
192.168.2.0/2	4	Ű			

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:

- 1. 配置 P1 提议。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。



阶段1提议配置		•
提议名称:	提议名称随意选择 P1 × (1~31)字符	
认证:	pre-share ORSA-Signature ODSA-Signature	
验证算法:	○ MD5	
加密算法:	● 3DES ◯ DES ◯ AES ◯ AES-192 ◯ AES-256	
DH组:	◯ Group1	
生存时间:	86400 (300~86400)秒,缺省值:(86400)	
	认证方式 , 验证算法 , 加密算法 , DH组可以 自己设定。一般默认即可 , 两端必须一致	
	确定现消	

- 3. 配置 P2 提议。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『P2 提议』标签,进入 P2 提议标签页。
- 4. 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。

阶段2提议配置	8
提议名称:	P2 (1~31)字符
协议:	● ESP ○ AH
验证算法 1 :	○ MD5
验证算法2:	●无 ○ MD5 ○ SHA ○ SHA-256 ○ SHA-384 ○ SHA-512 ○ NULL
验证算法3:	●无 ○ MD5 ○ SHA ○ SHA-256 ○ SHA-384 ○ SHA-512 ○ NULL
加密算法 1 :	● 3DES ◯ DES ◯ AES ◯ AES-192 ◯ AES-256 ◯ NULL
加密算法2:	●无 ○ 3DES ○ DES ○ AES ○ AES-192 ○ AES-256 ○ NULL
加密算法3:	●无 ○ 3DES ○ DES ○ AES ○ AES-192 ○ AES-256 ○ NULL
加密算法 <mark>4</mark> :	●无 ○ 3DES ○ DES ○ AES ○ AES-192 ○ AES-256 ○ NULL
压缩:	None O Deflate
PFS组:	◯ Group1
生存时间:	28800 (180~86400)秒,缺省值:(28800) 此处必须选择Group2
启用生存大小:	□ 启用
	确定取消

5. 配置 VPN 对端。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『VPN 对端列表』标签,进入 VPN 对端列表标签页。



##1: 打描 基本配置 1.50%若年自治指定 パ端谷称: PNP 推口: 住田emet0/1 ♥ 2.送公网修口 根式: 主根式< ● 野蛮儀式 水池口: ● 充 ● 月戸组 送择AAA服务器: bcal ● 送得AAA服务器: bcal ● 水池口: ● 充 ● FQDN ● LFQDN ● 方 ● FQDN ● LFQDN ASN1-DN 水池口: ● 元 ● FQDN ● LFQDN ASN1-DN 水池口: ● 元 ● FQDN ● LFQDN ASN1-DN KEY-ID 北湖ID: ● 元 ● FQDN ● LFQDN ASN1-DN KEY-ID 4. (#持款以不需配置 建议1: P1 ● 「 ● SLE2 的新建的P1提议, 密钥自定 4. (#持款以不需配置 建议1: P1 ● SLE2 的新建的P1提议, 密钥自定 ● SUBHP+P1指定如 4. (#持款以不需配置 「法 ● エ ● エ ● 「 ● SUBHP+P1指定如 ● SUBHP+P1指定如 「法 ● エ ● エ ● SUB ● SUB <t< th=""><th>IKE VPN配置</th><th></th><th></th><th></th><th></th><th></th><th>8</th></t<>	IKE VPN配置						8
ZJ薄客称: PNP (1~31)字符 写入 推口: ethemet0/1 2.送公例按訂案様式,用户组类型设置、 集工: 主模式<●野蛮復式 3.必须按野蛮模式,用户组类型设置、 类型: 静态IP 动态IP ●用户组 送择AAA服务器: bca 小店口: ● 元 FQDN U-FQDN ASN1-DN A.保持款认不需配置 J端口: ● 元 FQDN U-FQDN ASN1-DN KEY-ID 4.保持款认不需配置 J端菜口: ● 元 ● FQDN U-FQDN ASN1-DN KEY-ID 4.保持款认不需配置 J端菜口: ● 元 ● 元 ● 5.送焊之前新建的P1提议, 密钥自定 ● 示 提示非 ● 5.送焊之前新建的P1提议, 密钥自定 ● 小 ● 5.送焊之前新建的P1提议, 密钥自定 ● 小 提供專密钥: ● 二 ● 1.177, 关闭 ● 二 ● 点击主式応后,将 修建32: 隧道 ● 近 ● 点击主式応后,将 ● 点击主式応后,将 修建32: ● 認道 ● 近 ● 法 ● 小 ● 小 「 ● 「 ● 「 ● 「 ● 「 ● 小 ● 「 ● 「 ● 「 ● 「 ● □ ● □ ● 「 ● 「 ● 「	步骤1: 对端 基本配置 高级] 四二二	1.对端名字	自己指定			
描口: ethemetU/1 2.送公网按J 概式:	对端名称:	PNP	(1~31)	字符 导入			
银云: ○ 主银云 ● 野蛮俱云 3. 必须按野蒸偡式 , 用户组类型设 量。 炎型: ● 赤芯 P ● 动态 P ● 用户组 量。 法择AAA服务器: ● cal ▼ 本地口: ● 元 ● FQDN ● U-FQDN ● ASN1-DN ● KEY-ID 4. 保持款以不需配置 对端口: ● 元 ● FQDN ● U-FQDN ● ASN1-DN ● KEY-ID 4. 保持款以不需配置 对端口: ● 元 ● FQDN ● U-FQDN ● ASN1-DN ● KEY-ID 4. 保持款以不需配置 建议1: P1 ▼ \$. 达择之前新建的P1/提议 , 密钥自定 提议1: P1 ▼ * 5. 达择之前新建的P1/提议 , 密钥自定 「按示 「5~127)字符 * 4. 保持款以不需配置 生成用户密钥 ● 6. 创建用户时指定的工 · · · · · · · · · · · · · · · · · · ·	接口:	ethernet0/1	2.选公网)	医口	1		
 朱型: ● 静态IP ● 动态IP ● 用户组 ■ 法择AAARB分器: ● cal ● ● 元 ● FQDN ● U-FQDN ● ASN1-DN ○ KEY-ID ● .(\$1550, A.(\$1550, A.(\$1550,	模式:	○王視式	 野蛍視式 		3.必须按	野蛮模式,用户组类型设	
这样AAA服务器: local	类型:	○静态IP	○动态IP	● 用户组	置。		
 本地ID: ● 元 「FQDN ○ U-FQDN ○ ASN1-DN ○ KEY-ID 4.保持款认不需配置 7.与於以子常新建的P1提议, 密钥自定 6.何建用户时指定的II 6.何建用户时指定的II 7.与上方密钥相同 6.信建工成后,将 4.保持款认不需配置 5~127)字符 4.成用户密钥 6.何建用户时指定的II 6.何建用户时指定的II 6.何建用户时指定的II 6.何建用户时指定的II 6.何建用 4.保持款认不需配置 4.保持款认不需 4.保持款认不需<!--</td--><td>选择AAA服务器:</td><td>local</td><td>*</td><td></td><td></td><td></td><td></td>	选择AAA服务器:	local	*				
対端ID: ● 无 ● FQDN ● U-FQDN ● ASN1-DN ● KEY-D 提议1: P1 ● 5.选择之前新建的P1提议,密钥自定 持共享密钥: ● 5.选择之前新建的P1提议,密钥自定 生成用户密钥: 生成用户密钥 修理用户的指定的I ● 6.创建用户的指定的I 修理结果: ● 7.与上方密钥相同 ● 修理2: 隧道 ● 「 少骤2: 隧道 ● 「 ● 授弊2: 隧道 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● 「 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● <	本地ID:	●无 ○ F	QDN 🔿 U-FQD	N () ASN1-DN	() KEY-ID	4.保持默认不需配置	
提议1: P1 ▼ 5.选择之前新建的P1提议,密钥自定 6.41至70字符 生成用户密钥 6.41重用户时指定的I 生成用户密钥 ● 41重用户时指定的I ● 41重用户时指定的I 「KE标识: pnp 「标识 「扱共享密钥: ● 41重 ● 41重 「安潔1: ● 11 ● 11 「法学業2: ● 200 ● 200 「安潔1: ○ 11 ○ 11 「法学 路由: ● 200 ● 次起者 「中広者 ● 11 「安潔3: ● 200 「公式書 ● 11	对端ID:	●无 ○ F		N O ASN1-DN	KEY-ID		
•••••• ••••••	提议1:	P1	▼ 🕈 5.选	择之前新建的P1	提议,密钥自治	te a constant a consta	
生成用户密钥: 生成用户密钥 6.创建用户时指定的口标只 「KE标识: pnp 预共享密钥: 1.5 広賓钥相同 生成 美湖 8.点击生成后,將 生成 美湖 8.点击生成后,將 管螺2: 隧道 0kke3nFFDcDb3bYcp5M86Ce4+0 即可 夢螺2: 隧道 0ke3nFFDcDb3bYcp5M86Ce4+0 即可 夢螺1: 双点 文起者 0 「小田 空話 ○次記者 ●向应者 NAT穿越: 2 自用 产生路由: 2 自用 接受对端任意口: 自用 加端存活检测: 自用 你说: (De255)专菜	预共享密钥:	•••••	(5~127)字符			
	生成用户密钥:	牛成	生成用户密钥				htive
Material Material <t< td=""><td></td><td></td><td></td><td>nnn</td><td></td><td></td><td>ЛКЕ</td></t<>				nnn			ЛКЕ
			私共宣应知•	php			
夢娜2: 隧道 确定 取消 确定 取消 KE VPN面活 基本配活 高级配置 连接类型: 0 双向 发起者 NAT穿越: ② 自用 产生路由: ② 自用 接受对端任意ID: 自用 对端存活检测: 自用 描述: (0~255) 支注			创建结果:	生成 Okke3nFFE) 关i DcDb3bYcpSM8	闭 8.点击生成后,将 6Ce4+0 即可	
确定 取消 KE VPN配置 步骤1: 对端 基本配置 高级配置 连接类型: ① 双向 ② 发起者 响应者 NAT穿越: ② 启用 产生路由: ② 启用 接受对端任意ID: □ 自用 对端存活检测: □ 自用 描述: (0~255) 字符	步骤2: 隧道						_
KE VPN酒:: 步骤1: 对端 基本配置 高级配置 连接类型: ② 双向 ② 发起者 ◎ 响应者 NAT穿越: ② 启用 产生路由: ③ 启用 接受对端任意ID: □ 启用 对端存活检测: □ 自用 描述: (0~255)字符						· · · · · · · · · · · · · · · · · · ·	
歩骤1: 対端 基本配置 高級電置 连接类型: ● 双向 ● 发起者 ● 响应者 NAT穿越: ● 启用 产生路由: ● 倉用 接受对端任意ID: ● 启用 対端存活检测: ● 自用 (0~255)字符	KE VPN配置						8
基本配置 高級配置 连接类型: ① 双向 ② 发起者 响应者 NAT穿越: ② 启用 产生路由: ③ 启用 接受对端任意ID: □ 启用 对端存活检测: □ 自用 ////////////////////////////////////	步骤1: 对端						
连接类型: ● 双向 ● 发起者 ● 响应者 NAT穿越: ☑ 启用 产生路由: ☑ 启用 高級配置中选择自动产生路由 接受对端任意ID: □ 启用 对端存活检测: □ 启用 描述: (0~255)字符	基本配置高级	配置					
NAT穿越: ☑ 启用 产生路由: ☑ 启用 接受对端任意ID:	连接类型:	• 双向	○ 发起者	○ 响应者			
产生路由: 図 启用 接受对端任意ID: □ 自用 功端存活检测: □ 自用 協調: □ (0~255)字符	NAT穿越:	☑ 启用					
接受对端任意ID:	产生路由:	☑ 启用	高级配置中注	选择自动产生】	路由		
対端存活检测: □ 启用 描述:	接受对端任意ID:	🗌 启用					
場ば: (1)~255)字符	对端存活检测:	□ 启用					
	描述:			(0~255)字符			
XAUTH 服务器: IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	XAUTH 服务器:	□ 启用					

6. 点击列表左上方的『新建』按钮, 弹出 < VPN 对端配置 > 对话框。

- 7. 配置隧道。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『IPSec VPN』标签,进入 IPSec VPN 标签页。
- 8. 点击 IKE VPN 列表左上方的『新建』按钮, 弹出<IKE VPN 配置>对话框。
- 9. 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。用户せ	1可以直接在该页面新建对端(ISAKMP	网关)。
---------	----------------	---------------	------

IKE VPN配置		0
步骤1:对端 基本配置 高级		
对端名称: 接口: 模式: 类型: 选择AAA服务器: 本地ID:	PNP 新建 在下拉菜单中选择之前新建 的VPN对端,下面内容会自 动填充。 ● 主模式 ● 野蛮模式 静态IP 动态IP ● 用户组 local ▼ ● 无 FQDN U-FQDN ASN1-DN ● 工 ● DDDN ● DDN ● DDN ● DDN	
对端ID: 提议1: 预共享密钥: 生成用户密钥:	 ● 元 (FQDN () U-FQDN () ASN1-DN() KEY-ID P1 () ↓ (5~127)字符 生成 	
步骤2:隧道	确定职法	肖

10. 点击<步骤2:隧道>,展开隧道具体配置选项。



IKE VPN配置		0
步骤1: 对端		
步骤2:隧道		
基本配置	高级配置 1名称自定	
名称:	ipsec (1~31)字符	
模式:	● tunnel ○ transport 2.默认Tunnel模式,不需修改	
p2 提议:	▶2	
代理ID:	● 自动 ○ 手工 建P2提议	
		75
		确定

隧道接口配置

请按照以下步骤进行隧道接口配置:

- 点击"配置->网络->网络连接",进入网络连接页面。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。
- 2. 接口创建完成之后,进入该隧道接口,配置隧道绑定。



接口配置	8
常规 属性 高级 RIP	
管理方式 Telnet SSH I Ping I HTTP HTTPS SNMP	^
隧道绑定配置 隧道淋刑· ● IPSec VPN ● SSL VPN 1.选择IPsec VPN	
WPN名称: ipsec 2.在下拉菜单中选择之前新建的隧道名称	
网关: 3.不用填写 添加 4.点击添加	
·····································	
VPN名称 类型 网关	
ipsec ipsec	
\sim	~
确定	取消

策略配置

根据网络拓扑情况,配置相应的访问策略。

- 1. 从页面左侧导航树选择并点击"配置->安全->策略",进入策略页面。
- 点击列表左上角的『新建』按钮, 弹出<策略配置>对话框, 在该对话框对策略规则进行编 辑。



策略配置	8
基本配置 高级控制	
名称:	(0~95)字符
当满足下列条件时—1.隧道接口所在安全	域2.内网所在安全域
源安全域: Any	目的安全域: 到 Any ✓
源地址: Any	目的地址: 到 Any
服务簿: Any	时间表:
<u>源用户:</u> 多个	3.全部any即可 , 有其他要求 可细化配置
──做如下控制 行为:	
○ 拒绝 Web ì	从证只能工作在trust-vr。
○ 安全连接 WEBi,	↓证 ✓ local ✓
	确定取消

PnPVPN 客户端配置

请按照以下步骤进行配置:

- 1. 将设备接入互联网,配置外网 IP 以及默认路由。
- 2. 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。
- 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。依次填写或者选择各项。



PnPVPN配置		8
PnPVPN配置 服务器地址: ID: 密码: 重新输入密码: 自动保存: VPN出接口: VPN入接口:	221.224.30.141 pnp ● 由 ● 接口 ● 接口 ● 接口 ● 按口	 1.Sever端公网IP (A.B.C.D)/(1~255)字符 2.Sever端用户IKE标识 (1~255)字符 (6~31)字符 3.Sever端建VPN第一阶段时 , IKE标识和密钥生成的新密钥 5.VPN公网接口 6.内网接口, Sever端配置 的DHCP网关IP将被配置在该 接口。并在该接口启用DHCP 服务。所有配置都由Sever端 下发,本地不需要其他配置。 包括路由和策略。
		确定 取消 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。

5. 大概需要1分钟协商,之后接入端 VPN 配置以及内网 IP 配置均自动完成。



第8章 高可靠性

高可靠性介绍

高可靠性(High Availability),简称为 HA,能够在通信线路或设备产生故障时提供备用方案, 从而保证数据通信的畅通,有效增强网络的可靠性。实现 HA 功能,用户需要配置两台采用完全相 同的硬件平台、固件版本,均安装相同的许可证、且所有接口对应关系一致的 Hillstone 设备组成 HA 簇。当一台设备不可用或者不能处理来自客户端的请求时,该请求会及时转到另外的可用设备 来处理,这样就保证了网络通信的不间断进行,极大地提高了通信的可靠性。

Hillstone 设备支持 HA 的 2 种工作模式 :Active-Passive(A/P)模式和 Active-Active(A/A) 模式:

◆ Active-Passive (A/P)模式:系统会将安全网关A选举为主设备,进行流量转发。安全 网关B为备份设备,安全网关A会将其配置信息以及状态数据同步到安全网关B。当安全 网关A出现故障不能正常转发流量或安全网关A的TRACK生效时,安全网关B会在不影 响用户通信的状态下切换为主设备,继续转发流量,拓扑如下:



◆ Active-Active (A/A)模式:两台设备均会开启 HA 功能。系统将安全网关 A 选举为 group0 的主设备。安全网关 A 向安全网关 B 进行同步配置。同步配置完成后,安全网 关 B 抢占为 group1 的主设备。在正常情况下,两台设备独立运行各自的工作:安全网关 A 对财务部和研发部访问网络的流量进行转发;安全网关 B 对研发服务器群访问网络的流

量进行转发。如果其中一台设备发生故障或者 TRACK 生效时,另外一台设备可运行自身工作的同时接管故障设备的工作,保证工作不间断。例如:安全网关 B 故障无法工作,安全 网关 A 在转发财务部和研发部访问网络流量的同时 将转发研发服务器群访问网络的流量, 拓扑如下:



高可靠性配置

请按照以下步骤进行配置:

1. 从工具栏的<系统管理>下拉菜单选择『HA』, 弹出<HA>对话框。按照下图配置:



HA	选择物理接口作	为心跳接口	5	元余心跳接口 (可	[选]	8
HA连接接口1:	无	▼ 接	<u>ق</u> ا2:	无 1	*	
IP地址:		/			_	
HA簇ID:	无	*				
	数值低成为主设备	z		主设备配置 0表示	不抢占	
优先级:	100 🗘	(1-254)	抢占时间:	0	(0-600秒)	
Hello报文间隔:	1000 🗘	(50-10000毫秒)	Hello报文警戒值:	3 🗘	(3-255)	主监测
免费ARP包个数:	15 🗘	(10-20)	监测对象:	无	天效时,备机会 主设备	会切换为
描述:					(1-31字符)	
组1						
优先级:	100 🗘	(1-254)	抢占时间:	0	(0-600秒)	
Hello报文间隔:	1000 🗘	(50-10000毫秒)	Hello报文警戒值:	3	(3-255)	
免费ARP包个数:	15 🗘	(10-20)	监测对象:	无 💙		
描述:					(1-31字符)	-
					人 /(月65)	
A/P 惧式只须能正 主语名 门实现	急组U, A/A 摆入	可的配直组U和组	11,网络正吊的匠	小小设备只允当	一门组的	
工议田, 以天地	业务的分担负载					
工议田,以关税	业务的分担负载					
	业务的分担负载				78-2	田 (出

- 配置监测对象。从工具栏的<对象用户>下拉菜单选择『监测对象』, 弹出<监测对象>对话框。点击监测对象列表左上方的, 弹出<监测对象配置>对话框。
- 3. 如果选择"接口"监测类型,点击 『添加』 按钮,然后在<添加接口对象>部分添加监测条目, 用来监测接口的物理状态,可以添加多个接口,每个接口有一个权值,该数值表示该接口 DOWN 后将释放的数值,当所有释放的权值累计数值大于等于警戒值的时候,该检测对象 就生效,权值和警戒值都可以自行调整。



▲ ⇒≤24				
「割頭」	▶编辑 懂删除			
监测对象配置				E
- 监测时象 -				
名称:	test			
警戒值:	255	(1~255),缺省值:255		
监测类型:	◎ 接口	HTTP Ping ARP DNS TCP		
│ 添加监测成	 员			
_ 类型	1	接口	权值	添加
■ 接口		ethernet0/0	255	
				Ŧ
财象			确	定
「新建」	■编辑 懂 刪除			
高洲対象間市				
<u> </u>				
血测闪家間面 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□				
★ 2015 第二章 1000 1000 1000 1000 1000 1000 1000 10	test	(1255))))		
血测X1家間(五 监测)对象 - 名称: 警戒值:	test 255	(1~255),缺省值:255		
血观(x)家町五 监观)対象 - 名称: 警戒值: 监观类型:	test 255 ⑨ 接口	(1~255),缺省值:255 ⑥ HTTP Ping ARP DNS TCP		
★ 河(x)家町五 监测対象 - 名称: 警戒值: 监测类型:	test 255 @ 接口 象	(1~255),缺省值:255 ◎ HTTP Ping ARP DNS TCP		
▲ 观幻家町五 监测対象 一 名称: 警戒值: 监测类型: 添加接口对 接口:	test 255 ④ 接口 象	(1~255),缺省值:255 ⑦ HTTP Ping ARP DNS TCP		
血测(x)家町五 监则对象 - 名称: 警戒值: 监测类型: 添加接口对 接口: 权值:	test 255 ④ 接口 象 	(1~255),缺省值:255 ◎ HTTP Ping ARP DNS TCP ▼ (1~255),缺省值:255		
★ 期内家町五 监別対象 一 名称: 警戒値: 监別类型: 添加接口対接口: 按口: 収値:	test 255 ④ 接口 象 ///////////////////////////////////	(1~255),缺省值:255 ◎ HTTP Ping ARP DNS TCP ▼ (1~255),缺省值:255		
▲ 测兴 家町五 监测对象 - 名称: 警戒值: 监测类型: 添加接口对 接口: 权值:	test 255 ④ 接口 象 	(1~255),缺省值:255 ◎ HTTP Ping ARP DNS TCP ▼ (1~255),缺省值:255		
血吻(x)家町五 监则)対象 - 名称: 警戒値: 监列类型: 添加接口対 接口: 权値:	test 255 ④ 接口 象 	(1~255),缺省值:255 ◎ HTTP Ping ARP DNS TCP ▼ (1~255),缺省值:255		
★ 期内家町五 监测対象 一 名称: 警戒値: 监测类型: 客称: 警戒値: 近初接口対 接口: 权值:	test 255 ④ 接口 象 ///////////////////////////////////	(1~255),缺省值:255 ⑦ HTTP Ping ARP DNS TCP ▼ (1~255),缺省值:255		
★ 期内家町五 当別対象 一 名称: 警戒値: 当別类型: ※加接口对 接口: 权値:	test 255 ④ 接口 象 ///////////////////////////////////	(1~255),缺省值:255 ◎ HTTP Ping ARP DNS TCP ▼ (1~255),缺省值:255		
▲ 別(x)家町五 监测)対象 一 名称: 警戒值: 监测类型: 添加接口对 接口: 权值:	test 255 ④ 接口 象 ///////////////////////////////////	(1~255),缺省值:255 ◎ HTTP Ping ARP DNS TCP (1~255),缺省值:255	确定	取消
血吻內家酯五 监测对象一 名称: 警戒值: 监测类型: 添加接口对 接口: 权值:	test 255 ④ 接口 象 ///////////////////////////////////	(1~255),缺省值:255 ◎ HTTP Ping ARP DNS TCP ▼ (1~255),缺省值:255	确定	取消

 如果选择"HTTP Ping ARP DNS TCP"监测类型,点击『添加』,从下拉菜单中选择需要的 报文类型,然后在<添加/HTTP/Ping/ARP/DNS/TCP>部分添加监测条目。用来监测链路 逻辑状态,可以配置多种形式的探测。

以 PING 为例,如下图配置中,设备没 3 秒发一个 PING 包,连续 3 个包不通,该条目即生效, 设备会优先使用配置的收包接口的管理 IP 为源地址(如没有管理 IP 就用接口的 IP 为源地址)



通过配置的发包接口把 PING 包发出。

	2 👬 mir£			
 监测对象 名称: 警戒值: 监测类型: 添加监测成员 ア 1P ア 1P 	255 ② 接口	(1~255),缺省值:255)HTTP Ping ARP DNS TCP 权值 重试次数 间隔 封	2 褒收报文 发送报文	添加 HTTP Ping ARP DNS TCP
				Ŧ
对象 全球法学 一。他 监测对象配置	ta ∰ αυφ≙		确定	取消
X対象 上別対象配置 监別対象配置 上別対象 名称: 왕戒值: 出別共型: 添加Ping对象 [P/主机・	★書 ▲▲ ■▲ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	(1~255),缺省值:255 ④ HTTP Ping ARP DNS TCF	· 确定	取消

5. 配置接口。在 AP 模式下,配置方式和普通配置一致,直接在接口上进行配置即可,请参阅接



口配置。在 AA 模式下,组 0 和普通配置一致,组 1 需要配置 Virtual Forward 接口。点击接口列表左上角的『新建』按钮 ,弹出接口类型下拉菜单。从下拉菜单中选择并点击 < Virtual Forward 接口 > ,系统弹出 < 接口配置 > 对话框。如下图:

妾口配置						8
常规 属性	高级 RIP			• 11		
名称	ethernet0/0	×.1		(1~4094)		
绑定安全域:	◉ 三层安全域		宝安全域	○ 无绑定		
安全域:	trust	*				
IP配置						
类型:	● 静态IP	○ 自动获取IP	PPPoE			
IP地址:	10.10.10.1					
网络掩码:	30					
□ 启用DNS代理						
高级选项	DHCP	DDNS				
一管理方式	U Ding					
路由		 关闭 	● 白井			
					确定	取消

6. 配置管理 IP。由于备机是不转发流量的,所以需要在组 0 的接口上配置管理 IP,用于设备的管理和进行 TRACK 监测。在<接口配置>对话框,点击『高级选项』按钮,在<管理 IP> 文本框中输入 IP 地址,为接口指定管理 IP。



及选项		8
_管理IP		
IP地址:	10.10.10.2	
— <u>二</u> 级IP——		
IP地址1:	/	
IP地址2:	/	
IP地址3:	/	
IP地址4:	/	
IP地址5:	/	
IP地址6:	/	

提示:管理 IP 可以和接口 IP 在同一网段,也可以是单独的 IP,只需路由可达即可。

- 7. 配置 NAT 规则。在 AP 模式下,配置 NAT 规则的方法和普通配置一致,直接配置即可,请参阅源 NAT 配置。在 AA 模式下,组 0 配置 NAT 和普通配置一致,组 1 配置 NAT 需要选择组1。
- 8. 源 NAT。点击源 NAT 列表中的『新建』按钮, 弹出<新建源 NAT>对话框。在『更多配置』标签页中,选择<HA 组>单选按钮, 指定源 NAT 规则所属的 HA 组。



源NAT配置		8
基本配置	更多配置	
HA组:	O O 1	
NAT日志:	□ 启用	
列表位置:	列表最后 💙	
	位置越前,优先级越高。	
ID:	◎ 自动分配ID	
	◎ 手动分配ID	(1-4096)
		确定则消

 9. 目的 NAT。从页面左侧导航树选择并点击"配置->网络->NAT",进入源 NAT 页面。点击 『目的 NAT』标签,进入目的 NAT 页面。选择<HA 组>单选按钮,指定目的 NAT 规则所 属的 HA 组。



以下条件时			
trust-vr	_		*
0 0 1			
地址条目	×		*
Any			×
地址条目	~		*
		(1~65535)	
		(0~63)字符	
	以下条件时 trust-vr 0 0 1 地址条目 Any 地址条目	以下条件时 trust-vr ● 0 ● 1 地址条目 ▼ Any Any	以下条件时 trust-vr ● 0 ● 1 地址条目 ▼ Any Mny (1~65535) (0~63)字符

10. 配置路由以及策略,确保网络的畅通。配置方法请参阅路由配置和策略配置。



HA									8
HA控制连接接口1:	ethernet0/5		~	接口2:	无		×		
HA数据连接接口:	无		~						
IP地址:	1.1.1.1			/ 30					
HA簇ID:	1		~	节点ID	. 0		¥		
Peer-mode:									
	50		(1-254	4)	抢占时间:	0	<u>^</u>	(0-600秒)	
Hello报文间隔:	1000	÷	(50-10	0000毫秒)	Hello报文警戒值	: 3	÷	(3-255)	
免费ARP包个数:	15	-	(10-20))	监测对象:	无	~		
描述:								(1-31字符)	
								福宁	取谐
								- WINE	42/13
HA								MAL	×ו•
HA HA控制连接接口1:	ethernet0/5		~	接口2:	无		Y	WIAL	
HA HA控制连接接口1: HA数据连接接口:	ethernet0/5 无		¥ ¥	接口2:	无		v	WILL	× × × × × × × × × × × × × × × × × × ×
HA HA控制连接接口 1: HA数据连接接口: IP地址:	ethernet0/5 无 1.1.1.2		~	接口2: / 30	无		•		× × × × × × × × × × × × × × × × × × ×
HA HA控制连接接口1: HA数据连接接口: IP地址: HA簇ID:	ethernet0/5 无 1.1.1.2		¥ ¥	接口2: / <u>30</u> 节点ID	无		•		× × × × × × × × × × × × × × × × × × ×
HA HA控制连接接口1: HA数据连接接口: IP地址: HA簇ID: Peer-mode:	ethernet0/5 无 1.1.1.2 1 — 启用		v v	接口2: / 30 节点ID	无 :: 0		•	09342	
HA HA控制连接接口1: HA数据连接接口: IP地址: HA簇ID: Peer-mode: 组0	ethernet0/5 无 1.1.1.2 1 一 启用		v v	接口2: / 30 节点ID	无 :: 0		•		
HA HA控制连接接口1: HA数据连接接口: IP地址: HA簇ID: Peer-mode: 组0 优先级:	ethernet0/5 无 1.1.1.2 1 。 启用	▲	▼ ▼ ▼ (1-254	接口2: / <u>30</u> 节点ID	无 : 0 抢占时间:	0	▼ ▼	(0-600秒)	
HA HA控制连接接口1: HA数据连接接口: IP地址: HA簇ID: Peer-mode: 	ethernet0/5 无 1.1.1.2 1 。 启用 50 1000	<>> <>>	▼ ▼ (1-254 (50-10	接口2: / <u>30</u> 节点ID 4) 0000毫秒)	无 : 0 抢占时间: Hello报文警戒值	0 : 3	* * * * *	(0-600秒) (3-255)	
HA HA控制连接接口1: HA数据连接接口: IP地址: HA簇ID: Peer-mode: 	ethernet0/5 无 1.1.1.2 1 。 启用 50 1000 15	<><>	▼ ▼ (1-254 (50-10) (10-20)	接口2: / <u>30</u> 节点ID 4) 0000毫秒) 0)	无 : 0 抢占时间: Hello报文警戒值 监测对象:	0 : 3 无	• •	(0-600秒) (3-255)	
HA HA控制连接接口1: HA数据连接接口: IP地址: HA簇ID: Peer-mode: 	ethernet0/5 无 1.1.1.2 1 。 启用 50 1000 15	<>	▼ ▼ (1-254 (50-10 (10-20	接口2: / <u>30</u> 节点ID \$) 0000毫秒) 0)	无 : 0 抢占时间: Hello报文警戒值 监测对象:	0 : 3 无		(0-600秒) (3-255) (1-31字符)	
HA HA控制连接接口1: HA数据连接接口: IP地址: HA簇ID: Peer-mode: 	ethernet0/5 无 1.1.1.2 1 。 启用 50 1000 15		▼ ▼ (1-254 (50-10 (10-20	接口2: / <u>30</u> 节点ID 0000毫秒) 0)	无 : 0 抢占时间: Hello报文警戒值 监测对象:	0 : 3 天		(0-600秒) (3-255) (1-31字符)	



监测对象配置								6
监测对象 名称: 警戒值: 监测类型:	HA-Track 255 ● 接口	 О н	(1~31 (1~25 TTP Pir)字符 5),缺省值:255 ng ARP DNS TCP				
添加监测成员 ● 类型 ● 接口 ● 接口			接口 etherr etherr	net0/0 net0/2		权值 255 255		一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
							确定	取消
HA								8
HA控制连接接口1: HA数据连接接口: IP地址: HA簇ID: Peer-mode:	ethernet0/5 无 1.1.1.1 1 白田	▼ ▼	接口2: / 30 节点ID	无 : 0		¥ ¥		
Peer-mode: 组0 优先级: Hello报文间隔: 免费ARP包个数: 描述:	□ 月月 1000 15 ↓	(1-254) (50-1000 (10-20)	0毫秒)	抢占时间: Hello报文警戒值: 监测对象:	0 3 HA-Track		(0-600秒) (3-255) (1-31字符)	•
							确定	取消