# 网络卫士防火墙系统

# 配置案例

天融信 TOPSEC® 北京市海淀区上地东路1号华控大厦100085 电话:+8610-82776666 传真:+8610-82776677 服务热线:+8610-8008105119 http://www.topsec.com.cn

## 版权声明

本手册中的所有内容及格式的版权属于北京天融信公司(以下简称天融信)所有,未经天融信许可,任何人不得仿制、拷贝、转译或 任意引用。

版权所有 不得翻印© 2009 天融信公司

## 商标声明

本手册中所谈及的产品名称仅做识别之用。手册中涉及的其他公司的注册商标或是版权属各商标注册人所有,恕不逐一列明。

TOPSEC® 天融信公司

信息反馈

http://www.topsec.com.cn

目



削 員	1
文档目的	
读者对象	
约定	1
相关文档	2
技术服务体系	2
配置导入、导出	4
	-
配置 守出	
<i>基本需求</i>	
<u> </u>	
WEBUI	
<i> </i>	
能直安只 WEDUI	0
WEBUI	0
在线升级	6
基大雲或	6
<i>平平而入</i>	
<u> </u>	
WFRIII配置先骤	
注意可能量少 44 ··································	9
	<i>,</i>
动本路由配置	10
动态路由配置	
<b>动态路由配置</b>	<b>10</b>
<b>动态路由配置</b>	
<b>动态路由配置</b>	
<b>动态路由配置</b>	10 
<b>动态路由配置</b>	10 10 10 11 11 11 13
<b>动态路由配置</b>	10 10 10 11 11 11 13 14
<b>动态路由配置</b>	10 10 10 11 11 11 13 14 14
<b>动态路由配置</b>	10 10 10 11 11 11 13 14 14 14 15
<b>动态路由配置</b>	10 10 10 10 11 11 13 14 14 15 15 18
<b>动态路由配置</b>	10 10 10 10 11 11 11 13 14 14 15 15 18
<ul> <li>动态路由配置</li></ul>	10 10 10 11 11 13 14 14 15 15 18 18
<b>动态路由配置</b>	10 10 10 10 11 11 13 13 14 14 14 15 15 15 18 18 18
动态路由配置	10 10 10 10 11 11 11 13 14 14 14 14 15 15 15 18 18 18 19
<ul> <li>动态路由配置</li></ul>	10 10 10 11 11 11 13 14 14 15 15 15 18 18 18 19 19 19 19
动态路由配置	10 10 10 11 11 13 14 14 14 15 15 15 18 18 18 19 22
<ul> <li>动态路由配置</li> <li>OSPF动态路由配置</li> <li>基本需求</li> <li>配置要点</li> <li>WEBUI配置步骤</li> <li>注意事项</li> <li>RIP动态路由配置</li> <li>基本需求</li> <li>配置要点</li> <li>WEBUI配置步骤</li> <li>注意事项</li> <li>策略路由配置</li> <li>基本需求</li> <li>配置要点(需求1)</li> <li>WEBUI配置步骤</li> <li>配置要点(需求2)</li> <li>WEBUI配置步骤</li> </ul>	10 10 10 10 11 11 13 14 14 14 14 15 15 15 18 18 18 19 19 22 22 22
<ul> <li>动态路由配置</li> <li>OSPF动态路由配置</li> <li>基本需求</li> <li>配置要点</li> <li>WEBUI配置步骤</li> <li>注意事项</li> <li>RIP动态路由配置</li> <li>基本需求</li> <li>配置要点</li> <li>練路由配置</li> <li>基本需求</li> <li>配置要点(需求1)</li> <li>WEBUI配置步骤</li> <li>配置要点(需求2)</li> <li>WEBUI配置步骤</li> <li>和電置步骤</li> </ul>	10 10 10 11 11 13 14 14 15 15 15 18 18 18 18 19 19 22 22 22
<ul> <li>动态路由配置</li></ul>	10 10 10 10 11 11 13 14 14 14 14 15 15 15 18 18 18 18 19 19 22 22 22 22 24
<ul> <li>动态路由配置</li></ul>	10 10 10 10 10 11 11 11 11 13 13 14 14 14 14 15 15 15 15 18 18 18 18 19 19 19 22 22 22 22 22 22 24 24
<ul> <li>动态路由配置</li> <li>OSPF动态路由配置</li> <li>基本需求</li> <li>配置要点</li> <li>WEBUI配置步骤</li> <li>注意事项</li> <li>RIP动态路由配置</li> <li>基本需求</li> <li>配置要点</li> <li>第略路由配置</li> <li>基本需求</li> <li>配置要点 (需求1)</li> <li>WEBUI配置步骤</li> <li>配置要点 (需求2)</li> <li>WEBUI配置步骤</li> <li>配置要点 (需求2)</li> <li>WEBUI配置步骤</li> <li>多播</li> <li>基本需求</li> <li>配置要点</li> </ul>	10 10 10 10 11 11 11 11 13 13 14 14 14 15 15 15 18 18 18 18 19 19 22 22 22 22 22 24 24 24

注意事项	
DHCP	
DUCD服久哭	26
DHCI 加力研 <i>基大雲  </i>	
<i>坐平而</i> <b>小</b>	
和且女点 WFRIII	
"LDOT 能且少禄	20
<i>社志争次</i>	29
基本需求	29
<i>亚平而为</i>	30
和五头系。 WFRIII	30
计自动记录多数 注音事项	33
ロンディス	34
基大雲求	34
<i>亚平而为</i>	34
而且又然而置先骤 WFRIIIm置先骤	35
WEDDTR正少禄	37
网络链路	
ADSL配置	
基本需求	
配置要点	
WEBUI 配置步骤	
注意事项	
GRE通道配置	
基本需求	
配置要点	
WEBUI 配置步骤	
注意事项	
PPTP隧道	
基本需求	
配置要点	
WEBUI 配置步骤	
注意事项	
L2TP隧道	
带宠管理	64
<i>基本需求</i>	
<u> </u>	
WEBUI	
汪意事坝	
用户认证	
本地密码认证	
基本需求	
<u>。</u> 配置要点	
WEBUI 配置步骤	
第三方 <b>RADIUS</b> 服务器认证	
基本需求	
<u> </u>	
WEBUI配置步骤	
注意事项	
证书认证	

基本需求	
配置要点	
WEBUI 配置步骤	
注意事项	
报文阻断规则配置	
二层报文过滤	
基本需求	
WEBUI 配置步骤	
注意事项	
三层报文过滤	
基本需求	
<u> </u>	
WEBUI配置步骤	92
注意事项	
地址转换	
甘工业县社会协调业县社会	05
基丁地亚刈家的源地址转换	
<i>基本清米</i>	
<u> </u>	
WebUI	
基于IP地址的目的地址转换	
<i>基本需求</i>	
配置要点	
WebUI 配置步骤	
注意事项	
双向地址转换	
基本需求	
配置要点	
WEBUI配置步骤	
注意事项	
访问控制规则配置	
基本需求	
WebUI配置步骤	
IPS策略配置	
#+霍北	11/
<i>奉平而米</i>	
能直安只	
WLDUI	
<i>社息争</i>	
深度过滤	
HTTP过滤	
基本需求	
配置要点	
WebUI配置步骤	
注意事项	
IPSEC VPN隧道管理	
远程用户本地管理	
基本需求	126
	120

配置要点	
WebUI 配置步骤	
注意事项	
远程用户集中管理	
基本需求	
配置要占	142
Po-エク minimum WebIII 配置 步骤	142
<i>注音重项</i>	
ロボダベー VPN語太隊道(木地配署)	151
VITT的心应定(平地配直)	
至平而入 配罢更占	
<u> </u>	
Web01 <u>即且少</u> 琢 计音車项	
<i>往息争火</i>	
VPN <b>动</b>	
基 <i>半 而 米</i>	
WebUI 配直步線	
<i>汪意事坝</i>	
SSL VPN配置案例	
WEB转发	
基本需求	
配置要点	
防火墙A的配置步骤	
WEBUI配置步骤	
端口转发	
基本需求	
配置要点	
防火墙A的配置步骤	
WEBUI 配置步骤	
全网接入	
基本需求	
配置要点	
防火墙A的配置步骤	
WEBUI 配置步骤	
注意事项	
本地证书认证	
基本需求	
配置要点	
防火墙A的配置步骤	
WEBUI配置步骤	
<u></u> 注意事项	229
第三方证书认证	229
<u> </u>	229
<i>至于而为</i> 配置要占	230
<sup>μ</sup> 旦久加 防水墙Δ的配置先骤	230
WFRIII配告》称	
порот <sub>по</sub> 且少來	
тороз улш <i>其太季 載</i>	239 220
<u>ヱ</u> , , , , , , , , , , , , , , , , , , ,	
<u>即</u> 旦又局	239 120
的八個山則也且少水。 Dadua的配要生哪	
NUUUUSIUEL业业。 WEDUEL型生趣	
WEDUI癿且少琢	

注意事项	
双因子认证	
基本需求	
m冒要点	
防火墙A的配置步骤	
WEBIII配置步骤	245
注意可能量少 媒	259
	209
与IDS联动	
基本需求	260
配置要占	260
記ユ <i>ス</i> 系に WFRIII	261
<i>试音車而</i>	201
江芯芋火	
双机热备	
亚却执久描式	266
· <u> </u>	
<i>坐平而</i> <b>小</b>	
癿且女品	
WEDUI乱直少琢	
<i>社息争坝</i>	
路出按口下的贝软均衡快式	
基本高米	
<u> </u>	
WEBUI 配置步骤	
TRUNK口卜的负载均衡模式	
基本需求	
配置要点	
WEBUI配置步骤	
连接保护模式	
基本需求	
配置要点	
WEBUI配置步骤	
注意事项	
子接口的负载均衡模式	
基本需求	
配置要点	
WEBUI 配置步骤	
链路备份	
基本需求	
配置要点	
WEBUI 配置步骤	
注意事项	
服务器负载均衡	
基本需求	
WEB服务器配置步骤	318
客户端配置步骤	318
H / MHLL	318
₩22017=12.2.9 % 注音事项	374
虚拟系统	
基本需求	326

配置要点	
<i>主机的配置</i>	
WEBUI 配置步骤	
注意事项	
日志分析	
设置日志服务	
基本需求	
配置要点	
WEBUI	
<i>注意事项</i>	
日志报警	
基本需求	
WEBUI 配置步骤	
注意事项	

## 前言

本配置案例手册主要介绍网络卫士防火墙的各种典型配置、使用和管理。通过阅读本 文档,用户可以了解网络卫士防火墙在实际应用环境中的操作和配置方法。

本章内容主要包括:

- 文档目的
- 读者对象
- 约定
- 相关文档
- 技术服务体系

## 文档目的

本文档通过各种典型案例介绍如何配置网络卫士防火墙。通过阅读本文档,用户能够 在实际应用环境中配置网络卫士防火墙,并综合运用安全设备提供的多种安全技术,包括 访问控制、VPN、入侵检测和 QoS 管理等有效地保护用户网络,控制网络的非法访问和 抵御网络攻击,实现高效可靠的安全通信。

## 读者对象

本用户手册适用于具有基本网络知识的系统管理员和网络管理员阅读,通过阅读本文档,他们可以独自完成以下一些工作:

- ▶ 网络卫士防火墙的基本网络配置和系统配置,包括导入、导出配置文件、在线升级、路由配置、多播、DHCP和 PPTP/L2TP 配置以及带宽管理。
- ▶ 网络卫士防火墙的用户管理。
- 防火墙访问控制规则的配置,提供了从二层到七层的访问控制配置方法,包括报 文阻断规则配置、访问控制规则配置以及深度过滤的配置案例。
- ▶ 制定地址转换策略。
- ▶ 虚拟专网的配置。
- ▶ 网络卫士防火墙的高可用性功能,如双机热备、负载均衡等。
- ▶ 网络卫士防火墙的日志管理。

## 约定

本文档遵循以下约定:

命令语法描述采用以下约定:

尖括号 (<>) 表示该命令参数为必选项。

方括号([])表示该命令参数是可选项。

竖线())隔开多个相互独立的备选参数。

加粗大写表示需要用户输入的命令或关键字,例如 help 命令。

斜体表示需要用户提供实际值的参数。

图形界面操作的描述采用以下约定:

""表示按钮。

点击(选择)一个菜单项采用如下约定:

点击(选择) 高级管理 > 特殊对象 > 用户。

为了叙述方便,本文档采用了大量网络拓扑图,图中的图标用于指明天融信安全设备 和通用的网络设备、外设和其他设备,以下图标注释说明了这些图标代表的设备:



文档中出现的提示、警告、说明、示例等,是关于用户在安装和配置网络卫士防火墙 过程中需要特别注意的部分,请用户在明确可能的操作结果后,再进行相关配置。

## 相关文档

《NGFW 管理手册》

《NGFW 安装手册》

《NGFW 命令行手册》

## 技术服务体系

天融信公司对于自身所有安全产品提供远程产品咨询服务,广大用户和合作伙伴可以 通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页 http://www.topsec.com.cn/ 在线技术资料 http://www.topsec.com.cn/support/down.asp 安全解决方案 http://www.topsec.com.cn/solutions/qw.asp 技术支持中心

<u>http://www.topsec.com.cn/support/support.asp</u> 天融信全国安全服务热线

800-810-5119

## 配置导入、导出

系统提供了设备配置维护功能,用户可以方便地进行诸如查看、保存和上传等维护操 作。

系统配置分为两种:保存配置,指的是用户最后一次手工保存在设备上的配置文件, 当系统重新启动后,会自动加载该配置文件。运行配置,指的是设备当前运行状态下的配 置情况,该配置可以随用户的操作而动态调整,但当系统重新启动后,该配置失效。运行 配置不同于保存配置,比如用户添加了某些规则后,该规则立即加入运行配置并生效,但 直至用户手工保存,该规则不会加入到保存配置,重启后该规则便会失效。

在使用安全设备时,可以随时点击页面右上方的"保存配置",将当前的"运行配置" 转换为"保存配置",以避免因电源或其他严重异常造成的当前系统配置丢失。

## 配置导出

#### 基本需求

管理员对远程安全设备的配置文件进行导出。

### 配置要点

- ▶ 下载配置文件
- ▶ 保存配置文件

#### WEBUI 配置步骤

1) 管理员登录远程安全设备,选择 系统管理 > 维护,并点击"配置维护"页签。

<b>配置维护</b>			
配置替换	浏览 替换		
配置下载	加密 🔽 💿 运行配置 🖸 存盘配置 下载		
	各份配置		
	B M HUEL		
复制主配置到备份配置	<b>复制</b> 备份配置最近保存时间 警告:无备份配置文件.		
复制备份配置到主配置			
批量配置处理			
部分导出	地址 □ 服务 □ 时间 □ 阻断策略 □ 安全策略 □ 用户角色 □		
	下载		
部分导入	● 选择文件 浏览		
	C 输入配置		
	上传		

2) 在"加密"处设置是否要将配置文件加密。

3)选择"运行配置",并点击"下载"按钮,将设备当前的运行配置下载到本机;选择"保存配置"并点击"下载"按钮将设备的保存配置下载到本机。

4) 点击蓝色链接,保存配置文件。

	配置维护
配置替换	浏览
	替换
配置下载	加密 🗹 · ⓒ 运行配置 ○ 存盘配置 下载
	当前运行配置点击下载[密文][或用右键另存]

## 配置导入

## 基本需求

某企业的网络管理员将旧设备的配置文件导入到新设备上。

## 配置要点

- ▶ 导入配置文件
- ▶ 配置文件生效

## WEBUI 配置步骤

 1)管理员登录远程安全设备,选择 系统管理 > 维护,并点击"配置维护"页签, 在"配置维护"处进行设置。

	配置维护
配置替换	浏览
配置下载	加密 🔽 💿 运行配置 🔿 存盘配置

2) 点击"浏览..."按钮,选择旧设备的配置文件。

3) 点击"替换"按钮,导入配置文件。

配置文件导入成功后,用户需要重新登录网络卫士防火墙。

## 在线升级

网络卫士防火墙支持基于 TFTP 协议、HTTP 协议(WEBUI 升级)和 FTP 协议的升级方式,以便用户方便、及时地使用天融信不断发布的升级包对设备的性能和功能进行扩充和完善。通过 WEBUI 进行升级比较简单,本案例将重点介绍如何通过 TFTP 协议对网络卫士防火墙进行升级。

## 基本需求

背景:某PC机(IP: 192.168.83.5)与网络卫士防火墙的eth2口(IP: 192.168.83.2) 相连,网络卫士防火墙的eth1口(IP: 202.59.63.8)通过Internet与TFTP服务器(IP: 202.59.65.8)相连,如图1所示。

需求:通过 TFTP 服务器对本地网络卫士防火墙进行远程升级。





## 配置要点

- ▶ 获取网络卫士防火墙升级包,并将其存放于 TFTP 服务器的工作目录中
- ▶ 验证升级包
- ▶ 在网络卫士防火墙上设置 TFTP 服务器
- ▶ 对网络卫士防火墙进行升级

### TFTP 服务器设置

本案例以 WINDOWS 系统的 Cisco TFTP Server 作为 TFTP 服务器。

1) 设置 TFTP 服务器的工作目录。

通过 View > Option 目录设置工作目录,如下图。

Cisco TFTP Server (192.168.83.226) = C:\Program Files\Cisco	- O ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>H</u> elp	
🗁 😤 Options 🗙	
✓ Show file transfer progress ✓ Enable loggin Log  C:\Program Files\Cisco Systems\Cisco TFTP Sep Browse Maximum log file size (KB): 20	×
TFTP server root D:\tftp folder OK Cancel	
Ready	<u>ب</u> // ۱

2) 将网络卫士防火墙升级包存放于工作目录中。

3) 启动 TFTP 服务。

#### 验证升级包

为了保证升级包下载正确,需要使用 MD5 程序校验工具进行验证。MD5 程序校验工 具由网络卫士防火墙的随机光盘提供。

1)运行程序校验工具(MD5),如下图所示。

<mark>輕</mark> 程序校验工具 www.17577.com	×
正在处理:	
拖动文件图标到上面框中计算MD5校验值,复制校验值请按Ctrl+C。	[[]] 退出

2)将升级包拖动至"程序校验工具"上面的方框中进行校验。校验值及其对应的升级包名称显示在下面的方框中,如下图所示。

📮 程序校验工具,	rww. 17577. com		×
正在处理:			
ceOf30a64690	e874e30af4662abb63d8	3.3.002.008.:	1 upt
			_
, 拖动文件图标到上	面框中计算MD5校验值,复制校验	值请按Ctrl+C。	退出

3)将该校验值及其升级包名称与天融信公司提供的 MD5 验证内容进行对比,如果 完全一致,表示该升级包是正确的,可以进行升级;否则,请重新下载升级包。

## WEBUI 配置步骤

1)选择系统管理>维护,并点击"升级"页签,如下图。

配置维护 升级 重启 健康记录 诊断	
系统升级	
进行系统升级(注意:升级过程中诸不要做任何操作,并退出终端!) TFTP 升级 FTP 升级 网页升级	

2) 点击"TFTP升级"按钮设置 TFTP 服务器。

🌽 系统升级 网页对话	框	×
	TFTP 升级	
服务器地址 文件名称 升级系统	202.59.65.8 * 3.3.006.035.1_upt *	
https://192.168.83.237:808	0/update_sys.html 😜 Internet	1.

3) 点击"升级系统",便可完成升级。

网络卫士防火墙升级成功后设备会自动重启,导致管理用户与网络卫士防火墙的通信中断。这种情况下,用户只需重新登录网络卫士防火墙即可。

至此,WEBUI 方式的配置完成。

## 注意事项

1)升级前,请确保 TFTP 服务器设置正确。

2) 相应版本的升级包只能在对应版本的硬件上进行升级,不能混用。

3) 在升级过程中,请确保网络卫士防火墙与 TFTP 服务器的通信不会中断。

4)升级过程大约 10 分钟左右,请耐心等待。并避免对网络卫士防火墙进行任何操作,特别是不能按键 CTRL+C。

5)升级完成后,正常情况下网络卫士防火墙的原有配置不会丢失;但为了安全,请 在升级设备前做好相关备份工作。如遇特殊情况,可以向天融信当地的技术支持工程师寻 求帮助。

## 动态路由配置

本节主要介绍网络卫士防火墙动态路由的配置案例,包括 OSPF 动态路由和 RIP 动态路由案例。

## OSPF 动态路由配置

OSPF协议是一个基于链路状态的动态路由协议,其基本原理是:在一个 OSPF 网络中,每一台路由器首先与自己的邻居建立邻接关系,然后向形成邻接关系的邻居之间发送链路状态通告(LSA),链路状态通告描述了所有的链路信息,每一个路由器接收到 LSA都会把这些通告记录在链路数据库中,并发送一个副本给他的邻居,通过 LSA 泛洪到整个区域,所有的路由器都会形成相同的链路状态数据库,当所有路由器链路状态数据库相同时,会以自己为根,通过 SPF 算法计算出一个无环的拓扑,从而计算出自己到达系统内部可达的最佳路由。

#### 基本需求

背景: 某企业内部网络拓扑比较复杂, 各网段间路由信息的传播已经造成网络流量一定的负担, 故该企业决定采用 OSPF 动态路由协议来解决这一问题。企业内部的网络环境为: 网络卫士防火墙 A、网络卫士防火墙 B、路由器 A 和路由器 B 共四台设备参与动态路由, 网络卫士防火墙 B 的 eth0 口(IP: 10.0.0.2)和网络卫士防火墙 A 的 eth1 口(IP: 10.0.0.1)相连, 网络卫士防火墙 A 的 eth0 口(IP: 172.16.0.1)和路由器 A 的 F0/0 口(IP: 172.16.0.2)相连, 路由器 A 的 F0/1 口(IP: 11.0.0.1)又与路由器 B 的 F0/0 口(IP: 11.0.0.2)相连, 同时这四台设备分别连接了内网 A 区、内网 B 区、内网 C 区和内网 D 区, 其网络拓扑如图 1-1 所示。

需求:在网络卫士防火墙 A、网络卫士防火墙 B、路由器 A 和路由器 B 之间实现 OSPF 动态路由。



图 2 OSPF 动态路由配置网络拓扑图

## 配置要点

- ▶ 启动 OSPF 动态路由服务
- ▶ 设置参与 OSPF 动态路由的网段

## WEBUI 配置步骤

#### 网络卫士防火墙 A 配置:

1) 启动 OSPF 服务。

选择 网络管理 > 路由,并选择"动态路由 OSPF"页签,点击"启动"按钮启动 OSPF 服务,如下图。

动态路由OSPF 动态路	由RIP 动态路由BGP 多打
0SPF &	± ۲
启动	停止    查看

启动后界面如下图所示。

动态路由	OSPF	动态器	备曲RIP	(动态)	备由BGP	\$	
	OSPF设置						
	启动		停止	查	看		
区域配置	╋添加						
	运行网段		区域ID		删除		
路由重发布	设置						
acl	╋添加						
	名称	运行网	段	权限	删除		
acl分发	╋添加						
	名称	路E	由类型		删除		
接口设置	╋添加						
	接口名称			修改			

3) 在"区域配置"处,点击"添加"按钮,将网络172.16.0.0/24 添加到 area 0,将 网络10.0.0.0/24 添加到 area 1。

将 172.16.0.0/24 添加到 area 0, 如下图。

<b>OSPF区域</b>	
运行网段: 172.16.0.0    /24 区域ID: 0	* [子网/掩码] [0-4294967295] <sup>*</sup>
确定 取消	

添加 10.0.0.0/24 到 area 1,如下图。

OSPF区域	
运行网段: 10.0.0.0 /24 区域ID: 1	* [子网/掩码] [0-4294967295]   *
确定取消	

#### 网络卫士防火墙 B 配置:

1) 启动 OSPF 服务。

选择 网络管理 > 路由,并选择"动态路由 OSPF",点击"OSPF 启动"按钮启动 OSPF 服务,如下图。

动态路由OSPF	动态路由RIP	动态路由B	GP 🛛 🏂
	OSPF设置		
启动	停止	查看	]

3) 将网络 10.0.0/24 添加到 area 1。

在"OSPF区域配置"处点击"添加"按钮将 10.0.0.0/24 添加到 area 1,如下图。

OSPF区域	
运行网段: 10.0.0.0 /24 区域ID: 1	* [子网/掩码] [0-4294967295]   *
确定 取消	

#### 路由器 A 配置:

- 1) 设置 F0/0 口和 F0/1 口的 IP 地址分别为 172.16.0.2 和 11.0.0.1
- 2) 启动 OSPF 服务
- 3) 将网络 172.16.0.0/24 加入 area 0
- 4) 将网络 11.0.0.0/24 加入 area 1

#### 路由器 B 配置:

- 1) 设置 F0/0 口的 IP 地址为 11.0.0.2
- 2) 启动 OSPF 服务
- 3) 将网络 11.0.0.0/24 加入 area 1

本案例只给出网络卫士防火墙上 OSPF 动态路由的配置,其他设备的配置请参考该设备相关的使用说明。

#### 注意事项

1)设置网络卫士防火墙的 IP 地址时一定要将该 IP 的 label 设置为 0,方可利用该 IP 地址启动 OSPF 服务。

2)通过在"OSPF协议访问控制"处设置访问控制还可以控制参与动态路由的网络中的哪些网段可以使用 OSPF 协议,进而达到对 OSPF 网络更细粒度的控制。

## RIP 动态路由配置

RIP(Routing Information Protocol),路由信息协议,是推出时间最长的路由协议, 也是最简单的路由协议。RIP 通过广播或多播 UDP 报文来交换路由信息,每 30 秒发送一 次路由信息更新,同时根据收到的 RIP 报文更新自己的路由表。RIP 提供跳跃计数(hop count)作为尺度来衡量路由距离,跳跃计数是一个包到达目标所必须经过的路由器的数 目。网络卫士防火墙支持 RIP 的 v1、v2 版本。

## 基本需求

背景: 某企业内部网络拓扑比较复杂, 各网段间路由信息的传播已经造成网络流量一定的负担, 故该企业决定采用 RIP 动态路由协议来解决这一问题。企业内部的网络环境为: 网络卫士防火墙 A、网络卫士防火墙 B、路由器 A 和路由器 B 共四台设备参与动态路由, 网络卫士防火墙 B 的 eth0 口(IP: 10.0.0.2)和网络卫士防火墙 A 的 eth1 口(IP: 10.0.0.1)相连, 网络卫士防火墙 A 的 eth0 口(IP: 172.16.0.1)和路由器 A 的 F0/0 口(IP: 172.16.0.2)相连, 路由器 A 的 F0/1 口(IP: 11.0.0.1)又与路由器 B 的 F0/0 口(IP: 11.0.0.2)相连, 同时这四台设备分别连接了内网 A 区、内网 B 区、内网 C 区和内网 D 区, 其网络拓扑如图 1-1 所示。



需求: 在网络卫士防火墙 A、网络卫士防火墙 B、路由器 A 和路由器 B 之间实现 RIP 动态路由。

#### 图 3 RIP 动态路由配置网络拓扑图

## 配置要点

- ▶ 启动 RIP 动态路由服务
- ▶ 开放防火墙的 RIP 服务
- ▶ 设置参与 RIP 动态路由的网段

## WEBUI 配置步骤

#### 网络卫士防火墙 A 配置:

1) 开放 eth0 口和 eth1 口的 RIP 服务。

选择 系统管理 > 配置,并点击"开放服务"页签。点击"添加"开放 eth0 口的 RIP 服务,如下图。

开放服务	时间	SNMP 邮件设置	短信设置
		添加配置	
	服务名称	RIP	~
	控制区域	area_eth0	•
	控制地址	any [范围]	*
		确定 取消	

#### 点击"添加"开放 eth1 口的 RIP 服务,如下图。

开放服务	时间	SNMP 邮件设置	短信设置
		添加配置	
	服务名称	RIP	~
	控制区域	area_eth1	•
	控制地址	any [范围]	*
		确定 取消	

2) 启动 RIP 服务。

选择 网络管理 > 路由,并选择"动态路由 RIP"页签,点击"启动"按钮启动 RIP 服务,如下图。

铀OSPF	动态路由RIP	动态路由BGP
	RIP设置	
启动	停止	查看

启动 RIP 协议后,界面如下图所示。

动态路由	OSPF	动态路由	#RIP	动态路由B	GP 🛛 🏂	
	BIP设置					
	启动		停止	查看	]	
网络配置	╋添加					
	运行网段			删除		
路由重发布	设置					
邻居配置	➡添加					
	IP		删除			

3) 在"邻居配置"处,点击"添加"按钮,添加网络172.16.0.0/24 和网络10.0.0.0/24。 添加172.16.0.0/24 网络,如下图。

	RIP	区域
运行网段	172.16.0.0	/24 * [子网/掩码]
	确定	取消

添加 10.0.0.0/24 网络,如下图。

	RI	P区域
运行网段	10.0.0.0	/ 24 * [子网/掩码]
	确定	取消

#### 网络卫士防火墙 B 配置:

1) 开放 eth0 口的 RIP 服务。

选择 系统管理 > 配置,并点击"开放服务"页签,点击"添加"开放 eth0 口的 RIP 服务,如下图。

开放服务	时间	SNMP 邮件设置	短信设置
		添加配置	
	服务名称	RIP	~
	控制区域	area_eth0	•
	控制地址	any [范围]	~
		确定 取消	

2) 启动 RIP 服务。

选择 网络管理 > 路由,并选择"动态路由 RIP",点击"启动"按钮启动 OSPF 服务,如下图。

诸由OSPF	动态路由RIP	动态路由BGP
	RIP设置	
启动	停止	查看

启动 RIP 协议后,界面如下图所示。

动态路由	OSPF	动态路由RI	P 🔪	动态路由BGP	3
		BIP设置			
	启动	停止		查看	
网络配置	╋添加				
	运行网段			删除	
路由重发布	设置				
邻居配置	╋添加				
	IP	删除	i		

3) 设置网络 10.0.0/24 参与 RIP 动态路由。

在"邻居配置"处点击"添加"按钮添加网络10.0.0/24,如下图。

	<b>RT</b> )	P区域
运行网段	10.00.0	/24 * [子网/掩码]
	确定	取消

#### 路由器 A 配置:

- 1) 设置 F0/0 口和 F0/1 口的 IP 地址分别为 172.16.0.2 和 11.0.0.1
- 2) 启动 RIP 服务
- 3) 设置网络 172.16.0.0/24 和网络 11.0.0.0/24 参与 RIP 动态路由

#### 路由器 B 配置:

- 1) 设置 F0/0 口的 IP 地址为 11.0.0.2
- 2) 启动 RIP 服务
- 3) 设置网络 11.0.0.0/24 参与 RIP 动态路由

本案例只给出网络卫士防火墙上 RIP 动态路由的配置,其他设备的配置请参考该设备 相关的使用说明。

#### 注意事项

1)设置网络卫士防火墙的 IP 地址时一定要将该 IP 的 label 设置为 0,方可利用该 IP 地址启动 RIP 服务。

2)通过在"RIP协议.访问控制"处设置访问控制还可以控制参与动态路由的网络中的哪些网段可以使用 RIP 协议,进而达到对 RIP 网络更细粒度的控制。

## 策略路由配置

策略路由与静态路由都用于定义数据包转发规则,但基于策略的路由比传统路由控制能力更强,使用更灵活,它使网络管理者不仅能够根据目的地址,而且能够根据协议类型、应用、IP 源地址或者其它的策略来选择转发路径。这种方式可以实现内部网络的指定对象使用特定外部线路与外部网络通信,从而进一步增强了网络的通信安全。

#### 基本需求

背景:企业网络通过防火墙连接了两个 ISP(电信和网通),其中电信与 eth1 口: 202.98.1.2 相连;网通与 eth2 口: 202.99.1.2 相连;企业内网服务器地址为: 172.16.98.222。

其中网通用户使用企业提供的地址: 202.99.1.3 访问内部网络; 电信用户使用企业提供的地址: 202.98.1.3 访问内部网络。

需求 1: 电信和网通用户可以分别通过两个不同的公网地址来访问企业内网的一台服 务器; 而且内网服务器回复报文遵循电信用户使用电信出口, 网通用户使用网通出口的规则。

需求 2: 电信和网通用户可以分别通过两个不同的公网地址来对防火墙进行管理。



图 4 策略路由配置拓扑图

### 配置要点(需求1)

- ▶ 配置主机资源
- ▶ 配置目的地址转换策略
- ▶ 配置策略路由

### WEBUI 配置步骤

1) 配置主机资源

选择 资源管理 > 地址,在"主机"页面中点击"添加"添加下列主机资源,如下 图。

主机 范围 子网	地址组	
➡ 添加 前 清空		
		总计 <mark>: 4</mark>
名称 🔶	IP地址 🔶	操作
webserver	192, 168, 83, 234	23
202.99.1.3	202. 99. 1. 3	23
202.98.1.3	202. 98. 1. 3	23
172.16.98.222	172. 16. 98. 222	23

2) 配置目的地址转换策略

选择 防火墙 > 地址转换, 配置网通及电信的公网 IP 与内网服务器 IP 的转换 (202.99.1.3->172.16.98.222, 202.98.1.3->172.16.98.222), 如下图。

🕂 添加	Ω			总计:	2 毎页: 30条	•
ID	类型	源	目的	服务	转换	操作
8049	目的转换	地址: any	地址: 202.99.1.3		目的: 172.16.98.222	
8050	目的转换	地址: any	地址: 202.98.1.3		目的: 172.16.98.222	
				∢	▶ ▶ 转到	/1 Go

3)配置策略路由,限制从内网服务器回复的报文,电信用户使用电信出口 eth1,网通用户使用网通出口 eth2。

①添加策略路由并设置绑定属性

选择 网络管理 > 路由,并点击"策略路由"页签,点击"添加",添加一条策略路由"eth0\_p"与属性 eth0 绑定,用于设置从 Eth0 口接收的数据报文的处理策略。如下图。

策略路由 🛛 🗟	b态路由OSPF 动态路由RIP 动态路由BGP 多播路由
	添加策略路由
名称 绑定	eth0_policy * □ 全局 □ 本地外出 ☑ 入接口
可用接口 eth1 eth2 eth3 ipsec0 ipsec1	已选接口 ▲ → × ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
	确定取消

#### ②添加路由条目

在已添加的策略路由 eth0\_policy 上点击"路由条目",添加下列路由条目,如下图。

	添加路由条目
3/Б1-0 +.L	P00.00.1.0
视界地址	202.99.1.3
源掩码	255. 255. 255. 255
目的地址	
目的掩码	
网关	202. 99. 1. 1
接口	eth2
高级	
源端口	- [0-65535;单个端口只填起始端口]
目的端口	- [0-65535;单个端口只填起始端口]
协议	-选择协议▼
NAT转换后的源	☑ 开启
度量值	[1-65535]
权重值	[1-128]

	添加路由条目
源地址 源掩码	202. 98. 1. 3 255. 255. 255. 255
目的地址 目的掩码	
网关 接口	202.98.1.1 eth1
高级	
目的端口	-     [0-65535;单个端口只填起始端口]
DNX NAT转换后的源	-选择协议- ▼
度量值 权重值	[1-65535]
	确 定 取 消

"源地址"处要填入服务器对于网通和电信用户的公网 IP 地址。

"转换后的源"要设为开启。

## 配置要点(需求2)

▶ 配置策略路由

## WEBUI 配置步骤

1) 添加策略路由并设置绑定属性

选择 网络管理 > 路由,并点击"策略路由"页签,点击"添加",如下图。

	添加策略路由
名称 绑定	local_policy * □全局 ☑本地外出 □入接口
	确定 取消

#### 2) 添加路由条目

在已添加的策略路由 local\_policy 点击"路由条目",添加两条路由条目,如下图。

添加路由条目	
源地址	202.98.1.2
源掩码	255. 255. 255. 255
目的地址	
目的掩码	
网关	202. 98. 1. 1
接口	eth1
高级 🔽	
源端口	
目的端口	- [单个端口或范围,0-65535;单个端口只填起始端口]
协议	-选择协议
NAT转换后的源	一 开启
度量值	[1-65535]
权重值	[1-128]
确定	取消

添加路由条目	
源	地址: 202.99.1.2
源	掩码: 255.255.255.255
目的	地址:
目的	掩码:
	网关: 202.99.1.1
	接口: eth2 🔽
高	a 🔽
源	端口:[单个端口或范围,O-65535;单个端口只填起始端口]
目的	端口: _ [单个端口或范围,0-65535;单个端口只填起始端口]
	协议: ─选择协议──
NAT转换后	的源: 🗖 开启
度	量值: [1-65535]
权	重值: [1-128]
确定	取 消

"源地址"处要填入网通和电信用户所访问设备的真实地址。

## 多播

随着Internet的发展,出现了电视会议、视频点播、远程教育等新兴应用,传统的点 到点通信方式(单播)对于这些新应用来说,不仅浪费网络带宽,而且效率不高。解决 这一问题的一种有效方式就是使用多播技术(Multicast)。网络卫士防火墙可以转发IP多 播数据报文,并简单处理IGMP协议。当网络卫士防火墙工作在路由模式及混合模式下, 如果需要转发多播数据包,管理员必须定义多播路由。



### 基本需求

图 5 网络卫士防火墙转发多播数据包的网络示意图

功能需求及实例说明:

上图中网络卫士防火墙位于企业边界路由器(支持多播路由协议)及内部网络之间, 网络卫士防火墙的 eth0 和 eth1 口均工作在路由模式,内网主机需要接收国际互联网上的 多播服务器(IP 172.16.1.1,此处使用了私有地址,仅为示意)发出的多播数据(多播组地址 为 226.1.1.5,仅为示意)。

## 配置要点

▶ 设置多播路由策略

#### WEBUI 配置步骤

选择 网络管理 > 路由, 在"多播路由"页签点击"添加"添加一条多播路由。

路由表 策略路由 动态路由OSP	F 动态路由RIP 动态路由BGP 多播路由 动态				
	添加多播路由				
源地址	172.16.1.0 *				
源掩码	255. 255. 255. 0 *				
多播组	226.1.1.5 *				
源接口	ethi 💌 *				
发送加入报告	☑ 开启				
目的接口					
可用接口	目的接口				
ethi eth2 eth3 sslvpn0 vlan.0001	→ × eth0				
确定取消					

选择"发送加入报告"项,是因为网络卫士防火墙目的接口 eth0 有下游多播路由器, 需要由网络卫士防火墙定时地向上游多播路由器发送加入报告(joining report),以保证 多播报文顺利地转发给下游多播路由设备,维护多播树结构。反之,如果网络卫士防火墙 和内部子网间不存在多播路由器,无须选择"发送加入报告"复选项。

## 注意事项

 源地址的设定:当网络卫士防火墙接收到多播数据报文时,为了避免出现环路和 多播风暴的发生,可以检查多播的源和多播数据接收的接口,如果多播的源对应的接口和 实际接收接口不匹配,则会丢弃该多播报文。

2)多播流量的源接口可以是路由接口也可以是 VLAN 虚接口,不能为交换接口。

## DHCP

网络卫士防火墙提供比较全面的 DHCP 服务功能,能够很好地结合到客户网络环境中。网络卫士防火墙可以提供以下 DHCP 服务:

- ▶ 作为 DHCP 客户端,从 DHCP 服务器获取动态 IP 地址;
- ▶ 作为 DHCP 服务器,集中管理和维护客户网络主机 IP 地址分配;
- ▶ 作为 DHCP 中继,转发 DHCP 报文;
- ▶ 同时作为 DHCP 服务器和 DHCP 客户端(需工作在网络卫士防火墙的不同接口上)。

## DHCP 服务器

### 基本需求

网络卫士防火墙作为 DHCP 服务器,为 eth1 口所在区域的客户机自动分配 IP 地址及 其他配置参数,如默认网关、DNS 等等。



图 6 网络卫士防火墙作为 DHCP 服务器示意图

### 配置要点

- ▶ 配置相关接口的 IP 地址
- ▶ 开放相关接口的 DHCP 服务
- ▶ 配置 DHCP 服务器

#### WEBUI 配置步骤

1) 配置 eth1 口的 IP 地址

选择 网络管理 > 接口 菜单,在"物理接口"页签点击 eth1 口的设置图标,为 eth1 口添加 IP 地址 10.10.10.1/24,如下图。

物理接口 子掛	理接口 子接口			
	接口设置			
名称	eth1 ( 00:13:32:02:23	3: <b>F</b> 5 )		
描述	internet			
状态	□ 停用			
模式	⑥ 路由 ○ 交換	○ IDS监听		
地址 10. 10. 10. 1	<b>掩码</b> 255. 255. 255. 0	非同步地址 [_]	添加	
地址	掩码	属性	删除	
高级				
确 定 取 消				

2) 开放 eth1 口的 DHCP 服务

a) 设置 eth1 口所属区域。

选择 资源管理 > 区域 菜单, 添加 area\_eth1 区域,并与 eth1 属性绑定。

b) 开放 area\_eth1 区域的 DHCP 服务

选择 系统管理 > 配置,选择"开放服务"页签,点击"添加",开放 DHCP 服务。

系统参数 开放服务 时间 SNMP	V
添加配置	
服务名称 DHCP 🚽	
控制区域 area_eth1 ▼	
控制地址 any [范围]	
确 定 取 消	

3) 配置 DHCP 服务器

选择菜单 网络管理 > DHCP,并选择"DHCP 服务器"页签,配置网络卫士防火墙的 eth1 口作为 DHCP 服务器端的属性:添加地址池、添加地址绑定并启动 DHCP 服务器。

a) 点击"添加地址池", 配置地址池及其他配置参数。

添加DHCP地址池		
子网	10. 10. 10. 0 *	
掩码	255. 255. 255. 0 *	
分配起始地址	10. 10. 10. 10 *	
分配结束地址	10.10.20 *	
缺省租用期	1 天 0 时 0 分	
最大租用期	7 天 0 时 0 分	
网关地址		
ZINS		
次DNS		
域名		
客户端类型		
供应商详情		
	确 定 取 消	

b)在eth1口启动DHCP服务器。

DHCP服务器 DHCP客户端 DHCP中继					
配置					
运行接口	eth1		[ <- ] X	eth0 eth2 eth3 sslvpn0	* *
运	行	停止			

点击"运行"启动 DHCP 服务器。

4) 查看已分配地址

点击"查看已分配地址"按钮,可以在右侧界面中查看网络卫士防火墙上 DHCP 服 务器分配地址情况。

已分配地址				
			总计: 1	
IP	MAC	租约开始	租约结束	
10.10.10.20	00:50:04:c3:b0:31	2009/09/07 16:46:32	2009/09/08 16:46:32	
### 注意事项

1) DHCP SERVER 服务可以运行在一个或多个物理接口(或虚接口)上。

2)如果接口工作在交换模式,如下图所示,则应在所属的 VLAN 虚接口上启动 DHCP 服务。



这种情况下,如果在运行接口中填入"eth0",系统会提示错误!

3) 地址池暂不支持排除地址

比如,不支持从地址范围 10.10.10.101-10.10.10.120 中排除地址 10.10.10.103

4) 已分配的 IP 既可以在 WEBUI 下查看, 也可以在命令行下使用 network dhcp show binded 命令查看。

TopsecOS.network#	dhcp show binded		
TopsecOS.network# IP	dhcp show binded start time	end time	Mac address
10.10.10.20	2009/09/07 16:46:32	2009/09/08 16:46:32	00:50:04:c3:b0:31

但目前无法查看已和 MAC 绑定的 IP 地址的分配情况。

### DHCP 客户端

默认情况下网络卫士防火墙需要手工配置物理接口或 VLAN 虚接口的 IP 地址。网络卫士防火墙的物理接口或虚接口也可以作为 DHCP 客户端从 DHCP 服务器端动态获取 IP 地址。

#### 基本需求

网络卫士防火墙需要作为 DHCP 客户端,动态地为 eth0 口获取 IP 地址及其他配置参数,如默认网关、DNS 等等。



图 7 网络卫士防火墙作为 DHCP 客户端示意图

#### 配置要点

- ▶ 配置相关接口的工作模式
- ▶ 开放相关接口的 DHCP 服务
- ▶ 配置 DHCP 客户端

### WEBUI 配置步骤

1) 查看 eth0 口的工作模式

选择 网络管理 > 接口 菜单,在"物理接口"页签,查看并设置 eth0 接口的工作在 路由模式,如下图。

物理接口	子接口
	接口设置
名称	eth0 ( 00:13:32:02:23:F4 )
描述	intranet
状态	□ 停用
模式	◎ 路由 ○ 交換 ○ IDS监听

接口 eth0 有无 IP 配置对于该接口动态获取 IP 地址没有影响,即使原来有 IP 地址设置,当在该接口成功启用 DHCP 客户端后自动删除原有的 IP 地址。

如果 eth0 工作在交换模式,则只有其所属的 VLAN 虚接口能作为 DHCP 客户端动态 获取 IP 地址。

2) 开放 eth0 口的 DHCP 服务

a) 设置 eth0 所属区域

选择 资源管理 > 区域 菜单, 添加 area\_eth0 区域, 并与 eth0 属性绑定。

区域		
	区域	
	名称 area_eth0 * 访问权限 允许 ▼ 注释	
可用属性: eth1 eth2 eth3 ads1 ads11	成员: -> eth0	
	确定取消	

b)选择菜单 资源管理 > 地址,在"主机"页签点击"添加"添加 DHCP 服务器主 机资源。

主机 范围 子网 地址組					
主机雇性					
名称 DHCPServer * 物理地址 00:00:00:00:00 IP地址 192.168.83.234  ( ) 192.168.83.234  ( ) 192.168.83.234  ( ) )					
确 定 取 消					

c)选择菜单 系统管理 > 配置,在"开放服务"页签点击"添加"开放 DHCP 服务。

系统参数 开放服务 时间 SNMP 邮件设置
添加配置
服务名称 DHCP
控制区域 area_eth0 🔽
控制地址 DHCPServer [主机]
确 定 取 消

3) 配置 DHCP 客户端

选择菜单 网络管理 > DHCP,并选择 "DHCP 客户端"页签,设置网络卫士防火墙 的 eth0 口作为 DHCP 客户端。

DHCP服务器	DHCP客户端 D	HCP中维
	配置	
指定接口	eth0	<pre>     eth1     eth3     sslvpn0     vlan.0001     vlan.0001 </pre>
	运行	停止

选择"启用",并点击"应用",启动 DHCP 客户端,如果系统提示配置成功,表示接口已正常获取 IP 地址,配置完成。

4) 查看网络卫士防火墙获取的接口 IP

在命令行下查看网络卫士防火墙接口是否自动获取了 IP,如下图。

Topsec0S#	network interface eth0 show
eth0	Description:intranet
	Link encap:Ethernet HWaddr 00:13:32:05:39:24
	Link status: established, Autoneg enable
	Full-duplex, 100Mb/s
(	inet addr:192.168.83.219
Р	
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
	RX packets:85646 errors:0 dropped:0 overruns:0 frame:0
	TX packets:36335 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:100
	RX bytes:7284722 (6.9 Mb) TX bytes:2651101 (2.5 Mb)
	Interrupt:12

在 WEBUI 下查看网络卫士防火墙接口是否自动获取了 IP,如下图。

物理接口		子接口							
接口名称	描述	接口模式	地址	MTU	状态	链接	协商	速率	设置
eth0		路由	192, 168, 83, 219/255, 255, 255, 0 (dhep)	1500	启用	0	全双工	100M	
eth1		路由	172.16.1.1/255.255.255.0	1500	启用	0	全双工	100M	
eth2		路由		1500	启用	۲			
eth3		路由		1500	启用	0			

### 注意事项

1)网络卫士防火墙接口作为 DHCP 客户端时所连接的 DHCP 服务器不能与别的物理 接口或 VLAN 虚接口处于同一个网段,否则即使此处运行成功也不能正确获取 IP。

2) DHCP CLIENT 服务可以运行在 VLAN 虚接口上。如下图所示,网络卫士防火墙的 eth0 口工作在交换模式,属于 vlan.0002 接口,通过 DHCP 服务器获取 IP 地址。



接口设置如下图所示。

物理接口 子接口	
	接口设置
名称 描述 状态 模式 交换相 类型 Acces <b>高级</b>	eth0 (00:13:32:02:23:F4 ) intranet 「 停用 〇 路由 ● 交換 〇 IDS监听 武 ● access 〇 trunk s 21 [1-4094] <b>藍性</b>
(	确定取消

此时在"DHCP 接口"项中需要输入 VLAN 虚接口名 vlan.0002,如下图所示。

DHCP客户端	DHCP中维
	配置
指定接口	vlan. 0002 X eth3 sslvpn0 vlan. 0001 lo
	启动 停止

如果在 DHCP 接口中填入 "eth0", 系统会提示错误!

2)网络卫士防火墙作为 DHCP 客户端时不会从 DHCP 服务器获取 DNS 信息。用户可以通过 网络管理 > 域名解析 配置 DNS 服务器。

3)网络卫士防火墙作为 DHCP 客户端可以从 DHCP 服务器获取路由信息。当网络卫士防火墙成功获取 IP 的同时,会在系统的静态路由表中添加一条路由。可以通过 网络管理 > 路由 的"静态路由"页签进行查看。

4)网络卫士防火墙可以在多个接口同时启用 DHCP CLIENT 的服务。

### DHCP 中继

### 基本需求

网络卫士防火墙作为 DHCP 中继代理,帮助客户机(位于 eth1 口所在区域)从其他 网段(192.168.83.0/24)的 DHCP 服务器(192.168.83.234)获取 IP 地址及其他配置参数, 如默认网关、DNS 等等。



图 8 网络卫士防火墙作为 DHCP 中继示意图

### 配置要点

- ▶ 开放相关接口的 DHCP 服务
- ▶ 配置 DHCP 中继

### WEBUI 配置步骤

1)开放服务器和客户机所属区域的 DHCP 服务。

a)选择 **资源管理 > 区域** 菜单,添加 area\_eth0/area\_eth1 区域,并与 eth0/eth1 属性 绑定。

区域					
中 添加	而 清空				
					总计 <b>: 2</b>
名称	\$	绑定属性	\$ 权限	\$ 注释	\$ 操作
area_eth0		eth0	允许	1	2
area_eth1		eth1	允许		2
urcu_con1			2001		

b)选择菜单 资源管理 > 地址,在"主机"页签,点击"添加"添加 DHCP 服务器 主机资源。

主机 范围 子网 地址組					
主机尾性					
名称 DHCPServer 物理地址 00:00:00:00:00 IP地址 192.168.83.234	* 192. 168. 83. 234 ×				
确定 取消					

c)开放 DHCP 客户端和服务器端所在区域的 DHCP 服务。

选择菜单 系统管理 > 配置,并选择"开放服务"页签,点击"添加"开放 DHCP 服务。

开放 area\_eth0 区域的 DHCP 服务,如下图。

系统参数 开放服务 时间 SNMP 邮件设置
添加配置
服务名称DHCP
控制区域 area_eth0 🔽
控制地址 DHCPServer [主机]
确 定 取 消

开放 area\_eth1 区域的 DHCP 服务,如下图。

系统参数 开放服务 时间 SNMP 邮件设置
修改配置
服务名称 DHCP 🗸
控制区域 area_eth1 🔽
控制地址 any [范围]
确 定 取 消

#### 2) 配置 DHCP 中继

选择菜单 网络管理 > DHCP,并选择"DHCP 中继"页签,配置 DHCP 中继的属性。

DHCP服务器 DHCP客户端	DHCP中继
ñ	置
指定接口 eth0 eth1	← k13 sslvpn0 vlan.0001 vlan.0002
服务器地址 192.168.83.234	✓ 192. 168. 83. 234
运行	停止

选择"启用",同时输入与服务器和客户机连接的接口(或虚接口),然后点击"应用"启动 DHCP 中继。

至此,网络卫士防火墙作为 DHCP 中继的配置完成。

#### DHCP 服务器的相关配置:

1) 配置 DHCP 服务器的作用域,要与 DHCP 客户端连接的端口在同一个子网内。

在本例中, DHCP 服务器上 DHCP 作用域的地址池应该在 10.10.10.0 子网内。

2)如果 DHCP 服务器的默认网关不是网络卫士防火墙的接口或 VLAN 虚接口的地址, 必须在该服务器上添加一条静态路由,否则客户机无法正确获取 IP。



上图中, DHCP 服务器的默认网关是路由器的 E0 接口(192.168.83.1/24),这种情况下,需要在服务器的路由表里添加一条静态路由,如下图。

Interface	List				
Øx1		MS 1	CP Loopback inter	face	
0×200 数据包计划	11 d8 a8 9 月程序微型端	c 26 Real	ltek RTL8139 Famil	y PCI Fast Ether	rnet NIC
Active Rou	utes:				
Network De	estination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.83.240	192.168.83.234	30
1	10.1.1.0	255.255.255.0	192.168.83.240	192.168.83.234	1
10.	.10.10.0	255.255.255.0	192.168.83.240	192.168.83.234	1
12	27. 0.0	255.0.0.0	12 9.0.1	127.0.0.1	1
192.1	168.8 9	255.255.255.0	192.168.2 34	192.168.83.234	30
192.10	E CANADA TO DA	CDEL 5.255.255	网关地址为防火地	与 127.0.0.1	30
192.10	日口地址 / J D T	5.255.255	197 DHCP服务器相连	的 :.168.83.234	30
	步位[F/1]残[1][	240.0.0.0	19: 接口地址,此处》	1.168.83.234	30
255.255	山江 为10.10.10	5.255.255	192 192.168.83.240	168.83.234	1
Default Ga	ateway:	192.168.83.240			

### 注意事项

1) DHCP 中继服务可以运行在 VLAN 虚接口上。



在上图中,因 eth0 是交换接口,此时 DHCP 中继配置参数如下图所示。

DHCP服务器 DHCP客户端 DHCP中继
配置
指定接口 vlan.0002 X eth3 sslvpn0 vlan.0001 lo
服务器地址 192.168.83.234 <
运 行 停止

此时,若在指定接口中填入"eth1"和"eth0",系统会提示错误!

2)中继服务需要同时开放服务器和客户机所属区域的 DHCP 服务。

3)运行中继服务时,需要同时输入与服务器和客户机连接的接口(或虚接口)。

4)网络卫士防火墙可以在多个接口同时启用 DHCP RELAY 服务。

## 网络链路

网络卫士防火墙不仅支持客户端通过标准的 IPsec 协议与网络卫士防火墙建立 VPN 连接,而且支持动态接入的 PPPoE 协议通过拨号与外网建立通信链路,此外还支持 L2TP 和 PPTP 协议,远端用户可通过 Windows 自带的拨号连接组件或安装相应的客户端组件 与网络卫士防火墙通过 L2TP 服务或 PPTP 服务建立连接,从而访问整个网络。另外,网络卫士防火墙支持 GRE (Generic Routing Encapsulation)协议并可以实现与 Cisco 设备之间建立 GRE 隧道相互通信。

### ADSL 配置

网络卫士防火墙支持动态接入的 PPPoE 协议,便于小型办公场所或是公司分支机构 利用广泛使用的 ADSL 业务实现网络互连。网络卫士防火墙可以通过拨号与外网(如 Internet)建立通信链路,在进行 ADSL 连接时,网络卫士防火墙是通过 PPPoE 协议拨号 到 ISP 以获得一个动态的 IP 地址。ADSL 拨号成功后,系统自动创建 ppp0 接口并将其与 连接外网的以太网口绑定,使用 ISP 分配的动态 IP 地址,并使系统默认网关指向 ppp0。

### 基本需求

某企业内部网络通过 ADSL 拨号与外部网络建立连接,网络卫士防火墙的 eth1 口与 内部网络相连,eth0 口则通过路由器与外部网络及 ISP (ADSL 拨号服务器)相连,其网 络拓扑图如下。



图 9 内网通过 ADSL 拨号与外网建立链路示意图

需求:内部用户可以通过网络卫士防火墙与外部网络连接(即网络卫士防火墙的 eth0 口需要通过 ADSL 拨号获取一个公网 IP 地址);内网用户访问外网时使用 eth0 口获取的 公网 IP。

### 配置要点

- ▶ 设置 ADSL 拨号参数
- ▶ 定义外网区域
- ▶ 配置基于属性的源 NAT 策略

#### WEBUI 配置步骤

"adsl"属性是网络卫士防火墙上默认提供的属性,用户无须自行设置和修改。

1) 设置 ADSL 拨号参数

选择 网络管理 > 接入,并选择 "ADSL" 页签,如下图所示。

链路名称	描述	状态	带宽	分配IP地址	对端IP地址	收到报文	发送报文	拨号持续时间	操作	设置属性
adsl		未连接								2
adsl1		未连接								2
ads12		未连接								2
ads13		未连接						-		

点击"设置属性"按钮设置 ADSL 拨号参数,如下图。

ADSL 虚拟线 链路聚合 802.1x VLAN-VPN
ADSL雇性
绑定属性 adsl
接口 eth0 ▼
用户名 adsluser *
密码 ●●●●●●● *
按需拨号 🖂
高級
确 定

用户名/密码由 ISP 服务商提供,需要用户根据情况自行设置。另外,只有在服务商要求使用静态 IP 地址时才需要设置"本地地址"。

2) 定义外网区域 (adsl-a)

选择 资源管理 > 区域,点击"添加"定义外网区域"adsl-a"。

区域		
	区域	
可田居性·	名称 adsl_area * 访问权限 允许 ▼ 注释	
eth1 eth2 eth3 ads11 ads12		
	确 定 取 消	_

3) 配置基于属性的源 NAT 策略

选择 防火墙 > 地址转换,点击"添加"配置地址转换策略,使内网用户能够通过 ADSL 访问外网。

		添加地址转换	
模式		源转换	V
源			
	地址	任意	
	其它	<b>v</b>	
	VLAN	任意	
	区域		
		area_eth1	Ó
	端口	任意	
目的			
	地址	任意	
	其它	V	
	VLAN	任意	
	区域		
		adsl_area	í
服务		任意	
源地址	转换为	adsl [属性]	¥
源端口	不做转换	🔲 [源端口固定]	
规则描	述		
		确定 取消	

4) 拨号

选择 网络管理 > ADSL, 点击"开始拨号"便可建立 ADSL 连接。连接成功后的截 图如下。

链路名称	描述	状态	带宽	分配IP地址	对端IP地址	收到报文	发送报文	拨号持续时间	操作	设置属性
adsl		已连接	0	10.67.15.1	10.0.0.1	3	9	0:02:13	00	
adsl1	10	未连接			5. j		·			
ads12		未连接								
ads13		未连接								

拨号成功后,在网络卫士防火墙的路由表中会增加一条接口为 ppp0 的 ADSL 的路由 信息,如下图。

路由表 策略路由	动态路由OSPF	र का	态路由RIP	动态路	由BGP S播路	🖽 🔍 क्रोड़	S多播PIM
标记: V-Vp, G-Gateway spec Interface specified	ified, L-Local,	C-Connec	ted, S-Stat	ic O-Ospf,	R-Rip, B-Bgp, D-Dho	p, I-Ipsec,	i-
🕂 添加 🗴 清空						,ê	\$i <b>†: 13</b>
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除
172.16.1.1/32	0.0.0.0	ULi	1	1	10	-	-
10.1.10.1/32	0.0.0.0	ULi	1	1	10	-	-
192. 168. 83. 237/32	0.0.0.0	ULi	1	1	10	-	-
10. 10. 10. 1/32	0.0.0.0	ULi	1	1	10	-	-
10.67.15.1/32	0.0.0.0	ULi	1	1	10	-	-
10.0.0.1/32	0.0.0.0	UCi	10	1	рррО	-	-
10.0.0.1/32	0.0.0.0	UCi	100	1	ipsec0	-	-
172.16.1.0/24	0.0.0.0	UCi	10	1	eth1	-	-
10.1.10.0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-
192. 168. 83. 0/24	0.0.0.0	UCi	10	1	eth0	-	-
10.10.10.0/24	0.0.0.0	UCi	10	1	eth2	-	-
11.11.11.0/24	10. 1. 10. 1	UGSi	1	1	sslvpnO	-	3
0.0.0/0	10.0.0.1	UGSi	1	1	рррО	-	3

### 注意事项

1) 网络卫士防火墙只有在不指定默认网关的情况下才能自动按需拨号。如果网络卫 士防火墙上指定了默认路由,则 ADSL 拨号成功后会添加一条接口为 ppp0 的默认路由, 网络卫士防火墙上会存在两条默认路由,如下图所示。

路由表 策略路由	动态路由OSPF	🔪 动态	路由RIP	<b>动态路</b> 6	甘BGP 🔰 多播路(	🗄 🔪 को 🕯	S多播PIM
标记: U-Up, G-Gateway spe Interface specified	ecified, L-Local, C-	Connecte	d, S-Statio	c O-Ospf, R	-Rip, B-Bgp, D-Dhey	p, I-Ipsec,	i-
🕂 添加 🧴 清空						Ê	計:14
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除
172.16.1.1/32	0.0.0.0	ULi	1	1	10	-	-
10.1.10.1/32	0.0.0.0	ULi	1	1	10	-	-
192.168.83.237/32	0.0.0.0	ULi	1	1	10	-	-
10. 10. 10. 1/32	0.0.0.0	ULi	1	1	10	-	-
10.67.15.1/32	0.0.0.0	ULi	1	1	10	-	-
10.0.0.1/32	0.0.0.0	UCi	10	1	рррО	-	-
10.0.0.1/32	0.0.0.0	UCi	100	1	ipsec0	-	-
172.16.1.0/24	0.0.0.0	UCi	10	1	ethi	-	-
10.1.10.0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-
10.10.10.0/24	0.0.0.0	UCi	10	1	eth2	-	-
11.11.11.0/24	10. 1. 10. 1	UGSi	1	1	sslvpn0	-	3
0.0.0.0/0	10.0.0.1	UGSi	1	1	рррО	-	3
0.0.0.0/0	192. 168. 83. 1	UGSi	1	1	eth0	-	3

此时两条默认路由会分担流量,内网用户的拨号连接请求不能保证通过 ppp0 接口转发,因此拨号连接无法保证成功。

2) 一定不能在物理接口配置页面将 eth0 口与 adsl 属性绑定,否则无法拨号成功。

### GRE 通道配置

GRE 属于 VPN (Virtual Private Network )的第三层隧道协议,即在协议层之间采用 了一种被称之为 Tunnel (隧道)的技术,规定了如何用一种网络协议去封装另一种网络协 议的方法。GRE 的隧道由两端的源 IP 地址和目的 IP 地址来定义,允许用户使用 IP 包封 装 IP、IPX、AppleTalk 包,并支持全部的路由协议(如 RIP2、OSPF 等)。通过 GRE, 用户可以利用公共 IP 网络连接 IPX 网络、AppleTalk 网络,还可以使用保留地址进行网络 互连,或者对公网隐藏企业网的 IP 地址。

GRE 隧道主要用于两个边缘路由器或者终端系统与边缘路由器之间定期的安全通信链接。与 IPSec VPN 相比,GRE VPN 由于只是对报文的重新封装,并未进行加密,所以对路由器的性能影响较小,设备档次要求相对较低,但安全性比 IPSec VPN 较低。GRE VPN 适合一些小型点对点的网络互连,实时性要求不高、要求提供地址空间重叠支持的网络。

网络卫士防火墙支持 GRE (Generic Routing Encapsulation)协议并可以实现与 Cisco 设备之间建立 GRE 隧道相互通信。

#### 基本需求

背景: 某企业的两个分公司内网分别通过网络卫士防火墙 A、网络卫士防火墙 B 的 eth0 口与外网相连,其网络拓扑图如下图。



图 10 内网区域之间通过 GRE 隧道建立连接示意图

需求: 内网区 A (192.168.10.0/24) 要通过 GRE 隧道与内网区 B (172.16.1.0/24) 进行通信。

### 配置要点

- ▶ 分别在网络卫士防火墙 A 与网络卫士防火墙 B 上配置 GRE 隧道
- ▶ 分别在网络卫士防火墙 A 与网络卫士防火墙 B 上设置 GRE 隧道路由信息

### WEBUI 配置步骤

#### 网络卫士防火墙 A 上相关配置

1)选择 虚拟专网 > GRE,并点击"添加"添加 GRE 隧道 gre-AandB,如下图。

GRE		
	<b>GRE</b> 隧道	
名称	gre-AandB	━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
远程地址	202. 16. 8. 5	*
本地地址	202. 19. 9. 6	#
隧道关键字	12345	[0-4294967295]
隧道生存时间		[1-255]
校验和检查	□ 开启	
序列号检查	□ 开启	
	确定	取消

需要注意的是,两台网络卫士防火墙上的"KEY"必须相同。点击"确定"完成 GRE 隧道设置,如下图所示。

GRE									
☞ 添加	健 清空							总证	; <b>†: 1</b>
名称	远程地址	本地地址	隧道关键字	生存时间	序列号检查	校验和检查	接口属性	隧道属性	删除
gre-AandB	202. 16. 8. 5	202. 19. 9. 6	12345		off	off		2	3

2) 在上图中点击"接口属性"设置 GRE 虚接口的属性。

GRE		
	接口设置	
夕称	or o- 4 on dB	
状态		
接口地址	נהצו 🗆	
地址	掩码	
		添加
地址	掩码	删除
高级	V	
MTU	1380	[68-1500]
接口绑定	eth0	
虚系统ID	þ	[0-254]
	确定 取 ;	肖

3)选择 网络管理 > 路由,并在"静态路由"页签,点击"添加"添加静态路由, 如下图。

路由表 策略路由 动态路由OSPF 动态路由RIP
添加配置
目的地址 172.16.1.0 *
目的掩码 255.255.255.0 *
网关
接口 gre-AandB 🗨
高級
确 定 取 消

#### 在网络卫士防火墙 B 上相关配置

1)选择 虚拟专网 > GRE,并点击"添加"添加 GRE 隧道 gre-AandB,如下图。

GRE		
	GRE <b>隆</b> 道	
名称 远程地址 本地地址	gre-AandB gre-开头 203. 19. 9. 6 202. 16. 8. 5	*隧道名称必须以 * *
隧道关键字 隧道生存时间 校验和检查 序列号检查	12345     开启   开启	[0-4294967295] [1-255]
	确定 取消	

需要注意的是,两台网络卫士防火墙上的"KEY"必须相同。

点击"确定"完成 GRE 隧道设置,如下图所示。

GRE									
♂ 添加	健 清空							息	i <b>†: 1</b>
名称	远程地址	本地地址	隧道关键字	生存时间	序列号检查	校验和检查	接口属性	隧道属性	删除
gre-AandB	203, 19, 9, 6	202. 16. 8. 5	12345		off	off		2	3

2) 在上图中点击"接口属性"设置 GRE 虚接口的属性。

GRE			
	接口设置	ť	
名称 状态	gre-AandB		
接口地址			
地址	掩码 	添加	
地址	掩码	删除	
高级	V		
MTU	1380	[68-1500]	
接口绑定	eth0		
虚系统ID	p	[0-254]	
	确定	取消	

3) 设置路由信息。

添加 GRE 隧道后,会自动在网络卫士防火墙上添加与隧道同名的虚拟 GRE 接口(本 例中为 gre-AandB),需要管理员添加该接口的路由信息后,数据报文才会通过 GRE 隧 道。

选择 网络管理 > 路由,并在"静态路由"页签,点击"添加"添加静态路由,如 下图。

路由表 策略路由 动态路由OSPF	动态路由RIP
添加配置	
目的地址 192.168.10.0	*
目的掩码 255.255.255.0	*
网关	
接口 gre-AandB 🗨	]
高级	
确定即消	

至此, GRE 隧道配置完成, 内网区 A 中的主机便可与内网区 B 中的主机通过 GRE 隧道进行通信了。

### 注意事项

在设置 GRE 隧道时要保证两台网络卫士防火墙上的"KEY"相同。

### **PPTP** 隧道

### 基本需求

远程客户端与网络卫士防火墙建立 PPTP VPN 隧道,安全访问内网资源。





本例中网络卫士防火墙的 eth0 口连接内网区域 area\_eth0,禁止用户访问。eth1 口使用了私有 IP: 10.10.10.1/24,仅为示例,应用环境中,该接口 IP 应为用户可以访问的公网地址。

### 配置要点

- ▶ 配置远程用户
- ▶ 配置用户角色
- ▶ 开放相关接口的 PPTP 服务
- ▶ 配置 PPTP 服务
- ▶ 配置 PPTP 客户端
- ▶ 配置 PPTP 的访问控制

### WEBUI 配置步骤

1) 配置区域属性。

选择资源管理 > 区域,设置区域属性。

区域				
🕂 添加 🗴 清空				总计: 3
名称 🔶	绑定属性	权限 ◆	注释 ◆	操作
area_eth0	eth0	禁止	1	2
area_eth1	eth1	允许		
adsl_area	adsl	允许		

2) 配置远程用户。包括添加远程用户并设置用户角色。

a)选择 用户认证 > 用户管理, 在"用户管理"页签中点击"添加用户"添加用户 "pptpuser"。

用户管理 在线用户	用户设置	
	用户属性	
田白々	nntnur or	
认证方式	本地口令认证	V
口令	•••••	* [6-31个字符]
确认口令	•••••	*
可用角色	<u>я</u>	f属角色
doc_role ldap_HelpServicesGr ldap_TelnetClients ldap_IIS_WPG ldap_WINS_Users ldap_DHCP_Users ldap_DHCP_Administr ldap_Administrators	oup	
	□ 高级	
(	确定 电	2 消

b)为 PPTP 用户设置所属角色,不属于任何用户角色的用户无法通过认证服务器的认证。

选择 用户认证 > 角色管理,点击"添加角色"按钮,设置 PPTP 用户角色。

角色管理	
	角色属性
角色名 角色描述 DHCP地址池 法格田白	pptp_group * 不添加 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
DE3年用戸 IUSR_ADMIN-3B1012EB9 IWAM_ADMIN-3B1012EB9 ASPNET krbtgt u1 ftpuser u2 test doc_test	
高级	
	确定 取消

3) 开放 eth0 口的 PPTP 服务。

选择 系统管理 > 配置, 在"开放服务"页签中点击"添加"开放 PPTP 服务。

系统参数 开放服务 时间 SNMP 邮
添加配置
服务名称 PPTP 📃
控制区域 area_eth0 🔽
控制地址 any [范围]
确定取消

默认情况下,系统已经将 eth0 口添加到区域 area\_eth0。

4) 配置 PPTP 服务

选择 虚拟专网 > PPTP 菜单,在 "PPTP 设定"处设置 PPTP 服务属性,如下图。

рртр				
	PPTP设定			
本地地址	20. 0. 0. 1 *			
起始地址	20. 0. 0. 100 *			
结束地址	20. 0. 0. 200 *			
	☑ 要求数据加密			
应用	<b>启用</b> 停止			
	PPTP状态			
原始地址	指派地址			
PPTP停止				

需要**注意**的是: PPTP 服务器的"起始地址"、"结束地址"必须和"本地地址"在 同一个网段,且结束地址的值一定要大于等于起始地址。

设置完成后,需要首先点击"应用"按钮,然后点击"启动"按钮才能启动 PPTP 服务器。

5) 设置内网资源。

选择 资源管理 > 地址,并选择"主机"页签添加内网资源 webserver,如下图。

主机 范围	目 子网 地址組
	主机属性
名称 物理地址	webserver * 00:00:00:00:00
TP地址	192. 168. 83. 234 <- X
	确 定 取 消

6) 对远程 PPTP 客户端作访问控制

对于远程 PPTP 客户端的访问控制可以通过对 PPTP 区域的控制完成,也可以通过对 包含 PPTP 远程用户的用户角色的访问控制来完成。

通过对 PPTP 区域的控制完成访问控制。

a)	选择	资源管理	>	区域,	添加区域 pptp_area。
----	----	------	---	-----	-----------------

区域	
	区域
	名称 pptp_area * 访问权限 允许 ▼ 注释
可用属性: lan ssn ppp l2tp bond0	成员: -> × 、 、 、 、 、 、 、 、 、 、 、 、 、
	确 定 取 消

pptp\_area 区域可以作为源或目的区域在访问控制规则中使用。

"pptp"属性是 PPTP 的动态属性,不需要用户设置,用户只需要设置该属性绑定的 区域即可。

b)选择 防火墙 > 访问控制,点击"添加策略"设置访问控制规则。

		添加访问控制策略	
源			
	区域	pptp_area	 €
	地址	任意	
	其它		
目的			
	区域	area_eth0	_ <u>∕</u>
	地址	wahsarvar	
	其它		
服务		任意	
动作 日志证	渌	<ul> <li>○ 允许</li> <li>○ 禁止</li> <li>○ 收集</li> <li>○ 不记录</li> <li>○ 记录</li> <li>○ 系统报警</li> </ul>	
连接选 保护内	:项  容表  級	□ 长连接           无         ▼	

#### 通过基于认证用户角色的访问控制来实现对 PPTP 用户的访问控制。

在设置访问控制规则时,用户也可选择源为用户角色,如下图。

访问控制	
	添加访问控制策略
源	
区域	
	area_eth1
地址	任意
其它	
角色	
	pptp_group
VLAN	任意
端口	任意
目的	
区域	
	area_eth0
地址	
	webserver
其它	
服务	任意
动作	● 允许 C 禁止 C 收集
日志记录	◎ 不记录 ○ 记录 ○ 系统报警
连接选项 (G. 拉内尔吉	
「 高绒	7u 💌
- 1 1	
	确定取消

其他的设置与基于区域的访问控制规则相同。

7) 配置 PPTP 客户端(以 windows 2000 为例)

需要确认 PPTP 客户端可以访问网络卫士防火墙的 eth1 接口。

a) 在控制面板中打开网络连接

S 网络连接	×
文件 (E)编辑 (E) 查看 (Y) 收藏 (A) 工具 (E) 高级 (B) 帮助 (H) 🥻	7
🚱 后退 ▼ 🕥 - 🏂 🔎 搜索 🍋 文件夹 🛄 -	
地址 (2) 🛸 网络连接 🛛 🚽 转到 链接	»
<ul> <li>网络任务</li> <li>② 创建一个新的连接</li> <li>③ 设置家庭或小型办公网络</li> <li>● 更改 Windows 防火墙</li> <li>● 内网</li> </ul>	
相关主题	
(1) 网络疑难解答程序	
其它位置 *	
<ul> <li></li></ul>	
洋细信息	
6 个对象	

b) 点击"创建一个新连接",新建一个连接(VPN)。



c)选择网络连接类型为"连接到我的工作场所的网络"。

新建连接向导
<b>网络连接</b> 您想要在工作点如何与网络连接?
创建下列连接:
<ul> <li>○ 拔号连接 (D)</li> <li>用调制解调器和普通电话线连接,或通过综合业务数字网(ISDN)电话线连接。</li> <li>④ <u>虚拟专用网络连接 (V)</u></li> <li>使用虚拟专用网络(VFN)通过 Internet 连接到网络。</li> </ul>
〈上一步(8)下一步(8)〉 取消

d)选择创建"虚拟专用网络连接"。

新建连接向导	
<b>连接名</b> 指定连接到您的工作场所的连接名称。	Ì
在下面框中输入此连接的名称。	
公司名 (A)	
PPTP连接	
例如,您可以输入您的工作地点名或您连接到的服务器名。	
< 上一步 (8) 下一步	(2) > 取消

e) 输入为此 VPN 连接定义的名字(例如 PPTP 连接)。

新建连接向导
<b>公用网络</b> Windows 可以先确认公用网络是否已接好。
Windows 在建立虚拟连接之前可以自动拨到 Internet 或其它公用网络的初始 连接。
● 不拔初始连接 @)
○ 自动拨此初始连接 (A):
▼
< 上一步 (B) 下一步 (B) > 取消

f)如果在拨 VPN 之前需要拨公网,可以选择是拨 VPN 同时自动启动公网连接还是 先连接公网以后,再进行 VPN 连接。

新建连接向导
VPN 服务器的名称或地址是什么?         Image: Control of the second secon
输入您正连接的计算机的主机名或 IP 地址。
主机名或 IP 地址(例如,microsoft.com 或 157.54.0.1)(H):
10. 10. 10. 1
< 上一步 (B) 下一步 (D) > 取消

g) 输入网络卫士防火墙上开放 PPTP 服务的接口的 IP 地址,此例中为 10.10.10.1, 如上图所示。



h) 点击"完成"完成设置,会出现该连接,右键修改其属性。



◆ PPTP连接 雇性
常规 选项 安全 网络 高级
目的地的主机名或 IP 地址(如 microsoft.com 或 157.54.0.1)(出):
10. 10. 1
第一次连接 在试图建立虚拟连接之前,Windows 可以先连接到公用 网络,如 Internet 上。
□ 先拨另一个连接 @):
☑ 连接后在通知区域显示图标(₩)

PN 类型(E):	- 1	
PTF VPR	VPN连接类型为 PPTP	〕 设置(S)
☑ — Internet 协ì ☑ — QoS 数据包计 ☑ — Microsoft 网 ☑ — WMware Bridg	义(TCP/IP) ·划程序 ]络的文件和打印机共 ge Protocol	淳
安装(图)	卸載①	<b>属性</b> (E)
描述 Netmon 数据包捕获	失驱动程序允许 Netm 数据包。	on 用户界面获



8) 建立 PPTP VPN 隧道

输入已在网络卫士防火墙上设好的远程用户的用户名(pptpuser)和密码,点击连接 按钮。

连接 PPTP连接		? ×
用户名 (1):	pptpuser	
密码(E):	****	
☑ 为下面用户	P保存用户名和密码(S):	
ⓒ 只是我	(H)	
○ 任何使用	用此计算机的人 (A)	
连接 (C)	取消 属性 (0)	帮助(H)

连接成功后如下图。

● PPTP连接 状态			?	×
常规 详细信息				
注接 状态: 持续时间:			已连接上 00:00:11	
- 活动	发送 ——	<u>-</u>	收到	
字节: 压缩: 错误:	1,897 0 % 0		374 0 % 0	
属性の	断开 @)			
			关闭(C)	

9)网络卫士防火墙上可以通过 虚拟专网 > PPTP 来查看已建立 PPTP 隧道的客户端状态。

РРТР		
PPTP 设	定	
本地地址 20.0.0. 起始地址 20.0.0. 结束地址 20.0.0. □ 要求	1 * 100 * 200 * 数据加密	
应用	用 停止	
рртр状	态	
原始地址	指派地址	
192. 168. 83. 224 20. 0. 0. 100		
隧道总数:1		

管理员可以通过选择 **用户管理 > 用户认证**,并激活"在线用户"页签查看当前在 线用户。

用户管理	在线用户	用户设置	i			
						总计 <b>:</b> 1
用户名	地址	服务器	在线时间(HH:MM:SS)	类型	删除此地址	删除此用户
pptpuser	20.0.0.100	localdb	0:0:10	pptp	-	-

### 注意事项

1) 客户端(win2000) 可用 ipconfig /all 命令查看 PPTP 隧道分配的 IP。

```
PPP adapter pptpvpn:
       Connection-specific DNS Suffix
                                        . :
       Description . . . . . . .
                                          : WAN (PPP/SLIP) Interface
       Physical Address.
                                          : 00-53-45-00-00-00
       DHCP Enabled. . .
                                            No
        IP Address. . .
                                          : 172.16.200.101
       Subnet Mask . .
                                          : 255.255.255.255
       Default Gateway .
                                            172.16.200.101
       DNS Servers .
```

2) 客户端(win2000) 可用 route print 查看本地路由表。

224.0.0.0	224.0.0.0	172.16.200.101
224.0.0.0	224.0.0.0	192.168.42.1
224.0.0.0	224.0.0.0	192.168.133.1
255.255.255.255	255.255.255.255	192.168.42.1
Default Gateway:	172.16.200.101	
	===================	, ====================================
Persistent Routes:		

3) PPTP 设定的"本地地址"、"起始地址"与"结束地址"不要使用任何已用的 IP。

4) PPTP 隧道成功连接后,如果客户端不能正常访问内网资源,请检查从内网资源到 网络卫士防火墙的路由设置,确保该内网资源的返回数据包可以到达网络卫士防火墙。

### L2TP 隧道

L2TP 隧道的配置和 PPTP 隧道的配置类似,值得说明的是在 windows 的客户端必须 安装一个 TOPSEC 提供的小程序,该程序在网络卫士防火墙随机光盘和 TOPSEC 的网站 上均可获取。



安装该程序后,必须重启系统才可以生效。

运行该程序,如下图。

사 L2TP 设置	
TOS/L2TP 连接配置 ✓ 允许 TOS 到 L2TP 的连接 (2) 修改 TOS 到 L2TP 的连接配置需要重新启动机器才 能起作用。	
确定	

选中"允许 TOS 到 L2TP 的连接"。

客户端上 L2TPVPN 隧道的配置步骤与 PPTP 基本一致,只需要修改 VPN 隧道的属性为"L2TP",如下图。

◆ L2TP连接 届性 ? ×
常规 选项 安全 网络 高级
VPN 类型 (E):
L2TP IPSec VFN
设置 (S)
此连接使用下列项目 (0):
<ul> <li>✓ Y Network Monitor Driver</li> <li>✓ W Internet 协议 (TCP/IP)</li> <li>✓ 및 QoS 数据包计划程序</li> <li>✓ 및 Microsoft 网络的文件和打印机共享</li> <li>✓ 및 VMware Bridge Protocol</li> </ul>
<b>安装 (2) 卸載 (2)</b> 属性 (2)
描述 Netmon 数据包捕获驱动程序允许 Netmon 用户界面获 取来自本地网络的数据包。

详细配置请参考 PPTP 案例。

# 带宽管理

通过在访问控制规则中引用预先定义的 QoS 对象,或直接在 ACL 规则中定义"限制 带宽"(仅针对下行数据),网络卫士防火墙实现带宽的集中管理。同时,还可以根据业 务需求,设置带宽策略的优先级,为关键业务流量优先分配带宽,从而合理、有效地为用 户网络分配带宽资源。


图 12 网络卫士防火墙分层带宽管理示意图

### 基本需求

子网1(10.10.10.0/24)连接在防火墙的 Eth2 口,通过 Eth0 口访问 FTP 服务器(192.168.83.234/24),通过 Eth1 口连接 Internet,链路带宽为 28K。子网1为研发部门所在网段,分为普通员工、配置人员和经理三类人员,通过设置带宽管理策略,要求:

(1) 在工作时间内,配置人员和普通员工通过 Eth1 口连接外网,共享 15K 限制带宽,不保证带宽;

(2)研发部经理级员工每人独享 5K 的限制带宽,3K 的保证带宽。优先保证经理的外网连接;

(3) 子网1内的每个人员,向 FTP 服务器上传数据时独享 7K 限制带宽,但总的限制带宽不超过 18K;从 FTP 服务器下载数据时每个员工独享 8K 限制带宽,总的限制带宽不允许超过 20K;

(4)子网1内的配置人员、员工和经理均可访问 BugZilla 服务器,要求分别单独享有3K 的限制带宽。而且访问 BugZilla 的优先级高于访问 FTP 服务器。

## 配置要点

带宽策略的设置包括以下方面:

- ▶ 设置资源
- ▶ 设置 QoS 对象,以及出接口的保证带宽。
- ▶ 设置 ACL 规则并引用 QoS 对象。

## WEBUI 配置步骤

1) 设置资源对象

a) 设置"时间"资源。用户可以根据目己的需求,通过 <b>资源管理 &gt; 时</b>
---

时间多次时间单次	
	时间属性
名称	work_time *
毎周时段	
	星期→ ▼
	星期二 ▶
	星期三 ▶
	星期四 ▶
	星期五 ▶
	星期六 🔽
	星期日 🔽
毎日时段	
	开始时间时 09 💌 *分 00 💌
	结束时间 时 17 💌 *分 30 💌
	确定 取消

b) 设置范围地址对象

选择资源管理 > 地址,并激活"范围"页签进行设置,设置完成后界面如下图。

主机 范	主机 范围 子网 地址组						
➡ 添加							
名称 ◆	起始地址    ◆	终止地址 🔶	排除地址 🔶	操作			
any	0. 0. 0. 0	255. 255. 255. 255		2			
nat-pool	202. 10. 10. 1	202. 10. 10. 10		23			
配置人员	10. 10. 10. 201	10. 10. 10. 210		2 3			
普通员工	10, 10, 10, 11	10, 10, 10, 200		🕗 🗿			
研发经理	10. 10. 10. 2	10. 10. 10. 10		2 3			

C) 设置 FTP 服务器和 BugZilla 服务器

选择资源管理 > 地址,并激活"主机"页签进行设置,设置完成后界面如下图。

主机 范围 子网 地址组						
➡ 添加 前 清空						
		总计 <mark>: 1</mark> 1				
名称	IP地址 ◆	操作				
ftpserver	192. 168. 83. 234	23				
bugserver	192. 168. 83. 221	23				

2) 在工作时间内,配置人员和普通员工通过 Eth1 口连接外网,共享 15K 限制带宽, 不保证带宽。

添加 QoS 对象然后在 ACL 规则中引用 QoS 对象来配置规则;

a)选择 网络管理 > 流量管理,选择 "QoS"页签,点击"添加",设置 QoS 对象。 上行的限制带宽为 15K,优先级为"中",配置界面如下图。

		QOS策略属性		
	策略名称	share_outer	*	
下行	共享 💽	优先级	中 🔽	
		保证带宽		
		限制带宽		
上行	共享 👤	优先级	<b>中 ▼</b>	
		保证带宽		
		限制带宽	15	
	(默认单位为KBps)			
确定 取消				

之后,选择 防火墙 > 访问控制,点击"添加策略"设置访问控制规则,设置完成 后界面如下图所示。

访问控制								
目的区域	目的区域 所有区域 🗨 策略組 所有组 💌 高级搜索 🔲 显示策略统计							
🕂 添加	组 🕂	添加策略			总计: 2	毎页: 30条 👤		
ID	控制	源	目的	服务	选项	操作		
8049	~	区域: area_eth2 地址: 普通员工	区域: area_eth1		QOS:share_outer 时间:work_time			
8046	8046 V V Area_eth2 区域: area_eth2 区域: 地址: 配置人员 area_eth1 V POS:share_outer 时间:work_time V POS:share_outer							
	M 《 1 》 N 转到 /1 Go							

上图中, ID 为 8046 和 8049 的规则引用"策略类型"为"共享"的 QoS 对象 share\_outer,因此匹配规则的源地址对象——"配置人员"和"普通员工"中的所有地址对象在工作时间内共同分享 15K 的限制带宽。

#### 需要注意的是:

- ▶ 如果在 QoS 策略中设置了保证带宽,则引用该 QoS 策略的 ACL 规则必须设定"目的区域"(针对上行数据)或"源区域"(针对下行数据)。
- ▶ 如果 share\_outer 的策略类型为"策略独享",上述两条 ACL 规则同样表示普通员工和配置人员分别共享 15K 的限制带宽。

4)研发部经理级员工也通过 Eth1 口连接外网,每人独享 5K 的限制带宽,3K 的保证带宽。而且在分配带宽上,经理比普通员工享有优先权。

a)设置出接口的保证带宽。当需要保证带宽时必须设置。

选择 网络管理 > 流量管理,选择 "QoS 对象"页签,在"接口有效带宽"处点击 "添加",添加采用上传带宽配置策略的物理接口 eth1。

Qos对象	印流量	地址统计	端口统计
接口带宽			
接口名称:	eth1	•	
带宽:	500		KBps 💌
确定		取消	)

接口的配置原则是以数据流流向为准,在数据流出网络卫士防火墙的物理接口上配置 才能生效,本例中即 eth1 接口。

b)选择 网络管理 > 流量管理,选择 "QoS 对象"页签,点击"添加",设置 QoS 对象,策略类型为"独享",上行的保证带宽为 3K、限制带宽为 5K,优先级为"特权",如下图;

		QOS策略属性	
	策略名称	manager	*
下行	策略独享 ▼	优先级	中
		保证带宽	
		限制带宽	
上行	独享 ▼	优先级	特权
-		保证带宽	ЗК
		限制带宽	5K
	(默认单位为KBps)	-	
		确定	取消

需要注意的是:每个 QoS 对象中保证带宽不能大于限制带宽。

访问控制	访问控制					
目的区域	所有区域	☆ ▼ 策略组 所	有组 🔹 高级搜索	Ŕ	🔲 显示策略统计	
🕂 添加約	1 + i	忝加策略			总计:3 毎页: 30条	-
ID	控制	源	目的	服务	选项	操作
8049	•	区域: area_eth2 地址: 普通员工	区域: area_eth1		QOS:share_outer 时间:work_time	<b>2</b> •
8050	•	区域: area_eth2 地址: 研发经理	区域: area_eth1		QOS:manager	<ul> <li>•</li> </ul>
8046	8046 V V V V V V V V V V V V V V V V V V V					
	K < 1 ▶ N 转到 /1 Go					

c)在ACL规则中引用QoS对象。

当"研发经理"对象中的 IP 地址访问外网时,每个 IP 地址单独享有 3K 的保证带宽、5K 的限制带宽。

5) 子网 1 内的每个 IP 地址,向 FTP 服务器上传数据时独享 7K 限制带宽,但总的限制带宽不超过 18K;从 FTP 服务器下载数据时每个员工独享 8K 限制带宽,总的限制带宽不允许超过 20K。

a) 设置 QoS 对象,界面如下图所示。

QOS策略雇性							
策略名称	ftp_qos	*					
下行 受控 💌	优先级	低					
	总限制带宽	20					
	毎主机限制帯宽	8					
上行 受控 💌	优先级	<u></u>					
	总限制带宽	18					
	毎主机限制帯宽	7					
(默认单位为KBps)							
确。		2消					

B) 配置 ACL 规则引用 QoS 对象。

访问控制							
目的区域	目的区域 所有区域 💌 策略組 所有组 💌 高級搜索 🔲 显示策略统计						
╋ 添加約	e + 2	添加策略			总计:4 毎页: 30条	-	
ID	控制	源	目的	服务	选项	操作	
8052	v	区域: area_eth2 地址: 普通员工 配置人员 研发经理	区域: area_eth0 地址: ftpserver		QOS:ftp_qos 时间:work_time	<ul> <li>•</li> </ul>	
8049	-	区域: area_eth2 地址: 普通员工	区域: area_eth1		QOS:share_outer 时间:work_time	<ul> <li>*</li> </ul>	
8050	1	区域: area_eth2 地址: 研发经理	区域: area_eth1		QOS:manager	<ul> <li>•</li> </ul>	
8046	1	区域: area_eth2 地址: 配置人员	区域: area_eth1		QOS:share_outer 时间:work_time	<ul> <li>*</li> </ul>	
					₩ ◀ 1 ▶ ₩ 转到	/1 Go	

"源地址"选择"配置人员"、"普通员工"和"研发经理", QoS 对象选择"ftp\_qos",因此匹配该 ACL 的所有源地址对象向 FTP 服务器上传文件匹配"上行"规则、下载数据时匹配"下行"规则。

6) 子网 1 内的配置人员、员工和经理访问 BugZilla 服务器时,所有配置人员共享 3K 的限制带宽,所有的员工和所有的经理也分别共享 3K 限制带宽。而且访问 BugZilla 的优 先级高于访问 FTP 服务器。

a)选择 网络管理 > 流量管理,选择 "QoS 对象"页签,点击"添加",设置 QoS 对象。上行的限制带宽为 3K,不设保证带宽,优先级为"特权",配置界面如下图。

		QOS策略属性	
	策略名称	bug_qos	*
下行	策略独享 💌	优先级	中 💌
		保证带宽	
		限制带宽	
上行	策略独享 ▼	优先级	特权
-		保证带宽	
		限制带宽	ЗК
	(默认单位为KBps)		I
	研		<b>収消</b>

之后,选择 防火墙 > 访问控制,点击"添加策略"设置访问控制规则,设置完成 后界面如下图所示。

访问控制						
目的区域 所有区域 ▼ 策略组 所有组 ▼ 高級搜索 □ 显示策略统计						
╋ 添加	+ 添加策略       急计:8 每页: 30条					
ID	控制	源	目的	服务	选项	操作
8058	•	区域: area_eth2 地址: 研发经理	区域: area_eth0 地址: bugserver		QOS:bug_qos 时间:work_time	
8057	v	区域: area_eth2 地址: 普通员工	区域: area_eth0 地址: bugserver		QOS:bug_qos 时间:work_time	
8056	•	区域: area_eth2 地址: 配置人员	区域: area_eth0 地址: bugserver		QOS:bug_qos 时间:work_time	
8046	•	区域: area_eth2 地址: 配置人员	区域: area_eth1		QOS:share_outer 时间:work_time	
8054	1				QOS:总带宽限制:3KBps;每主机带宽限制:	
M 《 1 ▶ M 转到 /1 Go						

上图中, ID 为 8356、8357 和 8358 的规则都引用"策略类型"为"策略共享"的 QoS 对象 bug\_qos, 表示各个规则彼此独立,不共享带宽;但是每一条规则的源地址对象中包含的所有地址对象共同分享 3K 的限制带宽。

需要特别注意的是,此处不能在 ACL 规则中"源地址"处同时选择"配置人员、普通员工和研发经理"来合并 3 条规则,合并后设置的 ACL 规则表示所有的配置人员、普通员工和研发经理共享 3K 的限制带宽。

## 注意事项

1)网络卫士防火墙的带宽单位 Bps 指的是字节/秒,不是通常的比特/秒。

2)网络卫士防火墙的带宽管理指的是出口带宽,且只能对经网络卫士防火墙转发的 流量进行限制。

# 用户认证

用户认证的主要目的是为了对用户进行身份鉴别、授权以及进行细粒度的访问控制, 比如进行基于认证用户的访问控制和 HTTP 会话认证。用户认证的方式主要包括本地认证 (密码和证书)和第三方认证(Radius、Tacacs、SecurID、LDAP 以及域认证等等)。

成功配置用户认证有几个基本前提,一是在相关接口开启认证服务,二是根据认证方 式设置不同的认证服务器。

# 本地密码认证

## 基本需求

用户通过 TopSEC 认证客户端在网络卫士防火墙上进行认证。



图 13 认证示意图

## 配置要点

- ▶ 开放区域 area\_eth1 的认证服务
- ▶ 增加用户
- ▶ 验证

## WEBUI 配置步骤

1) 开放区域 area\_eth1 的认证服务

选择 系统管理 > 配置 菜单,在"开放服务"页签点击"添加"开放 AUTH 服务。

系统参数 开放服务 时间 SNMP 邮件设置
添加配置
服务名称 AUTH
控制区域 area_eth1 🛛 🗸
控制地址 any [范围]
确 定 取 消

2) 增加用户(user1)

选择 用户认证 > 用户管理 菜单,并在"用户管理"页签中点击"增加用户"添加 名称为 user1 的用户。

用户管理 在线用户 用户设置				
用户雇性				
用户名	user1 *			
认证方式	本地口令认证			
口令	●●●●●●● * [6-31个字符]			
确认口令	*			
可用角色	所属角色			
doc_role     Idap_KelpServicesGroup       ldap_TelnetClients     ->       ldap_IIS_WPG     ×       ldap_DHCP_Users     Idap_DHCP_Vsers       ldap_DHCP_Administrators     •				
□ 高级				
确 定 取 消				

- 3) 验证
- a)在主机 A 运行 TopSEC 认证客户端,界面如下图。

TOPSEC认证客户端				
🛛 🚠 认证登录	₹			
认证方式 僆	用密码认证			
用户名(图)	user1			
密码(P)	*****			
▶ 保存密码	□ 开机启动 🔽 自动重连			
   状态:未登录				
登录(I)	注销 (1) <b>设置 (2) 退出 (2)</b>			

b) 点击"设置", 输入防火墙的接口 IP。

登录设置	×
┌认证设备信息	
设备地址(12) 10 . 10 . 10 . 1	
认证方式 密码认证 🔽	
● 普通认证   ○ 0tp认证   ○ SecurID认证 确认     取消	

c)输入用户名 user1 及密码,点击"登录"按钮,用户认证通过,登录设备成功后 会在任务栏显示金色小钥匙。

📄 🙆 💓 Internet	
J: 🗲 🚇 🔧 🔇 😻 🕬	14:41

d) 查看在线用户

通过选择菜单 用户认证 > 用户管理,并点击"在线用户"页签查看通过认证的用户。

用户管理 在线用户 用户设置						
						总计 <b>: 2</b>
用户名	地址	服务器	在线时间(HH:MM:SS)	类型	删除此地址	删除此用户
user1	10. 10. 10. 22	localdb	0:0:54	common	0	3
doc	172.16.1.2	localdb	0:5:43	sv	-	-

至此,该案例验证通过。

# 第三方 RADIUS 服务器认证

### 基本需求

CGI 用户以 HTTP(8000 端口)方式在网络卫士防火墙上通过第三方服务器(Radius Server, 192.168.83.234,认证端口 UDP 1812)进行身份认证。



图 14 RADIUS 身份认证网络示意图

### 配置要点

- ▶ 设置认证服务器
- ▶ 设置认证用户角色
- ▶ 开放相关接口的认证服务
- ▶ 设置映射策略
- ▶ 设置认证客户端软件

### WEBUI 配置步骤

1) 设置 Radius 认证服务器

选择菜单 用户认证 > 外部认证,点击"添加服务器",设置 Radius 认证服务器相关参数,如下图。

认证服务器属性					
服务器名称 radius 认证协议 RADIU 认证服务器地址 192.16 认证服务器端口 1812	s_server 5 <b>v</b> 8. 83. 234	* * *			
超时时间 秒] 预共享密钥 ●●●●		[5-180秒, 武省万5 *			
认证客户端地址 0.0.0.0					
认证方法 PAP	•				
确定	□ □ 取 消	¥			

### 需要注意: "预共享密钥"字段需要和第5)步中 RADIUS 服务器上的设置一致。

### 2) 设置 Radius 认证用户角色

设置认证用户角色的主要目的是将外部服务器的用户映射到本地角色,基于用户角色 对外部用户作访问控制。

选择菜单 用户认证 > 角色管理,点击"添加角色"添加 Radius 用户角色。

角色管理				
角色属性				
角色名 角色描述 DHCP地址池	radius_role * 不添加			
选择用户	已经选择			
doc letp_user lp Guest SUPPORT_388945a0 IUSR_ADMIN-3B1012EB9 IWAM_ADMIN-3B1012EB9 ASPNET krbtgt				
	□ 高级配置			
	确 定 取 消			

3) 开放 eth1 口的认证服务

选择菜单 系统管理 > 配置,选择"开放服务"页签,开放 area\_eth1(系统中,已 将 eth1 口加入区域 area\_eth1)区域的认证服务。本例中客户端使用 IE 浏览器,通过 8000 端口登录防火墙,故需要开放 CGI 服务。如果使用 Topsec 认证客户端,则需开放 auth 服 务。

系统参数 开放服务 时间	SNMP
添加配置	
服务名称: CGI	•
控制区域: area_eth1	•
控制地址: any [范围]	•
确定 取消	

4) 设置映射策略。

选择菜单用户认证 > 认证设置,点击"添加映射"添加 Radius 服务器的映射策略。

认证设置				
映射属性				
本地角色集合 ldap_RAS_and_IAS_Set ldap_Server_Operato ldap_Account_Operat ldap_DnsAdmins ldap_DnsUpdateProxy ldap_group1 ldap_iiii pptp_group	认证服务器名称 是否启用 授权类型 rvers rs ors	radius_server         是         本地角色集合映射         已经选择         ▲         ▲         ▲         ▲         ▲         ▲         ▲         ▲         ●		
	确定	取消		

5) Radius 服务器的相关设置。

本例中使用 WinRadius 服务器作为 Radius 服务器。

a)运行 WinRadius.exe 程序,如下图。

STinRadius - 无标题	
操作日志 高级 设置 查看 帮助	
) 🗅 📽 🖬 🛛 🗙 🕂 —	₽ <b>,\$</b>
ID 时间	消息
1 2008年1月23日11时32分29秒 2 2008年1月23日11时32分29秒 3 2008年1月23日11时32分29秒 4 2008年1月23日11时32分29秒 5 2008年1月23日11时32分29秒	认证服务启动失败,诸使用其它端口。 计费服务启动失败,诸使用其它端口。 LDAD DB : 未发现数据源名称并且未指定默认驱动程序 诸使用"设置/数据库"为您的 RADIUS 数据库设置ODBC 加载账户数据失败。
	<b>&gt;</b>
就绪	数字 ///

### b)选择 设置 > 系统, 弹出如下窗口。

系统设置	×
NAS 密钥:	aaa
认证端口:	1812
计费端口:	1813
🗆 在系统启动时自动	加载
□ 启动时最小化窗口	l i i i i i i i i i i i i i i i i i i i
确定	

NAS 密钥是共享密钥,在此,需要和防火墙上的设置一致。

c)选择 操作 > 添加帐号,添加 radius 用户,如下图。

添加账号	×
用户名:	snap
密码:	111111
组名:	
地址:	
預付金額:	0 分钱
到期日:	
注意: yyyy/mm/dd表表 接入开始的有效夭数:	下到期日:数字表示从第一次 空白表示永不过期。
○ 預付费用户	⊙ 后付费用户
计费方法:	按时间计费 🗾
确定	取消

5) 设置用户认证客户端

a)在参与认证的主机上,Radius 服务器上设置的用户"snap"在主机上通过HTTP的 8000 端口向网络卫士防火墙进行认证。



b)登录成功后,界面如下图所示。



c)用户可以通过选择菜单 用户认证 > 用户管理,并点击"在线用户"页签查看 通过认证的 CGI 用户,如下图所示。

用户管理	· 在线用户	用户设置				
						总计: 2
用户名	地址	服务器	在线时间(HH:MM:SS)	类型	删除此地址	删除此用户
snap	10. 10. 10. 22	radius_server	0:0:10	cgi	0	3
doc	172.16.1.2	localdb	0:18:57	sv	_	-

配置完成。

### 注意事项

1)保证网络卫士防火墙和 Radius 服务器的正常通信,网络卫士防火墙需要访问 Radius 服务器的认证端口(一般是 UDP:1812)。

2)保证客户端和网络卫士防火墙之间的正常通信,客户端需要访问网络卫士防火墙的 UDP:10000 及 UDP:20000 端口。

3)网络卫士防火墙可以设置基于认证用户的访问控制规则,只需在源/目的处选择相应的用户角色便可。

# 证书认证

网络卫士防火墙的证书认证是通过导入证书管理软件生成的 CA 根证书和 CRL 列表 对客户端进行认证。

### 基本需求

用户使用认证客户端软件,在网络卫士防火墙上内置的 CA 对客户端进行证书认证。



图 15 采用证书认证网络示意图

### 配置要点

- ▶ 内置 CA 为客户端颁发证书
- ▶ 设置认证用户角色
- ▶ 设置映射关系,将证书用户按照某个属性映射到 LocalDB 的角色上。
- ▶ 开放相关接口的认证服务

▶ 设置认证客户端软件

## WEBUI 配置步骤

1) 生成并下载证书

a)选择菜单 **PKI 设置 > 本地 CA 策略**,并选择"签发证书"页签,点击"生成新 证书",为客户端签发证书。

根证书 签发证书 证书撤销	列表
	签发证书
夕称	Thomas an
日初	
省	
城市	
电子邮件	
组织	
单位	
失效时间	[输入格式:YYYY/MM/DD]
	确定取消

生成后界面如下图所示。

根证书	签发证书 证书撤销列表						
@ 生成新证书	弓 🕝 全部导出 📿 清空证书						总计 <b>: 3</b>
证书	有效起止日期	状态	属性	下载	写入	撤销	删除
webui	Sep 04 07:27:23 UTC 2009- Sep 02 07:27:23 UTC 2019	1	<b></b>	ß	I	3	3
doc	Sep 01 08:03:29 UTC 2009- Aug 30 08:03:29 UTC 2019	1	A state	ß	I	3	3
ZhangSan	Sep 09 07:54:01 UTC 2009- Sep 07 07:54:01 UTC 2019	1	A state	ß	l)	3	3

b) 下载证书

点击"下载"图标,界面如下图。

根证书 签发证书 证书撤销列表
导出签发证书
证书类型 PEM格式 ▼ 导出证书
返回

然后选择证书类型,点击"导出证书",将证书下载到管理主机本地,界面如下图。

	根证书 签发证书 证书撤销列表
	导出签发证书
	证书类型 PEM格式 ▼ 导出证书
-	返回
	私钥点击下载[或用右键另存]

按照提示将用户证书和私钥下载到本地。

2) 添加本地用户角色,基于角色对证书认证的用户进行权限控制。

选择 **用户认证 > 角色管理**, 点击"添加角色"添加证书认证用户对应的角色,用 于证书认证权限映射,基于角色进行权限控制。

角色管理	
	角色属性
角色名 角色描述信息 DHCP地址池	cert_role * /
选择用户	已经选择
doc letp_user lp Guest SUPPORT_388945a0 IUSR_ADMIN-3B1012EB9 IWAM_ADMIN-3B1012EB9 ASPNET krbtgt	
	□ 高级配置
	确 定 取 消

### 说明:

如果认证客户端为 VRC 客户端,而且管理员设置"证书权限控制"和"验证控制证 书权限"均为"OFF"时(选择菜单 **虚拟专网 > VRC 管理**,并点击"基本设置"页签), 将对 VRC 用户授权默认权限,无需设置本地用户角色。

3) 设置证书用户到 LocalDB 的用户角色的认证映射策略,本例中所有的证书用户授 予相同的访问权限。

选择用户认证 > 认证设置,如下图所示。

认证设置					
➡ 添加映射 ● 清空映	討				
					总计 <b>: 3</b>
服务器名	状态	修改	上移	下移	删除
cert	启用	10000000000000000000000000000000000000	-	-	-
localdb	启用	-	t	1	-
radius_server	启用		t	Ĵ	3

a)所有的证书用户授予相同的访问权限,则点击"cert"服务器对应的修改图标,设置映射关系。

认证设置		
		映射属性
本地角色集合	认证服务器名称 是否启用 授权类型	cert 是 本地角色集合映射 已经选择
ldap_Server_Op ldap_Account_O ldap_DnsAdmins ldap_DnsUpdate ldap_group1 ldap_iiii pptp_group radius_role	erators perators Proxy	<pre>cert_role X </pre>
	确;	E 取消

4)开放 area\_eth1 区域的认证服务(系统默认已将 eth1 口加入区域 area\_eth1)

选择菜单 **系统管理 > 配置**,激活"开放服务"页签,点击"添加"开放 area\_eth0 区域的认证服务。

系统参数 开放服务 时间	SNMP 邮件设置
添加配置	
服务名称 AUTH	•
控制区域 area_eth1	•
控制地址 any [范围]	-
确定	取消

5) 设置用户认证客户端

在参与认证的主机上,安装随机光盘里的 Topsec 客户端认证软件。启动该软件,界 面如下图所示。

TOPSEC认证客户端
│
认证方式 使用密码认证
用户名(M) test
密码 ( <u>e</u> ) ******
▶ 保存密码 ▶ 开机启动 ▶ 自动重连
登录(L) 注销(D) 设置(S) 退出(A)

点击"设置"按钮,将认证方式设为证书认证,如下图。

登录设置		×
┌ 认证设备信息 — 设备地址 ⑪)	10 . 10 . 10 . 1	
认证方式	证书认证	
	确认 取消	

点击"确认",弹出导入证书界面,如下图所示。

TOPSEC认证客户端
│
认证方式 使用证书认证
证书文件路径 (C) 册\ZhangSan-pem.pem
密钥文件路径 低)D:\TOS\3.3.006\手册'
□ 开机启动 🔽 自动重连
状态:未登录
登录(L) 注销(0) 设置(2) 退出(X)

点击"登录"按钮,登录成功后会在任务栏显示金色小钥匙。



证书用户的用户名为该用户的证书序列号,此处仅为演示,实际应用中会有所不同。

用户管理 在线用户 用户设置						
	台注- 2					
用户名	地北	服务器	在线时间(HH:MM:SS)	类型	删除此地址	#除此用户
ZhangSan	10.10.10.22	cert	0:0:13	common	3	3
doc	172.16.1.2	localdb	0:15:57	sv	_	-

### 注意事项

1)如果采用第三方 CA 证书认证方式,则网络卫士防火墙上必须同时导入 CA 的根证书和 CRL 列表。

设置本地证书时,必须导入 CA 根证书以及 CRL 列表,如果仅导入 CA 根证书,证书认证不会成功。

2)本案例使用的证书是防火墙内置的 CA 签发的证书,用户也可以使用第三方 CA 签发的证书用户进行认证。

3)保证客户端和网络卫士防火墙之间的正常通信,客户端需要访问网络卫士防火墙的 UDP:10000 及 UDP:20000 端口。

4) 对于非 IPSec VPN 和 SSL VPN 的普通用户,网络卫士防火墙可以设置基于用户角 色的访问控制规则,只需在源/目的处选择相应的用户角色便可。

5) 对于 IV 和 SV 的认证用户,则既可以基于角色也可以基于用户进行权限控制。

6)如果用户需要防火墙分配 IP 地址,则需选择 网络管理 > DHCP,并选择"DHCP 服务器"页签,当 DHCP 服务器为"停止"状态时,设置 DHCP 地址池,并在 lo 口启动 DHCP 服务器。

# 报文阻断规则配置

当数据包进入防火墙的某个接口时,经过 VPN 解密后,防火墙首先检查该数据包是 否满足该端口中定义的报文阻断规则,如果报文阻断规则不允许该数据包通过,则防火墙 将丢掉该数据包。如果允许该数据包通过,则防火墙才会继续进行访问控制规则查询。

当设备接收到一个数据报文后,会顺序匹配报文阻断策略,如果没有匹配到任何策略, 则会依据默认规则对该报文进行处理。默认规则可能是以下两种情况:

- 默认拒绝所有的流量,这需要配置允许哪些报文通过,否则设备将不会转发和处理任何数据报文。
- 允许所有的流量,这种情况需要你特殊指定要拒绝哪些报文通过,否则任何报文都可通过防火墙。

网络卫士防火墙的出厂配置中默认的报文阻断策略为允许所有流量,即为第二种情况。

## 二层报文过滤

### 基本需求

防火墙最基本的作用就是控制内、外网络通信。MAC 地址可用于直接标识某个网络 设备,网络卫士系列防火墙支持基于 MAC 地址进行报文过滤,用于限定只有 MAC 地址 符合过滤条件的数据包才能够通过防火墙访问目的区域。通过 MAC 地址过滤技术可以保 证只有授权的 MAC 地址才能对网络资源进行访问。

在下图中,要求只禁止 Area\_eth2 区域 MAC 地址为 00:50:04:C3:B0:31 的主机访问在 Area\_Eth0 区域的文档服务器(192.168.83.234/24 的 8000 端口)。



图 16 防火墙在网络中进行报文过滤控制示意图

## 配置要点

- ▶ 定义服务器主机地址对象
- ▶ 配置报文阻断策略

## WEBUI 配置步骤

1)选择 资源管理 > 地址,选择"主机"页签,添加地址对象 webserver。

主机 范围 子网 地址組			
主机雇性			
名称       webserver       *         物理地址       00:00:00:00:00          IP地址       192.168.83.234			
确定取消			

2) 配置数据阻断规则: 拒绝 MAC 地址为 00:50:04:C3:B0:31 的主机访问 WEB 服务

器

选择菜单 防火墙 > 阻断策略,点击"添加"。

阻断策略	
	阻断策略屈性
	访问权限 💿 允许 🔿 拒绝
	日志记录 否 🔽
	来源区域 area_eth2 💌
	协议类型 IP ▼
	源MAC地址 00:50:04:C3:B0:31 [格式如 AA:BB:CC:DD:EE:FF]
	目的MAC地址 AA:BB:CC:DD:EE:FF] [格式如
	IP协议类型 TCP 🗨
	源地址任意地址 ▼
	目的地址 webserver [主机]
	源端口 - [1-65535]
	目的端口 80 [1-65535]
	确 定 取 消

设定访问权限为"拒绝",来源区域选择为"area\_eth2"(即 MAC 地址为 00:50:04:C3:B0:31 的主机所在区域)、目的地址和端口号分别设定为 WEB 服务器所在的 主机(webserver)和所占用的端口号 80。IP 协议类型为"TCP"。其余选项不需设定。

### 注意事项

1) MAC 地址中的字母十六进制数位应当大写,例如本例 MAC 地址为 00:50:04:C3:B0:31,则如果输入为 00:50:04:c3:b0:31,则系统会提示错误信息。

2)如果定义包过滤策略时同时输入了源 MAC 地址和源 IP 地址选项,则只有主机的 MAC 地址和 IP 地址均匹配此条件时,此规则才会生效。

3)如果是拒绝访问目的主机的某些端口,则如果端口为连续的,可以在目的端口处 设定范围,否则需要对每一个端口设定相应的报文阻断策略。如果端口为唯一端口号,则 可以只输入起始端口号,也可以起始和终止端口号设定为同一个值。例如本例设定为 8000-8000。

4)目的MAC地址最好不要输入,如果输入则只能为区域所属防火墙物理接口的MAC 地址,而不能是其他值。

## 三层报文过滤

### 基本需求

要求不对网段 10.10.10.0/24 开放 192.168.83.234 的 8000 端口。也就是说,只有 10.10.10.0/24 网段的用户不能访问服务器 192.168.83.234 的 8000 端口,其他网段的数据报 文均能顺利访问服务器 192.168.83.234 的 8000 端口。

### 配置要点

- ▶ 定义服务器主机地址资源和子网地址资源
- ▶ 配置报文阻断策略

### WEBUI 配置步骤

1) 选择菜单 资源管理 > 地址,并选择"主机"页签,添加主机地址资源 webserver。

主机 范围 子网 地址组			
	主机属性		
名称 物理地址	<pre>webserver * 00:00:00:00:00:00</pre>		
IP地址	192. 168. 83. 234		
	确 定 取 消		

3)选择资源管理 > 地址,并选择"子网"页签,添加子网地址资源。

主机 范围 子网 地址组
子网属性
名称 10.10.10.0 *
网络地址 10.10.10.0 *
子网掩码 255.255.255.0 *
排除地址
确 定 取 消

4)选择 防火墙 > 阻断策略,点击"添加"按钮,添加阻断策略,禁止10.10.10.0/24 网段访问文档服务器。

阻断策略		
		阻断策略雇性
ù	方问权限	○ 允许 ● 拒绝
E	日志记录	▲
ş	<b>来源区域</b>	area_eth2
t	协议类型	IP
ji ji	原MAC地址	[格式如 AA:BB:CC:DD:EE:FF]
Ē	目的MAC地址	[格式如 AA:BB:CC:DD:EE:FF]
I	P协议类型	TCP
R.	原地址	10.10.10.0 [子网]
E	目的地址	webserver [主机]
Ű.	原端口	- [1-65535]
E	目的端口	8000 - [1-65535]
Ļ		,
	确	定 取消

设定访问权限为"拒绝",区域对象选择"area\_eth2"(即 10.10.10.0/24 网段所在区域)、协议类型选择为"IP"、IP 协议类型选择为"TCP",源地址选择前面定义的"10.10.10.0 子网",目的地址和端口号分别设定为文档服务器所在的主机(docserver)和所占用的端口号 8000。其余选项不需设定。

### 注意事项

如果同时设定了 IP 地址和 MAC 地址,则只有两项同时满足时才会匹配报文阻断策略。

# 地址转换

在一般情况下,企业拥有的公有合法 IP 地址十分有限。所以,在企业内网中,一般 使用私有 IP 地址。为了解决通过私有 IP 地址访问公网(Internet)的问题,和隐藏内部网 络拓扑及真实 IP 的需要,地址转换技术(Network Address Translation, NAT)经常会被应 用到位于网络出口的路由设备,如防火墙上。

## 基于地址对象的源地址转换

网络卫士防火墙的防火墙模块的源地址转换策略支持基于地址资源的源地址转换,可 转换的地址资源包括单个主机、主机地址范围和子网,对源地址可以进行的转换方式有: 将源地址固定映射为某一合法 IP 地址和将源地址动态映射某一网段或某一地址范围的地 址。

### 基本需求

网络卫士防火墙的接口 Eth0 连接企业内网,内网为 192.168.100.0/24, Eth0 的 IP 地 址为 192.168.100.1; Eth1 连接外网, Eth1 的 IP 地址为 202.10.10.1。企业可用的公网 IP 地址范围为 202.10.10.1-202.10.10.10,网络拓扑结构的示意图如下所示。



#### 图 17 基于地址资源的源地址转换示意图

### 配置要点

- 定义内网地址资源,可定义的地址资源包括主机地址资源、范围地址资源、子网 地址资源、区域和 VLAN。
- ▶ 定义要转换的公网地址资源。

▶ 定义源地址转换策略。

### WebUI 配置步骤

1)选择资源管理 > 区域,点击"添加",定义区域资源。

设置内网区域 area\_eth0 与属性 eth0 绑定且禁止访问。

区域	
	区域
	名称 area_eth0 * 访问权限 禁止 I
可用属性: eth1 eth2 eth3 ads1 ads11	成员: → × eth0
	确 定 取 消

外网区域 area\_eth1 与属性 eth1 绑定且允许访问。

区域	
	区域
	名称 area_eth1 * 访问权限 允许 ▼ 注释
可用属性: eth0 eth2 eth3 ads1 ads11	成员: 
	确 定 取 消

2)定义内部地址资源,选择资源管理 > 地址,并选择相应页签,点击"添加"可 以定义主机地址资源、地址范围资源和子网地址资源。

a) 定义 NAT 主机资源:选择"子网"页签,点击"添加"。

主机 范围 子网 地址組
子网属性
名称 子网100.X * 网络地址 192.168.100.0 * 子网掩码 255.255.0 * 排除地址
确 定 取 消

b) 定义 NAT 地址池:选择"范围"页签,点击"添加"。

主机 范围 子网 地址组
地址范围尾性
名称 nat-pool * 起始地址 202.10.10.1 * 终止地址 202.10.10.10 * 排除地址
确 定 取 消

3) 定义 NAT 地址转换策略。选择 防火墙 > 地址转换,点击右上角"添加",进入 NAT 规则配置界面,如下图所示。

添加地址转换		
定更	源转换	•
原		
地力	Ł	
	子网100.X	Ó
其它		
VL	N 任意	
<u>t</u>	或	
	area_ethO	í
端	日任意	
的		
地址	住意	
其它		
VLA	N 任意	
t	戎	
	area_eth1	Í
服务	任意	
酒+N+I-转拍·		
源端口不做3		•
换	□ [源端口固定]	1
规则描述		
	确定	取消

点击"确定",配置完成。

需要注意的是,系统默认情况下,在源地址转换同时也会转换源端口。只有在上图中选择"源端口不作转换"时,数据包在经过防火墙时不改变源端口。

# 基于 IP 地址的目的地址转换

## 基本需求

由于来自 INTERNET 的对政府、企业的网络攻击日益频繁,因此需要对内网中向外 网提供访问服务的关键设备进行有效保护。采用目的地址 NAT 可以有效地将内部网络地 址对外隐藏。



图 18 基于 IP 地址的目的地址转换示意图

图中: 公网 Internet 用户需要通过防火墙访问 WEB 服务器,为了隐藏服务器在内网中的真实地址 192.168.83.234,使用公网地址 202.99.27.201 作为用户的访问地址,提供HTTP 服务的端口为 8080。

## 配置要点

- ▶ 定义区域资源: area\_eth1。
- ▶ 定义 WEB 服务器真实地址对应地址资源。
- ▶ 定义 WEB 服务器的公网虚拟 IP 地址资源。
- ▶ 定义 WEB 服务器真实端口。
- ▶ 定义地址转换策略。

### WebUI 配置步骤

选择 资源管理 > 区域,点击"添加",定义区域资源。
 设置内网区域 area\_eth0 与属性 eth0 绑定且禁止访问。

区域	
	区域
	名称 area_eth0 * 访问权限 禁止 I 注释
可用属性: eth1 eth2 eth3 ads1 ads11	成员: → × eth0
	确 定 取 消

外网区域 area\_eth1 与属性 eth1 绑定且允许访问。

区域	
	区域
	名称 area_eth1 * 访问权限 允许 ▼ 注释
可用属性: eth0 eth2 eth3 adsl adsl1	成员: 
	确 定 取 消

2) 定义 WEB 服务器的内网真实地址资源。

选择 资源管理 > 地址,选择"主机"页签,点击"添加",系统出现添加主机资源的页面,如下图所示。
主机 范围 子网 地址組				
	主机属性			
名称 物理地址	webserver *			
IP地址	192. 168. 83. 234 <			
确定取消				

3) 定义 WEB 服务器的公网 IP 地址资源

选择 资源管理 > 地址,选择"主机"页签,点击"添加",系统出现添加主机资源的页面,如下图所示。

	主机雇性	
名称 物理地址 IP地址	MAP_IP * 00:00:00:00:00 202.99.27.201 × 202.99.27.201 ×	
	确定 取消	

4) 定义服务端口

由于 WEB 服务器提供服务的端口是: 8080,不是默认端口,在设置 NAT 转换规则时需要写明该服务端口。设置自定义服务端口的过程如下:

点击 资源管理 > 服务,并选择"自定义"页签,进入自定义服务页面。点击右侧 "添加"按钮,如图所示。

	服务属性	
名称	webport *	
类型	TCP	
端口	8080 - *	
[单个端口或范围,单个端口只填起始.ICMP是类型值0-18及特征码]		
	确定取消	

#### 5) 定义目的地址转换策略

在导航菜单选择 防火墙 > 地址转换,进入地址转换规则列表界面,点击"添加"进入 NAT 规则配置界面,如下图所示,选择"目的转换"选项设定目的地址转换策略。

		添加地址转换	
模式		目的转换	•
源			
	地址	任意	
	其它	<b>v</b>	
	VLAN	任意	
	区域		
		area_eth1	í
	端口	任意	
日的			
	地址		
		MAP_IP	Ó
	其它		
m H			
服务		HTTP	Ó
目的地	址转换为	webserver [主机]	~
目的端口转换为		webport (TCP:8080)	~
规则描	述		
		确定 取消	

设置完成后,点击"确定"按钮,完成目的 NAT 规则设置。

### 注意事项

1) 定义目的地址转换策略时,只需目的地址,不能指定目的区域或目的 VLAN。

2)如果 WEB 服务器提供 WEB 服务使用的是标准的 80 端口,则定义地址转换策略时,在"目的端口转换为"处不作设置即可。

3)如果希望防火墙对访问内容进行深度过滤,需要对应用端口进行绑定操作。因为 服务器使用了非标准的端口 8080,防火墙不会对报文进行处理,导致不能正确检验数据 包。

# 双向地址转换

#### 基本需求

企业 WEB 服务器(IP: 192.168.83.234)通过防火墙 MAP 为 202.99.27.201 对内网用 户提供 WEB 服务,网络示意图如下。



图 19 双向地址转换示意图

如上图所示,管理主机和 WEB 服务器同样处于网段 192.168.83.0/24。正常情况下, 管理主机与服务器之间的通信可以不经过防火墙,而经过其他路由达成。但是当管理主机 使用公网地址(或域名)访问服务器时,数据包的源 IP 为管理主机地址,目的地址为服 务器公网地址。如果防火墙仅作目的 NAT,则服务器收到数据包的源 IP 为管理主机地址, 目的地址为自身地址。当其回应管理主机时,发出的数据包会不经过防火墙,而经过其他 路由达成。此情况会导致会话无法建立。因此需要设置双向地址转换规则。

## 配置要点

- ▶ 定义区域资源。
- ▶ 定义主机地址资源。
- ▶ 定义地址转换规则。

## WEBUI 配置步骤

1) 定义区域资源

选择菜单 资源管理 > 区域,点击"添加",分别设置接口 Eth0 对应的区域为 area\_eth0,区域权限为"禁止";

区域		
	区域	
	名称 area_eth0 * 访问权限 禁止 I	
可用届性: eth1 eth2 eth3 ads1 ads11	成员: → × eth0	
	确 定 取 消	

接口 Eth1 对应的区域为 area\_eth1,设置区域的访问权限为"允许"。

区域		
	区域	
可用属性: eth0 eth2 eth3 ads1 ads11	名称 area_ethi * 访问权限 允许 ▼ 注释	
	确 定 取 消	-

2) 定义主机地址资源: webserver、MAP\_IP 和 MAP\_USERIP

选择 资源管理 > 地址,并选择"主机"页签,点击"添加"添加主机地址资源。 定义 webserver 主机资源,如下图。

主机 范围 子网 地址組		
主机属性		
名称 webserver * 物理地址 00:00:00:00:00 IP地址 192.168.83.234 <-  ×		
确 定 取 消		

定义 MAP\_IP 和 MAP\_USERIP 可以参考上图。设置完成后界面如下图。

主机 范围 子网 地址组			
+ 添加 前 清空		总计 <b>: 9</b>	
名称 🔶	IP地址 ◆	操作	
webserver	192. 168. 83. 234	2	
MAP_IP	202. 99. 27. 201	2	
MAP_USERIP	192. 168. 83. 237	2	

3) 定义地址转换规则

定义地址转换策略过程如下:

选择 防火墙 > 地址转换,并点击"添加"添加地址转换规则。如下图所示,选择 "双向转换"选项设定双向地址转换策略。

	添加地址转换
模式	双向转换
源	
地址	任意
其它	
VLA	任意
区域	
	area_ethO 🔟
端口	任意
目的	
地址	
	MAP_IP 🔟
其它	
미상	
服务	нттр 🔟
源地址转换为	MAP_USERIP [主机]
目的地址转换	为 webserver [主杭]
目的端口转换	为不做转换 🔽
源端口不做转	换 [[源端口固定]
规则描述	
	确定 取消

设置完成后,点击"确定"按钮,完成 NAT 规则设置。

## 注意事项

定义双向 NAT 规则时,可以将源 IP 转换为任意一个虚拟 IP 地址,本例中将源地址转换为了防火墙 eth0 口的 IP。

# 访问控制规则配置

访问规则描述了网络卫士防火墙允许或禁止匹配访问控制规则的报文通过。防火墙接 收到报文后,将顺序匹配访问规则表中所设定规则。一旦寻找到匹配的规则,则按照该策 略所规定的操作(允许或丢弃)处理该报文,不再进行区域缺省属性的检查。如果不存在 可匹配的访问策略,网络卫士防火墙将根据目的接口所在区域的缺省属性(允许访问或禁 止访问),处理该报文。

在进行访问控制规则查询之前,网络卫士防火墙将首先查询数据包是否符合目的地址 转换规则。如果符合目的地址转换规则,网络卫士防火墙将把接收的报文的目的 IP 地址 转换为预先设置的 IP 地址(一般为真实 IP)。因此在进行访问规则设置时,系统一般采 用的是真实的源和目的地址(转换后目的地址)来设置访问规则;同时,系统也支持按照 转换前的目的地址设置访问规则,此时,报文将按照转换前的目的地址匹配访问控制规则。

某企业的网络结构示意图如下图所示。



图 20 访问控制规则设置示意图

## 基本需求

用户要求如下:

- ▶ 内网 area\_eth2 区域的文档组(10.10.10.0/24)可以上网;允许项目组领导 (10.10.11.2 和 10.10.11.3)上网,禁止项目组普通员工上网。
- ▶ 外网和 area\_eth0 区域的机器不能访问研发部门内网;
- ▶ 仅允许外网用户访问 area\_eth0 区域的 WEB 服务器:真实 IP 为 172.16.1.3,虚拟
   IP 为 192.168.100.143。内网用户不允许访问 WEB 服务器。

## 配置要点

- ▶ 设置地址对象
- ▶ 设置区域对象的缺省访问权限: area\_eth0、area\_eth2 为禁止访问, area\_eth1 为 允许访问。
- ▶ 定义源地址转换规则,保证内网用户能够访问外网;定义目的地址转换规则,使 得外网用户可以访问 area\_eth0 区域的 WEB 服务器。
- ▶ 定义访问控制规则,禁止项目组除领导外的普通员工上网;
- ▶ 定义访问控制规则,允许用户访问 area\_eth0 区域的 WEB 服务器。

## WebUI 配置步骤

1) 定义主机、子网地址对象。

a)选择 资源管理 > 地址,选择"主机"页签, 定义主机地址资源。定义完成后的 界面如下图所示:

主机 范围 子网 地址組			
➡ 添加 6 清空		总计: 9	
名称 🔶	IP地址 🗢	操作	
webserver	192. 168. 83. 234	23	
MAP_IP	202. 99. 27. 201	2	
host_eth1	202. 99. 27. 199	23	

webserver 表示 WEB 服务器, IP 为 192.168.83.234;

MAP\_IP 表示 WEB 服务器的公网 IP 地址对象, IP 为 202.99.27.201;

host\_eth1 表示接口主机地址对象, IP 为 202.99.27.199;

b)选择 资源管理 > 地址,选择"子网"页签, 点击"添加"定义子网地址资源 rd\_group,表示项目组除了领导以外的普通员工。

主机 范围 子网 地址組		
子网属性		
名称 rd_group * 网络地址 11.11.11.0 * 子网掩码 255.255.0 * 排除地址 11.11.11.2 		
确 定 取 消		

4) 定义区域资源的访问权限(整个区域是否允许访问)。

选择 资源管理 > 区域,设定外网区域 area\_eth1 的缺省属性为"允许"访问,内网 区域 area\_eth0 和 area\_eth2 的缺省属性为"禁止"访问。以 area\_eth0 为例,设置界面如 下图所示。

区域	
	区域
	名称 area_eth0 * 访问权限 禁止 I
可用届性: eth1 eth2 eth3 ads1 ads11	成员: -> x eth0
	确 定 取 消

设置完成后的界面如下图所示。

区域							
♣ 添加  6  6  6  1:5							
名称 🔶	绑定属性     ◆	权限 ◆	注释   ◆	操作			
area_eth0	eth0	禁止		2			
area_eth1	eth1	允许		2			
area_eth2	eth2	禁止		2			

5) 选择 防火墙 > 地址转换, 定义地址转换规则。

a) 定义源地址转换规则, 使得内网用户能够访问外网:

		添加地址转换	
模式		源转换	
源			
	地址	任意	
	其它		
目的			
	地址	任意	
	其它		
	VLAN	任意	
	区域		
		area_eth1	Í
服务		任意	
源地址	转换为	host_eth1 [主机]	~
源端□	]不做转换	□ [源端口固定]	
规则描	謎述		
		确定 取消	)

b) 定义目的地址转换规则, 使得 area\_eth1 区域的外网用户可以通过访问公网 IP: 202.99.27.201, 访问 area\_eth0 区域的 WEB 服务器。

		添加地址转换	
模式		目的转换	<b>•</b>
源			
	地址	任意	
	其它		
	VLAN	任意	
	区域		
		area_eth1	Ó
	端口	任意	
目的			
	地址		
		MAP_IP	í
	其它		
服务		HTTP	í
目的地	址转换为	webserver [主机]	~
目的端	口转换为	不做转换	*
规则描	述		

6) 选择菜单 防火墙 > 访问控制, 点击"添加策略"定义访问控制规则。

a) 配置规则允许访问 WEB 服务器

由于 Web 服务器所在的 area\_eth0 区域禁止访问,所以要允许用户访问 Web 服务器, 需要定义访问控制规则如下图所示。

		添加访问控制策略	
源			
	区域	任意	
	地址	任意	
	其它		
目的			
	区域		
		area_eth0	
	地址		
	其它	webserver	
服务		нттр	6
动作		○ 允许 ○ 禁止 ○ 收集	
日志记	录	◎ 不记录 ○ 记录 ○ 系统报警	
连接选	:项	□ 长连接	
保护内 ▶ 高級	容表 す	无	•
		确定 取消	

#### 注意事项:

①在"源"处不设置任何参数,表示不对数据报文的源加以限制。

②在"目的地址"处需要选择 WEB 服务器的真实 IP 地址(webserver),因为防火 墙要先对数据包进行目的地址转换处理,当内网用户利用 http://202.99.27.201 访问 area\_eth0 区域的 Web 服务器时,由于符合目的地址转换规则,所以数据包的目的地址将 被转换为 192.168.83.234。然后才进行访问规则查询,此时只有设定为 WEB 服务器的真 实 IP 地址才能达到内网用户访问 area\_eth0 区域区域 WEB 服务器的目的。

如果需要根据服务器的公网 IP 对访问进行控制,只需要在"目的"处勾选"其它", 然后在"目的 NAT 前的地址"处选择 MAP\_IP 即可。无须在"目的地址"中再选择地址。 如下图所示。

目的			
	区域	任意	
	地址	任意	
	其它		
	VLAN	任意	
	转换前		
	地址	MAP_IP	Ó
	目的域 名	无	•

③ 如果 WEB 服务器采用非标准端口提供 HTTP 服务,只需要添加自定义服务资源, 然后在上图的"服务"处选择自定义的服务对象即可。

b)禁止项目组领导以外的普通员工访问外网。

由于外网区域 area\_eth1 允许访问, 所以需要添加禁止访问外网的规则如下下图所示。

		添加访问控制策略	
源			
	区域		
		area_eth2	Í
	地址		
		rd_group	í
	其它		
	角色	任意	
	VLAN		
		vl an. 0002	Í
	端口	任意	
目的			
	区域		
		area_eth1	Ó
	地址	任意	
	其它		
服务		任意	
动作		○ 允许 ⓒ 禁止 ○ 收集	
日志记	录 	<ul> <li>● 不记录</li> <li>○ 记录</li> <li>○ 系统报警</li> </ul>	
保护内	── ]容表	□ 长连接 	-
▶ 高翁	g		_
		确定 取消	

#### 注意事项:

1)如果要求用户只能使用特殊源端口访问 WEB 服务器,不能使用其他端口,只需在"源"的"端口"处选择定义好的"自定义服务对象"即可。

2)如果只要求指定角色的用户可以使用某些资源,需要配置"用户角色",并在访问控制规则的"源""角色"处引用该角色,并开放认证相关的服务,即可实现基于角色的访问控制。用户认证相关设置请参见相关案例。

# IPS 策略配置

本案例将介绍当将网络卫士防火墙作为网关时,如何配置防火墙对访问控制规则中允 许的业务流量执行 IPS 策略。

## 基本需求

背景:网络卫士防火墙作为网关接入网络,设备的 eth2 口(接口 IP: 202.99.65.100/24, 网关 IP: 202.99.65.1) 与外网相连,设备的 eth1 口(接口 IP: 192.168.1.1/24) 与内网(192.168.1.0/24) 相连,内网用户通过 Eth1 口访问外网,如图 6 所示。

需求:实现网络卫士防火墙对访问控制规则允许的流量进行攻击防御。



图 21 IPS 策略示意图

## 配置要点

- ▶ 配置网络部分
- ▶ 配置区域对象
- ▶ 配置攻击检测规则
- ▶ 配置入侵防御策略
- ▶ 配置访问控制规则

## WEBUI 配置步骤

1) 配置网络部分

选择 网络管理 > 接口,将 Eth1 和 Eth2 口设置为路由模式并为其配置相应的 IP 地址,如下图所示。

物理接口	子接口								
接口名称	描述	接口模式	地址	MTU	・ 状态	链接	协商	速率	设置
eth0	intranet	路由	192, 168, 83, 237/255, 255, 255, 0	1500	启用	0	全双工	100M	
eth1		路由	192, 168, 1, 1/255, 255, 255, 0	1500	启用	0			
eth2		路由	202.99.65.100/255.255.255.0	1500	启用	0			
eth3		路由		1500	启用	0			

2) 配置区域对象。

选择资源管理 > 区域,将 Eth1 和 Eth2 口所连的区域分别设置为 area\_eth1 和

area\_eth2,如下图所示。

区域						
+ 添加      · <td< th=""></td<>						
名称	绑定属性	权限	注释	操作		
area_eth0	eth0	允许		2		
area_eth1	eth1	允许		20		
area_eth2	eth2	允许		]> 🗟		

3) 配置攻击检测规则

选择 入侵防御 > 攻击检测规则,点击"添加"添加一条攻击检测规则"IPS 规则", 该规则引用系统默认攻击检测规则模板,如下图所示。

攻击检测规则								
➡添加 mā空 总计:1								
名称	规则条目	风险统计	动作统计	状态	修改	删除		
IPS规则	2440	高:392, 中:0, 低:2048	警告:2048, 丢弃:392	未引用	2	3		

4) 配置入侵防御策略

选择 入侵防御 > 入侵防御策略,点击"添加"添加一条引用攻击检测规则"IPS 规则"的入侵防御策略"IPS 策略",如下图所示。

	入侵防御策略
名称 攻击检测规则 启用	IPS策略 IPS规则
	确定 取消

5) 配置访问控制策略

选择 防火墙 > 访问控制,点击"添加"添加一条访问控制策略,该策略对所有从 区域 area\_eth2 到达区域 area\_eth1 的数据包执行入侵防御策略"IPS 策略",如下图所示。

访问控制								
目的区域	所有区域	•	策略组 所有	组 🔽	高级搜索		显示策略统计	
🕂 添加組	i 🕂 添	加策略					总计: 1 毎页: <mark>30条</mark>	-
ID	控制	源		目的		服务	选项	操作
8061	•	区域: area_eth2		区域: area_eth1			IPS:IPS策略	2 -
K ◀ 1 → N 转到 /1 Go								

## 注意事项

入侵防御策略只能对防火墙访问控制策略允许的业务流量进行检测防御,而对于访问 控制策略禁止的业务入侵防御策略不会进行检测。

# 深度过滤

深度过滤策略可以实现对应用层协议的内容进行检测和过滤,目前深度过滤支持的应 用层协议包括:HTTP、FTP、SMTP、POP3、IMAP、TELNET、RSH等。深度过滤策略 设置好以后不能够单独生效,用户必须在访问控制规则中引用深度过滤策略,匹配了该条 访问控制规则的数据包才会进行深度内容检测处理。防火墙的深度过滤功能不能工作在纯 交换模式下,只能工作在路由或混合模式下。

# HTTP 过滤

## 基本需求

1) URL 过滤。

禁止测试部员工访问外网 URL 中含有"www.falun.com"的网站。

2) 关键字过滤。

禁止测试部员工访问外网 web 页面中含有"法轮功"文字的网站。





#### 图 22 HTTP 访问过滤示意图

## 配置要点

- ▶ 绑定 HTTP 协议的端口。
- ▶ 添加关键字对象。
- ➢ 添加 URL 对象。
- ▶ 配置内容安全策略。
- ▶ 配置外网所在区域"area\_eth0"和测试部所在区域"area\_eth1"。
- ▶ 配置访问控制规则。
- ▶ 验证。

## WebUI 配置步骤

1. 绑定 HTTP 协议的端口。

选择内容过滤 > 应用端口绑定,将 HTTP 协议绑定到 80 端口,如下图所示。

应用端口绑定								
♣ 添加 C 重置  着 清空 总计: 7								
应用协议类型	协议/端口	目的子网/掩码	操作					
ftp	tep/21	0.0.0.0/0.0.0.0	[ 🖉 🕄					
smtp	tep/25	0.0.0.0/0.0.0.0	[ 🖉 🕄					
tftp	udp/69	0.0.0.0/0.0.0	[ 🖉 🕄					
http	tcp/80	0.0.0.0/0.0.0.0	2 🗟 💵					
рорЗ	tep/110	0.0.0.0/0.0.0.0	2 🗟 💵					
sqlnet	tep/1521	0.0.0/0.0.0	[ 🖉 🕄					
telnet	tcp/23	0.0.0/0.0.0.0	2 🗟 💵					

#### 2. 添加关键字对象。

1)选择 内容过滤 > HTTP 过滤, 然后激活"内容过滤"页签, 点击"添加"链接 配置关键字"法轮功", 如下图所示。

URL过滤	内容过滤						
关键字属性							
名称 关键字	法轮功     *       法轮功     <-       法轮功     ×						
类型	<ul> <li>□ 区分大小写</li> <li>◎ 禁止</li> <li>确定</li> <li>取消</li> </ul>						

2)参数设置完成后,点击"确定"按钮。

#### 说明

- ◆ HTTP 协议内容过滤不支持正则表达式,支持通配符"?"和"\*"。
- ◆ 在进行内容检索时,遵循搜索方式进行匹配。
- 3. 添加 URL 对象。

1)选择 内容过滤 > HTTP 过滤, 然后激活 "URL 过滤"页签, 点击"添加"链接 配置 URL "禁止访问 falun", 如下图所示。

URL过滤	内容过滤								
	URL雇性								
名称	名称 禁止访问falun *								
URL	www.falun.com*								
类型	○ 允许 ● 禁止								
	确定取消								

2) 参数设置完成后,点击"确定"按钮

#### 说明

- ◆ HTTP 协议 URL 的过滤不支持正则表达式,但支持通配符 "\*"。
- ◆ 在进行 URL 检索时,遵循从前往后顺序匹配的方式,即:一旦匹配到 URL 前面的字符就表示匹配成功。

#### 4. 配置内容安全策略。

1)选择 防火墙 > 内容安全策略,然后点击"添加"链接,设置 HTTP 过滤策略。 参数设置如下图所示。

安全策略 🔪		
	内容安全策略	
	内容表名称 HTTP_filter * 注释信息	□ (最多63个字符)
▼ HTTP过滤		
	内容过滤	
	VRL过滤	禁止访问falun ▼
	URL最大长度	[0-4096,0为不限制]
	网页内容过滤	法轮功
	http头过滤	未选择
	ActiveX过滤	
	Applet过滤	
	Seript过滤	
	识别伪装HTTP连接	允许 💌
	登录标题替换	未选择  ▼
	重定向	
	重定向地址(最多127个字符)	周期: [0-604800秒]
▶ FTP过滤		
▶ WEB过滤		

2)参数配置完成后,点击"确定"按钮。

### 5. 配置外网所在区域"area\_eth0"和测试部所在区域"area\_eth1"。

假设防火墙上 Eth0 口的 IP 地址 "192.168.83.237"和 Eth1 口的 IP 地址 "10.10.10.1" 已经配置完成。

1) 选择 资源管理 > 区域, 然后点击"添加"链接, 配置外网所在区域"area\_eth0", 如下图所示。

区域		
		区域
	名称 访问权限 注释	area_eth0    * 允许
可用属性: adsl [属性] adsl1 [属性] adsl2 [属性] adsl3 [属性] bond0 [属性]		成员: -> ×
		确定 取消

参数设置完成后,点击"确定"按钮即可。

2)选择 资源管理 > 区域, 然后点击"添加"链接, 配置测试部所在区域"area\_eth1", 如下图所示。

区域			
		区域	
	名称 访问权限 注释	area_eth1 * 允许	
可用属性: adsl [属性] adsl1 [属性] adsl2 [属性] adsl3 [属性] bond0 [属性]		成员: -> eth1	
		确定 取消	

参数设置完成后,点击"确定"按钮即可。

#### 6. 配置访问控制规则。

1)选择 防火墙 > 访问控制,点击"添加策略"配置访问控制规则,如下图所示。

访问控制			
		添加访问控制策略	
	洍		
	™ ⊽htt		
	<u>E 1</u> 494	area_eth1	í
	おお	任意	
			L
	其它		
	目的		
	区域		
		area_eth0	Ó
	地址	任意	
	其它		
	服务		
		HTTP	Ó
	动作	⊙ 允许 ○ 禁止 ○ 收集	
	日志记录	⊙ 不记录 ○ 记录 ○ 系统报警	
	连接选项	□ 长连接	
	保护内容表	HTTP_filter	-
	▶ 高级		
		确定 取消	

2)参数设置完成后,点击"确定"按钮即可。

#### 7. 验证。

从测试部(属于区域 area\_eth1)的一台主机(10.10.10.22/24)依次访问外网的下列 URL。

a) http://www.falun.com

结果:因其 URL 匹配"www.falun.com\*",无法访问。

b)访问http://192.168.83.235

结果:因其网页中含有关键字"法轮功",无法访问。

## 注意事项

1) HTTP 过滤可以和重定向功能一起使用,并且会先进行重定向,再进行 HTTP 过滤。

注意访问控制规则的顺序匹配:如果在本访问控制规则前已经有了一条符合源、
 目的、时间等条件的规则,本条访问控制规则不会生效,启用的应用程序识别策略也不能
 实现。所以,启用应用程序识别策略的访问控制规则应尽可能的精确、前置。

# IPSec VPN 隧道管理

天融信 IPSec VPN 支持标准的 IKE 和 IPSec 协议,也就是说,该 IPSec VPN 不仅可 以和天融信的 IPSec VPN 建立隧道,也可与其他支持 IKE 标准协议的 VPN 设备协商并建 立标准的 IPSec VPN 隧道。安装天融信 IPSEC VPN 引擎的网络卫士防火墙,具备一切 VPN 网关的功能,可作为一台标准的 VPN 网关使用。同时,移动远程用户(VRC, VPN Romote Client)可以通过 VPN 远程客户端与网络卫士防火墙建立 VPN 隧道。

# 远程用户本地管理

在天融信 IPSec VPN 网关中,既可以在网关中对 VRC 用户进行本地管理,也可以通 过 TopPolicy 安全设备与策略管理系统(以下简称 TopPolicy 系统)对 VRC 用户进行集中 管理。本地管理模式下,客户端认证由 IPSec VPN 网关或其他认证服务器等完成;TP 集 中管理方式下,客户端认证由 TopPolicy 系统完成。本案例主要介绍如何使用 IPSec VPN 网关对 VRC 用户进行本地管理。

## 基本需求

1) 通过 IPSec VPN 网关本地管理 VRC 用户"test"。

2) IPSec VPN 网关对 VRC 用户"test"采用"本地口令+证书认证"的认证方式进行 认证,并且使用网关本地 CA 系统为其颁发用户证书。

3) VRC 用户"test"认证成功并建立隧道后,获得本地数据库中用户"test"的访问 权限(即:可以访问内网 FTP 服务器"10.10.10.2"),禁止访问其他内网资源。



#### 图 23 远程用户本地认证示意图

#### 配置要点

- ▶ 开放 Eth0 口所属区域的 IPSecVPN 服务。
- ▶ 绑定 IPSec 虚接口。

- ▶ 创建本地根证书。
- ▶ 签发并下载用户证书。
- ▶ 配置 DHCP 服务器。
- ▶ 配置 VRC 认证的基本参数。
- ▶ 配置本地用户"test",该用户名称必须与 VRC 用户的用户证书名称保持一致。
- ▶ 配置权限对象。
- ▶ 配置 VRC 用户"test"的用户权限。
- ➢ 验证: VRC 用户 "test"使用 "本地口令+证书认证"的认证方式登录 IPSec VPN 网关后,获得内网 FTP 服务器 "10.10.10.2"的访问权限。

### WebUI 配置步骤

#### 1. 开放 Eth0 口所属区域的 IPSecVPN 服务。

1)选择 资源管理 > 区域,设置 Eth0、Eth1 所属区域,缺省访问权限为"允许", 如下图所示。

区域						
🕂 添加 🗴	宦					总计: 2
名称	♦ 绑?	定属性	¢	权限	注释	操作
area_eth0	etl	40		允许		2
area_eth1	etl	h1		允许		D

2) 开放 Eth0 口所属区域的 IPSecVPN 服务。

选择 **系统管理 > 配置**,然后激活"开放服务"页签,点击"添加"增加一条规则, 如下图所示。

开放服务 时间 SNMP 邮件设	】 】
漆加配置	
服务名称 IPSecVPN 🗸 🗸 🗸 🗸	
控制区域 area_eth0 🔽	]
控制地址 any [范围] 🛛 👻	
确定 取消	

参数设置完成后,点击"确定"按钮。

2. 绑定 IPSec 虚接口。

选择 虚拟专网 > 虚接口绑定, 然后点击"添加", 绑定虚接口 ipsec0, 如下图所示。

虚接口绑定 🔪	
	虚拟接口绑定
	虚接口名 ipsec0 💌
	通告TP地址
	绑定接口名 ethO ▼
	接口地址
	确定

参数设置完成后,点击"确定"按钮。

#### 3. 创建本地根证书。

a)选择 PKI 设置 > 本地 CA 策略, 然后选择"根证书"页签。

b) 点击"获取证书"链接, 生成新的根证书, 配置信息如下图所示。

根证书 签发证书 证书撤销列表		
	获取根证书	
○ 文件方式导入		
证书		浏览
私钥		浏览
○ PKCS12文件格式导入	<	
证书文件		浏览
证书文件密码		
〇 以本机设备证书导入	<	
⊙ 生成新证书		
名称	RootCA	*
国家	CN	[两个英文字符]
省	ВЈ	
城市	Ю	
电子邮件	doc@topsec.com.cn	
组织	RD	
单位	doc	
确	定取消	

3) 参数设置完成后,点击"确定"按钮。

4. 签发并下载用户证书。

1)选择 **PKI 设置 > 本地 CA 策略**,然后激活"签发证书"页签,点击"生成新证书",为 VRC 用户"test"生成一个新证书,如下图所示。

签发证书	正书撤销列表
	签发证书
名称	test *
国家	[两个英文字符]
省	
城市	
电子	邮件
组织	
单位	
失效	时间 [格式:YYYY/MM/DD]
	确定

参数设置完成后,点击"确定"按钮即可。

2) 在证书列表页面,点击"test"用户证书条目右侧的"下载"图标,将客户端证书 下载到本地,如下图所示。

根证书	ち 医发证书 证书撤销	例表					
<b>(</b> ) 4	② 生成新证书 ③ 全部导出 前 清空证书						
证书	有效起止日期	状态	属性	下载	写入	撤销	删除
test	Dec 22 01:20:01 UTC 2009- Dec 20 09:20:01 UTC 2019	1	<b>E</b>	ß		3	3

选择证书类型为"PKCS12格式",输入密码,如下图所示。

<b>签发证书</b> 证书撤销列表	
<u> </u>	导出签发证书
选择要使用的文件格: 密码	式 PKCS12 ▼ 导出证书 ●●●●●●●● [如果需要 密码保护,请先输入密码再导出]
	返回

参数设置完成后,点击"导出"按钮,如下图所示。

签发证书	证书撤销列表
	导出签发证书
	选择要使用的文件格式 PKCS12 ▼ 导出证书 密码 [如果需要 密码保护,请先输入密码再导出] 证书点击下载[或用右键另存]
	返回

点击"证书点击下载"链接,弹出文件保存对话框,如下图所示。

文件下载			×
您想打	开或保存此了	文件吗?	
<b>B</b>	名称: 类型: 发送者:	test.p12 Personal Information Exchange, 1.72 KB 192.168.83.237	
2	来自 Inte 危害您的讨 该文件。 <u>看</u>	rnet 的文件可能对您有所帮助,但某些文件可能 计算机。如果您不信任其来源,请不要打开或保存 可何风险?	

点击"保存"按钮,选择文件保存路径后,将证书文件保存到本地备用。

#### 5. 配置 DHCP 服务器。

1) 配置 DHCP 地址池。

a)选择 网络管理 > DHCP, 然后激活 "DHCP 服务器"页签。

b) 点击"添加地址池",配置 DHCP 地址池,用于为 VRC 用户分配虚拟 IP,如下 图所示。

DHCP服务器	DHCP客户端 DHCP中维	
	添加DHCP地址池	
	子网 11.11.11.0	*
	掩码 255.255.255.0	*
	分配起始地址 11.11.11.10 *	*
	分配结束地址 11.11.11.20 *	*
	缺省租用期 1 天 0 时 0 分	
	最大租用期 7 天 0 时 0 分	
	网关地址	
	主 d ns	
	次dns	
	域名	
	客户端类型	
	供应商详情	
	确定 取消	

c)参数设置完成后,点击"确定"按钮。

#### 说明

- ◆ 只有停止 DHCP 服务器的运行,才能够配置 DHCP 地址池。
- ♦ DHCP 地址池不能与内部网段有包含关系,更不能分配与内部网络在同一网段的地址 池。
- 2)在lo接口启用DHCP服务器。
- a) 在列表框中选择"lo", 然后点击" <---" 按钮, 如下图所示。

DHCP服务器	DHCP客户端	DHCP中继	
		DHCP服务	
运行接口	10	<- X	eth3 sslvpn0 ▼
	启动	停止	查看分配地址

b) 点击"运行"按钮,即可在 lo 接口上启用 DHCP 服务器,如下图所示。

DHCP服务器 DHCP客户端	DHCP中维
	DHCP服务
运行接口 1。	<pre>     eth0     eth1     eth2     eth3 </pre>
启动	停止查看分配地址

#### 6. 配置 VRC 认证的基本参数。

a)选择 **虚拟专网 > VRC 管理**,然后激活"基本设置"页签,设置相关内容,如下 图所示。

基本设置	权限对象	用户权限 月	自色枳限	时间对象	在线用户
			基本	CE .	
		认证管理模式	本地管理	-	
		DHCP地址池	11.11.11.0	)/255.255.255	5.0 💌
		▼高级	,		
		检查超时间隔	30		[10-600秒,缺省:30]
		保活超时时间	120		[30-300秒,缺省:120]
		内部首选DWS服务器	0.0.0.0		[IP地址]
		内部备用DNS服务器	0.0.0.0		[IP地址]
		内部首选WINS服务器	0.0.0.0		[IP地址]
		内部备用WINS服务器	0.0.0.0		[IP地址]
		与防火墙联动	否	•	
		客户端版本控制	否	•	
		强制短信认证	否	•	
		短信口令长度	5		[1-255,缺省:5]
		短信尝试次数	3		[1-10次,缺省:3]
		短信有效时间	180		[1-255秒,缺省:180]
			证书认证和	双限控制	
		查找证书用户 	是	<b>•</b>	
		允许无证书用尸登录	不允许 	•	
		CN域选择	月		
		MAIL域选择	不启用	•	
		应用		重启	服务

◆ 本案例中,配置了"证书认证权限控制"功能,即:必须查找证书用户,并且不允许 无证书用户登录,如上图所示。此时,当 IPSec VPN 网关的本地数据库中没有同名用 户时,证书用户"test"无法登录 IPSec VPN 网关;有同名用户时,"test"才能够成功 登录网关,并获得该同名用户以及该用户所属角色的权限。

b)参数设置完成后,点击"应用"按钮。

7. 配置本地用户"test",该用户名称必须与 VRC 用户的用户证书名称保持一致。

a)选择 用户认证 > 用户管理, 然后激活"用户管理"页签, 点击"添加用户"设置 VRC 用户, 如下图所示。

用户管理 在线用户 用户设置					
	用户属性				
用户名 用户描述 认证方式 口令 确认口令 可用角色 <sup>doc_role</sup> test_role cert_role	test 本地口令+证书认证 ●●●●●●● ●●●●●●●	<ul> <li>*</li> <li>[6-31个字符]</li> <li>*</li> </ul>			
高级					
	确定	取消			

#### 8. 配置权限对象。

a)选择 **虚拟专网 > VRC 管理**,然后激活"权限对象"页签,点击权限对象列表左 上方的"添加",配置权限对象,如下图所示。

说明

基本设置 权限对象	用户权限	角色权限 时间	対象 在线
		权限对象	
	名称 访问策略	FTP服务器 ↑	]
	协议	all	<-
	目的端口策略		
	目的端口起点		[范围:1~65535]
	目的端口终点		[范围:1~65535]
	IP地址	10. 10. 10. 2	]
	子网掩码	255. 255. 255. 255	]
	<del>a</del>	<b>航定 取消</b>	

b)参数设置完成后,点击"确定"按钮。

#### 9. 配置 VRC 用户 "test" 的用户权限。

a)选择 **虚拟专网 > VRC 管理**,然后激活"用户权限"页签,点击 VRC 用户"test" 右侧的"权限设置"图标,进入"test"的用户权限显示页面,如下图所示。

基本设置 权限对象	用户权限 角色相	皮限 时间对象 在	线用户
用户权限			
➡ 添加			总计: 0
名称	上移	下移	删除
返回			

b) 点击用户权限列表左上方的"添加",配置 VRC 用户"test"的用户权限,如下 图所示。

基本设置 权限对象 用月	中权限限 角色权限 时间
	用户权限对象
权限名称	FTP服务器 💌
	确定 取消

c)选择完毕,点击"确定"按钮。

10. 验证: VRC 用户 "test" 使用 "本地口令+证书认证"的认证方式登录 IPSec VPN 网关后,获得内网 FTP 服务器 "10.10.10.2"的访问权限。

- a) 在远程 VRC 客户机器上安装 VPN 远程客户端。
- b) 打开 VPN 客户端,如下图所示。

💭 VFII客户端连接管理	
文件 编辑 视图 语言 帮助	
新建VPN连接 VPN	
<u> </u>	

c) 双击"新建 VPN 连接"图标,进入配置 VPN 客户端属性的窗口,如下图所示。

📲 VPII客户端属性		×
常规 认证		
连接名	新建VFX连接	
	⊙ IP ○ 域名	
中心网关地址	0.0.0.0	
中心网关地址2	0.0.0.0	
	确定 取消	

d) 在"常规"选项卡中, 配置"中心网关地址"为 IPSec VPN 网关 Eth0 口的 IP 地址"192.168.83.237", 如下图所示。

📲 VPJI客户端属性		×
常规 认证		
连接名	237	
	● IP ○ 域名	
中心网关地址	192 . 168 . 83 . 237	
中心网关地址2	0.0.0.0	
	确定 取消	

e) 激活"认证"选项卡, 然后选择认证方式为"X509证书认证", 选中"X509证书 书是否需要口令认证", 然后选中"本地文件", 如下图所示。

₽ <mark>₽</mark> ¥P31客户端屈性	x
常规 认证	
认证方式————————————————————————————————————	
Ⅻ509证书认证	
▼ X509证书是否需要口令认证 证书加载方式	
● 本地文件	
C USB KEY	
清空CSP设置 □ 记住USB口令	
加载证书 释放证书 证书信息 修改口令	
确定    取消	

点击"加载证书"按钮,在"导入证书"窗口中为用户"test"配置证书加载方式和 证书加载路径,如下图所示。
导入证书	×
┌ 证书类型	
○ DER编码二进制X.509(.CER)	
○ Base64编码二进制X.509(.CER)	
C tar文件格式	
● PKCS12文件 C:\Documents and Settings\w	
文件密码: *****	
┌ 证书路径	
证书文件	
私钥文件	
确定	

参数设置完成后,点击"确定"按钮,提示"证书加载成功",如下图所示。

VPH	×
(į)	证书加载成功
	确定

点击提示框中的"确定"按钮,然后点击"VPN 客户端属性"窗口中的"确定"按钮,新建连接显示在"VPN 客户端连接管理"窗口中,如下图所示。



f) 双击新建连接"237", 打开 VRC 用户登录窗口, 如下图所示。

■見VPII客户端		×
Le l'i	577751	1, 1, 1, 1, 1
and the second second		THEF
		1
口 令:		
☑ 保存X509订	正书认证的口令	
连接	取消    属性	退出

g) 在登录窗口中输入 VRC 用户口令, 然后点击"连接"按钮, 开始进行认证, 稍后, 隧道协商成功。

① 通过"VPN 客户端属性"窗口, VRC 用户可以查看隧道状态,接收/发送字节, 以及虚拟网卡地址和中心网关地址等信息,如下图所示。

٩ <u>ٿ</u>	123客户端属性		×
策	略支持		
	隧道		
	状态	隧道协商成功	
	隧道持续时间	0:01:20	
	正确接收字节数	1400	
	正确发送字节数	2108	
	未知错误字节数	0	
	<u> </u>	重新协商 修改密码	
Г	显示IKE协商进程	断开 关闭	

策略       支持         本地       隧道本地端点       192.168.83.220         虚拟网卡地址       11.11.11.20         「詳細信息」         中心网关         IP地址       192.168.83.237         访问控制	📲 VPB客户端属性		×
本地 隧道本地端点 192.168.83.220 虚拟网卡地址 11.11.11.20 〔详细信息〕 中心网关 IP地址 192.168.83.237 访问控制	策略 支持		
访问控制	本地 隧道本地端点 虚拟网卡地址 中心网关 IP地址 192.168.83	192. 168. 83. 220 11. 11. 11. 20 [注释 8. 237	田信息
		访问	

点击"访问控制"按钮,可以查看 VRC 用户的访问权限,如下图所示。

ù	问控制列表					×
	目的IP	目的掩码	协议	端口	策略	有效时间
	10.10.10.2	255.255.255.255	ANY	端口未	允许	永久
	•					▶
				刷新	<u></u>	关闭

② 在 VRC 用户主机中,可以通过命令 "route print" 查看本地路由配置,如下图所

示。

			==================				
Active Routes:							
Network Destination	n Netmask	Gateway	Interface	Metric			
0.0.0.0	0.0.0	192.168.83.1	192.168.83.220	20			
10.10.10.2	255.255.255.255	11.11.11.1	11.11.11.20	1			
11.11.11.0	255.255.255.0	11.11.11.20	11.11.11.20	10			
11.11.11.20	255.255.255.255	127.0.0.1	127.0.0.1	10			
11.255.255.255	255.255.255.255	11.11.11.20	11.11.11.20	10			
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1			
192.168.83.0	255.255.255.0	192.168.83.220	192.168.83.220	20			
192.168.83.220	255.255.255.255	127.0.0.1	127.0.0.1	20			
192.168.83.255	255.255.255.255	192.168.83.220	192.168.83.220	20			
224.0.0.0	240.0.0.0	11.11.11.20	11.11.11.20	10			
224.0.0.0	240.0.0.0	192.168.83.220	192.168.83.220	20			
255.255.255.255	255.255.255.255	11.11.11.20	11.11.11.20	1			
255.255.255.255	255.255.255.255	11.11.11.20	4	1			
255.255.255.255	255.255.255.255	192.168.83.220	192.168.83.220	1			
Default Gateway:	192.168.83.1						

h) 在 IPSec VPN 网关中,选择 网络管理 > 路由,然后激活"路由表"页签,可以 查看网关上新增的目的地址为虚拟网卡 IP 的路由信息,如下图所示。

路由表 策略路由	动态路由OSPI	ः 🔪 ह	カ <mark>态路由</mark> R1	IP 🔪 च्चे	态路由BGP	多播路由	动态	
标记: U-Up, G-Gateway specified, L-Local, C-Connected, S-Static O-Ospf, R-Rip, B-Bgp, D-Dhcp, I- Ipsec, i-Interface specified								
♣ 添加  ★ 添加  ★ 添加  ★ 通								
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除	
192.168.83.237/32	0.0.0.0	ULi	1	1	10	-	-	
12. 12. 12. 1/32	0.0.0.0	ULi	1	1	10	-	-	
10.10.10.1/32	0.0.0.0	ULi	1	1	10	-	-	
11.11.11.20/32	192. 168. 83. 237	UGIi	1	1	ipsec0	-	-	
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-	
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-	
12. 12. 12. 0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-	
10. 10. 10. 0/24	0.0.0.0	UCi	10	1	eth1	-	-	

选择 虚拟专网 > VRC 管理, 然后激活"在线用户"页签, 可以查看防火墙上的 VRC

用户信息,如下图所示。

基本设计	置 权限	对象	用户权限 角	迫色权限	时间对象	在线用户		
面清空	在线用户						息	i+: 1
用户名	认证服务器	认证类型	短信认证状态	隧道状态	远端地址	虚拟地址	登录时间	删除
test	localdb	LOCAL	不需要短信认证	协商成功	192.168.83.220	11.11.11.20	19:03:13	3

i) 在 VRC 用户主机中,通过 CuteFTP 客户端工具可以成功登录并访问内网 FTP 服务器"10.10.10.2",如下图所示。

🔟 (10. 10	). 10. 2) - GlobalS	CAPE, Inc	CuteFTP	5.0 XP				
文件(2) 第	編辑(2) 査看(⊻) 书:	签(B) 命令(C)	传输 (I)	窗口()	帮助(H)			
🔰 🖉	in 🖉 🎾 🖓	V 🕜 🔁			🗉   P B]	🗙 🥺 💆	ų.	
状态:>	正在连接数据 socket							
	125 Data connection a	ilready open; Tran	sfer startin	g.				
状态:>	已接收 200 字节,正	常。						
状态:>	时间:0:00:01,效率	: 0.20 KB/秒 (200	字节/秒)					
	226 Transfer complete	·.						
状态:>	完成。							•
•								
C:\Docur	nents and Settings\wang	gfurong\桌面		- 🖻	1			<b>_</b>
名称				大小□▲	名称		大小日期	时间
🚞 communi	tation			0 20	🚞 公司产品		2008-1.	16:10
Economy				0 2C	(二) 实用工具		2008-3-	27 14:3
E7 IE7				0 2C	🚞 学习资料		2008-1-	18 10:5
🚞 new				0 2C	🔁 英文手册参考	5	2009-4-	2 16:3
🚞 share				0 2C				
🚞 temp				0 2C				
🚞 标准版				0 2C				
🚞 鸟巢				0 20				
🦳 呜哩 啡 🖷	ψ <b></b>			0 20				
本地		大小	远程			主机	状态	
E:\		5KB <	<- /Hap	opy99.zip		192.168.83.218	已取消	
E:\		351 <	<- /Bat	282.zip		192.168.83.218	已取消	
EX .		64U <	<- /BEF	(Y.ZIP 202 -iin		192.168.83.218	错误	
15		301 4	<- /Bat	.282.2lp		192.108.83.218	错误	-
							队列: 852+ KB / O KB	

## 注意事项

1) 在 IPSec VPN 网关中,必须开启与客户端主机相连的网关接口所属区域的 IPSec 功能;必须关闭"包校验和"开关(默认情况下是关闭的)。

2) VPN 远程客户端的安装请参见《VRC 用户手册》。

3) VRC 用户访问授权资源前,必须关闭客户端主机中的软件防火墙和防病毒软件, 否则即使 VRC 隧道协商成功,也可能会无法正常通讯。

# 远程用户集中管理

在天融信 IPSec VPN 网关中,既可以通过 TopPolicy 安全设备与策略管理系统(以下 简称 TopPolicy 系统)对 VRC 用户进行集中管理,也可以在网关中对 VRC 用户进行本地 管理。TP 集中管理方式下,客户端认证由 TopPolicy 系统完成;本地管理模式下,客户端 认证由 IPSec VPN 网关或其他认证服务器等完成。本案例主要介绍如何使用 TopPolicy 系 统对 VRC 用户进行集中管理。

# 基本需求

1) 通过 TopPolicy 系统对 VRC 用户"test"进行集中管理。

2) TopPolicy 系统对 VRC 用户"test"采用口令认证方式。

3) VRC 用户 "test" 认证成功并建立隧道后,获得 TopPolicy 系统赋予该用户的内网 资源 "10.10.10.0/24" 的访问权限。



图 24 远程用户集中认证示意图

## 配置要点

- ▶ 开放 Eth0 口所属区域的 GUI 服务和 IPSecVPN 服务。
- ▶ 绑定 IPSec 虚接口。
- ▶ 配置 VRC 认证的基本参数。
- ▶ 配置 TopPolicy 服务器。
- ➢ 验证: VRC 用户 "test"使用口令证书方式登录 IPSec VPN 网关后,获得内网 "10.10.10.0/24"的访问权限。

# WebUI 配置步骤

1. 开放 Eth0 口所属区域的 GUI 服务和 IPSecVPN 服务。

1)选择 资源管理 > 区域,设置 Eth0、Eth1 所属区域,缺省访问权限为"允许", 如下图所示。

区域				
🕂 添加 🗴 清空				总计: 2
名称 🔶	绑定属性     ◆	权限	注释	操作
area_eth0	eth0	允许		
area_eth1	eth1	允许		2

2) 开放 Eth0 口所属区域的 GUI 服务。

选择 **系统管理 > 配置**,然后激活"开放服务"页签,点击"添加"增加一条规则, 如下图所示。

系统参数	开放服务	时间	SNMP	部件设
		修改	配置	
	服务名和	弥 GUI		*
	控制区均	或 area_et	h0	•
	控制地址	止 any 隊吉昌	3]	*
		确定	取消	

参数设置完成后,点击"确定"按钮。

3) 开放 Eth0 口所属区域的 IPSecVPN 服务。

选择 **系统管理 > 配置**,然后激活"开放服务"页签,点击"添加"增加一条规则, 如下图所示。

系统参数	开放服务	时间 SNMP	邮件设置
		修改配置	
	服务名称	IPSecVPN	*
	控制区域	area_eth0	•
	控制地址	any (范围)	*
	व		(2)消

参数设置完成后,点击"确定"按钮。

#### 2. 绑定 IPSec 虚接口。

选择 虚拟专网 > 虚接口绑定, 然后点击"添加", 绑定虚接口 ipsec0, 如下图所示。

虚接口绑定	
	虚拟接口绑定
	虚接口名 ipsec0 ▼ 通告TP地址 绑定接口名 eth0 ▼ 接口地址
	确定 取消

参数设置完成后,点击"确定"按钮。

3. 配置 VRC 认证的基本参数。

a)选择 **虚拟专网 > VRC 管理**,然后激活"基本设置"页签,设置相关内容,如下 图所示。

基本设置	权限对象	用户权限 角	自色枳限 📃	时间对象	在线用户
			基本配	置	
		认证管理模式	TP集中管理	•	
		DHCP地址池	不添加		•
		▼高级			
		检查超时间隔	30		[10-600秒,缺省:30]
		保活超时时间	120		[30-300秒,缺省:120]
		内部首选DNS服务器	0.0.0.0		[IP地址]
		内部备用DNS服务器	0.0.0.0		[IP地址]
		内部首选WINS服务器	0.0.0.0		[IP地址]
		内部备用WINS服务器	0.0.0.0		[IP地址]
		与防火墙联动	否	•	
		客户端版本控制	否	•	
		强制短信认证	否	•	
		短信口令长度	5		[1-255,缺省:5]
		短信尝试次数	3		[1-10次,缺省:3]
		短信有效时间	180		[1-255秒,缺省:180]
			证书认证权	限控制	
		查找证书用户	否	•	
		允许无证书用户登录	不允许	-	
		CN域选择	启用		
		MAIL域选择	不启用	~	
		应用		重启	服务

b)参数设置完成后,点击"应用"按钮。

#### 4. 配置 TopPolicy 服务器。

假设 TopPolicy 服务器能够管理本案例中的 IPSec VPN 网关,并且该网关主动向 TopPolicy 系统注册。在 TopPolicy 系统中还需要进行以下配置:

- a) 设置邮件参数。
- b) 配置 web 服务器。

c)设置地址池(地址网段为"172.16.1.0")。

d)添加用户角色"doc\_role",然后为该角色配置可访问的网关(允许访问本案例中的 IPSec VPN 网关),最后自定义网关权限(允许访问网段"10.10.10.0/24")。

e)添加移动用户组"doc\_group"(该移动用户组的地址网段为"172.16.1.0",需要验证口令,关联的用户角色为"doc\_role")。

f) 在移动用户组"doc\_group"中添加 VRC 用户"test"。

g)对"test"进行软件分发。

相关操作步骤请参见《TopPolicy 安全设备与策略管理系统用户手册》的介绍,此处不再赘述。

5. 验证: VRC 用户 "test" 使用口令证书方式登录 IPSec VPN 网关后,获得内网 "10.10.10.0/24"的访问权限。

VRC 用户"test"收到主题为"VRC 分发邮件通知"的邮件后,还需要进行以下配置:
a)将邮件附件解压到本地某文件夹中(包括:TPDownload.exe、config.ini、config.xml,
因为 test 用户为口令认证,所以该文件夹中没有用户证书和私钥),然后运行解压后的
TPDownload.exe 执行文件,弹出如下图所示界面。

🛷 软件分发程序	4		_ <b>_</b> X
服务器地址1:			
服务器地址2:			
下载文件列表			
文件名称	文件大小	下载状态	
[	获取	下载	取消
<u> </u>			

b) 点击"获取"按钮,可以从 TP 服务器端得到 VRC 安装程序,界面如下图所示。

ᢦ 软件分发程	序		
服务器地址1:	http://192.168.83.2	218:8080	
服务器地址2: 下载文件列表	пср.//0.0.0.0.0000		
文件名称		下載状态	
VRC.exe	6096658	未完成	
	获取	下载	取消

c)点击"下载"按钮,可以将 VRC 软件下载至管理器所在主机上 TPDownkload.exe 所在文件夹中,然后弹出下载成功提示框,如下图所示。

TPDownl	oad X	I
1	文件全部下载成功 <b>!</b>	
	确定	

d) 点击"确定"按钮, 然后点击"完成"按钮即可。

e)下载完成后,双击自解压压缩文件 VRC.exe 文件,将 VRC 安装程序解压到当前目录中。

f)运行 setup.exe 进行 VRC 安装。安装过程比较简单,在此不再详述。

安装完成后,会在桌面创建启动 VPN 连接的快捷方式,如下图所示。



g) 双击 VPN 连接的快捷图标,进入 VPN 客户端。根据 TopPolicy 系统分配的权限, VRC 安装系统已经自动为 VRC 用户建立了 VPN 连接"237.root"。VPN 连接的名称即是 TP 上 VPN 网关设备的名称,如下图所示。

🌄 VPII客户端	连接管理			<u>- 🗆 ×</u>
文件 编辑	视图语言 🖣	習助		
3				
新建VPN连接	237	237.root		

h) 双击"237.TPRoot"图标, 弹出 VPN 客户端认证窗口。由于用户"test"所属用 户组要求验证口令和证书,因此 VPN 客户端窗口中已经导入了用户证书和密码,无需用 户手动输入,如下图所示。

- <sup>且</sup> ¥PII客户i		0. Ú.	24	11.5	×
					7
口 令:	***	****	1.0		
<ul><li>✓ 保存X</li><li>连接</li></ul>	509证书认证 取消	£的口令 	属性		5

i) 在"VPN 客户端"窗口中点击"连接"按钮,稍后,即可与 VPN 网关建立连接。

① 通过 "VPN 客户端属性"窗口, VRC 用户可以查看隧道状态,接收/发送字节, 以及虚拟网卡地址和中心网关地址等信息,如下图所示。

₽ <mark>.</mark> VPII客户端属性	2
策略 支持	
┌隧道	
状态	隧道协商成功
隧道持续时间	0:00:09
┌活动	
正确接收字节数	0
正确发送字节数	0
未知错误字节数	0
[] 启动选项	重新协商 修改密码
□ 显示IKE协商进程	断开 关闭

۹ <b>L</b> I	VPI客户端尾性	×
策	食略 支持	
	□本地	
	隧道本地端点 192.168.83.220	
	虚拟网卡地址 172.16.1.1	
	(詳細)	
	IP地址 192.168.83.237	
	XX.X+14	
Γ	显示IKE协商进程 断开	关闭

点击"访问控制"按钮,可以查看 VRC 用户的访问权限,如下图所示。

ù	问控制列表					×
	目的IP	目的掩码	协议	端口	策略	有效时间.
	10.10.10.0	255.255.255.0	ANY	端口未	允许	永久
	4					
				刷新		关闭

② 在 VRC 用户主机中,可以通过命令 "route print" 查看本地路由配置,如下图所示。

Active	Routes:				
Network	Destination	n Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0	192.168.83.1	192.168.83.220	20
	10.10.10.0	255.255.255.0	172.16.1.2	172.16.1.1	1
· ·	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
	172.16.1.0	255.255.255.0	172.16.1.1	172.16.1.1	10
	172.16.1.1	255.255.255.255	127.0.0.1	127.0.0.1	10
172.	16.255.255	255.255.255.255	172.16.1.1	172.16.1.1	10
19	2.168.83.0	255.255.255.0	192.168.83.220	192.168.83.220	20
192.	168.83.220	255.255.255.255	127.0.0.1	127.0.0.1	20
192.	168.83.255	255.255.255.255	192.168.83.220	192.168.83.220	20
	224.0.0.0	240.0.0.0	172.16.1.1	172.16.1.1	10
	224.0.0.0	240.0.0.0	192.168.83.220	192.168.83.220	20
255.2	55.255.255	255.255.255.255	172.16.1.1	172.16.1.1	1
255.2	55.255.255	255.255.255.255	172.16.1.1	4	1
255.2	55.255.255	255.255.255.255	192.168.83.220	192.168.83.220	1
Default	Gateway:	192.168.83.1			
======					
Persist	ent Routes:				
None					

g)在 IPSec VPN 网关中,选择 网络管理 > 路由,然后激活"路由表"页签,可以 查看网关上新增的目的地址为虚拟网卡 IP 的路由信息,如下图所示。

路由表 策略路由	动态路由OSPF	्रह	うる路由RI	P 动	态路由BGP	多播路由	্ৰ ক্যা;	
际记: U-Up, G-Gateway specified, L-Local, C-Connected, S-Static O-Ospf, R-Rip, B-Bgp, D-Dhcp, I- Ipsec, i-Interface specified								
🕂 添加 🗴 清空						È.	急计: 8	
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除	
192.168.83.237/32	0.0.0.0	ULi	1	1	10	-	-	
10.10.10.1/32	0.0.0.0	ULi	1	1	10	-	-	
12, 12, 12, 1/32	0.0.0.0	ULi	1	1	10	-	-	
172, 16, 1, 1/32	192, 168, 83, 237	UGIi	1	1	ipsec0	-	-	
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-	
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-	
10, 10, 10, 0/24	0.0.0.0	UCi	10	1	eth1	-	-	
12. 12. 12. 0/24	0.0.0	UCi	200	1	sslvpnO	-	-	

选择 **虚拟专网 > VRC 管理**, 然后激活"在线用户"页签, 可以查看防火墙上的 VRC 用户信息, 如下图所示。

基本设计	置 权限	对象	用户权限 角	色权限	时间对象	在线用户		
面清空	在线用户						息	ì†: 1
用户名	认证服务器	认证类型	短信认证状态	隧道状态	远端地址	虚拟地址	登录时间	删除
test	TP	OTHER	不需要短信认证	协商成功	192. 168. 83. 220	172. 16. 1. 1	18:46:59	3

h)在 VRC 用户主机中,通过 CuteFTP 客户端工具可以成功登录并访问内网 FTP 服务器"10.10.10.2",如下图所示。

🔟 (10.10	. 10. 2) - GlobalSC	APE, Inc	CuteFTP	5.0 XP				_	
文件(で) 鎌	辑(E) 查看(Y) 书签	(B) 命令(C)	传输(I)	窗口())	帮助(H)				
🔰 🖉	in 🖉 🖉 🖓	D 🕜 👧			💷   P B]	🗙 🥺 🌽	ų.		
状态:>	正在连接数据 socket								
	125 Data connection alr	eady open; Trar	nsfer startin	<u>]</u> .					
状态:>	已接收 200 字节,正常	<b>.</b>							
状态:>	时间: 0:00:01,效率: 0	).20 KB/秒 (200	字节/秒)						
11	226 Transfer complete.								
状态:>	完成。								
C:\Docum	ients and Settings\wangfi	urong\桌面		<u> </u>	μ			•	
名称				<u>大小 日</u> 一	名称		大小	日期	时间
📄 communic	ation			0 2C	🚞 公司产品			2008-1	16:10
Economy				0 2C	🚞 实用工具			2008-3-27	14:3·
E7				0 2C	一学习资料			2008-1-18	10:5
new				0 2C	🛅 英文手册参考			2009-4-2	16:3
Share				0 2C					
i temp				0 2C					
🗋 标准版				0 2C					
🗀 鸟巢				0 20					
「「「「「「」」「「」」「「」」「」」「」」「」」「」」「」」「」」「」」「」	Ĩ			0 20					
								1	
本地		大小	远程	:		主机		状态	
E:\		5KB	<- /Hap	py99.zip		192.168.83.218		已取消	
E:\		351	<- /Bat - /DEC	282.zip		192.168.83.218		<b>出取</b> 得 2番2回	
EN EN		351	<- /85 <- /8at	(1,21) 282 zin		192.100.03.218		相厌 错误	
155			< )bac /oer			100,100,00,210			_
							队列: 852+ M	CB/0KB	

## 注意事项

1) TP 集中管理模式下, TP 管理员只能为用户组设置访问权限,属于该用户组的用户拥有与用户组相同的访问权限。详细说明请参见《TopPolicy 安全设备与策略管理系统用户手册》。

2) 在 IPSec VPN 网关中,必须开启与客户端主机相连的网关接口所属区域的 IPSec 功能;必须关闭"包校验和"开关(默认情况下是关闭的)。

3) VPN 远程客户端的安装请参见《VRC 用户手册》。

4) VRC 用户访问授权资源前,必须关闭客户端主机中的软件防火墙和防病毒软件, 否则即使 VRC 隧道协商成功,也可能会无法正常通讯。

# VPN 静态隧道(本地配置)

## 基本需求

企业通过两个网络卫士防火墙构建 VPN 通道,保证总部和分支机构的安全通信。

▶ 防火墙 A 的 Eth0 口和防火墙 B 的 Eth0 口参与 VPN 隧道的协商和建立。

- ➢ 防火墙 A 的本地保护子网为 10.10.11.0/24。
- ▶ 防火墙 B 的本地保护子网为 10.10.10.0/24。



#### 图 25 VPN 静态隧道构建示意图

# 配置要点

- 在防火墙 A 和防火墙 B 上开放 Eth0 接口所属区域 "area\_eth0"的 IPSec VPN 服
   务。
- ▶ 在防火墙 A 和防火墙 B 上,绑定虚接口 ipsec0。
- ▶ 在防火墙 A 和防火墙 B 上, 配置静态隧道。
- ▶ 在防火墙 A 和防火墙 B 上查看协商成功的静态隧道。

# WebUI 配置步骤

1. 在防火墙 A 和防火墙 B 上开放 Eth0 接口所属区域 "area\_eth0"的 IPSec VPN 服务。

a) 在导航菜单中选择 资源管理 > 区域, 然后点击"添加", 在弹出的窗口中设置 Eth0 所属区域(area\_eth0), 如下图所示。

区域			
		区域	£
	名称	area_eth0	*
	访问权限	允许	•
	注释		
可用属性:			成员:
ads1 [属性] ads11 [属性] ads12 [属性] ads13 [属性] bond0 [属性]			> eth0
		确定	取消

参数设置完成后,点击"确定"按钮。

b) 在导航菜单中选择 **系统管理 > 配置**, 然后激活"开放服务"页签, 点击"添加" 开放区域 area\_eth0 的 IPSecVPN 服务, 如下图所示。

系统参数	开放服务 时间 SNMP 目	8件设
	添加配置	
	服务名称 IPSecVPN	*
	控制区域 area_ethO	•
	控制地址 any [范围]	*
	确定 取消	

参数设置完成后,点击"确定"按钮。

#### 2. 在防火墙 A 和防火墙 B 上,绑定虚接口 ipsec0。

a)在导航菜单栏选择 **虚拟专网 > 虚接口绑定**,点击"添加",将虚接口与物理接口 eth0 绑定。

虚接口绑定			
		虚拟接口绑定	
	虚接口名 通告TP地址 绑定接口名 接口地址	ipsec0 💌 eth0 💌	
	确定	定 取消	)

b)参数设置完成后,点击"确定"按钮。

#### 3. 在防火墙 A 和防火墙 B 上, 配置静态隧道。

1) 在防火墙 A 中的配置如下图所示:

a) 在导航菜单栏选择 **虚拟专网 > 静态隧道**, 然后点击"添加隧道"配置静态隧道 参数。

① 选择"第一阶段协商",设置参数如下图所示。

静态隧道 多线	路策略 一際道	i保活 TP下发静态	隴道						
<b>陇道设置</b>									
第一阶段协商	第二阶段协商								
隧道名 认证方式		233-237 预共享密钥 🔽	】*[不能包含-Ipsec或者-Line]						
预共享密钥 本地标识		•••••	】* [必须包含@]						
对方标识 线路类型		● 建路 ●	[必须包含@]						
动动之王 对方地址或域名 选择TPSEC链路		192.168.83.237	*						
NEJ-11 DIGRIED									
		确定	取消						

高级配置使用系统默认值。

② 选择"第二阶段协商",设置参数如下图所示。

静之	医脱道 多线器	格策略 化隧道	保活 TP下发静态随	道
			離道设	置
	第一阶段协商	第二阶段协商		
	本地子网		10. 10. 11. 1	]
	本地掩码		255, 255, 255, 0	]
	对方子网		10. 10. 10. 1	]
	对方掩码		255, 255, 255, 0	]
			🗌 高级配置	
			确定	取消

高级配置使用系统默认值。

③ 参数设置完成后,点击"确定"按钮。

2) 在防火墙 B 中的配置如下图所示:

a) 在导航菜单栏选择 **虚拟专网 > 静态隧道**, 然后点击"添加隧道"配置静态隧道 参数。

① 选择"第一阶段协商",设置参数如下图所示。

静态隧道 多线	<b>静态隧道</b> 多线路策略 隧道保活 TP下发静态隧道								
隆道设置									
第一阶段协商	第二阶段协商								
隧道名 认证方式		237-233 预共享密钥 🔽	*[不能包含-Ipsec或者-Line]						
预共享密钥 本地标识		•••••	】* Ⅰ 2 / (石) - (A) - 1						
本地称 ki 对方标识			[必须包含@] [必须包含@]						
线路类型 对方地址或域名		单线路 192.168.83.233	*						
选择IPSEC链路		ipsec0 💌							
		□ 高级配置 确定	取消						

高级配置使用系统默认值。

② 选择"第二阶段协商",设置参数如下图所示。

静之	新羅道 🔷 多线器	格策略 一一隧道(	保活 TP下发静态隙	道
			隧道设	置
	第一阶段协商	第二阶段协商		
	本地子网		10. 10. 10. 0	]
	本地掩码		255, 255, 255, 0	]
	对方子网		10.10.11.0	]
	对方掩码		255, 255, 255, 0	]
			🗆 高级配置	
			确定	取消

高级配置使用系统默认值。

③ 参数设置完成后,点击"确定"按钮。

#### 4. 在防火墙 A 和防火墙 B 上查看协商成功的静态隧道。

 防火墙 A 上可以通过选择 虚拟专网 > 静态隧道, 查看到协商成功的隧道, 如下 图所示。

静态隧道	多线路策■	各 🔪 隧道保活	TP下发静	态隧道						
♣添加隧道 C 默认参数设置 m 清空隧道 总计:1										
隧道	本地子网	远端网关	对方子网	隧道状态	活跃接口	协商	拆除	修改	删除	状态
233-237	10, 10, 11, 1/24	192. 168. 83. 237	10.10.10.1/24	第二阶段 协商成功	192. 168. 83. 237	7	7		3	
					н	• 1	► H	转到	ı∏/:	1 Go

防火墙 A 的静态路由表中会添加一条静态路由,目的地址为防火墙 B 的本地保护子网(10.10.10.0/24),如下图所示(选择 网络管理 > 路由,然后激活"路由表"页签)。

路由表 策略路由	动态路由OSPF	R	b态路由RI	P क्रि	态路由BGP	多播路由	动 초
标记: U-Up, G-Gateway : i-Interface specified	specified, L-Local,	C-Conne	cted, S-St	atic O-Os;	pf, R-Rip, B-Bgp	, D-Dhep, 1	I-Ipsec,
🕂 添加 🗴 清空						;	急计: 8
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除
192.168.83.233/32	0.0.0.0	ULi	1	1	10	-	-
12. 12. 12. 1/32	0.0.0.0	ULi	1	1	10	-	-
10.10.11.1/32	0.0.0.0	ULi	1	1	10	-	-
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-
12. 12. 12. 0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-
10.10.11.0/24	0.0.0.0	UCi	10	1	eth1	-	-
10.10.10.0/24	192. 168. 83. 233	UGIi	100	1	ipsec0	-	-

② 防火墙 B 上可以通过选择 **虚拟专网 > 静态隧道**,查看到协商成功的隧道,如下 图所示。

<b>静态隧道</b> 多线路策略 隧道保活 TP下发静态隧道										
♣添加隧道 C 默认参数设置 前 清空隧道 总计:1										
隧道	本地子网	子网 远端网关 对方子网			活跃接口	协商	拆除	修改	删除	状态
237-233	10, 10, 10, 0/24	192. 168. 83. 233	10.10.11.0/24	第二阶段 协商成功	192. 168. 83. 233	7	7		3	
	K ◀ 1 ▶ N 转到 /1 Go									

防火墙 B 的静态路由表中会添加一条静态路由,目的地址为防火墙 A 的本地保护子

网(10.10.11.0/24),如下图所示(选择 网络管理 > 路由,然后激活"路由表"页签)。

路由表 策略路由	动态路由OSPF	্বর	)态路由RI	P 】动	态路由BGP	多播路由	ু কার			
标记: U-Up, G-Gateway specified, L-Local, C-Connected, S-Static O-Ospf, R-Rip, B-Bgp, D-Dhcp, I- Ipsec, i-Interface specified										
♣ 添加										
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除			
192. 168. 83. 237/32	0.0.0.0	ULi	1	1	10	-	-			
12, 12, 12, 1/32	0.0.0.0	ULi	1	1	10	-	-			
10.10.10.1/32	0.0.0.0	ULi	1	1	10	-	-			
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-			
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-			
12. 12. 12. 0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-			
10, 10, 10, 0/24	0.0.0.0	UCi	10	1	eth1	-	-			
10.10.11.0/24	192, 168, 83, 237	UGIi	100	1	ipsec0	-	-			

## 注意事项

隧道协商选项设置,至少有一端防火墙设置成为"主动发起隧道协商"。

# VPN 动态隧道(集中管理)

# 基本需求

企业通过两个网络卫士防火墙及 TopPolicy 系统构建 VPN 通道,保证总部和分支机构的安全通信。

- ▶ 防火墙 A 的 Eth0 口和防火墙 B 的 Eth0 口参与 VPN 隧道的协商和建立
- ➢ 防火墙 A 的本地保护子网为 10.10.11.0/24
- ➢ 防火墙 B 的本地保护子网为 10.10.10.0/24

▶ TP 服务器地址为 192.168.83.218



图 26 集中管理 VPN 隧道示意图

## 配置要点

- ➤ 在防火墙 A 和防火墙 B 上,开放与 TP 服务器相连的接口 "eth0"所属区域 "area\_eth0"的 GUI 服务。
- ▶ 配置 TP 服务器。
- 在防火墙 A 和防火墙 B 上开放 Eth0 接口所属区域 "area\_eth0"的 IPSec VPN 服
   务。
- ▶ 在防火墙 A 和防火墙 B 上,绑定虚接口 ipsec0。
- ▶ 在防火墙 A 和防火墙 B 上配置本地保护子网(可选)。
- ▶ 在防火墙 A 和防火墙 B 上查看 TopPolicy 系统下发的动态隧道。

# WebUI 配置步骤

1. 在防火墙 A 和防火墙 B 上,开放与 TP 服务器相连的接口 "eth0" 所属区域 "area\_eth0"的 GUI 服务。

a) 在导航菜单中选择 资源管理 > 区域, 然后点击"添加", 在弹出的窗口中设置 Eth0 所属区域(area\_eth0), 如下图所示。

区域		
		区域
	名称 访问权限 注释	area_eth0 * 允许
可用属性: ads1 [属性] ads11 [属性] ads12 [属性] ads13 [属性] bond0 [属性]		成员: -> × (eth0)
		确定取消

参数设置完成后,点击"确定"按钮。

b) 在导航菜单中选择 系统管理 > 配置, 然后激活"开放服务"页签, 点击"添加" 开放区域 area\_eth0 的 GUI 服务, 如下图所示。

系统参数	开放服务 时间 SNMP	邮件设
	修改配置	
	服务名称 GUI 控制区域 area_eth0 控制地址 any 范围)	<ul><li>✓</li><li>✓</li></ul>
	确定 取消	

参数设置完成后,点击"确定"按钮。

#### 2. 配置 TP 服务器。

在 TP 服务器中配置相关参数,使防火墙 A 和防火墙 B 分别上线,然后配置 VPN 策略,最后配置防火墙 A 与防火墙 B 之间的 VPN 隧道。具体操作步骤请参见《TopPolicy 安全设备与策略管理系统用户手册》的介绍,此处不再赘述。

3. 在防火墙 A 和防火墙 B 上开放 Eth0 接口所属区域 "area\_eth0"的 IPSec VPN 服务。

a) 在导航菜单中选择 **系统管理 > 配置**, 然后激活"开放服务"页签, 点击"添加" 开放区域 area\_eth0 的 IPSecVPN 服务, 如下图所示。

系统参数	开放服务 时间	SNMP 邮件设
	添加配置	Ē
	服务名称 IPSecVPN 控制区域 area_eth0 控制地址 any 范围]	<ul> <li></li> <li></li></ul>
	确定	取消

b)参数设置完成后,点击"确定"按钮。

#### 4. 在防火墙 A 和防火墙 B 上,绑定虚接口 ipsec0。

a)在导航菜单栏选择 **虚拟专网 > 虚接口绑定**,点击"添加",将虚接口与物理接口 eth0 绑定。

虚接口绑定	
	虚拟接口绑定
	虚接口名 ipsec0 ▼ 通告TP地址 绑定接口名 eth0 ▼ 接口地址
	确定 取消

b)参数设置完成后,点击"确定"按钮。

#### 5. 在防火墙 A 和防火墙 B 上配置本地保护子网(可选)。

如果 TopPolicy 系统管理员在添加设备时配置了设备子网,则此步骤的配置可以省略。

1) 在防火墙 A 上的配置如下所示:

a)选择 **虚拟专网 > 动态隧道**,然后激活"本地保护子网"页签,点击"添加", 设置防火墙 A 的本地保护子网,如下图所示。

本地保护子网	下载设行	备列表		下载子网	列表
	VD	<b>:本地保</b>	护子	9	
	子网	10.10.1	1.0		
	掩码	255, 255	5. 255.	0	
	确定			取消	

b)参数设置完成后,点击"确定"按钮。

2) 在防火墙 B 上的配置如下所示:

a)选择 **虚拟专网 > 动态隧道**,然后激活"本地保护子网"页签,点击"添加", 设置防火墙 B 的本地保护子网,如下图所示。

本地保护子网	下载设	备列表	下载子网列
	<b>UV</b>	C本地保护于	× [0]
	子网	10. 10. 10. 0	
	掩码	255, 255, 25	5.0
	确定		取消

b)参数设置完成后,点击"确定"按钮。

#### 6. 在防火墙 A 和防火墙 B 上查看 TopPolicy 系统下发的动态隧道。

上述配置完成后,防火墙 A 和防火墙 B 之间将自动协商动态隧道。

a) 在防火墙 A 上查看协商成功的动态隧道:

① 选择 虚拟专网 > 动态隧道, 然后激活"下载设备列表"页签, 如下图所示。

本地保护	本地保护子网 下载设备列表 下载子网列表 下载隧道列表 下载隧道状态 设备优先级							
总计: 1								
设备状态	设备名称	公网地址	接口名	接口地址	线路优先级	设备优先级	nat状态	
在线	237. TopPolicy	192. 168. 83. 237	eth0	192. 168. 83. 237	0	0	设备不在NAT后面	

② 选择 虚拟专网 > 动态隧道, 然后激活"下载子网列表"页签, 如下图所示。

本地保护子网 下载设备列表	下载子阿列表	下载隧	道列表	下载隧道状态	\ 设备优
					总计: 1
设备名称	子网IP地址		子网掩码		
237. TopPolicy	10. 10. 10. 0		255, 255, 2	55.0	

③ 选择 虚拟专网 > 动态隧道, 然后激活"下载隧道列表"页签, 如下图所示。

本地保护子网 下载设备列表 下载子网列表 下载隧道列表 下载隧道状态 设备优先级										
	总计: 1									
隧道状态	隧道名称	左端设备名称	右端设备名称	中间设备名称	认证方式	封装协议	封装模式	加密算法	数据压缩	
活跃	233-237	233. TopPolicy	237. TopPolicy		证书认证	ESP	隧道模式	3DES-MD5	不压缩	

④ 选择 虚拟专网 > 动态隧道, 然后激活"下载隧道状态"页签, 如下图所示。

本地保护子	「阿」 下載	战役备列表 下語	载子网列表 下	载隧道列表 下	载隧道状态	设备优务
						总计: 1
隧道名称	隧道状态	服务器名	左端地址	右端地址	左端接口	右端接口
233-237	活跃	237. TopPolicy	192.168.83.233	192.168.83.237	eth0	eth0

⑤ 防火墙 A 的静态路由表中会添加一条静态路由,目的地址为防火墙 B 的本地保护 子网(10.10.10.0/24),如下图所示(选择 网络管理 > 路由,然后激活"路由表"页签)。

路由表 策略路由	动态路由OSPF	ः ह	カ <mark>态路由</mark> RI	iP 】动	态路由BGP	多播路由	动 쳐
标记: U-Up, G-Gateway i-Interface specified	specified, L-Local,	C-Conne	cted, S-St	tatic O-Os	pf, R-Rip, B-H	8gp, D-Dhep, 1	I-Ipsec,
🕂 添加 🗴 清空							总计: 8
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除
192.168.83.233/32	0.0.0.0	ULi	1	1	10	-	-
12. 12. 12. 1/32	0.0.0.0	ULi	1	1	10	-	-
10.10.11.1/32	0.0.0.0	ULi	1	1	10	-	-
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-
12. 12. 12. 0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-
10.10.11.0/24	0.0.0.0	UCi	10	1	eth1	-	-
10, 10, 10, 0/24	192, 168, 83, 233	UGIi	100	1	ipsec0	-	-

b) 在防火墙 B 上查看协商成功的动态隧道:

① 选择 虚拟专网 > 动态隧道, 然后激活"下载设备列表"页签, 如下图所示。

本地保护	子网下载	设备列表 🛛 下	载子网羽	刘表 下载隆	道列表	下载隧道状	态 🔪 设备优先级
							总计: 1
设备状态	设备名称	公网地址	接口名	接口地址	线路优先级	设备优先级	nat状态
在线	233. TopPolicy	192. 168. 83. 233	eth0	192, 168, 83, 233	0	0	设备不在NAT后面

② 选择 虚拟专网 > 动态隧道, 然后激活"下载子网列表"页签, 如下图所示。

本地保护子网 下载设备列表	下载子网列表 下载隧道	刘表 下载雕道状态 设备优先级
		总计: 1
设备名称	子网IP地址	子网掩码
233. TopPolicy	10. 10. 11. 0	255. 255. 255. 0

③ 选择 虚拟专网 > 动态隧道, 然后激活"下载隧道列表"页签, 如下图所示。

本地保护	7M	下载设备列表	【 下载子网列	表下载陶	缝列表	下载隧	道状态	设备优务	缬
									总计: 1
隧道状态	隧道名称	左端设备名称	右端设备名称	中间设备名称	认证方式	封装协议	封装模式	加密算法	数据压缩
活跃	233-237	237. TopPolicy	233. TopPolicy		证书认证	ESP	隧道模式	3DES-MD5	不压缩

④ 选择 虚拟专网 > 动态隧道, 然后激活"下载隧道状态"页签, 如下图所示。

本地保护子	可 下载记	と 後日	网列表 下载隧道	·列表 下载雕道状	<b>凌</b>	优先级
						总计: 1
隧道名称	隧道状态	服务器名	左端地址	右端地址	左端接口	右端接口
233-237	活跃	233. TopPolicy	192. 168. 83. 237	192. 168. 83. 233	eth0	eth0

⑤ 防火墙 B 的静态路由表中会添加一条静态路由,目的地址为防火墙 A 的本地保护 子网(10.10.11.0/24),如下图所示(选择 网络管理 > 路由,然后激活"路由表"页签)。

路由表 策略路由	动态路由OSPF	न्द्र	b态路由RI	P रियो	态路由BGP	多播路由	ন্যার
标记: U-Up, G-Gateway Ipsec, i-Interface spe	specified, L-Local, cified	C-Conne	cted, S-St	tatic O-Os	pf, R-Rip, B-Bgp,	D-Dhep,	I-
🕂 添加 🗴 清空						È	急计: 8
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除
192.168.83.237/32	0.0.0.0	ULi	1	1	10	-	-
12. 12. 12. 1/32	0.0.0.0	ULi	1	1	10	-	-
10.10.10.1/32	0.0.0.0	ULi	1	1	10	-	-
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-
12. 12. 12. 0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-
10.10.10.0/24	0.0.0.0	UCi	10	1	ethi	-	-
10.10.11.0/24	192, 168, 83, 237	UGIi	100	1	ipsec0	-	-

# 注意事项

1) Tp 服务器的根证书在软件安装时会自动生成或导入。

2) 隧道的启用、停用等操作可以在 TP 管理中的相应的通信中进行操作。

3)本例中防火墙参与 VPN 隧道协商的接口使用了私有 IP,在实际环境中,可以使用公有 IP。

# SSL VPN 配置案例

加载了天融信 SSL VPN 引擎的网络卫士防火墙,具备一切 SSL VPN 网关的功能,可 作为一台标准的 SSL VPN 网关使用。如无特殊说明,本文档中涉及到的 SSL VPN 网关均 指加载了天融信 SSL VPN 引擎的网络卫士防火墙。

# Web 转发

用户的应用系统为 B/S 结构应用,应用系统中没有复杂的 javascript、flash、activex 控件等页面元素。用户希望能够远程访问应用系统,并进行基于 URL 的访问内容安全控 制,无需安装客户端浏览器控件。使用网关内置的用户数据库进行认证授权,用户登录采 用用户+口令的认证方式,不需要图形认证码。所有移动用户分为普通职员和经理两个角 色,分别授权访问内部不同的应用服务器。所有用户都不允许多点登录。网关设备采用快 速简易的安装方式,不影响用户原有的网络环境。

## 基本需求

- ➤ 采用单臂模式,将 SSL VPN 网关部署在网络内部。SSL VPN 网关的对外 IP 为 "172.16.1.6",内网 IP 为 "192.168.83.237"。
- ▶ 采用"用户+口令"的认证方式对用户进行认证。
- ▶ 禁止角色 "user"中的用户 "user1"多点登录,只允许该用户访问公司内网的 Web 服务器 "192.168.83.218"。
- 禁止角色"manager"中的用户"manager1"多点登录,并且允许该用户访问公司内网的 Web 服务器"192.168.83.218"和"192.168.83.235"。
   网络示意图如下所示。



图 27 SSL VPN 网关 Web 转发示意图

# 配置要点

- ▶ 在防火墙 A 上进行相关配置
- ▶ 添加用户
- ▶ 添加角色
- ▶ 配置授权资源
- ➤ 配置 ACL 规则
- ▶ 配置安全策略
- ▶ 配置虚拟门户
- ▶ 验证:在 SSL VPN 网关的用户界面中,用户成功登录后可以访问授权资源。

# 防火墙 A 的配置步骤

为了保护 SSL VPN 网关的安全,管理员一般将防火墙 A 的 eth0 口所属区域的权限设置为"禁止访问",然后通过配置访问控制规则,只允许远程用户对 SSL VPN 网关上特定端口进行访问。

1) 在防火墙 A 上开放 TCP 443 端口,用于远程用户访问 SSL VPN 网关用户界面,如下图所示。

預定义	自定义	服务组		
十 添加 (	前清空			
				总计: 1
名称			\$ 详细	\$ 操作
443			TCP/443	2

#### 2) 定义访问控制规则,如下图所示。

访问控制									
目的区域	所有区域	•	策略组	所有组	•	高级推	建索	□ 纺	计信息
十 添加約	由十添	加策略					总计:1 🕯	毎页: 30条	•
ID	控制	源		目的			服务	选项	操作
8088	1	<mark>区域:</mark> area_eth1		区域: area_eth(	)		443		
						н	< 1 →	▶ 转到	/1 Go

3) 配置主机地址,即 SSL VPN 网关的真实地址"192.168.83.237"和对外地址

"172.16.1.6"	,	如下图所示。
--------------	---	--------

主机 范围 子网 地址組						
✤ 添加  6 清空 总计: 2						
名称 🔶	IP地址 ◆	操作				
SV	172. 16. 1. 6	2				
SV_MAP 192. 168. 83. 237						

#### 4) 配置双向地址转换(到 SSL VPN 网关的映射),如下图所示。

地址转换							
目的区域	所有区域	▶ 高级搜索	□ 统	计信息			
十 添加	+ 添加 总计:1 毎页: 30条 ▼						
ID	类型	源	目的	服务	转换	操作	
8092	双向转换	区域: area_eth1	<del>地址</del> : SV		源: ethO 目的: SV_MAP		
				H 4	1 1 1 转到 /	1 Go	

# WEBUI 配置步骤

1. 添加用户。

a) 点击导航菜单 **用户认证 > 用户管理**, 然后激活"用户管理"页签 , 点击"添加 用户"。

- b)分别添加普通职员用户 user1 和经理用户 manager1。
- ① 添加普通职员用户 user1, 禁止多点登录, 如下图所示。

用户管理 🔪 🧃	至线用户 用户设	置	
		用户属性	
	田白夕		*
	찌/ 집	useri	
	用尸描还		_
	认证方式	本地口令认证	-
	口令	•••••	* [6-31个字符]
	确认口令	•••••	*
	可用角色		所属角色
	doc_role		
	cert_role	->	
		×	
	1		
	高级		
	用户邮箱		
	用户手机号码		
	登录地址范围		[IP±地址]
			[掩码地址]
	用户有效期		[起始时间]
		F+2-+	[结束时间]
	指定小时地址	LY谷元G:IIII-MM-DD HH:MM	1:55] 
	用户状态		
	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
	硬件特征码绑定	停用 🔽	
	IPsecVPN认证配置		
	客户端版本控制	默认 💌	
	SSLVPN认证配置		
	是否允许多点登录	禁止 🔽	
		確定	田治
		NHIXE	40.10

参数设置完成后,点击"确定"按钮完成配置。

② 添加经理用户 manager1, 禁止多点登录, 如下图所示。

用户管理	在线用户 用户设置				
	用户属性				
	田白夕	1	*		
	用户一组	manageri			
	用尸抽还				
	认证方式	本地口令认证	<b>_</b>		
	口令	•••••	* [6-31个字符]		
	确认口令	•••••	*		
	可用角色		所属角色		
	doc_role test role				
	cert_role	->			
		×			
	高绑	J			
			1		
	用户手机号码		]		
	容录地址范围		┎┰┲┾╫┾╟┨		
			[11 203][]		
	用户有效期		「記憶時」		
			[結束时间]		
		[格式:ҮҮҮҮ-ММ-ДД ЮН:М	M:SS]		
	指定VIP地址				
	用户状态	启用			
	是否允许用户修改密码	Ŋ 允许	]		
	硬件特征码绑定	停用	]		
	IPsecVPN认证配置				
	客户端版本控制	默认 💽			
	SSLVPN认证配置		-		
	是否允许多点登录	禁止 🔽			
			The Ma		
		确定	取消		

参数设置完成后,点击"确定"按钮完成配置。

#### 2. 添加角色,并为其添加成员。

a) 点击导航菜单 **用户认证 > 角色管理**, 激活"角色管理"页签, 然后点击"添加 角色"。

b)分别添加普通职员级角色 user 和经理级角色 manager。

① 添加普通职员级角色 user,并为其添加成员"user1",如下图所示。

角色管理 分级管理				
	角色属性			
角色名 角色描述 DHCP地址池 选择用户 doc() test() manager1()	user * clerk 不添加			
高级				
	确定 取消			

参数设置完成后,点击"确定"按钮完成配置。

② 添加经理级角色 manager,并为其添加成员"manager1",如下图所示。

角色管理 分级管理	角色管理 分级管理				
	角色属性				
角色名 角色描述 DHCP地址池 选择用户 doc() test() user1()	manager * manager 不添加 ■ E经选择 manager1 () ×				
高级					
	确定取消				

参数设置完成后,点击"确定"按钮完成配置。

3. 配置授权资源。

a) 点击导航菜单 SSLVPN > 资源管理, 然后点击资源列表左上方的"添加", 配置 web 转发资源"webforward\_218", 如下图所示。

资源管理	
	添加资源
资源名称 描述 访问方式 资源地址	webforward_218 * [WEB转发 ] [http://192.168.83.218 *
目动打开 在页面显示 单点登陆	
确定	取消

参数设置完成后,点击"确定"按钮。

b)点击导航菜单 SSLVPN > 资源管理,然后点击资源列表左上方的"添加",配置 web 转发资源"webforward\_235",如下图所示。

资源管理			
		添加资源	
	资源名称 描述	webforward_235	*
	访问方式 资源地址	₩EB转发 ▼ http://192.168.83.235	*
	自动打开		
	在贝面显示 单点登陆		
	确定	取消	)

参数设置完成后,点击"确定"按钮。

#### 4. 配置 ACL 规则。

默认禁止远程用户访问内网资源,然后配置两条 ACL 规则,分别允许访问内网资源 "webforward\_218"和 "webforward\_235"。

a) 点击导航菜单 SSLVPN > ACL 管理, 然后在右侧界面中选中 "ACL 默认策略" 右侧的"禁止", 如下图所示。

ACL管理		
ACL默认策略 〇 允许	⊙ 禁止	确定

设置完成后,点击"确定"按钮即可。

b)点击 ACL 规则列表左上方的"添加规则",配置一条允许访问"webforward\_218"的 ACL 规则,如下图所示。

ACL管理		
		添加規則
	规则名称 资源名称 操作 毎周时段 时间 チ 策略 (	允许访问Doc webforward_21▼ 全部 ▼ ▼ 星期→ ▼ 星期二 ▼ 星期三 ▼ 星期四 ▼ 星期五 ▼ 星期六 ▼ 星期日 ▼ 全选* T始: 00:00:00 结束: 23:59:59 [格式 HH:MM:SS] ● 全天 ○ 上午 ○ 下午 ○ 自定义* ● 企注 ○ 禁止
		确定 取消

参数设置完成后,点击"确定"按钮。

c)点击 ACL 规则列表左上方的"添加规则",配置一条允许访问"webforward\_235"的 ACL 规则,如下图所示。

ACL管理		
		添加規則
	规则名称 资源名称 操作 毎周时段 时间 策略	允许访问Test webforward_23 全部 ✓ 星期→ ✓ 星期二 ✓ 星期三 ✓ 星期四 ✓ 星期五 ✓ 星期六 ✓ 星期日 ✓ 全选* 开始: 00:00:00 结束: 23:59:59 [格式 ਮt:MM:SS] ● 全天 ○ 上午 ○ 下午 ○ 自定义* ● 允许 ○ 禁止
		确定 取消

参数设置完成后,点击"确定"按钮。此时,"ACL管理"页面的配置如下图所示。

ACL管理							
ACL默认策略(	ACL默认策略 ⊙ 允许 ○ 禁止   确定						
	-		-				
ACL規則列表							
@添加规则	健 清空规则				总计:2 毎页: 全部	8	•
规则名称	资源名称	行为	策略	星期	时间	修改	删除
允许访问Doc	webforward_218	全部	允许	星期一 星期二 星期三 星期四 星期五 星期六 星期日	00:00:00-23:59:59		3
允许访问Test webforward_235 全部 允许 星期一 星期二 星期三 00:00:00-23:59:59 ♪ ()							
M < 1 ▶ N 转到 /1 Go							

#### 5. 配置安全策略。

为用户"user1"配置一条安全策略,允许该用户访问公司内网的Web服务器 "192.168.83.218";为用户"manager1"配置一条安全策略,允许该用户访问公司内网 的Web服务器"192.168.83.218"和"192.168.83.235"。

a)为用户"user1"配置安全策略。

① 点击导航菜单 SSLVPN > 安全策略,然后选择"用户安全策略"页签,点击用 户"user1"条目右侧的"安全策略设置"图标。

② 勾选"自定义模块设置",然后选中"启用 web 转发",如下图所示。

角色安全策略月	1户安全策略
○ 继承角色配置或启用	默认模块 (WEB转发、应用WEB化、端口转发)
④ 自定义模块设置 (端)	口转发模块和全网接入模块不能同时启用)
☑ 启用₩EB转发	🗌 启用端口转发
🗌 启用全网接入	🗌 启用应用WEB化
确定	返回

设置完成后,点击"确定"按钮。

③ 点击"添加规则",为用户"user1"赋予访问控制权限。由于只允许该用户访问 内网资源"webforward\_218",所以将允许访问该资源的 ACL 规则"允许访问 Doc"赋 予该用户,如下图所示。
角色安全策略	用户安全第	ŧ <b>n</b> a		
		添加規則		
	用户名称 ACL名称	user1 允许访问Doc	•	
	确定		取消	

参数设置完成后,点击"确定"按钮。至此,用户"user1"的安全策略配置完成。

b)为用户"manager1"配置安全策略。

① 点击导航菜单 SSLVPN > 安全策略,然后选择"用户安全策略"页签,点击用 户"manager1"条目右侧的"安全策略设置"图标。

② 勾选"自定义模块设置",然后选中"启用 web 转发",如下图所示。

角色安全策略	目户安全策略
○ 继承角色配置或启用	】默认模块 (WEB转发、应用WEB化、端口转发)
④ 自定义模块设置 (端)	口转发模块和全网接入模块不能同时启用)
☑ 启用WEB转发	□ 启用端口转发
🗌 启用全网接入	🗆 启用应用WEB化
确定	返回

设置完成后,点击"确定"按钮。

③ 点击"添加规则",将允许访问内网资源"webforward\_218"的 ACL 规则"允许 访问 Doc"赋予该用户,如下图所示。

角色安全策略	用户安全第	t i i i i i i i i i i i i i i i i i i i		
		添加規則		
	用户名称 ACL名称	manager1 允许访问Doc	•	
	确定		取消	

参数设置完成后,点击"确定"按钮。

④ 点击"添加规则",将允许访问内网资源"webforward\_235"的 ACL 规则"允许 访问 Test"赋予该用户,如下图所示。

角色安全策略	用户安全策略	
	添加規則	
	用户名称 manager1 ACL名称 允许访问Test 💌	]
	确定 取消	

参数设置完成后,点击"确定"按钮。至此,用户"manager 1"的安全策略配置完成。

## 6. 配置虚拟门户。

a) 点击导航菜单 SSLVPN > 虚拟门户。

b)点击虚拟门户列表左上方的"添加",自定义远程用户访问 SSL VPN 网关的用户 界面。自定义虚拟门户时,参数"地址"必须配置为远程用户登录 SSL VPN 网关时的地 址,即 SSL VPN 网关的对外 IP "172.16.1.6",参数"认证服务器名称"必须配置为对远 程用户进行认证的服务器名称,此案例为本地认证服务器"localdb",而且必须启用 web 转发开关,具体配置页面如下图所示。

6#20		
		委拥行自
		-11 1/81 av
	名称	portal_172 •
	地址	172.16.1.6
	认证服务器名称	localdb -> ×
		localdb
	肥友與	
	80.00 88	
	公告信息	
	选择登录风格	
		Concept (? Mite
	0	
		R (B)
	Logue and Aller	2 他以2 用四子以22 7
	E 13	· · · · · · · · · · · · · · · · · · ·
		USHTE JOHNTE
		111
		● 风格1
		C toath C Mite
	全有信息 无数国际可信用网络 安全世界"作力品牌理会,共同的	RPS:
	■一个米米对在的、日本的、安全的时候也想。	
		ursare lookore
		111
		C 风格2
		C Exten C MP
		C research will
		DOUR HANK METOR
		R/61
	了天殿信	r entresa
		LINETE ADDRESS
		1
		C 风格3
		C Example of Mills
	了医眼的	
	DARA III	KUI 3071UI
	RAS: SVES	B LINETE UNDERS FRANKS
		111
		11
		C 风格4
		3
	白宗兴西东	
	日疋乂以圓	
	控件	◎ 启用 ○ 不启用
		○ 手动安装控件 ● 自动安装控件
	模块开关	▶ 启用端口转发
		▶ 启用全网接入
		☑ 启用web转发
		☑ 启用应用¥EB化
	显示控制	☑ 显示证书信任链下载连接
		▶ 允许关闭浏览器,只显示为小图标
	USB Key 那动下载连接	
	图形认证码设置	● 不显示 ○ 总显示 ○ 登录失败三次后显示
	用户登录认证方式	☑ 口令 ☑ 证书 ☑ 双因子
	企业门户	○ 启用 ④ 不启用
	资源名称	不添加
	是否关闭主页	● 是 ○ 否
	确定	目していていていていていた。

7. 验证:在 SSL VPN 网关的用户界面中,用户成功登录后可以访问授权资源。

1) 在浏览器的 URL 地址栏输入 SSL VPN 网关的外网地址 "https://172.16.1.6",进入用户登录界面,界面如下图所示。

營用户登录 - ■icrosoft Internet Explorer	
文件(E) 编辑(E) 查看(V) 收藏(A) 工具(E) 帮助(H)	) 🥂
🔾 后退 🔹 🕥 🖌 😰 🏠 🔑 搜索 🧙 收藏夹 🤗	<u>ه</u> کې د
地址 (D) @ https://172.16.1.6/index1.html	▼ 🗲 转到   链接 ≫
	En English (? 帮助
了 天 融信	
口令认证 证书认证	双因子认证
用户名:	
密 码:	————————————————————————————————————
□ 使用代理服务器	
尊る	
4 <u>2</u>	
é	

输入"user1"正确的用户名、密码,并成功登录后,尽管网关中已经定义了多个Web转发资源,但该用户只能访问可用资源(即:webforward\_218),如下图所示。

●用户控制界面 - ■icrosoft Internet Explorer	
文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(T) 帮助	ክው 💦
🔇 后退 🔹 🕥 🖌 🗷 😰 🏠 🔎 搜索 👷 收藏夹 🍕	) 😥 - 💺 🖻
地址 @) @ https://172.16.1.6/vone/portal/index.htm	1# 🗾 🔁 转到 链接 >>
<b>资源列表</b> 配置状态	user1
名称	描述
🥭 webforward 218	
(2) 完毕	

点击 "webforward\_218" 后,成功进入服务器 "192.168.83.218" 的访问页面,如下图 所示。



2) 角色 "manager" 中的用户 "manager 1" 成功登录 SSL VPN 网关的用户界面后, 可以访问网关中设置的 "webforward\_218" 和 "webforward\_235",如下图所示。

●用户控制界面 - ■icrosoft Internet Explorer	
文件 (E) 编辑 (E) 查看 (V) 收藏 (A) 工具 (T) 帮 E	<del>ந</del> ி மு
🔇 后退 🔹 🕥 👻 😰 🟠 🔎 搜索 📩 收藏夹 🍕	9 😥 - 💺 🖻
地址 @) 🗃 https://172.16.1.6/vone/portal/index.htm	1 🗾 🔁 转到 链接 »
<b>     安 源列表</b> 配 置 状态	A manager1
名称	描述
🥭 webforward 235	
🥭 webforward 218	
•	
② 完毕	📄 📄 🕒 可信站点 🥢

点击任意 Web 转发资源后,均可以成功进入相应服务器的访问页面。

# 端口转发

# 基本需求

- ➤ 采用单臂模式,将 SSL VPN 网关部署在网络内部。SSL VPN 网关的对外 IP 为 "172.16.1.6",内网 IP 为 "192.168.83.237"。
- ▶ 采用"用户+口令"的认证方式对用户进行认证。
- ▶ 允许角色"test"中的用户"test1"以域名的方式(域名为"www.bbs.com")访问公司内网 Web 服务器"192.168.83.235",同时允许该用户访问公司内网 FTP 服务器"192.168.83.220",禁止其它访问。

网络示意图如下所示。



## 图 28 SSL VPN 网关端口转发示意图

# 配置要点

- ▶ 在防火墙 A 上进行相关配置。
- ▶ 在网关的管理员界面中,配置域名参数。
- ▶ 在网关的管理员界面中,添加用户"test1"信息。
- ▶ 在网关的管理员界面中,添加角色"test",然后将用户"test1"添加到该组中。
- ▶ 在网关的管理员界面中,配置授权资源。
- ▶ 在网关的管理员界面中,配置 ACL 规则。
- ▶ 在网关的管理员界面中,配置安全策略。
- ▶ 在网关的管理员界面中,配置虚拟门户。
- ▶ 验证:用户"test1"登录成功后,可以访问授权的端口转发资源"web\_235"和 "ftp\_220"。

# 防火墙 A 的配置步骤

为了保护 SSL VPN 网关的安全,管理员一般将防火墙 A 的 eth0 口所属区域的权限设置为"禁止访问",然后通过配置访问控制规则,只允许远程用户对 SSL VPN 网关上特定端口进行访问。

1) 在防火墙 A 上开放 TCP 443 端口,用于远程用户访问 SSL VPN 网关用户界面,如下图所示。

預定义 <b>自定义</b>	服务组			
🕂 添加 🗴 清空				
				总计: 1
名称	\$	详细	¢	操作
443		TCP/443		2 🗟

2) 定义访问控制规则,如下图所示。

访问控制										
目的区域	所有区域	•	策略组	所	î有组	T T	高级推	建索	🔲 统计	信息
十 添加約	1 十添	加策略						总计:1 毎页	ī: 30条	-
ID	控制	源			目的			服务	选项	操作
8088	~	<mark>区域:</mark> area_eth1			<mark>区域:</mark> area_ethO			443		
							Н	< 1 >	▶ 转到	/1 Go

3) 配置主机地址,即 SSL VPN 网关的真实地址"192.168.83.237"和对外地址

主机 范围 子网 地址组							
➡ 添加      面 清空     总计: 2							
名称 🔶	IP地址	操作					
sv	172, 16, 1, 6						
SV_MAP 192. 168. 83. 237							

## 4) 配置双向地址转换(到 SSL VPN 网关的映射),如下图所示。

地址转换						
目的区域	所有区域	▼ 高级搜索	□ 纷	计信息		
十 添加				总计	┼:1 毎页: 30条	-
ID	类型	源	目的	服务	转换	操作
8092	双向转换	区域: area_eth1	<del>地址</del> : SV		源: ethO <mark>目的:</mark> SV_MAP	
				H 4	1 🕨 🗏 转到	/1 <b>Go</b>

# WEBUI 配置步骤

## 1. 配置域名参数

1) 在左侧导航树上,点击 SSL VPN > 基本设置,然后激活"登录设置"页签,配 置域名参数,如下图所示。

登录设置	加密卡设置	: 端点安全设置	置 端口设置
		用户登录空闲时间	3600 [范围30086400秒]
		加密卡	○ 启用 • ◎ 停止
		是否启用压缩算法	○启用 ● 停止
		域名设置	🔽 使用修改HOSTS文件方式 🔽 还原HOSTS文件
			应用

2) 参数设置完成后,点击"应用"按钮即可。

2. 添加用户"test1"。

a) 点击导航菜单 用户认证 > 用户管理, 然后激活"用户管理"页签, 点击"添加 用户", 进入用户的添加界面。

b)设置用户"test1"的用户信息,如下图所示。

用户管理	在线用户 月	1户设置	
		用户属性	
	用户名 用户描述 认证方式 口令 确认口令 可用角色 <sup>doc_role</sup> test_role cert_role user manager	test1 本地口令认证 ●●●●●●● ●●●●●●●	* ▼ [6-31个字符]  新属角色
	高级		
		确定	取消

c)参数设置完成后,点击"确定"按钮完成配置。

3. 添加角色"test",然后将用户"test1"添加到该组中。

a) 在左侧导航树上,点击 **用户认证 > 角色管理**,激活"角色管理"页签,然后点击"添加角色",进入角色配置界面。

b)设置角色"test"的信息,然后将用户"test1"添加到该组中,如下图所示。

角色管理 分级管理		
	角	色属性
角色名 角色描述 DHCP地址池 选择用户 doc() user1() manager1()	test 不添加	* -> ×
高级		
	确定	取消

参数设置完成后,点击"确定"按钮完成配置。

## 4. 配置授权资源。

a) 点击导航菜单 SSLVPN > 资源管理, 然后点击资源列表左上方的"添加", 配置端口转发资源"ftp\_220", 如下图所示。

资源管理	
	添加资源
资源名称	ftp_220 *
描述	
访问方式	端口转发
资源地址	ftp://192.168.83.220
域名	[如果域名和IP地址同时 设定,表示手动指定域名和IP对应关系]
IP地址	192. 168. 83. 220
协议类型	tep-ftp 💌
添加端口	-> ×
	21
端口列表	*
应用程序	
自动打开	
在页面显示	V
却登点单	
	确定取消

b) 点击导航菜单 SSLVPN > 资源管理, 然后点击资源列表左上方的"添加", 配 置端口转发资源"web\_235", 如下图所示。

资源管理	
	添加资源
资源名称	web_235 *
描述	
访问方式	端口转发
资源地址	http://www.bbs.com
域名	www.bbs.com [如果域名和IP地址同时 设定,表示手动指定域名和IP对应关系]
IP地址	192. 168. 83. 235
协议类型	tcp-http 💌
添加端口	-> ×
	80
端口列表	*
应用程序	
自动打开	
在页面显示	
单点登陆	
	确定 取消

## 5. 配置 ACL 规则。

默认禁止远程用户访问内网资源,然后配置两条 ACL 规则,分别允许访问内网资源 "ftp\_220"和 "web\_235"。

a) 点击导航菜单 SSLVPN > ACL 管理, 然后在右侧界面中选中 "ACL 默认策略" 右侧的"禁止",如下图所示。

ACL管理		
ACL默认策略 〇 允许	⊙ 禁止	确定

设置完成后,点击"确定"按钮即可。

b) 点击 ACL 规则列表左上方的"添加规则",配置一条允许访问"ftp\_220"的 ACL 规则,如下图所示。

ACL管理		
		添加規則
	规则名称 资作 毎周时段 时间 策略	FTF服务器_220 ftp_220 ▼ 「上传文件 ▼ 打开 ▼ 重命名 ▼ 创建目录 ▼ 删除目录 ▼ 删除文件 ▼ 全选* ▼ 星期→ ▼ 星期二 ▼ 星期三 ▼ 星期四 ▼ 星期五 ▼ 星期六 ▼ 星期日 ▼ 全选* 开始: 00:00:00 结束: 23:59:59 [格式 ਮt:MM:SS] ● 全天 ○ 上午 ○ 下午 ○ 自定义* ● 允许 ○ 禁止
		确定取消

c) 点击 ACL 规则列表左上方的"添加规则", 配置一条允许访问"web\_235"的 ACL 规则, 如下图所示。

ACL管理		
		添加規則
	规则名称 资源名称 婚件	web服务器_235 web_235 ▼
	₩1F 毎周时段 时间	□     □       □     星期一     □       □     星期二     □       □     星期二     □       □     23:59:59       □     福東:       □     23:59:59       □     福東:       □     ○       □     ○       □     □
	策略	<ul> <li>① 允许 〇 禁止</li> <li>确定</li> <li>取消</li> </ul>

参数设置完成后,点击"确定"按钮。此时,"ACL管理"页面的配置如下图所示。

ACL管理									
						रंग?	_		
◎ 添加规则 (	3				息计:2 毎页: 王	an	<b>_</b>		
规则名称	资源名称	行为	策略	星期	时间	修改	删除		
FTP服务器_220	ftp_220	全部	允许	星期一 星期二 星期三 星期四 星期五 星期六 星期日	00:00:00-23:59:59		3		
web服务器_235	web服务器_235 web_235 全部 允许 星期一 星期二 星期三 00:00:00-23:59:59 [> 3								
	▲ K 【 】 ▶ N 转到 /1 Go								

6. 配置安全策略。

为用户"test1"配置两条安全策略,允许该用户以域名的方式访问公司内网的Web服务器"192.168.83.235",同时允许该用户访问公司内网的FTP服务器"192.168.83.220"。

a)点击导航菜单 SSLVPN > 安全策略,然后选择"用户安全策略"页签,点击用 户"test1"条目右侧的"安全策略设置"图标。

b) 勾选"自定义模块设置", 然后选中"启用端口转发", 如下图所示。

角色安全策略 用	沪安全策略
○ 继承角色配置或启用	默认模块 (WEB转发、应用WEB化、端口转发)
④ 自定义模块设置 (端口)	口转发模块和全网接入模块不能同时启用)
□ 启用WEB转发	☑ 启用端口转发
📃 启用全网接入	🗆 启用应用WEB化
确定	返回

设置完成后,点击"确定"按钮。

c) 点击"添加规则",将允许访问公司内网 Web 资源的 ACL 规则"web 服务器\_235" 赋予该用户,如下图所示。

角色安全策略	用户安全策	<b>*</b>		
		添加热	見則	
	用户名称 ACL名称	test1 web服务	器_235▼	
	确知		取消	

参数设置完成后,点击"确定"按钮。

d) 点击"添加规则",将允许访问公司内网 ftp 资源的 ACL 规则"FTP 服务器\_220" 赋予该用户,如下图所示。

角色安全策略	用户安全策■	8		
		添加規	則	
	用户名称 ACL名称	test1 FTP服务署	B_22C ▼	
	确定		取消	

参数设置完成后,点击"确定"按钮。至此,用户"test1"的安全策略配置完成。

7. 配置虚拟门户。

a) 点击导航菜单 SSLVPN > 虚拟门户。

b)点击虚拟门户列表左上方的"添加",自定义远程用户访问 SSL VPN 网关的用户 界面。自定义虚拟门户时,参数"地址"必须配置为远程用户登录 SSL VPN 网关时的地 址,即 SSL VPN 网关的对外 IP "172.16.1.6",参数"认证服务器名称"必须配置为对远 程用户进行认证的服务器名称,此案例为本地认证服务器"localdb",而且必须启用端口 转发开关,具体配置页面如下图所示。

虚拟门户	
	度視门户
名称	portal_172 *
地址	172. 16. 1. 6 *
认证服务器名称	localdb -> ×
	localdb
肥久或	
ND, 55' 88	
公告信息	
法探禁员可能	
选择更深风格	C C
	(~ mass ( ) #80
	「天際島
	RPS:
	「第月代登録名書
	LINEYE LORENYE
	〇 回移1
	PYIG1
	C ruge () an
0.000	
天静国际"可国际路 安全世界"作3 建一个未来可信的。母亲的、母亲的、母亲	
	使用代理服务器 夏泉
	LINETE LIGHTIE
	○ 风格2
	C Excelo (? #2b
	<b>114112</b> 275742
	用户S1 图 码: 面 <u>522</u> 6日
	了天職信 Trondec
	LINKYE MORDYE
	● 风格3
	C inside (C Mills
	で大照信
	DOUL UNUE METOR
	RPS: ENERGY COMPANY
	C 凤榕4
	C
目定义页面	
控件	· 启用 C 不启用
	○ 手动安装校件 ● 自动安装校件
框块开关	
	▶ 月用全网接入
	☑ 启用yshbbb
	☑ 启用应用WEB化
显示控制	▶ 显示证书信仟罅下载连接
	✓ 加许关闭测器器 只易示为小图标
11SB Keversternet	11. フロマンズ1910年9月1日日本
四本(1)定証20.000 (1)定証20.000	
田口家會行進去=- 四次公開的区面	い 小型ボ い 志亜不 い 登録失敗上伏后量不 だ ローム 反 はまれ 反 ままつて
小 五本以近月3 会业门户	
<u>上</u> 业1 2 溶源 <b>反</b> 称	
具不关闭士而	
<b>地</b> 自天的主贝	で通じ山
	确定取消

8. 验证:用户"test1"登录成功后,可以访问授权的端口转发资源"web\_235"和 "ftp\_220"。

1) 在浏览器的 URL 地址栏输入 SSL VPN 网关的外网地址 "https://172.16.1.6",进入用户登录界面,界面如下图所示。

叠用户登录 - ∎icrosoft Internet Explore	r _ 🗆 🗙
文件(E) 编辑(E) 查看(V) 收藏(A) 工具(	[) 帮助(H) 🥂
G 后退 • 🕤 • 🛛 👔 🏠 🔎 搜索 👷 收	藏夹 🤣 😥 - 😓 🔄
地址 @ 🍯 https://172.16.1.6/index3.html	▼ → 转到 链接 ※
	En English ② 帮助
	1令认证
用	
TOPSEC	○ 使用代理服务器       □ 使用代理服务器       ● 予
<b>ë</b>	

2) 输入"test1"正确的用户名、密码,并成功登录后,用户界面中显示可用资源 "web\_235"和"ftp\_220",如下图所示。

参用户控制界面 - ■icrosoft Internet Explorer	
文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(E) 帮助	ክ(£) 🦧
🔇 后退 🔹 🗇 👻 😰 🟠 🔎 搜索 📩 收藏夹 🍕	3 😥 - 💺 🗖
地址 @) 🍯 https://172.16.1.6/vone/portal/index.htm	1 • 转到 链接 >
天融信	and the second
> TOPSEC	🙆 test 1 🚽
资源测表 配置 状态	_
17.5h	HIVE .
名称	描述
🛒 <u>ftp 220</u> 👶	
🥭 <u>web 235</u>	
(2) 完毕	

3)点击"web\_235" 链接后,成功以域名"www.bbs.com"访问 Web 服务器"192.168.83.235",如下图所示。



4)点击"ftp\_220"条目右侧的"壶",选择客户端程序为"CuteFTP",然后在用 户界面中点击"ftp\_220"链接,自动弹出 CutpFTP 客户端,在客户端界面中输入主机地 址、用户名和密码后点击连接图标"↓,如下图所示。

💼 没有连接 - GlobalSCAPE Texas, LP CuteFIP 5.0 IP	
文件 (2) 编辑 (2) 查看 (Y) 书签 (3) 命令 (2) 传输 (2) 窗口 (3) 帮助 (4)	
🔽 🏁 💘 🙋 👁 🕢 🐼 🖻 🔳 🖻 📖 🗸	< 🕺 🎢 🚦
中机: 192.168.83.220 ■ 用户名: administrator      奈码: ●●●●	••• 端口: 21 🔰 🔪 🧳
	<b>_</b>
	Ď
C:\WINDOW5\system32\confin\systemprofile\My_Doc	
本地   大小     远程   注	E机 状态
	[队列:0KB/0KB / //

稍候,远程用户通过 CuteFTP 客户端登录到 FTP 服务器"192.168.83.220",如下图

胢	「示	0
---	----	---

🔯 (192.)	168.83.	220) - (	lobalSC	APE Tex:	as, LP.	- CuteFT	P [	- 🗆 🗵
文件化)《	扁锚(匠)	査者(⊻)	书签(B)	命令(C)	传输 ( <u>T</u> )	窗口(1)	帮助(H)	1
🛛 🕡 🔪	j 🖗	🖉   🌂		<b>d</b> R		3	•••	f e
	227 En	tering Passi	ve Mode (1	92,168,83	,220,1,212	)		
命令:>	LIST							
状态:>	正在连	接数据 soo	:ket					
	125 Da	ita connectii	on already	open; Tran	isfer startin	g.		
	226 Tra	ansfer comp	lete.					
状态:>	已接收	(の字节,]	E常。					
状态:>	- 町间: ( - 一一一	0:00:01 , 🕅	【率: 0.00 k	(B/秒 (0 字	节/秒)			_
状念:>	元成。							
	) OWS\svs	stem32\conf	ialisvs 👻	e I				- ⊜
2章		1	 大小		<del>۵</del>			<u>一</u> 一
- <u>-</u>			<u> </u>		n 1			
<u> </u>			]					
本地		大小	远程		主	机		状态
						认列: O KB	/0KB	[ <i> </i> //

# 全网接入

IPSec/SSL SSL VPN 网关可以给远程机构或个人使用者提供到内部网络的虚拟连接, 这种连接一旦建立,远程节点就变成企业内网的一个节点,在未进行访问控制的情况下, 它的接入权限与用户真正身处内网使用时一样,如果需要对远程用户进行访问控制,可以通过在 SSL VPN 网关上添加访问控制规则实现。

在进行全网接入配置时,管理员首先要进行虚拟网络参数的配置,为远程用户提供接入内网的接口,以及为远程用户分配 IP 地址,最后,对用户进行访问控制,通过设置针对用户或角色的访问控制规则,限定只有匹配访问控制规则的用户才能够远程访问某资源,同时,还可针对服务进行访问控制,从而实现对远程接入用户的更细粒度的访问控制。

## 基本需求

某企业采用双臂模式将 SSL VPN 部署于网络出口处,以便实现对内部网络中的核心 业务进行有效保障,同时为移动客户和分支客户提供安全的 VPN 通路。要求如下所示:

- ▶ 采用网络隔离的隧道模式,以便用户接入 VPN 后不能在访问 Internet。
- ▶ 使用内置数据库使用"用户+口令"的方式对移动用户进行认证。
- ▶ 用户"user"和用户"manager"同属于角色"doc\_role",且低级用户"user"
   只能访问 WEB 服务器 "192.168.83.235",而高级用户"manager"机既能访问
   该 WEB 服务器,也能够访问 FTP 服务器 "192.168.83.234"。

组网拓扑如下图所示:



#### 图 29 SSL VPN 网关全网接入示意图

## 配置要点

- ▶ 在防火墙 A 上进行相关配置。
- ➤ 开启 Eth1 所属区域的 SSLVPN 服务。
- ▶ 配置全网接入模块。
- ▶ 配置网关提供 DHCP 服务的接口和 DHCP 地址池。
- ▶ 配置源地址转换,将用户的虚拟网卡所在网段转换为 SSL VPN 网关的接口地址。
- ▶ 添加用户"user"和"manager"。
- ▶ 添加角色"doc\_role",然后将用户"user"和"manager"添加到该组中。
- ▶ 配置授权资源。

- ▶ 配置 ACL 规则。
- ▶ 配置安全策略。
- ▶ 配置虚拟门户。
- ▶ 验证:用户"user"登录成功后,可以访问授权的全网接入资源"web\_235"; 用户"manager"登录成功后,可以访问授权的全网接入资源"web\_235"和 "ftp\_220"。

# 防火墙 A 的配置步骤

为了保护 SSL VPN 网关的安全,管理员一般将防火墙 A 的 eth1 口所属区域的权限设置为"禁止访问",然后通过配置访问控制规则,只允许远程用户对 SSL VPN 网关上特定端口进行访问。

1) 在防火墙 A 上开放 TCP 443 端口,用于远程用户访问 SSL VPN 网关用户界面,如下图所示。

預定义 自定义 服务组		
🕂 添加 🗴 清空		
		总计:1
名称 🔶	详细 🔶	操作
443	TCP/443	2

2) 定义访问控制规则,如下图所示。

访问控制								
目的区域	所有区域	V	策略组	所有组	▶ 高级	搜索	□ 显:	示策略统计
╋ 添加雞	i 十添	加策略				总计: 1	毎页; 30条	<b>•</b>
ID	控制	源		目的		服务	选项	操作
8063	~	区域: area_ethO		区域: area_eth1		443		<ul> <li>*</li> </ul>
						₩ ◀ 1	▶ ▶ 转到	/1 Go

3) 配置主机地址,即 SSL VPN 网关的真实地址"172.16.1.1"和对外地址"10.10.10.10",

如下图所示。

主机 范围 子网 地址组		
➡ 添加 ● 清空		总计: 2
名称 🔶	IP地址 🔶	操作
sv	10. 10. 10. 10	2
SV_MAP	172. 16. 1. 1	2

地址转换						
目的区域	所有区域	▲ 高级搜索		显示策略统计		
十添加				į	急计:1 毎页: 30条	•
ID	类型	源	目的	服务	转换	操作
8067	双向转换	区域: area_ethO	<mark>地址</mark> : SV		<mark>源:</mark> eth1 目的: SV_MAP	<ul> <li>*</li> </ul>
				М	◆ 1 ▶ ▶ 转到	/1 Go

4) 配置双向地址转换(到 SSL VPN 网关的映射),如下图所示。

# WEBUI 配置步骤

## 1. 开启 Eth1 所属区域的 SSLVPN 服务。

选择 **系统管理 > 配置**, 激活"开放服务"页签, 然后点击"添加", 开放 Eth1 口 所属区域的 SSLVPN 服务, 如下图所示。

系统参数	开放服务	时间	SNMP	邮件设置	<u>بر</u>
			添加費	置	
	服务	·名称 S	SLVPN		~
	控制 控制	区域 ∣s l地址 a	area_eth1 ny [范围]		<ul><li>▼</li></ul>
		The second secon	<sup>确定</sup>	取消	

参数设置完成后,点击"确定"按钮即可。

## 2. 配置全网接入模块。

1)选择 SSL VPN > 模块管理,点击"全网接入"条目右侧的"模块设置"图标, 配置全网接入参数,如下图所示。

<b>模块管理</b>	
	全网接入设置
DHCP服务器类型 虚拟网卡接口IP	<ul> <li>①本地 〇 外部</li> <li>11.11.11.1</li> </ul>
虚拟网卡接口子网掩码	255. 255. 255. 0
隧道模式	○ 透明访问 ⊙ 网络隔离
是否允许自动启动	○ 允许 ◎ 不允许
是否允许自动重连	○ 允许 ◎ 不允许
是否允许永不超时	○ 允许 ④ 不允许
	确定 恢复默认

本例中 DHCP 服务器为 SSL VPN 网关本身,因此"DHCP 服务器类型"选择"本地"。

## 说明

- ◆ 如果 DHCP 服务器不使用 SSL VPN 网关,则在上图中设置"DHCP 服务器类型"选择 "外部",然后设置 DHCP 服务器的 IP 和请求端口。
- ◆ "虚拟网卡接口 IP" 用于与客户端的虚拟 IP 进行通信,管理员可以自行设置,可以 不与内网资源的 IP 地址设定在同一个网段,但一定不能与其它 IP 地址冲突。

参数设置完成后,点击"确定"按钮。

## 3. 配置网关提供 DHCP 服务的接口和 DHCP 地址池。

1)选择 网络管理 > DHCP, 然后选择"DHCP 服务器"页签, 点击"添加地址池", 添加作用域为"12.12.12.0/24"的 DHCP 地址池(用于分配给全网接入客户端), 如下图 所示。

DHCP服务器	DHCP客户端 DHCP中维	
	添加DHCP地址池	
	+mj 12.12.12.0 +	
	推动 255.255.255.0 *	c
	分配起始地址 12.12.12.10 *	¢
	分配结束地址 12.12.12.30 *	c
	缺省租用期 1 天 0 时 0 分	
	最大租用期 7 天 0 时 0 分	
	网关地址	
	主DNS	
	次DNS	
	域名	
	客户端类型	
	供应商详情	
	确定 取消	

2)将 DHCP 服务器的"运行接口"设置为"lo",然后点击"运行"按钮启动 DHCP 服务器进程,如下图所示。

DHCP服务器 DH	HCP客户端	DHCP中维	
			DHCP服务
运行接口	1.	<- X	eth0 eth1 eth2 eth3
	启动	停止	查看分配地址

4. 配置源地址转换,将用户的虚拟网卡所在网段转换为 SSL VPN 网关的接口地址 (或能与应用服务器通信的地址)。

1)选择 资源管理 > 地址, 然后选择"子网"页签, 点击"添加", 添加子网地址 资源, 子网地址必须与分配给远程用户的虚拟地址所属的地址池一致, 如下图所示。

主机 范围 子网	地址组	
	子阿雇	性
名称 网络地址 子 网掩码 排除地址	sv_12. 12. 12. 0 12. 12. 12. 0 255. 255. 255. 0	* * *
	确定	取消

2)选择 防火墙 > 地址转换,点击"添加",勾选"源转换"前的单选按钮,然后 设定源地址转换规则的源为"sv\_12.12.12.0",设置源地址转换为"eth0[属性]",最后 点击"确定"按钮。配置完成的地址转换规则如下图所示。

地址转换						
目的区域	所有区域	▼ 高级搜索		显示策略	统计	
╋ 添加				总计:1 每	≨页: 30条	•
ID	类型	源	目的	服务	转换	操作
8072	源转换	<mark>地址:</mark> sv_12.12.12.0			<mark>源:</mark> ethO	<b>~</b>
			М	∢ 1 ▶	▶ 转到	/1 <b>Go</b>

5. 添加用户"user"和"manager"。

a) 点击导航菜单 用户认证 > 用户管理, 然后激活"用户管理"页签。

b) 点击"添加用户",设置用户"user"的用户信息,如下图所示。

用户管理 在线用户	用户设置	
	用户属性	
用户名 用户描述 认证方式 口令 确认口令 可用角色 <sup>doc_role</sup> test_role cert_role user manager test	user 本地口令认证 ●●●●●●● ●●●●●●●	* ▼ [6-31个字符]  *  所属角色
高级		
	确定	取消

参数设置完成后,点击"确定"按钮使配置生效。

c)点击"添加用户",设置用户"manager"的用户信息,如下图所示。

用户管理 在线用户	用户设置	
	用户属性	
用户名 用户描述 认证方式 口令 确认口令 可用角色 <sup>doc_role</sup> test_role cert_role user manager test	manager 本地口令认证 ●●●●●●●	* ▼ [6-31个字符]  新属角色
高级		
	确定	取消

参数设置完成后,点击"确定"按钮使配置生效。

6. 添加角色 "doc\_role", 然后将用户 "user"和 "manager" 添加到该组中。

a) 在左侧导航树上,点击 **用户认证 > 角色管理**,激活"角色管理"页签,然后点击"添加角色",进入角色配置界面。

b)设置角色"doc\_role"的信息,然后将用户"user"和"manager"添加到该组中,如下图所示。

角色管理 分级管理	
	角色属性
角色名 角色描述 DHCP地址池 选择用户	doc_role * 12.12.12.0/255.255.0 ▼ 日经选择 user() manager()
高级	
	确定取消

参数设置完成后,点击"确定"按钮完成配置。

#### 7. 配置授权资源。

a) 点击导航菜单 SSLVPN > 资源管理, 然后点击资源列表左上方的"添加", 配置全网接入资源"ftp\_220", 如下图所示。

资源管理	
	添加资源
资源名	称*
描述	
访问方	式 全网接入 🔽
资源地	北上 ftp://192.168.83.220
域名	[如果域名和IP地址 同时设定,表示手动指定域名和IP对应关系]
IP地址	192. 168. 83. 220
网络掩	码 255.255.255.0
协议类	型 ip 🔽
自动打	ЭЛ 🗆
在页面	显示 🔽
单点登	
	确定 取消

b) 点击导航菜单 SSLVPN > 资源管理, 然后点击资源列表左上方的"添加", 配置全网接入资源"web\_235", 如下图所示。

资源管理	
	添加资源
资源名称 描述 访问方式	web_235 *
资源地址	http://192.168.83.235
域名	[如果域名和IP地址 同时设定,表示手动指定域名和IP对应关系]
IP地址	192.168.83.235
网络掩码	255. 255. 255. 0
协议类型	ip 💌
自动打开	
在页面显示	
却登点单	
	确定 取消

参数设置完成后,点击"确定"按钮。

8. 配置 ACL 规则。

默认禁止远程用户访问内网资源,然后配置两条 ACL 规则,分别允许访问内网资源 "ftp\_220"和 "web\_235"。

a) 点击导航菜单 SSLVPN > ACL 管理, 然后在右侧界面中选中 "ACL 默认策略" 右侧的"禁止", 如下图所示。

ACL管理		
ACL默认策略 〇 允许	⊙ 禁止	确定

设置完成后,点击"确定"按钮即可。

b) 点击 ACL 规则列表左上方的"添加规则",配置一条允许访问"ftp\_220"的 ACL 规则,如下图所示。

ACL管理	
	添加規则
	規则名称 FTF服务器_220 资源名称 ftp_220 ▼ 毎周时段 ☑ 星期→ ☑ 星期二 ☑ 星期三 ☑ 星期四 ☑ 星期五 ☑ 星期六 ☑ 星期日 ☑ 全选* 时间 开始: 00:00:00 结束: 23:59:59 [格式 HH:MM:SS] ⑥ 全天 〇 上午 〇 下午 〇 自定义* 策略 ⑥ 允许 〇 禁止
	确定 职消

参数设置完成后,点击"确定"按钮。

c) 点击 ACL 规则列表左上方的"添加规则", 配置一条允许访问"web\_235"的 ACL 规则, 如下图所示。

ACL管理	
	添加規則
	規则名称 web服务器_235 资源名称 web_235 ▼ 毎周时段 ☑ 星期→ ☑ 星期二 ☑ 星期三 ☑ 星期四 ☑ 星期五 ☑ 星期六 ☑ 星期日 ☑ 全选* 时间 开始: 00:00:00 结束: 23:59:59 [格式 Ht:MM:SS] ④ 全天 〇 上午 〇 下午 〇 自定义* 策略 ⑥ 允许 〇 禁止
	确定取消

参数设置完成后,点击"确定"按钮。此时,"ACL管理"页面的配置如下图所示。

ACL管理								
ACI默认策略 <sup>①</sup> 允许 <sup>〇</sup> 禁止 确定								
ACL規則列表								
♂添加规则 (	C				总计:2 毎页: 全部	<b>1</b> 7	•	
规则名称	资源名称	行为	策略	星期	时间	修改	删除	
FTP服务器_220	ftp_220		允许	星期一 星期二 星期三 星期四 星期五 星期六 星期日	00:00:00-23:59:59		3	
web服务器_235	web_235		允许	星期一 星期二 星期三 星期四 星期五 星期六 星期日	00:00:00-23:59:59		ā	
K ◀ 1 ▶ N 转到 /1 Go								

## 9. 配置安全策略。

为角色"doc\_role"配置一条安全策略,允许该用户访问公司内网的Web服务器 "192.168.83.235";为用户"manager"配置一条安全策略,允许该用户访问公司内网的 FTP服务器"192.168.83.220"。

a)为角色"doc\_role"配置安全策略。

点击导航菜单 SSLVPN > 安全策略,然后选择"角色安全策略"页签,点击角
 色 "doc\_role" 条目右侧的"安全策略设置"图标。

② 勾选"自定义模块设置",然后选中"启用全网接入",如下图所示。

角色安全策略 用户	安全策略
〇 启用默认模块 (WEB转发	<sub>觉、</sub> 应用WEB化、端口转发)
● 自定义模块设置 (端口報)	5发模块和全网接入模块不能同时启用)
□ 启用WEB转发	□ 启用端口转发
☑ 启用全网接入	□ 启用应用WEB化
确定	返回

设置完成后,点击"确定"按钮使配置生效。也可以勾选"自定义模块设置",然后 选中"启用全网接入"。

③ 点击"添加规则",将允许访问公司内网 Web 资源的 ACL 规则"web 服务器\_235" 赋予该角色,如下图所示。

角色安全策略	用户安全策略	
	添加規則	
	角色名称 doc_role ACL名称 web服务器_235	
	确定 取消	

参数设置完成后,点击"确定"按钮使配置生效。此时,属于角色"doc\_role"的用户"user"和"manager"都被赋予了访问指定 web 服务器的权限。

b)为用户"manager"配置安全策略。

点击导航菜单 SSLVPN > 安全策略,然后选择"用户安全策略"页签,点击用
 户"manager"条目右侧的"安全策略设置"图标。

② 勾选"自定义模块设置",然后选中"启用全网接入",如下图所示。

角色安全策略 月	1户安全策略
○ 继承角色配置或启用	默认模块 (WEB转发、应用WEB化、端口转发)
⑥ 自定义模块设置 (端)	口转发模块和全网接入模块不能同时启用)
□ 启用WEB转发	□ 启用端口转发
☑ 启用全网接入	□ 启用应用WEB化
确定	返回

设置完成后,点击"确定"按钮。

③ 点击"添加规则",将允许访问公司内网 ftp 资源的 ACL 规则"FTP 服务器\_220" 赋予该用户,如下图所示。

角色安全策略	用户安全策略
	添加規則
	用户名称 manager ACL名称 FTF服务器_22C▼
	确定 取消

参数设置完成后,点击"确定"按钮使配置生效。此时,用户"manager"被赋予了 访问指定 FTP 服务器的权限。

#### 10. 配置虚拟门户。

a) 点击导航菜单 SSLVPN > 虚拟门户。

b)点击虚拟门户列表左上方的"添加",自定义远程用户访问 SSL VPN 网关的用户 界面。自定义虚拟门户时,参数"地址"必须配置为远程用户登录 SSL VPN 网关时的地 址,即 SSL VPN 网关的对外 IP"10.10.10.10",参数"认证服务器名称"必须配置为对 远程用户进行认证的服务器名称,此案例为本地认证服务器"localdb",而且必须启用全 网接入模块开关,具体配置页面如下图所示。

度相门户		-
		虚拟门户
名称		sv_10.10.10.10 *
地址	75h	10. 10. 10. *
认证服务器	各称	localdb
		Tocardo
服务器		
公告信息		
选择登录风	16	
		(© Ecolity (?) Mile
	34	a te
	D\$UV	ERACUE TOESPELE
	E 4	
		22
		LINETE ASSESSTE
		2
		し 风格1
		C tosts (? Hits
2758		
无能准书"可准将体 安 接一个未来可保护。但	主任书"作力品和是七,共同创 1910、安全的引导社界。	
		29
		UTSHYR LOREDYR
		C 风格2
		C toold () Mit
		ПРКЕ 127012 2027/02 ДР8:
	了天雕信	6 H: miczeła
		I R USATE USANTE
		C 风格3
		Co Ecolado ( 🔿 Millo
	7500	
	Detty H	NUE 7857UE
	RP8	:ен: ен
	222	6 EBETE LOSSATE FRENERA
		• E #84
自定义页面		
控件		· の 启用 〇 不启用
		○ 手动安装控件 ◎ 自动安装控件
模块开关		☑ 启用端口转发
		☑ 启用全网接入
		✓ 启用web转发
		☑ 启用应用WEB化
显示控制		☑ 显示证书信任链下载连接
		▶ 允许关闭浏览器,只显示为小图标
USB KeyBER	り下載连接	
图形认证码	设置	◎ 不显示 ○ 总显示 ○ 登录失败三次后显示
用户登录认	矿方式	☑ 口令 ☑ 证书 ☑ 救因子
企业门户		
<u> </u>	<b>T</b>	
是古关闭主	д.	◎ 是 ○ 否
	确会	E 取消

11. 验证:用户"user"登录成功后,可以访问授权的全网接入资源"web\_235"; 用户"manager"登录成功后,可以访问授权的全网接入资源"web\_235"和"ftp\_220"。

假设用户"user"和"manager"使用同一主机"10.10.10.2"登录,并且该主机已经下载完所有的控件。

1) 用户"user"登录 SSL VPN 网关。

a) 在浏览器的 URL 地址栏输入 SSL VPN 网关的外网地址 "https://10.10.10.10",进入用户登录界面,界面如下图所示。

参用户登录 - ■icrosoft Internet Explorer		<u>- 0 ×</u>
文件(E) 编辑(E) 查看(V) 收藏(A) 工具(E)	帮助任	A.
🔾 后退 🔹 🕤 🔹 👔 🚮 🔎 搜索 🧙 收藏夹	\varTheta 😥 - 💺 🖻	
地址 (1) 🗃 https://10.10.10.10/index4.html		▼ → 转到 链接 ※
		En English ? 帮助
口令认证	证书认证 双因子认证	
	用户名: 密码: 圖 登录	
	<u>忘记密码 证书链下载 USB Key驱动下载</u> [] 使用代理服务器	/
		1
é		)可信站点

b) 输入"user"正确的用户名、密码,并成功登录后,用户界面中显示可用资源 "web\_235",如下图所示。

●用户控制界面 - ■icrosoft Internet Explorer		_ 🗆 ×
文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(E) 帮助	助 ( <u>H</u> )	alia 💦 💦
🔾 后退 🔹 🕞 🔹 😰 🚮 🔎 搜索 🦙 收藏夹 🎸	3 😥 - 💺 🕞	
地址 @) 🗃 https://10.10.10.10/vone/portal/index.htm	ml	▼ ● 转到 链接 ≫
了 天 融 信 TOPSEC		♀ <mark>要</mark> ▲ user <u>设置风</u>
资源列表 配置 状态		
名称	描述	
遵 <u>web 235</u>		
		<b>.</b>
•		
🙆 完毕		🔒 🕗 可信站点

由于没有启动全网接入客户端,所以该资源名称为灰色不可用状态。

c)激活"状态"页签,点击全网接入状态一栏中的"启动"链接开启全网接入客户端,如下图所示。

詹用户控制界面 - ■icrosoft Internet Explor	er			
文件(E) 编辑(E) 查看(V) 收藏(A) 工具(E)	帮助(出)			<b>1</b>
🔇 后退 🔹 🕥 🖌 🖹 😰 🚮 🔎 搜索 📩 收藏界	🥴 🔊 - 💺 🖻			
地址 @) 🍯 https://10.10.10.10/vone/portal/inde	x.html		🔽 ラ 转到	链接 »
了 天 融信		📥 user		? <del>常</del> 设置风
资源列表 配置 状态				_
·····································				
当前的状态: SSL VPN没有连接				日初
接收字节数: 0	发送字节数: 0		连接的时间:	0
<b>虚网卡地址:</b> 0	连接的方式:		虚网卡掩码:	0
端口转发状态				
当前的状态:端口转发启动成功			÷	关闭
接收字节数: 0	<b>发送字节数:</b> 0		连接的时间:	67
登录信息				<b>_</b>
				•
e			)可信站点	11.

d) 全网接入客户端与服务器成功建立连接后,客户端状态如下图所示。

参用户控制界面 - ■icrosoft Internet Explor	er		_	
文件 (E) 编辑 (E) 查看 (Y) 收藏 (A) 工具 (T)	帮助创			-
🔾 后退 🗸 🕤 🖌 📓 🐔 🔎 搜索 👷 收藏夹	🛛 🙆 - 💺 🖂			
地址 @) 🗃 https://10.10.10.10/vone/portal/index	c.html#		💌 🔁 转到 🕴	链接》
了 Topsec		📥 user	1 L	▲ 帮 段置风
资源列表 配置 状态				_
全网接入状态				_
当前的状态: SSL VPN隧道建立成功			关闭	6
接收字节数: 0	发送字节数: 0		<b>连接的时间</b> : 8	
<b>虚网卡地址:</b> 12.12.12.30	<b>连接的方式</b> : 网络隔离		<b>虚网卡掩码:</b> 25	55.25
端口转发状态				
当前的状态:端口转发启动成功			<u></u> ξį	đ
<b>接收字节数:</b> 0	发送字节数: 0		<b>连接的时间:</b> 90	)
登录信息				<b>–</b>
æ			✔ 可信站点	11.

e) 激活"资源列表"页签, "web\_235"资源可用, 如下图所示。

叠用户控制界面 - ∎icrosoft Internet Explorer	_	
文件(E) 编辑(E) 查看(V) 收藏(A) 工具(E) 帮助	助 (£)	<b></b>
🚱 后退 🔻 🕤 👻 👔 🔥 🔎 搜索 🦙 收藏夹 🍕	🛛 🔊 • 🚴 🖻	
地址 @) 💣 https://10.10.10.10/vone/portal/index.htt	ml# 🔽 🄁 转到 🦉	·····································
て天融信	3	帚
TOPSEC	📤 user 👘 😟	置风
资源则表 配置 状态		
名称	描述	
遵 <u>web 235</u>		
		_
<b>T</b>		⊾
(2) 完毕		

f) 点击"web\_235"链接后,可以成功访问 Web 服务器"192.168.83.235",如下图 所示。


2) 用户"manager"登录 SSL VPN 网关。

a) 在浏览器的 URL 地址栏输入 SSL VPN 网关的外网地址 "https://10.10.10.10",进入用户登录界面,界面如下图所示。

叠用户登录 - ■icrosoft Internet Explorer	
文件 (E) 編辑 (E) 查看 (Y) 收藏 (A) 工具 (E) 帮助 (H)	
地址 1 @ https://10.10.10/index4.html	▼ → 转到 链接 ≫
了 不 融信	En English (? 帮助
口令认证 双因子认证	
用户名: 密码: 圖 登录	
<u>忘记密码 证书链下载 USB Key 驱动下载</u>	
	)可信站点

b) 输入"manager"正确的用户名、密码,并成功登录后,用户界面中显示可用资源 "web\_235"和"ftp\_220",如下图所示。

<ul> <li>登用户控制界面 - ■icrosoft Intern</li> <li>文件(2) 编辑(2) 查看(V) 收藏(A)</li> <li>③ 后退 • ③ • ▲ 20 (△) 戶 搜索</li> </ul>	eet Explorer 工具① 帮助他 ஜ 收藏夹 ❷ 😥 ♣ 🛃	
地址 @) 🚳 https://10.10.10.10/vone/j	ortal/index.html	☑ 🔁 转到 链接 >>
了 天 融 信 TOPSEC		22 <del>要</del> ● ● ● ● ● ● ● ● ● ● ● ● ●
资源初表 配置 状态	ž	
名称	描述	
🛃 <u>ftp 220</u>	÷	
🥭 <u>web 235</u>		
		•
<u>ــــــــــــــــــــــــــــــــــــ</u>		
🙋 完毕		

由于没有启动全网接入客户端,所以资源名称为灰色不可用状态。

c)激活"状态"页签,点击全网接入状态一栏中的"启动"链接开启全网接入客户端,如下图所示。

参用户控制界面 - ■icrosoft Internet Explo	rer		<u>_ 0 ×</u>
文件(E) 编辑(E) 查看(V) 收藏(A) 工具(T)	帮助任		
🔇 后退 🔹 🕥 🖌 👔 😰 🏠 🔎 搜索 👷 收藏3	ਞ 🙆 😥 = 💺 🚍		
地址 @) 🙋 https://10.10.10.10/vone/portal/inde	ex. html		💌 🔁 转到 链接 꽏
了 天 融信 TOPSEC		📥 manager	2 # 设置风
资源列表 配 置 状态			
王阳贲入认念			
当前的状态: SSL VPN没有连接			启动
<b>接收字节数:</b> 0	发送字节数: 0		<b>连接的时间:</b> 0
<b>虚网卡地址:</b> 0	连接的方式:		<b>虚网卡掩码:</b> 0
端口转发状态			
<b>当前的状态:</b> 端口转发启动成功			关闭
<b>接收字节数:</b> 0	发送字节数: 0		<b>连接的时间:</b> 17
登录信息			Ŧ
			Þ
(2) 完毕			)可信站点 //

d) 全网接入客户端与服务器成功建立连接后,客户端状态如下图所示。

晋用户控制界面 - ■icrosoft Internet Explorer			
文件 (E) 编辑 (E) 查看 (Y) 收藏 (A) 工具 (I) 帮助	<b>ხ</b> (ყ)		2
🕓 后退 🔻 🕤 👻 😰 🚮 🔎 搜索 👷 收藏夹 🧔	9   🔊 - 📚 🖻		
地址 @) 🗃 https://10.10.10.10/vone/portal/index.htm	1#		💌 🔁 转到 🙀 🎽
了 天 融信 TOPSEC		🖄 manager	▲ 7 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日
资源列表 配置 状态			
全网接入状态			
当前的状态: SSL VPN隧道建立成功			关闭
接收字节数: 0	发送字节数: 0		连接的时间: 9
<b>虚网卡地址:</b> 12.12.12.30	<b>连接的方式:</b> 网络隔离		<b>虚网卡掩码:</b> 255.25
<b>端口转发状态</b>			
当前的状态:端口转发启动成功			长闭
<b>接收字节数:</b> 0	发送字节数: 0		<b>连接的时间:</b> 42
登录信息			<b>•</b>
			<ul> <li>✓</li> <li>✓</li></ul>

e) 激活"资源列表"页签, "web\_235"和"ftp\_220"资源可用, 如下图所示。

@用户控制界面 - ■icrosoft Internet Explorer	
文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(E) 幕	助田 👔
🚱 后退 🔻 🕥 🖌 🗾 😰 🏠 🔎 搜索 📩 收藏夹	🛛 🔊 - 📚 🖻
地址 @) 🕘 https://10.10.10.10/vone/portal/index.h	tml# 🗾 🎅 转到 链接 »
<b>了</b> 天融信	3 <del>骤</del> ▲ manager <u>没置风</u>
资源资利表配置状态	
名称	描述
🛒 <u>ftp 220</u> 🕹	
<i>i</i> web 235	

f)点击"ftp\_220"条目右侧的"壶",选择客户端程序为"CuteFTP",然后在用 户界面中点击"ftp\_220"链接,自动弹出 CutpFTP 客户端,在客户端界面中输入主机地 址、用户名和密码后点击连接图标"№",如下图所示。

💼 没有连接 - GlobalSCAPE Texas, LP CuteFIP 5.0 IP	
文件 (2) 编辑 (2) 查看 (Y) 书签 (3) 命令 (2) 传输 (2) 窗口 (3) 帮助 (4)	
🔽 🏁 💘 🙋 👁 🕢 🐼 🖻 🔳 🖻 📖 🗸	< 🕺 🎢 🚦
中机: 192.168.83.220 ■ 用户名: administrator      奈码: ●●●●	••• 端口: 21 🔰 🔪 🧳
	<b>_</b>
	Ď
C:\WINDOW5\system32\confin\systemprofile\My_Doc	
本地   大小     远程   注	E机 状态
	[队列:0KB/0KB / //

稍候,远程用户通过 CuteFTP 客户端登录到 FTP 服务器"192.168.83.220",如下图

- r.r		_	
閁	TZ	$\underline{V}$	0

🔃 (192	. 168. 83. 220)	- GlobalS	CAPE Tex	as, LP. –	- CuteFT	P 💶 🗖	×
文件 (2)	编辑(E) 查看	(V) 书签(B)	) 命令(C)	传输(I)	窗口())	帮助(H)	
0	🗸 🍣 🌾	₫ 🕑			1	II P	Ré
· ·	227 Entering	Passive Mode	(192,168,83	,220,1,212)	I		
命令:>	LIST						
状态:>	正在连接数	居 socket					
	125 Data con	nection alread	ly open; Tran	sfer starting	<u>]</u> .		
	226 Transfer	complete.					
状态:>	已接收0字	节,正常。					
状态:>	时间: 0:00:0	1,效率:0.00	) KB/秒 (0 字	节/秒)			
状态:>	完成。						2
						<u> </u>	
C:\WI	NDOWS\system32	2\config\sys 🔻	1 🖻 /			•	
名称			小日名和	尔			小
•							▶
本地	大	小」。	程	主	机	状态	\$
					ചച	( O VP	Γ
]		]]		AI I	∧≫∐: O KB	/UKB	L ///

g) 点击"web\_235" 链接后,可以成功访问 Web 服务器"192.168.83.235",如下图 所示。



#### 注意事项

1)全网接入的远程用户必须属于某一个角色,并在角色中设置地址池。远程客户端进行全网接入时,从用户所属的第一个角色中相关联的地址池中分配 IP 地址。该地址池必须是 DHCP 服务器上设定的地址池中的一个。

2)必须保证客户端主机开放了"DHCP Client"服务,否则即使成功建立隧道,客户端也无法获取到虚拟 IP。

3)如果没有配置全网接入 ACL 规则, SSL VPN 网关默认隧道模式为网络隔离的隧道模式。

4)由于为全网接入客户端分配的地址网段与企业内部网不能在同一网段,因此如果 不希望改变内网设备的路由配置,实现 SSLVPN 的透明接入,则需要在网关的内网口上 做源 NAT 设置,将客户端访问数据报文的源地址转换为网关内网口的 IP 地址;当然也可 以通过在内网设备上增加一条到全网接入客户端网段的路由来解决这个问题。

# 本地证书认证

#### 基本需求

客户需要高安全等级的接入方式,希望采用数字证书对移动用户进行身份认证。但是 客户没有独立的 CA 系统,需要 SSL VPN 网关的支持。所有移动用户根据安全等级分为 两级:安全等级高的用户"manager1"采用 USB KEY 的方式发放证书;安全等级低的用 户"user1"采用文件方式发放证书。根据证书OU(unit)字段,将用户映射到不同的角色。



#### 图 30 本地证书认证的网络部署图

#### 配置要点

- ▶ 在防火墙 A 上进行相关配置。
- ▶ 开启 Eth1 所属区域的 SSLVPN 服务。
- ▶ 创建本地根证书。
- ▶ 启用 USBKEY 端口,并正确设置 USB 的厂商和 PIN 码。
- ▶ 签发并保存用户证书。
- 配置用户证书映射(假设映射角色已经配置完成,并且已经配置完成这些角色的 安全策略)。
- ▶ 验证:证书用户 "user1"登录后,被赋予映射角色 "clerk"的访问权限;证书 用户 "manager1"登录后,被赋予映射角色 "manager"的访问权限。

## 防火墙 A 的配置步骤

为了保护 SSL VPN 网关的安全,管理员一般将防火墙 A 的 eth1 口所属区域的权限设置为"禁止访问",然后通过配置访问控制规则,只允许远程用户对 SSL VPN 网关上特定端口进行访问。

1) 在防火墙 A 上开放 TCP 443 端口,用于远程用户访问 SSL VPN 网关用户界面,如下图所示。

預定义 自定义 服务组		
🕂 添加 🗴 清空		
		总计: 1
名称	详细 🔶	操作
443	TCP/443	23

2) 定义访问控制规则,如下图所示。

访问控制								
目的区域	所有区域	T	策略组	所有组	▶ 高級	搜索	□ 显	示策略统计
中 添加維	i 🕂 添	加策略				总计: 1	毎页: 30条	•
ID	控制	源		目的		服务	选项	操作
8063	•	<mark>区域:</mark> area_eth0		区域: area_eth1		443		<ul> <li>*</li> </ul>
						₩ 4 1	▶ ▶ 转到	/1 Go

3)配置主机地址,即 SSL VPN 网关的真实地址"172.16.1.1"和对外地址"10.10.10.10",如下图所示。

主机 范围 子网 地址组		
➡添加 面清空		总计: 2
名称	IP地址 🔶	操作
sv	10. 10. 10. 10	2
SV_MAP	172, 16, 1, 1	2

4) 配置双向地址转换(到 SSL VPN 网关的映射),如下图所示。

地址转换						
目的区域	所有区域	▼ 高级搜索		显示策略统计		
十 添加				د	总计:1 毎页: 30条	-
ID	类型	源	目的	服务	转换	操作
8067	双向转换	区域: area_ethO	<mark>地址</mark> : SV		源: eth1 <mark>目的:</mark> SV_MAP	<ul> <li>•</li> </ul>
K < 1 ▶ N 转到 /1 Go						

## WEBUI 配置步骤

1. 开启 Eth1 所属区域的 SSLVPN 服务。

选择 系统管理 > 配置, 激活"开放服务"页签, 然后点击"添加", 开放 Eth1 口 所属区域的 SSLVPN 服务, 如下图所示。

系统参数 开	放服务 时间	SNMP 邮件设置	短
		添加配置	
	服务名称 控制区域 控制地址	SSLVPN area_eth1 any[范围]	<ul><li>✓</li><li>✓</li></ul>
		确定 取消	

参数设置完成后,点击"确定"按钮即可。

#### 2. 创建本地根证书。

1)管理员登录管理界面后,点击导航菜单 **PKI 设置 > 本地 CA 策略**,然后选择"根 证书"页签,点击"获取证书",如下图所示。

根证书 签发证书 证书撤销列表	
◎ 获取证书 ◎ 存出证书	
Version: V3 CN: VoneRootCA SerialNumber: 0x00 Issuer: CN=VoneRootCA Subject: CN=VoneRootCA NotBefore : Oct 29 10:24:19 UTC 2009 NotAfter : Oct 27 10:24:19 UTC 2019 RSA Public Key: (1024 bits) Modules:	•

2) 选中"生成新证书"前的单选按钮,然后填写相应项目,如下图所示。

根证书 签发证	书 计书撒销列表		
		获取根证书	
	<ul> <li>○ 文件方式导入</li> <li>证书</li> <li>私钥</li> </ul>		浏览
	<ul> <li>PKCS12文件格式导入</li> <li>证书文件</li> <li>证书文件密码</li> </ul>		浏览
	○ 以本机设备证书导入		
	◎ 生成新证书		
	名称	LocalCert	*
	国家	CN	[两个英文字符]
	省	ВЈ	
	城市	Ю	
	电子邮件	doc@topsec.com.cn	
	组织	TOPSecBJ	
	单位	RD	
	确定	E 取消	

3) 点击"确定"按钮,完成根证书创建。

#### 3. 启用 USBKEY 端口,并正确设置 USB 的厂商和 PIN 码。

1) 点击导航菜单 PKI 设置 > USB KEY ,如图所示。

USB KEY		
		USB设置
	USB厂商 PIN码 确认PIN码	epass1000 💌
		应用

2) "USB 厂商"用于选择 USBKey 设备厂商/型号,该选项请根据插在安全设备上的不同 USBKey 进行选择。目前只支持 epass1000。

"PIN 码"用于输入 USBKey 的管理员 PIN 码。

"确认 PIN 码"管理员再次输入 USBKey 的管理员 PIN 码。

3) 点击"应用"按钮,完成设置。

#### 4. 签发并保存用户证书。

1) 点击导航菜单 **PKI 设置 > 本地 CA 策略**, 然后选择"签发证书"页签, 点击"生成新证书"。

2) 配置普通职员证书	, 如下图所示。
-------------	----------

根证书 签发证书	证书	微销列表	
		签发证书	
名; 国; 省 城;	称  家  市	user1 CN BJ HD	* [两个英文字符]
电 组 单 人	子邮件 织 位 效时间	user1@topsec.com.cn TOPSecBJ clerk 2010/10/10	[格式:YYYY/MM/DD]
		确定 现	以消

参数设置完成后,点击"确定"按钮使配置生效。

3) 配置经理证书,如下图所示。

根证书 签发证书	证书撤销列表	
	签2	发证书
名称	manager1	*
国家	CN	[两个英文字符]
省	ВЈ	
城市	Ю	
电子	邮件 manager1@top	psec.com.c
组织	TOPSecBJ	
单位	manager	
失效	时间 2010/10/10	[格式:YYYY/MM/DD]
	确定	取消

参数设置完成后,点击"确定"按钮使配置生效。

两种移动用户的区别在于"单位(OU)"项的内容不同。根据该项的区别,SSL VPN 网关将在移动用户登录时判断身份,然后把用户归类入不同的角色中。

4) 将"user1"的证书保存到本地。

① 在"签发证书"页面,点击"user1"条目右侧的"下载"图标,如下图所示。

根证书	签发证书 证书撤销列表						
	5 🕃 全部导出 🕃 清空证书						总计: 2
证书	有效起止日期	状态	属性	下载	写入	撤销	删除
user1	Oct 29 06:36:35 UTC 2009- Oct 10 14:36:35 UTC 2010	1	<b></b>	ß	D	3	3
manager1	Oct 29 06:38:21 UTC 2009- Oct 10 14:38:21 UTC 2010	~	<b>E</b>	ß		3	3

② 选择证书的文件格式为 "PKCS12", 不输入密码, 然后点击"导出证书"按钮, 界面出现"证书点击下载"链接, 如下图所示。

根证书	签发证书	正书撒销列表	
		Ę	导出签发证书
	选择	译要使用的文件格式 3	式 PKCS12 < 导出证书 [如果需要 密码保护,请先输入密码再导出] 证书点击下载[或用右键另存]
			返回

③ 点击"证书点击下载"链接,弹出文件保存提示框,如下图所示。

文件下载			x
您想打错	甲或保存此的	文件吗?	
Ð	名称: 类型: 发送者:	user1.p12 Personal Information Exchange, 1.85 KB 192.168.83.237	
			j
1	来自 Inte 危害您的讨 该文件。有	rnet 的文件可能对您有所帮助,但某些文件可能 计算机。如果您不信任其来源,请不要打开或保存 可何风险?	

④ 点击"保存"按钮,在文件保存窗口中为证书文件指定保存路径后,点击"保存" 按钮即可。 5)将"manager1"的证书保存到本地。

① 在"签发证书"页面,点击"manager1"条目右侧的"下载"图标,如下图所示。

根证书	签发证书 证书撤销列表						
@ 生成新证书	ら 🕑 全部导出 🕑 清空证书						总计: 2
证书	有效起止日期	状态	属性	下载	写入	撤销	删除
user1	Oct 29 06:36:35 UTC 2009- Oct 10 14:36:35 UTC 2010	1	<b>E</b>	ß		3	0
manager1	Oct 29 06:38:21 UTC 2009- Oct 10 14:38:21 UTC 2010	1	Ë	ß		3	٦

② 选择证书的文件格式为 "PKCS12", 不输入密码, 然后点击"导出证书"按钮,界面出现"证书点击下载"链接,如下图所示。

根证书	签发证书	证书撤销列表	
		令	出签发证书
		选择要使用的文件格式 密码	PKCS12 ▼ 导出证书 [如果需要 密码保护,请先输入密码再导出] 证书点击下载[或用右键另存]
			返回

使用 USBKey 保存的证书必须是"PKCS12"格式。

③ 点击"证书点击下载"链接,弹出文件保存提示框,如下图所示。

文件下载	×	
您想打开或保存此文件吗?		
名称: manager1.p12 类型: Personal Information Exchange, 1.86 KB 发送者: 192.168.83.237		
来自 Internet 的文件可能对您有所帮助,但某些文件可能 危害您的计算机。如果您不信任其来源,请不要打开或保存 该文件。 <u>有何风险?</u>		

④ 点击"保存"按钮,在文件保存窗口中为证书文件指定保存路径后,点击"保存" 按钮即可。

6) 将经理证书"manager1"导入到 USBKEY (epass1000) 中。

a) 在导入前需要安装 USBKEY 驱动,双击驱动程序"eps1k\_full.exe",依照提示进 行安装即可。安装完成后,底部托盘出现"USB Token 1000 证书管理工具"的图标"▶"。

b)将 epass1000 插入主机的 USB 口。

c)双击证书写入工具"ePassMgr.exe",进入"USB Token 1000管理工具"界面,激活右侧界面下方的"验证用户 PIN",然后输入正确的 PIN 码,如下图所示。

🚵 USB Token 1000 管理工具		
文件 配置 帮助		
文件 配置 帮助	证书管理 - 登入     必须输入用户 FIN 码才可以访问这支 USB Token 1000     用户 FIN 码:     ********     登入     登入	
就绪	令牌 验证用户PIN 改变用户PIN 改变令牌名 改变管理员PIN 解锁	初始化

点击"登入"按钮,稍后弹出对话框,提示用户成功登入USBKEY,如下图所示。



点击"确定"按钮后,导入证书的界面如下图所示。

📚 USB Token 1000 管理工具		
文件 配置 帮助		
□ È epass1000 □ E E E E E E E E E E E E E E E E E E E	证书管理 您的证书: 颁发给	
	<u></u>	
删除证书完成!	NU	M

点击"导入"按钮,然后点击界面中的"..."按钮,因为导出证书时没有配置证书密码,所以此处无需输入证书密码,界面如下图所示。

为 VSB Token 1000 管理工具		
文件 配置 帮助		
文件 配置 帮助 epass1000 □ ○ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	导入证书         证书文件:         「!\test\manager1.pl2         证书密码:             下一步	
删除证书完成!		NUM

点击"下一步"按钮,稍后弹出对话框,提示证书导入成功,如下图所示。



点击"确定"按钮,可以看到 manager 用户的证书已经被导入到 USBKEY 中,如下

121	m			
	甘力	17	<u>_</u>	
131	11	⁄]	`	0

à USB Token 1000 管理工具		- 🗆 ×
文件 配置 帮助		
□ ≥ epass1000 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	证书管理  您的证书:  预发给 预发者 有效期终止日期  manager1 LocalCert 2010-10-10 14:38:21	
	<u>查看</u> 导入 删除	
导入证书完成!	N	พ 📃

5. 配置用户证书映射(假设映射角色已经配置完成,并且已经配置完成这些角色的 安全策略)。

将单位 (OU) 为 "clerk" 的证书用户 "user1" 映射到角色 "clerk", 然后将单位 (OU) 为 "manager" 的证书用户 "manager1" 映射到角色 "manager"。

假设已经配置完成映射角色"clerk"、"manager"及映射角色的安全策略,允许属于角色"clerk"的用户访问端口转发资源"web\_235"(即 web 服务器"192.168.83.235"); 允许属于角色"manager"的用户访问端口转发资源"ftp\_220"(即 ftp 服务器 "192.168.83.220")。

1)点击导航菜单 用户认证 > 认证设置,然后点击证书服务器 "cert"条目右侧的
 修改图标 "↓",配置后的界面如下图所示。

认证设置		
	映射策略	
	<ul> <li>认证服务器 cert</li> <li>启用 是</li> <li>授权类型 外部属性映射</li> </ul>	• •
	确定取消	

参数设置完成后,点击"确定"按钮。

2) 点击证书服务器 "cert" 条目右侧的 "外部属性映射" 链接,进入"证书属性" 窗口。点击"添加"链接,将证书用户 "user1"映射到角色 "clerk",如下图所示。

认证设置	
	外部映射属性
名称 国家 省 城市 组织 单位	等于          等于          等于          等于          等于          等于          「等于          「等于          「等于          「          「  <
邮箱	
本地角色集合 doc_role develop doc manager	E经选择 → ×
	确定 取消

参数设置完成后,点击"确定"按钮。

3) 在"证书属性"窗口中,点击"添加"链接,将证书用户"manager1"映射到角 色"manager",如下图所示

认证设置		
	外部映射雇性	
名称	等于 🔽	
国家	等于 🔽	
省	等于 🔽	
城市	等于 🔽	
组织	等于 🔽	
单位	等于 🔽 manager	
邮箱	等于 🔽	
逻辑关系	与	
本地角色集合	已经选择	
doc_role develop doc clerk	-> ×	
	确定 取消	

参数设置完成后,点击"确定"按钮。

6. 验证:证书用户"user1"登录后,被赋予映射角色"clerk"的访问权限;证书 用户"manager1"登录后,被赋予映射角色"manager"的访问权限。

假设用户"user1"和"manager1"使用同一主机"10.10.10.2"登录,并且该主机已 经下载完所有的控件。

1) 用户"user1"采用文件方式证书登录 SSL VPN 网关(对外 IP 为 10.10.10.10)。

a) 双击用户"user1"的"PKCS12"格式的文件证书,根据提示将客户端证书安装 到本机中。

b) 在浏览器的 URL 地址栏输入 SSL VPN 网关的公网 IP, 进入用户登录界面,如下 图所示。

個 用户登录 - ■icrosoft Internet Explorer	
文件 (2) 编辑 (2) 查看 (2) 收藏 (4) 工具 (2) 帮助 (4)	A
🔇 后退 ▼ 🕥 ァ 🖹 😰 🐔 🔎 搜索 👷 收藏夹 🚱 😥 😓	
地址 @) 🗃 https://10.10.10.10/index1.html	💌 🔁 转到 链接 »
了天融信 TOPSEC	En English ? 帮助
口令认证 证书认证 双因子认证	
用户名:	
· · · · · · · · · · · · · · · · · · ·	
□ 使用代理服务器	11
登录	
	) 🕑 可信站点 🍂

c) 激活"证书认证"页签, 然后点击"证书认证"按钮, 弹出选择证书界面, 如下 图所示。

ž	择数字	证书	<u>? ×</u>
	-标识	您要查看的网站要求标识。请选择证书。	
		名称	
		user1 LocalCert	
		更多信息 ( <u>M</u> ) 查看证书 ( <u>V</u> )	· _
		确定即非	<b>i</b>

d)选择 user1 用户证书后,点击"确定"按钮即可成功登录到 user1 用户界面中,并 且获取到映射角色"clerk"的访问权限,如下图所示。

参用户控制界面 - ■icrosoft Internet Explorer	
文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(E) 帮助	ክዊ) 🦧
🔾 后退 🔹 🗇 👻 👔 🔥 🔎 搜索 🌟 收藏夹 💰	3 🔊 🕹 🖻
地址 @) 🗃 https://10.10.10.10/vone/portal/index.ht	nl 🔽 🄁 转到 链接 »
了 天 融 信	seri 🤷 useri
资源列表 配置 状态	
名称	描述
🧔 <u>web 235</u>	-
2017年1月11日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日	

- 2) 用户"manager1"采用 USBKEY 证书登录 SSL VPN 网关(对外 IP 为 10.10.10.10)。
- a) 安装 epass1000 的驱动程序。
- b)将装有证书的 epass1000 插入主机的 USB 接口。

c) 在浏览器的 URL 地址栏输入 SSL VPN 网关的公网 IP, 进入用户登录界面,如下 图所示。

灣用户登录 - ■icroso	oft Internet Explorer	
文件(27) 编辑(28) 查	看 (Y) 收藏 (A) 工具 (T) 帮助 (H)	🥂
🔇 后退 🔹 🕘 🔹 👔	👔 🏠 🔎 搜索  ☆ 收藏夹 🥝 🛛 😥 🚽 🍃	(
地址 @) 🙋 https://10.	10.10.10/index1.html	▼ → 转到 链接 ≫
	了 天 融信	En English (? 帮助
	口令认证 证书认证 双因子认证	
	用户名:	
	密 码: 📄 忘记部	码
	□ 使用代理服务器	
	秦章	
( ) (		
E		🔒 🕑 可信站点 🛛 🎢

d) 激活"证书认证"按钮, 然后点击"证书认证"按钮, 弹出选择证书界面, 如下 图所示。

泷	择数字	正书		<u>?</u> ×
	-标识	您要查看的网站	\$要求标识。请选择证书。	
		名称		
		manager1	LocalCert	
		user1	LocalCert	
				)
			确定	以消

e)选择 manager1 用户证书后,点击"确定"按钮,弹出验证用户 PIN 码的对话框,如下图所示。

用户 PIN 码验证 🛛 🛛	:
你好 epass1000 ! 现在需要验证您的用户 PIN 码。	
用户PIN:	
登录[ <u>0]</u> 取消[ <u>c</u> ]	

f) 输入用户 PIN 后,点击"登录"按钮即可成功登录到 manager1 用户界面中,并且 获取到映射角色"manager"的访问权限,如下图所示。

🦉 (A	]户控制界面 - ∎icrosof	t Internet Explor	er		
文作	‡(2) 编辑(2) 查看(V)	收藏(A) 工具(E)	帮助(H)		20
3	后退 🕶 🕤 👻 😰 🏠	🔎 搜索 🖙 收藏夹	😧 🔗 🖏	E	
地址	🕲 🙋 https://10. 10. 10.	. 10/vone/portal/index	ĸ. html		💌 芛 转到  链接 🎽
0	<b>人</b> 天融信				🔺 manager 1
	资源列表配置	置 状态			
	名称		描述		
	🛒 <u>ftp 220</u>	1	d		
					<b>•</b>
E (2)					「信站点

#### 注意事项

1. 用户证书文件的下载需要在 WEBUI 界面中进行操作,命令行无法进行配置。

2. USBKEY 驱动程序和证书写入工具将会放在随机光盘中提供给客户。

# 第三方证书认证

SSL VPN 网关支持采用第三方 CA 签发的证书对移动用户进行认证。当远程用户采 用第三方 CA 颁发的证书登录 VPN 网关, VPN 网关在本地认证该用户时,亦需要在此导 入该 CA 的根证书。在这种方式下, VPN 网关将通过第三方 CA 的根证书验证客户端证书 是否合法。导入第三方 CA 的根证书后,可以设置该 CA 的 CRL 自动下载协议、下载地 址等,也可以手工导入 CRL。

当远程用户采用证书认证方式时,需要管理员将用户按照证书中的某个属性映射到本 地数据库中的角色上,然后基于角色进行访问权限控制。

### 基本需求

客户需要高安全等级的接入方式,希望采用第三方 CA 签发的数字证书对移动用户进行身份认证。用户自己有独立的 CA 系统,用户证书由 CA 生成并发放。用户 CA 不支持 LDAP/OCSP 等证书在线认证,CA 根证书可以导出。用户 CA 能够生成 CRL 列表文件, 并需要导入 VPN 网关进行证书合法性检查。 本例中第三方 CA 根证书为 VoneRootCA,为移动用户 zhangsan 和 lisi 签发的数字证书中"name"分别为 zhangsan 和 lisi。网关上设置根据证书"name"进行授权,"name"为"zhangsan"的外部证书用户被映射到本地角色"manager"并获得该角色的访问权限,"name"为"lisi"的外部证书用户被映射到本地角色"clerk"并获得该角色的访问权限。



#### 图 31 第三方证书认证的网络部署图

### 配置要点

- ▶ 在防火墙 A 上进行相关配置。
- ➤ 开启 Eth1 所属区域的 SSLVPN 服务。
- ▶ 导入第三方 CA 根证书和 CRL 列表文件。
- 配置用户证书映射(假设映射角色已经配置完成,并且已经配置完成这些角色的 安全策略)。
- ▶ 验证:外部证书用户"zhangsan"登录后,被赋予映射角色"manager"的访问 权限;外部证书用户"lisi"登录后,被赋予映射角色"clerk"的访问权限。

## 防火墙 A 的配置步骤

为了保护 SSL VPN 网关的安全,管理员一般将防火墙 A 的 eth1 口所属区域的权限设置为"禁止访问",然后通过配置访问控制规则,只允许远程用户对 SSL VPN 网关上特定端口进行访问。

1) 在防火墙 A 上开放 TCP 443 端口,用于远程用户访问 SSL VPN 网关用户界面,如下图所示。

預定义 自定义 服务组		
🕂 添加 🗴 清空		
		总计: 1
名称	详细 🔶	操作
443	TCP/443	23

2) 定义访问控制规则,如下图所示。

访问控制								
目的区域	所有区域	T	策略组	所有组	] 高級	搜索	口。	示策略统计
╋ 添加維	i 🕂 添	加策略				总计: 1	毎页: 30条	•
ID	控制	源		目的		服务	选项	操作
8063	~	<mark>区域:</mark> area_eth0		区域: area_eth1		443		<ul> <li>*</li> </ul>
						₩ ◀ 1	▶ ▶ 转到	/1 Go

3)配置主机地址,即 SSL VPN 网关的真实地址"172.16.1.1"和对外地址"10.10.10.10",如下图所示。

主机 范围 子网 地址組		
➡添加 前清空		总计: 2
名称 🗢	IP地址 🔶	操作
sv	10. 10. 10. 10	2
SV_MAP	172, 16, 1, 1	2

4) 配置双向地址转换(到 SSL VPN 网关的映射),如下图所示。

地址转换							
目的区域	所有区域	▼ 高级搜索		显示策略统计			
╋ 添加				;	急计:1 毎页: 30条	•	
ID	类型	源	目的	服务	转换	操作	
8067	双向转换	区域: area_ethO	地址: SV		源: eth1 <mark>目的:</mark> SV_MAP	<ul> <li>*</li> </ul>	
	K < 1 ▶ N 转到 /1 Go						

## WEBUI 配置步骤

本案例中假设所有模块的配置信息已经配置完成,只需将外部证书用户映射到某个角 色,然后获取该角色的访问权限。

#### 1. 开启 Eth1 所属区域的 SSLVPN 服务。

选择 系统管理 > 配置, 激活"开放服务"页签, 然后点击"添加", 开放 Eth1 口 所属区域的 SSLVPN 服务, 如下图所示。

系统参数	开放服务	时间	SNMP	邮件设计	置  短
			添加	加配置	
		服务名称 控制区域 控制地址	SSLVPN area_eth1 any[范围]		<ul><li>✓</li><li>✓</li><li>✓</li></ul>
			确定	取消	i )

参数设置完成后,点击"确定"按钮即可。

#### 2. 导入第三方 CA 根证书和 CRL 列表文件。

1)管理员登录管理界面后,点击导航菜单 PKI 设置 > 第三方 CA 证书,点击"导入 CA"。

2) 点击"浏览..." 按钮,选择 CA 根证书和证书撤销列表 CRL 的存放路径。

第三方CA证书		
		导入CA证书
	CA证书文件 证书撤销列表文件	C:\Documents and Sett 浏览 C:\Documents and Sett 浏览
	确定	取消

参数设置完成后,点击"确定"按钮,将其导入到 SSL VPN 网关中,如下图所示。

第三方CA证书								
@ 导入CA @ 配置CRL自动下载 。						总计: 1		
证书名称	有效期	详细信息	CA删除	CRL属性	CRL导入	CRL下载设置	CRL下载	CRL删除
VoneRootCA	Oct 10 15:41:51 UTC 2009- Oct 08 23:41:51 UTC 2019	E	3	<b>E</b>	<b>B</b>	2	ß	3

说明:

♦	根证书和 CRL 列表可以是 PEM 或者 DER 编码格式。此处的 CRL 列表可以为空,	管理
	员可以通过点击"CRL 导入"图标,导入新的 CRL 列表文件。	

3. 配置用户证书映射(假设映射角色已经配置完成,并且已经配置完成这些角色的 安全策略)。

将名称(name)为"zhangsan"的外部证书用户映射到角色"manager",然后将名称(name)为"lisi"的外部证书用户映射到角色"clerk"。

假设已经配置完成映射角色"clerk"、"manager"及映射角色的安全策略,允许属于角色"clerk"的用户访问端口转发资源"web\_235"(即 web 服务器"192.168.83.235"); 允许属于角色"manager"的用户访问端口转发资源"ftp\_220"(即 ftp 服务器 "192.168.83.220")。

1)点击导航菜单 用户认证 > 认证设置,然后点击证书服务器 "cert"条目右侧的
 修改图标 "☑",配置后的界面如下图所示。

认证设置			
		映射策略	
	认证服务器 启用 授权类型	cert 是 外部属性映射	<b>v</b> <b>v</b>
	确定	取消	

参数设置完成后,点击"确定"按钮。

2)点击证书服务器 "cert"条目右侧的"外部属性映射"链接,进入"证书属性"窗口。点击"添加"链接,将外部证书用户"zhangsan"映射到角色"manager",如下图所示。

认证设置	
	外部映射属性
名称	等于 🔽 zhangsan
国家	等于 🔽
省	等于
城市	等于
组织	等于
单位	等于
邮箱	等于
逻辑关系	与 💌
本地角色集合	已经选择
doc_role develop doc clerk	-> X
	确定 取消

参数设置完成后,点击"确定"按钮。

3) 在"证书属性"窗口中,点击"添加"链接,将外部证书用户"lisi"映射到角色 "clerk",如下图所示

认证设置		
		外部映射尾性
	名称 国家 省 城市	等于       lisi         等于       □         等于       □         等于       □         第丁       □
	组织 单位 邮箱	等于        等于        等于
本地 doo doo man	逻辑关系 也角色集合 c_role velop c nager	与 ■
		确定 取消

参数设置完成后,点击"确定"按钮。

4. 验证:外部证书用户"zhangsan"登录后,被赋予映射角色"manager"的访问 权限;外部证书用户"lisi"登录后,被赋予映射角色"clerk"的访问权限。

假设外部证书用户"zhangsan"和"lisi"使用同一主机"10.10.10.2"登录,并且该 主机已经下载完所有的控件。

1) 用户"zhangsan"采用文件方式证书登录 SSL VPN 网关(对外 IP 为 10.10.10.10)。

a) 双击用户"zhangsan"的文件证书,根据提示将客户端证书安装到本机中。

b) 在浏览器的 URL 地址栏输入 SSL VPN 网关 IP, 进入用户登录界面, 如下图所示。

個 用户登录 - ■icrosoft Internet Explorer	
文件 (2) 编辑 (2) 查看 (2) 收藏 (4) 工具 (2) 帮助 (4)	A
🔇 后退 ▼ 🕥 ァ 🖹 😰 🐔 🔎 搜索 👷 收藏夹 🚱 😥 😓	
地址 @) 🗃 https://10.10.10.10/index1.html	💌 🔁 转到 链接 »
了天融信 TOPSEC	En English ? 帮助
口令认证 证书认证 双因子认证	
用户名:	
· · · · · · · · · · · · · · · · · · ·	
□ 使用代理服务器	11
登录	
	) 🕑 可信站点 🍂

c) 激活"证书认证"页签, 然后点击"证书认证"按钮, 弹出选择证书界面, 如下图所示。

泷	择数字	正书		? ×
	-标识	您要查看的网站要	求标识。请选择证书。	
		名称	颁发者	
		lisi	VoneRootCA	
		zhangsan	VoneRootCA	
		J	更多信息 (M)   査看证书 (	D
			确定	取消

d)选择"zhangsan"的数字证书后,点击"确定"按钮即可成功登录到用户界面中, 并且获取到映射角色"manager"的访问权限,如下图所示。

❷ 用户控制界面 - ■icrosoft Inte	rnet Explorer	
文件(E) 编辑(E) 查看(V) 收藏(A	y) 工具(T) 帮助(H)	2
😋 后退 🔹 🕤 👻 😰 🚮 🔎 搜	索 🧙 收藏夹 🤣 🍛 🍡 🔛	
地址 @) 🙋 https://10.10.10.10/vone	/portal/index.html	▼ 封到 链接 ※
<b>了天融信</b> 変感列表 配置 状	态	🔺 zhangsan
7.54		
- 石柳	<u>ع</u> א <del>מ</del> ו	
<u>itp 220</u>	4	
(2) 完毕		

- 2) 用户"lisi"采用文件方式证书登录 SSL VPN 网关(对外 IP 为 10.10.10.10)。
- a) 双击用户"lisi"的文件证书,根据提示将客户端证书安装到本机中。
- b) 在浏览器的 URL 地址栏输入 SSL VPN 网关 IP, 进入用户登录界面, 如下图所示。

Ø用户登录 - ■icros	oft Internet Explorer	
文件(王) 编辑(王) 查	Ē看(⊻) 收藏(&) 工具(亚) 帮助(出)	
🔇 后退 🔹 🕘 👻 📘	👔 🏠 🔎 搜索 🌟 收藏夹 🤣 🍛 🍡 🔜	
地址 (1) 🙋 https://10	. 10. 10. 10/index1. html	💌 芛 转到 🛛 链接 🌺
	了 天 融信	En English ? 帮助
	口令认证 证书认证 双因子认证	
	用户名:	
	· · · · · · · · · · · · · · · · · · ·	<u>–</u>
	□ 使用代理服务器	11
	臣录	
é		🔒 🕑 可信站点 🍡 🏸

c) 激活"证书认证"页签, 然后点击"证书认证"按钮, 弹出选择证书界面, 如下 图所示。

泛	择数字	正书		? ×
	-标识	您要查看的网站要求	标识。请选择证书。	
		名称		
		lisi	VoneRootCA	
		zhangsan	VoneRootCA	
		更這	多信息(M) 査利	₩U
			确定	取消

d)选择"lisi"的数字证书后,点击"确定"按钮即可成功登录到用户界面中,并且 获取到映射角色"clerk"的访问权限,如下图所示。

叠用户控制界面 - ∎icrosoft Int	ernet Explorer	
文件(E) 编辑(E) 查看(V) 收藏	(A) 工具(T) 帮助(A)	2
😮 后退 👻 🕥 🖌 🖹 😰 🏠 🔎 推	雙索 👷 收藏夹 🥝 🔝 🚽 🍃	
地址 @) 🙋 https://10.10.10.10/vor	ne/portal/index.html	▼ → 转到 链接 ※
了 天 融信		
资源列表 配置 礼	大态	
名称	描述	
🥭 <u>web 235</u>		
	-	
		_

# Radius 认证

### 基本需求

采用单臂模式,将 SSL VPN 网关部署在网络内部。远程 Radius 用户"doc"登录 SSL VPN 网关后,被映射到本地角色"doc\_role",同时获得该角色的访问权限,拒绝访问其他资源,从而实现对内网资源的访问控制。网络示意图如下所示。



图 32 SSL VPN 网关 Radius 认证示意图

### 配置要点

- ▶ 在防火墙上进行相关配置。
- ▶ 在 Radius 上进行相关配置。
- ➤ 在 SSL VPN 网关上配置 Radius 认证服务器。
- ▶ 在 SSL VPN 网关上配置映射策略(假设映射角色已经配置完成,并且已经配置 完成该角色的安全策略)。
- ▶ 验证: Radius 用户"doc"登录后,被赋予映射角色"doc\_role"的访问权限。

## 防火墙的配置步骤

为了保护 SSL VPN 网关的安全,管理员一般将防火墙 A 的 eth0 口所属区域的权限设置为"禁止访问",然后通过配置访问控制规则,只允许远程用户对 SSL VPN 网关上特定端口进行访问。

1) 在防火墙 A 上开放 TCP 443 端口,用于远程用户访问 SSL VPN 网关用户界面,如下图所示。

預定义	自定义	服务组		
╋ 添加	─ 清空			
				总计: 1
名称			\$ 详细	\$ 操作
443			TCP/443	23

#### 2) 定义访问控制规则,如下图所示。

访问控制									
目的区域	所有区域	T	策略组	所	有组	▼ 高级	叟索	□ 紡	计信息
十 添加約	且 ╬ 添	加策略					总计:1 毎	页; 30条	•
ID	控制	源			目的		服务	选项	操作
8088	v	<mark>区域:</mark> area_eth1			<mark>区域:</mark> area_ethO		443		
						R	< <b>1</b> ►	▶ 转到	/1 Go

3) 配置主机地址,即 SSL VPN 网关的真实地址"192.168.83.237"和对外地址

"10.10.10.10"	,	如下图所示。
---------------	---	--------

主机 范围 子网 地址組						
♣添加 mā空 总计: 2						
名称	\$	IP地址 ◆	操作			
SV		10. 10. 10. 10	2			
SV_MAP		192. 168. 83. 237	🕗 🧟			

#### 4) 配置双向地址转换(到 SSL VPN 网关的映射),如下图所示。

地址转换						
目的区域	所有区域	▶ 高级搜索	□ 统	计信息		
十 添加	♣ 添加 总计: 1 每页: 30条					
ID	类型	源	目的	服务	转换	操作
8092	双向转换	区域: area_eth1	<mark>地址:</mark> SV		源: ethO 目的: SV_MAP	
K ◀ 1 ▶ N 转到 /1 Go						

# Radius 的配置步骤

1) 在 Radius 服务器上配置预共享密钥为"topsec",认证端口为"1812"。

2) 在 Radius 服务器上添加用户"doc"。

## WEBUI 配置步骤

#### 1. 配置 Radius 认证服务器。

1) 在左侧导航树上,点击 用户认证 > 外部认证,然后点击"添加服务器",设置 Radius 服务器参数,如下图所示。

外部认证			
	认证服务器属性		
	服务器名称 认证协议 服务器地址 服务器端口 超时时间 预共享密钥 认证客户端地址 认证方法	radius_server RADIUS 192. 168. 83. 220 1812 ••••••• 192. 168. 83. 237 CHAP	* * [5-180秒,缺省为5秒] *
	(	确定	取消

2)参数设置完成后,点击"确定"按钮,完成 Radius 认证服务器的配置。

2. 配置映射策略(假设映射角色已经配置完成,并且已经配置完成该角色的安全策略)。

将 Radius 服务器中的所有用户都映射到角色"doc\_role"。

假设已经配置完成映射角色"doc\_role"及其安全策略,允许属于角色"doc\_role"的 用户访问端口转发资源"ftp\_220"(即 ftp 服务器"192.168.83.220")。

 1)点击导航菜单用户认证 > 认证设置,然后点击"添加映射",配置映射策略, 界面如下图所示。

认证设置				
映射策略				
可用本地角色 develop doc clerk manager zhangsan lisi	认证服务器 启用 授权类型	radius_server       是       本地角色集合映射       Impr manage       doc_role		
<u> </u>				
	确定	取消		

参数设置完成后,点击"确定"按钮。

3. 验证: Radius 用户"doc"登录后,被赋予映射角色"doc\_role"的访问权限。

假设用户"doc"使用主机"10.10.10.2"登录,并且该主机已经下载完所有的控件。

1) 在浏览器的 URL 地址栏输入 SSL VPN 网关的外网地址 "https://10.10.10.10",进入用户登录界面,界面如下图所示。

叠用户登录 - Microsoft Internet Explorer	
文件 (E) 编辑 (E) 查看 (Y) 收藏 (A) 工具 (E) 帮助 (H)	🥂
③ 后退 · ○ · 区 ② 公 /> 搜索 · 欠 收藏来 ② ◎ · ◎ □	
地址 @) @ https://10.10.10/index4.html	▼ → 转到 链接 ※
了天融信	English ? 帮助
口令认证 双因子认证	
用户名: 密码: 置录	
<u>忘记密码 证书链下载 USB Key驱动下载</u>	
	0
	)可信站点 //

2) 输入"doc"正确的用户名、密码,并成功登录后,获取到映射角色"doc\_role"的访问权限,可以访问授权资源"ftp\_220",如下图所示。

▲用尸控制界面 - Microsoft Internet Explorer	JN				
文件 (E) 编辑 (E) 查看 (V) 收藏 (A) 工具 (T) 帮助 (H)	<b>*</b>				
③ 后退 ▼ ⑤ ▼ 図 図 🏠 🔎 搜索 📩 收藏夹 🥙 🙆 ▼					
地址 @) 🧉 https://10.10.10.10/vone/portal/index.html 🔽 ラ 转到 链	€ »				
了天融信 ▲ doc ↓					
夕 <u>物</u> 世法					
in the 22D in the second secon					
	-				
	-				

## 注意事项

SSL VPN 网关目前支持的第三方认证服务器包括: Radius、TACACS、AD、LDAP 和 SecurID。

# 双因子认证

## 基本需求

1) 网关使用双因子认证方式(需要进行口令认证和证书认证)对远程用户"test"进行认证。

2) SSL VPN 网关的 CA 系统负责为远程用户"test"颁发用户证书。

3) 认证通过后,用户"test"获得的访问权限包括:该用户自身的访问权限,该用户 所属角色"test\_role"的访问权限,以及该用户的证书映射角色"cert\_role"的访问权限。





### 配置要点

- ▶ 在防火墙 A 上进行相关配置。
- ▶ 开启 Eth1 所属区域的 SSLVPN 服务。
- ▶ 添加用户"test"。
- ▶ 配置角色"test\_role",然后将"test"添加到该角色中。
- ▶ 配置角色"cert\_role",用于证书映射。
- ▶ 配置证书映射。
- ▶ 创建本地根证书。
- ▶ 签发并保存用户证书。
- ▶ 配置授权资源。
- ▶ 配置 ACL 规则。
- ▶ 配置安全策略。
- ▶ 配置虚拟门户。
- ▶ 验证:本地用户"test"登录后,被赋予用户自身的访问权限,用户所属角色 "test\_role"的访问权限,以及证书映射角色"cert\_role"的访问权限。

### 防火墙 A 的配置步骤

为了保护 SSL VPN 网关的安全,管理员一般将防火墙 A 的 eth1 口所属区域的权限设置为"禁止访问",然后通过配置访问控制规则,只允许远程用户对 SSL VPN 网关上特定端口进行访问。

1) 在防火墙 A 上开放 TCP 443 端口,用于远程用户访问 SSL VPN 网关用户界面,如下图所示。
| 預定义  | 自定义  | 服务组 |          |   |       |
|------|------|-----|----------|---|-------|
| ╋ 添加 | ─ 清空 |     |          |   |       |
|      |      |     |          |   | 总计: 1 |
| 名称   |      |     | \$<br>详细 | ¢ | 操作    |
| 443  |      |     | TCP/443  |   | 2     |

#### 2) 定义访问控制规则,如下图所示。

访问控制									
目的区域	所有区域	•	策略组	所有组	•	高级	搜索	□ 显	示策略统计
十 添加約	i - ┣ 添:	加策略					总计: 1	毎页: 30条	•
ID	控制	源		目的			服务	选项	操作
8063	•	<mark>区域:</mark> area_ethO		区域: area_eth1			443		<ul> <li>*</li> </ul>
							H 4 1	▶ ▶ 转到	/1 Go

3)配置主机地址,即 SSL VPN 网关的真实地址"172.16.1.1"和对外地址"10.10.10.10",如下图所示。

主机 范围 子网 地址組		
➡ 添加 前清空		总计: 2
名称 🔶	IP地址 ◆	操作
SV	10. 10. 10. 10	2
SV_MAP	172. 16. 1. 1	2

## 4) 配置双向地址转换(到 SSL VPN 网关的映射),如下图所示。

地址转换						
目的区域	所有区域	▼ 高级搜索		显示策略统计		
十 添加				;	总计:1 毎页: 30条	-
ID	类型	源	目的	服务	转换	操作
8067	双向转换	区域: area_ethO	<mark>地址</mark> : SV		源: eth1 <mark>目的:</mark> SV_MAP	<ul> <li>•</li> </ul>
				М	▲ 1 ▶ ▶ 转到	/1 <b>Go</b>

## WEBUI 配置步骤

1. 开启 Eth1 所属区域的 SSLVPN 服务。

选择 系统管理 > 配置, 激活"开放服务"页签, 然后点击"添加", 开放 Eth1 口 所属区域的 SSLVPN 服务, 如下图所示。

系统参数	开放服务	时间	SNMP (	8件设置 短
			添加配置	
		服务名称	SSLVPN	~
	÷	控制区域	area_eth1	•
	:	控制地址	any [范围]	*
			确定	取消

参数设置完成后,点击"确定"按钮即可。

### 2. 添加用户"test"。

1) 点击导航菜单 用户认证 > 用户管理, 然后选择"用户管理"页签, 点击"添加 用户", 在弹出的窗口中配置用户"test"的信息, 如下图所示。

用户管理	在线用户	用户设置	
		用户属性	
	用户名 用户描述 认证方式 口令 确认口令	test 本地口令+证书认证 ●●●●●●●	】 ▼ 】* [6-31个字符] 】*
	<sup>可用用巴</sup>		
		确定	取消

输入用户名称,然后选择"认证方式"为"本地口令+证书认证",最后输入口令。 2)参数设置完成后,点击"确定"按钮。

## 3. 配置角色"test\_role",然后将"test"添加到该角色中。

1) 点击导航菜单 用户认证 > 角色管理, 然后选择"角色管理"页签, 点击"添加 角色", 在弹出的窗口中配置角色"test\_role"的信息, 如下图所示。

角色管理 分级管理	
	角色属性
角色名 角色描述 DHCP地址池 选择用户	test_role * 不添加
高级	
	确定取消

输入角色名称,最后选择用户"test"。

需要注意的是:本案例中的授权资源均属于端口转发资源,所以无需配置 DHCP 地 址池,如果要对角色或属于该角色的用户授予全网接入资源的访问权限,必须配置 DHCP 地址池。

2)参数设置完成后,点击"确定"按钮。

#### 4. 配置角色"cert\_role",用于证书映射。

1) 点击导航菜单 用户认证 > 角色管理, 然后选择"角色管理"页签, 点击"添加 角色", 在弹出的窗口中配置角色"cert\_role"的信息, 如下图所示。

角色管理 分级管理		
	角色属性	
角色名 角色描述 DHCP地址池 选择用户	cert_role * 不添加 已经选择	
test ()		
高级		
	确定 取消	

输入角色名称。

需要注意的是:本案例中的授权资源均属于端口转发资源,所以无需配置 DHCP 地址池,如果要对角色或属于该角色的用户授予全网接入资源的访问权限,必须配置 DHCP 地址池。

2)参数设置完成后,点击"确定"按钮。

## 5. 配置证书映射。

将所有证书用户全部映射到角色"cert\_role"。

1)点击导航菜单 用户认证 > 认证设置,然后点击证书服务器 "cert"条目右侧的
 修改图标 "↓",配置后的界面如下图所示。

认证设置		
	B	射策略
可用本地角色 test_role ldaprole	认证服务器 启用 授权类型	cert       是       本地角色集合映射       Impr 匹配角色
	确定	取消

2)参数设置完成后,点击"确定"按钮。

## 6. 创建本地根证书。

1)管理员登录管理界面后,点击导航菜单 **PKI 设置 > 本地 CA 策略**,然后选择"根 证书"页签,点击"获取证书",如下图所示。

根证书 签发证书 证书撤销列表	
◎ 获取证书 ◎ 导出证书	
Version: V3 CN: VoneRootCA SerialNumber: 0x00 Issuer: CN=VoneRootCA Subject: CN=VoneRootCA NotBefore : Oct 29 10:24:19 UTC 2009 NotAfter : Oct 27 10:24:19 UTC 2019 RSA Public Key: (1024 bits) Modules:	*

2) 选中"生成新证书"前的单选按钮,然后填写相应项目,如下图所示。

根证书 签2	发证书 证书撤销列ā	ŧ	
		获取根证书	
	<ul> <li>文件方式导入 证书 私钥</li> <li>PKCS12文件格式-</li> </ul>		
	证书文件 证书文件密码 〇 以本机设备证书-	导入	浏览
	<ul> <li>生成新证书</li> <li>名称</li> <li>国家</li> <li>省</li> <li>城市</li> <li>电子邮件</li> </ul>	LocalCert CN BJ HD doc@topsec.com.cn	* [两个英文字符]
	単位	RD 確定 取消	

3) 点击"确定"按钮,完成根证书创建。

#### 7. 签发并保存用户证书。

1) 点击导航菜单 **PKI 设置 > 本地 CA 策略**, 然后选择"签发证书"页签, 点击"生成新证书"。

2) 配置远程用户"test"的用户证书,如下图所示。

根证书 签发证书 证书	3撤销列表
	签发证书
名称	test *
国家	[两个英文字符]
省	
城市	
电子邮件	•
组织	
单位	
失效时间 	] [格式:YYYY/MM/DD]
	确定 取消

参数设置完成后,点击"确定"按钮使配置生效。

3)将"test"的证书保存到本地。

① 在"签发证书"页面,点击"test"条目右侧的"下载"图标,弹出"导出签发证书"页面。

② 在"导出签发证书"页面中,选择证书的文件格式为"PKCS12",不输入密码, 然后点击"导出证书"按钮,界面出现"证书点击下载"链接,如下图所示。

根证书 签发证书	证书撤销列表
	导出签发证书
	选择要使用的文件格式 PKCS12 < 导出证书 密码 [如果需要 密码保护,请先输入密码再导出] 证书点击下载[或用右键另存]
	返回

③ 点击"证书点击下载"链接,弹出文件保存提示框,如下图所示。

文件下载	×
您想打开或保存此	文件吗?
名称:	test.p12 Personal Information Exchange, 1.54 KB 192.168.83.237
来自 Inte 危害您的讨 该文件。至	rnet 的文件可能对您有所帮助,但某些文件可能 计算机。如果您不信任其来源,诸不要打开或保存 有何风险?

④ 点击"保存"按钮,在文件保存窗口中为证书文件指定保存路径后,点击"保存" 按钮即可。

### 8. 配置授权资源。

点击导航菜单 **SSLVPN > 资源管理**, 配置三条端口转发资源, 配置完成后的界面如 下图所示。

资源管理					
C 添加 (	夏清空	总	汁:3 毎页:	全部	•
资源名称	访问方式	资源地址	描述	修改	删除
ftp_220	端口转发	ftp://192.168.83.220			3
ftp_235	端口转发	ftp://192.168.83.235			3
ftp_234	端口转发	ftp://192.168.83.234			0
		M 4 1	► H	转到	/1 Go

### 9. 配置 ACL 规则。

点击导航菜单 SSLVPN > ACL 管理, 默认禁止远程用户访问内网资源, 然后配置三条 ACL 规则, 分别允许访问内网资源"ftp\_220"、"ftp\_235"和"ftp\_234", 如下图所示。

ACL管理							
ACI默认策略 ④ 允许 〇 禁止 确定 ACL规则列表							
⑦添加规则 ⑦ 清空	规则				总计:3 毎页: 全部		•
规则名称	资源名称	行为	策略	星期	时间	修改	删除
访问ftp服务器(220)	ftp_220	全部	允许	星期一 星期二 星期三 星期四 星期五 星期六 星期日	00:00:00-23:59:59		0
访问ftp服务器(235)	ftp_235	全部	允许	星期一 星期二 星期三 星期四 星期五 星期六 星期日	00:00:00-23:59:59		3
访问ftp服务器(234)	ftp_234	全部	允许	星期一 星期二 星期三 星期四 星期五 星期六 星期日	00:00:00-23:59:59	C2	ā
K < 1 ▶ N 转到 /1 Go							

#### 10. 配置安全策略。

1)为角色"test\_role"配置一条安全策略,将该角色与"访问 ftp 服务器(220)"相关联,即授权属于该角色的所有用户访问内网资源"ftp\_220"。

a)点击导航菜单 SSLVPN > 安全策略,然后选择"角色安全策略"页签,点击角 色"test\_role"条目右侧的"安全策略设置"图标。

b) 勾选"启用默认模块",如下图所示。

角色安全策略 用户安全策略				
⑥ 启用默认模块 (WEB转发、应用WEB化、端口转发)				
〇 自定义模块设置(端口转发模块和全网接入模块不能同时启用)				
确定返回				

设置完成后,点击"确定"按钮使配置生效。

c)点击"添加规则",将允许访问公司内网资源"ftp\_220"的ACL规则"访问ftp服务器(220)"赋予该角色,如下图所示。

角色安全策略	用户安全策略	
	添加規则	
	角色名称 test_role ACL名称 访问ftp服务器▼	
	确定 取消	)

参数设置完成后,点击"确定"按钮,如下图所示。

角色安全策略 用户安全策略					
<ul> <li>◎ 启用默认模块 (WEB转发、应用WEB化、端口转发)</li> <li>○ 自定义模块设置 (端口转发模块和全网接入模块不能同时启用)</li> </ul>					
确定返回					
acl規則					
C 添加規则         C 清空規则         总计:1					
acl名称         上移         下移         插入         删除					
访问ftp服务器(220) <b>1</b> 🕽 🗋					

2)为角色"cert\_role"配置一条安全策略,将该角色与"访问 ftp 服务器(235)" 相关联,即授权属于该角色的所有用户访问内网资源"ftp\_235"。

a)点击导航菜单 SSLVPN > 安全策略,然后选择"角色安全策略"页签,点击角 色"cert\_role"条目右侧的"安全策略设置"图标。

b) 勾选"启用默认模块",如下图所示。

角色安全策略 用户安全策略					
● 启用默认模块 (WEB转发、应用WEB化、端口转发)					
○ 自定义模块设置(端口转发模块和全网接入模块不能同时启用)					
确定返回					

设置完成后,点击"确定"按钮使配置生效。

c)点击"添加规则",将允许访问公司内网资源"ftp\_235"的ACL规则"访问 ftp 服务器(235)"赋予该角色,如下图所示。

角色安全策略	用户安全策略	
	添加規則	
	角色名称 cert_role ACL名称 访问ftp服务器	
	确定 取消	)

参数设置完成后,点击"确定"按钮,如下图所示。

角色安全策略 用户安全策略					
<ul> <li>● 启用默认模块 (WEB转发、应用WEB化、端口转发)</li> <li>● 自定义模块设置 (端口转发模块和全网接入模块不能同时启用)</li> </ul>					
确定返回					
acl規則					
C 添加規则         C 清空規则         总计:1					
acl名称         上移         下移         插入         删除					
访问ftp服务器(235) <b>1</b> 🕽 🗋					

3)为用户"test"配置一条安全策略,将该用户与"访问 ftp 服务器(234)"相关联,即授权该用户访问内网资源"ftp\_234"。

a) 点击导航菜单 SSLVPN > 安全策略, 然后选择"用户安全策略"页签, 点击用 户"test"条目右侧的"安全策略设置"图标。

b) 勾选"继承角色配置或启用默认模块",如下图所示。

角色	安全策略	用户	安全策略			
⊙继	承角色配置	或启用默	认模块 (₩	EB转发、	应用WEB化、	端口转发)
0 自注	定义模块设	置(端口郭	拔模块和	全网接入	、模块不能同时	1启用)
	确定		返回			

设置完成后,点击"确定"按钮使配置生效。

c)点击"添加规则",将允许访问公司内网资源"ftp\_234"的ACL规则"访问ftp 服务器(234)"赋予该用户,如下图所示。

角色安全策略 用户安全策略	
	添加規則
用户名称 ACL名称	test 访问ftp服务器▼
	确定 取消

参数设置完成后,点击"确定"按钮,如下图所示。

角色安全策略用户安全策略				
⑥ 继承角色配置或启用默认模块 (WEB转)	发、应用W	EB化、端口	转发)	
○ 自定义模块设置 (端口转发模块和全网)	<b>妾入模块不</b> 的	能同时启用	)	
确定返回	)			
acl規則				
● 添加规则 ● 清空规则				总计: 1
acl名称	上移	下移	插入	删除
访问ftp服务器(234)	t	Ŧ		0

#### 11. 配置虚拟门户。

a) 点击导航菜单 SSLVPN > 虚拟门户。

b)点击虚拟门户列表左上方的"添加",自定义远程用户访问 SSL VPN 网关的用户 界面。自定义虚拟门户时,参数"地址"必须配置为远程用户登录 SSL VPN 网关时的地 址,即 SSL VPN 网关的对外 IP "10.10.10.10",参数"认证服务器名称"必须配置为对 远程用户进行认证的服务器名称,此案例为本地认证服务器"localdb",参数"用户登录 认证方式"需要勾选"双因子",具体配置页面如下图所示。

虚拟门户		
		虚拟门户
	~a.	
	-白柳/ 	portal_10.10.10 *
	吧 <u>业</u> 汕ば服体器を務	10.10.10 ·······························
	6/ NE 80/ 39/ 88/ -C1401	local db
	服务器	
	公告信息	
	选择登录风格	,
		C Endez () Hits
	T	調信
	AL CONTRACTOR	-S:
		「 使用代理服务器
		instre underre
		101
		<ul> <li>回格1</li> </ul>
		C tosts/ C 100
		DOUL LEGUE TERRIE
	全有成品 天静电电"可见符4 安全世界"在力品牌整念,共同组	8/6: # 8:
	W-14EVON Den Sanijaun.	
		ETHETE LOODLYE
		C 风格2
		C tracks (?) Mits
		4
		0400 UHUU 202702 RPS:
	(天躔信	C H: E2EH
	TOPSED	
	/	LTHITE JOHNTE
		○ 风格3
		C Erado (? #B
	anen	
		STANLE MARYALE
	R/	8: 8 H: 8 H:
		IN LINETE LINETE CRIMINES
		C Eliza
	自定义页面	
	控件	·
	and the second sec	○ 手动安装控件 ● 自动安装控件
	模块开关	▶ 启用端口转发
		▶ 启用全网接入
		▶ 启用web转发
		☑ 启用应用WEB化
	显示控制	▶ 显示证书信任链下载连接
		▶ 允许关闭浏览器,只显示为小图标
	USB Key Non下载连接	
	图形认证码设置	● 不显示 ○ 总显示 ○ 登录失败三次后显示
	用户登录认证方式	□ □令 □ 证书 ☑ 双因子
	企业[ ]− 波通反称	
	) 武禄名称 月不关闭士百	
	<b>走</b> 百六回主贝	◎ 是 ∪ 否
	- au	定取消

c)参数设置完成后,点击"确定"按钮。

12. 验证:本地用户"test"登录后,被赋予用户自身的访问权限,用户所属角色 "test\_role"的访问权限,以及证书映射角色"cert\_role"的访问权限。

假设用户"test"等登录主机已经下载完所有的控件,用户"test"采用文件方式证书 登录 SSL VPN 网关(对外 IP 为 10.10.10.10)。

1) 双击用户"test"的"PKCS12"格式的文件证书,根据提示将客户端证书安装到本机中。

2) 在浏览器的 URL 地址栏输入 SSL VPN 网关的对外 IP, 进入用户登录界面,如下 图所示。

營用户登录 - ∎icrosoft Internet Explorer	
文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(T) 帮助	1 (E) 🥂
🔇 后退 🔻 🕥 🖌 🖹 👔 🏠 🔎 搜索 👷 收藏夹 🧔	🖉 🖓 🗟 🕶 🖵 🕲 🚉
地址 @) 餐 https://10.10.10.10/index1.html	▼ ➡ 转到 链接 >> ⑤ SnagIt 当
	C English C #Pth
TOPSEC	
教田子计证	
用户名: 与客户端证书	5主题相同
密 码:	■ 忘记密码
□ 使用代:	里服务器
秦登	
	- ///
	证书链下载 USB Key 驱动下载
e l	📄 📄 😭 Internet 🏼 🎢

3) 在"双因子认证"页签中,输入用户名和密码后,点击"登录"按钮,弹出选择 证书界面,如下图所示。

选择	数字词	正书	? ×
「村	f识— 【】	您要查看的网站要求标识。请选择证书。	
		名称	
		test. VoneRootCA	
		更多信息 (20) 查看证书 (2).	
		确定即消	1

4)选择 test 用户证书后,点击"确定"按钮即可成功登录到 test 用户界面中,并且 获取到用户自身的访问权限(即:内网资源"ftp\_234"),用户所属角色"test\_role"的 访问权限(即:内网资源"ftp\_220"),以及证书映射角色"cert\_role"的访问权限(即: 内网资源"ftp\_235"),如下图所示。

<b>ē</b> J	电户控	制界面 -	licrosof	't Intern	et Explor	er							[	
文	件(正)	编辑(E)	查看(V)	收藏(A)	工具(I)	帮助(	<u>H</u> )							2
G	后退	- 🕤 - 🕨	1 🗈 🏠	🔎 搜索	🥎 收藏夹	•	🔊 - 👌	🖕 🔜 🗸	· 📃 🕲 🛍					
地址	Ł@)∣	🕘 https:/	/10.10.10.	10/vone/p	ortal/index	c.html				•	🔁 转到	链接 >>	🌀 SnagI t	🖆 👘
•	5	天融	信										📤 tes	t
		资源列表	11111	t 状态	×									
	名彩	5				ħ	苗述							
		<u>ftp 220</u>			1	6								
	Ę	<u>ftp 235</u>				6								
	Ę	<u>ftp 234</u>				6								
														Ţ
<u></u>	完毕											👩 Inter	rnet	

# 注意事项

无。

# 与 IDS 联动

通常,网络卫士防火墙用于控制用户或信息在可信任网络和不可信任网络之间的访问,难以对内部用户的非法行为和已经渗透的攻击进行有效的检查和防范;同时,由于防火墙自身具有一定的局限性,如检查的颗粒度较粗等,难以对众多的协议细节进行深入的分析与检查。因此,对安全需求较高的企业往往需要在网络中同时部署 IDS(Intrusion Detective System,入侵检测系统)系统,与防火墙共同构筑企业的安全防御体系。IDS 对流经网络的报文进行详细的分析与检查,探测各种可能的异常情况和攻击行为,并报告给防火墙,由防火墙采取相应措施对攻击源或攻击目的进行阻断。

IDS 系统通常部署在企业防火墙的内部,具体采取的控制措施由使用的特定的 IDS 系统和配置情况决定,下面以 IDS 在防火墙内部署为例说明在防火墙上进行与 IDS 联动的配置方法。

## 基本需求

某企业将 IDS 系统部署在防火墙所保护的内网中, IDS 设备的管理口通过交换机与管理主机 PC3 相连,同时,通过此交换机与防火墙的 Eth0 口相连接,并在此接口上与防火墙进行联动,外网中某一主机 PC1 经过防火墙的外网接口 Eth1 向内网中的某台主机 PC2 发送攻击包,网络结构示意图如下图所示。

要求通过与 IDS 的联动功能配置,阻断 PC1 向内网 PC2 发送的攻击数据包。



#### 图 34 防火墙与 IDS 联动网络示意图

## 配置要点

- ▶ 配置防火墙各接口的 IP 地址,其中 Eth1 连接外网, Eth0 和 Eth2 连接内网。
- ▶ 开放各个接口所属区域的访问权限。
- ▶ 开放 Eth0 口所属区域中主机 PC3 的 IDS 联动服务"TOSIDS"。
- ▶ 配置防火墙的 IDS 联动功能。
- ▶ 配置 IDS 设备的防火墙联动功能。

## WEBUI 配置步骤

1) 配置 Eth0、Eth1 和 Eth2 的 IP 地址,其中 Eth1 连接外网, Eth0 和 Eth2 连接内网。

a)选择 网络管理 > 接口, 然后激活"物理接口"页签, 点击"eth1"接口条目右侧的"设置"图标, 设置接口的 IP 地址为"202.1.1.2/24", 如下图所示。

物理接口	子接口					
			ŧ	<b>赛口设</b> 置		
	名称 描述 状态 模式 地址	eth1	(00: 停用 路由 掩码	13:32:02:23:F O 交換	5) 非同步地址	添加
	地址 202.1.1.2 <b>) 高级</b>		/电冲) 255.2	55. 255. 0		
		Ť	角定		消	

参数设置完成后,点击"确定"按钮即可。

- b)同上所示,设置 eth0 的接口 IP 为"192.168.3.1/24"。
- c) 同上所示, 设置 eth2 的接口 IP 为"192.168.2.1/24"。

2) 开放各个接口所属区域的访问权限。

a)选择 资源管理 > 区域,点击"添加",配置内网区域 area\_eth0 绑定 eth0 属性, 权限为"允许",如下图所示。

区域		
		区域
	名称 访问权限 注释	area_eth0 * 允许 🔽
可用属性:		成员:
eth1 eth2 eth3 ads1 ads11		▲ → × eth0
		确定 取消

参数设置完成后,点击"确定"按钮即可。

b)选择 资源管理 > 区域,点击"添加",配置外网区域 area\_eth1 绑定 eth1 属性, 权限为"允许",如下图所示。

区域			
		<u>X</u>	s,
	名称 访问权限 注释	area_eth1 允许	*
可用属性:			成员:
eth0 eth2 eth3 adsl adsl1			→ ×
		确 定 🔵	取消

参数设置完成后,点击"确定"按钮即可。

c)选择 资源管理 > 区域,点击"添加",配置内网区域 area\_eth2 绑定 eth2 属性, 权限为"允许",如下图所示。

区域			
		区域	
	名称 访问权限 注释	area_eth2 允许	*
可用属性: eth0 eth3 ads1 ads11 ads12		-> ×	成员: eth2
		确定	取消

参数设置完成后,点击"确定"按钮即可。

3) 开放 Eth0 口所属区域中主机 PC3 的 IDS 联动服务"TOSIDS"。

a) 配置 IDS 管理主机对象。

选择 资源管理 > 地址, 然后激活"主机"页签, 点击"添加"配置管理主机 PC3 的地址 192.168.3.2, 如下图所示。

主机	范围 子网 地址組
	主机属性
	名称 PC3 * 物理地址 00:00:00:00:00 IP地址 192.168.3.2 <- 192.168.3.2 ×
	确 定 取 消

参数设置完成后,点击"确定"按钮即可。

b)开放 area\_eth0 区域中主机 PC3 的 IDS 联动服务"TOSIDS"。

选择 **系统管理 > 配置**,然后激活"开放服务"页签,点击"添加"进行配置,如 下图所示。

系统参数 开放服务 时间 SNMP 邮件设置
添加配置
服务名称 TOSIDS ▼ 控制区域 area_eth0 ▼ 控制地址 PC3 [主机]
确 定 取 消

参数设置完成后,点击"确定"按钮即可。

4) 配置防火墙的 IDS 联动功能。

a)选择 入侵防御 > IDS 联动,点击"设置"链接,然后打开 IDS 日志开关,如下 图所示。

IDS联动	
	IDS联动日志
	增加联动规则时记录日志 开 💽 报文被阻止时记录日志 开 💽
	应用

参数设置完成后,点击"应用"按钮即可。

b)选择入侵防御 > IDS 联动,点击"添加"链接,配置 IDS 联动信息,如下图所示。

IDS联动		
	IDSJ	美动配置
	防火墙地址 192. IDS地址 192.	168. 3. 1 168. 3. 3
	确定	取消

参数设置完成后,点击"确定"按钮,系统提示下载保存 IDS 联动密钥文件,如下 图所示。

IDS联动	
IDS联动密钥文件,	点击下载[或用右键另存]

点击"点击下载"链接,将 IDS 联动密钥文件"TOS[1].IDS[192.168.3.3]"保存到本 地即可。

5) 配置 IDS 设备的防火墙联动功能。

通过串口登录 IDS 设备,配置管理口的地址为 192.168.3.3,在 PC3 上安装 IDS 管理 软件,通过管理软件添加引擎,导入 IDS 联动密钥文件,编辑策略。具体请参见相关 IDS 产品的用户手册。

## 注意事项

通过命令行配置 IDS 设备地址后,仍需要回到 WebUI 界面中下载 IDS 联动密钥文件。

# 双机热备

网络卫士防火墙可以实现多种方式下的冗余备份,包括:双机热备模式、负载均衡模 式和连接保护模式。

在双机热备模式下(最多支持八台设备),任何时刻都只有一台防火墙(主墙)处于 工作状态,承担报文转发任务,一组防火墙处于备份状态并随时接替任务。当主墙的任何 一个接口(不包括心跳口)出现故障时,处于备份状态的防火墙经过协商后,由优先级高 的防火墙接替主墙的工作,进行数据转发。

在负载均衡模式下(最多支持八台设备),两台/多台防火墙并行工作,都处于正常的数据转发状态。每台防火墙中设置多个 VRRP 备份组,两台/多台防火墙中 VRID 相同的组之间可以相互备份,以便确保某台设备故障时,其他的设备能够接替其工作。

在连接保护模式下(最多支持八台设备),防火墙之间只同步连接信息,并不同步状态信息。当两台/多台防火墙均正常工作时,由上下游的设备决定流量由哪台防火墙转发, 所有防火墙处于负载分担状态,当其中一台发生故障时,上下游设备会将其上的数据流通 过其他防火墙转发。

# 双机热备模式

基本需求



图 35 双机热备模式的网络拓扑图

上图是一个简单的双机热备的主备模式拓扑图,主墙和一台从墙并联工作,两个防火墙的 Eth2 接口为心跳口,由心跳线连接用来协商状态,同步对象及配置信息。

## 配置要点

▶ 设置心跳口

- ▶ 设置备份接口
- ▶ 配置 HA 功能
- ▶ 启用 HA 功能
- ▶ 主从防火墙的配置同步

## WEBUI 配置步骤

1) 配置心跳口。

HA 心跳口必须工作在路由模式下,而且要配置同一网段的 IP 以保证相互通信。接口属性必须要选中"非同步地址",否则 HA 心跳口的 IP 地址信息会在主从墙运行配置同步时被对方覆盖。

▶ 主墙

a)点击 网络管理 > 接口,然后选择"物理接口"页签,在 eth2 接口条目右侧点击 "设置"图标,配置该接口为进行同步 HA 设置的 IP 地址,如下图所示。

物理接口 子接口							
	接口设置						
名称 描述 状态 模式	eth2 (00:13:32:02: □ 停用 ⓒ 路由 ○ 交換	23:F6 )					
地址	掩码	非同步地址	添加				
地址	掩码	属性	删除				
10.1.1.1	255, 255, 255, 0	HA	ā				
▶ 高级							
确定取消							

b)参数设置完成后,点击"确定"按钮即可。

▶ 从墙

配置从墙的 eth2 口 IP 地址为"10.1.1.2/24",具体操作请参见主墙的配置。

#### 2) 配置备份接口。

因为需求中要求两台防火墙的 eth1 口互相备份,两条防火墙的 eth3 口互相备份,所 以两台防火墙的 eth1 口需要设定相同的 IP 地址和 VRID;两台防火墙的 eth3 口也需要设 定相同的 IP 地址和 VRID。 ▶ 主墙

a) 点击 网络管理 > 接口, 然后选择"物理接口"页签, 点击 eth1 接口条目右侧的 "设置"图标, 配置 eth1 接口 IP 地址为 172.16.0.2/24, 如下图所示。

物理接口	子接口				
			接口设置		
	名称 描述 状态 模式 地址	eth1	. (00:13:32:02:23:F5 停用 路由 C 交換 掩码	; ) 非同步地址	添加
	172 16 0 2		790年9月 2月月 2月月 2月月 0	席庄	mies C
	112.10.0.2		233.233.233.0		Q
	▶ 高级				
		Ť	魚定 取消		

参数设置完成后,点击"确定"按钮即可。

b) 点击 eth3 接口条目右侧的"设置"图标,配置 eth3 接口 IP 地址为 172.16.1.3/24, 如下图所示。

物理接口	子接口				
			接口设置		
	名称 描述 状态 模式 地址	eth3	○ (00:13:32:02:23:F7 停用 路由 C 交换 掩码	") 非同步地址	
	地址			□	添加
	172.16.1.3	_	255, 255, 255, 0		3
	▶高级				
		Ð	龍 取れ	۱ ۱	

参数设置完成后,点击"确定"按钮即可。

▶ 从墙

从墙的配置与主墙完全一致,具体操作请参见主墙的配置。

## 说明

▶ 主墙

a) 点击 高可用性 > 高可用性, 然后在 "HA 模式" 右侧的下拉框中选择 "双机热备"。

b) 配置心跳口地址。

设置"本地"为心跳口 eth2 的 IP 地址(10.1.1.1)。

设置"对端"为另一台墙心跳口 eth2 的 IP 地址(10.1.1.2),超过两台设备时,必须将"对端"设为本地地址所在子网的子网广播地址(最多支持八台设备)。

c) 配置 VRID 组及其身份。

设置主墙的"组1"为"VRID1",其身份为主墙。

开启主墙的"抢占"模式,即主墙能在失效后,重新恢复正常工作时,重获主墙地位。 "抢占"模式,是指主墙宕机后,重新恢复正常工作时,是否重新夺回主墙的地位。只有 当主墙与从墙相比有明显的性能差异时,才需要配置主墙工作在"抢占"模式,否则当主 墙恢复工作时主从墙的再次切换浪费系统资源,没有必要。

d) 配置该 VRID 组包含的接口。

在"监控接口"右侧的下拉框中选择"eth1",然后点击"添加"按钮。

在"监控接口"右侧的下拉框中选择"eth3",然后点击"添加"按钮。

e) 主墙的 HA 参数设置完成后, 点击"应用"按钮保存配置, 界面如下图所示。

<sup>◆</sup> 互为备份的接口必须配置相同的 IP 地址,所以主墙的 Eth1 口必须与从墙 Eth1 口的 IP 地址相同,主墙的 Eth0 口必须与从墙 Eth0 口的 IP 地址相同。

<sup>3)</sup> 配置 HA 功能。

高可用性				
	高	可用性酶	置	
HA 模式	双机热备	•		
心跳地址	本地 10.1.1 对端 10.1.1	1.1 1.2	*	
热备组	热备组 身份	÷	抢占	工作状态
	1 * 主	•	开启 💌	未运行
监控接口	eth0 ▼ 接口名称	増加 接口监控	] 空 HA权	重
	eth1		0	
	eth3		0	
启用	停止		应用	
		同步操作	ŧ	
对如	<b>耑机同步到本机</b>		本机同	司步到对端机

▶ 从墙

a) 点击 高可用性 > 高可用性, 然后在 "HA 模式" 右侧的下拉框中选择 "双机热备"。

b) 配置心跳口地址。

设置"本地"为心跳口 eth2 的 IP 地址(10.1.1.2)。

设置"对端"为另一台墙心跳口 eth2 的 IP 地址(10.1.1.1)。

c) 配置 VRID 组及其身份。

设置从墙的"组1"为"VRID1",其身份为从墙。

d) 配置该 VRID 组包含的接口。

在"监控接口"右侧的下拉框中选择"eth1",然后点击"添加"按钮。

在"监控接口"右侧的下拉框中选择"eth3",然后点击"添加"按钮。

e)从墙的 HA 参数设置完成后,点击"应用"按钮保存配置,界面如下图所示。

高可用性						
	高	可用性配置				
HA 模式	双机热备	•				
心跳地址:	本地 10.1.1 对端 10.1.1	1.2	*			
热备组	热备组 身份	资 抢占	工作状态			
	1 * 从 🗨 关闭 🗨 未运行					
监控接口	eth0 💌	增加				
	接口名称	接口监控	HA权重			
	eth1	<b>V</b>	0			
	eth3		0			
启用	停止	应用	₿			
		同步操作				
对首	扁机同步到本机		本机同步到对端机			

4) 启用 HA 功能。

在主墙和从墙的"高可用性"界面中,分别点击"启用"按钮后,启动该双机热备模 式,心跳口建立连接,界面如下所示:

▶ 主墙

高可用性							
	高可用性配置						
HA模式	双机热备	Y					
心跳地址	本地 10.1.1 对端 10.1.1	l. 1 l. 2	*				
热备组	热备组 身份 1 * 主	<ul> <li>治占</li> <li>▼     <li></li></li></ul>	工作状态       I       I				
监控接口	eth0 🔻	增加					
	接口名称	接口监控	HA权重				
	eth1		0				
	eth3		0				
启用	停止	应用					
		同步操作					
34	端机同步到木机		木柑同步到对端柑				
	መወከካሪፖታህቶላቢ		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~				

▶ 从墙

高可用性			
	Ē	可用性配置	
HA 模	式 双机热备	V	
心跳封	地址 本地 10.1.1 对端 10.1.1	.2 *	
热备组	E 热备组 身( 1 * 从	分 抢占	<ul><li>工作状态</li><li>▲份</li></ul>
监控排	爰口 eth0 ▼	增加	
	接口名称	接口监控	HA权重
	eth1		0
	eth3		0
唐	·用 停止	应用	
		同步操作	
	对端机同步到本机	4	\$机同步到对端机

5) 主从防火墙的配置同步。

在主墙点击"本机同步到对端机"按钮,将主墙的当前配置同步到从墙。

至此,主墙和从墙的双机热备就可以正常使用了。

## 注意事项

1) 双机热备模式下,主、从防火墙管理口的地址需要配置为静态 IP,否则,启用双 机热备功能后,处于备份状态的防火墙中除心跳口之外的其它所有接口均处于 down 状态, 管理员将无法通过管理口对该防火墙进行任何操作。

2) 当主墙或从墙配置发生变更后,手工同步配置可以保证主从墙配置的一致性。

3) TOS3.3 版本中防火墙的接口均为自适应接口, HA 接口之间的连接可以使用交叉 线也可以使用直连线。

路由接口下的负载均衡模式

基本需求



图 36 路由接口下负载均衡模式的网络拓扑图

上图是一个简单的利用物理接口进行负载均衡的拓扑图,防火墙1和防火墙2并联工作,两个防火墙的 Eth3 接口间由一条心跳线相连用来同步状态及配置信息;两个防火墙的 Eth1 口属于同一 vrid1(防火墙1的优先级高于防火墙2);接口 Eth2 属于同一 vrid2(防火墙2 的优先级高于防火墙1)。

两台防火墙均正常工作时,网段1通过防火墙1利用电信链路上网,网段2通过防火墙2利用网通链路上网。当其中一条链路发生故障时,其上的数据流会自动切换,通过另一台防火墙转发,从而实现两台防火墙的负载均衡。

配置要点

- ▶ 配置 eth0 □
- ▶ 配置备份接口
- ▶ 配置心跳口
- ▶ 配置 HA 功能
- ▶ 启用 HA 功能

## WEBUI 配置步骤

- 1) 配置 eth0 口。
- ▶ 防火墙1

a) 点击 网络管理 > 接口, 然后选择"物理接口"页签, 点击接口 eth0 条目后的"设置"图标, 设定其 IP 地址为"192.168.83.237/24", 如下图所示。

物理接口 子接口				
		接口设置		
名称 描述 状态 模式 地址	eth0 □ 作 ④ 段 身	(00:13:32:02: 亨用 路由 〇 交換 掩码	23:F4 )  非同步地址	
地址		掩码	□ □ 属性	が加めた
192.168	), 83, 237	255, 255, 255, 0		3
▶ 高级				
	确	定 (	取消	

b)参数设置完成后,点击"确定"按钮保存配置。

▶ 防火墙 2

配置防火墙 2 的 IP 地址为 "202.1.1.2/24",具体步骤请参见防火墙 1 的配置。

2) 配置备份接口。

因为需求中要求两台防火墙的 eth1 口互相备份,两条防火墙的 eth2 口互相备份,所 以两台防火墙的 eth1 口需要设定相同的 IP 地址和 VRID;两台防火墙的 eth2 口也需要设 定相同的 IP 地址和 VRID。 ▶ 防火墙1

a) 点击 网络管理 > 接口, 然后选择"物理接口"页签, 点击 eth1 接口条目右侧的 "设置"图标, 配置 eth1 接口 IP 地址为 172.16.0.2/24, 如下图所示。

物理接口 子接口			
	接口设置		
名称 描述 状态 模式 地址	eth1 (00:13:32:02:23:F internet □ 停用 ④ 路由 □ 交换 掩码	25) 非同步地址	
地址	掩码	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	添加 删除
172. 16. 0. 2	255, 255, 255, 0		3
▶ 高级			
	确定 取	消 )	

参数设置完成后,点击"确定"按钮即可。

b) 点击 eth2 接口条目右侧的"设置"图标,配置 eth2 接口 IP 地址为 172.16.1.3/24, 如下图所示。

物理接口	子接口				
			接口设置		
	名称 描述 状态 模式 地址	eth2( 「 停戶 で路 睡 掩玩	00:13:32:02:23:F ] ] ] ] ]	6) 非同步地址	添加
	地址	11世	冯	唐性	删除
	172.16.1.3	25	5, 255, 255, 0		3
	▶ 高级				
		确定		消	

参数设置完成后,点击"确定"按钮即可。

▶ 防火墙 2

防火墙2的配置与防火墙1完全一致,具体操作请参见防火墙1。

3) 配置心跳口。

连接心跳线的 HA 通信接口必须工作在路由模式下,设定心跳口 IP 为同一个网段的不同 IP (分别为 10.0.0.1/24 和 10.0.0.2/24),并且必须要选中"非同步地址"。

▶ 防火墙1

a)点击 网络管理 > 接口,然后选择"物理接口"页签,在 eth3 接口条目右侧点击 "设置"图标,配置该接口为进行同步 HA 设置的 IP 地址,如下图所示。

物理接口 子	接口			
		接口设置		
名和描述	弥 eth3 龙	3 ( 00:13:32:02:23:F7	)	
状。	Š □	停用		
模	đ O	路由 🖸 交換		
地		<b>掩</b> 码	非同步地址 □	添加
地	8址	掩码	属性	删除
10	), 0, 0, 1	255, 255, 255, 0	HA	3
	高级			
	a to	确定	h	

b)参数设置完成后,点击"确定"按钮即可。

▶ 防火墙 2

配置防火墙 2 的 eth3 口 IP 地址为 "10.0.0.2/24",具体操作请参见防火墙 1 的配置。

4) 配置 HA 功能。

▶ 防火墙1

a) 点击 **高可用性 > 高可用性**, 然后在"HA 模式"右侧的下拉框中选择"负载均衡"。

b) 配置心跳口地址。

设置"本地"为心跳口 eth3 的 IP 地址(10.0.0.1)。

设置"对端"为另一台墙心跳口 eth3 的 IP 地址(10.0.0.2),超过两台设备时,必须将"对端"设为本地地址所在子网的子网广播地址(最多支持八台设备)。

c) 配置不同 VRID 组的优先级。

设置防火墙 1 的"组 1"为"VRID1",其优先级为 200,设置防火墙 1 的"组 2" 为"VRID2",其优先级为 100。因为防火墙 2 的 VRID 1 的优先级为 100,VRID 2 的优 先级为 200,所以,对于 VRID 1 来说防火墙 1 为主墙,防火墙 2 为备墙;对于 VRID 2 来说防火墙 2 为主墙,防火墙 1 为备墙。

开启主墙的"抢占"模式,即主墙能在失效后,重新恢复正常工作时,重获主墙地位。 "抢占"模式,是指主墙宕机后,重新恢复正常工作时,是否重新夺回主墙的地位。只有 当主墙与从墙相比有明显的性能差异时,才需要配置主墙工作在"抢占"模式,否则当主 墙恢复工作时主从墙的再次切换浪费系统资源,没有必要。

d) 配置每个 VRID 组包含的接口。

在"监控接口"右侧的下拉框中选择"eth1",然后点击"添加"按钮,最后选中"组 1"列的复选框。

在"监控接口"右侧的下拉框中选择"eth2",然后点击"添加"按钮,最后选中"组 2"列的复选框。

可用性 🦳							
	高可用性配置						
	HA 模式	负载	均衡	•			
	心跳地址;	本地 10.0.0.		). 1 ·		*	
	:	对端	10.0.0	). 2		*	
	热备组	组ID		优先级 抢		抢占	工作状态
		组1	1 *	200	*	开启 🖣	- 未运行
		组2	2 *	100	*	关闭 🖣	- 未运行
	监控接口	eth0 接口 eth	) <b>▼</b> 1名称 1	増加 組1 ☑	組	[2 HA表 ] 0	风重
		eth	3				
		eth	2				
	启用		停止			应用	
				同步措	鮓		
	对南	<b>耑机</b> 厅	司步到本机			本机同	司步到对端机

e)防火墙1的HA参数设置完成后,点击"应用"按钮保存配置,界面如下图所示。

▶ 防火墙 2

a) 点击 高可用性 > 高可用性, 然后在"HA 模式"右侧的下拉框中选择"负载均衡"。

b) 配置心跳口地址。

设置"本地"为心跳口 eth3 的 IP 地址(10.0.0.2)。

设置"对端"为另一台墙心跳口 eth3 的 IP 地址(10.0.0.1),超过两台设备时,必须将"对端"设为本地地址所在子网的子网广播地址(最多支持八台设备)。

c) 配置不同 VRID 组的优先级。

设置防火墙 2 的"组 1"为"VRID1",其优先级为 100,设置防火墙 2 的"组 2" 为"VRID2",其优先级为 200。因为防火墙 1 的 VRID 1 的优先级为 200,VRID 2 的优 先级为 100,所以,对于 VRID 1 来说防火墙 1 为主墙,防火墙 2 为备墙;对于 VRID 2 来说防火墙 2 为主墙,防火墙 1 为备墙。

开启主墙的"抢占"模式,即主墙能在失效后,重新恢复正常工作时,重获主墙地位。 "抢占"模式,是指主墙宕机后,重新恢复正常工作时,是否重新夺回主墙的地位。只有 当主墙与从墙相比有明显的性能差异时,才需要配置主墙工作在"抢占"模式,否则当主 墙恢复工作时主从墙的再次切换浪费系统资源,没有必要。

d) 配置每个 VRID 组包含的接口。

在"监控接口"右侧的下拉框中选择"eth1",然后点击"添加"按钮,最后选中"组 1"列的复选框。

在"监控接口"右侧的下拉框中选择"eth2",然后点击"添加"按钮,最后选中"组 2"列的复选框。

e)防火墙 2的 HA 参数设置完成后,点击"应用"按钮保存配置,界面如下图所示。

高可用性								
	高可用性配置							
на 模式	负载	匀衡	•					
心跳地址	本地	10.0.0	). 2		*			
	对端 10.0.0.1				*			
热备组		组ID	优先组	J I	抢占	工作状态		
	组1	1 *	100	*	关闭 🔽	未运行		
	组2	2 *	200	*	开启 💌	未运行		
监控接口	ethO	•	増加					
	接口名称 eth1		组1	组2 HA权量				
					0			
	eth2			✓	0			
启用		停止		应	用			
			BUCH	9.44-				
			回275	RTF.				
<b>X</b>	端机同	步到本机			本机同步到	的对端机		

5) 启用 HA 功能。

在防火墙1和防火墙2的"高可用性"界面中,分别点击"启用"按钮后,启动该负载均衡模式,心跳口建立连接,界面如下所示:

▶ 防火墙1
高可用性						
		高	可用性	配置		
HA 模式	负载	沟衡	V			
心跳地址	本地	10.0.0	). 1		*	
	对端	10.0.0	). 2		*	
热备组		组ID	优先级	〔 抢	占	工作状态
	组1	1 *	200	* 月	f启 👤	工作
	组2	2 *	100	* 🗎	闭 👤	备份
监控接口	ethO	•	増加			
	接□	名称	组1	组2	HA权重	i i
	ethi		•		0	
	eth2	2			0	
启用		停止		应用	日	
			同步操	作		
741	<b>湍</b> 机同	]步到本机			本机同步	到对端机

▶ 防火墙 2

高可用性						
		南	可用性	配置		
HA 模式	负载均	的衡	Y			
心跳地址	本地	10.0.0	.2	*		
	对端	10.0.0	. 1	*		
热备组		组ID	优先级	፬ 抢⊓	5	工作状态
	组1	1 *	100	* 关	闭 🔽	备份
	组2	2 *	200	* 开	启 👤	工作
监控接口	eth0		增加			
	接口:	名称	组1	组2	HA权重	
	eth1		•		0	
	eth2				0	
启用		停止		应用		
			同步撰	作		
সা	端机同	步到本机		격	的同步到	到对端机

Trunk 口下的负载均衡模式

## 基本需求



图 37 Trunk 口下负载均衡模式的网络拓扑图

上图是一个简单的利用 Trunk 接口进行负载均衡的拓扑图,防火墙 1 和防火墙 2 并联 工作,两个防火墙的 Eth2 接口间由一条心跳线相连用来同步状态及配置信息,两个防火 墙的 Eth1 口为 trunk 口,同时属于 vlan1 和 vlan2, vlan1 属于同一 vrid1(防火墙 1 的优先 级高于防火墙 2)、vlan2 属于同一 vrid2(防火墙 2 的优先级高于防火墙 1),这样两台 防火墙均正常工作时,网段 1 通过防火墙 1 利用电信链路上网,网段 2 通过防火墙 2 利用 网通链路上网。当其中一条链路发生故障时,其上的数据流会自动切换,通过另一台防火 墙转发,从而实现两台防火墙的负载均衡。

#### 配置要点

- ▶ 配置 Eth0 口
- ▶ 配置备份接口
- ▶ 配置心跳口
- ▶ 配置 HA 功能
- ▶ 启用 HA 功能

## WEBUI 配置步骤

- 1) 配置 Eth0 口。
- ▶ 防火墙1

a) 点击 网络管理 > 接口, 然后选择"物理接口"页签, 点击接口 eth0 条目右侧的 "设置"图标, 设定其 IP 地址为"192.168.83.237/24", 如下图所示。

物理接口	子接口				
			接口设置		
	名称 描述 状态 模式 地址	eth0	(00:13:32:02:23:F4 停用 路由 <sup>O</sup> 交換 掩码	) 非同步地址 □	添加
	地址		掩码	属性	删除
	192. 168. 83. 237		255, 255, 255, 0		a
	▶高级				
		碓		ŧ )	

b)参数设置完成后,点击"确定"按钮保存配置。

▶ 防火墙 2

配置防火墙 2 的通信用 IP 地址为 "202.1.1.2/24",具体步骤请参见防火墙 1 的配置。

2) 配置备份接口。

配置两台防火墙的 Eth1 口为 Trunk 口,属于 VLAN1 和 VLAN2;两台墙的 VLAN1 虚接口互相备份,VLAN2 虚接口也互相备份,因此在两台墙上必须将互为备份的 VLAN 虚接口设置为相同的 IP 地址。

▶ 防火墙1和防火墙2

a)选择 网络管理 > 接口,然后选择"物理接口"页签,点击 eth1 接口条目右侧的 "设置"图标,配置接口信息,如下图所示。

物理接口 子接口		
	接口设置	
名和 描述 状況 模式 で知	な eth1 (00:13:32:02:23 性 internet 医 □ 停用 た □ 路由 ● 交換 論模式	:F5)
i类 LIV 能性	型 Caccess Otrunk W范围 1-2 炭类型 O 802.1Q C ISL	[1-4094,多个范围中间用逗号分隔]
	 确定	取消

参数设置完成后,点击"确定"即可。

b) 点击 网络管理 > 二层网络,并选择"VLAN"页签,点击"添加 VLAN"链接 添加 VLAN,设置 VLAN 虚接口的属性,如下图所示。

ARP	LAN MAC CDP
	添加配置
	添加单个VLAN 〇 [1-4094] 添加VLAN范围 ④ 1 - 2 [总数最多是1024个]
	确定取消

参数设置完成后,点击"确定"按钮即可。

c) 点击 网络管理 > 二层网络, 然后选择"VLAN"页签, 点击 vlan.0001 后的修改 图标" <sup>[]</sup> →", 设置 VLAN 虚接口 vlan.0001 的 IP 地址为 172.16.0.2/24, 如下图所示。

ARP VLAN MAC CDP									
			VLAN设置						
名; 描; 状; 接 地	称   ▼ 述     [ 态	'lan	0001 停用 掩码	非同步地址					
H	也 址		掩码	□	添加删除				
1	72.16.0.2		255. 255. 255. 0		3				
•	高级								
		ł	确定 取消	۱ ۱					

参数设置完成后,点击"确定"按钮即可。

d)点击 网络管理 > 二层网络,然后选择"VLAN"页签,点击 vlan.0002 后的修改
 图标" <sup>↓</sup> ",设置 VLAN 虚接口 vlan.0002 的 IP 地址为 172.16.1.3/24,如下图所示。

ARP VLAN MA	AC CDP									
TLAT设置										
名称 描述 状态 接口地址 地址	vlan.0002 □ 停用 堆码	非同步地址								
	1474-0		添加							
地址	掩码	属性	删除							
172, 16, 1, 3	255, 255, 255, 0		ā							
▶高级										
	确定	取消								

参数设置完成后,点击"确定"按钮即可。

3) 配置心跳口。

连接心跳线的 HA 通信接口必须工作在路由模式下,设定心跳口 IP 为同一个网段的不同 IP (分别为 10.0.0.1/24 和 10.0.0.2/24),并且必须选中"非同步地址"。

▶ 防火墙1

a)点击 网络管理 > 接口,然后选择"物理接口"页签,在 eth2 接口条目右侧点击 "设置"图标,为该接口配置进行同步 HA 设置的地址,如下图所示。

物理接口	子接口				
			接口设置		
	名称 e 描述 [ 状态   模式 -	th2(( □ 停用 ● 路由 播码	0:13:32:02:23:F(      〇 交換	3 ) 非同步地址	
		145 +-			添加
	地址	掩幕	3	属性	删除
	10.0.0.1	255	. 255. 255. 0	НА	ð
	▶高级				
		确定		消	

b)参数设置完成后,点击"确定"按钮即可。

▶ 防火墙 2

配置防火墙 2 的 eth2 口 IP 地址为 "10.0.0.2/24", 具体操作请参见防火墙 1。

4) 配置 HA 功能。

▶ 防火墙1

a) 点击 高可用性 > 高可用性, 然后在 "HA 模式" 右侧的下拉框中选择 "负载均衡"。

b) 配置心跳口地址。

设置"本地"为心跳口 eth2 的 IP 地址(10.0.0.1)。

设置"对端"为另一台墙心跳口 eth2 的 IP 地址(10.0.0.2),超过两台设备时,必须将"对端"设为本地地址所在子网的子网广播地址(最多支持八台设备)。

c) 配置不同 VRID 组的优先级。

设置防火墙 1 的"组 1"为"VRID1",其优先级为 200,设置防火墙 1 的"组 2" 为"VRID2",其优先级为 100。因为防火墙 2 的 VRID 1 的优先级为 100,VRID 2 的优 先级为 200,所以,对于 VRID 1 来说防火墙 1 为主墙,防火墙 2 为备墙;对于 VRID 2 来说防火墙 2 为主墙,防火墙 1 为备墙。 开启主墙的"抢占"模式,即主墙能在失效后,重新恢复正常工作时,重获主墙地位。 "抢占"模式,是指主墙宕机后,重新恢复正常工作时,是否重新夺回主墙的地位。只有 当主墙与从墙相比有明显的性能差异时,才需要配置主墙工作在"抢占"模式,否则当主 墙恢复工作时主从墙的再次切换浪费系统资源,没有必要。

d) 配置每个 VRID 组包含的接口。

在"监控接口"右侧的下拉框中选择"vlan.0001",然后点击"添加"按钮,最后选 中"组1"列的复选框。

在"监控接口"右侧的下拉框中选择"vlan.0002",然后点击"添加"按钮,最后选 中"组 2"列的复选框。

e)防火墙1的HA参数设置完成后,点击"应用"按钮保存配置,界面如下图所示。

高可用性						
		高	可用性	配置		
HA 模式	负载均	匀衡	•			
心跳地址	本地	10.0.0.	1	*		
	对端	10.0.0.	2	*		
热备组		组ID	优先级	〔 抢	占	工作状态
	组1	1 *	200	* 月	F启 🔽	未运行
	组2	2 *	100	* 🗵	闭 🔽	未运行
监控接口	eth0	•	增	ba		
	接口	名称	组1	组2	HA权重	t
	vlan	. 0001			0	
	vlan	. 0002			0	
启用		停止		应用		
			同步提	<b>#</b>		
			PU 27 15	CIF.		
X	端机同	步到本机		Z	\$.机同步到	对端机

▶ 防火墙 2

a) 点击 **高可用性 > 高可用性**, 然后在"HA 模式"右侧的下拉框中选择"负载均 衡"。

b) 配置心跳口地址。

设置"本地"为心跳口 eth2 的 IP 地址(10.0.0.2)。

设置"对端"为另一台墙心跳口 eth2 的 IP 地址(10.0.0.1),超过两台设备时,必须将"对端"设为本地地址所在子网的子网广播地址(最多支持八台设备)。

c) 配置不同 VRID 组的优先级。

设置防火墙 2 的"组 1"为"VRID1",其优先级为 100,设置防火墙 2 的"组 2" 为"VRID2",其优先级为 200。因为防火墙 1 的 VRID 1 的优先级为 200,VRID 2 的优 先级为 100,所以,对于 VRID 1 来说防火墙 1 为主墙,防火墙 2 为备墙;对于 VRID 2 来说防火墙 2 为主墙,防火墙 1 为备墙。

开启主墙的"抢占"模式,即主墙能在失效后,重新恢复正常工作时,重获主墙地位。 "抢占"模式,是指主墙宕机后,重新恢复正常工作时,是否重新夺回主墙的地位。只有 当主墙与从墙相比有明显的性能差异时,才需要配置主墙工作在"抢占"模式,否则当主 墙恢复工作时主从墙的再次切换浪费系统资源,没有必要。

d) 配置每个 VRID 组包含的接口。

在"监控接口"右侧的下拉框中选择"vlan.0001",然后点击"添加"按钮,最后选 中"组1"列的复选框。

在"监控接口"右侧的下拉框中选择"vlan.0002",然后点击"添加"按钮,最后选 中"组 2"列的复选框。

e)防火墙 2的 HA 参数设置完成后,点击"应用"按钮保存配置,界面如下图所示。

高可用性						
		高	可用性	配置		
HA 模式	负载;	均衡	<b>•</b>			
心跳地址	本地	10.0.0	. 2	:	*	
	对端	10.0.0	. 1		*	
热备组		组ID	优先级	t 抢r	5	工作状态
	组1	1 *	100	*   关	闭 🔻	未运行
	组2	2 *	200	*   开	启 💌	未运行
监控接口	eth0	) 🔽	增	幼	]	
	接□	1名称	组1	组2	HA权量	Ē
	vla	n. 0001			0	
	vla	n. 0002			0	
启用		停止		应用	]	
			同步操	作		
সা	端机同	司步到本机			本机同步	到对端机

5) 启用 HA 功能。

在防火墙1和防火墙2的"高可用性"界面中,分别点击"启用"按钮后,启动该负载均衡模式,心跳口建立连接,界面如下所示:

▶ 防火墙1

高可用性						
		直	可用性	配置		
HA 模式	负载	均衡	V			
心跳地地	止本地	10.0.0.	1		*	
	对端	10.0.0.	2		*	
热备组		组ID	优先级	\$ ł	论占	工作状态
	组1	1 *	200	* [	开启 💌	工作
	组2	2 *	100	* [	关闭 👤	备份
监控接口	l eth0	•	增	ba 🛛		
	接口	名称	组1	组2	HA权重	t
	vlan	0001			0	
	vlan	. 0002			0	
启用	]	停止		应用	Ð	
			同步操	作		
X	讨端机同	步到本机			本机同步到	对端机

▶ 防火墙 2

高可用性						
		高	可用性育	置5		
HA 模式 [	负载均	勾衡	~			
心跳地址	本地	10.0.0	. 2	*	:	
	对端	10.0.0	. 1	*		
热备组	热备组 组ID 优先级				ī	工作状态
	组1	1 *	100 *	• [关]	闭 🔽	备份
	组2	2 *	200 *	• (开)		工作
监控接口	ethO	<b>_</b>	增	ha		
	接口	名称	组1	组2	HA权重	Ē
	vlan	0001			0	
	vlan	0002			0	
启用		停止		应用		
			同步操作	ŧ		
7dø	端机同	步到本机		7	本机同步	到对端机

# 连接保护模式

基本需求



图 38 连接保护模式拓扑图

上图是一个简单的连接保护模式拓扑图,四台防火墙并行工作,防火墙的 Eth2 口为 心跳口(IP 地址分别为"10.1.1.1/24"、"10.1.1.2/24"、"10.1.1.3/24"和"10.1.1.4/24"), 通过 HUB(或交换机)相连用来协商状态及同步对象和配置。

当两台/多台防火墙均正常工作时,由上下游的设备决定流量由哪台防火墙转发,所 有防火墙处于负载分担状态,当其中一台发生故障时,上下游设备会将其上的数据流通过 其他防火墙转发。

#### 配置要点

- ▶ 配置防火墙心跳口
- ▶ 配置防火墙中除心跳口以外的接口
- ▶ 配置 HA 功能
- ▶ 启用 HA 功能
- ▶ 设置关闭连接表的严格状态检测功能

### WEBUI 配置步骤

1) 配置防火墙心跳口。

▶ 防火墙1

HA 心跳口必须工作在路由模式下,而且要配置同一网段的 IP 以保证相互通信。接口属性必须要选中"非同步地址"。

a) 点击 网络管理 > 接口, 然后选择"物理接口"页签, 点击 eth2 接口条目右侧的 "设置"图标, 配置接口信息, 如下图所示。

物理接口	子接口					
			ž	<b>赛口设置</b>		
	名称 描述 状态 模式 地址	ethi D	2 ( 00: 停用 路由 掩码	13:32:02:23: C 交换	F6) 非同步地址 □□	添加
	地址		掩码		属性	删除
	10.1.1.1		255.25	55.255.0	НА	a
	▶高级					
			确定		Q消	

参数设置完成后,点击"确定"按钮保存配置。

▶ 防火墙 2

设置防火墙 2 的心跳口 IP 地址为"10.1.1.2/24",其操作与防火墙 1 的设置方法相同, 具体请参加防火墙 1 的配置步骤。

▶ 防火墙 3

设置防火墙 3 的心跳口 IP 地址为"10.1.1.3/24",其操作与防火墙 1 的设置方法相同, 具体请参加防火墙 1 的配置步骤。

▶ 防火墙 4

设置防火墙 4 的心跳口 IP 地址为"10.1.1.4/24",其操作与防火墙 1 的设置方法相同, 具体请参加防火墙 1 的配置步骤。

2) 配置防火墙中除心跳口以外的接口。

▶ 防火墙1

a) 配置 Eth0 口 IP 为 192.168.83.237。

点击 网络管理 > 接口, 然后选择"物理接口"页签, 点击 eth0 接口条目右侧的"设置"图标, 配置接口信息, 如下图所示。

物理接口	子接口					
			接口	1设置		
- 	名称 描述 状态 檀式	eth0 intr	(00:13: anet 停用	32:02:23:F4	• )	
	地址		掩码		非同步地址 □	添加
	地址		掩码		属性	删除
	192. 168. 83. 237		255, 255	. 255. 0		3
	▶高级					1
		確	定	<b>取</b> i	肖 )	

参数设置完成后,点击"确定"按钮保存配置。

b) 配置 Eth1 口 IP 为 172.16.1.1。

点击 网络管理 > 接口, 然后选择"物理接口"页签, 点击 eth1 接口条目右侧的"设置"图标, 配置接口信息, 如下图所示。

物理接口	子接口			
		接口设置		
2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	名称 et 描述 状态 E 模式 G	h1 (00:13:32:02:23:F5   停用   路由 C 交換	5)	
]	地址	推坍	非问步地址 []	添加
	地址	掩码	属性	删除
	172. 16. 1. 1	255, 255, 255, 0		3
	▶高级			
		确定 取	消	

参数设置完成后,点击"确定"按钮保存配置。

- ▶ 防火墙 2
- a) 配置 Eth0 口 IP 为 192.168.83.238。
- b) 配置 Eth1 口 IP 为 172.16.1.2。

操作步骤与防火墙1完全一致,请参照防火墙1进行配置。

▶ 防火墙3

a) 配置 Eth0 口 IP 为 192.168.83.239。

b) 配置 Eth1 口 IP 为 172.16.1.3。

操作步骤与防火墙1完全一致,请参照防火墙1进行配置。

▶ 防火墙 4

a) 配置 Eth0 口 IP 为 192.168.83.240。

b) 配置 Eth1 口 IP 为 172.16.1.4。

操作步骤与防火墙1完全一致,请参照防火墙1进行配置。

3) 配置 HA 功能。

指定 HA 网口本地地址以及对端地址。

▶ 防火墙1

a) 点击 **高可用性 > 高可用性**, 然后在 "HA 模式" 右侧的下拉框中选择 "连接保 护"。

b) 配置心跳口地址。

设置"本地"为心跳口 eth2 的 IP 地址(10.1.1.1)。

设置"对端"为 eth2 口的子网广播地址(10.1.1.255),当只有两台防火墙并行工作

- 时,建议设置为单播地址。
  - c)防火墙1的HA参数设置完成后,点击"应用"按钮保存配置,界面如下图所示。

高可用性			
	高可	可用性配置	
	HA 模式 连接保护	Þ 🔽	
	心跳地址 本地 对端 启用	10.1.1.1 10.1.1.255 停止	* * 应用
	F	司步操作	
	对端机同步到本机		本机同步到对端机

▶ 防火墙 2

防火墙 2 的操作请参见防火墙 1 的配置,需要设置本机地址为 10.1.1.2,对端地址为 10.1.1.255。

▶ 防火墙 3

防火墙 3 的操作请参见防火墙 1 的配置,需要设置本机地址为 10.1.1.3,对端地址为 10.1.1.255。

▶ 防火墙 4

防火墙 4 的操作请参见防火墙 1 的配置,需要设置本机地址为 10.1.1.4,对端地址为 10.1.1.255。

4) 启用 HA 功能。

▶ 防火墙 1、防火墙 2、防火墙 3 和防火墙 4

点击"启用"按钮,启动该连接保护模式,心跳口连接建立。防火墙1中界面如下图 所示。

高可用性	
高	可用性配置
<b>HA 模式</b> 连接伤	ii 🔽
心跳地址 本地 对端	10. 1. 1. 1 * 10. 1. 1. 255 *
启用	<b>停止</b> 应用
	同步操作
对端机同步到本机	本机同步到对端机

5) 设置关闭连接表的严格状态检测功能。

▶ 防火墙1、防火墙2、防火墙3和防火墙4

a) 点击 **系统管理 > 配置**, 然后选择"系统参数"页签, 选中"高级属性", 在"网络参数"处设置关闭连接完整性检查功能, 如下图所示。

系统参数 开放服务	时间 SNMP	邮件设置 短信设置 WEB管理
		基本属性
	设备名称 ▼	TopsecOS * 高级属性
		网络参数
	已建立TCP连接超时 握手时TCP连接超时 关闭时TCP超时时间 UDP连接超时时间 其他类型连接超时 不超时最大百分比 SYD代理参数 连接类型配额	600       * [10-7200秒,缺省600秒]         20       * [10-200秒,缺省20秒]         3       * [3-800秒,缺省3秒]         60       * [10-7200秒,缺省60秒]         20       * [10-7200秒,缺省20秒]         20       * [10-7200秒,缺省20秒]         20       * [5-90,缺省20]         2000       配额 * [10-200000个/秒,缺省2000个/秒]         5000       限额 * [10-200000个/秒,缺省5000个/秒]         0       TCP * [占总连接的百分比上限]         0       WDP * [占总连接的百分比上限]         0       TCP * [占总连接的百分比上限]
	ICMP重定向 TCP reset 包校验和 连接完整性 快速连接重用 MPLS透传 CDP透传 智能选路 扩展IP协议支持	○     其他 ** [占息注接的自分比上限]       关     ▼       关     ▼       关     ▼       关     ▼       关     ▼       ズ     ▼       ズ     ▼       ズ     ▼       〔0-255, 多个1       值以空格分隔〕
		应用

b)参数设置完成后,点击"应用"按钮即可。

### 注意事项

如果用户网络拓扑中有可能存在这样的情况:建立连接请求发送的 SYN 包经过一台 防火墙,而返回的 SYN/ACK 包通过另一台防火墙转发,则必须要关闭严格状态检测开关。

当 SYN 包通过墙 A 时,墙 A 上建立了一条状态为 handshake 的连接,同步到 B 墙上时,为了避免重复同步连接, B 墙上连接状态为 ESTABLISHED 状态;此时如果 SYN/ACK

报文从 B 墙的路径返回,发现墙上已经有一条 ESTABLISHED 的连接,就会把 ACK 包丢弃,导致 client 和 server 端无法真正建立起连接来,通信失败。此时,如果把严格状态检测开关 off 的话,ACK 包到达 B 墙,虽然发现已经有一条 ESTABLISHED 的连接,但也会放过,报文回复到 client 端时,就可以握手成功了。

# 子接口的负载均衡模式

基本需求



图 39 子接口负载均衡模式的网络示意图

上图是一个简单的利用子接口进行负载均衡的示意图。防火墙 A 和防火墙 B 并联工作,两个防火墙的 Eth3 接口间由一条心跳线相连用来同步状态及配置信息;两个防火墙的子接口 veth1.01 和 veth2.01 属于 VRID10(防火墙 B 的优先级高于防火墙 A);两个防火墙的子接口 veth1.02 和 veth2.02 属于 VRID20(防火墙 A 的优先级高于防火墙 B)。这样,两台防火墙均正常工作时,网段"172.16.0.0/24"的流量通过防火墙 A 进行转发,网段"172.16.1.0/24"的流量通过防火墙 B 进行转发。当其中一条链路发生故障时,其上的数据流会自动切换,通过另一台防火墙转发,从而实现两台防火墙的负载均衡。

#### 配置要点

- ▶ 配置备份子接口
- ▶ 配置心跳口
- ▶ 配置 HA 功能
- ▶ 启用 HA 功能

### WEBUI 配置步骤

1) 配置备份子接口。

▶ 防火墙 A

a) 点击 网络管理 > 接口, 激活"子接口"页签, 然后点击"添加子接口", 添加 eth1 接口的子接口 veth1.01 和 veth1.02。

b) 点击 网络管理 > 接口, 激活"子接口"页签, 然后点击"添加子接口", 添加 eth2 接口的子接口 veth2.01 和 veth2.02。

c) 在子接口列表中,分别点击各个子接口条目右侧的修改图标" ↓ ",配置 veth1.01 的 IP 地址为 192.168.0.1;配置 veth1.02 的 IP 地址为 192.168.0.2;配置 veth2.01 的 IP 地址为 172.16.0.1;配置 veth2.02 的 IP 地址为 172.16.1.1,如下图所示。

物理接口 子接口								
╋ 添加子接口								
名称	描述	地址	MTU	状态	操作			
veth1.01		192, 168, 0, 1/255, 255, 255, 0	1500	启用	D 词			
veth1.02		192, 168, 0, 2/255, 255, 255, 0	1500	启用	D 词			
veth2.01		172, 16, 0, 1/255, 255, 255, 0	1500	启用	D 词			
veth2.02		172, 16, 1, 1/255, 255, 255, 0	1500	启用	D 🗟			

▷ 防火墙 B

配置防火墙 B 的备份子接口,与防火墙 A 的配置完全相同,此处不再赘述。

2) 配置心跳口。

连接心跳线的 HA 通信接口必须工作在路由模式下,设定心跳口 IP 为同一个网段的 不同 IP (分别为 10.0.0.1/24 和 10.0.0.2/24),并且必须选中"非同步地址"。

▶ 防火墙 A

a) 点击 网络管理 > 接口, 然后选择"物理接口"页签, 在 eth3 接口条目的右侧点击"设置"图标, 为该接口配置进行同步 HA 设置的地址, 如下图所示。

物理接口	子接口				
			接口设置		
	名称 描述 状态 模式 地址	ethi D O	3 (00:13:32:02:23:F7 停用 路由 <sup>C</sup> 交換 掩码	) 非同步地址	
					添加
	地址		掩码	属性	删除
	10.0.0.1		255. 255. 255. 0	НА	3
	▶ 高级				
		ł	确定 取消		

b)参数设置完成后,点击"确定"按钮即可。

➢ 防火墙 B

配置防火墙 B 的 eth0 口 IP 地址为"10.0.0.2/24",具体操作请参见防火墙 A。

3) 配置 HA 功能。

▶ 防火墙 A

a) 点击 **高可用性 > 高可用性**, 然后在"HA 模式"右侧的下拉框中选择"负载均衡"。

b) 配置心跳口地址。

设置"本地"为心跳口 eth3 的 IP 地址(10.0.0.1)。

设置"对端"为另一台墙心跳口 eth3 的 IP 地址(10.0.0.2),超过两台设备时,必须将"对端"设为本地地址所在子网的子网广播地址(最多支持八台设备)。

c) 配置不同 VRID 组的优先级。

设置防火墙 A 的"组 1"为"VRID10",其优先级为 100,设置防火墙 A 的"组 2" 为"VRID20",其优先级为 200。因为防火墙 B 的 VRID 10 的优先级为 200,VRID 20 的优先级为 100,所以,对于 VRID 10 来说防火墙 B 为主墙,防火墙 A 为备墙;对于 VRID 20 来说防火墙 A 为主墙,防火墙 B 为备墙。

开启主墙的"抢占"模式,即主墙能在失效后,重新恢复正常工作时,重获主墙地位。 "抢占"模式,是指主墙宕机后,重新恢复正常工作时,是否重新夺回主墙的地位。只有 当主墙与从墙相比有明显的性能差异时,才需要配置主墙工作在"抢占"模式,否则当主 墙恢复工作时主从墙的再次切换浪费系统资源,没有必要。 d) 配置每个 VRID 组包含的接口。

在"监控接口"右侧的下拉框中选择"veth1.01",然后点击"添加"按钮,最后选 中"组1"列的复选框。

在"监控接口"右侧的下拉框中选择"veth2.01",然后点击"添加"按钮,最后选 中"组1"列的复选框。

在"监控接口"右侧的下拉框中选择"veth1.02",然后点击"添加"按钮,最后选 中"组 2"列的复选框。

在"监控接口"右侧的下拉框中选择"veth2.02",然后点击"添加"按钮,最后选 中"组 2"列的复选框。

e) 防火墙 A 的 HA 参数设置完成后, 点击"应用"按钮保存配置, 界面如下图所示。

高可用性				
	高	可用性	记置	
HA 模式 [	负载均衡	•		
心跳地址;	本地 10.0.0	). 1 ). 2	*	
热备组	组ID	优先级	抢占	工作状态
	组1 10 *	100 *	▶ 关闭 💌	未运行
	组2 20 *	200 *	▶ 开启 💌	未运行
监控接口	eth0 💌	増加	1	
	接口名称	组1	组2 HA权道	Ē
	veth1.01			
	veth2.01			
	veth1.02			
	veth2.02			
	停止		应用	
		同步操作	乍	
对贫	扁机同步到本机		本机同步	步到对端机

▶ 防火墙 B

a) 点击 **高可用性 > 高可用性**, 然后在 "HA 模式" 右侧的下拉框中选择 "负载均衡"。

b)配置心跳口地址。

设置"本地"为心跳口 eth3 的 IP 地址(10.0.0.2)。

设置"对端"为另一台墙心跳口 eth3 的 IP 地址(10.0.0.1),超过两台设备时,必须将"对端"设为本地地址所在子网的子网广播地址(最多支持八台设备)。

c) 配置不同 VRID 组的优先级。

设置防火墙 B 的"组 1"为"VRID10",其优先级为 200,设置防火墙 B 的"组 2" 为"VRID20",其优先级为 100。因为防火墙 A 的 VRID 10 的优先级为 100,VRID 20 的优先级为 200,所以,对于 VRID 10 来说防火墙 B 为主墙,防火墙 A 为备墙;对于 VRID 20 来说防火墙 A 为主墙,防火墙 B 为备墙。

开启主墙的"抢占"模式,即主墙能在失效后,重新恢复正常工作时,重获主墙地位。 "抢占"模式,是指主墙宕机后,重新恢复正常工作时,是否重新夺回主墙的地位。只有 当主墙与从墙相比有明显的性能差异时,才需要配置主墙工作在"抢占"模式,否则当主 墙恢复工作时主从墙的再次切换浪费系统资源,没有必要。

d) 配置每个 VRID 组包含的接口。

在"监控接口"右侧的下拉框中选择"veth1.01",然后点击"添加"按钮,最后选 中"组1"列的复选框。

在"监控接口"右侧的下拉框中选择"veth2.01",然后点击"添加"按钮,最后选 中"组1"列的复选框。

在"监控接口"右侧的下拉框中选择"veth1.02",然后点击"添加"按钮,最后选 中"组 2"列的复选框。

在"监控接口"右侧的下拉框中选择"veth2.02",然后点击"添加"按钮,最后选 中"组 2"列的复选框。

e)防火墙 B的 HA 参数设置完成后,点击"应用"按钮保存配置,界面如下图所示。

高可用性								
	高可用性配置							
НА	HA 模式 负载均衡							
心渴	心跳地址 本地 10.0.0.2 *							
	対端	10.0.0	J. 1	,	*			
热省	予組	组ID	优先级	抢占	5	工作状态		
	组1	10 *	200 '	*  开.		未运行		
	组2	20 *	100	*   关	闭 👤	未运行		
监想	空接口 eth	) 🔻	增加	חנ				
	接口	口名称	组1	组2	HA权重	Ī		
	vet	h1.01			0			
	vet	h2.01			0			
	vet	h1.02			0			
	vet	h2.02		✓	0			
	启用	停止		应用	]			
			同步操作	作				
	对端机同	司步到本机			本机同步	到对端机		

4) 启用 HA 功能。

在防火墙 A 和防火墙 B 的"高可用性"界面中,分别点击"启用"按钮后,启动该 负载均衡模式,心跳口建立连接,界面如下所示:

▶ 防火墙 A

高可用性						
		高	可用性	配置		
HA 模式 [	负载却	匀衡	Y			
心跳地址:	本地	10.0.0	). 1		*	
	对端	10.0.0	). 2	*	*	
热备组		组ID	优先纲	反 抢,	Ь	工作状态
	组1	10 *	100	* 🕅	闭 🚽	备份
	组2	20 *	200	* 开	追 👤	工作
监控接口	eth0	•	增	加		
	接口	名称	组1	组2	HA权重	-
	veth	1.01			0	
	veth	2.01			0	
	veth	.1.02			0	
	veth	2.02			0	
启用		停止		应用		
			同步操	ette 🛛		
对南	<b>耑</b> 机同	步到本机			本机同步	到对端机

▶ 防火墙 B

高可用性							
			高	可用性	配置		
:	HA 模式 🛛	负载均	勾衡	V			
	心跳地址 ; フ	本地 对端	10. 0. 0 10. 0. 0	). 2 ). 1		*	
	热备组		组ID	优先级	§ ł	仓占	工作状态
	:	组1	10 *	200	* [	开启 💌	工作
	:	组2	20 *	100	*	关闭 🔽	备份
	监控接口	eth0	•	増	加		
		接口	名称	组1	组2	HA权重	t
	,	veth	.1.01	◄		0	
	,	veth	2.01	•		0	
		veth	.1.02			0	
		vetł	2.02		<b>V</b>	0	
	启用		停止		<u>/5</u>	Z用	
				同生地	1		
				PJ2/58	IF.		
	对韓	<b>制机</b> 同	]步到本机			本机同步	到对端机

# 链路备份

网络卫士防火墙能够提供链路备份功能,防火墙上设置主链路和从链路两条互为备份 的链路,主链路正常时系统利用主链路来连接系统内外的通信。当主链路异常或断路时, 能够动态地切换到从链路,同时继续探测主链路的工作状态,一旦探测到主链路恢复正常, 系统会自动切换回主链路,从而为用户提供高的外出链路稳定性。

防火墙设置一个链路外部信任的 IP 地址,通过主、从链路的网络接口定时向该主机 发送 ping 包来探测主、从链路通讯是否正常。

如果主从链路均工作异常并设定了报警规则,系统会根据规则进行报警。

#### 基本需求

某公司内网用户通过网络卫士防火墙和路由器连接外网,防火墙工作在路由模式。为 了确保与外网连接的畅通,在防火墙上启用链路备份功能,在 eth1 口和路由器的 eth1 口 连接作为主链路,在 eth2 口和路由器的 eth2 口连接作为备用链路,利用路由器的 eth0 口 用作探测链路状态的 IP,防火墙会主动向探测主机定时发送 ping 报文,用来检测主、从 链路通讯是否正常。可以利用 PC1 和 PC2 之间的 ping 连接来验证链路情况。



#### 配置要点

- ▶ 配置防火墙接口属性(所属区域和 IP 地址)。
- ▶ 配置地址转换策略。
- ▶ 配置报警规则。
- ▶ 配置主链路和从链路的 IP 探测对象。
- ▶ 配置静态路由。
- ▶ 配置链路备份参数,然后启动链路备份功能。
- ▶ 验证主、从链路切换过程。

## WEBUI 配置步骤

1) 配置防火墙接口属性(所属区域和 IP 地址)。

a) 点击 **资源管理 > 区域**, 然后点击"添加", 配置 eth0、eth1 和 eth2 口对应的区 域。

① 设置 eth0 对应的区域,如下图所示。

区域			
		区域	
	名称 访问权限 注释	area_eth0    * 允许	
可用属性: adsl [属性] adsl1 [属性] adsl2 [属性] adsl3 [属性] bond0 [属性]		成员: -> ×	
		确定 取消	

参数设置完成后,点击"确定"按钮即可。

② 设置 eth1 对应的区域,如下图所示。

区域			
		区域	i
	名称 访问权限 注释	area_eth1 允许	*
可用属性:			成员:
ads1 [属性] ads11 [属性] ads12 [属性] ads13 [属性] bond0 [属性]			eth1
		确定	取消

参数设置完成后,点击"确定"按钮即可。

③ 设置 eth2 对应的区域,如下图所示。

区域			
		区域	i
	名称	area_eth2	*
	访问权限	允许	-
	注释		
可用属性:			成员:
adsl [属性] adsl1 [属性] adsl2 [属性] adsl3 [属性] bond0 [属性]			eth2
		确定	取消

参数设置完成后,点击"确定"按钮即可。

b) 点击 网络管理 > 接口, 然后选择"物理接口"页签, 点击各接口右侧的"设置" 图标配置其 IP 地址。

① 配置 eth0 接口的 IP 地址,如下图所示。

物理接口	子接口				
			接口设置		
	名称	eth0	( 00:13:32:02:23: <b>F</b> 4	)	
	描述				
	状态		停用		
	模式	$\odot$	路由 〇 交換		
	地址		掩码	非同步地址	
					添加
	地址		掩码	属性	删除
	192, 168, 83, 237		255, 255, 255, 0		3
	▶高级				
		硝	定 取消	<b>1</b>	

参数设置完成后,点击"确定"按钮即可。

② 配置 eth1 接口的 IP 地址,如下图所示。

物理接口	子接口			
		接口设置		
	名称 e <sup>4</sup> 描述 状态 [ 模式 ( 地址	th1 (00:13:32:02:23:F ☐ 停用 ● 路由 ○ 交換 掩码	5) 非同步地址	
	1.14 +.1_			添加
	твыс 10.1.1.1	r町149 255, 255, 255, 0	周任	mies.
	▶高级			9
		确定 取	消	

参数设置完成后,点击"确定"按钮即可。

③ 配置 eth2 接口的 IP 地址,如下图所示。

物理接口	子接口				
			接口设置		
	名称 描述 状态 模式 地址	eth2	2 (00:13:32:02:23:F6 停用 路由 <sup>C</sup> 交换 掩码	) 非同步地址 □	添加
	地址		掩码	属性	删除
	10. 10. 10. 1		255, 255, 255, 0		3
	▶高级				
		đ	确定 取补	¥ )	

参数设置完成后,点击"确定"按钮即可。

2) 配置地址转换策略。

点击 防火墙 > 地址转换,点击"添加",配置两条地址转换策略,如下图所示。

地址转换						
目的区域	所有区域	■ 高级打	叟索 「	- 显示第	策略统计	
╋ 添加			总	计:2 毎〕	页: 30条	•
ID	类型	源	目的	服务	转换	操作
8067	源转换	区域: area_eth0	<mark>区域:</mark> area_eth1		<mark>源:</mark> eth1	<b>~</b>
8068	源转换	区域: area_ethO	<mark>区域:</mark> area_eth2		<mark>源:</mark> eth2	<b>~</b>
M < 1 > M 转到 /1 Go						

3) 配置报警规则。

点击 **日志与报警 > 报警**,点击"添加",配置声音报警,然后选择"系统"报警 事件,当网络卫士防火墙出现链路故障时,就会触发声音报警,如下图所示。

报警											
÷	添加	<b>C</b> 报	警测试							急i	;†: 1
管理	系统	安全	策略	通讯	硬件	容错	测试	分类	名称	内容信息	操作
	•							beep	link_backup	长度:200 频率:440 延迟:100 重复:5	2

4) 配置主链路和从链路的 IP 探测对象。

a) 点击 网络管理 > IP 探测, 然后点击"添加"链接, 配置主链路的探测 IP 为 "172.16.1.2", 如下图所示。

IP探测				
		IP探测设置		
	接口	eth1	•	*
	探测IP	172.16.1.2		*
	探测时间间隔	5		] [1-3600秒]
	<b>a</b>	定 )	取消	$\supset$

参数配置完成后,点击"确定"按钮即可。

b)点击 网络管理 > IP 探测,然后点击"添加"链接,配置从链路的探测 IP 为
 "172.16.1.2",如下图所示。

IP探测	
	IP探测设置
接口	eth2 *
探测IP	*
探测时间间隔	5 [1-3600秒]
确	定取消

参数配置完成后,点击"确定"按钮即可。

主链路和从链路的探测 IP 配置完成后,可以在 IP 探测页面中查看这两条链路的探测 ID 号,如下图所示。

IP探测								
+	🕂 添加 🗴 清空							
ID	接口	探测IP	探测时间间隔	状态	引用模块	修改	删除	
100	eth1	172.16.1.2	5	初始状态			3	
101	eth2	172, 16, 1, 2	5	初始状态			3	

5) 配置静态路由。

设置两条静态默认路由,保证主、从链路的畅通。

a) 点击 网络管理 > 路由, 然后选择"路由表"页签, 点击"添加"。

① 添加一条默认路由:目的地址和目的掩码均为"0.0.0.0",网关为路由器的 eth1 接口的 IP 地址"10.1.1.2",如下图所示。

路由表	策略路由	动态路由OSPF	动态路由
		添加配置	
	目的地址	0.0.0.0	*
	目的掩码	0.0.0.0	*
	网关	10.1.1.2	
	接口	eth1	•
	高级		
	确注	定	

参数设置完成后,点击"确定"按钮即可。

② 添加一条默认路由:目的地址和目的掩码均为"0.0.0.0",网关为路由器的 eth2 接口的 IP 地址"10.10.10.2",如下图所示。

路由表	策略路由	动态路由OSPF	📃 动态路由
		添加配置	
	目的地址	0.0.0.0	*
	目的掩码	0.0.0.0	*
	网关	10. 10. 10. 2	
	接口	eth2	•
	高级		
	确:	æ 🔵 🤇	取消

参数设置完成后,点击"确定"按钮即可。

b)默认路由添加完毕后,点击 网络管理 > 路由,然后选择"路由表"页签,可以 看到新增默认路由及其 metric 值,如下图所示。

路由表 策略路日	目 🗌 动态路	₫OSP	F ्रिह्य	<mark>态路由</mark> RI	P 🔷 动态路由	1BGP 🔪	多播路	
标记: U-Up, G-Gateway specified, L-Local, C-Connected, S-Static O-Ospf, R-Rip, B-Bgp, D- Dhcp, I-Ipsec, i-Interface specified								
🕂 添加 🗴 清空	中 添加         面 清空         总计: 12							
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除	
10.10.11.1/32	0.0.0.0	ULi	1	1	10	-	-	
192.168.83.237/32	0.0.0.0	ULi	1	1	10	-	-	
10.1.1.1/32	0.0.0.0	ULi	1	1	10	-	-	
10.10.10.1/32	0.0.0.0	ULi	1	1	10	-	-	
10.10.11.0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-	
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-	
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-	
10.1.1.0/24	0.0.0.0	UCi	10	1	eth1	-	-	
10.1.1.0/24	0.0.0.0	UCi	100	1	ipsec1	-	-	
10.10.10.0/24	0.0.0.0	UCi	10	1	eth2	-	-	
0.0.0/0	10.1.1.2	UGSi	1	1	eth1	-	3	
0.0.0.0/0	10. 10. 10. 2	UGSi	1	1	eth2	-	3	

静态路由的 Metric 值表示路由的优先级,可以是从 0 开始的正整数,数字越大,优 先级越低。此时的 metric 值相同,均为 1。当启用链路备份后,防火墙将自动根据链路状 态为两条默认路由设定不同的 metric 值,保证同一时间只有一个链路启用,而另一条链路 则工作在备份状态。

6) 配置链路备份参数, 然后启动链路备份功能。

a) 点击 高可用性 > 链路备份,选择主链路的探测 ID 为"100",然后选择从链路的探测 ID 为"101",如下图所示。

链路备份			
链路类型	IP探测ID	状态	当前使用
主链路	100 💌 *		
从链路	101 💌 *		
启动	停止 设置者	逖	重置参数

b) 点击"设置参数"按钮,将链路备份参数写入系统内存。

c) 点击"启动"按钮,则界面会在"状态"一列显示主、从链路的工作状态,如下 图所示。

链路备份						
链路类型	IP探测ID	状态	当前使用			
主链路	100 💌 *	链路良好	*			
从链路	101 💌 *	链路良好				
启动	停止	设置参数	重置参数			

启用链路备份功能后,主从链路的链路状态均良好,但当前使用的是主链路,从链路 处于备份状态。

d)此时,可以在静态路由表中看到主从链路均可用(标记均为"U"),但是主链路静态路由的 Metric 值为"1",优先级最高;而从链路静态路由的 Metric 值变为 2,优先级降低,如下图所示。

路由表 策略路	由 动态器	储田OSF	ਾF <b>⊼</b> ੜ	)态路由R	IP 🔪 动态路I	<b>⋣</b> BGP	多播	
标记: U-Up, G-Gateway specified, L-Local, C-Connected, S-Static O-Ospf, R-Rip, B-Bgp, D- Dhcp, I-Ipsec, i-Interface specified								
🕂 添加 🗴 清空	♣ 添加  6 6 12							
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除	
10.10.11.1/32	0.0.0.0	ULi	1	1	10	-	-	
10.1.1.1/32	0.0.0.0	ULi	1	1	10	-	-	
10.10.10.1/32	0.0.0.0	ULi	1	1	10	-	-	
192.168.83.237/32	0.0.0.0	ULi	1	1	10	-	-	
10.10.11.0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-	
10.1.1.0/24	0.0.0.0	UCi	10	1	eth1	-	-	
10.1.1.0/24	0.0.0.0	UCi	100	1	ipsec1	-	-	
10.10.10.0/24	0.0.0.0	UCi	10	1	eth2	-	-	
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-	
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-	
0.0.0.0/0	10.1.1.2	UGSi	1	1	ethl	-	3	
0.0.0.0/0	10. 10. 10. 2	₩GSi	2	1	eth2	-	3	

7) 验证主、从链路切换过程。

a) 当主链路断开时, 主从链路进行切换, 主要表现在:

① 界面链路状态显示如下图所示。

链路备份							
链路类型	IP探测ID	状态	当前使用				
主链路	100 💌 *	链路不可达					
从链路	101 💌 *	链路良好	*				
启动	停止	设置参数	重置参数				

② 查看路由信息,主链路的路由不可用(标记为"GSi"),主、从链路静态路由的 Metric 值也发生变化,完成主、从链路切换。如下图所示。

路由表 策略路	由 🗌 动态器	备曲OSI	PF 🛛 👼	动态路由F	RIP 动态器	₩BGP	<b>\$</b> 1	
标记: U-Up, G-Gateway specified, L-Local, C-Connected, S-Static O-Ospf, R-Rip, B-Bgp, D-Dhcp, I-Ipsec, i-Interface specified								
🕂 添加 🗴 清空						道	it: 9	
目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除	
10.10.11.1/32	0.0.0.0	ULi	1	1	10	-	-	
10.10.10.1/32	0.0.0.0	ULi	1	1	10	-	-	
192.168.83.237/32	0.0.0.0	ULi	1	1	10	-	-	
10.10.11.0/24	0.0.0.0	UCi	200	1	sslvpnO	-	-	
10.10.10.0/24	0.0.0.0	UCi	10	1	eth2	-	-	
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-	
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-	
0.0.0.0/0	10, 10, 10, 2	UGSi	1	1	eth2	-	3	
0.0.0.0/0	10.1.1.2	GSi	2	1	ethi	-	3	

③ 根据设定的报警规则,防火墙进行声音报警。

b)当防火墙检测到主链路恢复后,默认路由的 Metric 值发生变化,数据链路由从链路切换回主链路。

#### 注意事项

1) 只有工作在路由模式的接口和 adsl 拨号动态接口才可以作为链路备份的主、从接口。当主、从接口选用 adsl 接口时还需要选择 网络管理 > ADSL, 配置 adsl 参数, 具体 配置方法请参考相关案例。并且添加默认路由时"接口"应选择 ADSL 链路启用后自动 添加的 ppp 接口名(例如 ppp0 接口)。

2) 链路备份中手动配置的默认路由应该指定出接口,否则链路切换时可能出现问题。

3) 链路备份中当 ADSL 为备用链路,并且主链路为"链路良好"状态时, ADSL 链路是处于关闭状态的;当主链路处于"链路不可达"状态时, ADSL 链路才会自动拨号。
# 服务器负载均衡

在高速网络中,服务器如果不具备大量并发访问能力,必然成为提供服务的瓶颈。如 果客户的增多导致通信量超出服务器所能承受的范围,此服务器必然会宕机。在这种情况 下,可以通过负载均衡在多个运行相同服务(例如 Web 服务)的主机间进行工作分配。

#### 基本需求

某企业提供的 Web 服务访问量较大,于是该企业准备使用 2 台 Web 服务器对外提供 WEB 服务,分别是 WebServer1(IP: 192.168.83.234)和 WebServer2(IP: 192.168.83.235)。

两台 WEB 服务器均通过防火墙的 eth0 口(IP: 192.168.83.240)采用 rr 算法对外提供服务。防火墙通过 eth1 口(IP: 10.1.1.1)与外网相连,来自外网的 HTTP 连接请求被按轮循的方式进行调度。



#### 图 41 防火墙负载均衡网络示意图

#### 配置要点

- ▶ 在两台 Web 服务器上添加路由
- ▶ 在客户端主机上配置 IP 和网关
- ▶ 配置防火墙接口属性(eth0和eth1的所属区域和IP地址)
- ▶ 配置主机对象
- ▶ 配置负载均衡服务器
- ▶ 配置负载均衡组
- ▶ 配置地址转换规则

▶ 验证 HTTP 连接请求是否被按轮循的方式进行调度

#### WEB 服务器配置步骤

在两台 Web 服务器上分别添加路由:

route add 10.1.1.0 mask 255.255.255.0 192.168.83.240

# 客户端配置步骤

在客户端 PC 上配置 IP 为 10.1.1.2, 掩码为 255.255.255.0, 默认网关为 10.1.1.1。

#### WEBUI 配置步骤

1) 配置防火墙接口属性(eth0 和 eth1 的所属区域和 IP 地址)

a) 点击 网络管理 > 接口,选择"物理接口"页签,然后点击 eth0 右侧的"设置" 图标,配置 eth0 口 IP 为 192.168.83.237/24,如下图所示。

物理接口	子接口				
			接口设置		
	名称 描述 状态 模式	eth0	(00:13:32:02:23:F4 停用 路由 <sup>C</sup> 交換	)	
	地址		掩码	非同步地址 □	添加
	地址		掩码	属性	删除
	192, 168, 83, 237		255, 255, 255, 0		ā
	▶高级				
		確	定 取消	1	

点击"确定"按钮即可。

b) 点击 网络管理 > 接口,选择"物理接口"页签,然后点击 eth1 右侧的"设置" 图标,配置 eth1 口 IP 为 10.1.1.1/24,如下图所示。

物理接口	子接口				
			接口设置		
	名称 描述 状态 模式 地址	ethi	. (00:13:32:02:23:F5 停用 路由 C 交換 掩码	) 非同步地址 □	添加
	地址		掩码	属性	删除
	10.1.1.1		255, 255, 255, 0		3
	▶ 高级				
		Ť	航定 取消	1 )	

点击"确定"按钮即可。

c)点击 资源管理 > 区域,然后点击"添加",配置防火墙 eth0 口和 eth1 口所属区 域,如下图所示。

区域						
🕂 添加	● 清空					总计: 3
名称	¢	绑定属性	¢	权限	注释	操作
area_eth0		eth0		允许		
area_eth1		eth1		允许		

2) 配置主机对象。

a) 点击 **资源管理 > 地址**, 然后选择"主机"页签, 点击"添加", 添加 web 服务器 "WebServer1", 如下图所示。

主机	范围	子网 地址組	
		主机属	性
	名称 物理地址	WebServer1	] *
	IP地址	192. 168. 83. 234	<- 192. 168. 83. 234 ×
		确定	取消

b) 点击 **资源管理 > 地址**, 然后选择"主机"页签, 点击"添加", 添加 web 服务器 "WebServer2", 如下图所示。

主机	范围	子网 地址組	
		主机属	性
	名称 物理地址	WebServer2	*
	IP地址	192, 168, 83, 235	<- 192.168.83.235 ×
		确定	取消

参数设置完成后,点击"确定"按钮即可。

c)点击 **资源管理 > 地址**,然后选择"主机"页签,点击"添加",添加两台 web 服务器对外提供服务的主机地址"WebServer",如下图所示。

主机	范围	子网 地址組	
		主机属	性
	名称 物理地址	WebServer 00:00:00:00:00:00	] *
	IP地址	192. 168. 83. 219	<- 192.168.83.219 ×
		确定	取消

3) 配置负载均衡服务器。

a) 点击 **高可用性 > 服务器负载均衡**, 然后选择"服务器"页签, 点击"添加"定 义负载均衡服务器 S1, 如下图所示。

<b>服务器</b> 均衡組	
	服务器尾性
名称	S1 *
主机	WebServer1 💌
权重	10 * [1-100]
探测选项	
	不作探测 〇
	主机探测 💿
	服务探测 🔘 端口 📃
	确定

参数设置完成后,点击"确定"按钮即可。

b)点击 高可用性 > 服务器负载均衡,然后选择"服务器"页签,点击"添加"定义负载均衡服务器 S2,如下图所示。

<b>服务器</b> 均衡組		
		服务器属性
	名称	\$2 *
	主机	WebServer2 💌
	权重	20 * [1-100]
	探测选项	
		不作探测 〇
		主机探测 💿
		服务探测 🔘 端口
		确定 取消

4) 配置负载均衡组。

a) 点击 **高可用性 > 服务器负载均衡**, 然后选择"均衡组"页签, 点击"添加"定 义负载均衡组 VS1, 如下图所示。

<b>服务器</b> 均衡組
均衡服务器組属性
名称 VS1 *
可用服务器
-> S1 [服务器] S2 [服务器] ×
负载均衡方式
⊙ 轮流
○ 根据权重轮流
○ 最少连接
① 加权最少连接(最少连接算法再加上加权值)
〇 根据源地址作HASH查找
〇 根据目的地址作HASH查找
备份组
确定取消

#### 说明**:**

◆ 对于负载均衡方式,用户可以根据自己企业内 WEB 服务器的具体情况选择使用。

5) 配置地址转换规则。

a) 点击 防火墙 > 地址转换, 然后在右侧页面中点击"添加"定义目的地址转换规则。

b)选中"目的转换"前的单选按钮,然后设定"源"为"any",设定目的为"WebServer", 设定服务为"HTTP",最后将目的地址转换为"VS1[负载均衡组]",如下图所示。

地址转换			
			添加地址转换
	相士		日的转换
	1¥30		
	源		
		地址	任意
		其它	
	目的		
		地址	
			WebServer 🔟
		其它	
	ᄪᄲ		
	版务	[	нттр 🔟
	-		
	目的地址	止转换为	VS1 [负载均衡组] 🛛 🛛 💙
	目的端口	口转换为	不做转换 💙
	规则描述	ŧ	
			明定 取得

c)参数设置完成后,点击"确定"按钮即可。

说明:

◆ 对于该目的地址转换规则,用户可以根据企业的具体情况选择源和目的。

6) 验证 HTTP 连接请求是否被按轮循的方式进行调度。

打开 IE 浏览器, 输入"http://192.168.83.219", 转入 WebServer1 (IP: 192.168.83.234) 的页面, 如下图所示。



由于设置了轮询机制,所以刷新页面时,转入WebServer2(IP: 192.168.83.235)的页面,如下图所示。



#### 注意事项

1) 在配置过程中,请确保没有与该规则相冲突的地址转换策略和阻断策略等。

2)通信时,如果从均衡组中删除一台 server,则连到此 server 上的连接并不会断开, 只有重新连接配置才会生效。

3)当正在通信时,如果所连接的服务器断开,客户机不会自动连上其它 active 的服务器,除非重新连接。

4)当选择主机探测时,如果所访问的服务停掉了而主机没有停掉,则这个主机仍然 会被分配连接。但因为服务没有了,所以处于始终无法连接的情况。

# 虚拟系统

#### 基本需求

将一台防火墙配置为两个虚拟系统 VS1 和 VS2,并且允许所有的通讯。使接口 eth0 和接口 eth1 的子接口 veth1.01 属于 VS1,可以互相通信(即:默认网关为 veth1.01 的主机 A 可以访问主机 C);使接口 eth1 的子接口 veth1.02 属于 VS2,不能与 VS1 中的任何接口通信(即:默认网关为 veth1.02 的主机 B 不能访问主机 C)。



图 42 防火墙虚系统示意图

#### 配置要点

- ▶ 在主机 A、主机 B和主机 C上配置 IP 地址和默认网关
- ▶ 配置接口的 IP 地址和 VS 属性
- ▶ 验证

# 主机的配置

在主机 A 上配置 IP 为 10.1.1.2, 掩码为 255.255.255.0, 默认网关为 10.1.1.1。

在主机 B 上配置 IP 为 10.1.2.2, 掩码为 255.255.255.0, 默认网关为 10.1.2.1。

在主机 C 上配置 IP 为 192.168.83.234, 掩码为 255.255.255.0, 默认网关为 192.168.83.237。

#### WEBUI 配置步骤

1) 配置接口的 IP 地址和 VS 属性。

a) 配置接口 eth0。

点击 网络管理 > 接口,然后选择"物理接口"页签,在 eth0 接口后点击"设置"
 图标,配置 IP 地址为"192.168.83.237",如下图所示。

物理接口	子接口				
			接口设置		
	名称 描述 状态 模式 地址	eth0	(00:13:32:02:23:F4 序用 路由 <sup>C</sup> 交換 掩码 :	) 非同步地址	添加
	地址		掩码	属性	删除
	192. 168. 83. 237		255, 255, 255, 0		3
	▶ 高级				
		確	定 取消		

② 点击"高级",在"虚系统 ID"中填入本接口所属虚拟系统 ID 号"1",如下图 所示。

物理接口	子接口						
			ŧ	<b>赛口</b> 设置			
	名称	eth0	(00:	13:32:02:23	:F4	)	
	描述				1		
	状态		停用				
	模式	$\odot$	路由	〇 交換			
	地址		掩码		3	非同步地址	
							添加
	地址		掩码			属性	删除
	192. 168. 83. 237		255.	255, 255, 0			3
	▼高级						
	MTU	1500			[68	8-1500]	
	虚系统ID	1			[0-	-254]	
		確	腚		取消	i	

③ 参数设置完成后,点击"确定"按钮即可。

b) 配置 eth1 的子接口 veth1.01 和 veth1.02。

① 点击 网络管理 > 接口, 然后选择"子接口"页签, 点击"添加子接口", 添加 子接口 veth1.01 和 veth1.02, 如下图所示。

物理接口 子接口	
添加子接!	
路由接口 eth1	•
添加单个子接口 🔿	[0-31]
添加子接口范围 💿 1	- 2
确定	取消

② 点击 veth1.01 接口右侧的修改图标" 🖙",配置该子接口的 IP 地址,如下图所示。

物理接口	子接口			
		子接口设置		
	名称 v 描述 □ 状态 『 接口地址 地址	eth1.01 停用 掩码	非同步地址	
	地址	掩码	属性	添加 删除
	10.1.1.1	255.255.255.0		3
	▶高级			
		确定 取	消	

在 veth1.01 接口配置页面,点击"高级"左侧图标,配置该子接口属于 VS1,如下图 所示。

物理接口	子接口						
				子接口设置			
	名称 描述 状态	vetl	u1.0 停戶	1			
	接口地址 地址		掩码	冯		非同步地址 □	法加
	地址		掩	冯		属性	删除
	10.1.1.1 <b>▼高级</b>		255	5. 255. 255. 0			٩
	VLAN-ID 接口绑定	0			[	)-4094]	
	虚系统ID	1			[(	0-254]	
		ł	角定		取	肖 )	

③ 点击 veth1.02 接口右侧的修改图标" 记", 配置该子接口的 IP 地址, 如下图所示。

物理接口	子接口			
		子接口设置		
	名称 · · · · · · · · · · · · · · · · · · ·	reth1.02 □ 停用 撞码	非同步地址	·沃加
	地址	掩码	属性	删除
	10.1.2.1	255, 255, 255, 0		3
	▶ 高级			
		确定 取;		

在 veth1.02 接口配置页面,点击"高级"左侧图标,配置该子接口属于 VS2,如下图 所示。

物理接口	子接口						
				子接口设置			
	名称 描述	i veth			1		
	状态		停用	]			
	地址		掩碑	3		非同步地址 □	添加
	地址		掩碼	9		属性	删除
	10.1.2.1		255	. 255. 255. 0			3
	▼高级						
	VLAN-ID 接口绑定	0			] [(	)-4094]	
	虚系统ID	2			] [(	)-254]	
		ł	确定		取	<u>ان</u>	

2) 验证。

a) 在主机 A 上 ping 主机 C,可以收到主机 C 的 ping 回应,如下图所示。

🔤 C:\WINDOWS\system32\cmd.exe				
C:\Documents and Settings>ping 192.168.83.234				
Pinging 192.168.83.234 with 32 bytes of data:				
Reply from 192.168.83.234: bytes=32 time<1ms TTL=127				
Reply from 192.168.83.234: bytes=32 time<1ms TTL=127				
Reply from 192.168.83.234: bytes=32 time<1ms TTL=127				
Reply from 192.168.83.234: bytes=32 time<1ms TTL=127				
Ping statistics for 192.168.83.234: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),				
Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms				
C:\Documents and Settings>				

在主机 B 上 ping 主机 C,不能收到主机 C 的 ping 回应,如下图所示。



b) 在主机 A 上访问主机 C 的 FTP 服务,可以正常显示 FTP 服务器上的文件目录, 并且可以从 FTP 服务器上正常下载文件,如下图所示。



在主机 B 上访问主机 C 的 FTP 服务,不能正常显示 FTP 服务器上的文件目录,也不能下载文件,如下图所示。

September 2017 Strategiese Str		] ×
文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(I) 帮助(出)		<b>.</b>
🕝 后退 🔹 🌖 🔹 🏂 🔛 搜索 🌔 文件夹 🛛 🔂 🔀 💙 📔	<b></b> •	
地址(D) 👰 ftp://192.168.83.234/	🔽 芛 转到	链接
YAHOO! ▼ 🎎 ▼ 🔍 🔍 搜索 ▼	» 🍕	•
Windows 无法访问此文件夹。诸确保输入的文件名是正确的, 详细信息: 操作超时	,并且您有权访问此文作	<b>‡</b> 夹。

# 注意事项

1) 规则名称定义时允许虚拟系统之间重名,但是同一虚拟系统内部不允许重名。

2)系统管理员可以配置虚拟系统管理员,虚拟系统管理员登录防火墙后,只能看到本虚拟系统的配置信息,并且可用功能会受到限制,具体说明请参见管理手册的相关描述。

# 日志分析

网络卫士防火墙为了方便用户更好地调试、监控和管理设备,提供日志和报警服务功能。用户还可以结合天融信的 TOPSEC 安全审计综合分析系统(TOPSEC Auditor),进行完善的日志和报警管理,下面将逐一进行介绍。

# 设置日志服务

# 基本需求

管理员通过管理主机上的 TOPSEC 集中管理器使用 TOPSEC 安全审计综合分析系统 (TOPSEC Auditor)对日志进行浏览。手工定制过滤条件,并对查询结果进行浏览和导出。



#### 图 43 防火墙与日志系统连接示意图

管理主机、网络卫士防火墙和日志服务器是网络连通的。本例中,日志服务器的 IP 地址: 10.200.2.111,网络卫士防火墙 IP 地址: 10.200.51.253。

#### 配置要点

- ▶ 在每台需要进行日志分析的网络卫士防火墙上配置日志服务器及相应参数
- ▶ 查看防火墙中的日志信息

# WEBUI 配置步骤

1) 在每台需要进行日志分析的网络卫士防火墙上配置日志服务器及相应参数。

管理员配置并应用日志服务器参数后,系统记录的日志除了被发送到设定的日志服务器中外,也在防火墙中缓存部分日志,以便管理员随时查看在防火墙中缓存的日志信息。 a)点击 **日志与报警 > 日志设置**,配置日志设置参数,如下图所示。

日志设置								
	服务器地址 服务器端口 传输类型 是否加密 加密密码 日志类型	10.200.2.1 514 SysLog ▼ 11111111 调试 □ 选择全i	□ □ □ □ □ □	*	*[可输/	入多个IP地址,	用空	湘分开]
		<ul> <li>✓ 配置管</li> <li>✓ 访问控</li> <li>✓ 端口流</li> <li>✓ 反垃圾</li> <li>SSLVPN日病</li> </ul>	理制量邮志	系统运行 防攻击 入侵防御 应用程序: 系统 端口转发	L (S) (S) (S) (S) (S) (S) (S) (S) (S) (S)	阻断策略 深度内容检测 虚拟专网 全网接入 WED转发	র র র	连接 用户认证 防病毒 应用web化
				应用				

日志级别各等级含义如下:

- ▶ 紧急:造成严重错误导致系统不可用,该日志被传送到日志服务器。
- ▶ 告警:警报信息,需要通知管理员,该日志被传送到日志服务器。
- ▶ 严重:严重错误信息,可能会造成某些功能无法正常工作。
- ▶ 错误:一般错误信息。
- ➢ 警示:所有攻击行为以及非授权访问(除通信日志外)。
- ▶ 通知:管理员操作。
- ▶ 信息:普通事件。
- ▶ 调试:开发人员调试信息。

设备根据日志类型和日志级别来记录和传输日志。例如:日志级别为"信息",日志 类型为"配置管理",表示设备将记录"紧急"到"信息"之间所有级别的日志信息。

b)参数设置完成后,点击"应用"按钮。

2) 查看防火墙中的日志信息。

网络卫士防火墙对系统日志提供简单查看功能,方便用户及时跟踪网络卫士防火墙的 工作状态。管理员可以查看六种类型的日志信息:

- "常规日志"指的是防火墙系统运行期间有关系统运行状况、管理情况以及策略 匹配情况等等的记录信息。
- "深度内容过滤日志"指的是防火墙系统运行期间有关 HTTP 过滤、FTP 过滤、 邮件过滤、DNS 过滤和命令过滤策略匹配情况等等的记录信息。
- "病毒过滤日志"指的是防火墙系统运行期间有关病毒过滤策略匹配情况的记录 信息。
- "反垃圾邮件日志"指的是防火墙系统运行期间有关反垃圾邮件模块过滤邮件情况的记录信息。
- "应用程序识别日志"指的是防火墙系统运行期间有关应用程序识别模块检测应用层数据情况的记录信息。
- "IPS 日志"是指所有攻击事件及事件本身的详细内容,包括:排名、事件号、 级别、次数及事件描述等。

下面以查询"常规日志"类型的日志为例,详细介绍如何进行日志查看操作:

a) 选择 日志与报警 > 日志查看, 进入"日志查询"窗口, 如下图所示。

常規日志 深度内容过滤日志 病毒过滤日志	反垃圾邮件日志 应用程序识别日志	IPS日志
日志类型系统运行 💌 查找	<b>查找</b>	
○ 刷新日志		总计: 0
日期/时间	級别 类型	描述

b) 激活"常规日志"页签,然后在"日志类型"右侧的下拉框中选择待查看日志的 类型,日志列表中将显示该日志类型的所有日志信息,管理员可以滚动查看相关日志。

例如:选择日志类型为"配置管理"后,日志列表中显示所有类型为"配置管理"的 日志信息,如下图所示。

常規日志 深度	内容词	过滤日志	気 病毒〕	过滤日志 🔪 反	垃圾邮件	日志	应用程序识别日志 IPS日志
日志类型配置管理	•	E	₹ 我	查	找	┓ 清雪	空所有类型日志 🗕
C 刷新日志							
日期/时间	级别	类型	用户	登陆IP	执行命令	执行结果	消息
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log set ipaddr '10.200.2.111' port ud
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add sv_cifs"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add sv_netacc"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add sv_system"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add sv_pf"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add sv_wf"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add ar"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add asse"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add avse"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add vpn"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add dpi"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add secure"
2009-12-16/15:52:59	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add ac"
2009-12-16/15:52:58	通知	配置管理	superman	192.168.83.220	"config"	0	"log log type_set add conn" 📃 👻
•							►

c)在"日志类型"右侧的下拉框中选择待查看日志的类型,然后在"查找"右侧的 文本框中输入待查看日志的关键字,最后点击"查找"按钮,日志列表中将显示包括该关 键字的所有属于该日志类型的日志信息,管理员可以滚动查看相关日志。

例如:选择"配置管理"后,然后在"查找"右侧的文本框中输入关键字 "192.168.83.225",最后点击"查找"按钮,日志列表中将显示属于"配置管理"日志 类型,并且包含"192.168.83.225"的所有日志信息,如下图所示。

常規日志 深度	内容达	せ渡日志	病毒〕	过滤日志 反	垃圾邮件日志	应用程序识别日志 IPS日志
日志类型     配置管理     查找     192. 168. 83. 22     查找     面 清空所有类型日志						
◎利新日志						
日期/时间	级别	类型	用户	登陆IP	执行命令执行结果	消息
2009-12-16/15:35:23	通知	配置管理	superman	192.168.83.225	"config" 0	"snmp set contact "
2009-12-16/15:35:23	通知	配置管理	superman	192.168.83.225	"config" 0	"snmp set location www.topsec.com.cn "
2009-12-16/15:35:19	通知	配置管理	superman	192.168.83.225	"config" 0	"snmp start"
2009-12-16/15:35:15	通知	配置管理	superman	192.168.83.225	"config" 0	"snmp stop"
2009-12-16/15:34:57	通知	配置管理	superman	192.168.83.225	"config" 0	"snmp set contact "
2009-12-16/15:34:57	通知	配置管理	superman	192.168.83.225	"config" ()	"snmp set location www.topsec.com.cn "
2009-12-16/15:34:44	通知	配置管理	superman	192.168.83.225	"config" 0	"snmp managehost add name kk hostip 192.
4						

#### 注意事项

 1)日志查询中输入的关键字不能包括特殊字符,如"/"、"="等。管理员输入查 询关键字后,网关将在本地缓存的日志信息中查找包括该关键字的所有日志信息。 2)由于防火墙存储日志的数量有限,不能全面详尽的提供日志查看功能。建议结合 天融信 TOPSEC 安全审计综合分析系统(TOPSEC Auditor)进行日志查看,具体操作请 参见相关手册。

# 日志报警

# 基本需求

当网络卫士防火墙出现系统故障(网卡掉线等)时,将向区域 area\_eth1 中的 SNMP 陷阱主机进行报警。

# 配置要点

- ▶ 开放 SNMP 服务
- ▶ 启动 SNMP 代理
- ▶ 设置陷阱主机
- ▶ 添加报警规则
- ▶ 设置报警触发

#### WEBUI 配置步骤

1) 开放 SNMP 服务。

开放 SNMP 陷阱主机所在区域 area\_eth1 的 SNMP 服务。

a) 点击 **系统管理 > 配置**, 然后选择"开放服务"页签, 点击"添加", 配置 area\_eth1 的 SNMP 服务, 如下图所示。

系统参数 开放服务 时间	SNMP 邮件设置 短信设置
	添加配置
服务名称 控制区域 控制地址	SNMP area_eth1 any [范围]
	确 定 取 消

b)参数设置完成后,点击"确定"按钮即可。

2) 设置陷阱主机。

a)选择 系统管理 > 配置,然后选择 "SNMP"页签,点击 SNMP 陷阱主机列表左 上方的"添加",配置陷阱主机参数,如下图所示。

系统参数 开放	最多 时间	SNMP的推动	设置   短					
SIMP陷阱主机								
	主机名称 sump 主机IP 192.	ohost 168. 96. 71	*					
	确定	取消						

- b)参数设置完成后,点击"确定"按钮。
- 3) 启动 SNMP 代理。

点击 **系统管理 > 配置**, 然后选择 "SNMP" 页签, 在 "SNMP 服务控制" 区域点击 "启动" 按钮, 如下图所示。

时间 SNMF	邮件设置 短信设置 W					
SIPP设置						
SNMP服务控制 位置 www.topsec.com.cn 联系 <support@topsec.com.cn></support@topsec.com.cn>						
应用 启动 停止						

- 4) 设置报警规则。
- a) 点击 日志与报警 > 报警, 点击"添加"设置报警服务规则, 如下图所示。

报警						
	报警服务规则					
报警类型 报警名称	SNMP  snmp *					
	确定 取消					

b)参数设置完成后,点击"确定"按钮。

5) 设置触发报警的安全事件。

点击 **日志与报警 > 报警**,在 snmp 报警服务规则中,选择安全事件"系统",如下 图所示。

报客											
	〒 添加 C 报告例は 忌け:1										
管理	系统	安全	策略	通讯	硬件	容错	测试	分类	名称	内容信息	操作
	•							sımp	sımp		

这条规则成功设置后,当网络卫士防火墙出现系统故障(网卡掉线等)时,就会触发 一个 SNMP 报警。网络卫士防火墙会向 SNMP 陷阱主机发送报警消息。

在 SNMP 陷阱主机的 HP Open View 中可以查看到 SNMP 报警。

# 注意事项

用户也可以使用 TOPSEC 安全审计综合分析系统(TOPSEC Auditor)进行日志的报警,具体方法请参见 TOPSEC 安全审计综合分析系统(TOPSEC Auditor)的相关文档。

声明:

1. 本手册所提到的产品规格及资讯仅供参考,有关内容可能会随时更新,天融信不另行通知。

 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差 异,此可能产生的差异为正常现象,产品功能和性能请以产品说明书为准。

 本手册中没有任何关于其他同类产品的对比或比较,天融信也不对其他同类产品表达意见, 如引起相关纠纷应属于自行推测或误会,天融信对此没有任何立场。

本手册中提到的信息为正常公开的信息,若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失,天融信及其员工不承担任何责任。