

Hillstone 山石网科 多核安全网关 高级功能配置手册

V 5.0 版本

ᅼ.	链路负载均衡	3
1. 1. 1. 1.	 基于目的路由的流量负载	4 6 7 9
<u> </u>	流量控制 QOS 配置	.10
2.	1 配置 IP QoS	.10
2.	2 配置应用 QoS	.14
2.	3 配置混合 QoS	.16
2.	4 配置 QoS 白名单	.18
Ξ.	NBC 网络行为控制配置	.19
3.	1 URL 过滤(有 URL 许可证)	.20
3.	2 URL 过滤(无 URL 库许可证)	.25
3.	3网页关键字过滤	.28
3.4	4 网络聊天控制	.33
四.	VPN 高级配置	.35
4.	1 基干 USB-KEY 的 SCVPN 配置	.35
4.	2 PNP-VPN	.48
五.	高可靠性 HA 配置	.60

一. 链路负载均衡

当防火墙有多条链路接入,同时需要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时,需要进行负载均衡的配置,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时,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。

配置多链路负载均衡前,先保证接口, snat 和策略都配置正确。

1. 确认接口的地址和掩码都配置正确,其中掩码的位数一定和运行商确认:

	新建 🔹 📝	辑 🗂 🕅	除		e0/0和e0/1作为公网口				
	接口名称	状态	获取类型	IP/撬码	安全场	接入用户/IP数	流入带宽(bps)	流出带宽(bps)	
	ethernet0/0		静态	1.1.1.1/24	untrust	0	0	0	1
	ethernet0/0.1	****	静态	192.168.20.1/74	trust	0	0	0	
	ethernet0/0.2		静态	192.168.30.1724	trust	0	0	0	
V	ethernet0/1		静态	3.3.3.3/24	untrust	0	0	0	
	ethernet0/2		静态	0.0.0/0	l2-trust	1	198	4148	8
	ethernet0/3	<u>4 2 4 4</u>	静态	0.0.0/0	l2-trust	0	0	0	

2. 两条源地址转换, 使内网的流量可以分别 nat 成对应公网出口地址池的地址, 去访问互联网:

JUIEOS TRANSA												
配置	-	源N	源NAT 目的NAT 服务器状态 雪田方田名中立 thereat									
🏠 主页		一個新建 歐編輯 前前前: 常优先级										
网络			ID	源地址(原始)	目的地址(原始)	服务	出接口 / 下—跳虚拟路齿器	转换为	模式	HA组	志	
🔒 网络连按			1	Any	Any		ethernet0/0	出接口IP	动态端口	0	关闭	
			2	Any	Any		ethernet0/1	出接口IP	动态端口	0	关闭	
🔞 NAT												
🕎 路由												
IPSec VPN												

3. 确认流量穿越防火墙时,防火墙**策略允许**(源和目的地址以及服务可以根据 具体情况作相应修改):



1.1 基于目的路由的流量负载

例: e0/1 口接入 10M 电信, e0/2 接入 20M 网通; 实现所有访问公网的流量按
1: 2 的比例分别从 e0/1 口和 e0/2 口转发出去。即当设备总共转发 3 数值的流量时, e0/1 转发 1 数值; e0/2 口转发 2 数值。

Web 页面配置如下:

1. 网络-> 路由-> 新建:



配置	-		anb da 🛛 🕅		. V V	h/minb ch					
🙆 主页	*	HUMAH 深始山 FSP信息 ISP路田 東哈路田 RIP									
网络			状态	IP/撬码	下一跳	下一跳接口	协议	优先权	度量	路由权值	
🎈 网络连接			A	0.0.0/0	1.1.1.2	ethernet0/0	静态	1	0	1 ^	
🔞 NAT			۵	0.0.0/0	3.3.3.1	ethernet0/1	静态	1	0	2	
二 路由			Å	10.88.16.0/24		vswitchif1	直连	0	0	1	
			۵	10.88.16.135/32	-	vswitchif1	主机	0	0		
Pa Insec Abia			۸	20.1.1.0/24		tunnel1	直连	0	0	1	
🍳 SSL VPN			۸	20.1.1.1/32		tunnel1	主机	0	0	1	
👩 Web认证											
🕼 802.1X											
Tique	Ε										
安全		保证有两条默认路由 流里汉 1:2万"难								Z/J 14t	
All himh											

2. 创建一条默认路由权值为2, 即可得到配置如下:

如此即可实现流量从 e0/1 转发和从 e0/2 转发的比是 10: 20 即流量的 1: 2 负载。具体比例可根据出口带宽的大小以及实际使用率确定。

1.2 基于源路由的流量负载

首先要确认流量需要负载的网段比如:192.168.1.1/24, Web 页面新建源路由如下

1. 网络->路由->源路由->新建:

StoneOS		
配置		
🏠 主页		、東略路田 RIP
网络		需要负载均衡的网段
😑 网络连接		
in the 🎯	源路田町:盂	8
🙄 路由	· 面IP· 192 168 1 1	
IPSec VPN		
SSL VPN		
👩 Web认证	下一跳: • 阿夫 • 接口	业处持定八网地址的网关
🕼 802.1X	网关: 1.1.1.2	- CC - C
安全	优先权: 1 (1~255),缺省值:1	
술 策略	路由权值: 1 (1~255),缺省值:1	
💛 攻击防护		填与流重分摊比例
👼 ARP防护	确定取消	
控制		

2. 重复上述操作并将网关改为 3.3.3.1; 路由权值改为 2 (根据需求):

配置	-	méh	nh da	YEab + YEikmak +		Arminh +		实现流量的			
🏠 主页	^	目的	沿出 コムにま	次済出 泉法山谷出	ISP信息 ISP路由	東略路出 R	IP	贝鞃以開	<u> </u>		
网络			利廷	U III/ 描码	和一批	下—跳挨口	执边	优牛权	度田	8 成中和值	
😑 网络连接			1705	192.168.1.0/24	1.1.1.2	ethernet0/0	静态	1	0	1	*
🏟 NAT			۸	192.168.1.0/24	3.3.3.1	ethernet0/1	静态	1	0	2	
🛫 路由											
PSec VPN											
🍳 SSL VPN											
👩 Web认证											

如此即可实现来自 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。

1.3 基于策略路由的流量负载

例子: 需要负载的网段是 192.168.1.1/24, 此网段去往 8.8.8 的 HTTP 流量 从 e0/1 口转发; 去往 8.8.8 的 ICMP 流量从 e0/2 口转发。

Web页面配置如下:

1. 网络->路由->策略路由->新建: 先配置源地址:

策略路由配置				
基本 源地	业 源用户	目的地址 服务		
地址类型:	P地址	◎ 主机名称	◎ IP范围	◎ 地址条目
IP: 网络掩码:	192.168.1.1 24			
■ 类型		成员		添加
添加源地均	μ	_		▲ 一 刑除 一 刑除
			L.	NH/E 41/1

2. 配置目的地址和服务:

第略路由歐置 🛛	範路由配置
基本 源地址 源用户 目的地址 服务	基本源地址源用户目的地址 服务
地址类型: IP地址 三机名称 IP范围 地址条目 	组成员:
IP: 8.8.8.8 网络缩码: 32 类型 成员 发型 成员	FTP Gnutella GOPHER GRE GTPCv1 GTPUv1 GTPV0 HTTP-EX HTTPE 选择服务 適定

StoneOS									系统
配置 -				bhahah I					
🟠 主页 🔄 📩	目的路田 源路	田 (県接口路日	田 ISP信息	ISP路由 東略路田	RIP				
	◆ 新建 👻	≥编辑	🛗 刪除规则 👘 👘	❷ 启用 ❷ 禁用	🏚 移动	節策略绑定	🛗 删除策略		
网络	规则ID	启用	状态	策略路由名称	源地址	目的地址	服务	下一跳	绑定到
🔵 网络连接	1	0	. 	负载均衡	192.168.1.1/	8.8.8.8/32	ICMP	1.1.1.2	trust-vr
🚳 NAT	1	0	. 	负载均衡1	192.168.1.1/	8.8.8.8/32	HTTP	3.3.3.1	untrust
🛒 路由									
IPSec VPN									
SSL VPN		如图配置	即可实现 📂						
🔏 Web认证		117月11日 11万同暇	源/日的吧 条的品裁						
₩ 802.1X			77 87/2 #4						

3. 同样方法再新建一条策略路由,其中的服务选择 ICMP 得到配置如下:

按上述流程配置即可实现 192.168.1.1/24 网段对目的地址是 8.8.8.8 的 http 和 icmp 流量负载。

1.4 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,系统对只匹配到缺省路由的流量 在符合条件的各条链路上进行探测,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。

配置如下图:

StoneOS		
配置 一	 出站负载均衡 入站负载均衡 	按照如图流程来配置
🏠 主页 🦰	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·····	虚拟路由器: trust-vr
🖤 虚拟系统	状态 IF/搐臼 下	こ 下一跳
🧔 NAT	出活就近探测接口	©
── 路由		
IPSec VPN	「「「」」「「「」」「「「」」」「「」」「」」「□」」「□」」「□」」	
SSL VPN		
🥙 Webi 🚈	▼ ethernet0/0	▼ ethernet0/10
802.1X	ethernet0/11 ethernet0/2	ethernet0/3
1 链路负载均衡	ethernet0/4 ethernet0/5	ethernet0/6
安全	ethernet0/7 ethernet0/8	ethernet0/9
运 病毒过滤		
👋 入侵防御		
👼 ARP防护		
控制		确宁 耶治
■ 流量管理		4X/FI

配置动态检测路由的老化时间和对应子网掩码:

							系统管理・	对象用户▼ 工具▼	
- 出	站负载均衡 📃 🔵 🕽	站负载均衡						任务 帮助	
出站就近	探测:出站就近探测接口							就近探测路由设置	
就近探测	就近探测路由: 配置就近路由老化时间 🔶								
下一跳接	D: ALL	▼ 虚拟路由器:	trust-vr 🗸					10 分钟	
状态	IP/掩码	下一跳	下一跳接口	协议	优先权	度量	路由权值	(1~1440),缺省值:10	
							^		
						即罢 前近路由	的墙码 🔶	子网演码:	
							1119610	255.255.255.0	
								保存恢复默认	
								*	

二. 流量控制 QOS 配置

2.1 配置 IP QoS

1. 进入配置界面,配置-控制-流量管理,点击 IP QoS-新建:

StoneOS		
配置		
🏠 主页	Âβ	16
网络		
🔵 网络连接		1
🏟 NAT		● QoS配置
🕎 路由		E 限流対象: ALL Y ALL Y
IPSec VPN		应用QoS / IP QoS
SSL VPN		白名单: 印范围 V 起始印 终止印
👩 Web认证	=	
🕼 802.1X		时间表: 添加
安全		
💰 策略		
🛣 病毒过滤		
🦺 入侵防御		确定 职消
💛 攻击防护	-	
🔒 ARP防护		
控制		
◎ 流量管理		
6 会话限制		

2. 设置 IP QoS 的具体参数:

	IP QoS		•
	基本配置高	级翻:置	
	规则名称:	qos1 (1~31)字符	入规则名称
	限流对象:	接口 🖌 🗸	————选择限流对象,一般选择某个接口
	IP:	IP范围 ▼ 起始IP 终	《止IP 添加
输入IP范围或选择某			冊修余
个地址余日 并点击添加加入列表	ŧ		可选中后删除列表中的条目
中	上行带宽:	毎IP ▼ 预留带宽 最大带宽	时间表 🗸 添加
			冊條余
	下行带宽:	毎₽ ▼ 预留带宽 最大带宽	时间表
			册除
			确定取消

3. 设置具体的限制带宽,以上行为例:



例:要配置 192.168.1.2 至 192.168.1.200 范围内 IP 在 e0/2 每 IP 上下行预 留带宽 200K,最大带宽 1M,配置如下图所示:

IP QoS										0
基本配置高級	吸配置									
规则名称:	qos		(1	~31)‡	符					
限流对象:	接口	*	ethernet0	/2	▼ 月	幅安全	è域为 trust			
IP:	IP范围	~	起始IP			终止	IP		添加	
	192.168.1.2	19	92.168.1.2	200					刪除	
上行带宽:	每IP 💙 预	四世	宽	最大帮	宽		时间表	~	添加	
	每IP: 预留带费	ξ 2	00Kbps 最	大带宽	1000)Kbps			刪除	
下行带宽:	毎IP ∨ 预	留带	宽	最大帮	宽		时间表	~	添加	
	每IP: 预留带宽	IP:预留带宽 200Kbps 最大带宽 1000Kbps						刪除		
								确定	取消	

IP QoS 的高级配置:

点击高级配置选项卡,进入高级配置页面:

IP QoS					8
基本配置	高级配置				
弹性QoS: 最大弹性带宽	上行 🔽 64~1,000, 下行 🔽	启用 000 Kbps Kbps 启用			
最大弹性带宽 —— 细粒度控缩	(: 64~1,000, 制	000 Kbps Kbps			
上行:	<u>添加嵌套应用Qos</u> 规则名称	····································	带宽控制(Kbps	;) 操(it i
					^
					*
	添加嵌套应用Qos	规则			
下行:	规则名称	匹配条件	带宽控制(Kbps) 操(îe
					^
					-
				确定	取消

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

					系统管理▼	对象用户▼ 工具▼
● QoS配置						任务帮助
限流对象: ALL 丶	 ALL 	¥				配置
应用QoS IP Qo	S					接口带宽
白名单: 印范围	▼起始印				开启全局弹性QoS 🚽	全局弹性QoS
utia = .						监控
N110136+		•				应用流量监控
						用户作派里面经
	贛 🅤 刑除 🗌 📀 启用 (∂禁用			🚰 优先	級
第定接口/安全	域 规则名称	状态	匹配条件	带宽控制(Kbps)	细粒度控制	•
ethernet0/1	ddī	后州	Q05标金:23	上行最小带宽:43Kbps		

细粒度控制:可在 IPQoS 的基础上,进行应用 QoS 的嵌套使用,进行更精确的 QoS 控制。

点击"添加嵌套应用 QoS 规则",进入配置页面:

嵌套应用QoS配置				8
	设置规则名	称		
规则名称:		(1~31) 字符		
应用:			~	添加
在下拉菜单中	中选择相应的应用,并滚	添加到菜单		刪除
带宽:	最小带宽 ▼ 1~75	%时间表		添加
设置最小带宽。 宽为该IP相应/ 大带宽为该IP相	或最大带宽,最小带 立用的保证带宽,最 目应应用的最大带宽	可配置时间, 在特定时间,	ē使Qo! 设内生效	
		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。

2.2 配置应用 QoS

1. 点击应用 QoS-新建,进入配置页面:

应用QoS		8
基本配置高	^{吸配置} 设定规则名称	
规则名称:	(1~31)字符	
限流对象:	接口 🗸 🗸 🗸 🗸 🗸 🗸)
匹配条件:	应用 🖌 添加	
洗掉	圣相应的应用并添加	
~	更多	
上行带宽:	最小带宽 ▼ 32~1000000 Kbps 时间表 ▼ 添加	
设	置上行最小保证带 删除	
宽	或最大带宽高级	
下行带宽:	最大带宽 ▼ 32~1000000 Kbps 时间表 ▼ 添加	
设	置下行最大带宽 删除	
	高级	
	确定	取消

例:限制 P2P 软件及 P2P 流媒体在 e0/2 接口上行最大流量为 10M, 如图所示:

应用QoS		8
基本配置	·级配置	
规则名称:	qos (1~31)字符	
限流对象:	接口 💙 ethernet0/2 🍸 所属安全域为trust	
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 ▼	添加
	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
		删除
		高级
	确定	取消

应用 QoS 的细粒度控制:

点击"高级配置"选项卡,进入高级配置:

基本配置	高级配	罟							
加权随机早	期检测:	上行	🔲 启用	基	于IP优先权	~			•
		下行	🔲 启用	基	于IP优先权	~			h
数据包标记 —— 细粒度排	;: 控制 ———	下行	🔲 启用						
	嵌套QoS	类型:	IP QoS	~	添加嵌套IP QoS	规则			
上行 <mark>:</mark>	规则名	称	IP地址		带宽控制(Kbps)		操作		
								-	
								Ŧ	н
	嵌套QoS	类型:	IP QoS	~	添加嵌套IP QoS	规则			
下行:	规则名	称	IP地址		带宽控制(Kbps)		操作		
								-	
								Ŧ	

嵌套IP QoS配置					8
			配置规则名称		
规则名称:			(1~31)	习符	
IP:	IP范围	~	起始IP	终止IP	添加
	配置限制的I	P范	围或地址条目		删除
最大带宽:	32-1,000,000 配置相应应	Kbp 用分	s 时间表 配给当前IP的	▼	添加
					開発
				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。

2.3 配置混合 QoS

HillStone 设备中的 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。

应用QoS			8
基本配置高级	國語		
规则名称:	(1~31)字符		
限流对象:	接口 マ マ		
匹配条件:	应用	~	添加
			删除
			更多
上行带宽:	最小带宽 ▼ 32~1000000 Kbps 时间表	~	添加
			删除
			高级
下行带宽:	最大带宽 ▼ 32~1000000 Kbps 时间表	~	添加
			删除
			高级
		确定	取消

1. 点击应用 QoS-新建, 进入配置页面, 如下图, 点击匹配条件右侧的"更多":

2. 如下图所示,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
1)应用条	目总数不能	超	过 10 条,测	流量控制只	需匹配其中	中一条即	可。
QoS标	έ ·	~	11024				添加
入接口		*					
QoS标	ŝ						删除
DSCP		=					
IP优先相	Q						
CoS							
IP范围							
地址条	∃	Ŧ			确定		取消

2.4 配置 QoS 白名单

以 IP QoS 的白名单为例,在流量管理界面上方,选择相应的限流对象,如下 图所示,根据 IP 及时间表配置相应的白名单即可。

● QoS配置					
限流对象: 接口		ethernet0/2	▶ 所属す	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	

三.NBC 网络行为控制配置

在配置 NBC 功能中的 URL 过滤、bypass 域名以及应用行为控制等于网络域名 有关的功能时,需要现在防火墙上进行防火墙 dns 的配置,并且尽量保证防火墙 使用的 dns 与内部电脑的 dns 一致。

防火墙 DNS 配置方法:

1. 点击界面右侧"网络连接",选择该界面右侧的"dns 列表":

StoneOS										系统管理・	7	対象用户▼ 工具▼
配置 -	- P	网络连接										任务 帮助
🟠 主页	安全	·域-接口视图 🗸										向导
		新建 1.点击网络										网络连接-路由模式
 网络连接 	-	安全域名称	类型	由	拟路由器/交换机	接口数	策略数	防病毒	入侵防御	其它		设备将采用类似路由器的
♥ 虚拟系统		trust	L3	tr	ust-vr	3	2					万式摄入网络。
😝 NAT		untrust	L3	tr	ust-vr	3	5		IPS	应用识别 WAN安全域		网络连接-透明模式
🕎 路由		dmz	L3	tr	ust-vr	0	0				11	设备将采用类似交换机的
IPSec VPN		l2-trust	L2	V	switch1	1	0				E	方式接入网络。
SSL VPN		I2-untrust	L2	v	switch1	0	0			WAN安全域		和黑
🐔 Webiki∓		I2-dmz	L2	V	switch1	0	0					EIG.
I 802 1X		VPNHub	L3	tr	ust-vr	3	2		2.点击DN	s列表 ———		DNS列表
1 8/10/ C2.17		HA	L3	tr	ust-vr	0	0		2.0M EI DIT			DHCP列表
【28 划田街以東以小開		tr2	TAP	tr	ust-vr	0	1		IPS		Ŧ	DDNS列表
安全	14 4	第 1页,总	页数1│▶ ♪	1 🗇					Ŧ	显示12个表项中的 1 -	12	PPPoE列表
📸 策略		新建 🔹 🍃 🚽 🧃	辑 🏾 🍈 删除	搜索接口	P							VLAN
🏂 病毒过滤		接口名称	状态	获取类型	IP/ 摘码	安全域	接入用户/IP数	流入带宽	(bps) 流	出带宽(bps)		成功和中心
👍 入侵防御		bgroup1	Q. Q. Q. Q.	静态	0.0.0/0	NULL	0	0	0			Mathemal Million
🦻 攻击防护		ethernet0/0		静态	122.193.30.109/28	untrust	0	0	0			Virtual-Wire
🔒 ARP防护		ethernet0/1	Q. Q. Q. Q.	静态	200.0.0.1/24	untrust	0	0	0			王中的自己的
		ethernet0/10	94 🔍 94 94	静态	3.3.3.3/24	untrust	0	0	0			监控
控制		ethernet0/11	ୟ ર ય ય	PPPoE	0.0.0/0	trust	0	0	0			接口流量监控
■ 涼里管理		ethernet0/2	લ ૧ લ લ	静态	12.12.12.1/24	trust	0	0	0			安全域流量监控
😪 会话限制	V	ethernet0/3	æ ø ø ø	静态	2.2.2/24	VSYS-1	0	0	0			
▲ URL过滤		ethernet0/4		静态	10.10.10.10/24	VSYS-1	0	0	0			

2. 在弹出的 DNS 列表中点击新建,填入 dns 服务器 ip 地址;

DNS列	表						۲
服务	器和代理	解析配置	缓存 NBT缓存	F			
DNS用	務器						
•	新建	🛗 删除					
	服务器I	Р	虚拟路由器		类型		
	221.22	8.255.1	trust-vr		手工配置		*
	202.10	6.0.20	trust-vr		手工配置		
	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	理	虚拟路由器:	trust-vr	~		。 启用DNS代现	₽
•	新建						
	域名			确定	取消	-	
	*		trust-vr		使用系统配置]	*
							Ŧ
						关闭	
	100.0.0	.1/24	PNH 0		0	0	

3.1 URL 过滤(有 URL 许可证)

1. 登陆设备主界面后,点 URL 过滤,再点新建:

安全		×		
<u> 1</u>	策略			
藏	病毒过滤		A	в
	入侵防御	2		
۲	攻击防护	目 ●新建 🕗	编辑 🍈 删除 丨 📀 启用	⊘禁用 │ 🚅 优先级
ABP	ARP防护	□ 名称	目的安全域	用户
控制				
	流量管理			
ē.	今话限制	1		
-10				
<u> </u>	URL过滤			

2. 进入 URL 过滤规则配置, 名称中填写该规则的名字

点击目的安全域的下拉菜单选择目的安全域,需要注意的是应该选择外网接口 所属安全域:

URL过滤规则配置		1.	.填写规则名称		8
名称:	test		(1~31)字符	2 计	· 音旦从网控
── 当满足以下条件时	j			∠. /±	:息定/FM按 所属安全域
目的安全域:		~		,	
用户:	trust		配罟		
时间表:	untrust		「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		
- 240-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	dmz		H.D.		
── 做如下控制 ───	l2-trust				
URL类别	12-untrust				
◆ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤ ≤	VPNHub				
	tr2			_	
UKL尖列		1		2	
光恵代码					(=)
挂马隐愚					C
钓鱼欺诈					
远程代理					
广告					
台店					Ŧ
列表外的所有URL	🔲 阻止访问		🔲 记录日志		
			确定	取消	

4. 用户配置选择相应的用户,默认是 any,即全部内网用户,如果要修改,则先删除 any 用户:

URL过滤规则配置			8	
名称: 当满足以下条件	test 时	(1~31)	字符 1 .点击霄	2置
用户:	Any		置	
用户配置				8
配置类型: ◎ 源地:	止 ◎用	ļ户		
添加值	11.00			
用户类型: 地 地址簿: Ai	址)神 「Y	• 2.选中该领	条目	添加 3.点击删除
用户		АААЛ	济器	刪除
Any		-	^	

5. 然后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:

用户配置				8
配置类型: 添加值 用户类型: IP地址:	● 源地址.选择 ip IP 192.168.1.2	 ● 用户 2.主机 ip ✓ ✓<	3.掩码 32 表 示单台主机	ē 4.添加
用户			AAA服务器	刪除
				5.确定
			确定	取消

6. 配置所要阻止的网站,也可以在用户访问该类网站的时候记录日志(可选):

URL过滤规则配置				8
名称: ┌── 当满足以下条件	test मर्ग			
目的安全域:	untrust	~		
用户:	192.168.1.2/32		置置	
时间表:			配置	
URL类别 ●新建	URL关键字类别	1.勾道 应类	选相 :别	2 .记录日 志(可选)
URL类别	- PEL J	访问	🗌 记录日志	
恶意代码				·
挂马隐患				Ξ
钓鱼欺诈				
远程代理				
广告				
合店		-		-
列表外的所有UF	RL: 📃 阻止访问		🔲 记录日志	
			3.,	京击确定
			确定	取消

通过上述配置,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。

自定义 URL 分类:

配置界面右侧的"URL 查询"功能可以用来查询网站属于哪个预定义的URL 类别,如果需要控制的网站不在预定义的URL 类别中,可通过自定义URL 库进行控制,方法如下:

日時 1小时 24小时 30天 配置 一位定义URL库 一位定义URL库 一位定义URL库 日定义URL库 日定义URL库			系统管理	- 对象用户→ 工具
即时 1小时 24小时 30天 配置 一位 一位 一位 一位 一位 一位 日本 ②有数据 一位 一位 一位 日本				任务帮
没有数据 ・ <th></th> <th>民旧寸</th> <th>1小时 24小时 30</th> <th>天面贵</th>		民旧寸	1小时 24小时 30	天面贵
没有数据 自定义URL库 没有数据 URL查询 文有数据 当該 C D E URL监控 URL出控 URL出控 URL当時 URL当時 社马隐患 ▲				预定义URL库
没有数据 URL查询 没有数据 URL查询 C D E URL描控 URL直流 URL直流 H间表 URL类别 挂马隐患 ▲				自定义URL库
没有数据 Bypass域名 Bypass域名 Bypass域名 Bypass域名 Bypassigta Bypassigta Bypassigta Bypassigta Bypassigta				URL <u>查</u> 询
没有数据 页面提示 Bypass域名 免出控用户 监控 C D E 时间表 URL类别 挂马隐患				关键字类别
WTF\$\$X\$34 Bypassik名 C D E URL监控 URLL型 URL型 推扫隐患 ▲	没方粉据			页面提示
C D E 时间表 URL类别 关键字类别 挂马隐患 ▲				Bypassi或名 会收检用户
<				光 血栓用尸
C D E URL监控 財间表 URL类别 关键字类别 挂马隐患 (日本)				监控
C D E URL日志 时间表 URL类别 关键字类别 挂马隐患 ▲				URL监控
时间表 URL类别 关键字类别 挂马隐患 ▲	c	D	E	URL日志
时间表 URL类别 关键字类别 挂马隐患 ▲				
时间表 URL类别 关键字类别 挂马隐患 ▲				
挂当隐患	时间表	URL类别	关键字类别	
		挂马隐患		

1. 点击页面右侧的"自定义 URL 库":

2. 在弹出的自定义页面中点击"新建",输入自定义的 URL 类别名称和需要过 滤的域名,点击添加后确定:

URL类别		8
	[义类别名称	
URL http:// www.sina.com.cn	(1~255)字符	添加
🔲 URL		
www.baidu.com	▶ 输入需要过滤的域名	
		-
	确定	取消

3. 在配置 URL 过滤时找到自定义的类别,选择控制动作:

目的安全域:	untrust	×		
田白:	Any		雨」栗	
	Ally		間面	
时间表:			配置	
URL类别	URL关键字类	别		
●新建	▶编辑			
URL类别		🗖 阻止访问	🔲 记录日志	
- 単火/日				
艺术				
教育				
非盈利组织				
儿童				(2)
ABC				+
2		12425		

3.2 URL 过滤 (无 URL 库许可证)

1. 选择应用行为控制,点击新建:



2. 进入应用行为控制规则配置,名称中填写该规则的名字,点击目的安全域的下拉菜单选择目的安全域,需要注意的是应该选择外网接口所属安全域:

应用行为控制规则配置		1.填写规则名称	8
名称:	test	(1~31)字符	2.注意是外网接
──当满足以下条件时	<u> </u>		口所属安全域
目的安全域:		*	
用户:	trust	配置	
时间表:	untrust	西2罟	
# 31-34% ·	dmz	HUL	
──做如下控制 ───	l2-trust		
FTP控制	l2-untrust		=
	l2-dmz		> T +n
GEI I Ifi制/	VPNHub	1 比來口志 👗	添加
类型	tr2	日志	编辑
		<u>^</u>	nnin

3. 用户配置选择相应的用户,默认是 any,即全部内网用户,如果要修改,则先删除 any 用户:

了编辑	应用行为控制规	四間置				8	
	名称:	tes	t		(1~31)字符		
	当满足以1 目的安全域:	「条件时 unt An	trust y	1	西晋	1.点击配置	
用户曹	配置						8
配置	类型: 💿 源:	地址	C	角户			
	添加值 户类型:	地址簿	v				
地	址簿:	Any		_	2.选中该条目	添加	3.点击删除
	用户 Any			1	AAA服务器 -		

4. 然后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:

用户配置	8
配置类型: ● 原地选择 ip ● 用户 添加值 用户类型: IP ・ 2.主材 IP地址: 192.168.1.2 /	3.掩码 32 表 几 ip 示单台主机 4.添加 32 添加
用户	AAA服务器 删除
	5.确定
	确定取消

5. 点击 HTTP 控制:

一做如下控制一					
FTP控制					-
GET ¥ 请	输入文件名	阻止	▶ 记录日志	~	添加
类型	文件/用户	动作	日志		编辑
				11	删除
	点击			Ŧ	
HTTP控制					+
	2				-

6. 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候记录日志(可选):

做如下控制 FTP控制 HTTP控制	1.填写域 名或者 ip	2.选择	译阻止	3.记录日 志(可选)	4.点击 添加
GET ¥ *.bai	du.com V	阻止	2 记录日志	→ → 添加	
类型	域名	动作	日志		₿ }
HTTP阻止下载				5.点击 确定	÷
			确注	定即	消

通过上述配置,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。

3.3 网页关键字过滤

1. 登陆设备主界面后,选择网页关键字,点击新建:



2. 进入网页关键字规则配置,名称中填写该规则的名字,点击目的安全域的下拉菜单选择目的安全域,需要注意的是应该选择外网接口所属安全域:

网页关键字规则配置		1.填写规则	则名称			8
名称: ──当满足以下条件时 目的安全域:	test 🚽	v	(1~3	31)字符	2. 注意 口所属	是外网接 属安全域
用户: 时间表:	trust untrust dmz			配置 配置		
做如下控制 ● 新建 关键字类别	I2-trust I2-untrust I2-dmz VPNHub test test1 VPN		 记:	录日志		
关键字控制范围:	所有网站					•
			确定		取消	

3. 用户配置选择相应的用户,默认是 any,即全部内网用户,如果要修改,则先删除 any 用户:

	网页关键字规则配置				
	名称:	test	(1~31)字符		
	──当满足以下条件的 目的安全域:	untrust 🗸		1.点击配置	
	用户:	Any	配置		
用户	配置			8	
配置	昆类型: ◎ 源地址	◎ 用户			
	添加值				
用	月户类型: 地址	簿 🔽	2.进由达夕日		2 占去删除
地	班演: Any	¥	2. 远中该余日	添加	3. 点山咖酥
	用户		AAA服务器	刪除	
	Any		-	^	

4. 然后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:

用户配置		8	
配置类型: 添加值一 用户类型: IP地址:	 ● 源地址 1.选择 ip ● 用户 2.主机 ip 192.168.1.2 / 32 	3.掩码 32 表 示单台主机 4.7 添加	忝加
用户		AAA服务器 删除	
		5.确定	
		确定取消	

5. 点击新建:	新建		
做如下控制	同论提		
□ 利建 并建立本别	■ 88 止访问	□ 记录日主	
Alle 1 XAI	- 1117 491-3		-
			Ŧ
关键字控制范围:	<u>所有网站</u>		
		确定职	肖

6. 填写关键字类别名称,然后点击新建:

如果关键字1信任值*匹配次数+.....+关键字n信任值*匹配次数>=100,则触发 相应的控制动作

关键字类别配	置	1.名称		8
类别名称:	www.	(1~31)字符		
● ● 新建 ○) 关 i	2 Ⅲ 删除 建字 2.新建	类型	信任值	
新建关键	字列表,点击添	四		
关键字类别配	王 山	1.关键字名称	3.匹配规则	8
类别名称 <mark>:</mark>	www		7/	
关键字:	赌博	(1~31)字符 完全	匹配 💙	2. 添加
信任值:	100	(1~100) ?		
如果关键字1 相应的控制运	∟信任值 [*] 匹配次数+ b作	⊦关键字□信任值*匹配次数>=100	,则触发 添加	取消

7. 点击确定,选择相应的控制动作:

网页关键字规则配置		8
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 ● 新建 关键字类别 www	 □ 注:打勾 □ □ □ □ □ 	2.记录日 志(可选)
关键字控制范围:	所有网站	3.确定
		确定取消

通过上述配置,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。

Baypass 域名

如果在设备上需要剔除某些不进行控制的网站,即配置白名单功能,可以在 bypass域名中进行设置,设置 Bypass 域名后,系统将无条件允许用户对Bypass 域名的访问,不受网络行为控制功能的控制。



注意:

- 1. 系统对 Bypass 域名采用精确匹配。
- 2. Bypass 域名对整个系统生效。

3.4 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。

以最常见的 QQ 控制为例, 配置方法如下:

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	手动刷新	*		
🖞 ÈÌ	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:	11035331000 DEMO2 SG-6000-G315 Dec/5/2012 W Standalone	22019 0 /ed 15:11:08 编辑 编辑	软件版本: 病毒特征库: IPS特征库: URL <u>库:</u> 应用特征库:	Version 5.0 SG60 <u>2.0.121126</u> 2012 <u>1.0.180</u> 2012-11- <u>1.0.14 2011-11-2</u> <u>3.0.121130</u> (Profe	00M-5.0R2.bin 2012/10/ 1126 22:50:19 16 12:00:29 9 17:00:22 ession) 2012-11-30 09:2	16 14:20:31 <u>升级</u> <u>升级</u> 升级 升级 升级	
91 9 66 18	IPSec VPN SSL VPN Web认证 802.1X 試路负载均衡	 流量监控 整机流量 			确计	↓应用特征库是否为量	最新版本	
安全 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	策略 病毒过速 入侵防御 攻击防护 ARP防护	z - Y - X -			没有数	8		
控制	流量管理	00:00	0 00:	15	00:30	00:45	01:00	01:15

2. 打开内外安全域的应用识别功能,点击"网络连接",双击相应的安全域,打 开"高级属性"中的"应用识别":

StoneOS									
配置 -		网络连接							
企 主页	安全	≥域-接口视图	~						
网络		「新建」 🦻 🦻 🥼	辑 🗂	删除					
 网络连接 		安全博名称		光刑	▶□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	接口劫	治略劫	Ric病毒	λGR
114 庄拟 玄结		trust		13	trust-vr	3	1	173771*9	7 (131)7
		untrust	_	L3	trust-vr	3	1		IPS
- 98.0									
		dmz		L3	trust-vr	0	0		
		12-trust		L2	vswitch1	2	0		
SSL VPN		12-untrust		L2	VSWITCHI	0	U		
Ø Web认证		VPNHub		安全域配置					8
🕷 802.1X		HA							
└〓 链路负载均衡		tr2		基本设置					
安全		(筐 1 页, 5	百数1	安全域名称:	untrust				
- A-L 				类型:	○ 二层安全域	◎ 三层安全域			
		新建 * / #	14月						
· 加普拉派		接口名称	状态	虚拟路田器:	trust-vr	Y			
·····································		bgroup1	<u>,</u>	接口选择:	可绑定接口	已绑定接			
♥ 攻击防护		ethernet0/0	6.0		bgroup1	ethernet	0/0		
🚥 ARP防护		ethernet0/1	9		ethernet0/11	ethernet	0/1		
控制		ethernet0/10	· 🛠 🍳		ethernet0/2	ethernet	0/10		
		ethernet0/11	9 <u>4</u> 9		ethernet0/3	+			
(二) 小王四年		ethernet0/2	· *		ethernet0/5				
		ethernet0/3	*		tuppol1	-			
		ethernet0/4	%		从城中移除接口将删除	接口的IP翻罟。			
◎ 四贝夫羅字		ethernet0/5	*	宣祝届州	10 (AM 1 12 PAILSE - 13 00 PAI	OSCIENCE DE LA COMPANY			
Web外发信息		ethernet0/6	*	合田 27 回。					
□ 邮件过滤		ethernetu//	*	应用识别。	☑ 启用				
🔄 网络聊天		ethernet0/8	Q. Q	WAN安全域:	☑ 启用				
📴 应用行为控制		ethernet0/9	Q. Q	NBT缓存:	启用				
		tunnel1	0.0						
		tunnel10	0.0						
		tunnel2	0.0					-	
		tunnel7	0.0					确定	取消
		1	0.0	a a 22 +-	0.0.0.0/0	NUL IL I	0	0	

3. 点击左侧"控制""网络聊天",新建规则:

	配置 -							
🙆 主团	ĩ	新建	🤰 编辑 🛛 🍈 删除 🗌 🕥 启	用 🖉禁用 🕌	• 优先级			
网络		名称						
	网络连接			Any				^
V	虚拟系统							
6	NAT	网络聊天规则置	13.11.11.11.11.11.11.11.11.11.11.11.11.1				8	
-	路由							
98	IPSec VPN	名称:	QQ		— 规则名称			
۹.	SSL VPN	当满足以"	下条件时		日約中人	. let		
6	Web认证	目的安全域	untrust	× •	- 日的女王	198		
18	802.1X	用户:	Any		配置 用户	ip		
E	链路负载均衡	时间表:			配置			
安全		46407100	+.I					
	策略	100.201127			需要控制的	账号		
藏	病毒过滤	MSN	QQ 雅虎通		6			
	入侵防御	账号:				添加		
0	攻击防护	账号	回阻止何	用	记录日志			
a	ARP防护	123456	5	V	-			
控制						控制行为		
	流重管理							
6	会话限制							
i ka	URL过滤					-		
TR	网页关键字	列表外的所 同 阻止使	T有QQ账号: 用		列表外其他账	(号行为		
9	Web外发信息							
	邮件过滤							
<u> </u>	网络聊天					TAC HINS	ж. П	
	应用行为控制					NRAE 4X4		

4. 如果想要阻止所有的 qq 账号都无法登录,则可以直接配置"列表外的所有 qq 账号阻止使用"或者直接通过防火墙的策略进行 qq 应用的阻止。

四. VPN 高级配置

4.1 基于 USB-KEY 的 SCVPN 配置

此处介绍的是基于 USB-KEY 的 SSL VPN 配置, 普通 SSL VPN 配置请参考 "Hillstone 基础配置手册"或者直接按照配置向导配置。

一. 创建 SSL VPN 信任域

1. 点击界面右上角"对象用户"—"PKI":

			🐴 🕶 🗟 👻 🖾	页面(P)	▼ 安全	:(S) ▼ T且(O) ▼ @ ▼	>>
手a	加利新	~		系统管理	 ◆ 	对象用户▼ 工具▼ 地址簿	Ø
<u>扁蜇</u> <u>扁蜇</u> <u>扁蜇</u>	软件版本: 病毒特征库: IPS特征库: URL库: 应用特征库:		Version 5.0 SG6000M-5.0R2.bin 2012/10/16 14:20:31 2.0.121109 20121109 22:50:18 1.0.179 2012-11-01 13:54:50 1.0.14 2011-11-29 17:00:22 3.0.121102 (Profession) 2012-11-02 09:42	 升级 升级 升级 升级 升级 升级 		服务簿 时间表 本地用户 LDAP用户 Active Directory用户 用户绑定	
				详情	24.	角色 角色组合 AAA服务器	
	没有数据				24 24 04 在线F	PKI 监测对象	

2. 选择"信任域",点击"新建":

PKI管理	1.创建信	任城					8
密钥	信任域 管理						
•	新建 🔰 📩 📊 👘 🛙 🕰 点击	新建					
	名称	密钥标签	证书获取方法	CA证书	本地证书	CRL	
	caca	Default-Key	手动输入	是	否	否	~
	hillstonetac	Default-Key	手动输入	是	是	否	
	network_manager_ca		手动输入	是	否	否	
	trust_domain_ssl_proxy	Default-Key	自签名证书	是	是	否	
	trust_domain_default	Default-Key	自签名证书	是	是	否	
14 4	第 1 页,总页数1 ▶ ▶ '	\$			ļ	显示表项 1 - 5 总数	数为 5

PKI配置		8
——基本 ——————————————————————————————————		▲ 1.输入信任域名称
信任域:	test	(1~31)字符
证书获取方法:	◎ 手动輸入 🚽 🚽	——— 2.选择手动输入
	◎ 自签名证书	
		3.点击下一步
	取消 应用	于一步

3. 输入信任域名称,选择"手动输入":

4. 导入需要使用的 CA 证书:

PKI管理						
密钥	信 PKI配置				8	
 新建 名和 	CA证书		1.选择本地CA证 书	2.点击导	¢ک ۱	
cac hill net tru	aca 信任域: illstor 导入CA证书: etwor ust_c ust_c		test 浏览	导入		
1	⊘ 选择要加载的文件			協売(A)工業	×	
		-x-1=		授亲 CA业力		
	1 组织 ▼ 新建文件	夹				
		*	名称	修改日期	类型	
	(清)库		illstone-root.cer	2011/1/14 11:43	安全证书	
	- 视频		hillstone-ukey.pfx	2011/1/14 11:41	Personal Inf	
	■ 图片		🗐 USB-Key密码和PIN码.docx	2011/1/11 14:49	Microsoft O	
	📄 文档		📄 保护口令hillstone默认PIN码为1111.txt	2011/1/11 12:25	文本文档	
	📄 迅雷下载		📄 新建 文本文档.txt	2011/8/19 17:12	文本文档	
	→ 音乐	=				
	🜏 家庭组					
	🖳 计算机					
◎●●●第	🏭 本地磁盘 (C:)					
vitchir2	🔊 本地磁盘 (D:)					
	🔮 CD 驱动器 (F:)	-	٠		۴	

5. 导入成功后可看到 CA 证书相关信息:

PKI配置		•
基本		
信任域:	test	
CA证书		
主题: 颁发者: 序列号: 指纹(SHA-1): 有效期:	/DC=com/DC=zlzhang/CN=hillstone /DC=com/DC=zlzhang/CN=hillstone 20:eb:bd:e9:be:bf:c0:8a:41:40:28:40:df:16:79:ef 8D:51:0A:38:2F:7C:C3:D9:9B:4E:0F:80:74:F5:01:0C:CC:B3:41:9B 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. 选择相应的"密钥对",其他信息可选填:

PKI配置		0
基本		
信任域: 密钥对:	Default-Key	选择相应的密钥对
 主题		
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
取消	上一步 应用	申请下一步

7. 根据需求填写 CRL; 如无,则直接"确认":

PKI配置	6
CRL(证书吊销列表)	
检查:	不检查
自动刷新:	每小时
URL1:	http:// ¥ (1~248)字符
URL2:	http:// v (1~248)字符
URL3:	http:// v (1~248)字符
取消	上一步 应用 获得CRL 确认

- 二. 配置 SSL VPN
- 1. WEB 界面登陆防火墙后,点击"配置","网络","SSL VPN":

StoneOS				
配置		SSL VPN		
🏠 主页	^	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	🍈 删除	
网络		□ 名称	用户数	接口
💿 网络连接				
🧔 NAT				
翠 路由				
IPSec VPN				
SSL VPN				
🥭 Web认证				
₩ 802.1X				
安全				
💰 策略	≡			
💛 攻击防护		名称	类型	登录时间
💩 ARP防护				

2. 新建 SSL VPN 名称,点击下一步:

SSL VPN配置	©
欢迎页	欢迎使用SSL VPN配置向导
接入用户 接入接口/隧道接口	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。
策略/隧道路由配置	SSL VPN名称: SSL VPN (1~31)字符
	典型应用场景
	SCVPN Client
	高級配置 上一步 下一步 取消

3. 新建拨入用户,添加 AAA 服务器, AAA 服务器中需要创建登陆 SSL VPN 的用户名和密码:

SSL VPN配置	0
SSL VPN配置	送择用于用户认证的AAA服务器 请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。 AAA服务器: local ▲ AA服务器: local

4. 接入接口选择,配置隧道接口和地址池,隧道接口地址和地址池须在同一 网段,且地址池地址段中不能包含隧道接口地址:

SSL VPN配置	C
欢迎页 接入用户 接入接口/隧道接口 策略/隧道路由配置	接入接口 出接口1: ethernet0/0 ▼ 出接口2: 元 ▼ 服务端口: 4433 (1~65535) VPN服务TCP端口。 窗户端访问VPN服务器的外网接口。一般配置一个出接口即可,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: tunnel1 電溫 所属安全域: VPNHub IP地址: 10.1.1.1 网络摘码: 255.255.255.0 地址池: pool1
	起始IP: 10.1.1.2 终止IP: 10.1.1.254 网络撞码: 255.255.255.0

接口配置		•
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:	VPNHub 👻	
IP配置		
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	
🔲 Telnet 🔲 SS	SH Ping HTTP HTTPS SNMP	
隧道绑定配置		7
隧道类型:	IPSec VPN	
VPN名称:	~	
网关:		-
	确定现	消

地址池配置				8
基本配置 IP用户	绑定 IP角色绑定			
地址池名称:	pool1 (1~31)字符		Â
起始IP:	10.1.1.2			
终止IP:	10.1.1.254			
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

5. 配置策略和隧道路由,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:

SSL VPN配置						(
欢迎页 接入用户								
接入接口/隧道接口	源安全域	目的安全域	地址	服务	时间表	行为		
策略/隧道路由配置	VPNHub	Any	Any-Any	Any	Any	允许		
	- 隧道路由 IP:	网络掩码:	度重值:					
	192.168.20.0	255.255.25	5.0 1	(1~999	9)	添加		
	IP IP		网络掩码		度里值	刪除		
	192.168.20	0.0	255.255.255.0		1	^		
			<u>ā</u> .	2 新)平 上	ш. (=	reft Brask		

6. 高级配置 (可选),参数配置保持默认即可:

SSL VPN配置	0
 	安全套件 SSL版本: ● 任意 ● SSLv3 ● TLSv1 信任域: trust_domain_defa ▼ 加密算法: 3DES ▼ Hash算法: SHA-1 ▼ 压缩算法: ● 无 ● Deflate
主机检测/绑定 短信口令认证 最优路径检测	客户端连接 空闲时间: 30 (15~1500)分钟 允许同名登录: ☑ 启用 登录数: 0 (0~99999999), 0:任意
	高級参数 防重放: ◎ 32 ● 64 ◎ 128 ◎ 256 ◎ 512 DF位: ◎ 设置 ● 拷贝 ◎ 清除 数据端口(UDP): 4433 (1~65535)

7. 启用 USB Key 证书认证,选择客户端证书认证的方法,包括"用户名/密码+USB Key"和"只用 USB Key"两种,添加之前新建的信任域:

欢迎页	客户端配置						
接入用户 接入接口/隧道接口 策略/隧道路由配置	重定向URL: 英文标题: 中文标题: 客白崎江共订证		(1~255)字 (1~31)字符 (1~63)字符	7 9 F			
多数1350 客户端/USB Key	USB KEY证书认证:	☑ 启用	● 用户名/密码 +	USB Key	0 R	用USB	Key
主机检测/绑定 短信口令认证	USB KEY下载网址: 客户端信任域:			- 7			
最优路径检测	富任城:	test	▼ 主题名字	2检查:	🗐 倉用		添加
	□ 信任域 □ test		主题名5 <i>②</i>	2检查		*	

- 三. 制作 USB-KEY
- 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:

	3 批量初始化工具	
	┌初始化参数	
	标签:	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
	└状态	
	Hillstone UKey HID C	·格式化成功.
1	,	,
L		

2. 导入认证证书,打开"Hillstone ukey admin管理工具",选择"数字证书","导入证书",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		
设备信息 修改口令 数字证书 设计	置网址	
	*	
	~	
	4	
导入证书	退出	
查看证书	删除密钥容器	

四. 使用 USB-KEY 认证方式登陆

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;

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。并 在弹出的"请输入用户口令"中输入UKey的用户口令(默认为"1111"):

选择数字证书	? 🛛
身份验证 您要查看的网站要求标识。请选择证书。	
名称	
详细信息 (M)) 查看证 确定 [书(y) 取消
请输入用户口令 🛛 🔀	
读卡器 UKey 名字 Hillstone UKey Hillstone	
请输入用户口令 ****	
原口令密码强度:弱	
确定 取消	

浏览器转到登录页面,输入用户名和密码,并点击"登录"。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;

5. 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;

6. 使用 web 界面方式登陆成功后下载并安装 SSL VPN 客户端,选择登陆方式:

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

7. 输入服务器 ip, 端口号, 用户名, 密码以及 pin 码:

@ 登录	×
Hillstone Secure	Connect
最近访问 :	test@61.161.171.138:4433 🔹
服务器:	61.161.171.138
端口:	4433
用户名:	test
密码:	•••••
PIN 码:	••••
	模式 登录 取消

4.2 PnP-VPN

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 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)。

配置 pnp vpn 主要分为3个步骤:

1. 配置用户

2. Server 端配置 IPSec VPN 实例

3. 客户端配置

一. 配置用户

1. WEB 管理页面>>点击右上角的"对象用户">>本地用户:

Sto	neOS						系统管理。	対象用户・ 工具・
	配置 -		(定时) (明新)	手动刷新	2		系统运	行 地址簿
金封	ធ	● 系統信息						● 服务簿
网络		序列号:	1103533100002019	软件版本:	Version 5.0 SG6000M-5.0R2.bin	2012/10/16 14:20:31	升级	时间表
	网络连接	王机名称:	SG-6000	INIX 用带针证库: IDSMATE:	2.0.121109 20121109 22:50:18	おキは)用白和愛家口 4	1110	本地用户
U	虚拟系统	101++==- 系統計圖:	Nov/16/2012 Fri 03:00:50	IPSHTER:	1.0.14 2011-11-29 17:00:22	MARVHL BURN	1140 1143	LDAP用户
	NAT	HAtto:	Standalone	编辑 应用特征库:	3.0.121102 (Profession) 2012-1	11-02 09:42	1145	Active Directory用户
122	新由							用户期定
-	IPSec VPN	● 流量出技					7	68
9	SSL VPN	整机造塑					详细	
8	Web认证	2.5bps -						моды
18	802.1X							AAA服务器
-	自由负载均衡	2.0bps -	1					PKI
安全								监测对象
100	10.65	1.50ps -						Ale in the second second
虚	病毒过进	1.0bps -						nime. 0
- 4	入部防御							EX.M(7-1 0
	攻击防护	0.5bps -					_	APREST-
-	ARP防护							● 京用設否
1281							_ 1	
103	12.00 M 12	11:00	17.00		23:00 0	5.00	1	NAT
5	会话限制	前10应用24小时	(会里	174	前10用户24小时流型		1148	6 8
R	URL过渡							
12	网页关键字							如何使系统运转起来
10	107-0-0100-00-00						3	第1步:网络连桅
	mir D=						j	· 62步:用户描入
0	Lie C	- E						A3也: 安全設置

2. 点击"本地用户"进入用户配置窗口:

本地用户	▼点击新建, 选	择用户		0
● 新建 ・	2 :11# 1 #1	🔹 🛛 🔗 IP/MAC绑定 👘 🗔 🐺	入・ 「「「日毎出・」 「捜索用户	P
本地服务器: local	用户配置			0
∋ □所有用户	基本配置	PnPVPN配置	填写用户名称	户到期日
	名称:	pnp	(1~63)字符	
	密码: 重新输入密码:	•••	(0~31)字符	
	手机号码: 描述:	₊₈₆ 请输入手机号	(0,6~16)字符 (0~127)字符	据自身需求制定
	IKE标识: IKE标识: 账户到期日:	◎ None)ASN1DN (1~255)字符	
	如果启用了短信	认证切能,想信认证码将友送到用,	P设立的电话号码 这个地方必须 IKE标识, IK	预选择FQDN,并且填写 B标识自己指定
			确定即消	
	14	▲ 第 1页,总页数1 ▶	M 📚	显示7个表项中的 1 - 7

3. 按照上图配置完基础配置之后, 先不要点确定关闭窗口, 选择"PnPVPN 配置"标签:

用户配置		0
基本配置	PnPVPN配置 点击进入PnPVPN	用户配置界面
名称:	pnp	(1~63)字符
密码:	•••	(0~31)字符
重新输入密码:	•••	
手机号码:	+86 请输入手机号	(0,6~16)字符
描述:		(0~127)字符
IKE标识:	○ None	
IKE标识:	pnp	(1~255) 字符
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	3
		确定取消



此时,用于给客户端登陆的用户信息已经设定完成。如果有多个分支客户端可 重复上述步骤。

二. 配置 IPSec VPN 实例(本配置只需在服务器端配置)

1. 配置>>网络>>IPSec VPN>>P1 提议>>新建:

	而聖		IDS	or VDN VDND北岸和主 D1担	D つ 担 (1)				
😭 主灵	асын Į	-	10		▶ 占丰新建四1担议				
F742			[]	名称	验证算法	认证	加密算法	DH组	牛存时间
			-	psk-md5-des-a2	md5	pre-share	des	2	86400
•	网络连接		P	psk-md5-3des-g2	md5	pre-share	3des	2	86400
•	虚拟系统			psk-md5-aes128-g2	md5	pre-share	aes	2	86400
- 👒	NAT		E	psk-md5-aes256-g2	md5	pre-share	aes-256	2	86400
	路由			psk-sha-des-g2	sha	pre-share	des	2	86400
81	IPSec VPN		E	psk-sha-3des-g2	sha	pre-share	3des	2	86400
a	SSL VPN			psk-sha-aes128-g2	sha	pre-share	aes	2	86400
-	Wohilit			psk-sha-aes256-g2	sha	pre-share	aes-256	2	86400
0	WebtAtt	H		rsa-md5-des-g2	md5	rsa-sig	des	2	86400
1-16	802.1X			rsa-md5-3des-g2	md5	rsa-sig	3des	2	86400
EB	链路负载均衡			rsa-md5-aes128-g2	md5	rsa-sig	aes	2	86400
***			E	rsa-md5-aes256-g2	md5	rsa-sig	aes-256	2	86400
安王				rsa-sha-des-g2	sha	rsa-sig	des	2	86400
	策略			rsa-sha-3des-g2	sha	rsa-sig	3des	2	86400
藏	病毒过滤			rsa-sha-aes128-g2	sha	rsa-sig	aes	2	86400
-	入侵防御			rsa-sha-aes256-g2	sha	rsa-sig	aes-256	2	86400
1	攻击防护			dsa-sha-des-g2	sha	dsa-sig	des	2	86400
-	ARPREI			dsa-sha-3des-g2	sha	dsa-sig	3des	2	86400
CLER #	· · · · · · · · · · · · · · · · · · ·			dsa-sha-aes128-g2	sha	dsa-sig	aes	2	86400
控制			E	dsa-sha-aes256-g2	sha	dsa-sig	aes-256	2	86400



2. 配置>>网络>>IPSec VPN>>VPN 对端列表>>新建:

StoneOS						
配置		IPSec VPN VPN对端列表 P1	提议 P2提议			
🏠 主页	-	● 新建 ● 编辑 1 删除				
网络		名称	模式	类型	本地ID	
🔵 网络连接						
💔 虚拟系统						
in the test in the test is the test in the test in the test is the						
፵ 路由						
IPSec VPN						
SSL VPN						
👸 Web认证	=					
₩ 802.1X						
11 链路负载均衡						
安全						
💰 策略						
🛣 病毒过滤						
🦺 入侵防御						
🦁 攻击防护						
📾 ARP防护	4					



3. 配置>>网络>>IPSec VPN>>P2 提议>>新建:

	配置	Ξ	IPS	ec VPN VPN对端列表 P1提议	P2提议						
1 主页	i	-		新建 🦳 🦻 编辑 🍏 册 (19)							
骆				名称	协议	验证算法	加密算法	压缩	PFS组	生存时间	生存大小
	网络连接 虚拟系统 NAT 路由 IPSec VPN SSL VPN Web认证			esp-md5-des-g2	esp	md5	des		2	28800	0
	市地安结			esp-md5-des-g0	esp	md5	des	-	0	28800	0
Y	DE19AREAC			esp-md5-3des-g2	esp	md5	3des	2	2	28800	0
1	NAT			esp-md5-3des-g0	esp	md5	3des	-	0	28800	0
-	路由			esp-md5-aes128-g2	esp	md5	aes	-	2	28800	0
95	IPSec VPN			esp-md5-aes128-g0	esp	md5	aes	2	0	28800	0
-	SSL VPN Web认证 ⊨ 802.1X			esp-md5-aes256-g2	esp	md5	aes-256	5	2	28800	0
4				esp-md5-aes256-g0	esp	md5	aes-256	2	0	28800	0
2				esp-sha-des-g2	esp	sha	des		2	28800	0
140				esp-sha-des-g0	esp	sha	des	÷	0	28800	0
E	链路负载均衡			esp-sha-3des-g2	esp	sha	3des	2	2	28800	0
-~		2		esp-sha-3des-g0	esp	sha	3des	-	0	28800	0
て王				esp-sha-aes128-g2	esp	sha	aes	*	2	28800	0
25	策略			esp-sha-aes128-g0	esp	sha	aes	5	0	28800	0
虛	病毒过滤			esp-sha-aes256-g2	esp	sha	aes-256	5	2	28800	0
da	入侵防御			esp-sha-aes256-g0	esp	sha	aes-256	2	0	28800	0
0	攻击防护										
	ARPREIA										
LINE	CARA MADE										
制											
100	法田管田										

	配置	Ξ		阶段2提议配置		0
) 〕 〕	ī	-	●新建			
3:2		- 19		提议名称:	P2 (1~31)字符	
н-с	网络连接			协议:	● ESP ◎ AH	
	虚拟系统			⊷证 省 注1・	MD5 @ SHA @ SHA-256 @ SHA-384 @ SHA-512 @ NULL	
ă	NAT			应证并以下		
	路由			验证算法2:	● 元 ◎ MD5 ◎ SHA ◎ SHA-256 ◎ SHA-384 ◎ SHA-512 ◎ NULL	
61	IPSec VPN			验证算法3:	● 元 ◎ MD5 ◎ SHA ◎ SHA-256 ◎ SHA-384 ◎ SHA-512 ◎ NULL	
-	SSL VPN			抽应省注1・	● 3DES ● DES ● 4ES ● 4ES-192 ● 4ES-256 ● NULL	
6	WebiliT	=		70421344724-		
1.2	802.1X			加密算法2:	● 无 ◎ 3DES ◎ DES ◎ AES ◎ AES-192 ◎ AES-256 ◎ NULL	
FB	销路负载均衡			加密算法3:	● 元 ◎ 3DES ◎ DES ◎ AES ◎ AES-192 ◎ AES-256 ◎ NULL	
	Man 2 Seat - Sing			hn应答注4·		
全				лации и		
	策略			压缩:	None O Deflate	
藏	病毒过滤			PFS组:	◎ Group1 💿 Group2 ◎ Group5 ◎ No PFS 🔶 此处必须选择	Grou
-	入侵防御			生 左时间 ·	180~86400)独特省值(28800)	
1	攻击防护			土1分时间,	(100-00400)///////////////////////////////	
0.00	ARP防护			启用生存大小:		
制						
-	流量管理				点击确定保存配置	
6	会话限制					
1	URL过滤	-			确定即消	
	些控	+				

Stone	OS								系統管理→ デ
酒	置		IPSec VPN VPNR	端列表 P1提议 P2提议					
🏠 主页		-	● IKE VPN列表						
网络			●新建 →	点击新建					
	络连接		□ 名称	对端	提议		DF位	防重放	
0 虚	拟系统								^
🤞 NA	АТ								
🌚 路	由								
Se IP	Sec VPN								
🧕 SS	SL VPN	E							
👩 W	eb认证								
18 80	02.1X								Ŧ
日 11日	路负载均衡		14 4 第 1页,总页	数1 ▶ ▶ 💝					无表项
安全			● 手工密钥VPN列表						
💰 箣	略		●新建 》编制	ti t					
遼 病	毒过滤		□ 名称	对端		算法	本地SPI	远程SPI	
📥 λi	侵防御	ш							
🤍 攻	击防护								
AR	RP防护								
控制									
👿 流	望管理								
👝 🗛	CORR de l	Ŧ							

4. 配置>>网络>>IPSec VPN>>IPSec VPN>>新建:



5. 点击导入后,在对端名称的下拉列表中选择之前创建的"VPN 对端列表"

后,下面的内容会自动填充,如图所示:



```
6. 点击"步骤二:隧道":
```

Stone	eOS			
● 主页 ● 三〇 ● ○ 四 ● ○ □ ○ ○ □ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	R置		IPSec VPN VPN就講 ● IKE VPN列表 ● 新建 ● 名称	步骤1: 对端 步骤2: 隧道 基本配置 高级配置 名称:
● 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	102.1X 翻答员载均衡 篇略 简考可源 入侵防御 故击防护 (RP防护		 Ⅰ () 第 1页, 总页款 ● 手工密钥VPN列表 ● 新建 ● 新建 ● 常報 	
控制	航里管理 会话限制 JRL过滤 钻控 日志	+	14 4 第 1页, 总页a	单击确定完成创建 ▲ 确定 取消

7. 点击确定完成后, IPSEC VPN 实例已经创建完成, 下面需要将实例绑定到 tunnel 接口, 点击配置>>网络>>网络连接, 在下面的接口列表中点击"新建", 选择"隧道接口":

Sto	neOS												
	配置			网络连接									
🙆 主团	Į	-	安全	域-接口视图 🗸 🗸									
网络	第二中	-		PPPoE接口	fiir	HILS	第三步,	点击;	之后完成接口创建				
THE CONTRACT	网络连接			隧道接口	7	本刊 応収路由哭/交換机		由哭/ 云	按口粉			笛略劫	
0	虚拟系统	-		Virtual Forward接口		L3 trust-vr		3	- 384		1		
l 🍒	NAT			回环接口		L3 trust-vr		3			3		
	路由			集聚接口		12		truct	r.	0			0
98	IPSec VPN			冗余接口		L2		vswitc	h1	0			0
•	SSL VPN			以太子接口		L2		vswitc	h1	0			0
6	Web认证	-		集聚子接口		L2		vswitc	h1	0			0
18	802.1X	=		冗全子接口		L3 trust-vr		1	1		1		
E	链路负载均衡			VSwitch按口		L3		trust-v	r 	0			0
				Wakited 第二	步			trust-v	T	0			1
安全	to to make		-			P P1							
	策略			新建 🔹 🖊 📝 编辑	i in	删除	搜索接口		Q		002200		100 100 00000
加度	病毒过渡			接口名称 ▲	状态		获取类型	IP	/掩码	安全	域	接入	用户/IP数
. 🦉	人侵防御			bgroup1	Q. Q.	8.8	静态	0.0	0.0.0/0	NUL	L	0	
<u> </u>	攻击防护			ethernet0/0		22	静态	12	2.193.30.109/28	unt	rust	0	
ARP	ARP防护			ethernet0/1		**	静态	20	0.0.0.1/24	unt	rust	0	
控制				ethernet0/10		14. 14. G. G.	静心	3.3	3.3.3/24	unt	rust	0	
11.01	法审管理			ethernet0/11			PPP0E	12	12 12 1/24	trus	at a	0	
l õ	今话限制			ethernet0/3		44	静态	0.0	0.0.0/0	NUI	1	0	
~	LIRI itire			ethernet0/4	4.2	4.4	静态	0.0).0.0/0	NUL	L	0	
76	11/2-4-22	-		ethernet0/5	Q. Q.	9.9	静态	0.0	0.0.0/0	NUL	L	0	
	通控	+	14 4	··· ···		13 13 N NI	+*					-	
	日志	+	14 4	用	口刻1	P P1	1						

8. 接口创建完成之后,进入该 tunnel 接口,配置隧道绑定,如图所示在 tunnel 接口配置框中:

割留		含在描				
配置 ● 网络 ● ● 网络连接 ● 皮膚(系统) ● 皮膚(系统) ● 水和 ● 路由 ● IPSec VPN ● SSL VPN		HETA 接口配置 常規 属性 高级 RIP ▼ Telnet ▼ SSH ▼ Ping ▼ 路由 逆向路由: ◎ 倉用 ◎ 隣道総定配書	нттр 📄 нттрs 关闭 💿 自	マ SNMP 約		
 Ø Web认证 \$802.1X 目 链路负载均衡 安全 一 资幣 資 新略 資 新略 		厳道类型: VPN名称: psec PK:	SSL VPN →选 下打 →下打 →不切	≩该选项 2列表中选择之前创建的 真写 ┓┓┓┓→ 点击添加	7隧道名称	25 X THE (hos)
 小侵防御 ジ 攻击防护 品 ARP防护 		W IIII/F VPN名称 回 ipsec	类型 ipsec	网关	E	0
控制				点击确定		
出 注 + 日 ま ・ +	44.4	第一1页,白石粉1 1 月 🔗				

9. 接下来需要配置 server 端的路由和策略:

路由配置:

Sto	oneOS										
	配置		目的	路由							
🙆 È	5	-	•	新建一	新二大 新		VI				
网络		-									
	网络连接			uille I							
V	虚拟系统					目的路由配置				0	
6	NAT										
-	路由					目的地:	192.168.1.0		승규 다리 한다. 소유 분장 가리		
9 8	IPSec VPN	7				子网撤码:	255.255.255.	0	36月29月又不日子电14日		
۹	SSL VPN					T-94					
6	Web认证	-				1,196.	● MA				
18	802.1X	-	宜_				◎ ヨ則系筑虚	以降田器 🔘 具他系	说虚拟暗田蓄		
E	链路负载均衡		35			接口:	tunnel1	→ → 选择	绑定的隧道接口		
安全						网关:			「填写		
1	策略					优先权:	1	(1~255).缺省值:1		
熾	病毒过滤					蛇山 切 值·	1	(1 200			
	入侵防御					[[[]]][]][]][]][]][]][]][]][]][]][]][]]	1	(1~255),缺首值:1		
0	攻击防护										
ABP	ARP防护						ہے جنہ جنہ جارج جارے				
坊街							点击佣正元则		确定 取消		
17.00	法备管理								24		
	小王自建										
10	LIRI 计语										
<u>M</u>	115-400	-									
	開拓	+									

策略配置:

Sto	neOS							
	配置	=	() 策明	8				
🏠 主动	5	-	源安全域	: Any		▼ 目的安全域: Anv ▼		
网络			•	新建		策略配置 第二步 🛽 😵		
	网络连接			ID	状态	基本配置 高級控制 隧道接口所在安全域 内网安全域	服务	特征
0	虚拟系统			1	启用	当满足下列条件时	Any	
	NAT			100	启用	源安全域: 目的安全域:	电驴*	
-	路由			-	èш	Any Y 到 Any Y	迅雷*	
98	IPSec VPN			3	白田	原地址:	SMTP	
0	SSL VPN			10	启用	Any 文 多个 到 Any 文 多个	Any	上结
Ø	Webili					服务簿: Anv		
19	802.1X	=		4	启用		Any	
HE I	铺路色载均衡					原用户:		
	笛二中							
安全	第一少							
	策略	Ц				f为: ● 允许 全部any即可,如果有其他要求可细化配直		
熾	病毒过滤					◎ 拒绝 Web 认证只能工作在trust-vr。		
-	入侵防御					◎ 安全连接 WEB认证 V local V		
(攻击防护							
<u></u>	ARP防护					×		
控制						行为选允许		
17.62	法留管理					点击完成配置		
Č.	今汪限制					▲ 100 100 100 100 100 100 100 100 100 10		
50 (#								
22	UNLOWS	-				NRAE 4X/FI		
	監控	+		Andre .] -	THE NUMBER		
	日志	+	14 4		[D, 思]	2数1 アーアル 🂝		

至此, server 端已经配置完成, 只需要在 cliect 端设备上填写几个简单参数 即可与 server 端建立 IPSec vpn。

三. PnP 客户端配置:

1. 将客户端防火墙接入互联网, 配置外网 ip 以及默认路由;

2. 配置>>网络>>IPSec VPN>>任务>>PnPVPN 客户端:

StoneOS						系统管理-	对象用户• 工具•
配置 -	IPSec VPN VPNzik	· P1提议 P2提议					任务 帮助
🏠 主页	● IKE VPN列表						前导
Eller.	EBE PART	值的社					
	2 名称	对端	提议		DF位	防重油	RE
ditt Eis	E ipsec	ipsec	P2		сору	0	PnPVPN番户端
● NAT 型 路由						古主語 入 Paperの文字 白澤町 間	當校 ISAKMP SA IPSec SA
PSec VPN ・ SSL VPN の Web认证 は 802.1X						Han and A Lancate Mark handler and	¥号用户
11日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	11 4 第 1页, 总页数	1 🤉 🖓 🌼				21.1 2.1 2.2 2.2 2.2 2.2 2.2 2.2 2.2 2.2	为1
安全 新町	 ● 手工密相VPN列表 ● 新建 ● 新建 	fame:					
· 病毒过速	□ 名称	对诸		算法	本地SPI	远程SPI	
▲ 入银防御 ● 攻击防护 ↔ ARP的护]•.
控制 該筆管理 会话限制 通 URL过速 预页关键字							



点击确定后,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。

五. 高可靠性 HA 配置

1. 配置 HA 所需要具备的条件:

本节介绍如何将两台设备配置为HA A/A 冗余模式。在配置之前,确认搭建成HA 典型组网模式的两台安全网关采用完全相同的硬件平台、固件版本,均启用VR及防病毒、IPS功能,安装防病毒、IPS许可证,并且两台设备使用同样的接口连接到网络。

2. HA 的两种模式介绍

AP 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:



AA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:



- 3. HA 的配置方式:
- 1. 点击系统管理中的 HA 按钮, 进入 HA 配置界面:

	_	_		- 0 - X	
✓ 4 ₂	× 🔁 E	ling		م	•
🏠 🕶 🗟	• 🖃 🖶	▼ 页面(P)	▼ 安全(S) ▼	工具(0) ▼ 🔞 ▼	»
	1	系统管理	- 対象用	户∙ 工具・	
		配置备	份还原	0 小时 54 分 51	眇
	_	配置文	:件管理		-
0/16 14:20:31		设备管	浬	CPU	
		日期和	时间	内存	
		许可证		会话	
:20	2	HA		储卡	
		短信口	令认证参数	_	
		SNMP		жh •	
		系统工	具	\$X.	
		版本升	-级	;总数:	Ξ
			0个 🕨		
			24小时IPSI	女击总数:	
			在线用户:	0	
			策略数:	4	
			● 常用配置	1	
		_	接口		
07:33			策略 NAT		
		谨慎	路田		
			10/7/47	7.451-144-49-44	
			— 以11月1使月	% 第21 运转起米	
			第1步:网络 第2步:用户	δ连接 ⊐接入	
			第3步:安全	2 配置 2015日11日11日11日11日11日11日11日11日11日11日11日11日1	
			勇4步: 网络 为控制	欲望管理和用户行	

2. 配置心跳接口,和心跳接口地址, HA 簇 ID 选 1,优先级数值小表示主机,数 值大表示备机,抢占时间只有主机需要配置(0 表示不抢占),配置检测对象来 控制主备的切换,当监测对象生效时,设备自动变成备机:

НА		妾口,可じ	从只配置一个,也可	以配置)	两个做保障		8
HA连接接口1:	ethernet0/4	~	接口2:	ethern	et0/5	~	
IP地址:	1.1.1.1		/ 30		配置心跳	 接口地址,保	证主备地址在同一网段
HA簇ID:	1	~			1		
40			数值低,表示主				
组0 优先级:	50	1	抢占时间:	0	~	(秒)	AP 模式只要配面组0. AA模式需要同时配置 组0和组1
Hello报文间隔:	3000 🗘	(臺秒)	Hello报文警戒值:	3	-	\	
免费ARP包个数:	15 🗘		监测对象:	track1	~] 主机配置,	,0表示不抢占
描述:							
							▶▶用于控制王备切换,生效 ▶ 时设备会自动转换为备
	100		抢占时间:	0	^	(秒)	状态
Hello报文间隔:	1000 🗘	<mark>(</mark> 臺秒)	Hello报文警戒值:	3	\$		
免费ARP包个数:	15		监测对象:	无	~		
描述:							│ ~ AA模式下需要配置 │ 一般组0和组1二个为
							」■ 王一个为备配置和组0 」 相似
							确定取消

3. 配置检测对象

点击对象用户中的监测对象按钮,进入配置界面:

系统管理▼	对象用户▼ 工具▼
	地址簿 服务簿 时间表
其它 应用识别 WAN安全 域	本地用户 LDAP用户 Active Directory用户 用户绑定
WAN安全域	角色 角色组合
	AAA服务器 PKI
示17个表项中的1-:	监测对象
ps)	虚拟路由器

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:

uwkiselu					e
监测对象 — 名称: 警戒值: 监测类型:	test 255 ④ 接口	(1~255),缺省值:255 ⑥ HTTP Ping ARP DNS TCP			
	l	- Ang	dri da:	×±1.	
		按山 ethernet0/0	1X III 255		

	S Super-		
则对家配古			
名称:	test		
警戒值:	255	(1~255),缺省值:255	
监测类型:	() 接口	HTTP Ping ARP DNS TCP	
按口: 权值:	255	_▼(1~255),缺省值:255	
			确定取消

监测链路逻辑状态,可以配置多种形式的探测,这里用 ping 举例,单机添加, Ping,名字自取,如图配置中,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:

监测对象配置 监测对象配置 名称: 警戒值: 监测类型: 添加监测	■:ett (255) ● 接 则成员 类型 IP地址	₩ mir≎ 口 /主… ÿ	(1 ④ HTT	~255),缺省 P Ping ARP	ì值:255 9 DNS TCF				6	3
监测对象 名称: 警戒值: 监测类型: 添加监测	 № 255 ● 接 № №<	口 /主… ^論	(1 ◎ HTT	~255),缺省 P Ping ARP	窅:255 P DNS TCF					1
	则成员 类型 IP地址	/主 端	1 权值			,				
				重试次教	间隔:	接收报文	发送报文	添加 HTT Pin ARF DN: TCF	P D	
则对象 							确觉	لا لا الله الله الله الله الله الله ال	¥	8
监测对象配置 监测对针 名称: 警戒值: 监测类型	象 255 : ○ 投	<u></u>	(1	~255),缺省 P Ping ARP	值:255 DNS TCP				8	-
添加Pi IP/主机 权值: 重试次数 发送报文 发送报文 接收报文	ng对象 : : : : : : : : : : : : : : : : : : :	 255 3 3	• •	(1~255) (1~255) (1~255)).缺省值:2).缺省值:3)秒,缺省值	55				
							确定	取消		

4. 配置接口

在 AP 模式下, 配置方式和普通上网一致, 直接在接口上进行配置即可。

在 AA 模式下, 组 0 正常配置, 组 1 需要配置 VF 接口, 如下:



接口配置
常规 属性 高级 RIP
名称 ethernet0/0 ▼ :1 -(1~1) 填1 绑定安全域: Image: Compared by the second by the
安全域: trust v IP配置
只要: ● 即恐吓 ● 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…
管理方式 「Telnet III SSH IIII Ping IIII HTTP IIII HTTPS IIII SNMP
路由 逆向路由: ◎ 启用 ◎ 关闭 ◎ 自动
确定取消

5. 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,配置如下:

常规 属性	E 高级 F	RIP			
名称:	ethernet	0/9			
绑定安全域:	 三层安: 	全域 💿 二	.层安全域	◎ 无绑定	
安全域:	trust	~			
— IP配置 —					
类型:	● 静态IP	' ◎ 目动狱り	NIP () PPPc	E	
IP地址:					
网络掩码:					
□ 启用DNS	5代理				
高级选项	DHCP	DDNS			
- 管理方式 -					
🔲 Telnet	SSH P	ing 🔲 HTTP	🔲 HTTPS 🔲 S	NMP	
- 路由					
逆向路由:	◎ 启用	◎ 关闭	◎ 自劫		
					确定 取消
日器/交换机		接口数	策略数	防病毒	确定 取消 入侵防1
田蕃/交换机 口配置		接口数	策略数	防病毒	确定 取消 入侵防闭
田器/交换机 口配置 常规 国	生 高级 1	接口数 RIP	策昭数	防病毒	确定 取消 入侵防1
田器/交換机 口配置 常規 名称:	生 高级 F ethernet	接口数 RIP 0/3	策昭数	防病毒	确定 取消 入侵防部 を
田蓋/交換机 口配置 常規 国 名称: 绑定安全塔	性 高级 fi ethernet	接口数 RIP 0/3	策昭数	防病毒	确定 取消 入侵防1 €
田蓉/交换机 口配置 常规 国 名称: 绑定安全球 安全域:	性 高级 F ethernet 高级选项	接口数 RIP 0/3	策曜数	防病毒	确定 取消 入侵防i €
田蓋/交換机 口配置 常規 名称: 绑定安全场: 安全域: 口P面置	性 高级 F ethernet 高级选项 管理IP	接口数 RIP 0/3	策昭数	防病毒	 确定 取消 入侵防
田藩/交換机 口配置 常规 国 名称: 绑定安全场 安全域: IP面置 类型:	性 高级 F ethernet 高级选项 管理IP IP地址:	接口数 RIP 0/3 10.10.10.2	策曜数	防病毒	 确定 取消 入侵防i 2
田藩/交換机 口配置 常規 国 名称: 绑定安全域: 丁P面置一 类型: IP地址:	生 高级 F ethernet 高级选项 FP地址: 二级IP	接口数 RIP 0/3 10.10.10.2	章昭数	防病毒	确定 取消 入侵防 €
田 古 古 古 古 古 大	性 高级 f ethernet 高级选项 管理IP IP地址: 二级IP IP地址1: IP地址1:	接口数 RIP 0/3 10.10.10.2	策昭数	防病毒	确定 取消 入侵防i
田藩/交換机 口配置 常规 名称: 郑定安全域: 子四配置 文型: IP地指海: 四州 网络 摘明 DI	性 高级 F ethernet 高级选项 正规IP IP地址: IP地址1: IP地址2: IP地址2:	接口数 RIP 0/3 10.10.10.2	策曜数	防病毒	确定 取消 入侵防1
田 蓋 / 交換机 口 配置 常規 国 名称: 绑定安全 域: IP電置 类型: IP地址: 网络 摘码: 自用 DI 高級选	生 高级 F ethernet 高级选项 管理IP IP地址: 二级IP IP地址1: IP地址2: IP地址3: IP地址4:	接口数 RIP 0/3 10.10.10.2	章曜数 	防病毒	确定 取消 入侵防 €
田蓉/交換机 口配置 常規 圍 名称: 绑定安全垟 好四配置 类型: IP晒置 IP地址: 网络箍码: 高規助 高級选 管理方式	性 高级 f ethernet 高级选项 管理IP IP地址: 二级IP IP地址1: IP地址2: IP地址3: IP地址4: IP地址5:	接口数 RIP 0/3 10.10.10.2	策略数	() 病毒	确定 取消 入侵防i
田 蓋 / 交換机 口 配置 常規 名称: 第定安全は 第定安全は 正 四間置 安全域: 1P西置 本型: IP地址: 内留置 意 の 道 の で の の の の の の の の の の の の の	生 高级 F ethernet 高级选项 管理IP IP地址: 二级IP IP地址1: IP地址2: IP地址3: IP地址4: IP地址5: IP地址5: IP地址6:	接口数 RIP 0/3 10.10.10.2	章昭数 	防病毒	确定 取消
田 蓋 / 交換机 口 配 置 常規 ■ 名称: 绑定 安全 域: 「P 西 置 ・ 「P 地 址: 四 路 滝 印 団 ・ 「 戸 地 址: 阿 路 滝 月 団 「 高 級 选」 で で 丁 Telnet		接口数 RIP 0/3 10.10.10.2	策 昭 数	防病毒	确定 取消 入侵防i
田 蓋 / 交換机 「口 配置 常規 風 名称: 第定安全は 「 ア型: 「P地址: 内留置 英型: 「P地址: 「 内留置 一 二 の 二 四 一 二 二 一 二 二 一 二 二 一 二 二 一 二 二 二 二 二 二 二 二 二 二 二 二 二	生 高級 F ethernet 高級选项 IP地址: 工級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:	接口数 RIP 0/3 10.10.10.2	策昭数	防病毒	确定 取消

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。

确定取消

6. 配置 NAT

AP 模式下, 配置 NAT 和普通配置一致, 直接配置即可。

AA 模式下,组0配置 NAT 和普通配置一致,直接配置即可,组1配置 NAT 是需要选择组1,如下:

SNAT:

源地址:	地址条目	~	Any		~
目的地址:	地址条目	~	Any		~
出流里:	出接口		Ƴ eth	ernet0/0	~
服务:					~
将地址转换为					
转换为:	● 出接口IP	()指定IP	◎ 不转换	
模式:	动态端口				
Sticky:	🔲 启用				
启用 <mark>sticky</mark> 后,每	再一个源IP产生的所有	有会话	将被映射到同-	— 个固定的IP地址。	

NAI的古			
基本配置	更多配置		
HA组:	© 0 @ 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)	
		72-	Ten 2242

DNAT:

端口映射配置		8
当IP地址址符合	议下条件时	
HA组(可选):	© 0 (0 1	
目的地址:	地址条目 💙 Any	v
服务:	Any	~
——映射 ——————————————————————————————————		
映射到地址:	地址条目 Y Any	¥
		确定 取消

7. 正常配置路由以及策略,确保网络的通畅。