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

商标声明

信息反馈

http://www.topsec.com.cn

目　录

前言 **1**

文档目的 1
读者对象 1
约定 1
相关文档 2
技术服务体系 2

配置导入、导出 **4**

配置导出 4
基本需求 *4*
配置要点 *4*
WEBUI配置步骤 *4*
配置导入 5
基本需求 *5*
配置要点 *6*
WEBUI配置步骤 *6*

在线升级 **6**

基本需求 *6*
配置要点 *7*
TFTP服务器设置 *7*
WEBUI配置步骤 *8*
注意事项 *9*

动态路由配置 **10**

OSPF动态路由配置 10
基本需求 *10*
配置要点 *11*
WEBUI配置步骤 *11*
注意事项 *13*
RIP动态路由配置 14
基本需求 *14*
配置要点 *15*
WEBUI配置步骤 *15*
注意事项 *18*

策略路由配置 **18**

基本需求 *18*
配置要点（需求1） *19*
WEBUI配置步骤 *19*
配置要点（需求2） *22*
WEBUI配置步骤 *22*

多播 **24**

基本需求 *24*
配置要点 *24*
WEBUI配置步骤 *24*

注意事项.....25

DHCP.....**26**

DHCP服务器.....26
基本需求.....26
配置要点.....26
WEBUI配置步骤.....26
注意事项.....29
DHCP客户端.....29
基本需求.....29
配置要点.....30
WEBUI配置步骤.....30
注意事项.....33
DHCP中继.....34
基本需求.....34
配置要点.....34
WEBUI配置步骤.....35
注意事项.....37

网络链路.....**38**

ADSL配置.....39
基本需求.....39
配置要点.....39
WEBUI配置步骤.....39
注意事项.....43
GRE通道配置.....44
基本需求.....44
配置要点.....45
WEBUI配置步骤.....45
注意事项.....48
PPTP隧道.....48
基本需求.....48
配置要点.....49
WEBUI配置步骤.....49
注意事项.....62
L2TP隧道.....62

带宽管理.....**64**

基本需求.....65
配置要点.....66
WEBUI配置步骤.....66
注意事项.....72

用户认证.....**73**

本地密码认证.....73
基本需求.....73
配置要点.....73
WEBUI配置步骤.....73
第三方RADIUS服务器认证.....76
基本需求.....76
配置要点.....76
WEBUI配置步骤.....76
注意事项.....82
证书认证.....82

基本需求.....82
配置要点.....82
WEBUI配置步骤.....83
注意事项.....88

报文阻断规则配置.....88

二层报文过滤.....89
基本需求.....89
配置要点.....90
WEBUI配置步骤.....90
注意事项.....91
三层报文过滤.....92
基本需求.....92
配置要点.....92
WEBUI配置步骤.....92
注意事项.....94

地址转换.....95

基于地址对象的源地址转换.....95
基本需求.....95
配置要点.....95
WebUI配置步骤.....96
基于IP地址的目的地址转换.....98
基本需求.....98
配置要点.....99
WebUI配置步骤.....99
注意事项.....103
双向地址转换.....103
基本需求.....103
配置要点.....104
WEBUI配置步骤.....104
注意事项.....106

访问控制规则配置.....107

基本需求.....108
配置要点.....109
WebUI配置步骤.....109

IPS策略配置.....116

基本需求.....116
配置要点.....116
WEBUI配置步骤.....116
注意事项.....118

深度过滤.....119

HTTP过滤.....119
基本需求.....119
配置要点.....119
WebUI配置步骤.....119
注意事项.....125

IPSEC VPN隧道管理.....126

远程用户本地管理.....126
基本需求.....126

配置要点.....126
WebUI配置步骤.....127
注意事项.....141
远程用户集中管理.....141
基本需求.....141
配置要点.....142
WebUI配置步骤.....142
注意事项.....151
VPN静态隧道（本地配置）.....151
基本需求.....151
配置要点.....152
WebUI配置步骤.....152
注意事项.....157
VPN动态隧道（集中管理）.....157
基本需求.....157
配置要点.....158
WebUI配置步骤.....158
注意事项.....163

SSL VPN配置案例.....164

WEB转发.....164
基本需求.....164
配置要点.....165
防火墙A的配置步骤.....165
WEBUI配置步骤.....166
端口转发.....178
基本需求.....178
配置要点.....179
防火墙A的配置步骤.....179
WEBUI配置步骤.....180
全网接入.....191
基本需求.....192
配置要点.....192
防火墙A的配置步骤.....193
WEBUI配置步骤.....194
注意事项.....213
本地证书认证.....213
基本需求.....213
配置要点.....214
防火墙A的配置步骤.....214
WEBUI配置步骤.....215
注意事项.....229
第三方证书认证.....229
基本需求.....229
配置要点.....230
防火墙A的配置步骤.....230
WEBUI配置步骤.....231
RADIUS 认证.....239
基本需求.....239
配置要点.....239
防火墙的配置步骤.....239
Radius的配置步骤.....240
WEBUI配置步骤.....241

注意事项.....243
双因子认证.....243
基本需求.....243
配置要点.....244
防火墙A的配置步骤.....244
WEBUI配置步骤.....245
注意事项.....259
与IDS联动.....260
基本需求.....260
配置要点.....261
WEBUI配置步骤.....261
注意事项.....265
双机热备.....266
双机热备模式.....266
基本需求.....266
配置要点.....266
WEBUI配置步骤.....267
注意事项.....273
路由接口下的负载均衡模式.....274
基本需求.....274
配置要点.....275
WEBUI配置步骤.....275
TRUNK口下的负载均衡模式.....283
基本需求.....283
配置要点.....284
WEBUI配置步骤.....284
连接保护模式.....293
基本需求.....293
配置要点.....293
WEBUI配置步骤.....293
注意事项.....298
子接口的负载均衡模式.....299
基本需求.....299
配置要点.....300
WEBUI配置步骤.....300
链路备份.....307
基本需求.....307
配置要点.....307
WEBUI配置步骤.....308
注意事项.....316
服务器负载均衡.....317
基本需求.....317
配置要点.....317
WEB服务器配置步骤.....318
客户端配置步骤.....318
WEBUI配置步骤.....318
注意事项.....324
虚拟系统.....326
基本需求.....326

配置要点.....*326*
主机的配置.....*326*
WEBUI配置步骤.....*326*
注意事项.....*332*
日志分析.....**333**
设置日志服务.....333
基本需求.....*333*
配置要点.....*333*
WEBUI配置步骤.....*333*
注意事项.....*336*
日志报警.....337
基本需求.....*337*
配置要点.....*337*
WEBUI配置步骤.....*337*
注意事项.....*339*

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

http://www.topsec.com.cn/support/support.asp

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

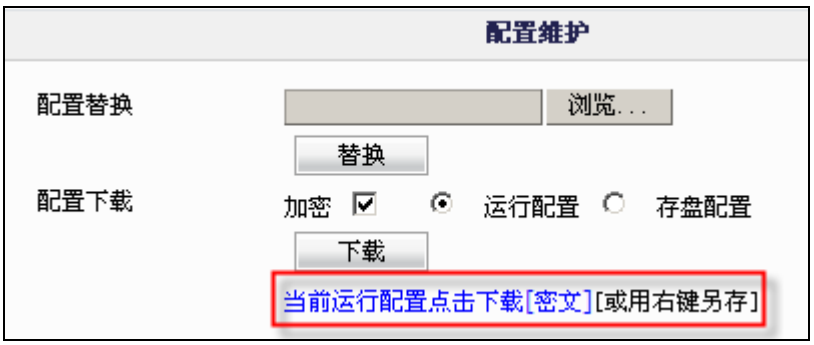
WEBUI 配置步骤

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。

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。

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。

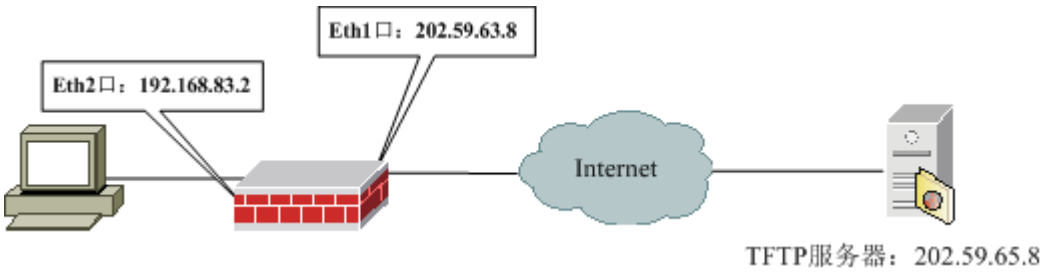


图 1 远程升级网络拓扑示意图

配置要点

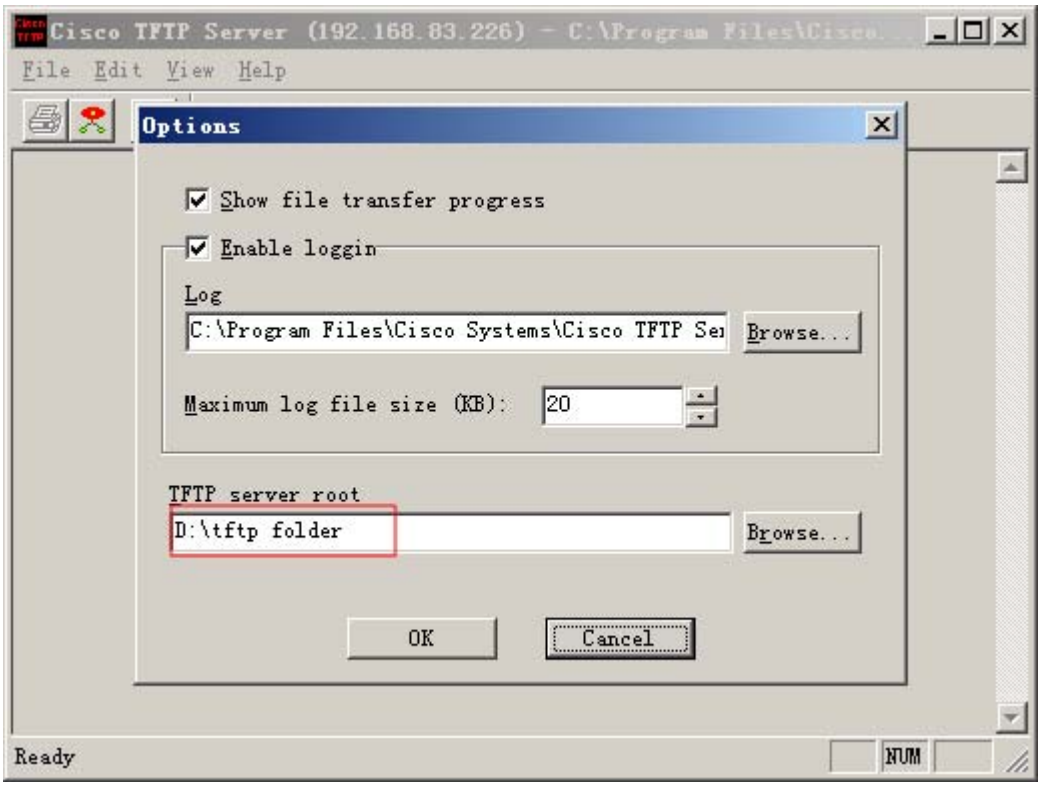
- 获取网络卫士防火墙升级包，并将其存放于 TFTP 服务器的工作目录中
- 验证升级包
- 在网络卫士防火墙上设置 TFTP 服务器
- 对网络卫士防火墙进行升级

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。



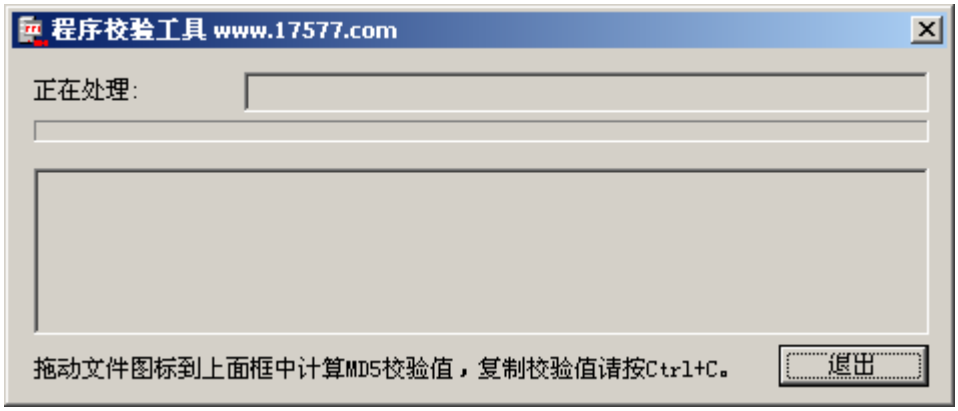
2）将网络卫士防火墙升级包存放于工作目录中。

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。



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。

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。

2）点击“TFTP 升级”按钮设置 TFTP 服务器。

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。

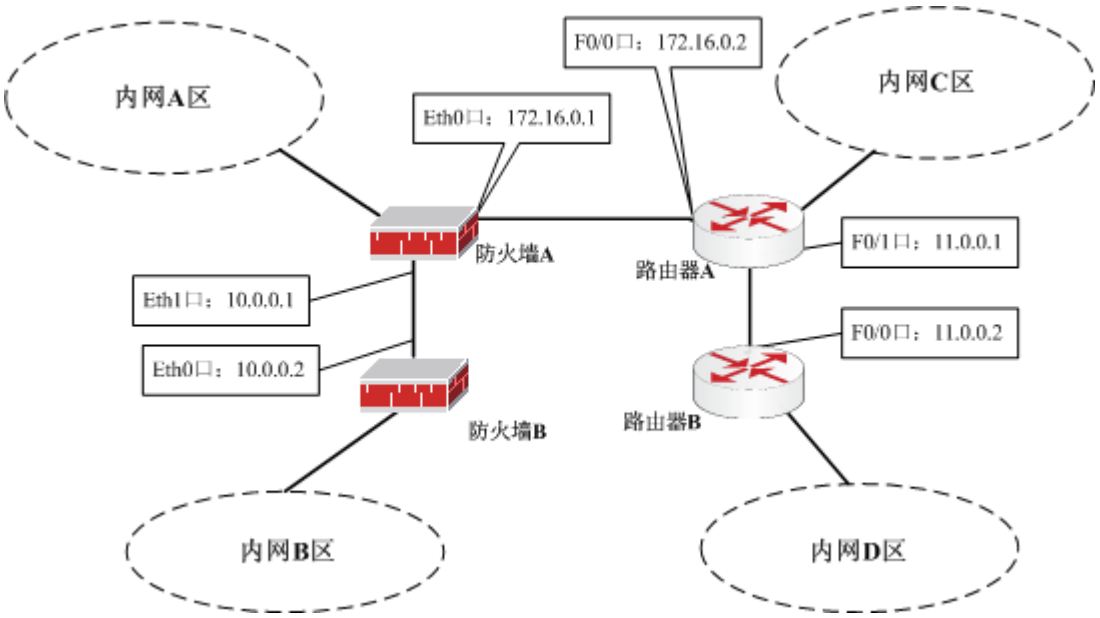


图 2 OSPF 动态路由配置网络拓扑图

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

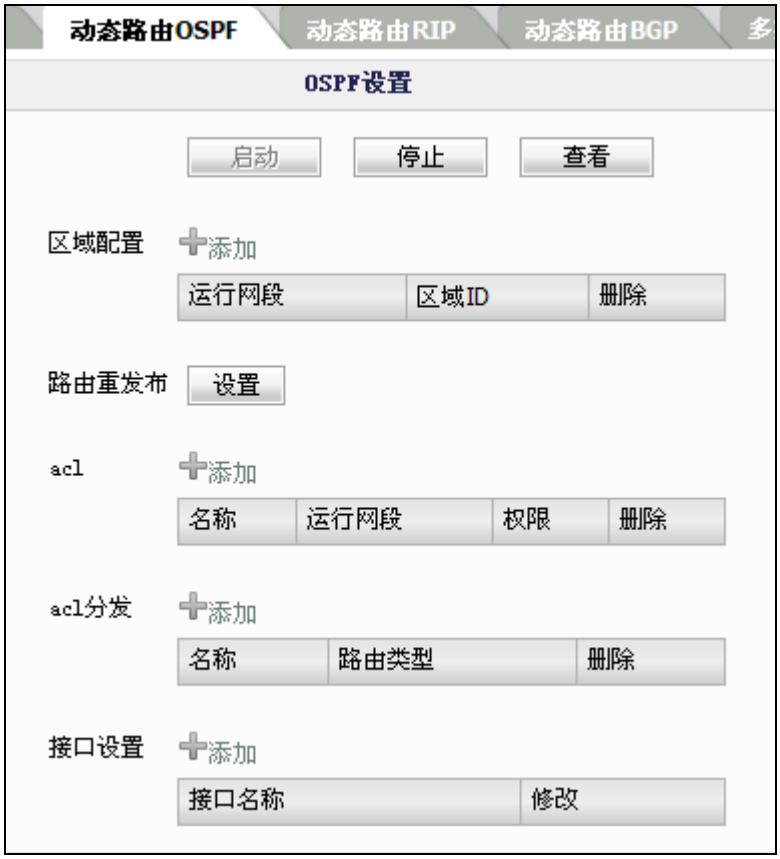
WEBUI 配置步骤

网络卫士防火墙 A 配置：

1）启动 OSPF 服务。

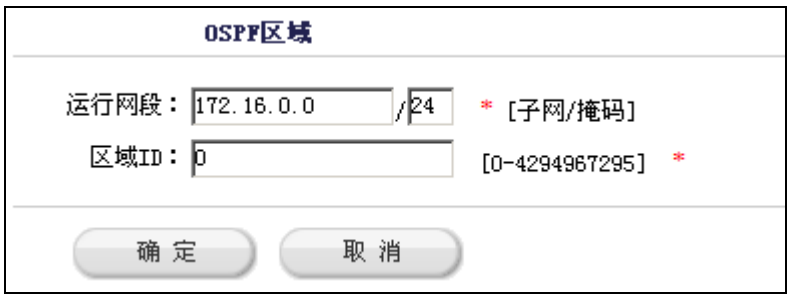
选择 **网络管理 > 路由**，并选择“动态路由 OSPF”页签，点击“启动”按钮启动 OSPF 服务，如下图。

启动后界面如下图所示。



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。



添加 10.0.0.0/24 到 area 1，如下图。

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。

3）将网络 10.0.0.0/24 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。

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。

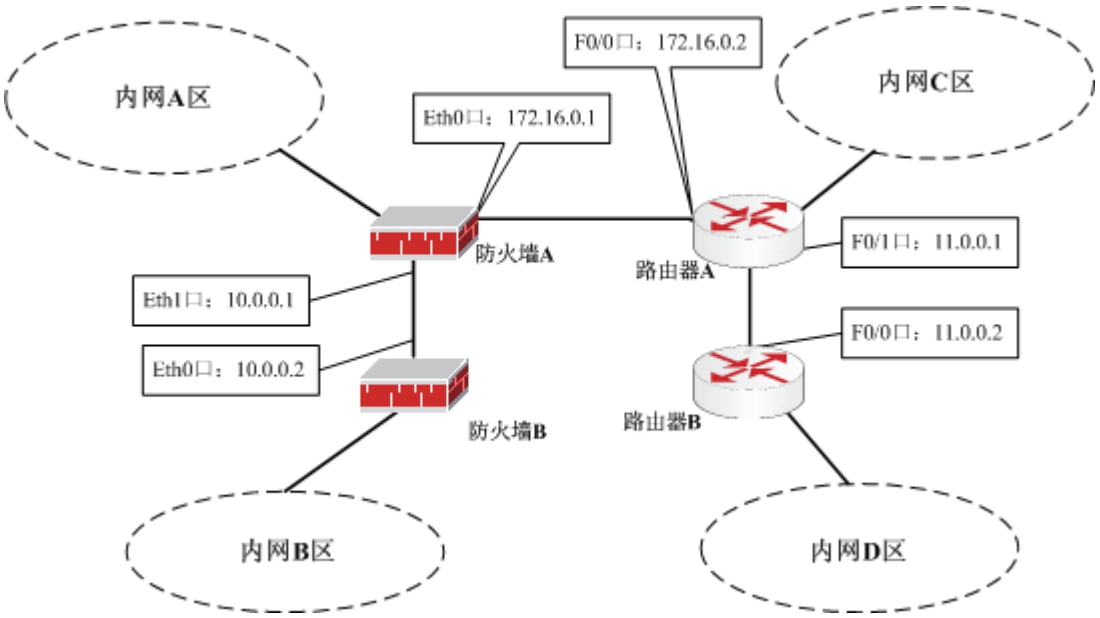


图 3 RIP 动态路由配置网络拓扑图

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。

点击“添加”开放 eth1 口的 RIP 服务，如下图。

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。

启动 RIP 协议后，界面如下图所示。

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。

添加 10.0.0.0/24 网络，如下图。

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。

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。

启动 RIP 协议后，界面如下图所示。

3）设置网络 10.0.0.0/24 参与 RIP 动态路由。

在“邻居配置”处点击“添加”按钮添加网络 10.0.0.0/24，如下图。

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。

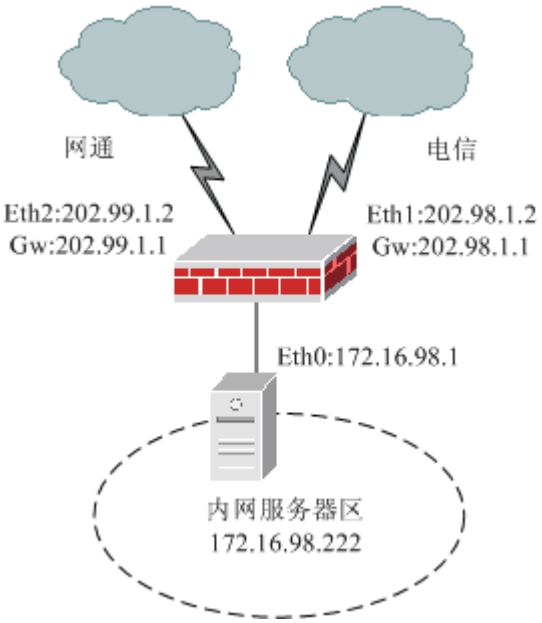


图 4 策略路由配置拓扑图

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。

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。

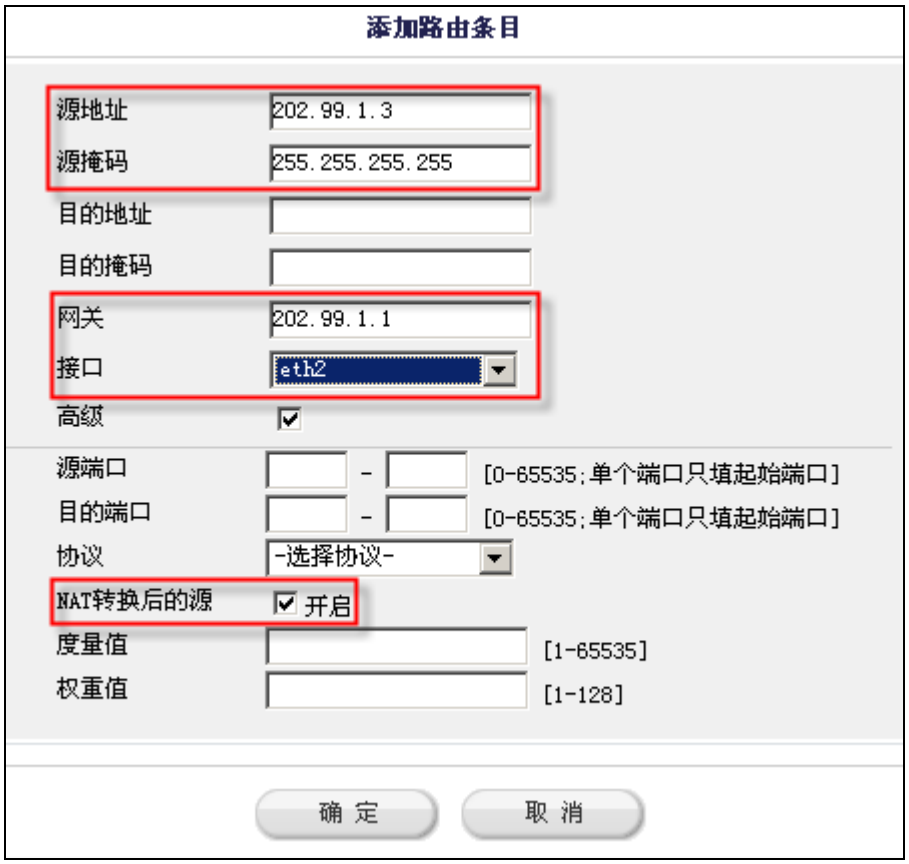
3）配置策略路由，限制从内网服务器回复的报文，电信用户使用电信出口 eth1，网通用户使用网通出口 eth2。

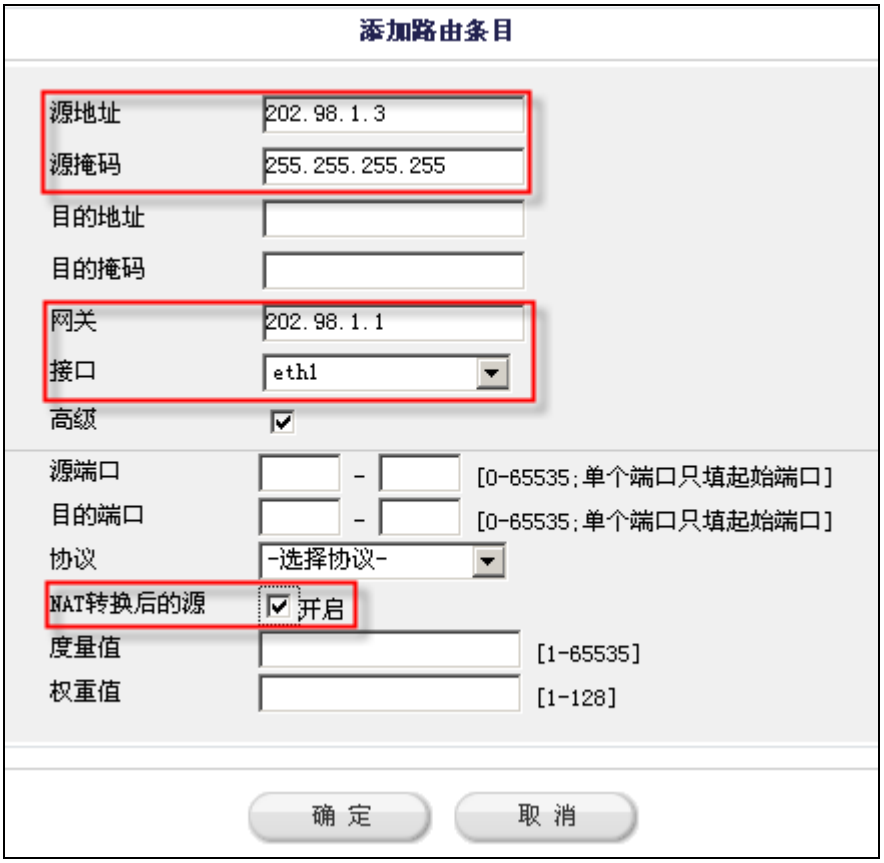
①添加策略路由并设置绑定属性

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。

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。





“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

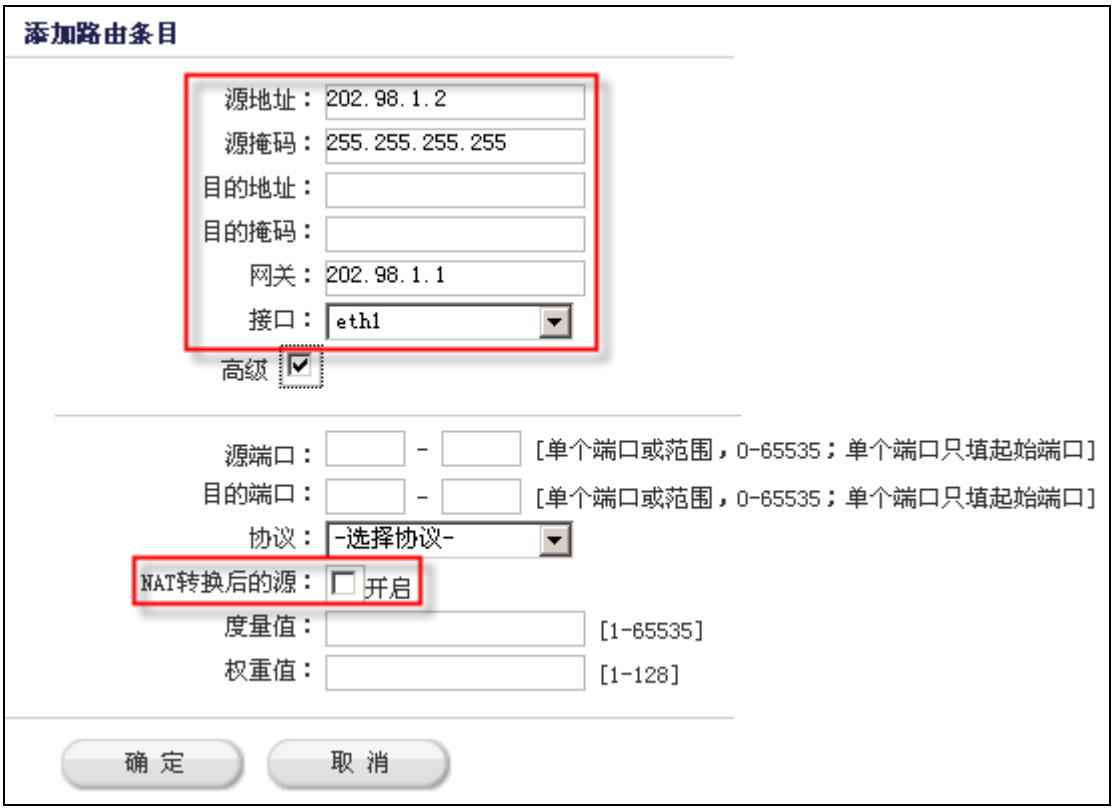
WEBUI 配置步骤

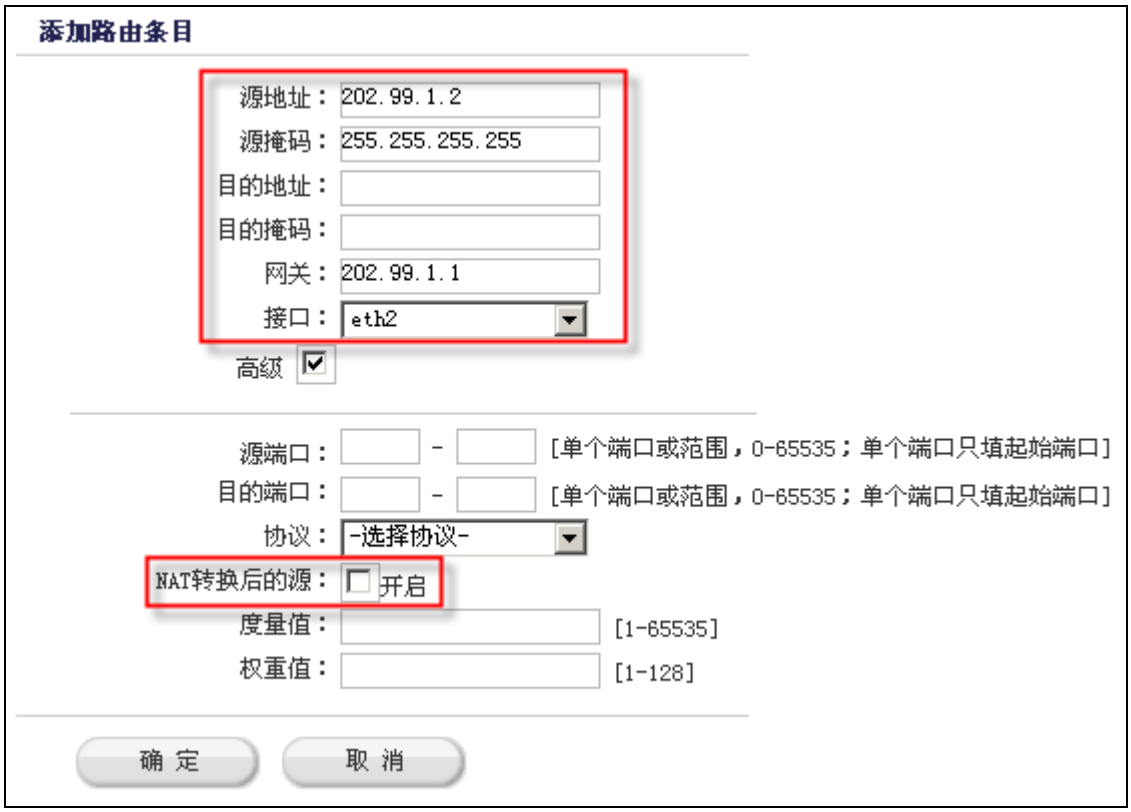
1）添加策略路由并设置绑定属性

选择 **网络管理 > 路由**，并点击“策略路由”页签，点击“添加”，如下图。

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。





“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

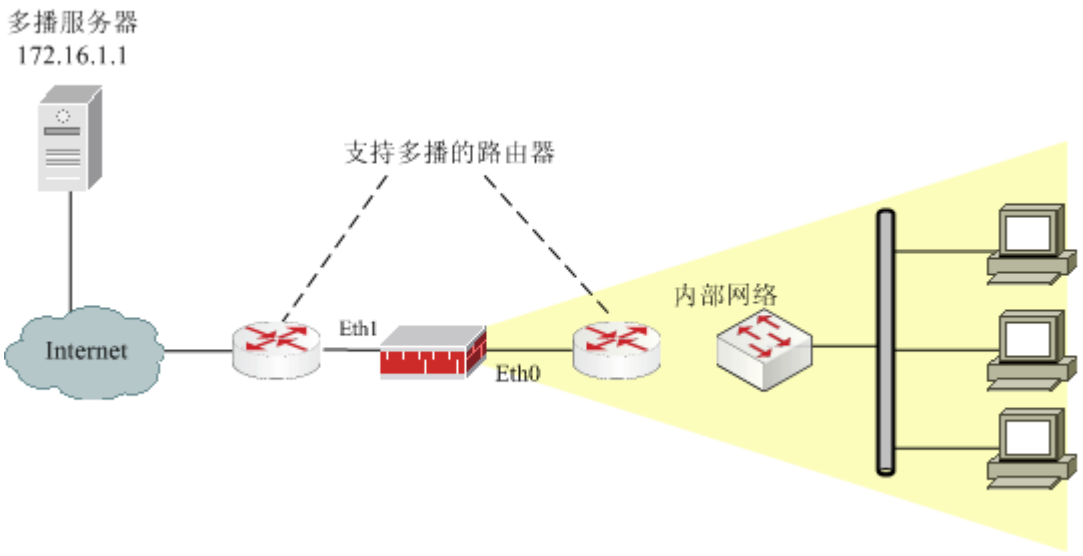


图 5 网络卫士防火墙转发多播数据包的网络示意图

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。

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

1）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。

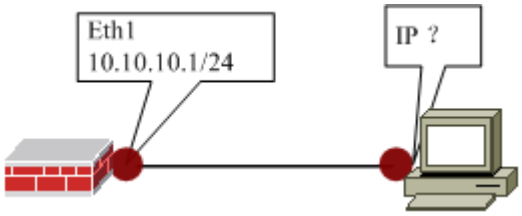


图 6 网络卫士防火墙作为 DHCP 服务器示意图

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。

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。

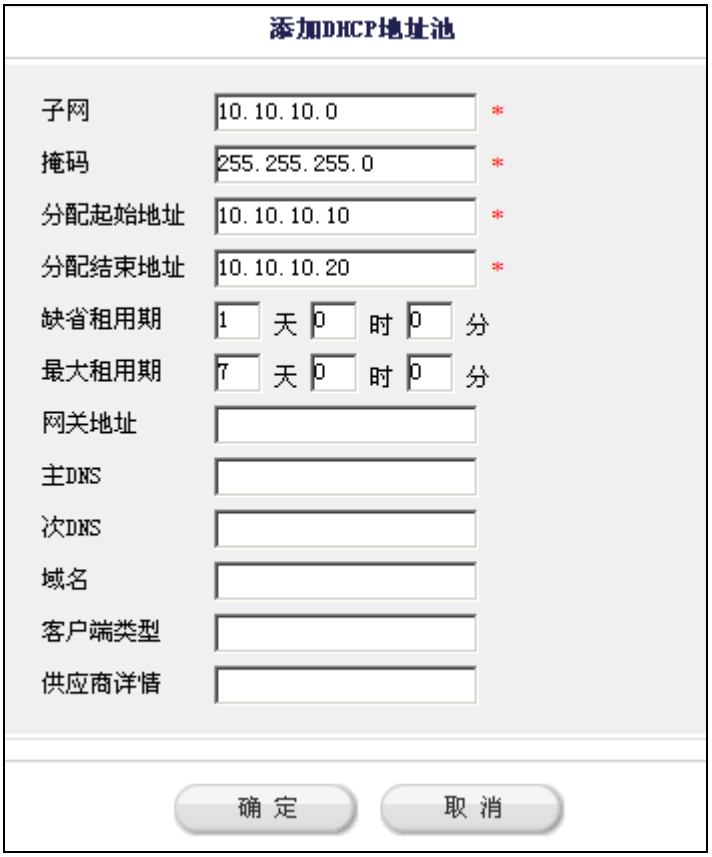
b）开放 area_eth1 区域的 DHCP 服务

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。

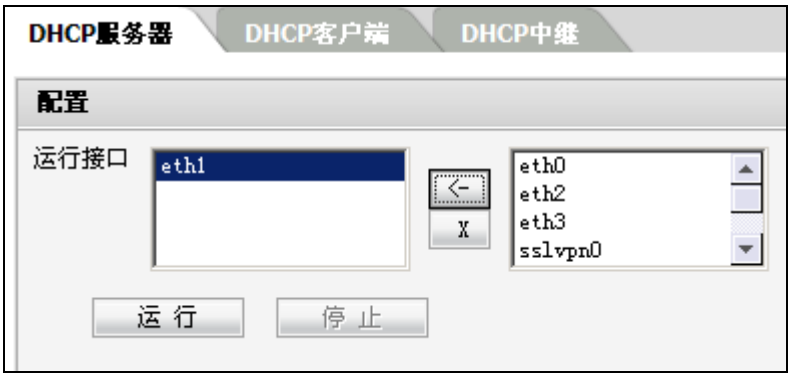
3）配置 DHCP 服务器

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。



b）在 eth1 口启动 DHCP 服务器。



点击“运行”启动 DHCP 服务器。

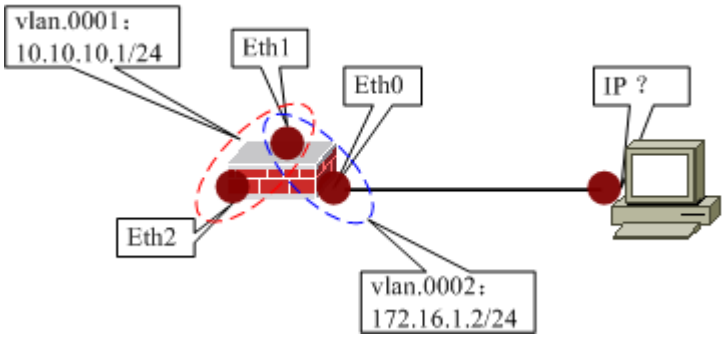
4）查看已分配地址

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。

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
  <cr>
TopsecOS.network# dhcp show binded
IP                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。

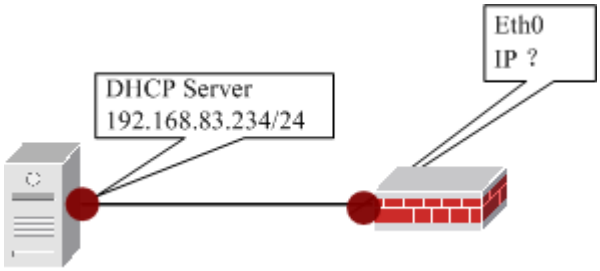


图 7 网络卫士防火墙作为 DHCP 客户端示意图

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。

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。

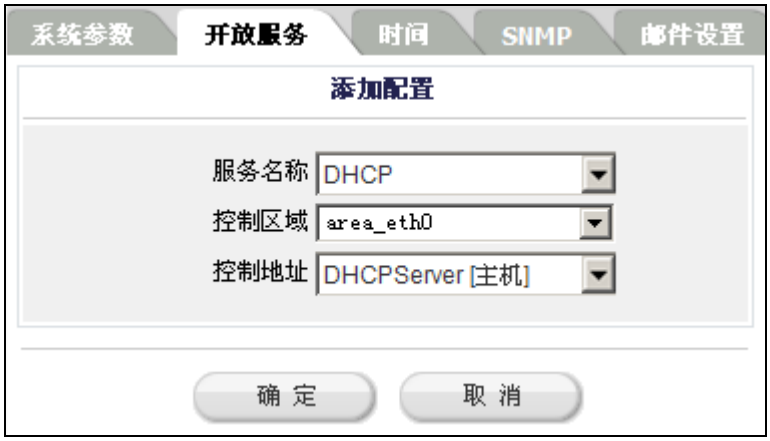
2）开放 eth0 口的 DHCP 服务

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。

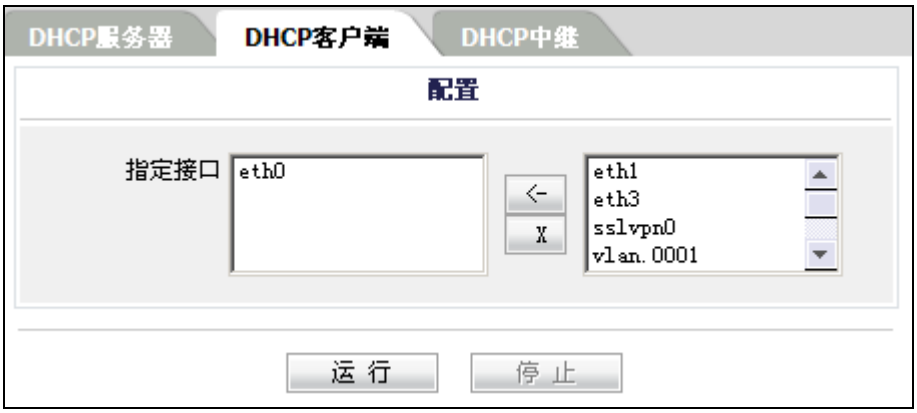
b）选择菜单 **资源管理 > 地址**，在“主机”页签点击“添加”添加 DHCP 服务器主机资源。

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。



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。



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。

```
TopsecOS# 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  Bcast:192.168.83.255  Mask:255.255.255.0 DHC
P
          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。

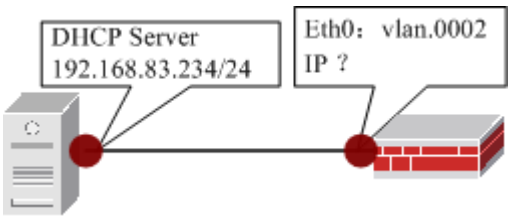
物理接口 子接口

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(dhcp)	1500	启用		全双工	100M	
eth1		路由	172.16.1.1/255.255.255.0	1500	启用		全双工	100M	
eth2		路由		1500	启用				
eth3		路由		1500	启用				

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。

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

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。

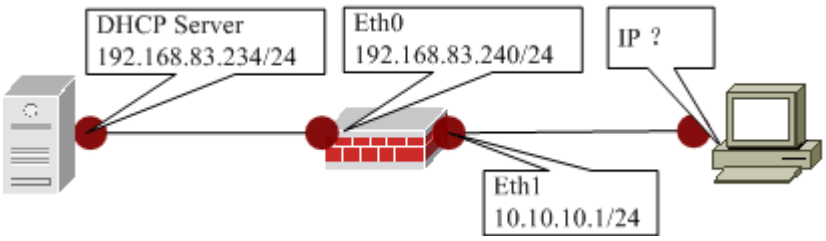


图 8 网络卫士防火墙作为 DHCP 中继示意图

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。

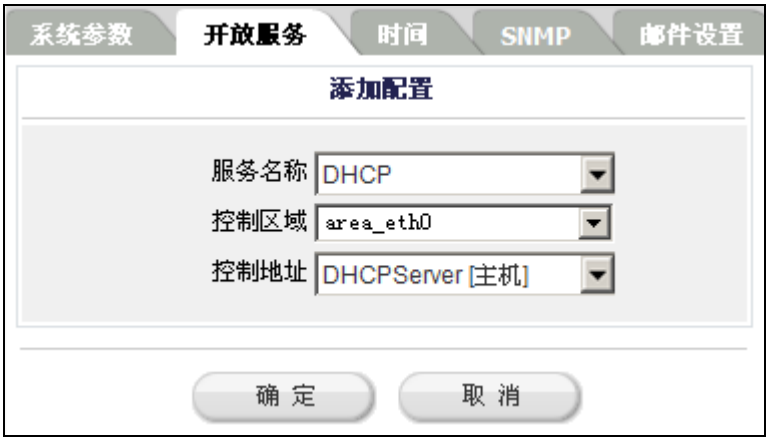
a）选择 **资源管理 > 区域** 菜单，添加 area_eth0/area_eth1 区域，并与 eth0/eth1 属性绑定。

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。

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。



开放 area_eth1 区域的 DHCP 服务，如下图。

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。

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。

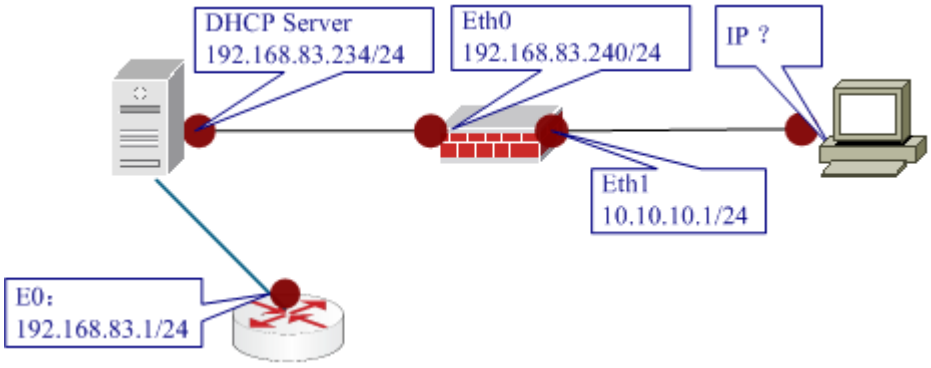
至此，网络卫士防火墙作为 DHCP 中继的配置完成。

DHCP 服务器的相关配置：

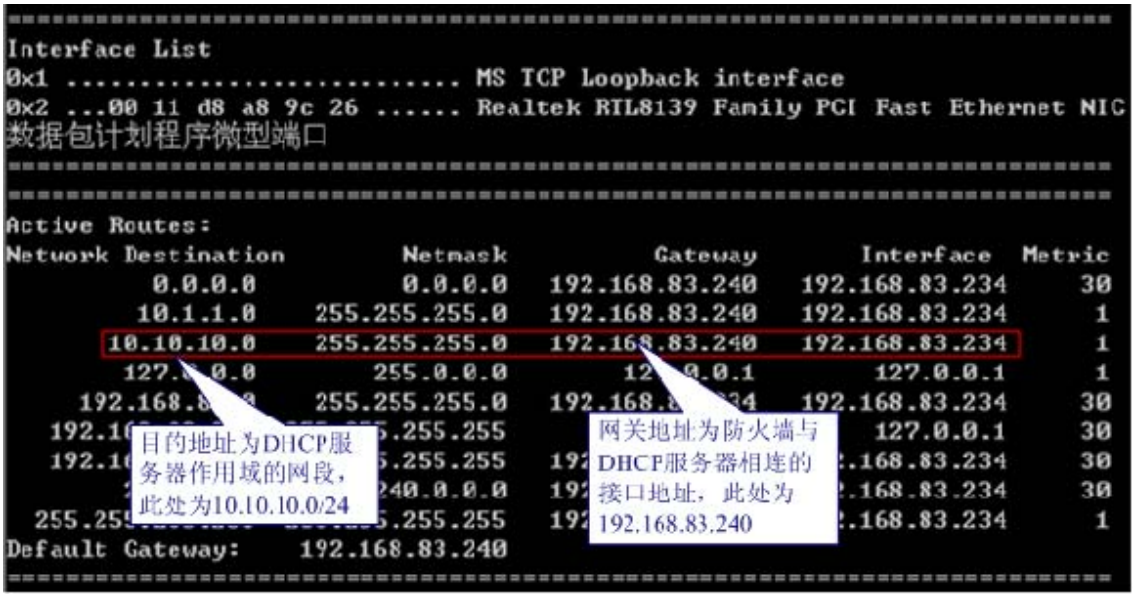
1）配置 DHCP 服务器的作用域，要与 DHCP 客户端连接的端口在同一个子网内。

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。

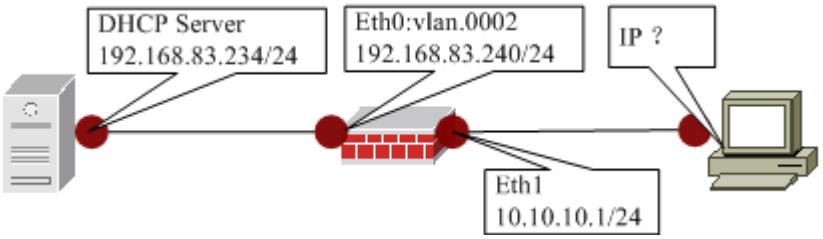


上图中，DHCP 服务器的默认网关是路由器的 E0 接口（192.168.83.1/24），这种情况下，需要在服务器的路由表里添加一条静态路由，如下图。

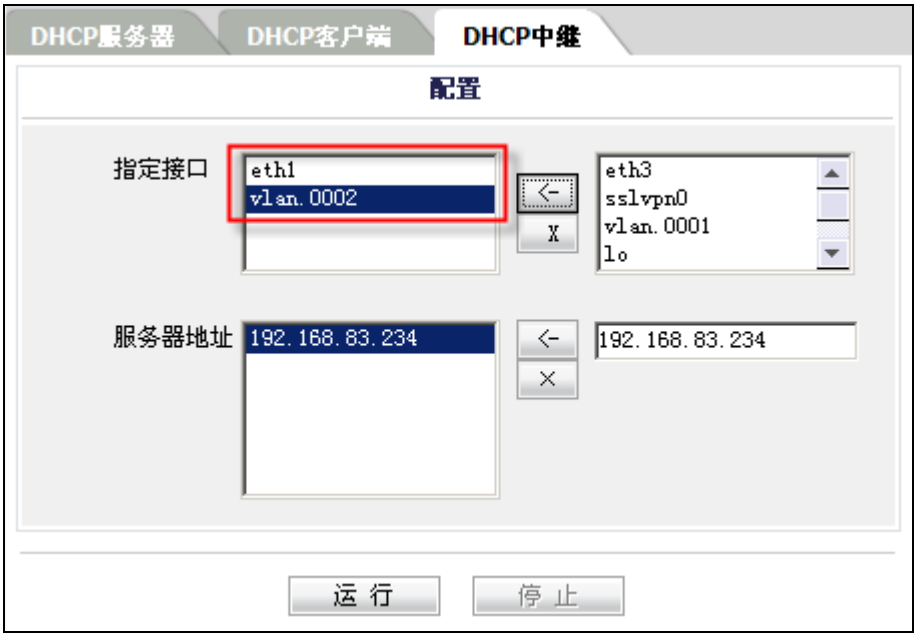


注意事项

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。



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。

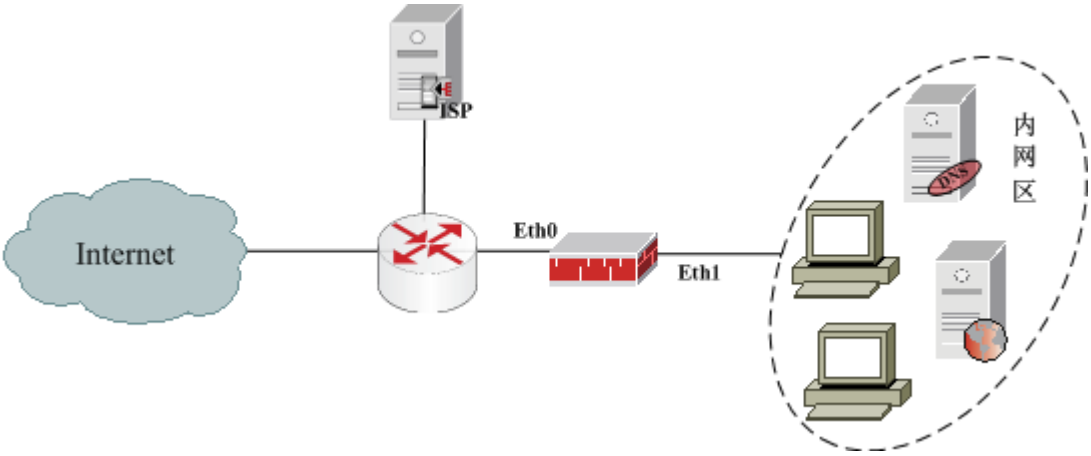


图 9 内网通过 ADSL 拨号与外网建立链路示意图

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

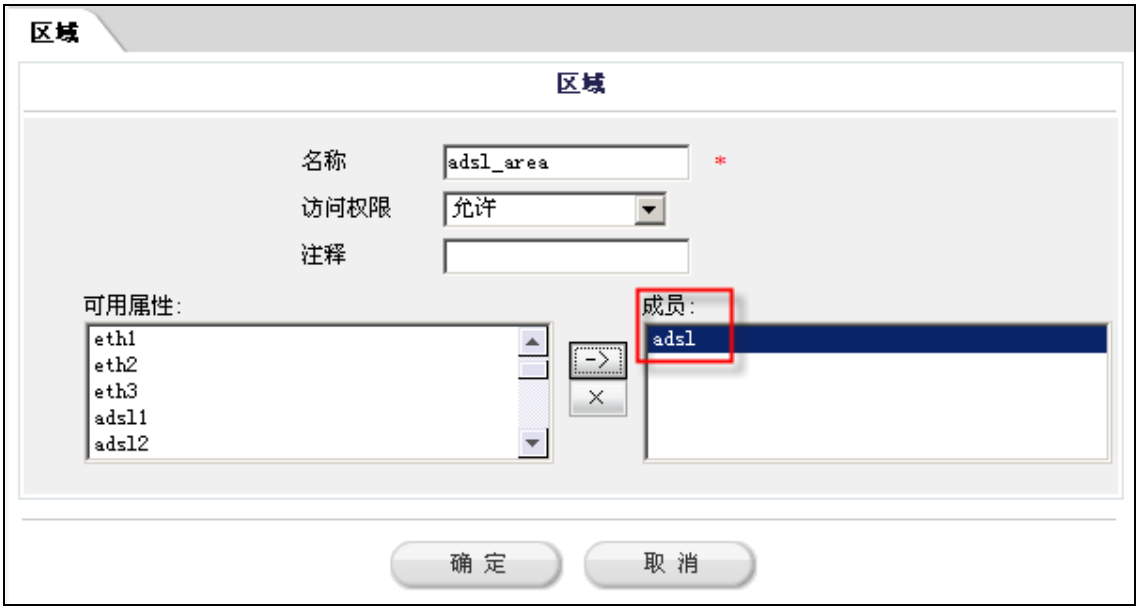
选择 **网络管理 > 接入**，并选择“ADSL”页签，如下图所示。

点击“设置属性”按钮设置 ADSL 拨号参数，如下图。

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”。



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。

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		
adsl1		未连接								
adsl2		未连接								
adsl3		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 | 动态路由RIP | 动态路由BGP | 多播路由 | 动态多播PIM-

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 总计：13

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	lo	-	-
10.1.10.1/32	0.0.0.0	ULi	1	1	lo	-	-
192.168.83.237/32	0.0.0.0	ULi	1	1	lo	-	-
10.10.10.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.67.15.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.0.0.1/32	0.0.0.0	UCi	10	1	ppp0	-	-
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	sslvpn0	-	-
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	-	
0.0.0.0/0	10.0.0.1	UGSi	1	1	ppp0	-	

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 | 动态路由BGP | 多播路由 | 动态多播PIM-

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 总计：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	lo	-	-
10.1.10.1/32	0.0.0.0	ULi	1	1	lo	-	-
192.168.83.237/32	0.0.0.0	ULi	1	1	lo	-	-
10.10.10.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.67.15.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.0.0.1/32	0.0.0.0	UCi	10	1	ppp0	-	-
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	sslvpn0	-	-
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	-	
0.0.0.0/0	10.0.0.1	UGSi	1	1	ppp0	-	
0.0.0.0/0	192.168.83.1	UGSi	1	1	eth0	-	

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。

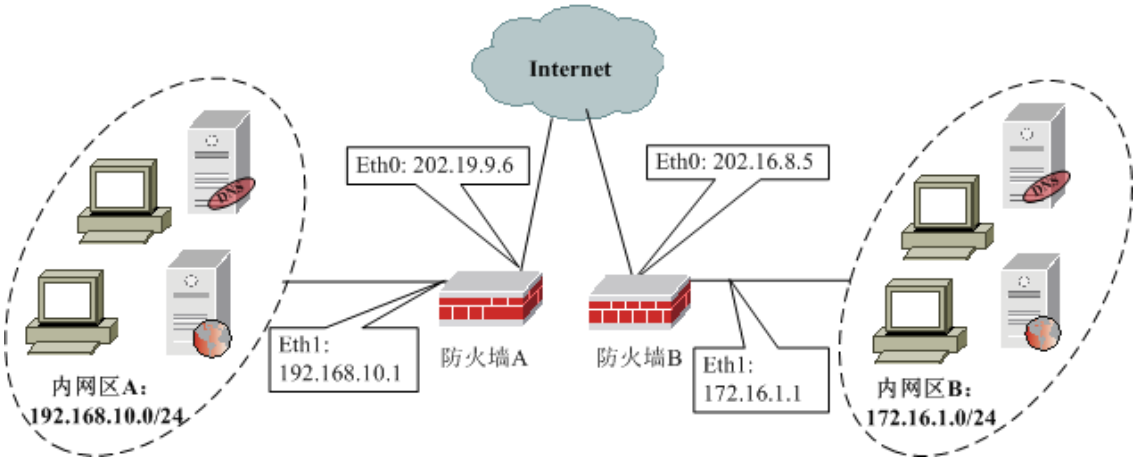


图 10 内网区域之间通过 GRE 隧道建立连接示意图

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

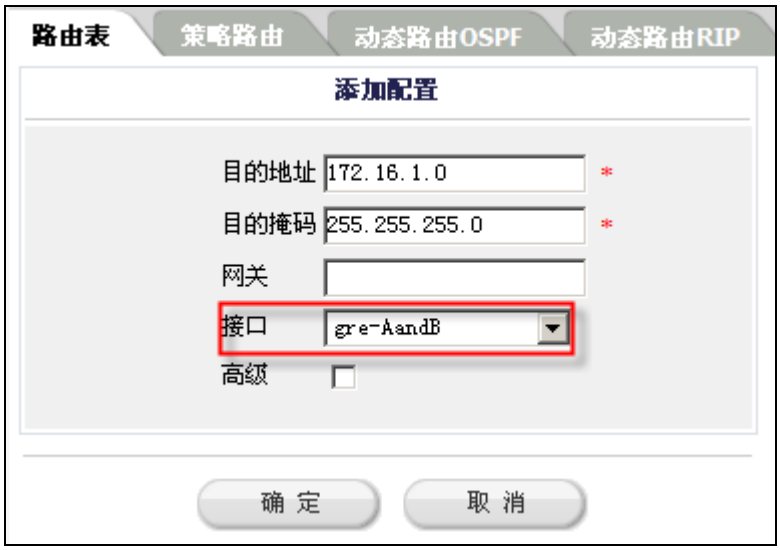
网络卫士防火墙 A 上相关配置

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

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。

2）在上图中点击“接口属性”设置 GRE 虚接口的属性。

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。



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。

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。

2）在上图中点击“接口属性”设置 GRE 虚接口的属性。

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。

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。

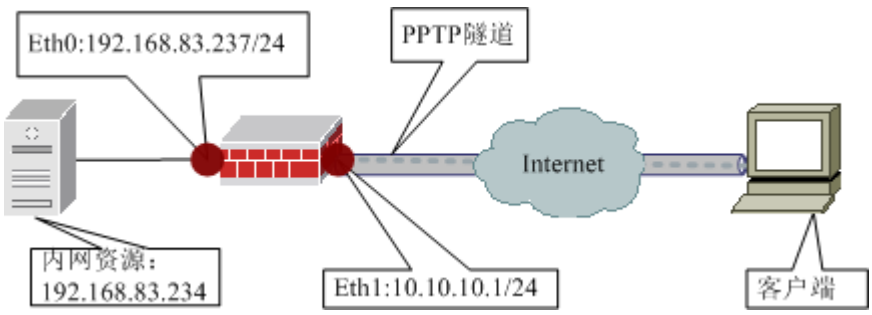


图 11 远程用户通过 PPTP 隧道访问内网示意图

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。

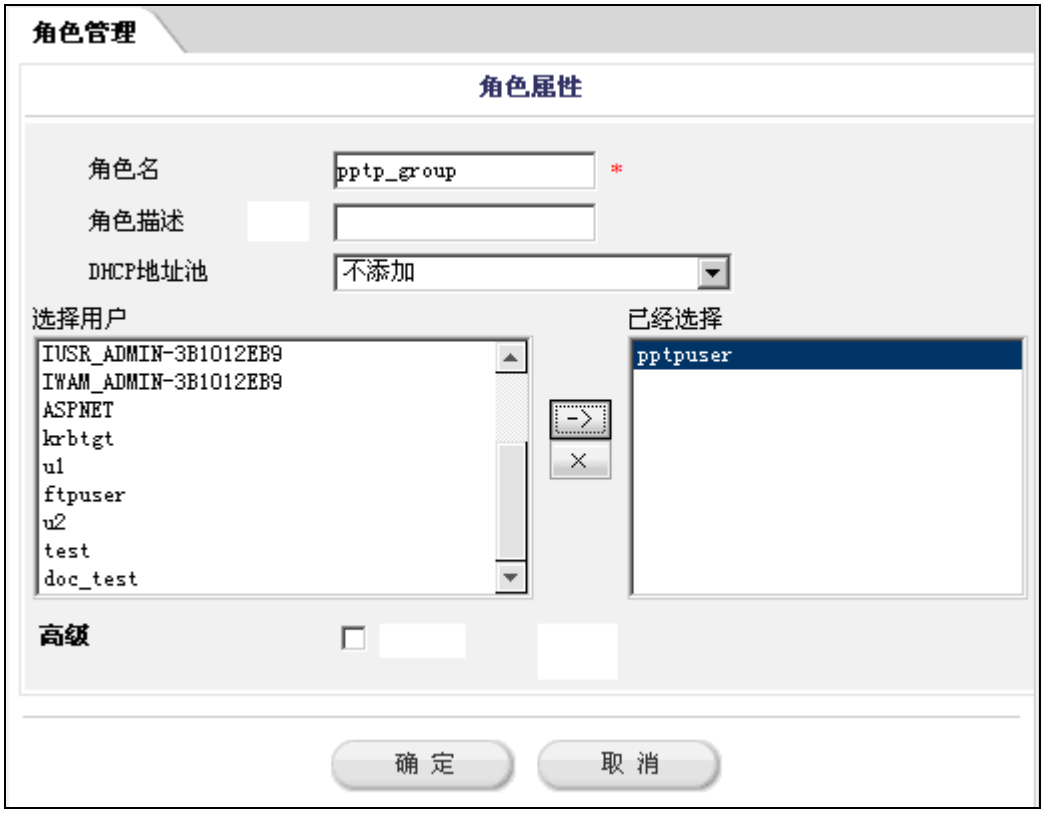
选择 **资源管理 > 区域**，设置区域属性。

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”。

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。



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。

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。

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。

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。

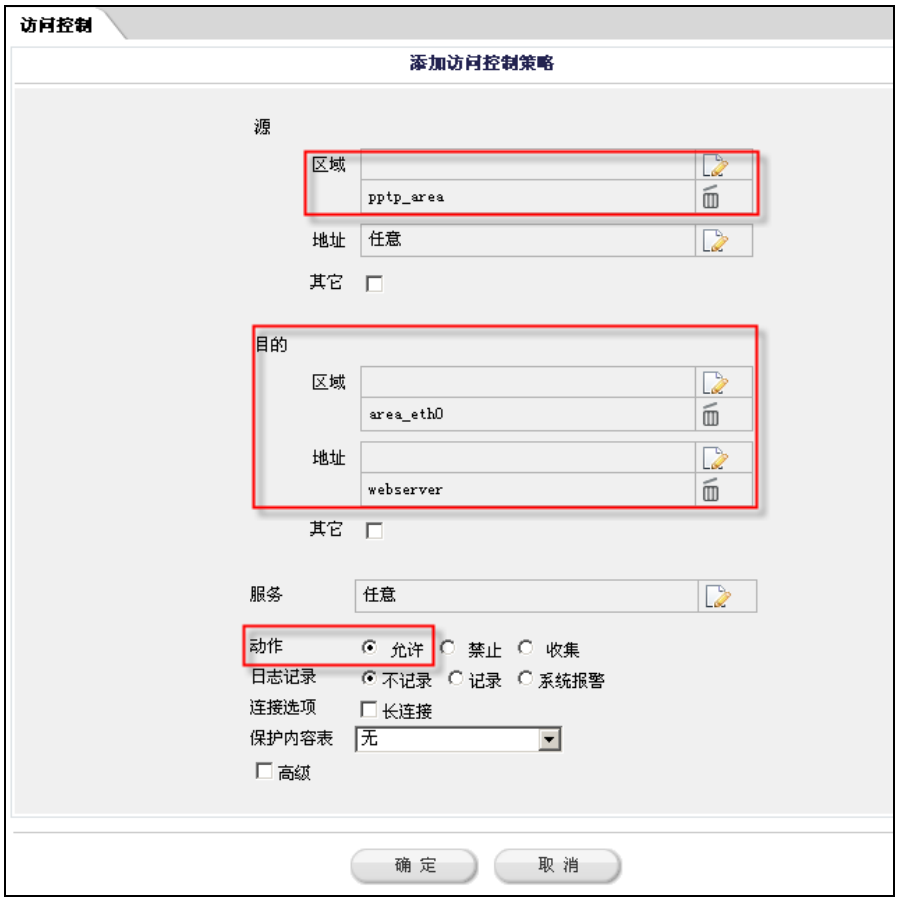
通过对 PPTP 区域的控制完成访问控制。

a）选择 **资源管理 > 区域**，添加区域 pptp_area。

pptp_area 区域可以作为源或目的区域在访问控制规则中使用。

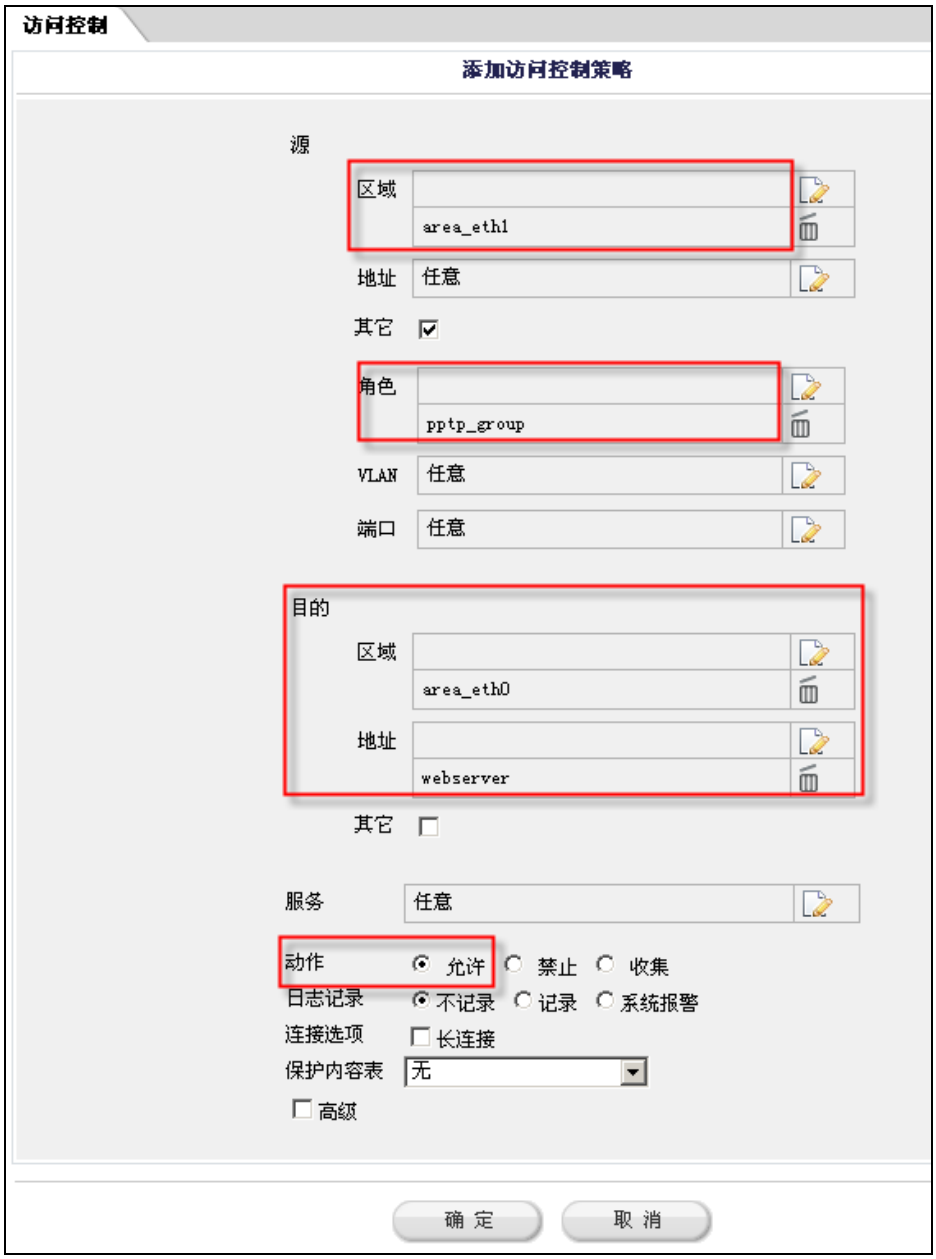
“pptp”属性是 PPTP 的动态属性，不需要用户设置，用户只需要设置该属性绑定的区域即可。

b）选择 **防火墙 > 访问控制**，点击“添加策略”设置访问控制规则。



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。

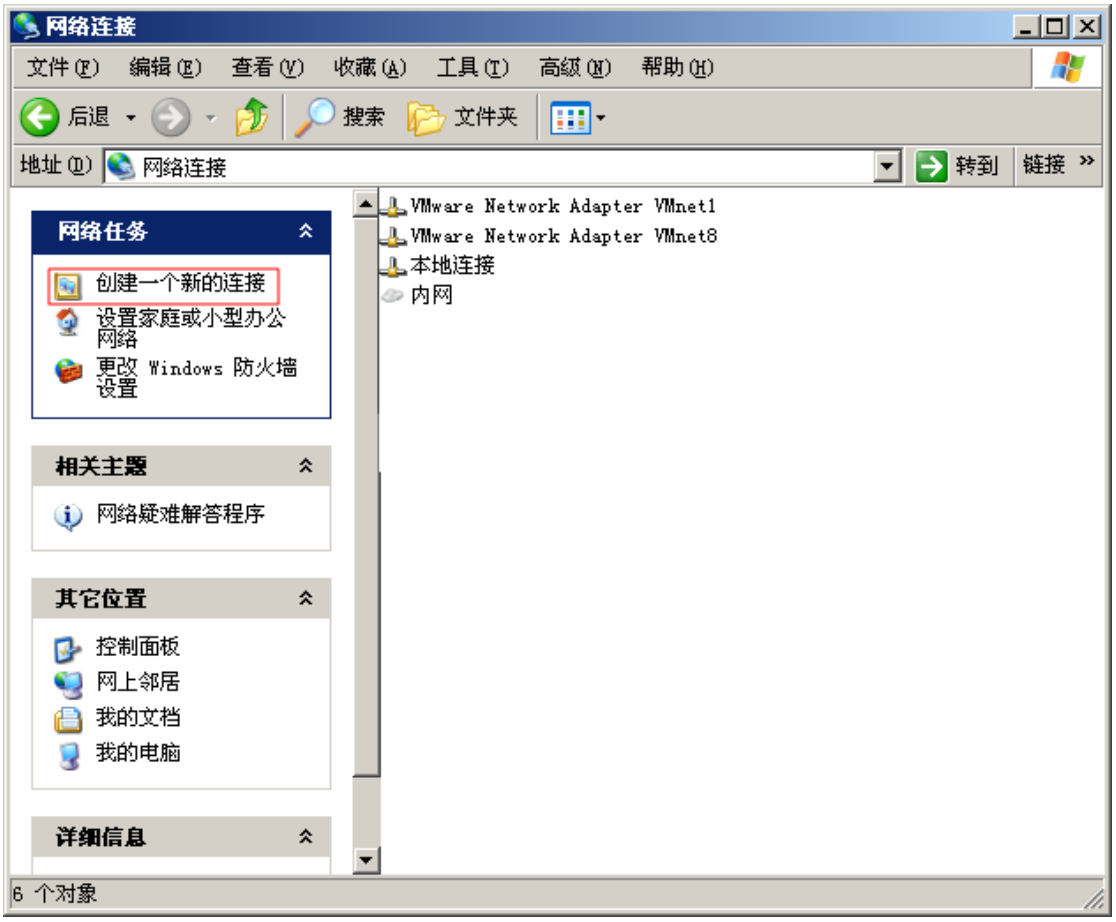


其他的设置与基于区域的访问控制规则相同。

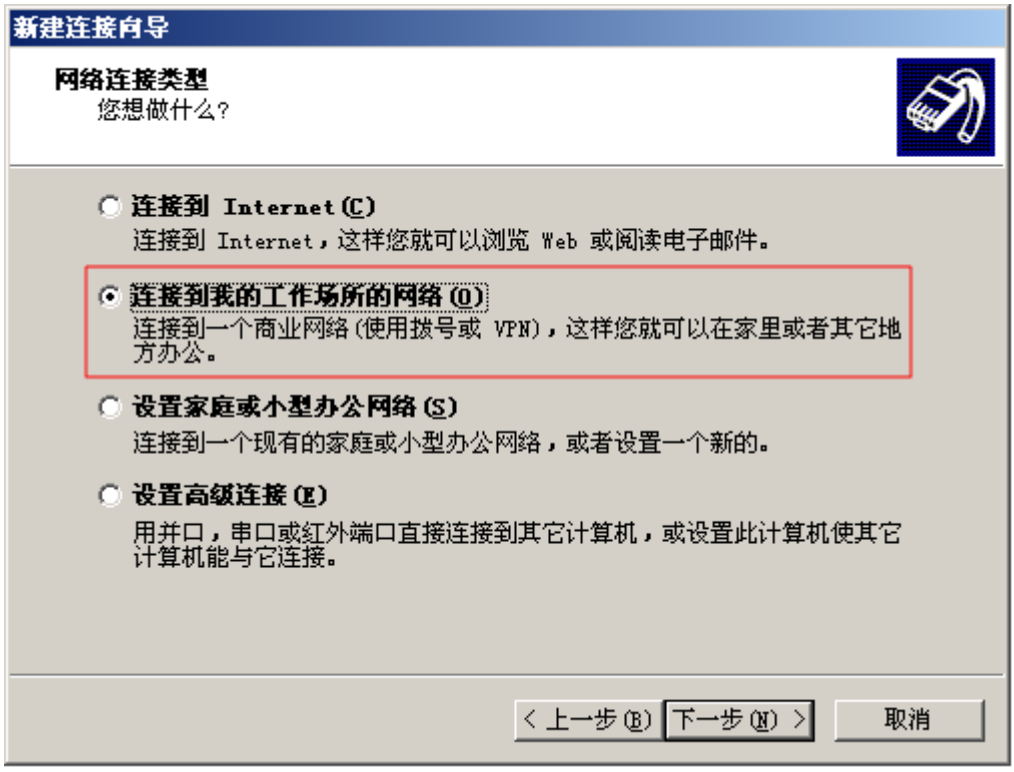
7）配置 PPTP 客户端（以 windows 2000 为例）

需要确认 PPTP 客户端可以访问网络卫士防火墙的 eth1 接口。

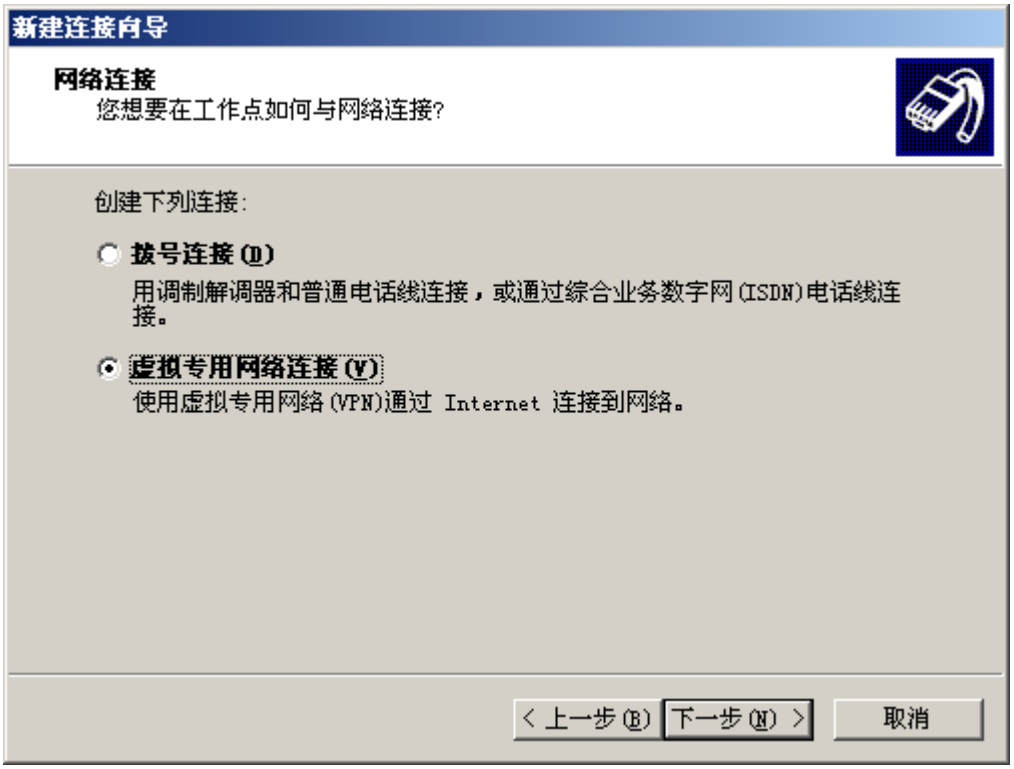
a）在控制面板中打开网络连接



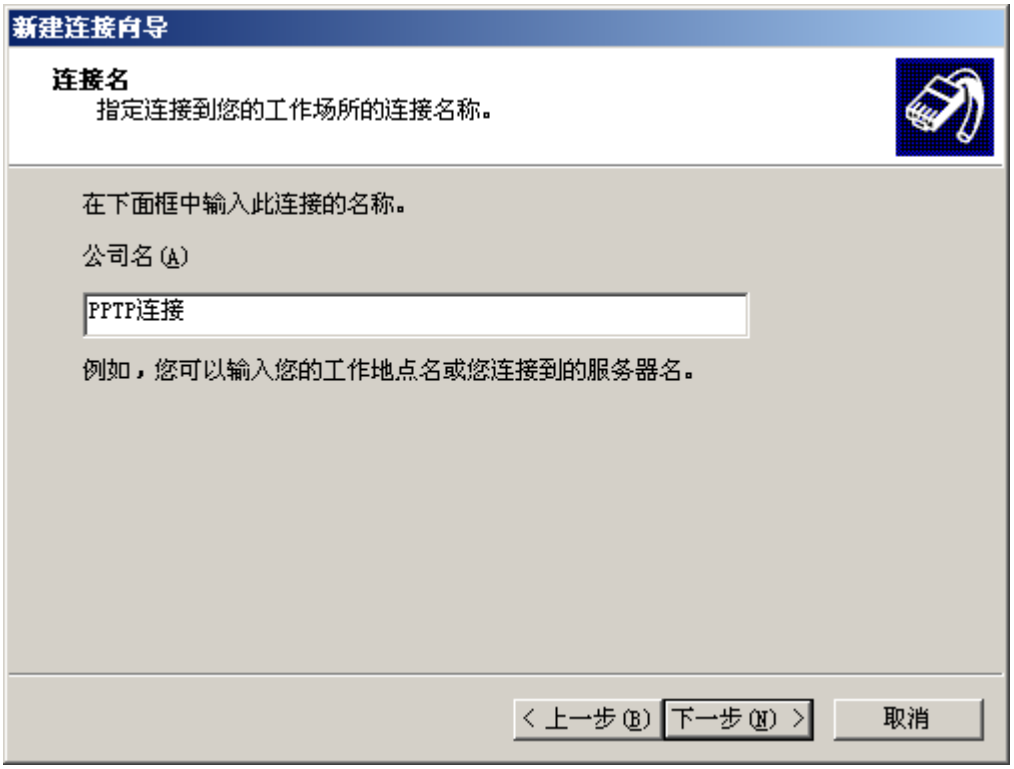
b）点击“创建一个新连接”，新建一个连接（VPN）。



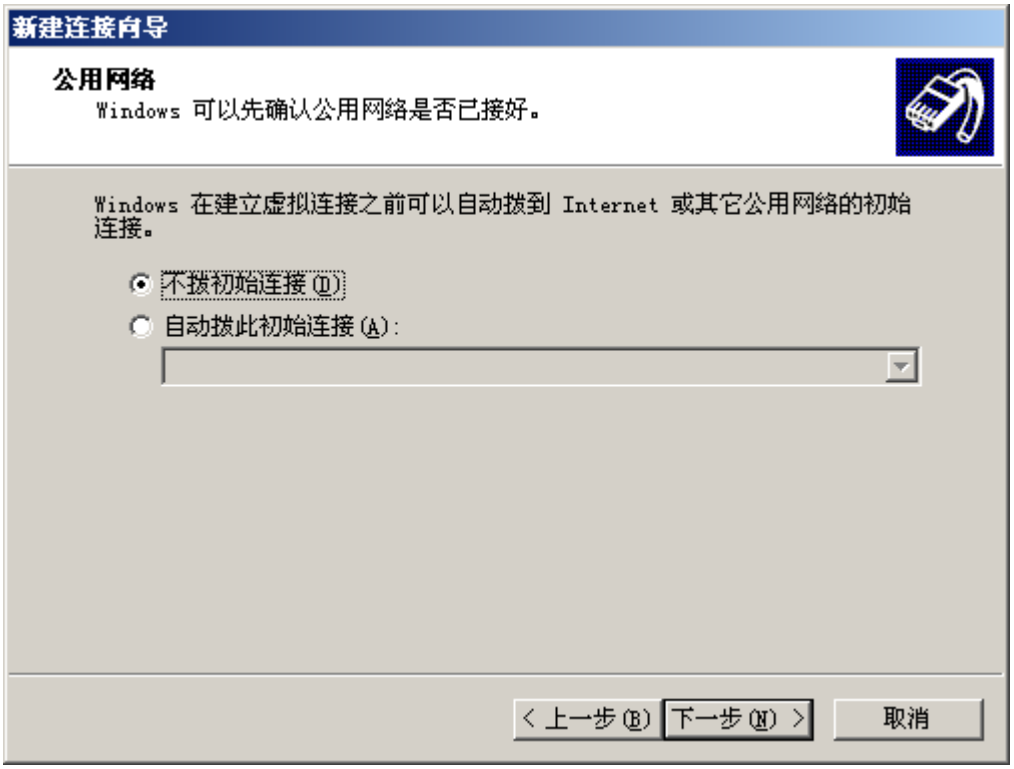
c）选择网络连接类型为“连接到我的工作场所的网络”。



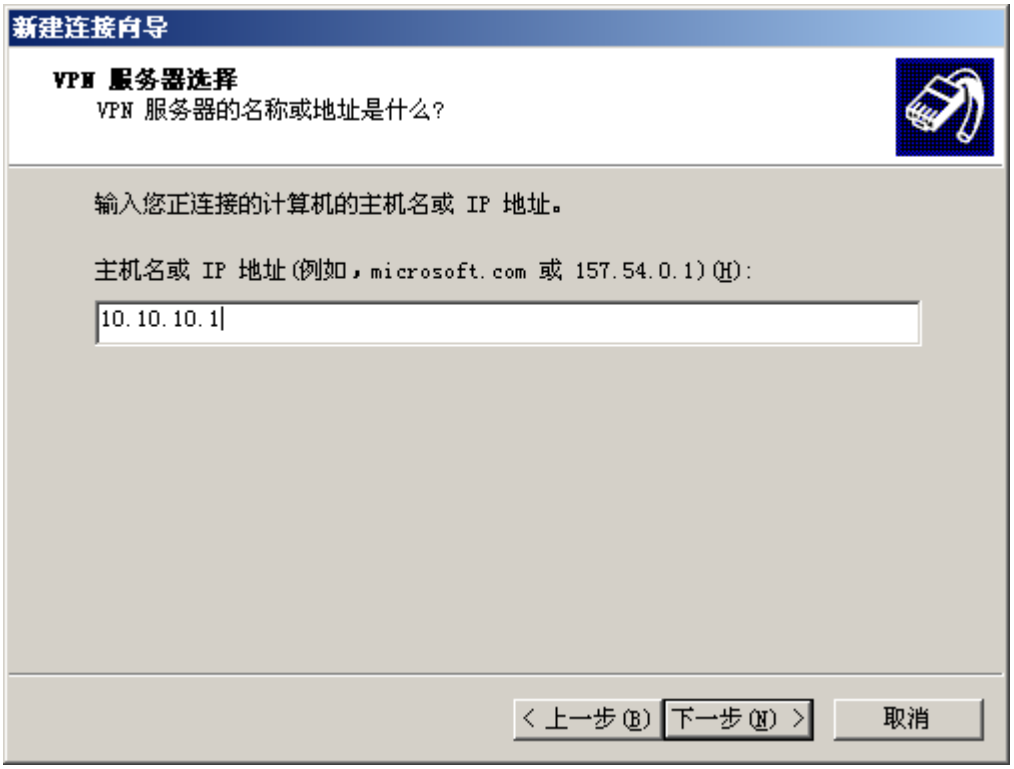
d）选择创建“虚拟专用网络连接”。



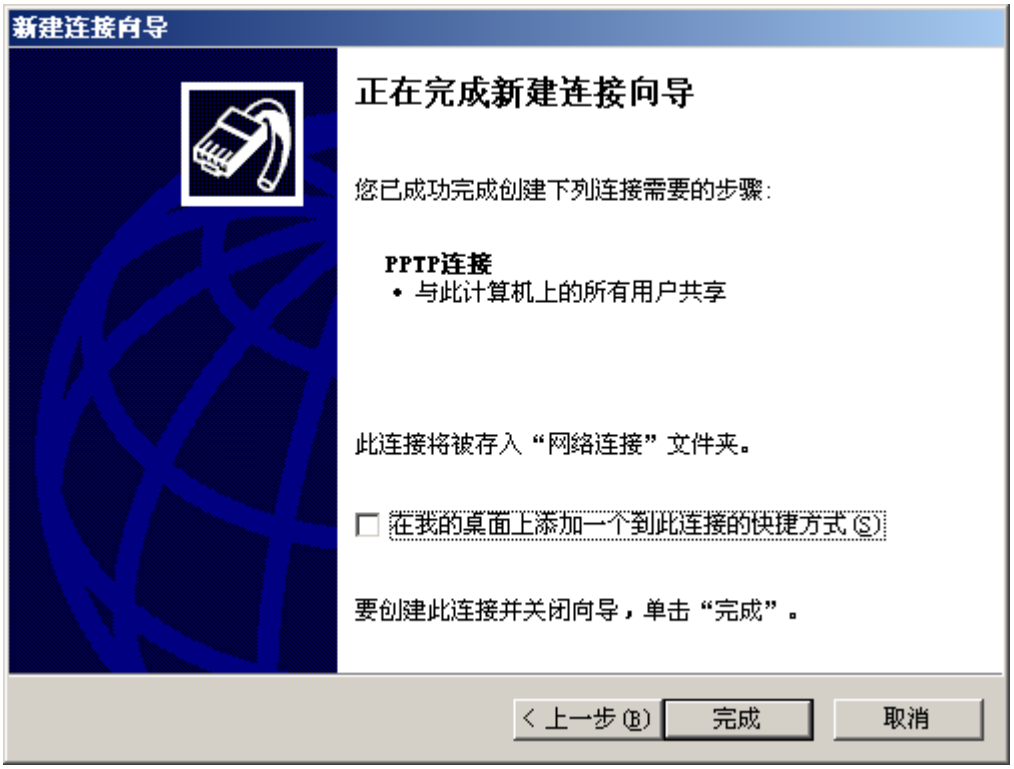
e）输入为此 VPN 连接定义的名字（例如 PPTP 连接）。



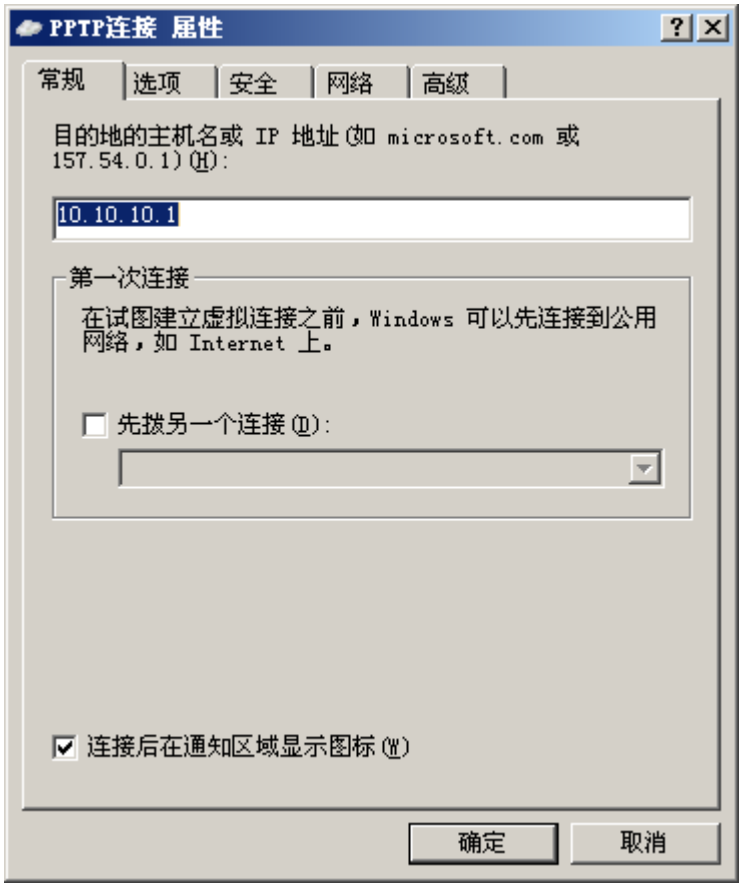
f）如果在拨 VPN 之前需要拨公网，可以选择是拨 VPN 同时自动启动公网连接还是先连接公网以后，再进行 VPN 连接。



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。

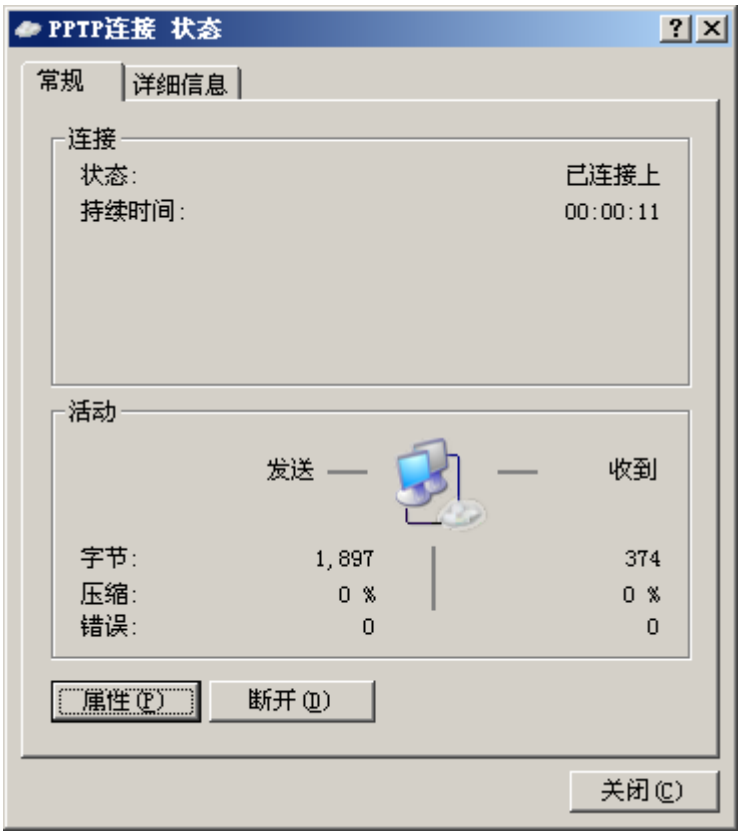

PPTP连接 属性
常规
选项
安全
网络
高级
目的地的主机名或 IP 地址(如 microsoft.com 或 157.54.0.1)(H):
10.10.10.1
第一次连接
在试图建立虚拟连接之前，Windows 可以先连接到公用网络，如 Internet 上。
先拨另一个连接(D):
连接后在通知区域显示图标(W)
确定
取消


PPTP连接 属性
常规
选项
安全
网络
高级
VPN 类型(E):
PPTP VPN
设置(S)
VPN连接类型为PPTP
此连接使用下列项目(
Network Monitor Driver
Internet 协议 (TCP/IP)
QoS 数据包计划程序
Microsoft 网络的文件和打印机共享
VMware Bridge Protocol
安装(N)...
卸载(U)
属性(R)
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。
确定
取消

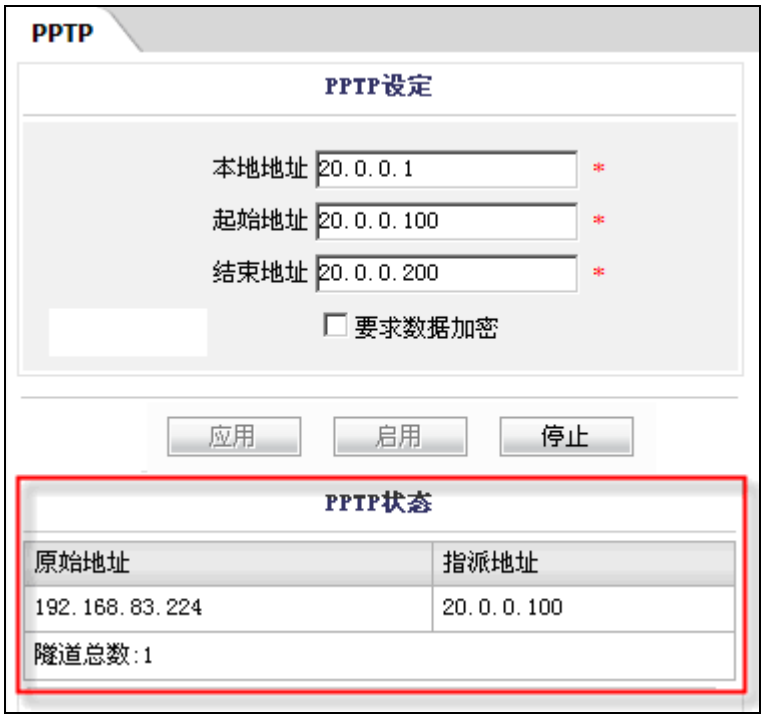
8）建立 PPTP VPN 隧道

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。

连接成功后如下图。



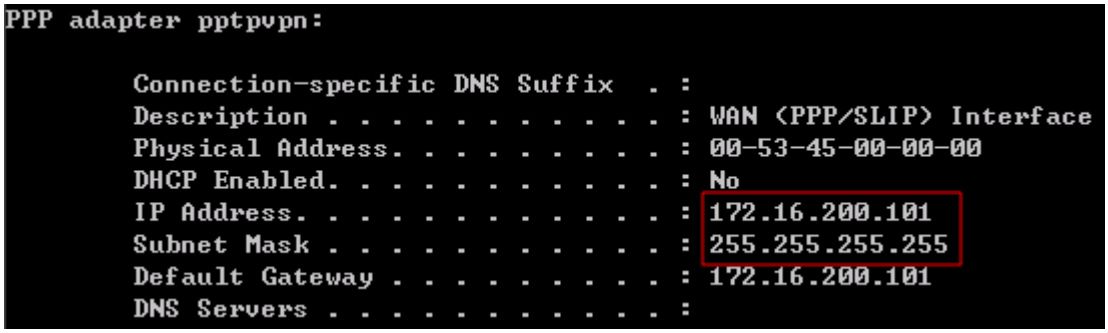
9）网络卫士防火墙上可以通过 **虚拟专网 > PPTP** 来查看已建立 PPTP 隧道的客户端状态。



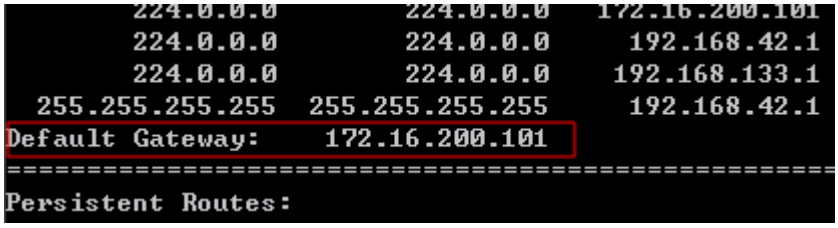
管理员可以通过选择 **用户管理 > 用户认证**，并激活“在线用户”页签查看当前在线用户。

注意事项

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



2）客户端（win2000）可用 route print 查看本地路由表。

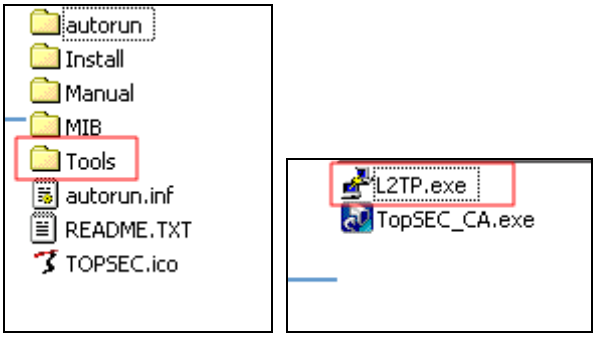


3）PPTP 设定的“本地地址”、“起始地址”与“结束地址”不要使用任何已用的 IP。

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。

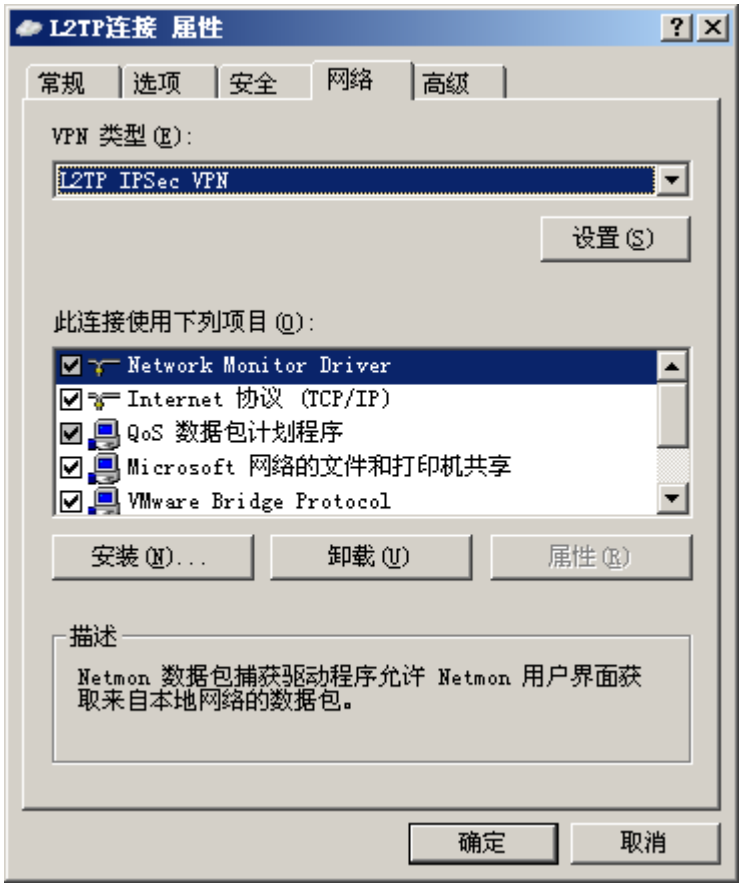


安装该程序后，必须重启系统才可以生效。

运行该程序，如下图。

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。



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。

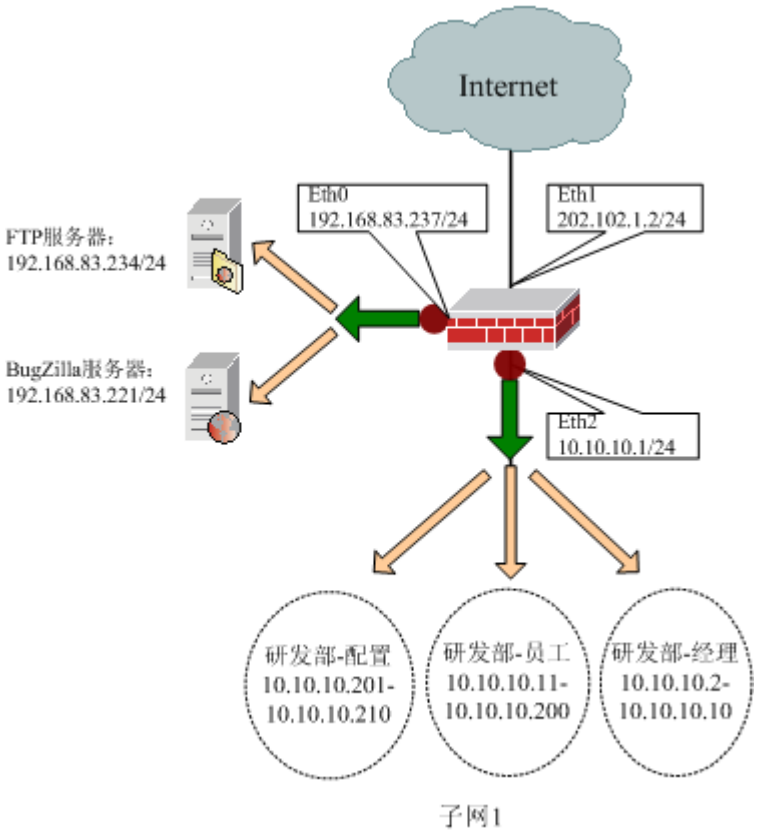


图 12 网络卫士防火墙分层带宽管理示意图

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。用户可以根据自己的需求，通过 **资源管理 > 时间** 进行设置。

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。

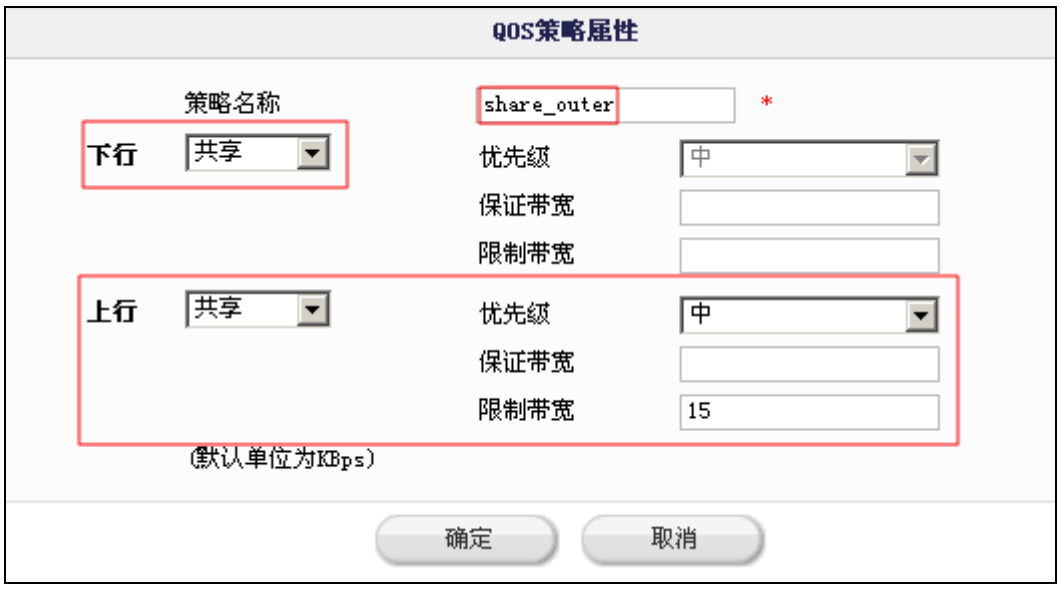
C）设置 FTP 服务器和 BugZilla 服务器

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。

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。



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。

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。

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；

需要注意的是：每个 QoS 对象中保证带宽不能大于限制带宽。

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。

B）配置 ACL 规则引用 QoS 对象。

“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。

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。

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。

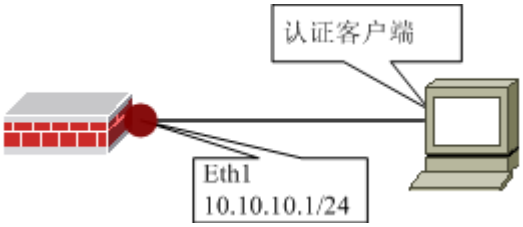


图 13 认证示意图

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

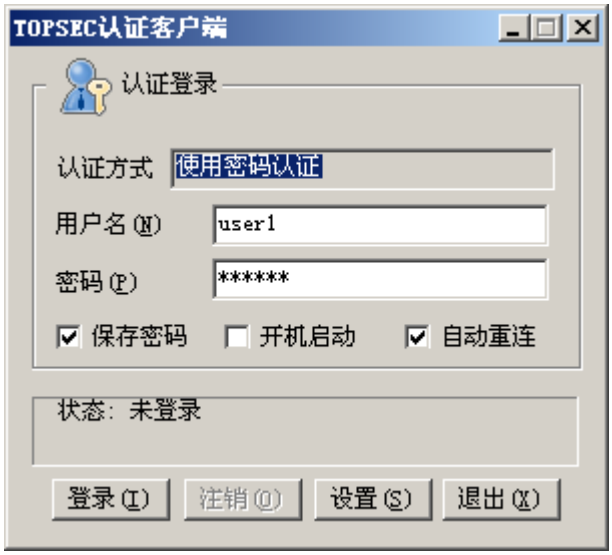
选择 **系统管理 > 配置** 菜单，在“开放服务”页签点击“添加”开放 AUTH 服务。

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。

3）验证

a）在主机 A 运行 TopSEC 认证客户端，界面如下图。

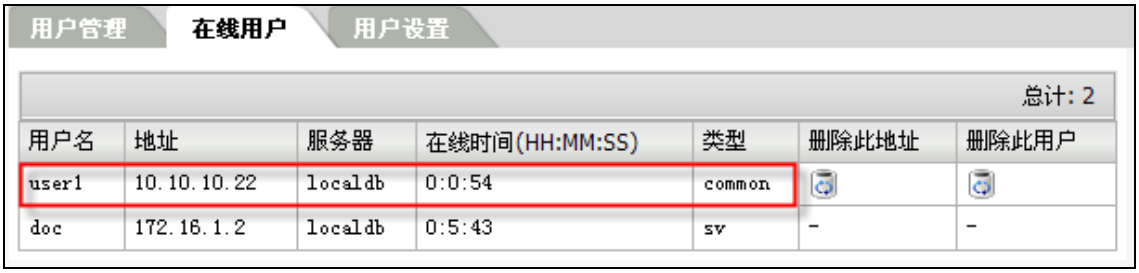


b）点击“设置”，输入防火墙的接口 IP。

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。

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。



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。

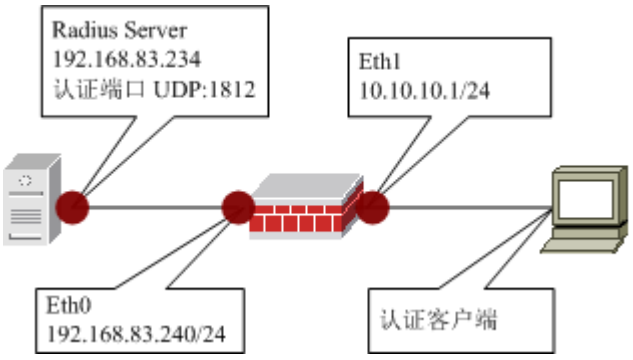


图 14 RADIUS 身份认证网络示意图

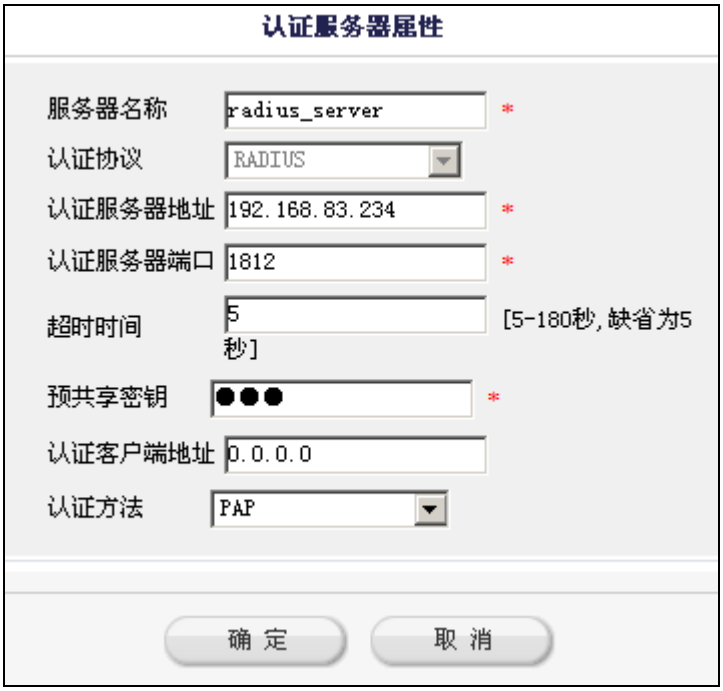
配置要点

- 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。



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。

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。

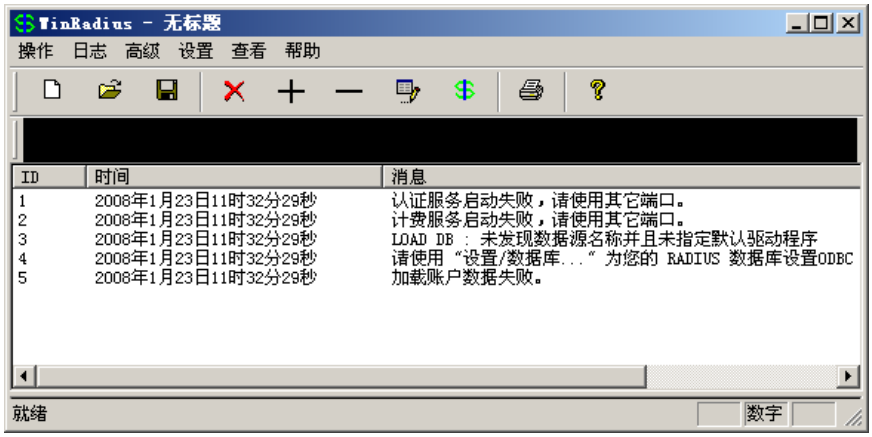
4）设置映射策略。

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。

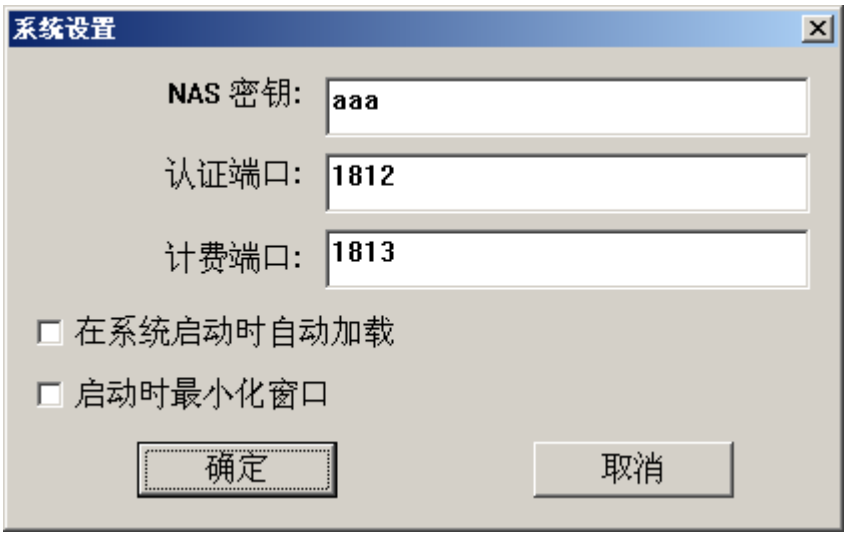
5）Radius 服务器的相关设置。

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。

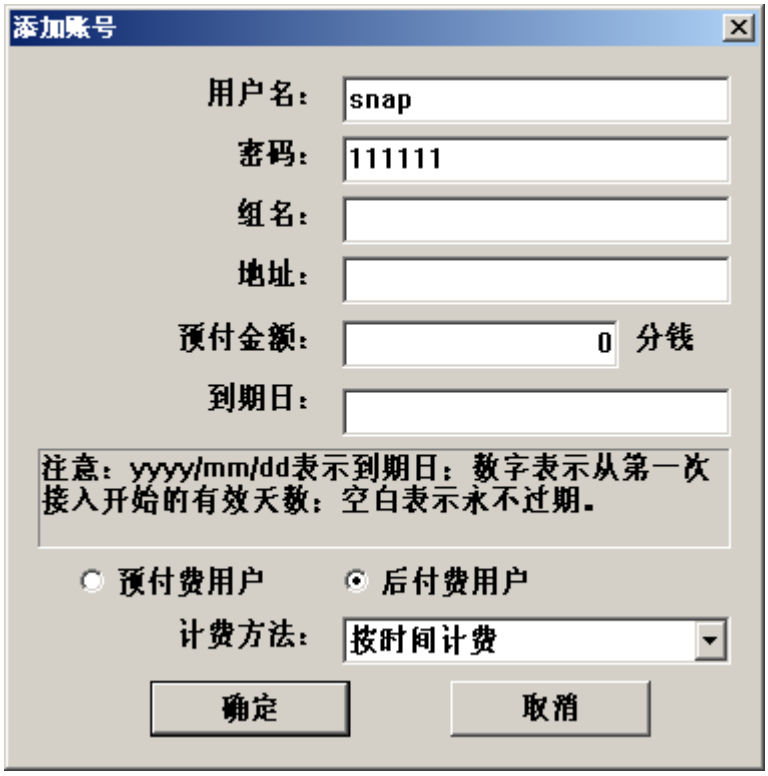


b）选择 **设置** > **系统**，弹出如下窗口。



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。



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		
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。

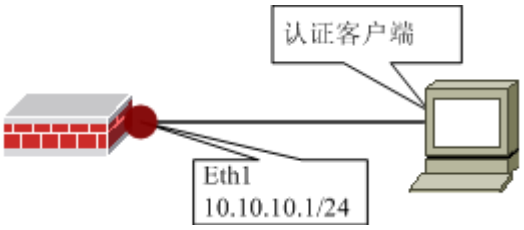


图 15 采用证书认证网络示意图

配置要点

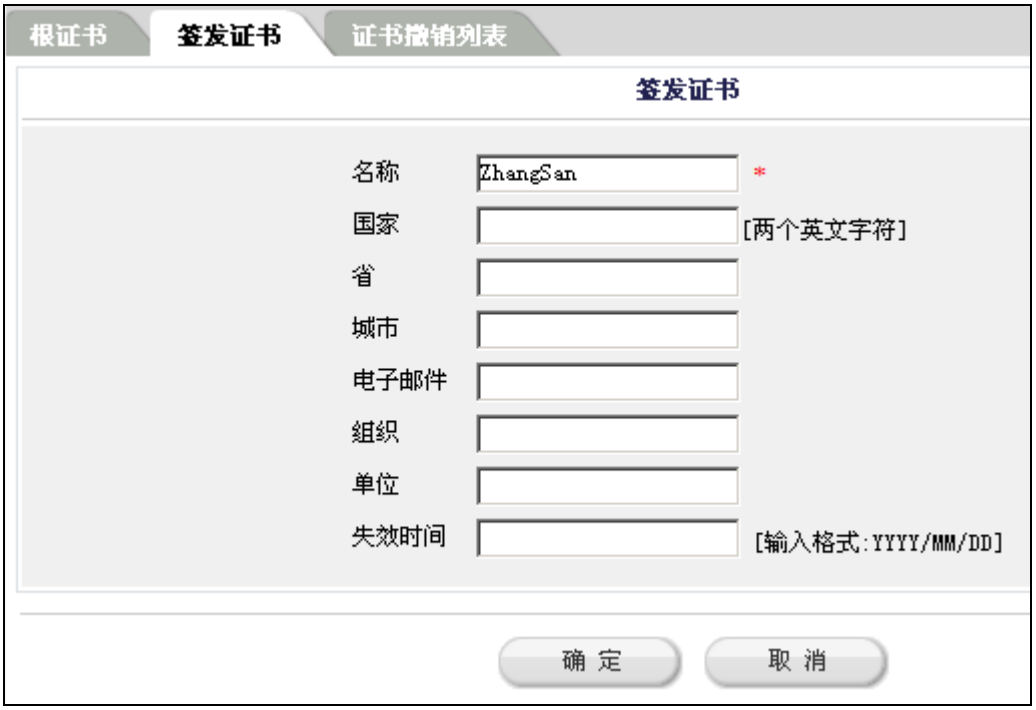
- 内置 CA 为客户端颁发证书
- 设置认证用户角色
- 设置映射关系，将证书用户按照某个属性映射到 LocalDB 的角色上。
- 开放相关接口的认证服务

- 设置认证客户端软件

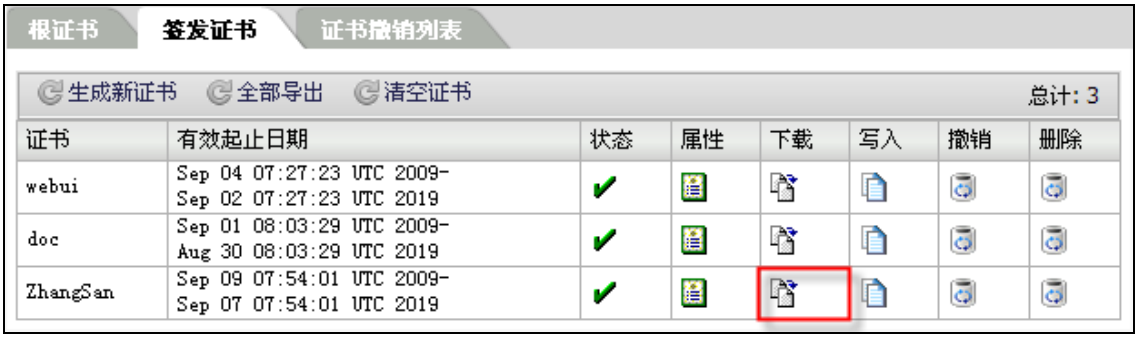
WEBUI 配置步骤

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。



生成后界面如下图所示。



b）下载证书

点击“下载”图标，界面如下图。

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。

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。

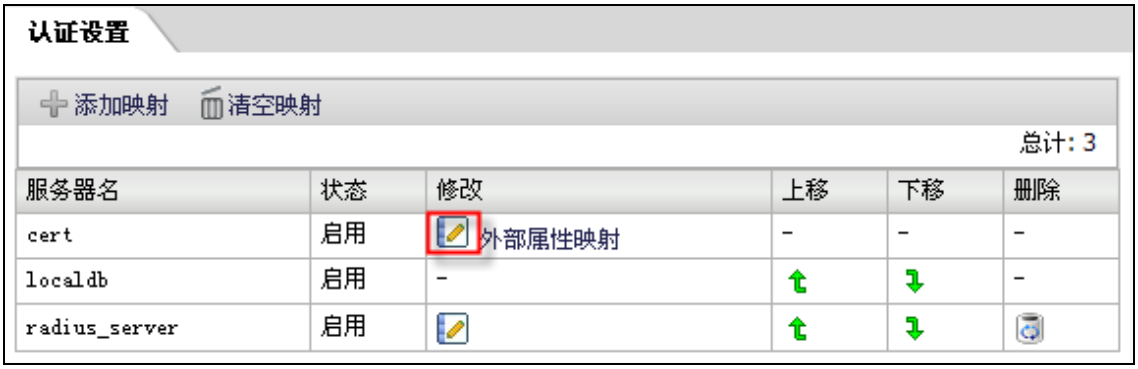
选择 **用户认证 > 角色管理**， 点击“添加角色”添加证书认证用户对应的角色，用于证书认证权限映射，基于角色进行权限控制。

说明：

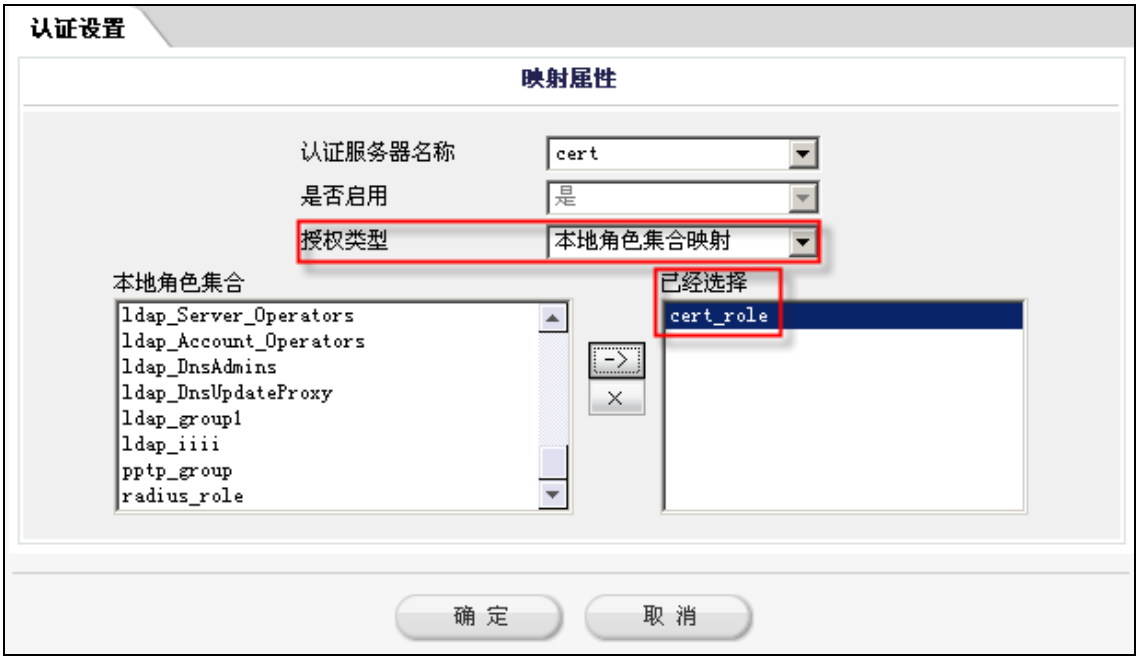
如果认证客户端为 VRC 客户端，而且管理员设置“证书权限控制”和“验证控制证书权限”均为“OFF”时（选择菜单 **虚拟专网 > VRC 管理**，并点击“基本设置”页签），将对 VRC 用户授权默认权限，无需设置本地用户角色。

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。



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。



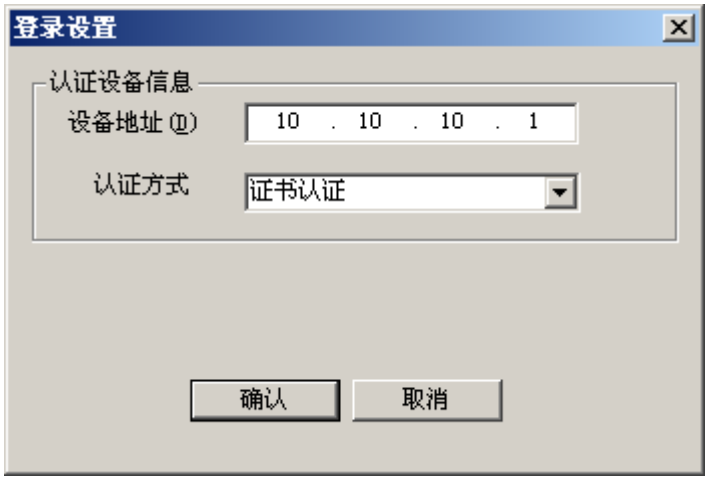
4）开放 area_eth1 区域的认证服务（系统默认已将 eth1 口加入区域 area_eth1）

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。

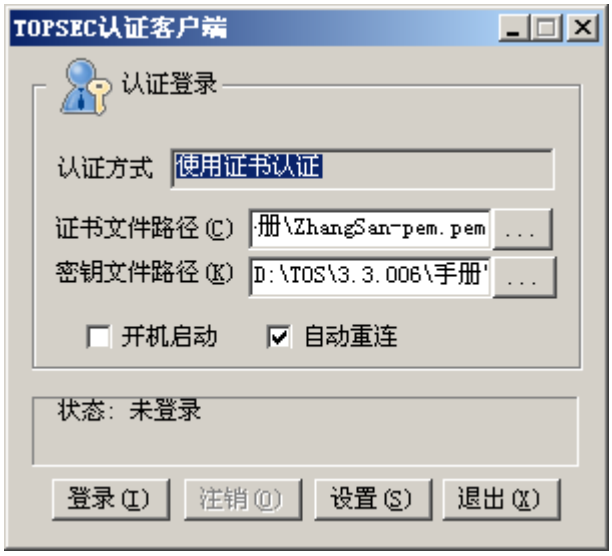
5）设置用户认证客户端

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。

点击“设置”按钮，将认证方式设为证书认证，如下图。



点击“确认”，弹出导入证书界面，如下图所示。



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。

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）。

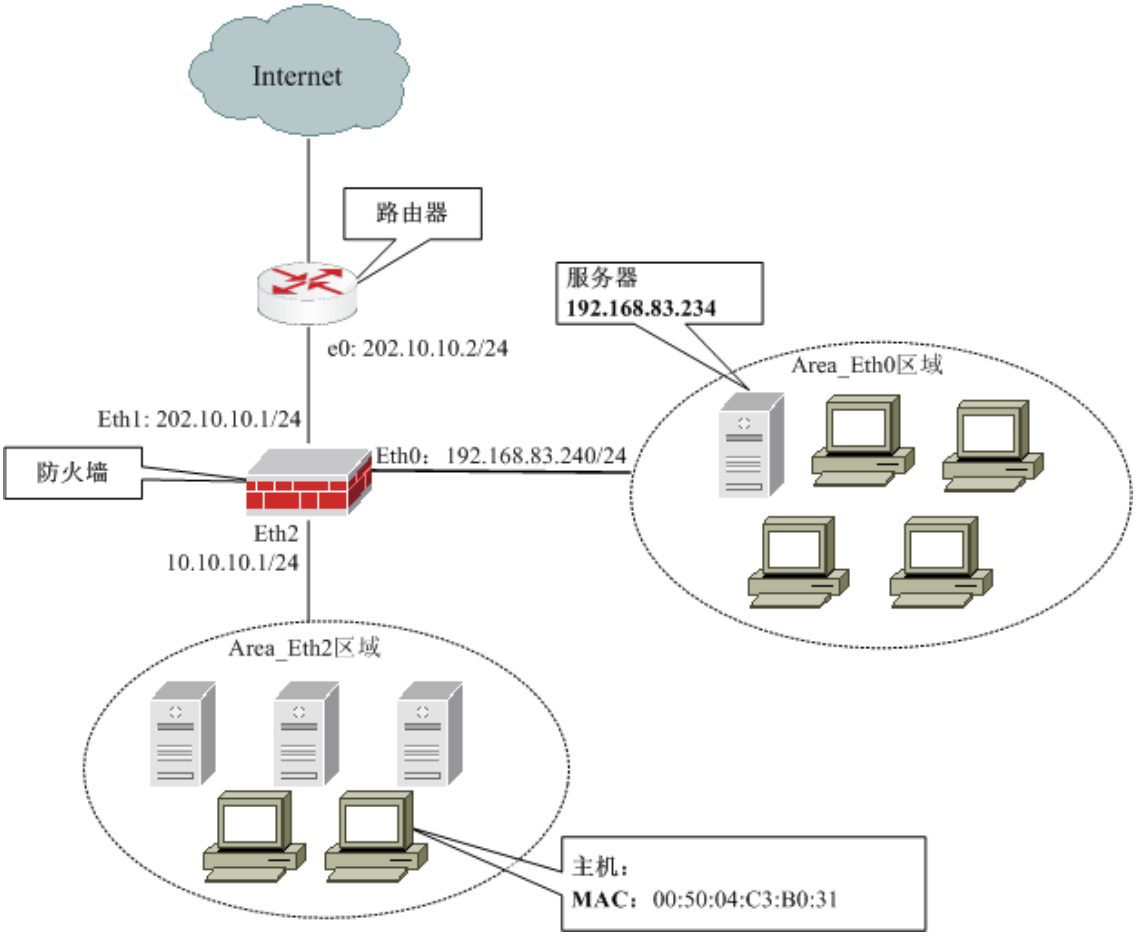


图 16 防火墙在网络中进行报文过滤控制示意图

配置要点

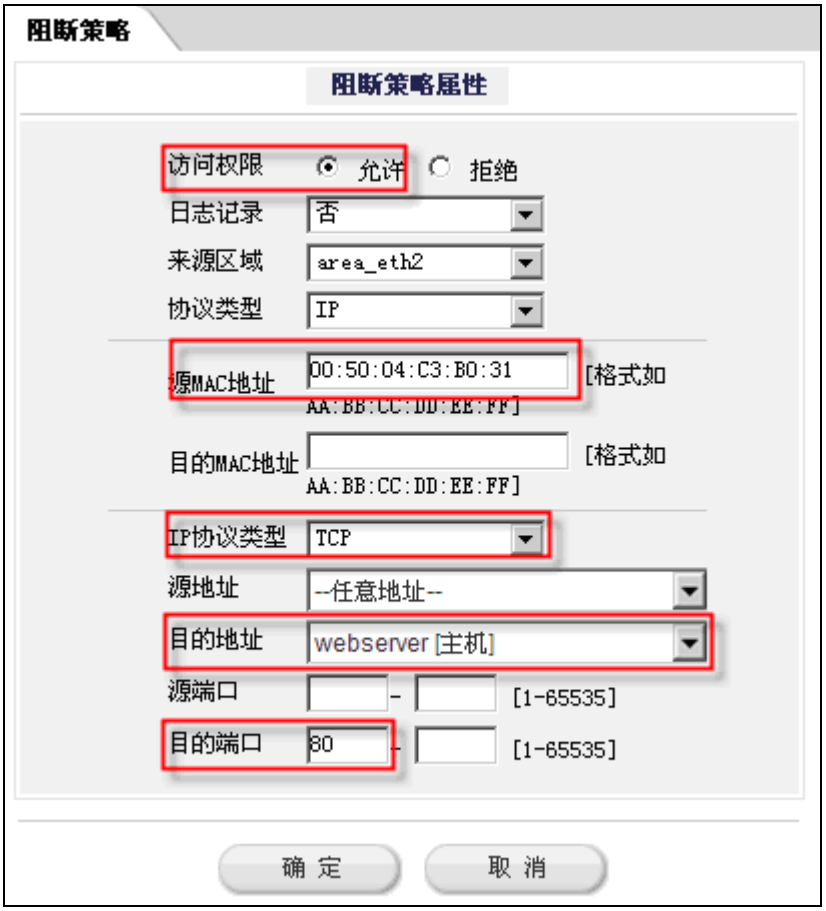
- 定义服务器主机地址对象
- 配置报文阻断策略

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。

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”。



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

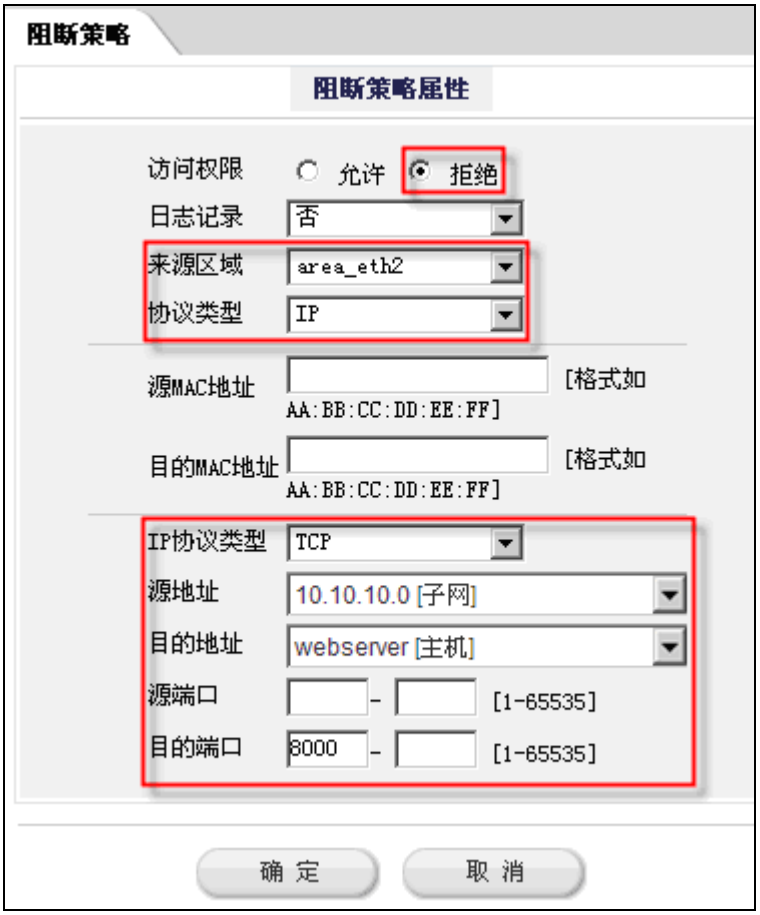
- 定义服务器主机地址资源和子网地址资源
- 配置报文阻断策略

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。

3）选择 **资源管理 > 地址**，并选择“子网”页签，添加子网地址资源。

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。



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。

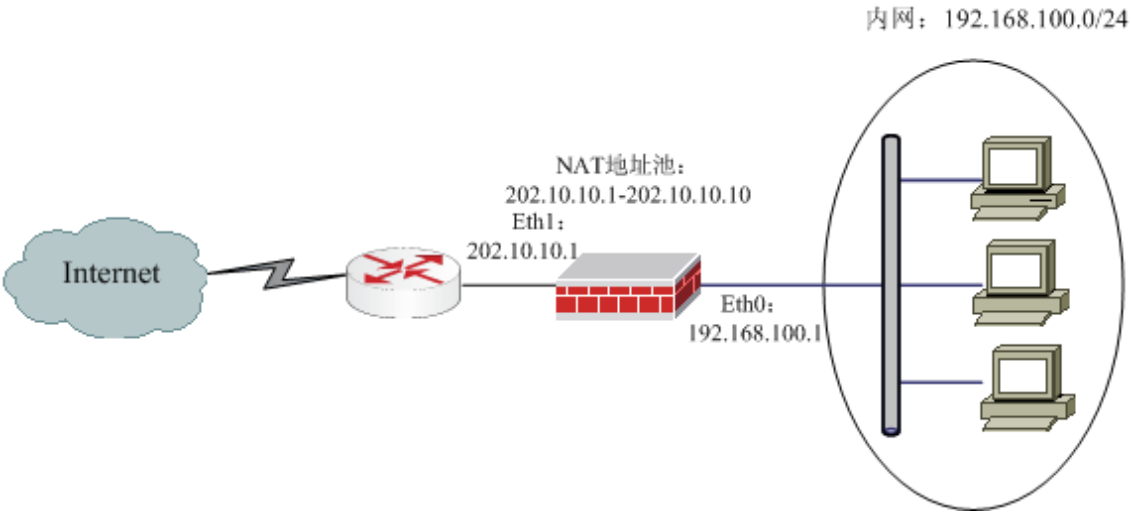


图 17 基于地址资源的源地址转换示意图

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。

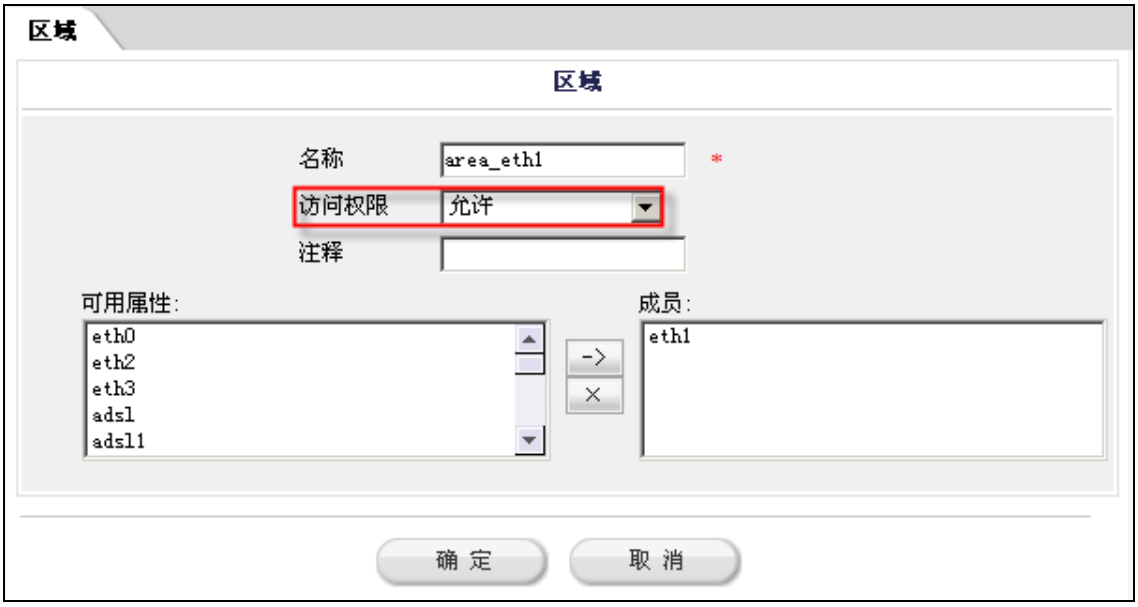
- 定义源地址转换策略。

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。

外网区域 area_eth1 与属性 eth1 绑定且允许访问。



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”。

b）定义 NAT 地址池：选择“范围”页签，点击“添加”。

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。

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。

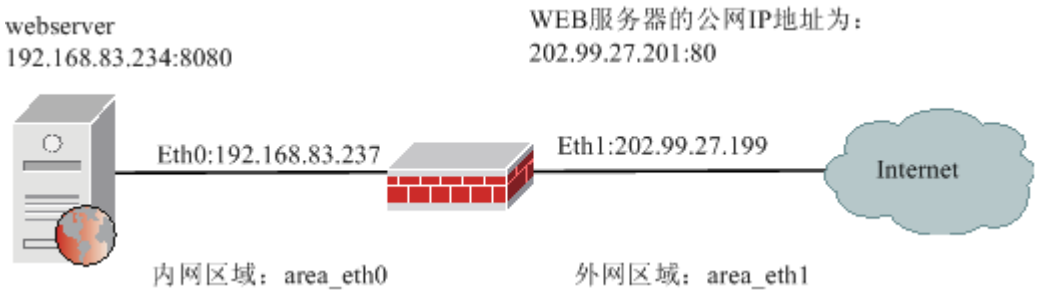


图 18 基于 IP 地址的目的地址转换示意图

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

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。

外网区域 area_eth1 与属性 eth1 绑定且允许访问。

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。

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。

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。

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。

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。

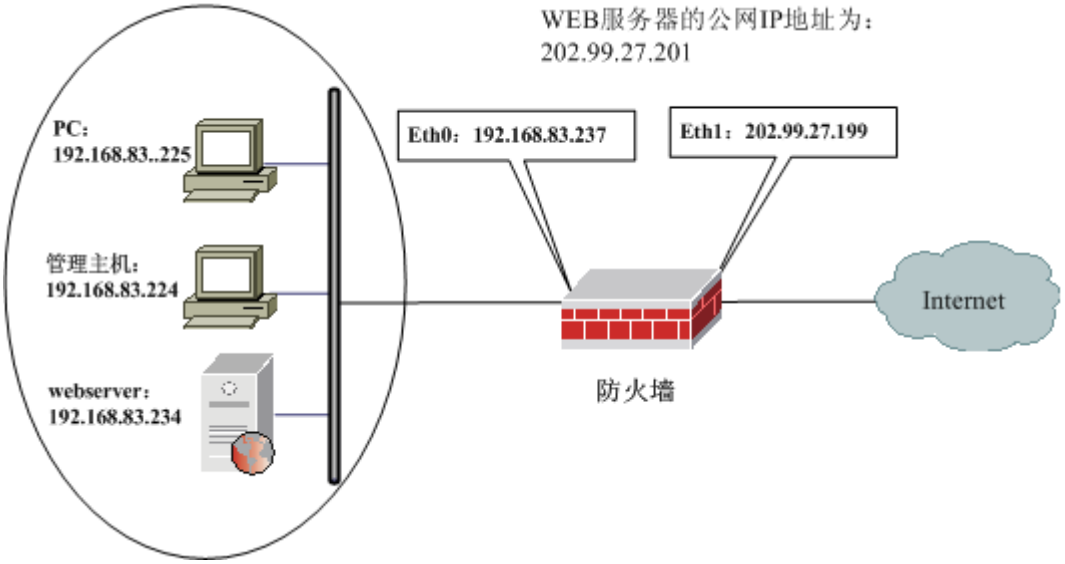


图 19 双向地址转换示意图

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”；

接口 Eth1 对应的区域为 area_eth1，设置区域的访问权限为“允许”。

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。

定义 MAP_IP 和 MAP_USERIP 可以参考上图。设置完成后界面如下图。

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。

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。

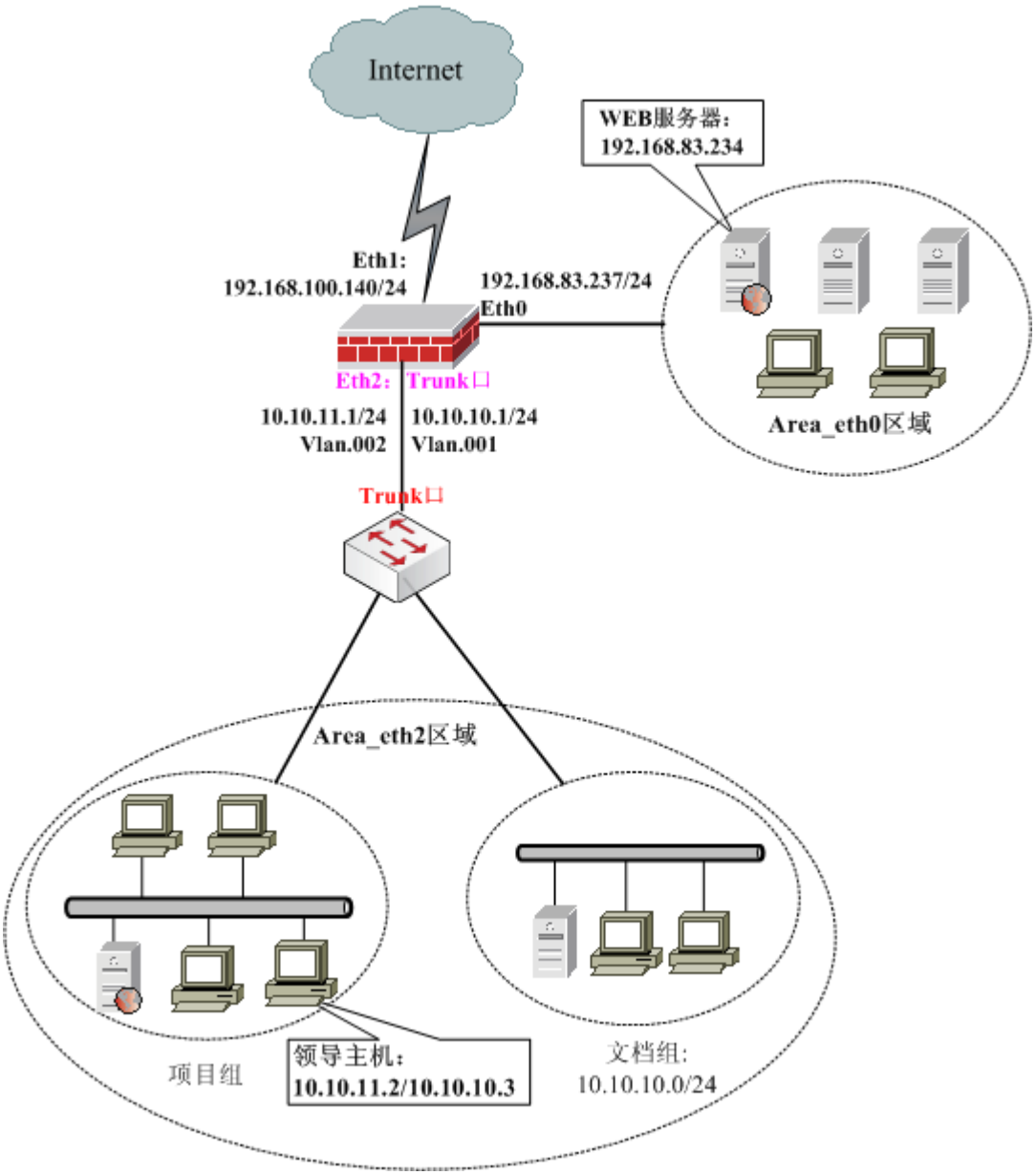


图 20 访问控制规则设置示意图

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：

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。

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。

设置完成后的界面如下图所示。

5）选择 **防火墙 > 地址转换** ，定义地址转换规则。

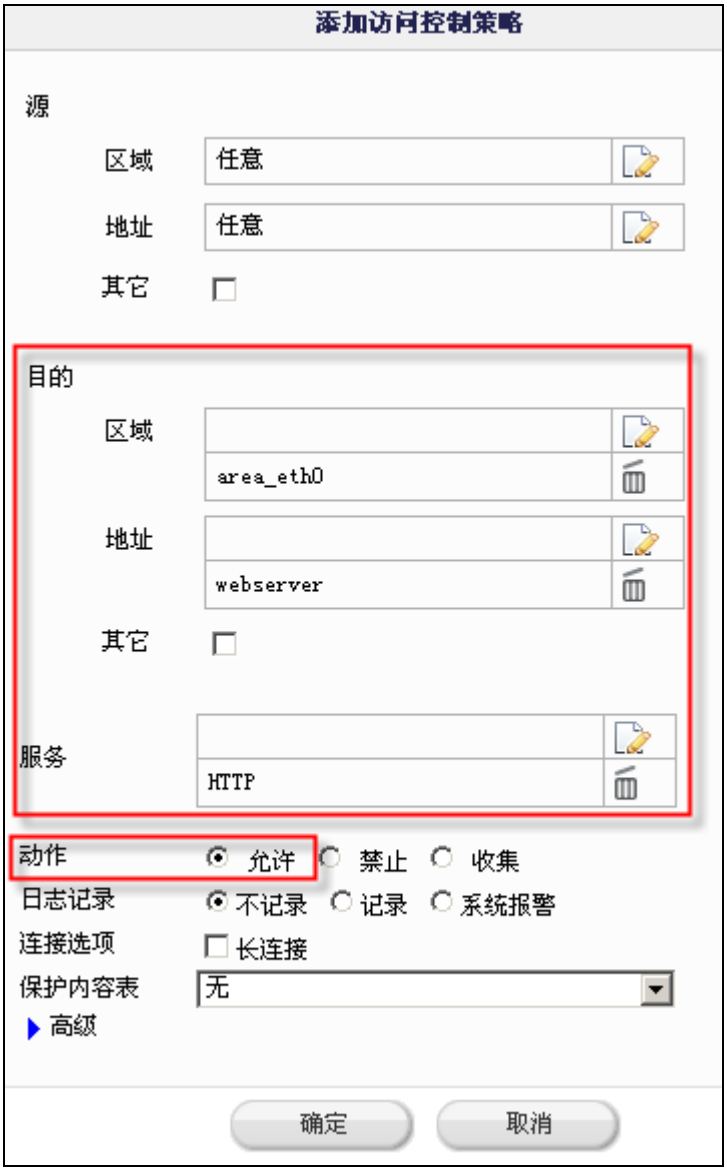
a）定义源地址转换规则，使得内网用户能够访问外网:

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。

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。



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。

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。

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。

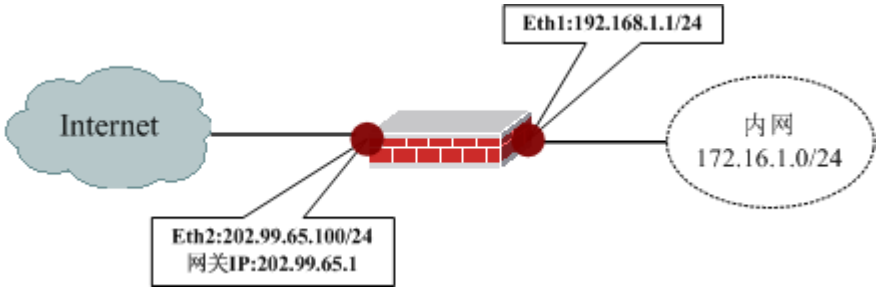


图 21 IPS 策略示意图

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		全双工	100M	
eth1		路由	192.168.1.1/255.255.255.0	1500	启用				
eth2		路由	202.99.65.100/255.255.255.0	1500	启用				
eth3		路由		1500	启用				

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 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		
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 清空 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		

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 IPS策略

攻击检测规则 IPS规则

启用 [默认启用规则，不选为暂不生效]

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。

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。

网络拓扑图如下所示：

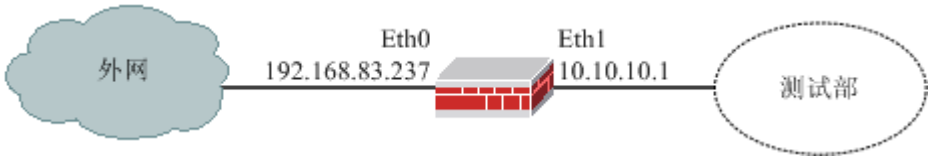


图 22 HTTP 访问过滤示意图

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。

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。

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。

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。

2）参数配置完成后，点击“确定”按钮。

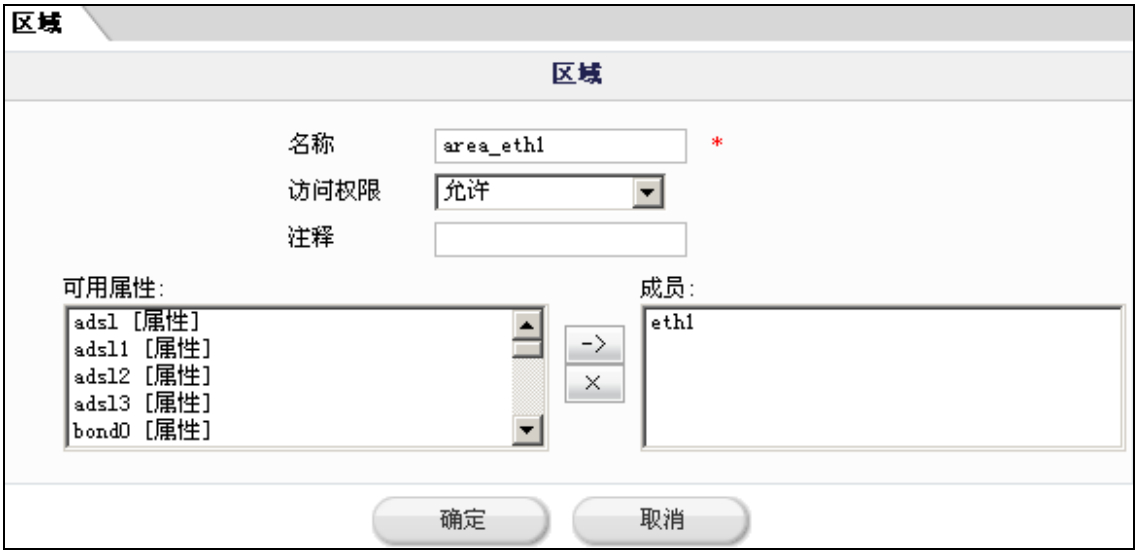
5．配置外网所在区域“area_eth0”和测试部所在区域“area_eth1”。

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。

参数设置完成后，点击“确定”按钮即可。

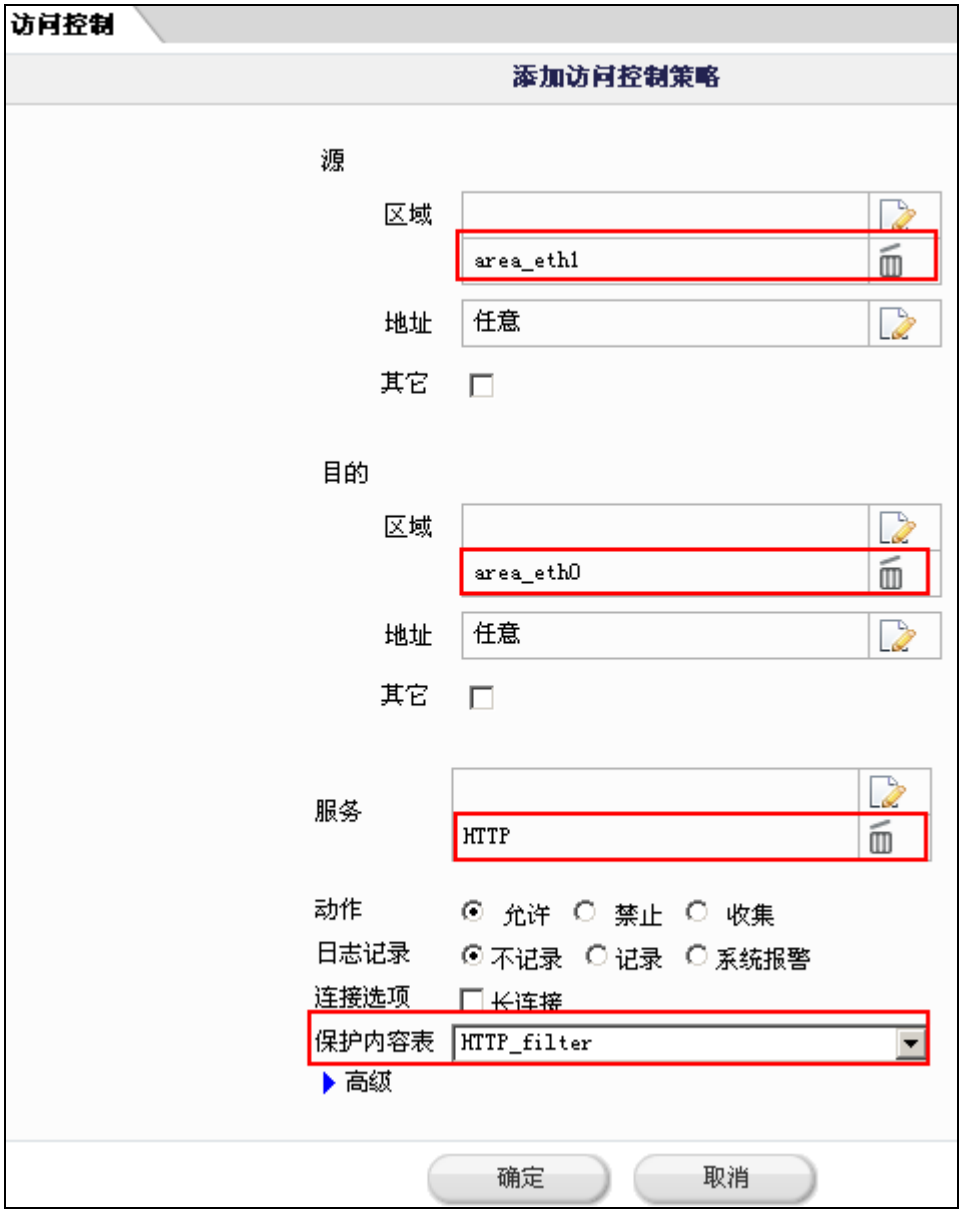
2）选择 **资源管理 > 区域**，然后点击“添加”链接，配置测试部所在区域“area_eth1”，如下图所示。



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。



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。

2）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。

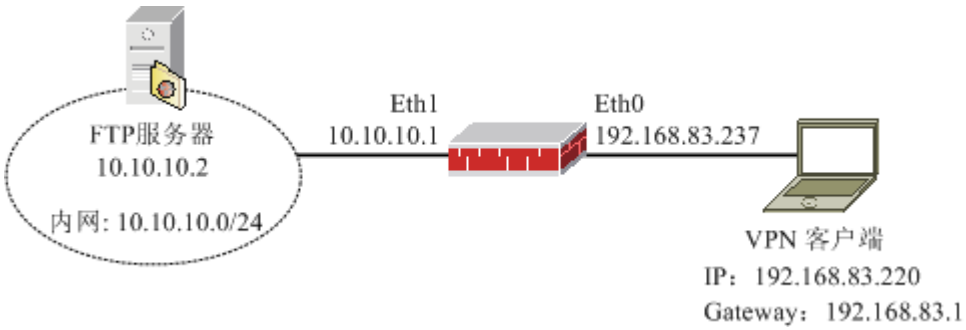


图 23 远程用户本地认证示意图

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。

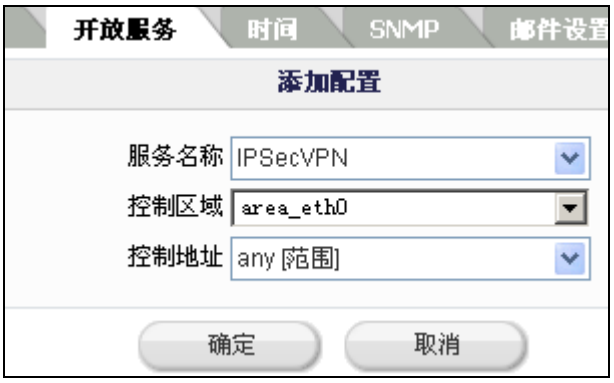
WebUI 配置步骤

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。

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。



参数设置完成后，点击“确定”按钮。

2．绑定 IPSec 虚接口。

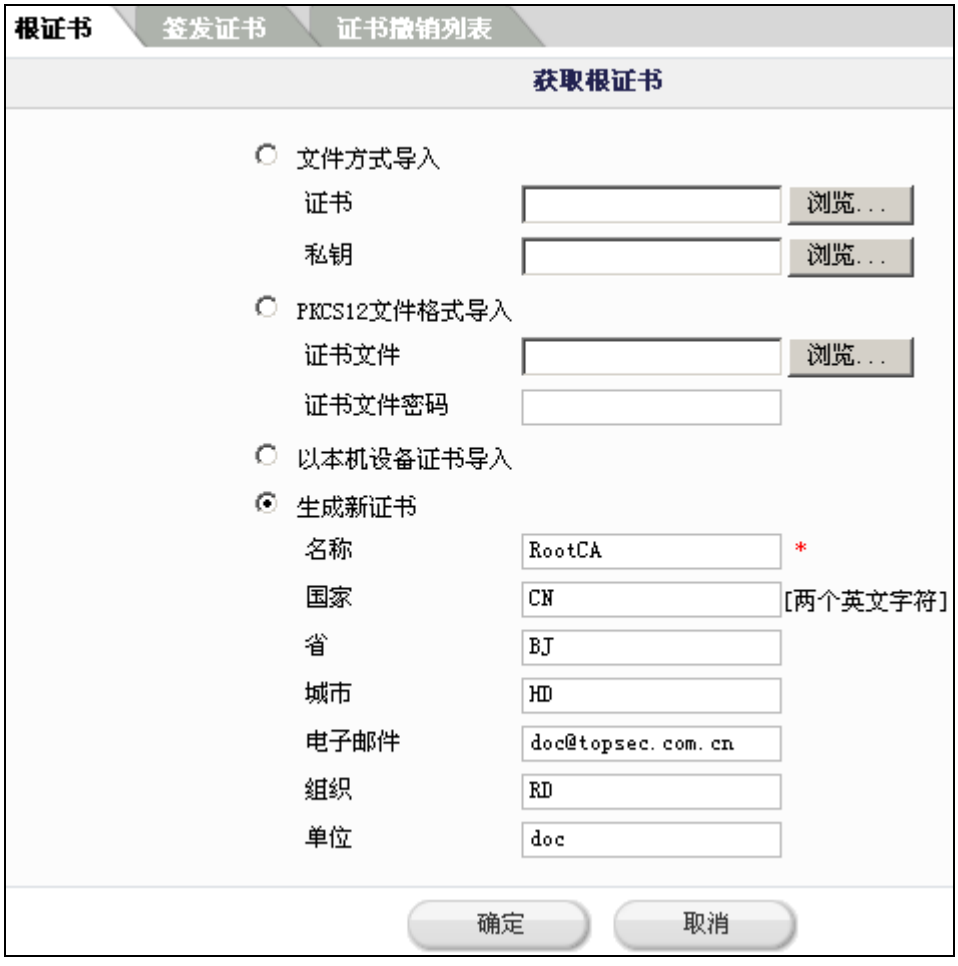
选择 **虚拟专网 > 虚接口绑定**，然后点击“添加”，绑定虚接口 ipsec0，如下图所示。

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。



3）参数设置完成后，点击“确定”按钮。

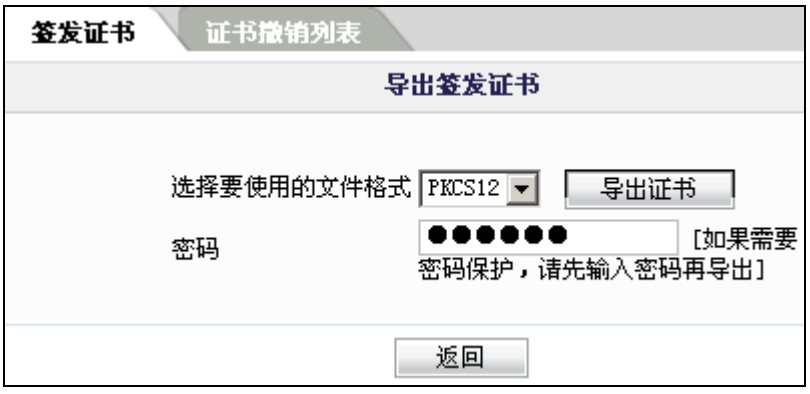
4．签发并下载用户证书。

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。

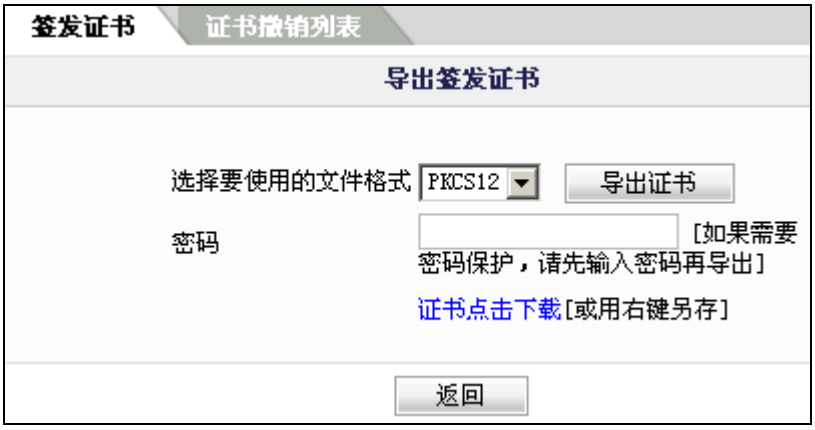
参数设置完成后，点击“确定”按钮即可。

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。

选择证书类型为“PKCS12 格式”，输入密码，如下图所示。



参数设置完成后，点击“导出”按钮，如下图所示。



点击“证书点击下载”链接，弹出文件保存对话框，如下图所示。

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。

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。

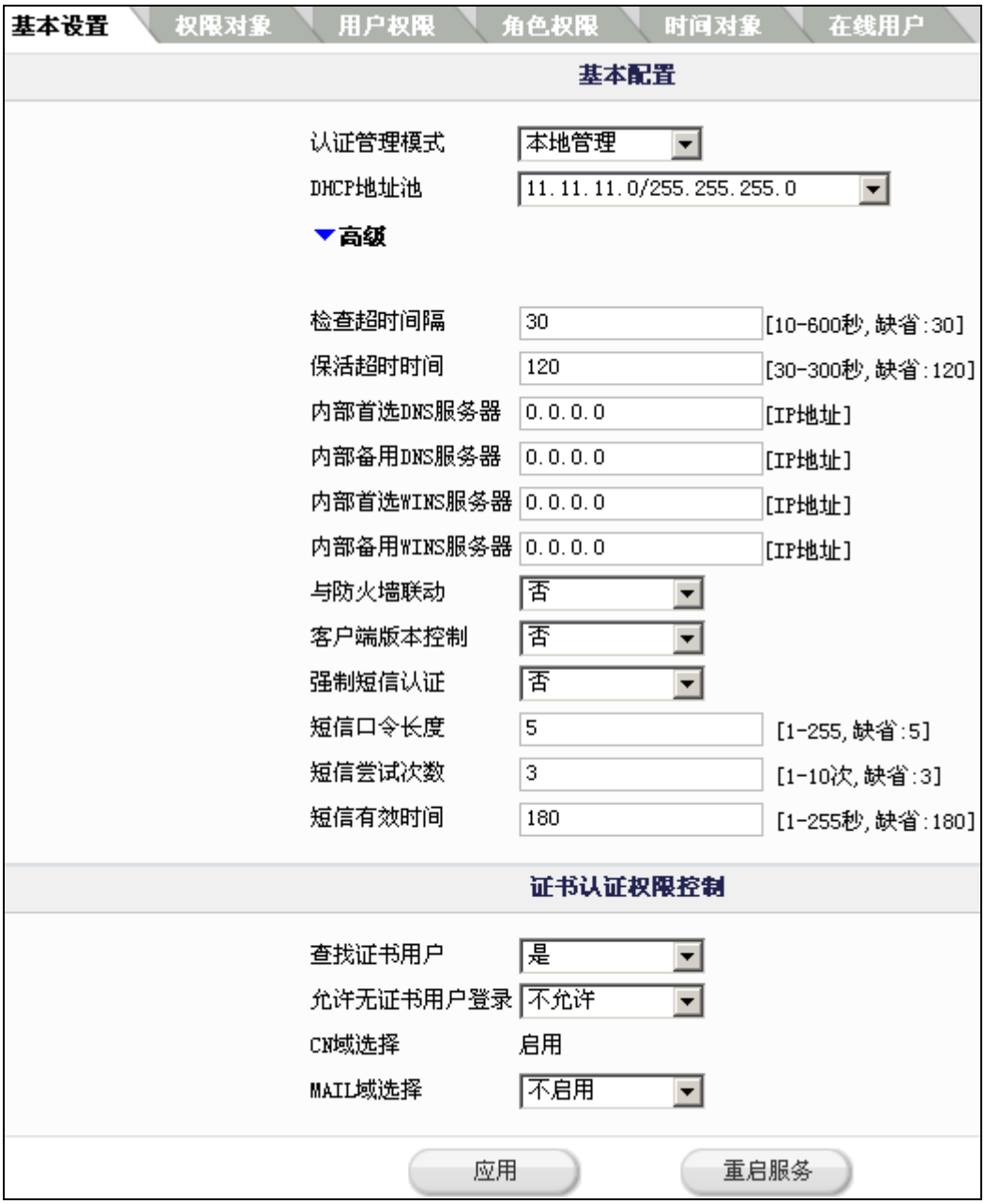
2）在 lo 接口启用 DHCP 服务器。

a）在列表框中选择“lo”，然后点击“<-”按钮，如下图所示。

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。

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。



说明

> ✧ 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。

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。

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。

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。

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。

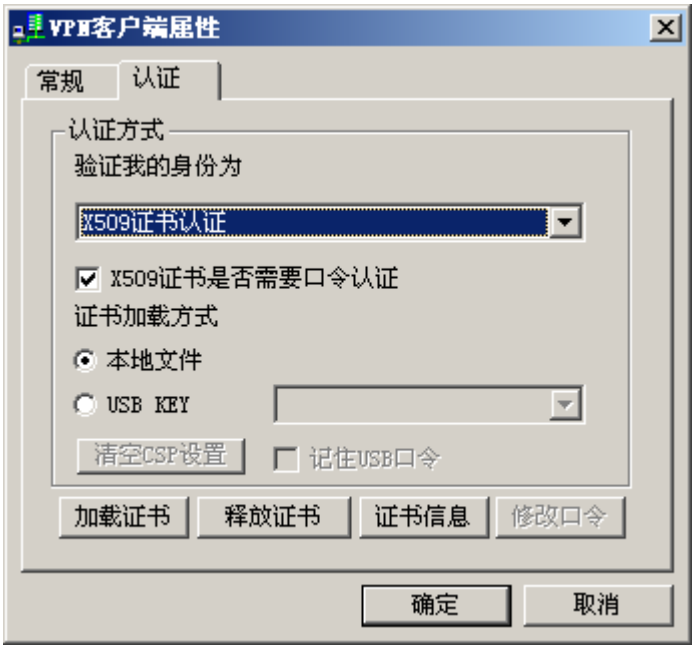
a）在远程 VRC 客户机器上安装 VPN 远程客户端。

b）打开 VPN 客户端，如下图所示。

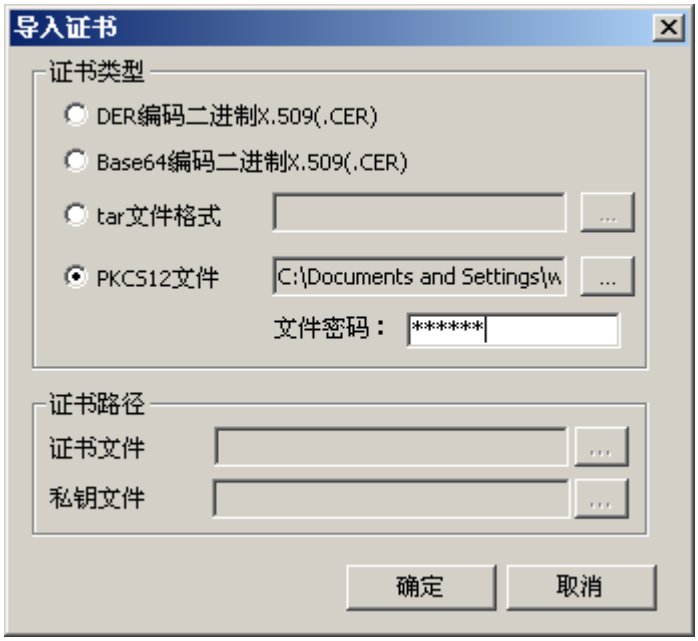
c）双击“新建 VPN 连接”图标，进入配置 VPN 客户端属性的窗口，如下图所示。

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。

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 证书是否需要口令认证”，然后选中“本地文件”，如下图所示。

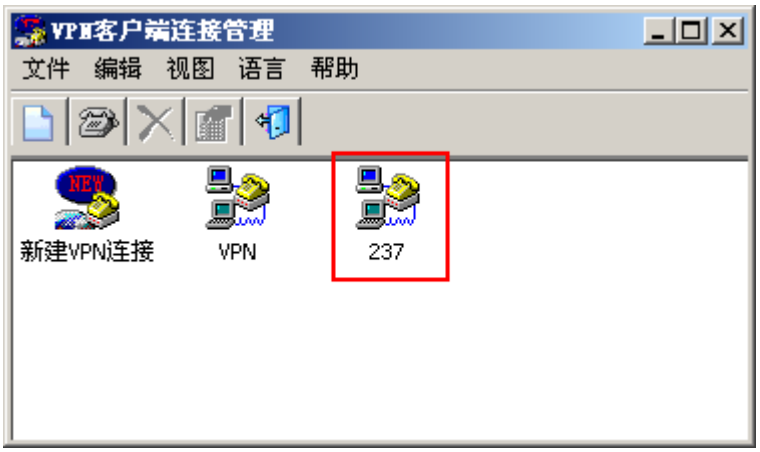


点击“加载证书”按钮，在“导入证书”窗口中为用户“test”配置证书加载方式和证书加载路径，如下图所示。



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。

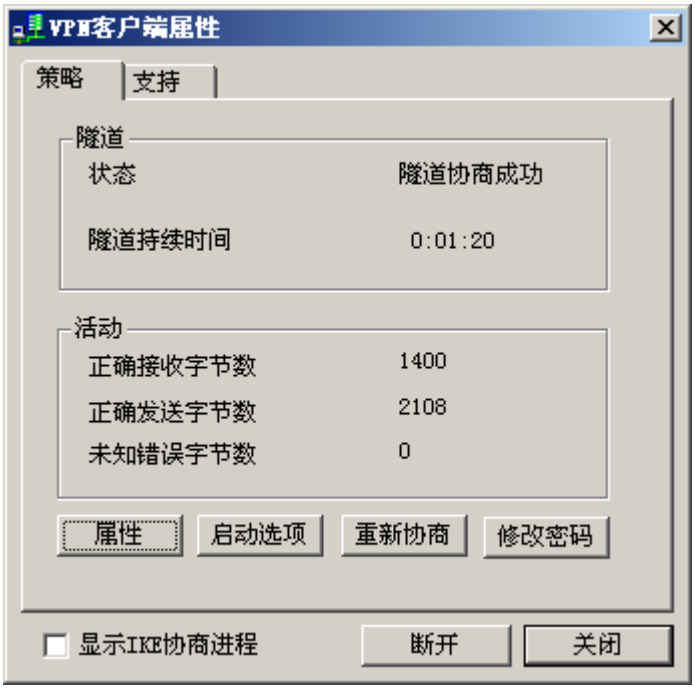
点击提示框中的“确定”按钮，然后点击“VPN 客户端属性”窗口中的“确定”按钮，新建连接显示在“VPN 客户端连接管理”窗口中，如下图所示。

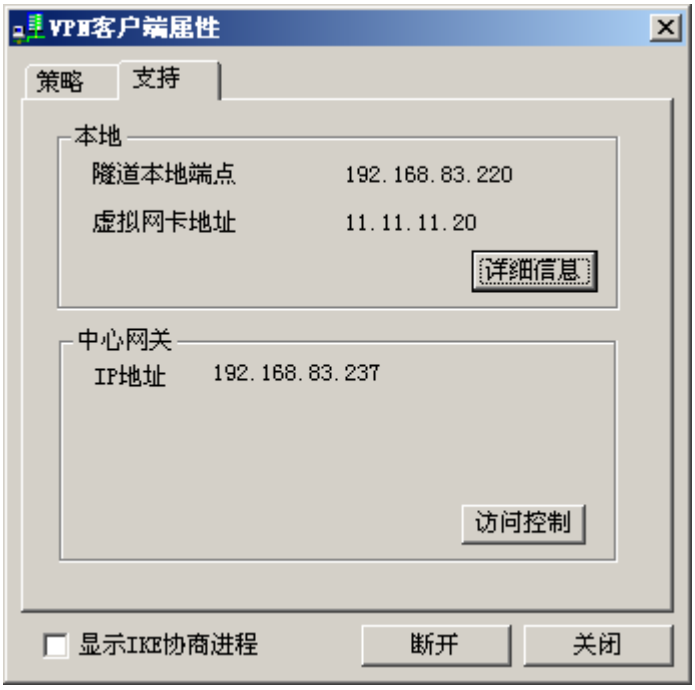


f）双击新建连接“237”，打开 VRC 用户登录窗口，如下图所示。

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。



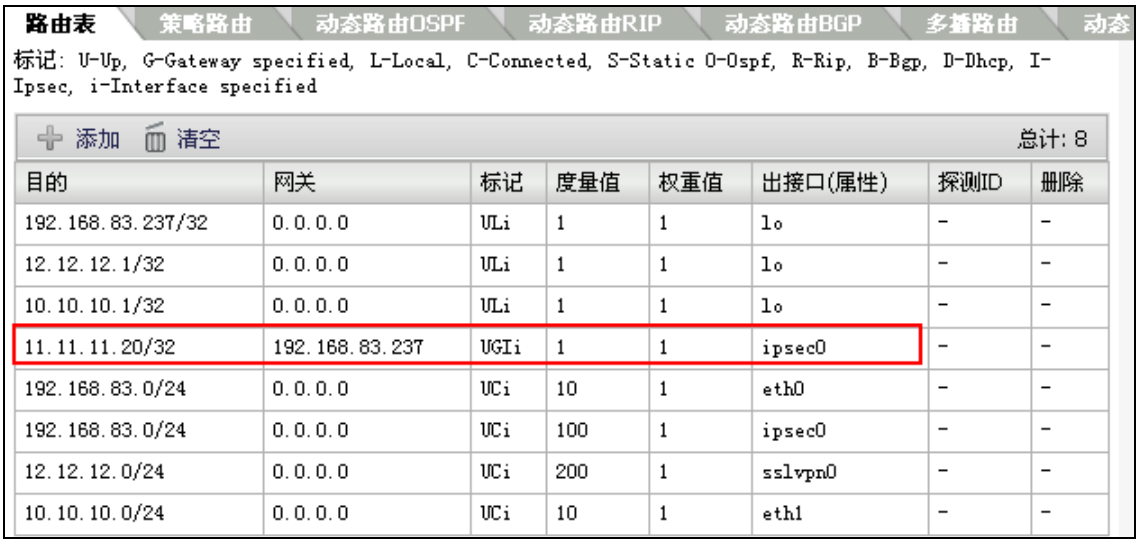


点击“访问控制”按钮，可以查看 VRC 用户的访问权限，如下图所示。

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        Netmask          Gateway       Interface  Metric
          0.0.0.0          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OSPF | 动态路由RIP | 动态路由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 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
192.168.83.237/32	0.0.0.0	ULi	1	1	lo	-	-
12.12.12.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.10.10.1/32	0.0.0.0	ULi	1	1	lo	-	-
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	sslvpn0	-	-
10.10.10.0/24	0.0.0.0	UCi	10	1	eth1	-	-

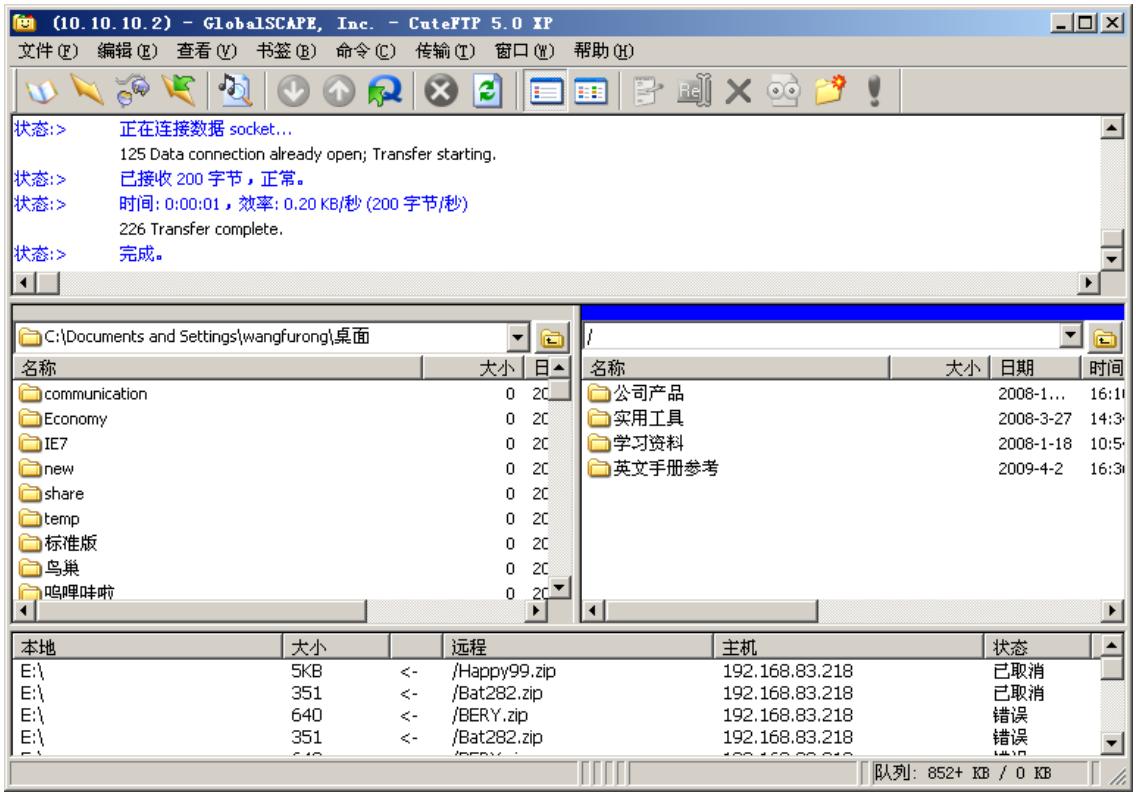
选择 **虚拟专网 > VRC 管理**，然后激活“在线用户”页签，可以查看防火墙上的 VRC 用户信息，如下图所示。

基本设置 | 权限对象 | 用户权限 | 角色权限 | 时间对象 | 在线用户

清空在线用户 总计：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	

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。



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。

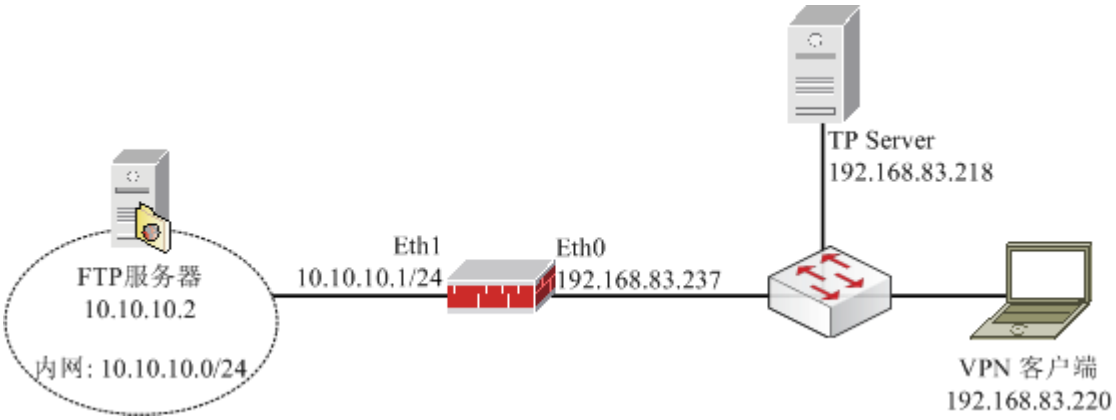


图 24 远程用户集中认证示意图

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。

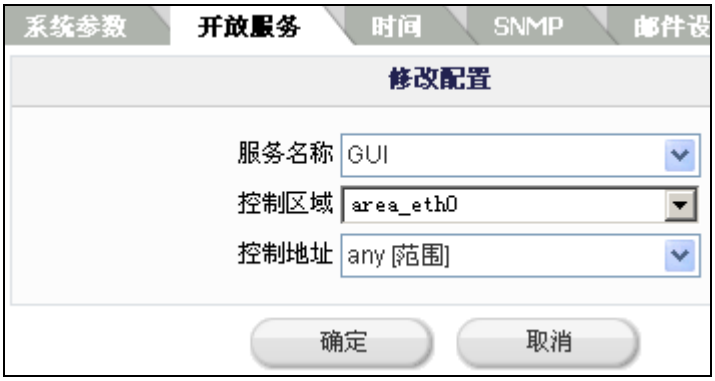
WebUI 配置步骤

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。

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。



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。

参数设置完成后，点击“确定”按钮。

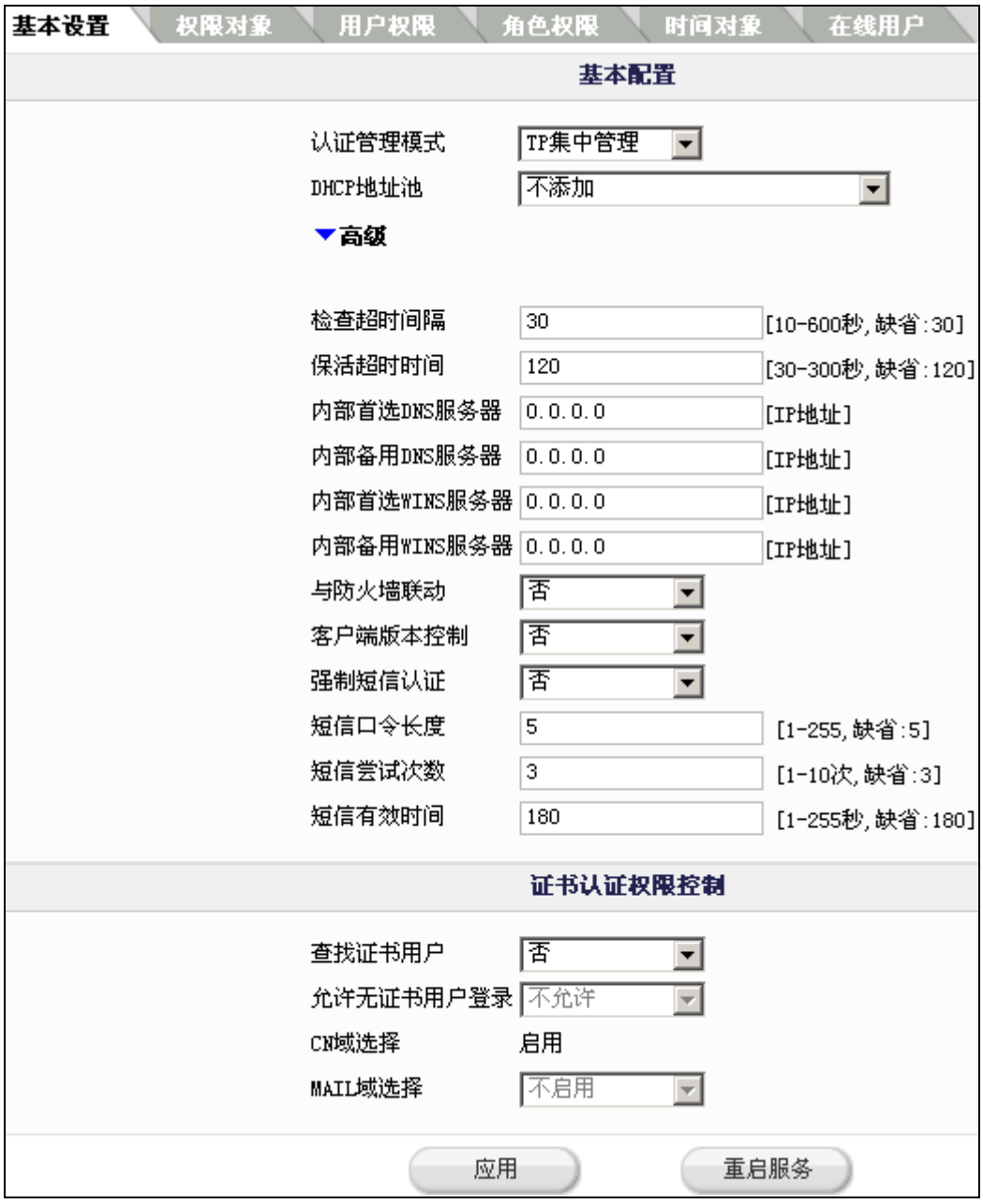
2．绑定 IPSec 虚接口。

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。

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。



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”。

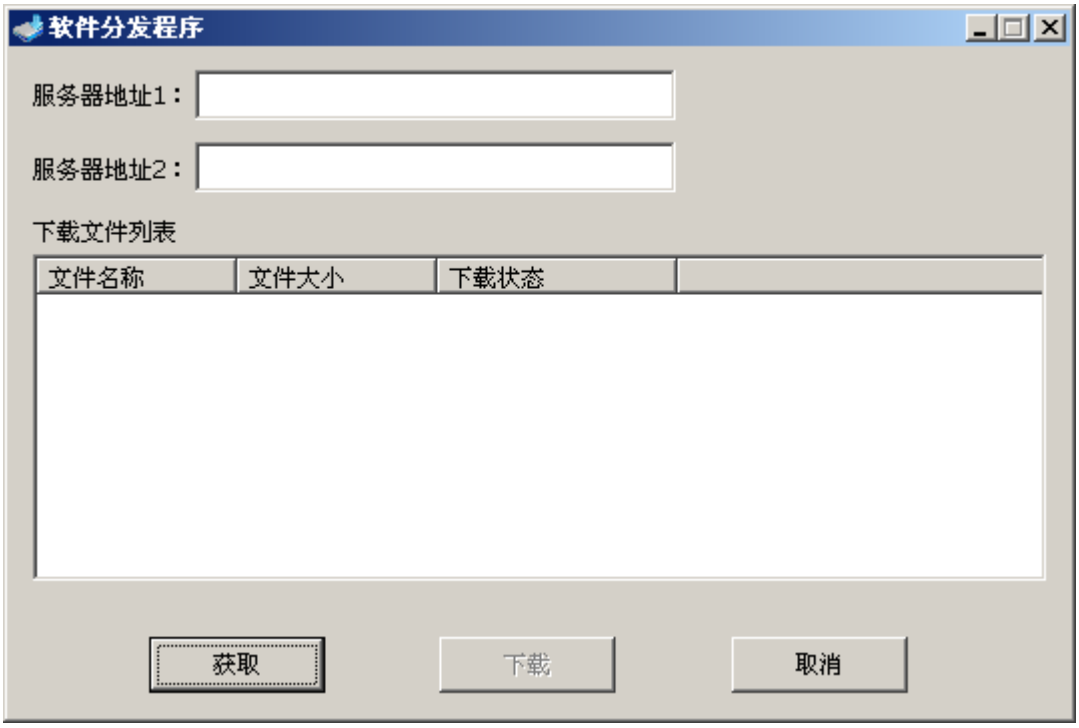
g）对“test”进行软件分发。

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。

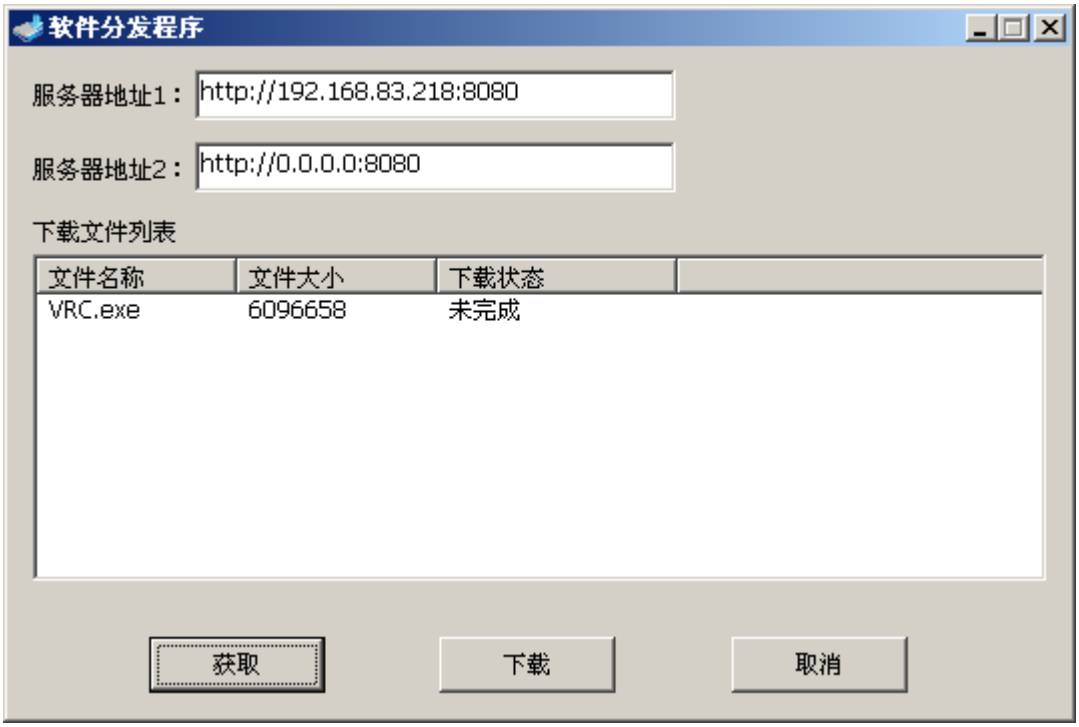
5．验证：VRC 用户“test”使用口令证书方式登录 IPSec VPN 网关后，获得内网“10.10.10.0/24”的访问权限。

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。



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。



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。

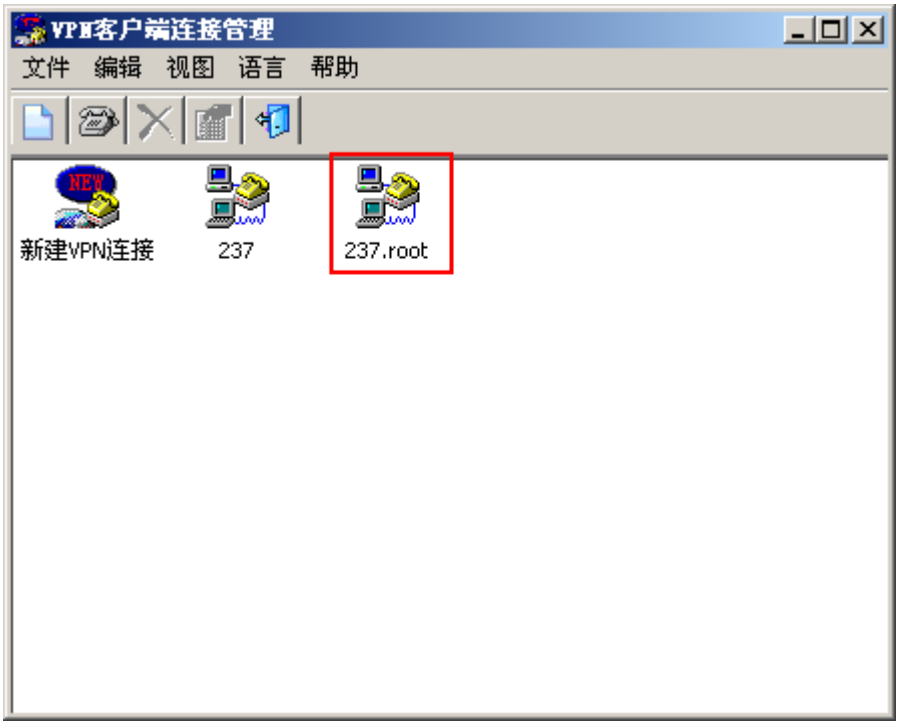
d）点击“确定”按钮，然后点击“完成”按钮即可。

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。

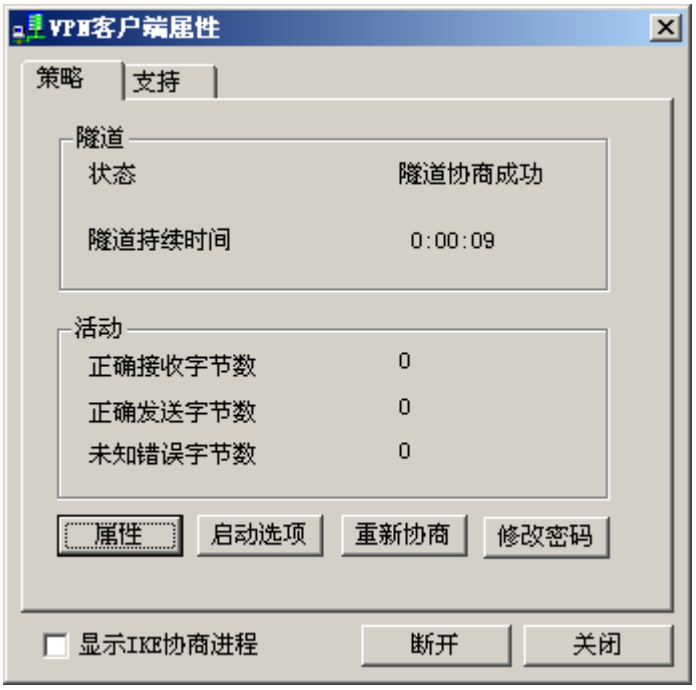
g）双击 VPN 连接的快捷图标，进入 VPN 客户端。根据 TopPolicy 系统分配的权限，VRC 安装系统已经自动为 VRC 用户建立了 VPN 连接“237.root”。VPN 连接的名称即是 TP 上 VPN 网关设备的名称，如下图所示。

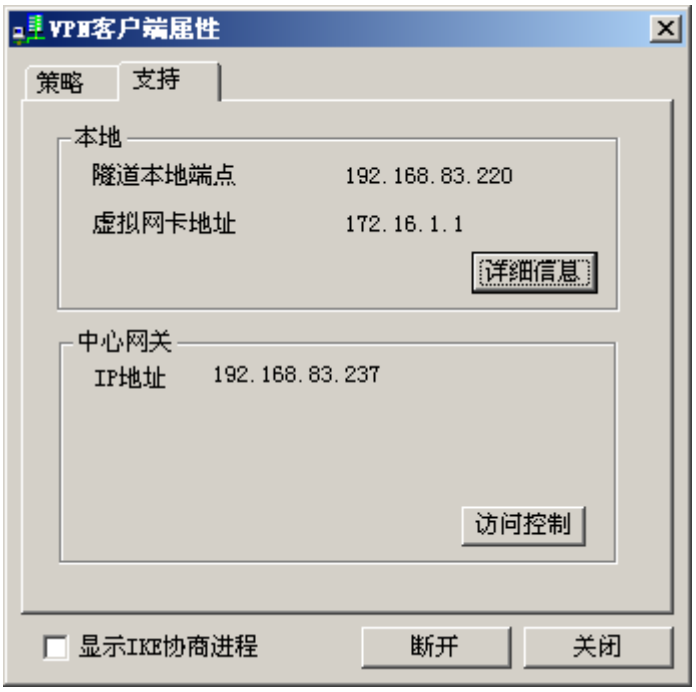


h）双击“237.TPRoot”图标，弹出 VPN 客户端认证窗口。由于用户“test”所属用户组要求验证口令和证书，因此 VPN 客户端窗口中已经导入了用户证书和密码，无需用户手动输入，如下图所示。

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。



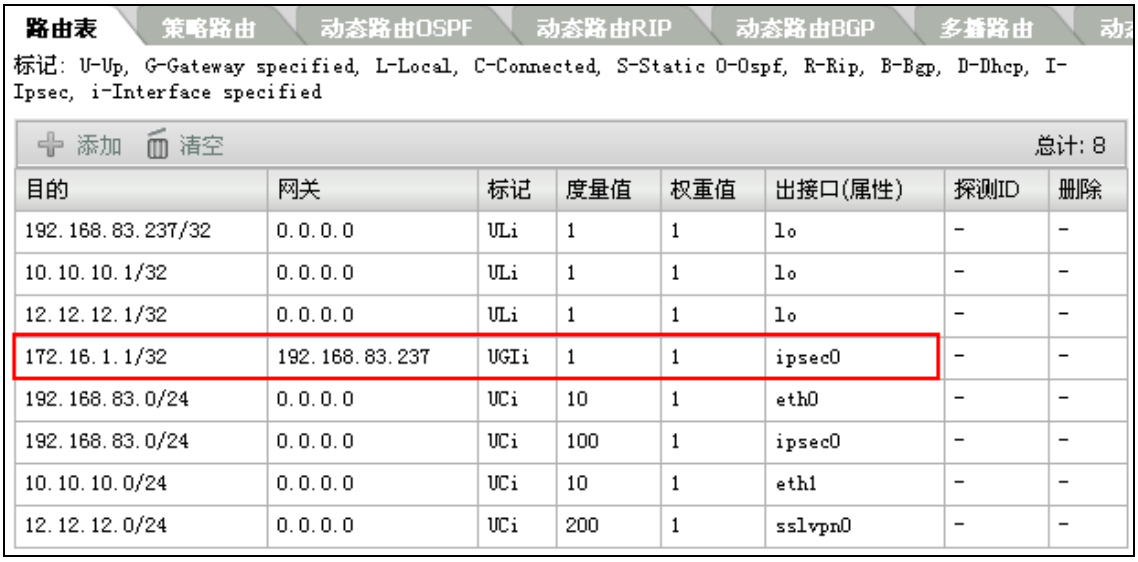


点击“访问控制”按钮，可以查看 VRC 用户的访问权限，如下图所示。

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。

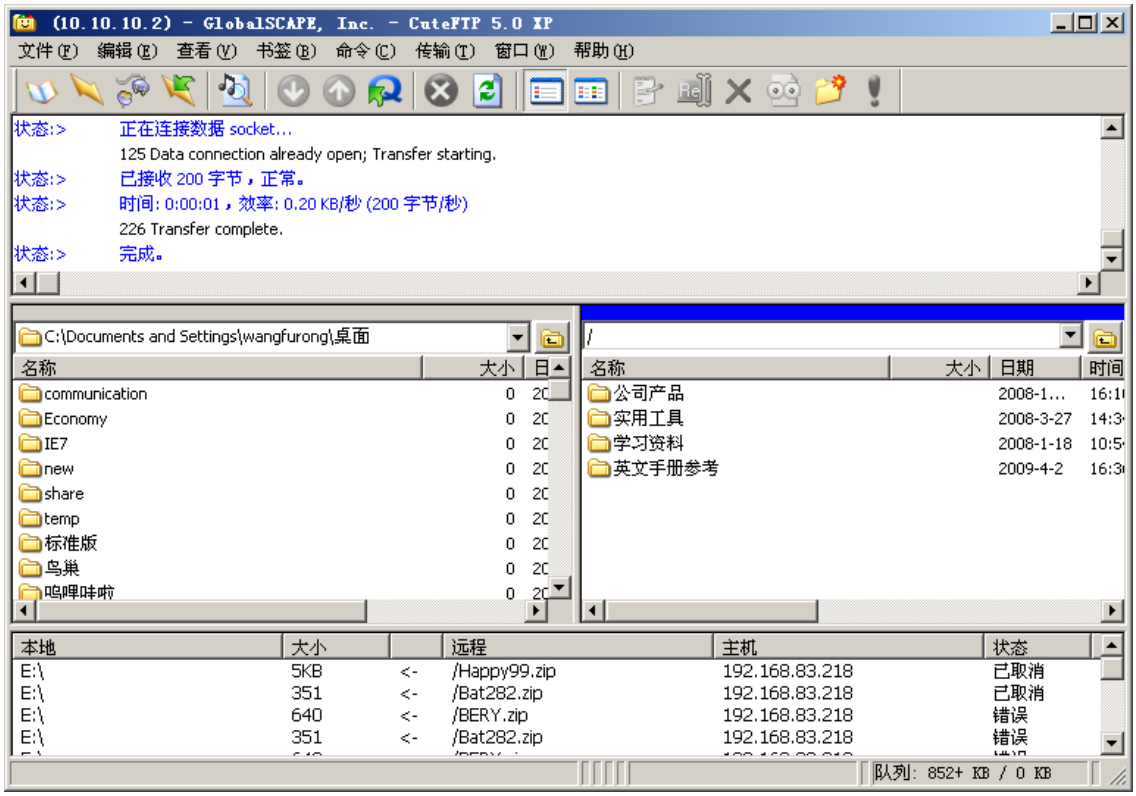
```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.83.1  192.168.83.220      20
       10.10.10.0    255.255.255.0      172.16.1.2      172.16.1.1       1
        127.0.0.0        255.0.0.0       127.0.0.1       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
     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       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
  255.255.255.255  255.255.255.255       172.16.1.1      172.16.1.1       1
  255.255.255.255  255.255.255.255       172.16.1.1               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
===========================================================================
Persistent 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。



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。

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。



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。

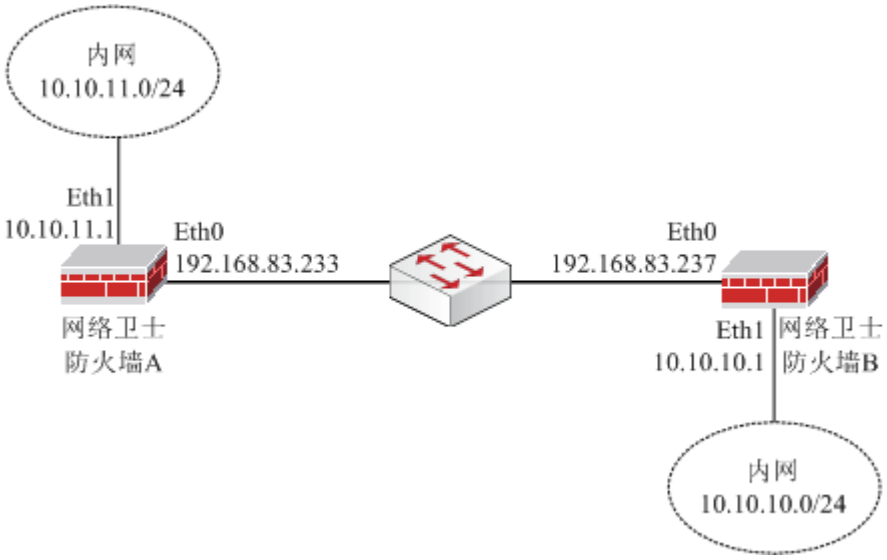


图 25 VPN 静态隧道构建示意图

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。

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。

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。

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。

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。

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。

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。

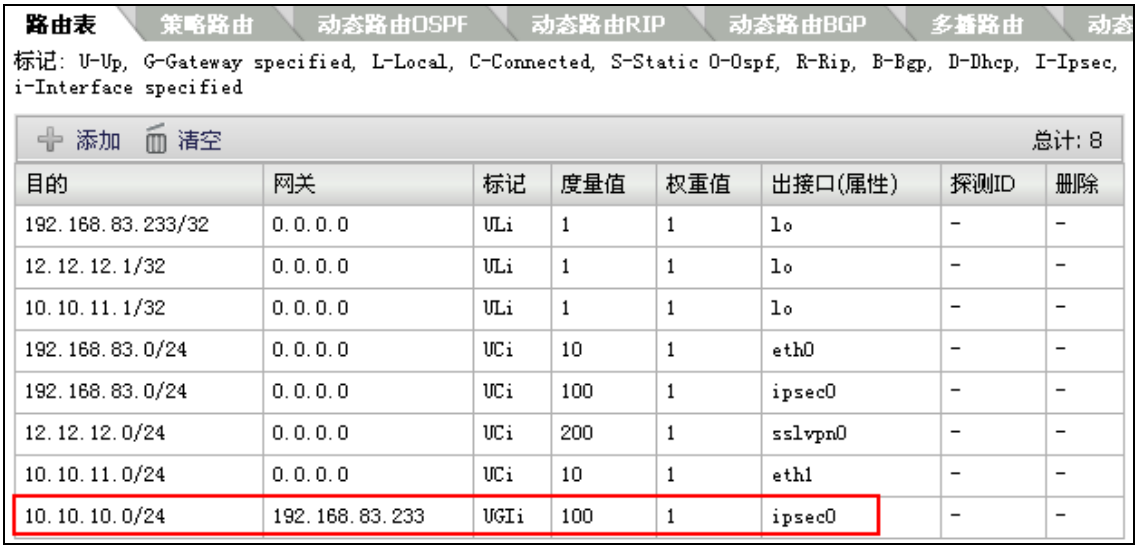
高级配置使用系统默认值。

③ 参数设置完成后，点击“确定”按钮。

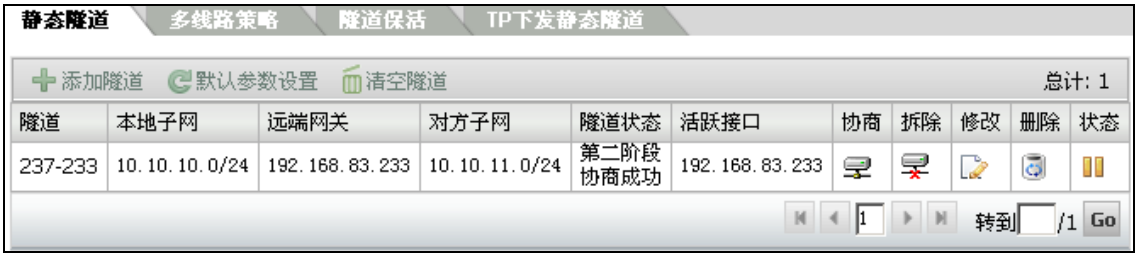
4．在防火墙 A 和防火墙 B 上查看协商成功的静态隧道。

① 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。

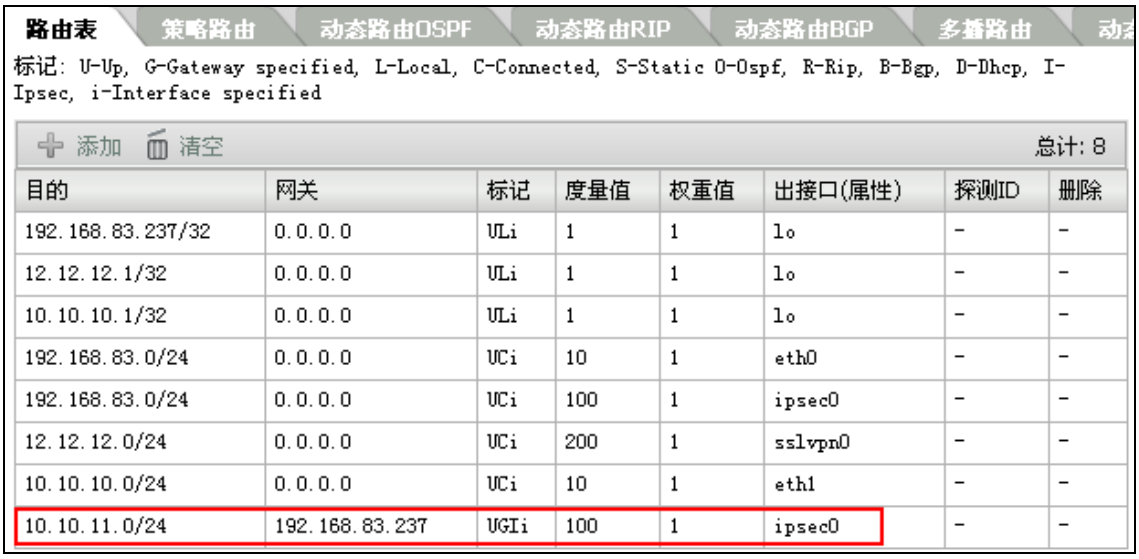
防火墙 A 的静态路由表中会添加一条静态路由，目的地址为防火墙 B 的本地保护子网（10.10.10.0/24），如下图所示（选择 **网络管理 > 路由**，然后激活“路由表”页签）。



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。



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）。



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

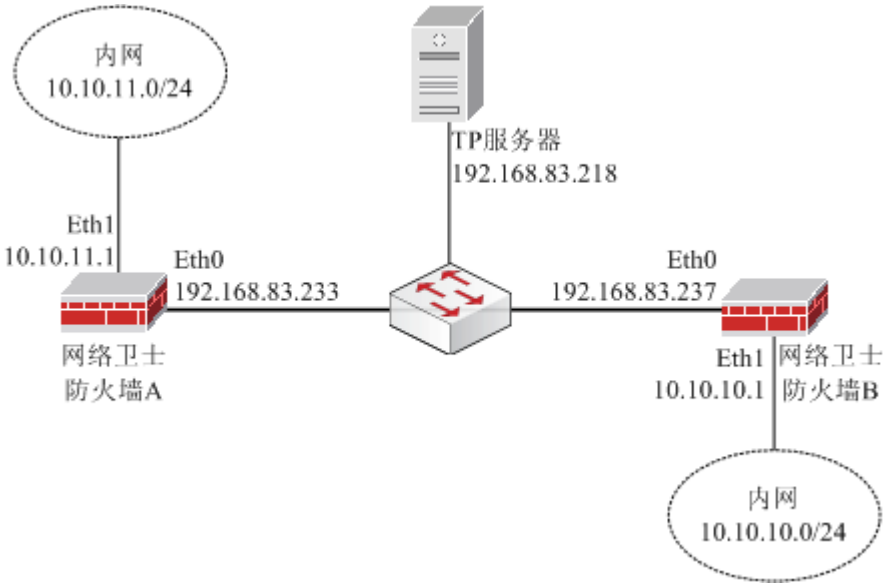


图 26 集中管理 VPN 隧道示意图

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。

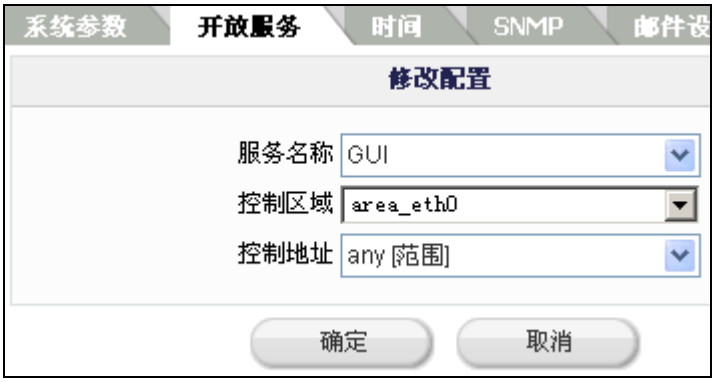
WebUI 配置步骤

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。

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。



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。

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。

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。

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。

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 | 下载子网列表 | 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	255.255.255.0

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

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 | 动态路由RIP | 动态路由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 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	lo	-	-
12.12.12.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.10.11.1/32	0.0.0.0	ULi	1	1	lo	-	-
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	sslvpn0	-	-
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	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** | 下载隧道列表 | 下载隧道状态 | 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	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 | 动态路由RIP | 动态路由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 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
192.168.83.237/32	0.0.0.0	ULi	1	1	lo	-	-
12.12.12.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.10.10.1/32	0.0.0.0	ULi	1	1	lo	-	-
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	sslvpn0	-	-
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

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。

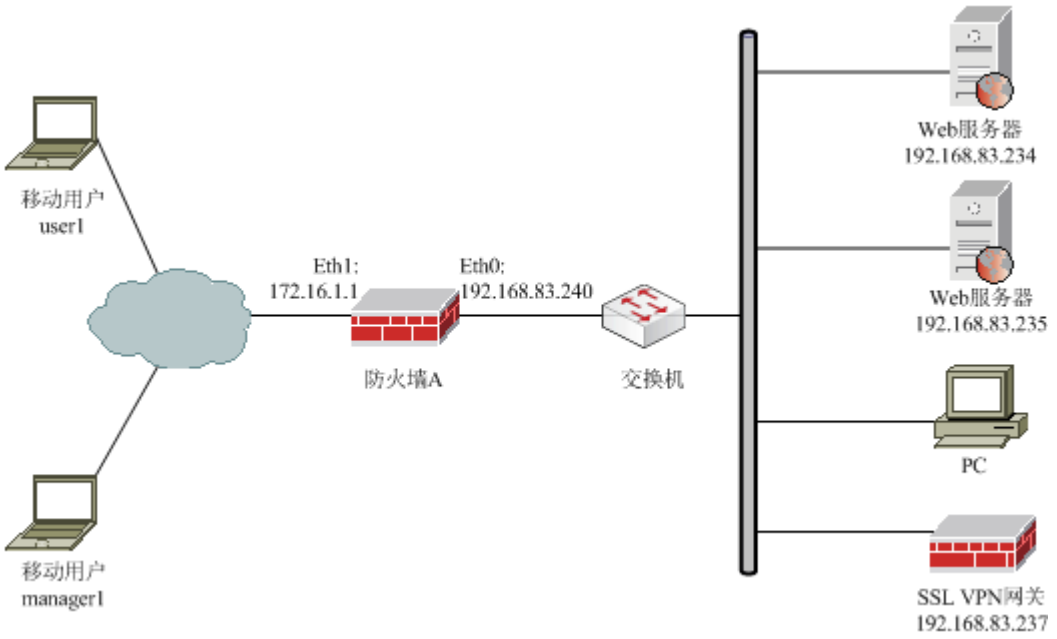


图 27 SSL VPN 网关 Web 转发示意图

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。

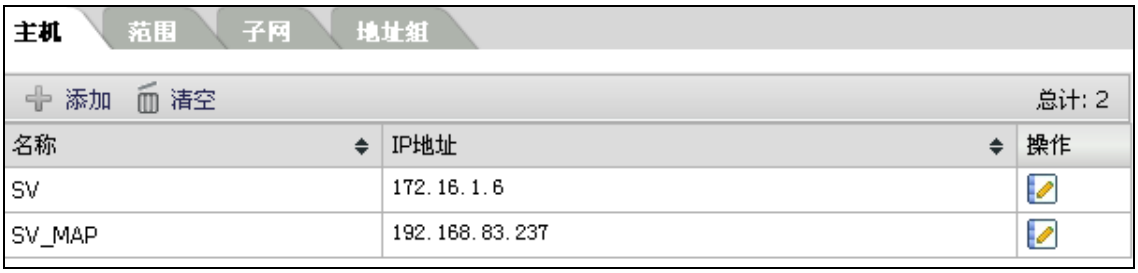
防火墙 A 的配置步骤

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。

2）定义访问控制规则，如下图所示。

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。



4）配置双向地址转换（到 SSL VPN 网关的映射），如下图所示。

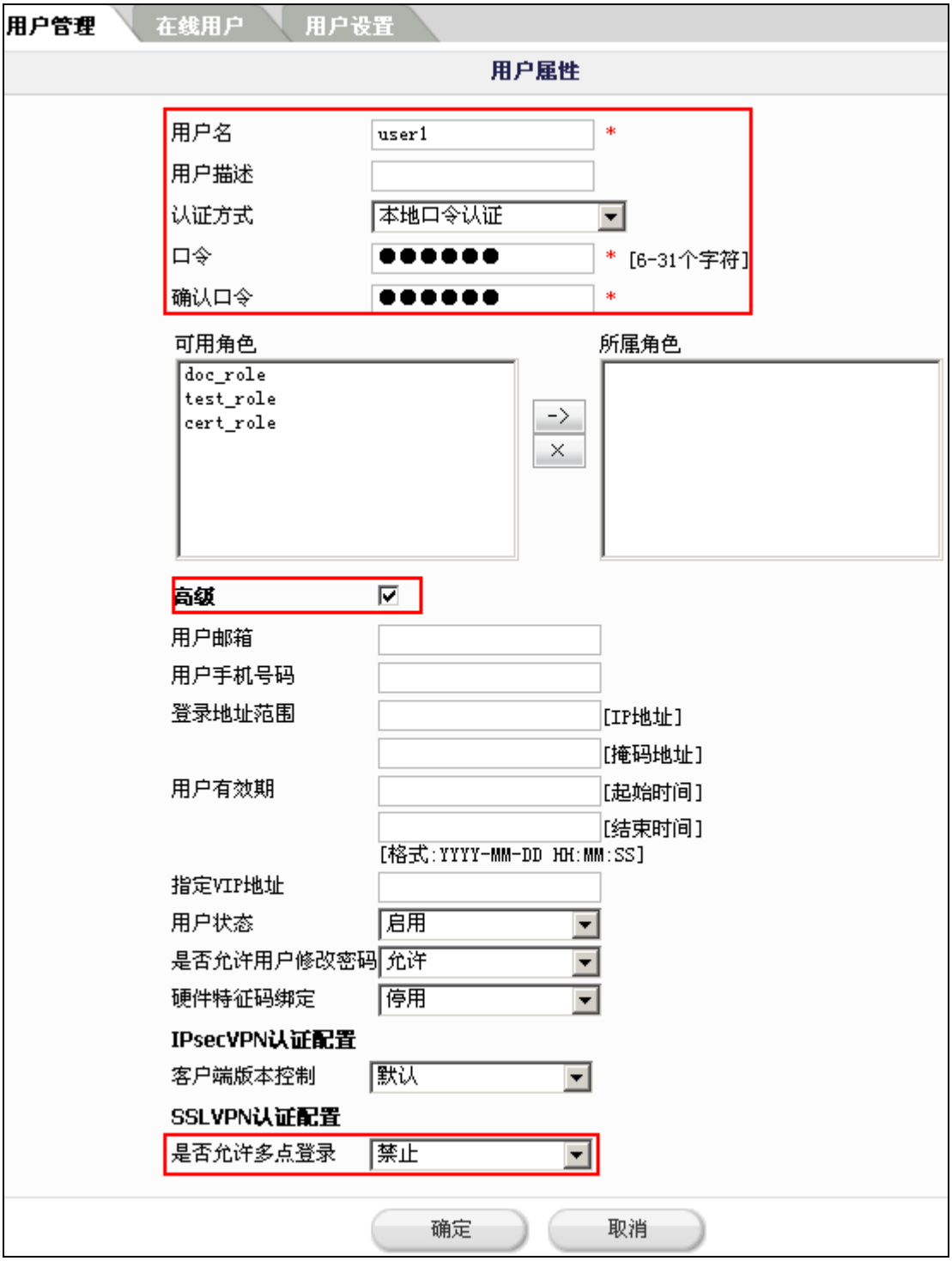
WEBUI 配置步骤

1．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”。

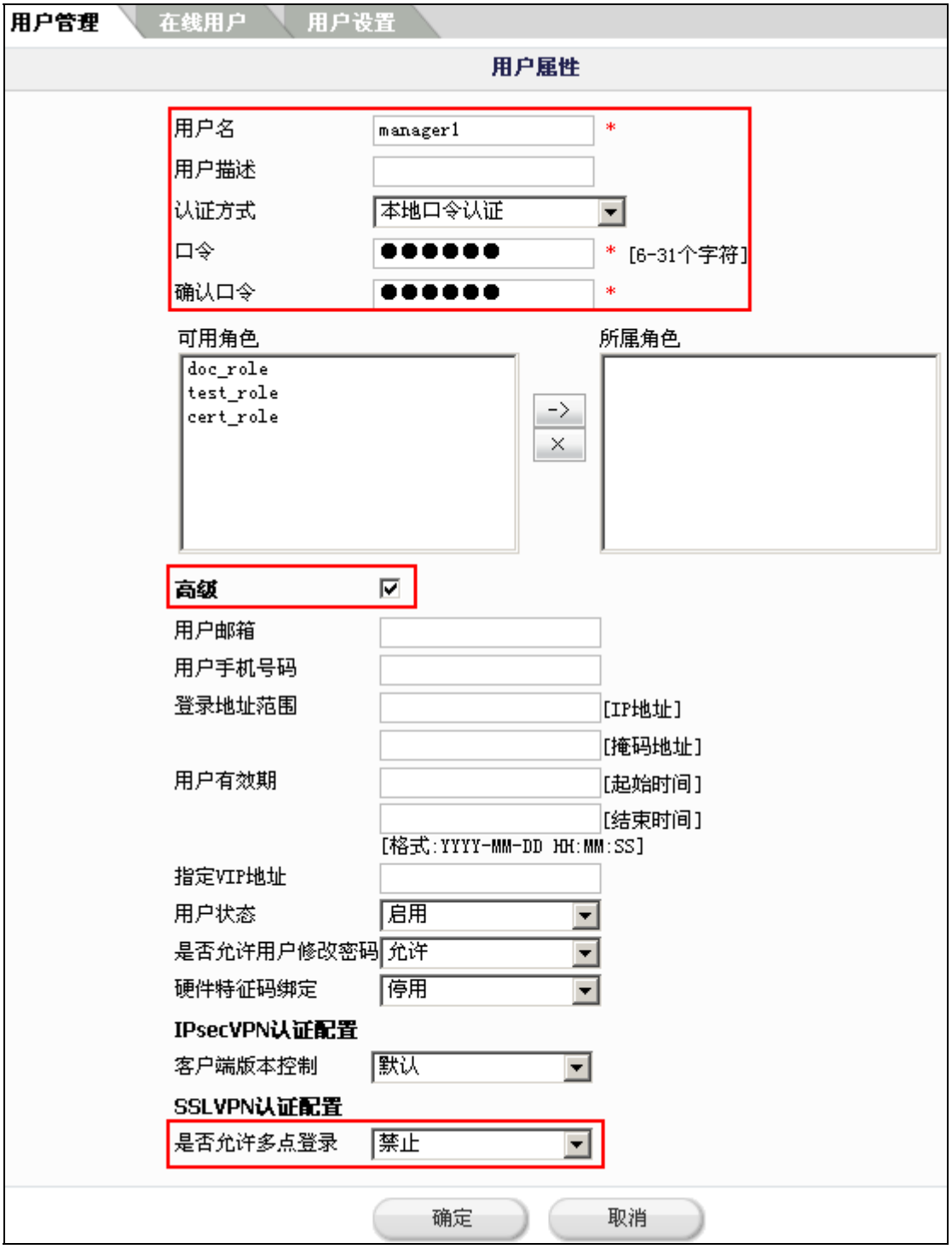
b）分别添加普通职员用户 user1 和经理用户 manager1。

① 添加普通职员用户 user1，禁止多点登录，如下图所示。



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。



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。

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。

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。

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。

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。

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。

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。

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。

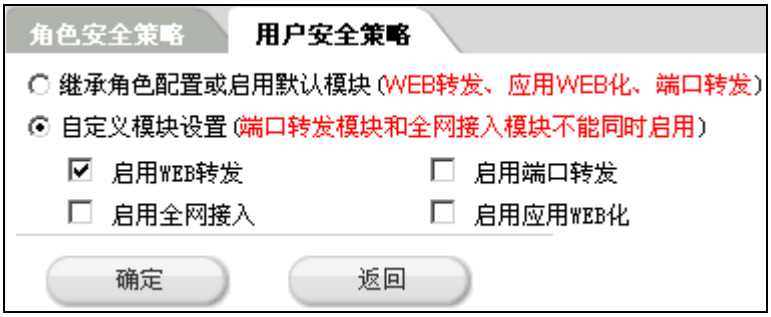
5．配置安全策略。

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。

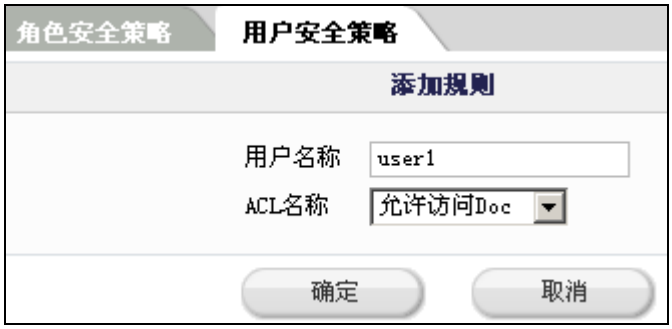
① 点击导航菜单 **SSLVPN > 安全策略**，然后选择“用户安全策略”页签，点击用户“user1”条目右侧的“安全策略设置”图标。

② 勾选“自定义模块设置”，然后选中“启用 web 转发”，如下图所示。



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。

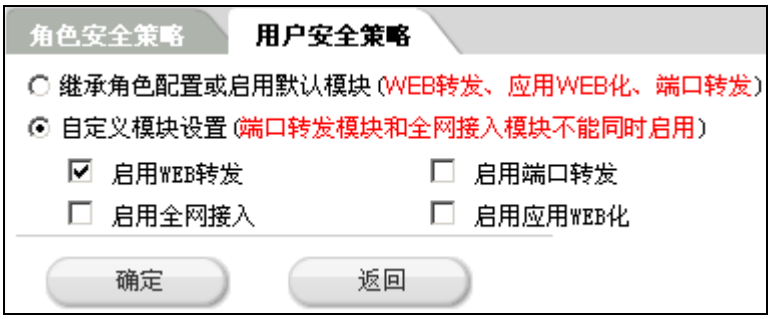


参数设置完成后，点击“确定”按钮。至此，用户“user1”的安全策略配置完成。

b）为用户“manager1”配置安全策略。

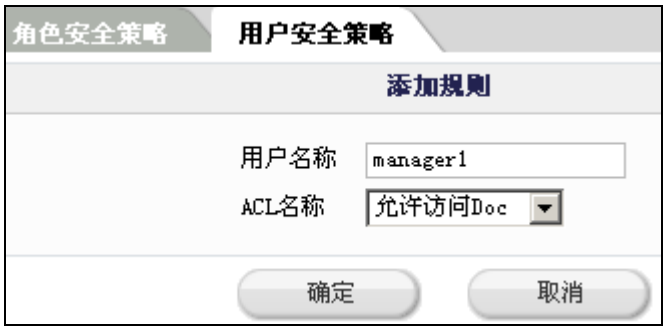
① 点击导航菜单 **SSLVPN > 安全策略**，然后选择“用户安全策略”页签，点击用户“manager1”条目右侧的“安全策略设置”图标。

② 勾选“自定义模块设置”，然后选中“启用 web 转发”，如下图所示。



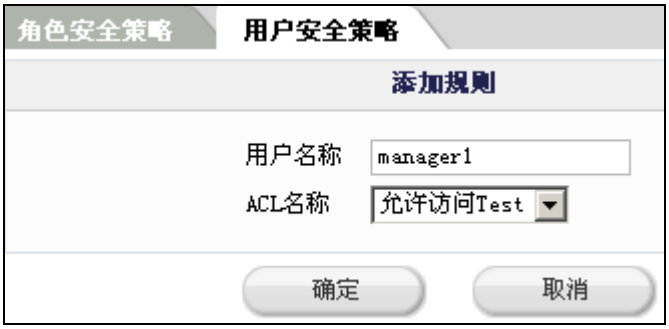
设置完成后，点击“确定”按钮。

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。



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。

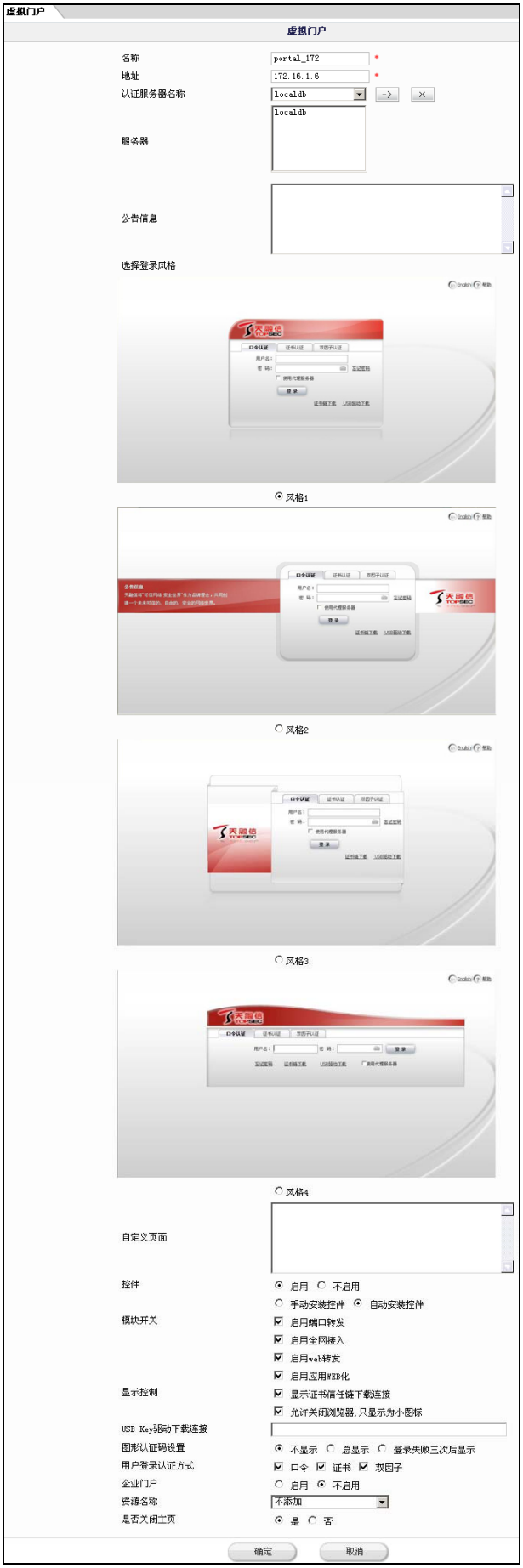


参数设置完成后，点击“确定”按钮。至此，用户“manager 1”的安全策略配置完成。

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。

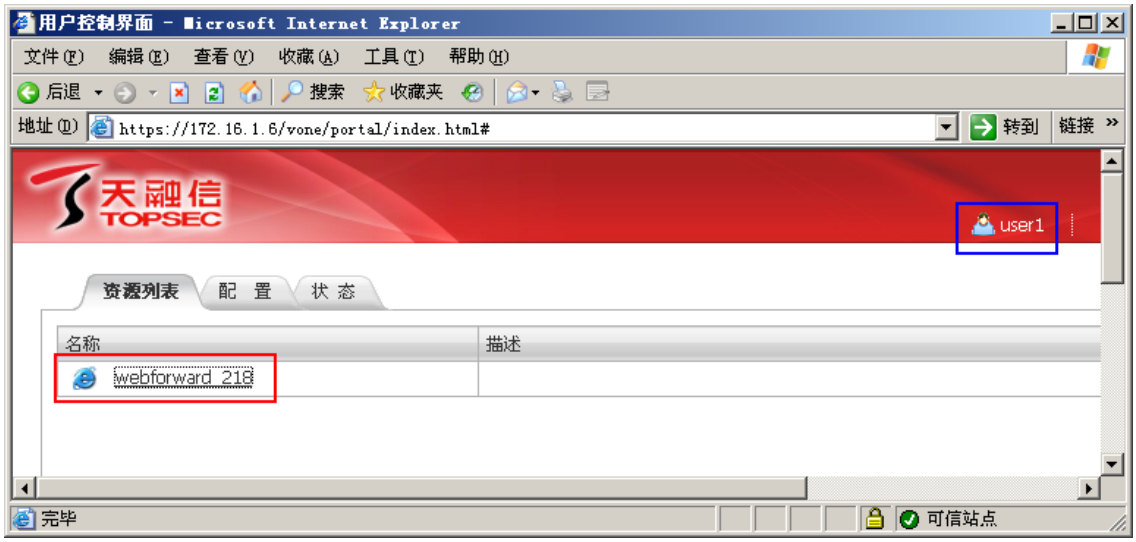

虚拟门户
虚拟门户
名称
portal_172
地址
172.16.1.6
认证服务器名称
localdb
服务器
localdb
公告信息
选择登录风格
风格1
风格2
风格3
风格4
自定义页面
控件
启用
不启用
手动安装控件
自动安装控件
模块开关
启用端口转发
启用全网接入
启用web转发
启用应用WEB化
显示控制
显示证书信任链下载连接
允许关闭浏览器,只显示为小图标
USB Key驱动下载连接
图形认证码设置
不显示
总显示
登录失败三次后显示
用户登录认证方式
口令
证书
双因子
企业门户
启用
不启用
资源名称
不添加
是否关闭主页
是
否
确定
取消

参数设置完成后，点击“确定”按钮。

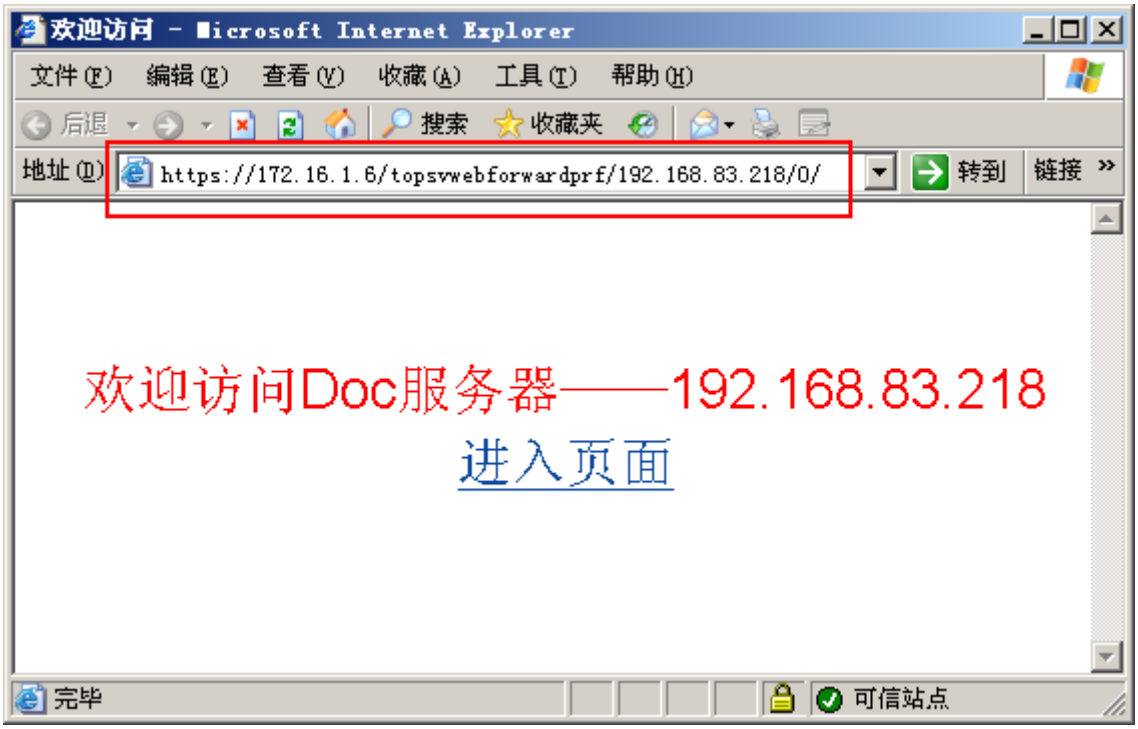
7．验证：在 SSL VPN 网关的用户界面中，用户成功登录后可以访问授权资源。

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。

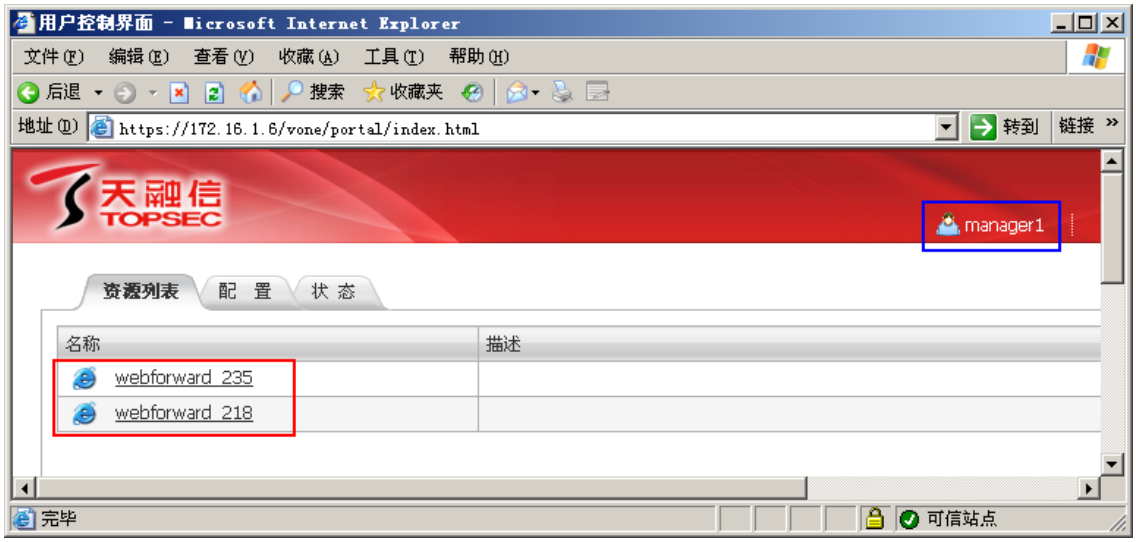
输入“user1”正确的用户名、密码，并成功登录后，尽管网关中已经定义了多个 Web 转发资源，但该用户只能访问可用资源（即：webforward_218），如下图所示。



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。



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。

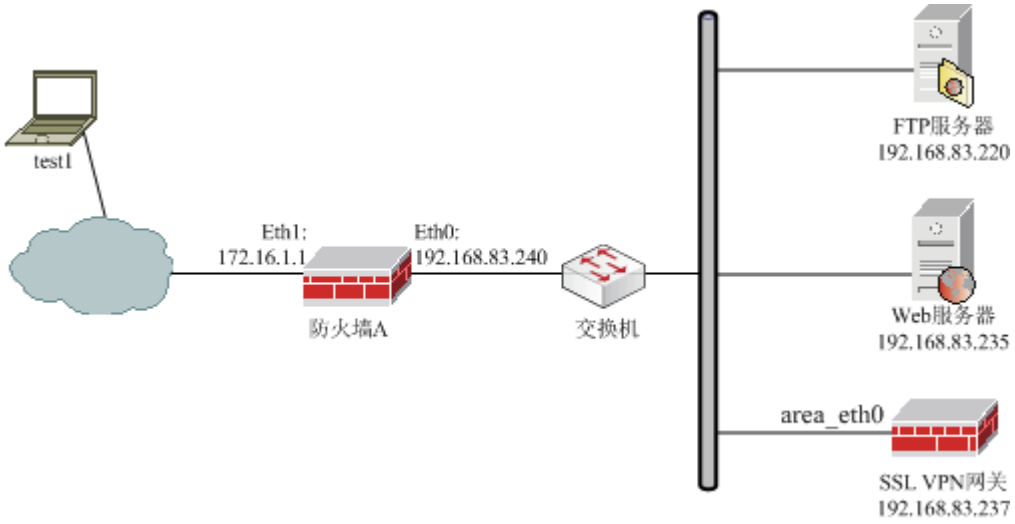


图 28 SSL VPN 网关端口转发示意图

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”。

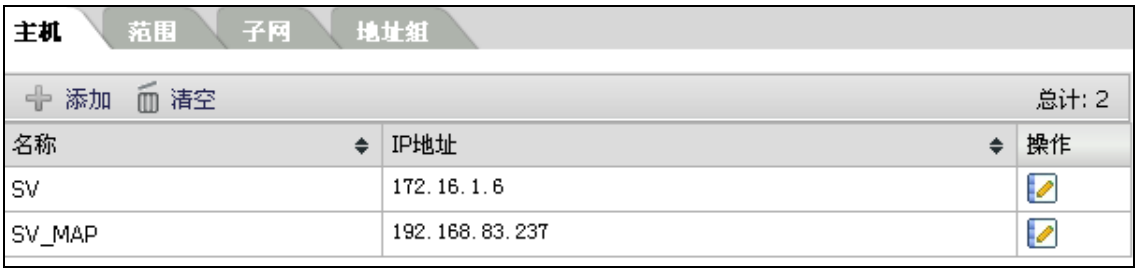
防火墙 A 的配置步骤

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。

2）定义访问控制规则，如下图所示。

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。

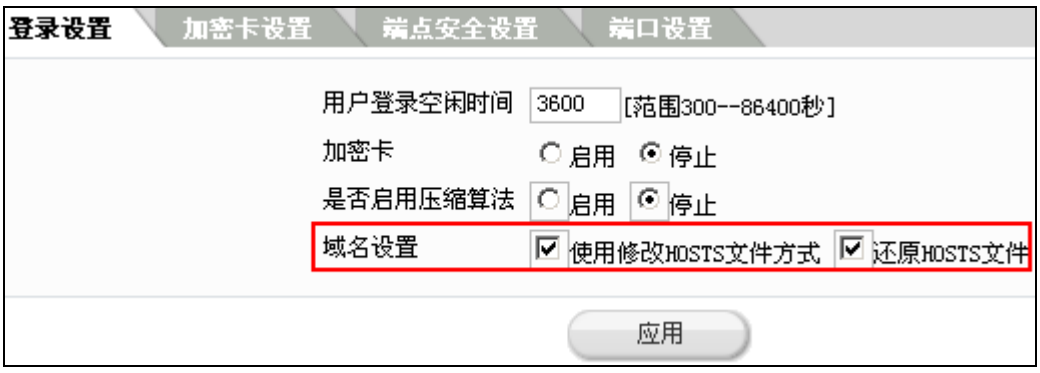


4）配置双向地址转换（到 SSL VPN 网关的映射），如下图所示。

WEBUI 配置步骤

1. 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。



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。

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。

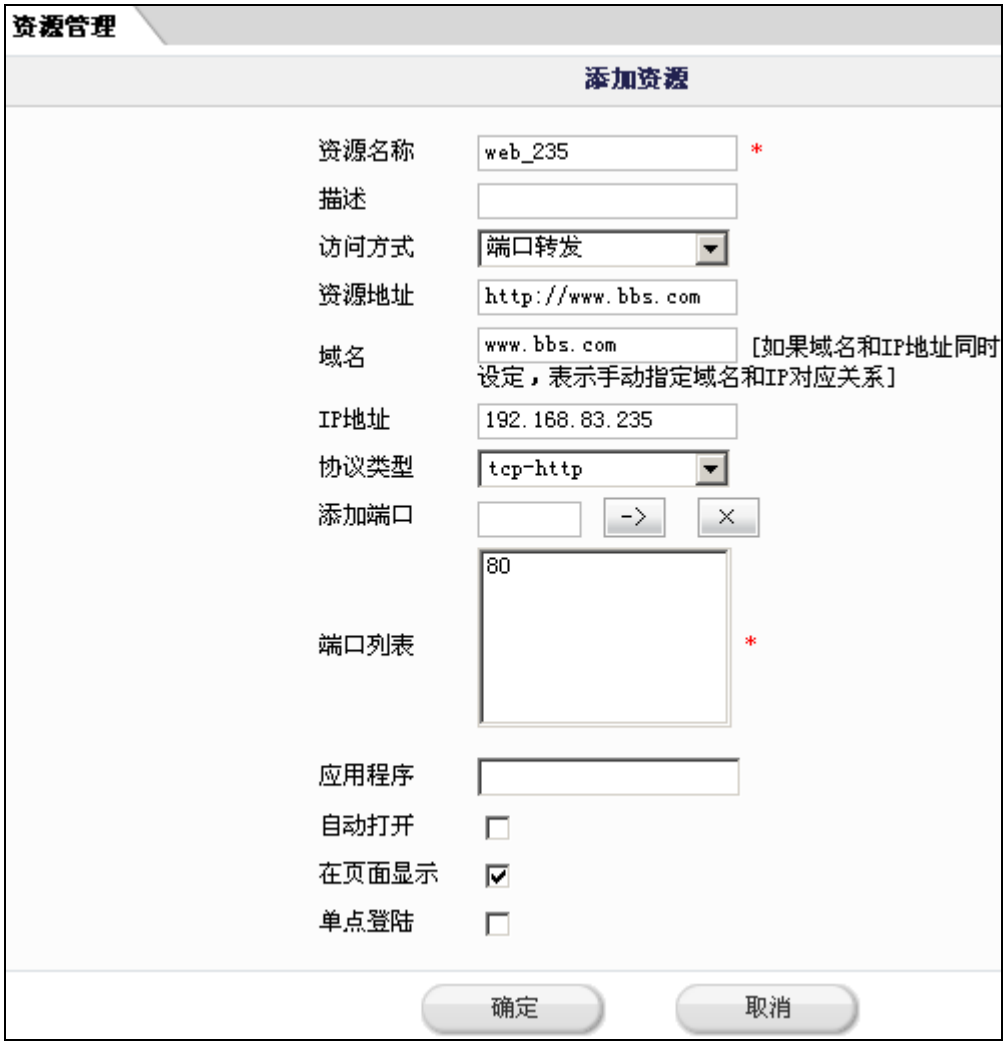
参数设置完成后，点击“确定”按钮完成配置。

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。

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”，配置端口转发资源“web_235”，如下图所示。



参数设置完成后，点击“确定”按钮。

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。

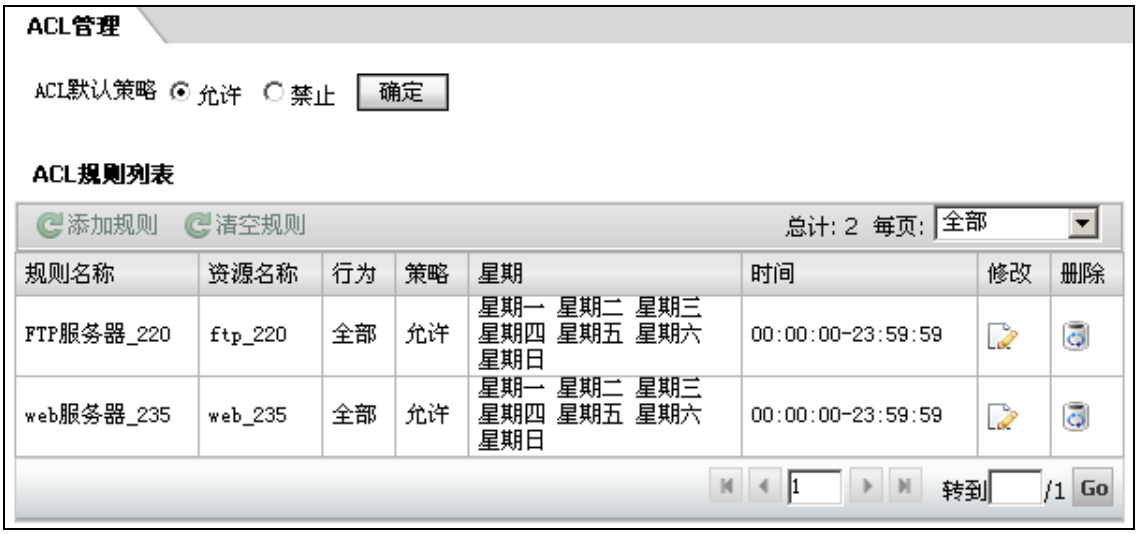
设置完成后，点击“确定”按钮即可。

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。

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。

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。

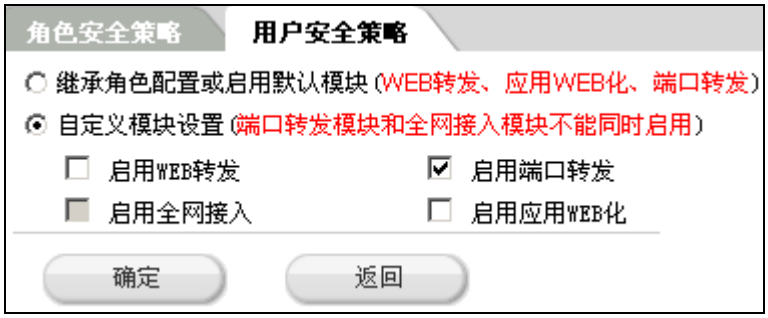


6．配置安全策略。

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。

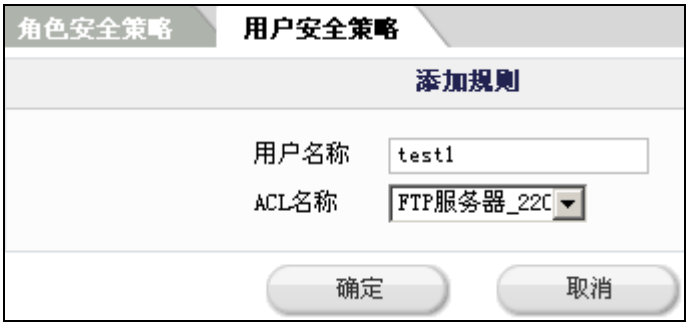


设置完成后，点击“确定”按钮。

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。

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。

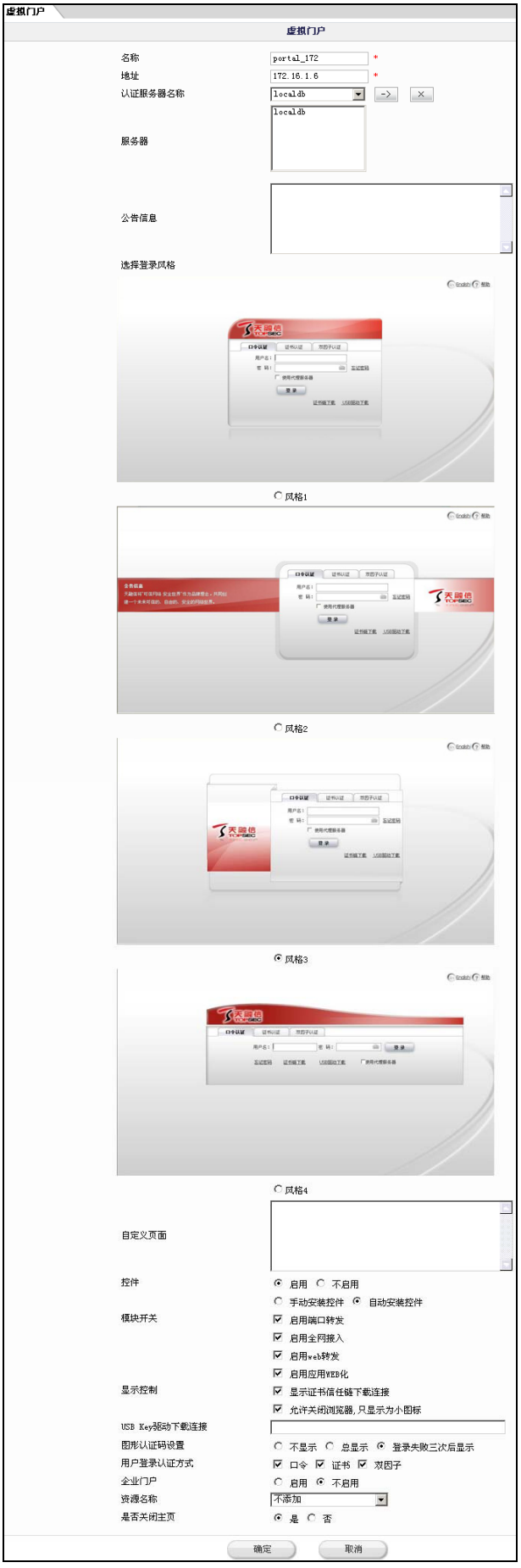


参数设置完成后，点击“确定”按钮。至此，用户“test1”的安全策略配置完成。

7．配置虚拟门户。

a）点击导航菜单 **SSLVPN > 虚拟门户**。

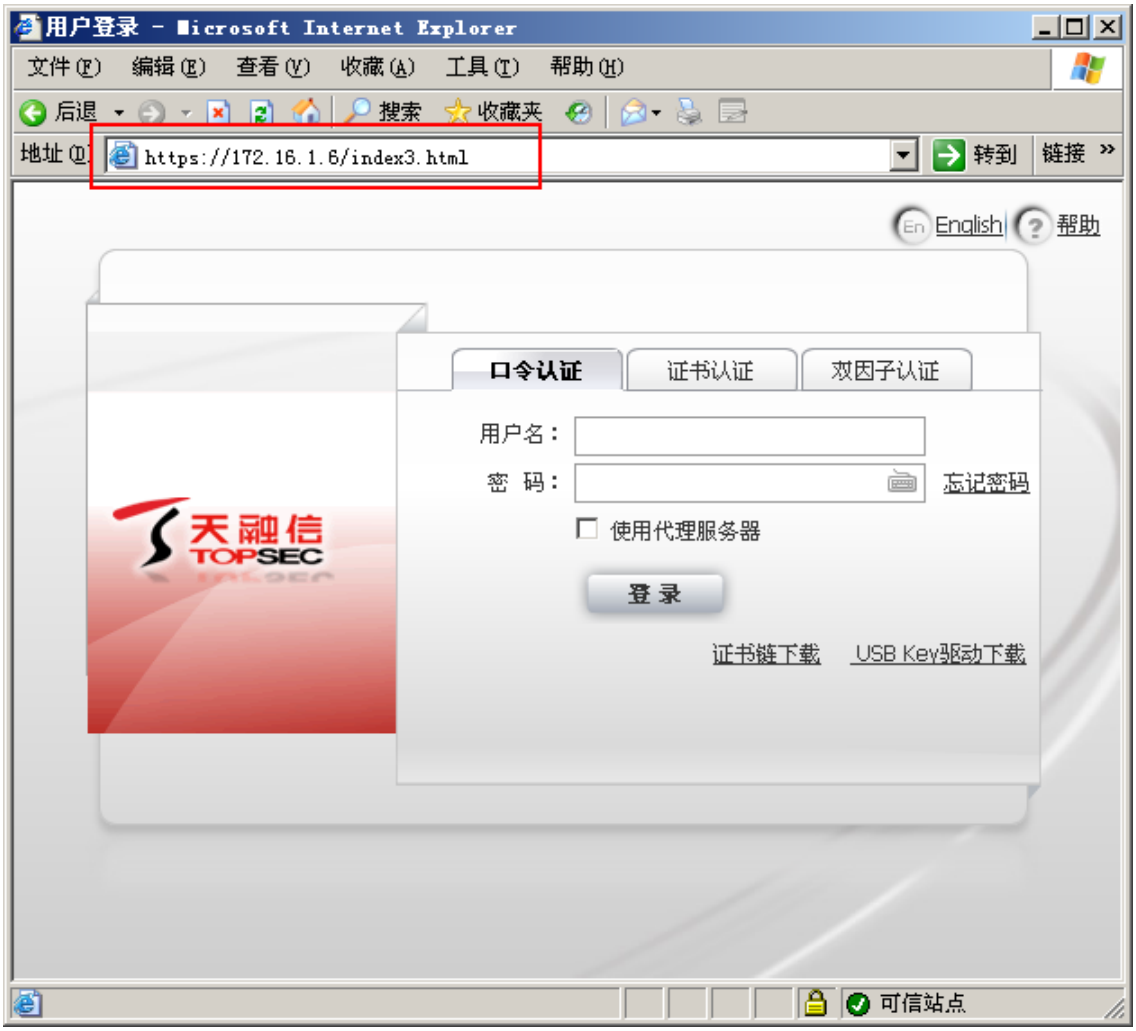
b）点击虚拟门户列表左上方的“添加”，自定义远程用户访问 SSL VPN 网关的用户界面。自定义虚拟门户时，参数“地址”必须配置为远程用户登录 SSL VPN 网关时的地址，即 SSL VPN 网关的对外 IP“172.16.1.6”，参数“认证服务器名称”必须配置为对远程用户进行认证的服务器名称，此案例为本地认证服务器“localdb”，而且必须启用端口转发开关，具体配置页面如下图所示。


虚拟门户
虚拟门户
名称
portal_172
地址
172.16.1.6
认证服务器名称
localdb
服务器
localdb
公告信息
选择登录风格
风格1
风格2
风格3
风格4
自定义页面
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驱动下载连接
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
不启用
资源名称
不添加
是否关闭主页
是
否
确定
取消

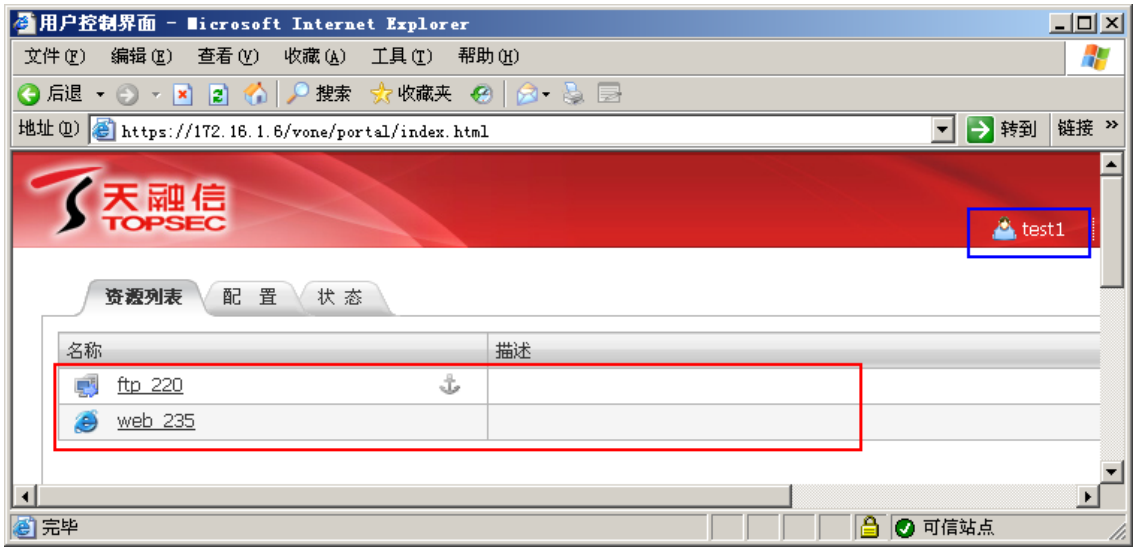
c）参数设置完成后，点击“确定”按钮。

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”。

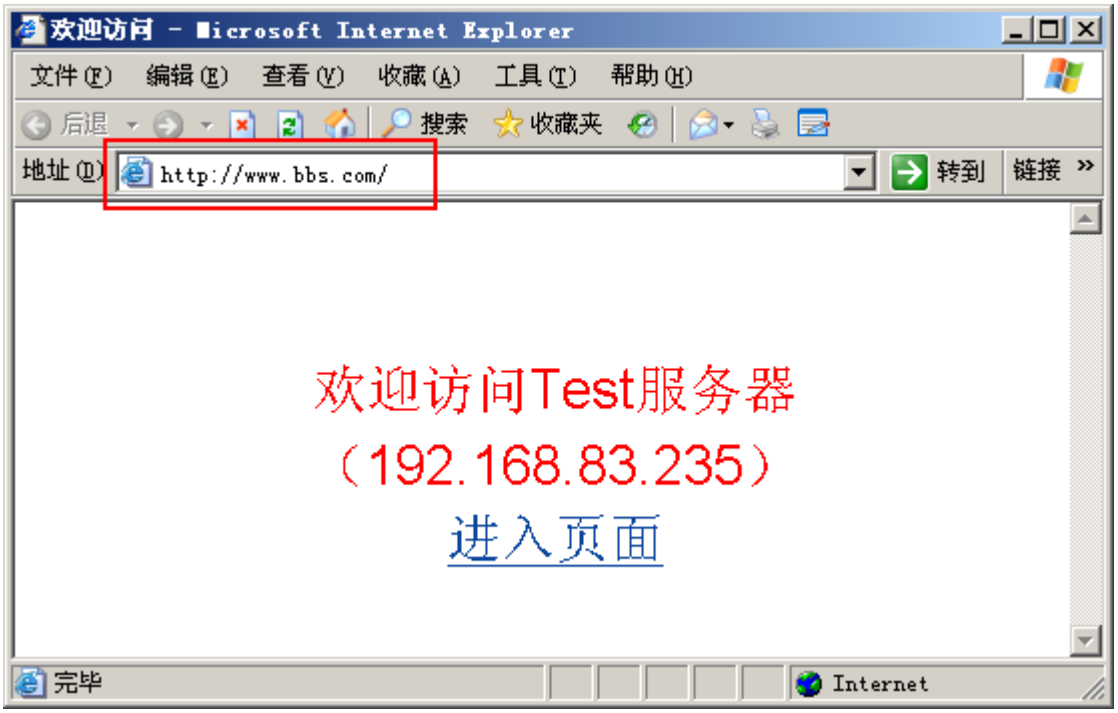
1）在浏览器的 URL 地址栏输入 SSL VPN 网关的外网地址“https://172.16.1.6”，进入用户登录界面，界面如下图所示。



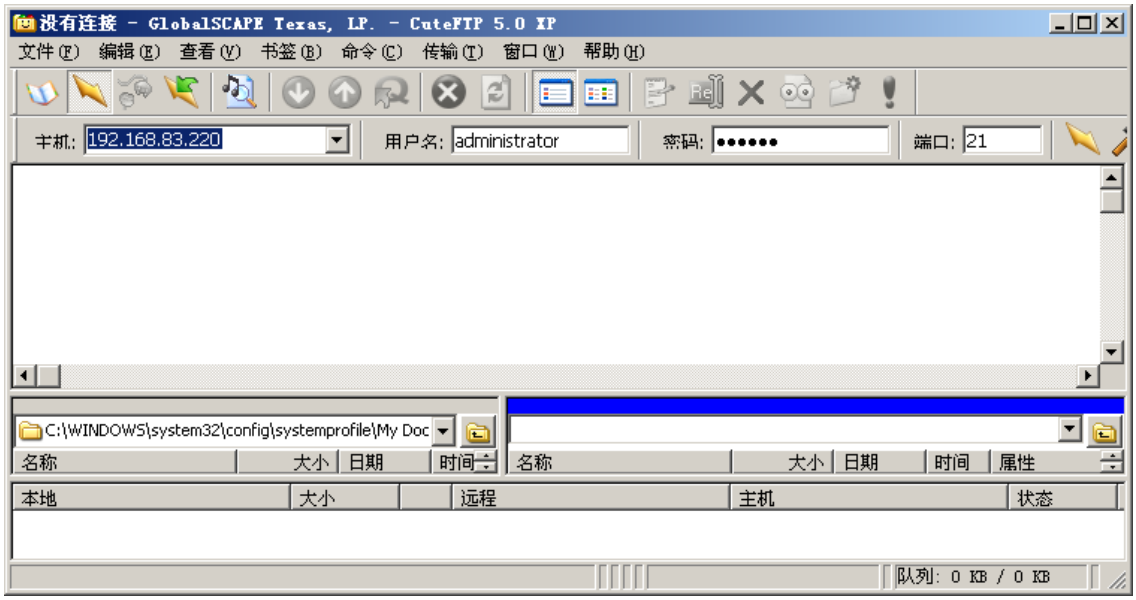
2）输入“test1”正确的用户名、密码，并成功登录后，用户界面中显示可用资源“web_235”和“ftp_220”，如下图所示。



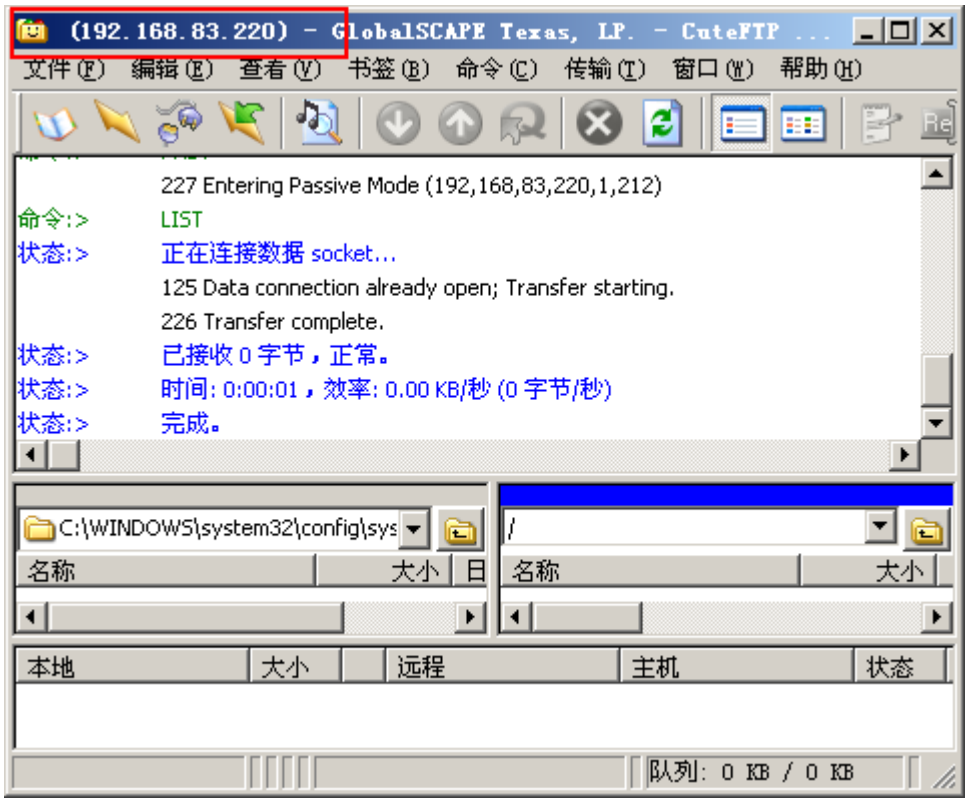
3）点击“web_235” 链接后，成功以域名“www.bbs.com”访问 Web 服务器“192.168.83.235”，如下图所示。



4）点击“ftp_220”条目右侧的“ ”，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。



稍候，远程用户通过 CuteFTP 客户端登录到 FTP 服务器“192.168.83.220”，如下图所示。



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：

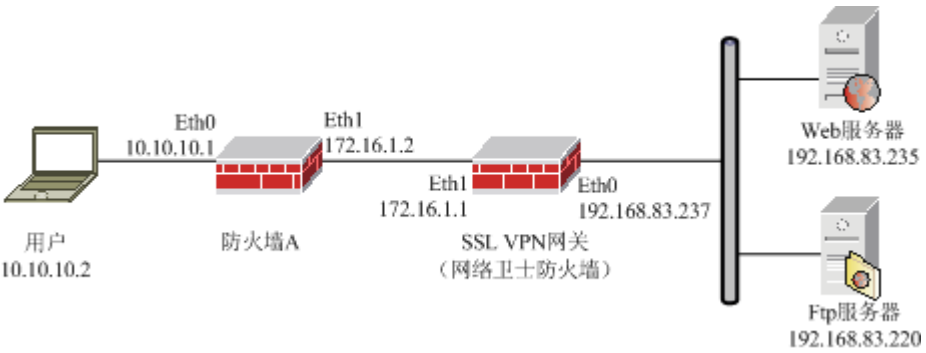


图 29 SSL VPN 网关全网接入示意图

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”。

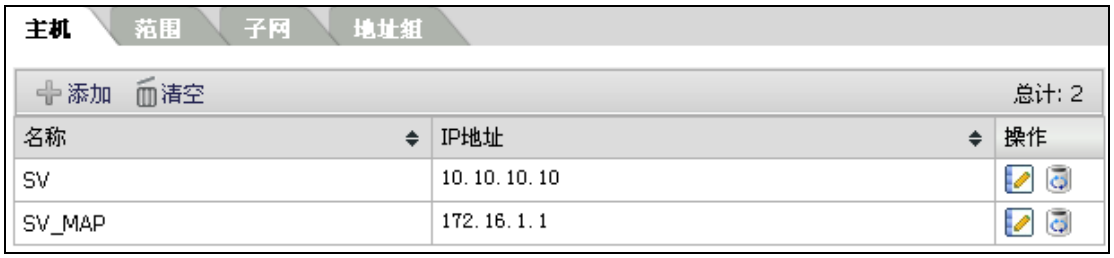
防火墙 A 的配置步骤

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。

2）定义访问控制规则，如下图所示。

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。



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。

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。

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。

参数设置完成后，点击“确定”按钮即可。

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。

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。

参数设置完成后，点击“确定”按钮即可。

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。

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。

参数设置完成后，点击“确定”按钮使配置生效。

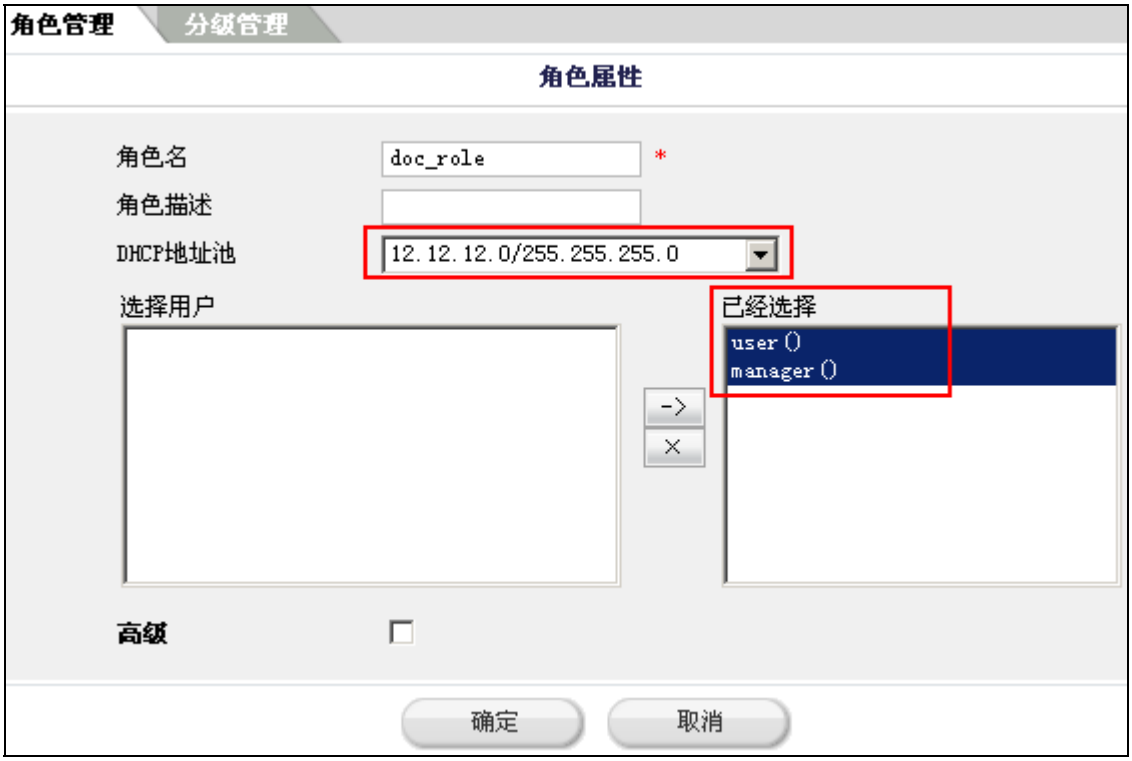
c）点击“添加用户”，设置用户“manager”的用户信息，如下图所示。

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。

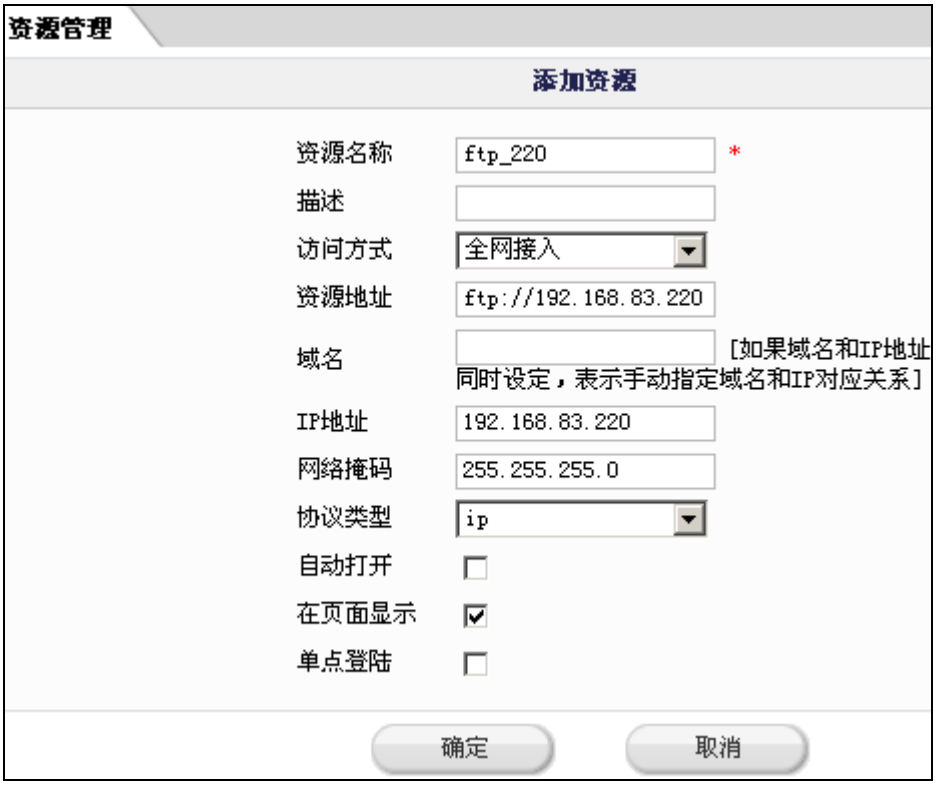
b）设置角色“doc_role”的信息，然后将用户“user”和“manager”添加到该组中，如下图所示。



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。



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”，配置全网接入资源“web_235”，如下图所示。

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。

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。

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。

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。

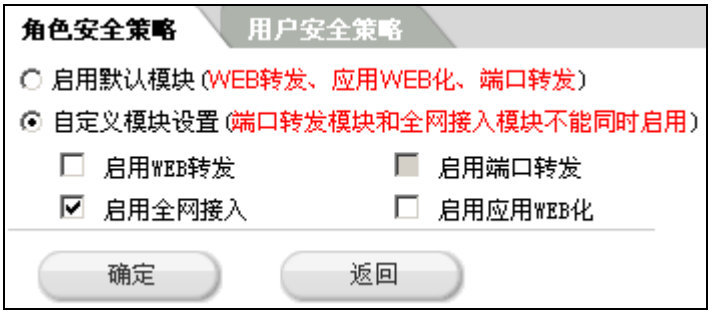
9．配置安全策略。

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。

① 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。



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”。

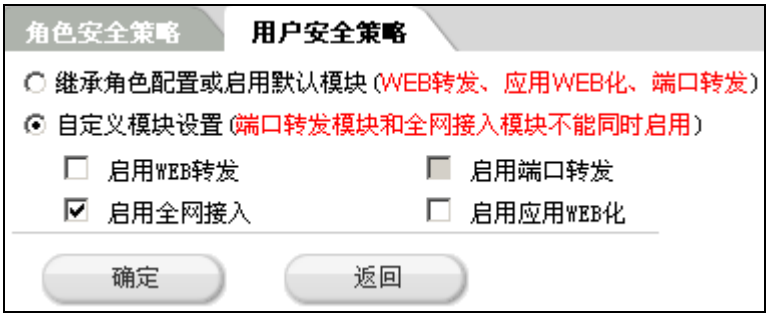
③ 点击“添加规则”，将允许访问公司内网 Web 资源的 ACL 规则“web 服务器_235”赋予该角色，如下图所示。

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。

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“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。



设置完成后，点击“确定”按钮。

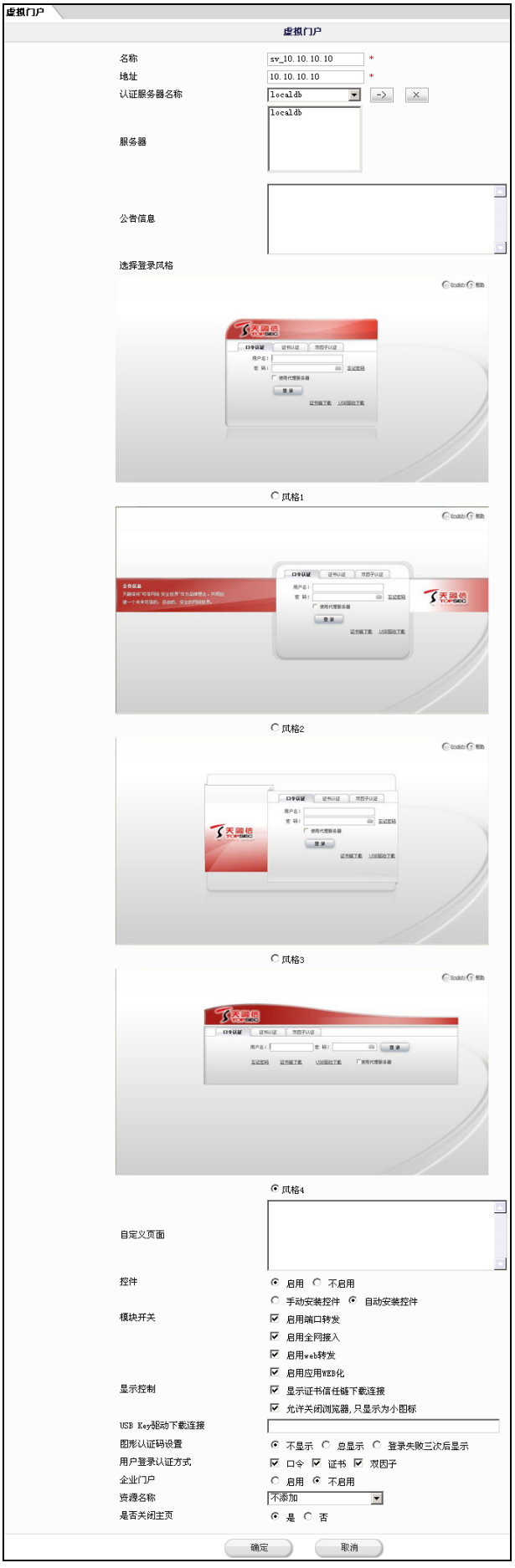
③ 点击“添加规则”，将允许访问公司内网 ftp 资源的 ACL 规则“FTP 服务器_220”赋予该用户，如下图所示。

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。


虚拟门户
虚拟门户
名称
sv_10.10.10.10
地址
10.10.10.10
认证服务器名称
localdb
服务器
localdb
公告信息
选择登录风格
风格1
风格2
风格3
风格4
自定义页面
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驱动下载连接
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
不启用
资源名称
不添加
是否关闭主页
是
否
确定
取消

c）参数设置完成后，点击“确定”按钮。

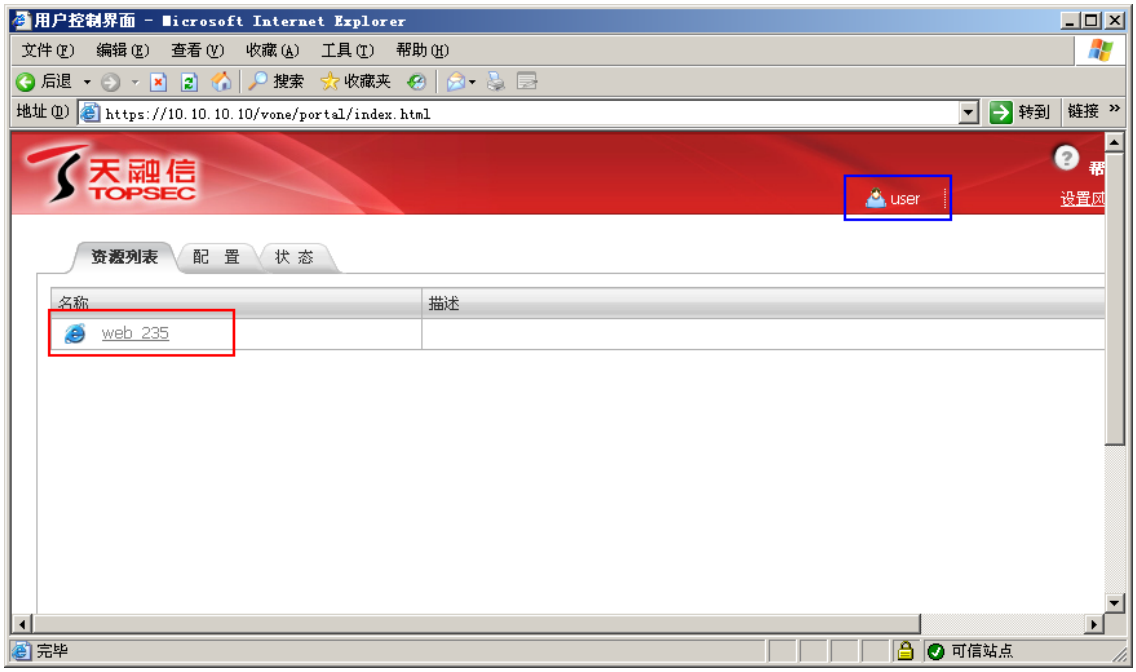
11．验证：用户“user”登录成功后，可以访问授权的全网接入资源“web_235”；用户“manager”登录成功后，可以访问授权的全网接入资源“web_235”和“ftp_220”。

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。

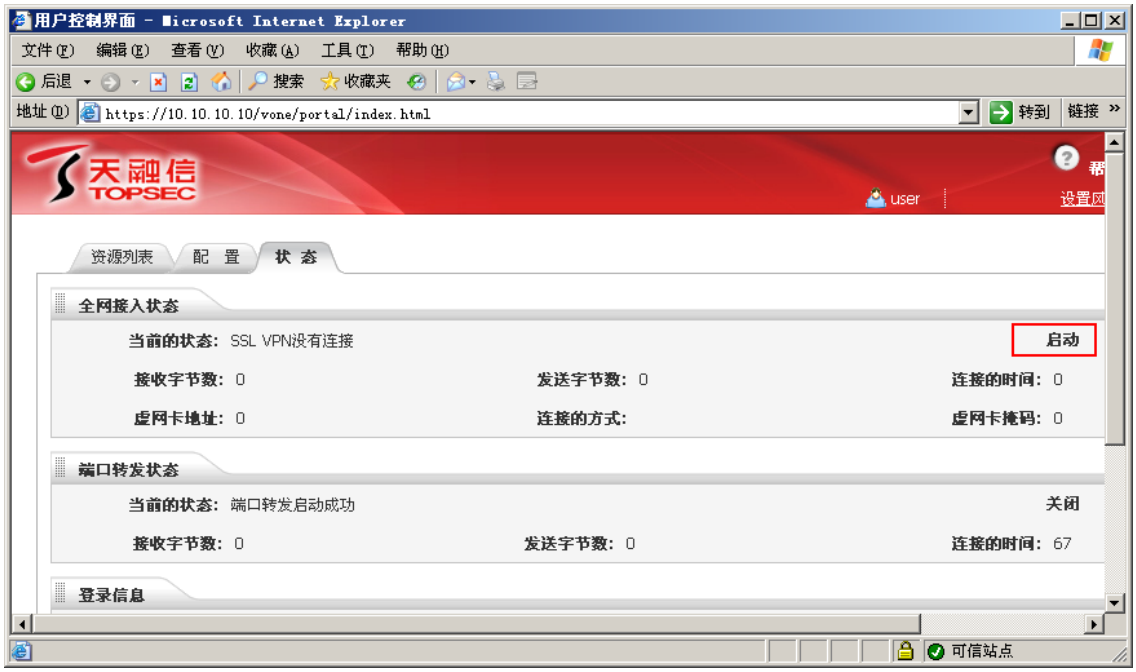
a）在浏览器的 URL 地址栏输入 SSL VPN 网关的外网地址“https://10.10.10.10”，进入用户登录界面，界面如下图所示。

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。



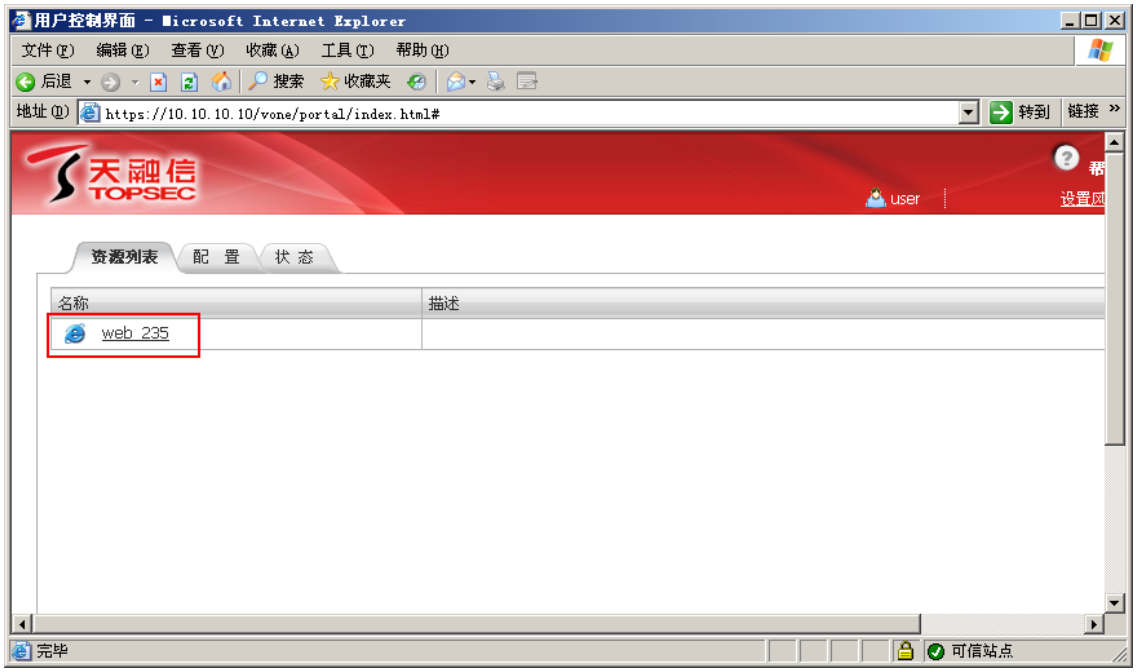
由于没有启动全网接入客户端，所以该资源名称为灰色不可用状态。

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。

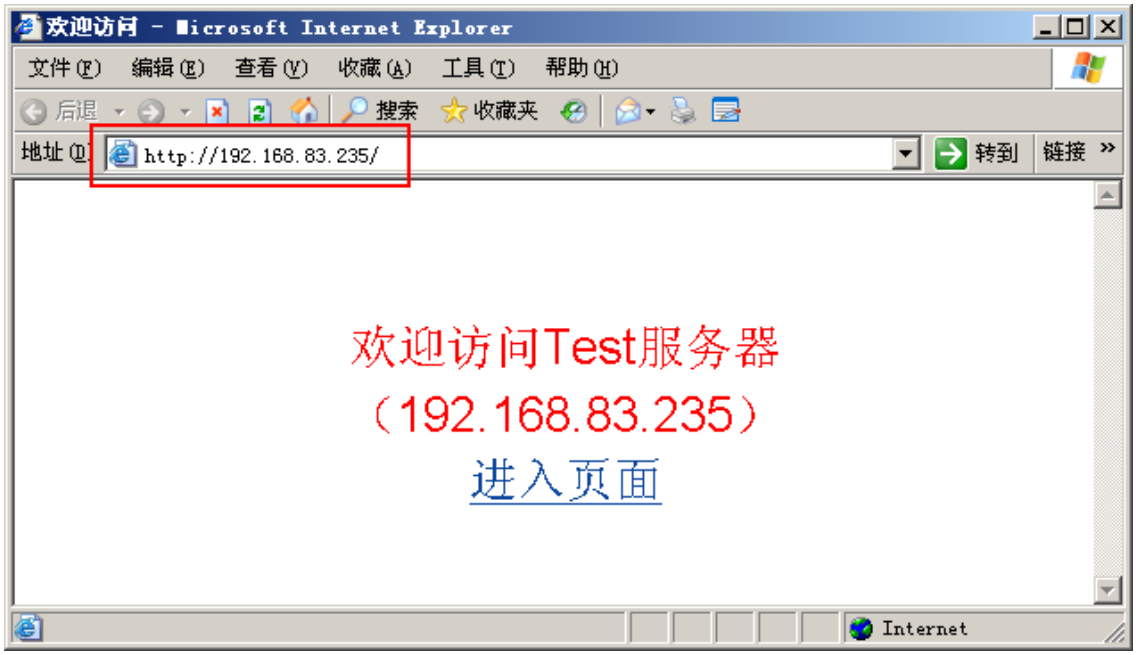


d）全网接入客户端与服务器成功建立连接后，客户端状态如下图所示。

e）激活“资源列表”页签，“web_235”资源可用，如下图所示。



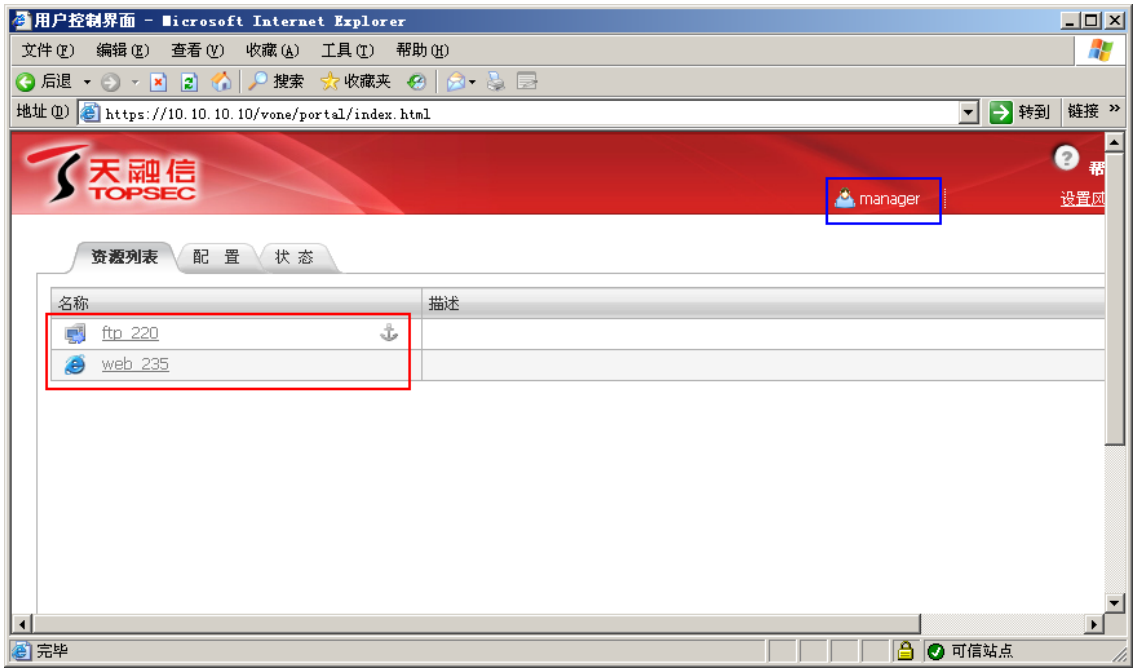
f）点击“web_235”链接后，可以成功访问 Web 服务器“192.168.83.235”，如下图所示。



2）用户“manager”登录 SSL VPN 网关。

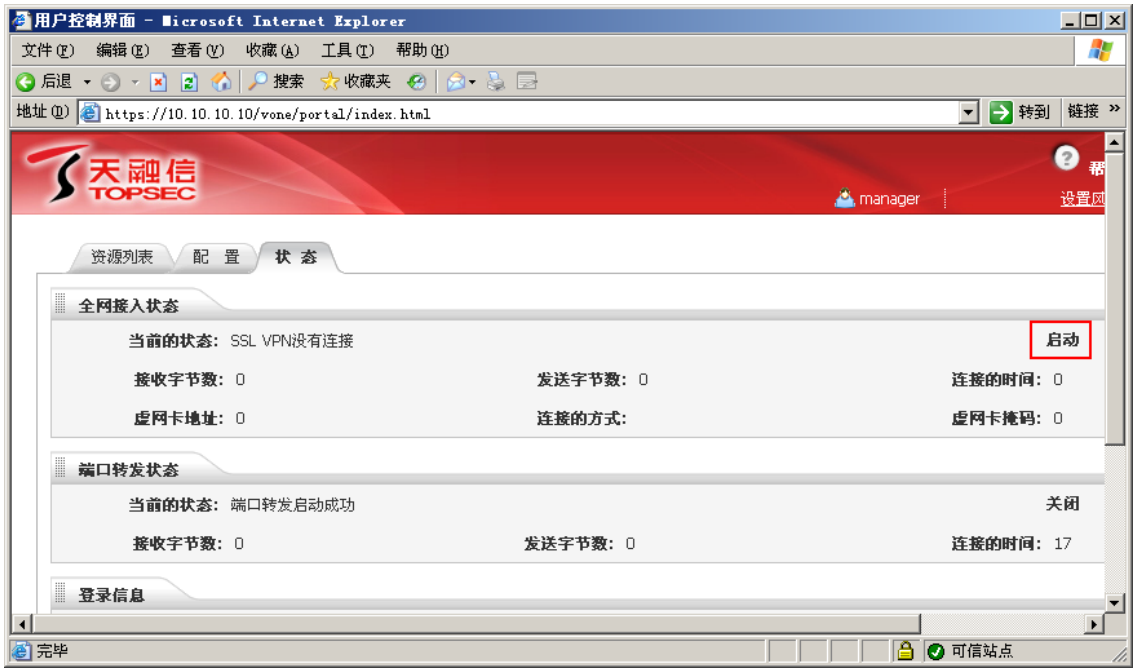
a）在浏览器的 URL 地址栏输入 SSL VPN 网关的外网地址“https://10.10.10.10”，进入用户登录界面，界面如下图所示。

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。



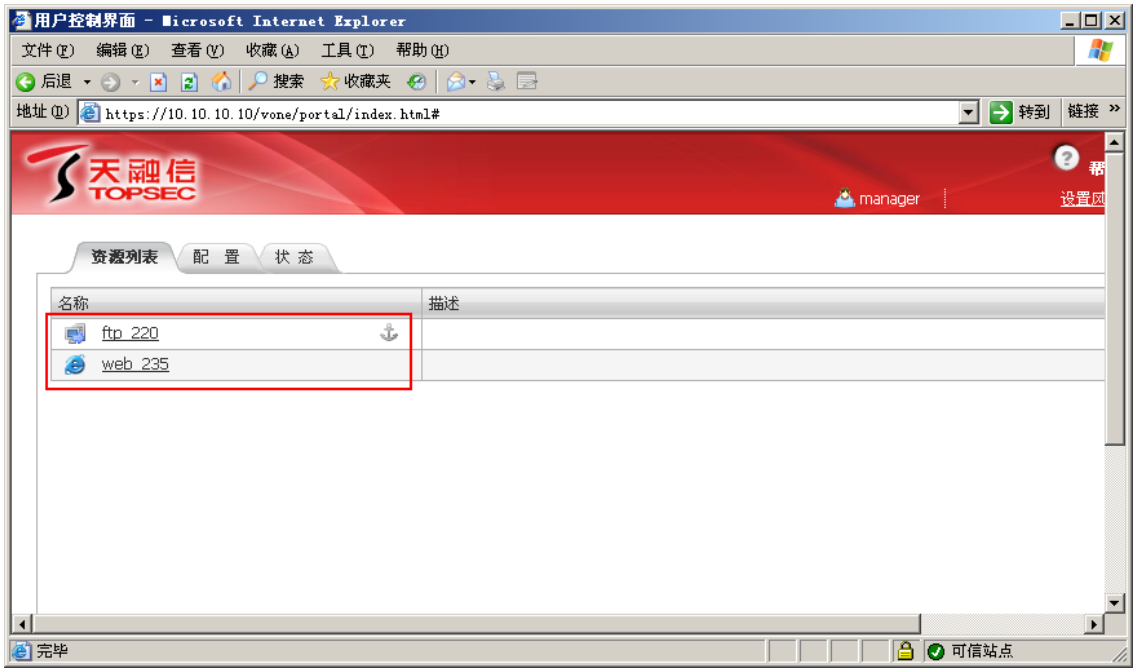
由于没有启动全网接入客户端，所以资源名称为灰色不可用状态。

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。

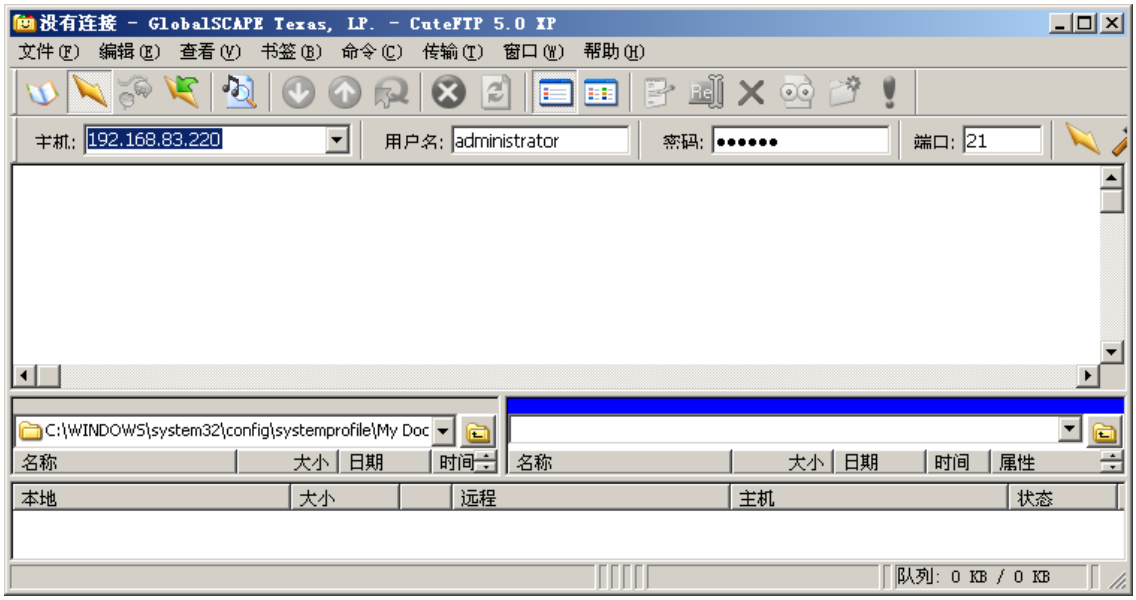


d）全网接入客户端与服务器成功建立连接后，客户端状态如下图所示。

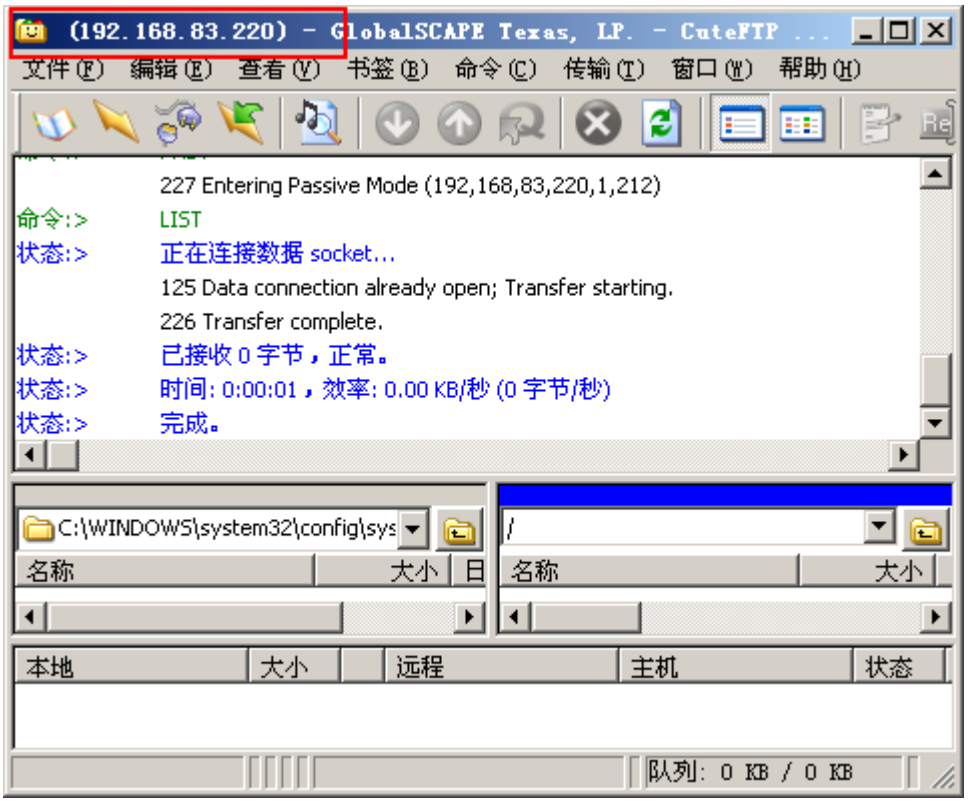
e）激活“资源列表”页签，“web_235”和“ftp_220”资源可用，如下图所示。



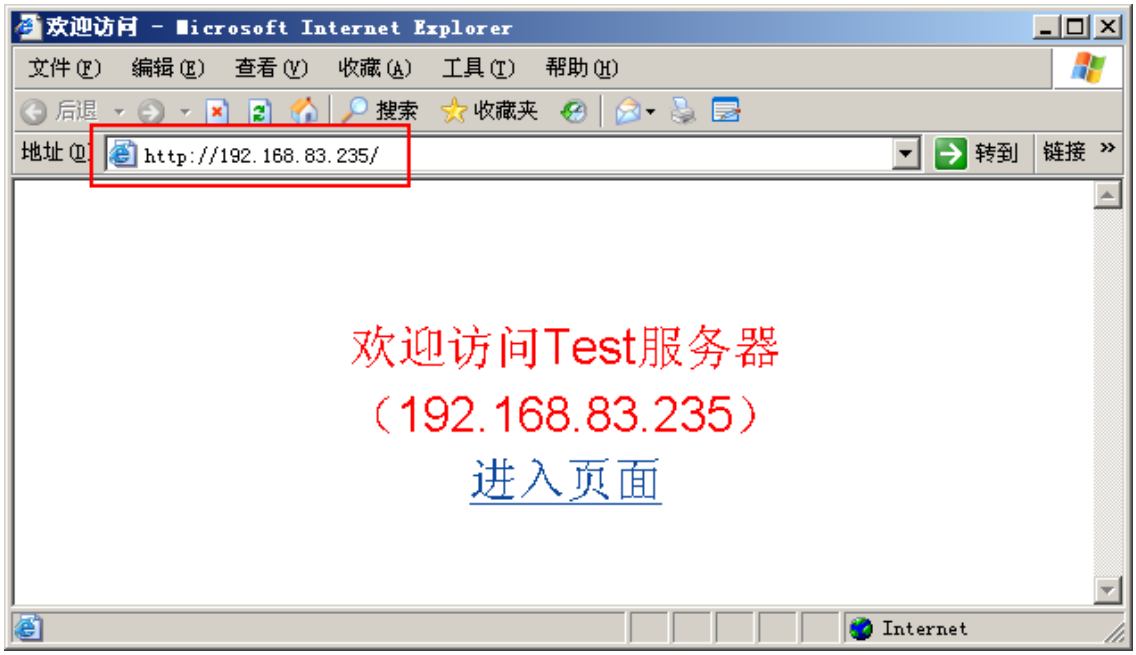
f）点击“ftp_220”条目右侧的“ ”，选择客户端程序为“CuteFTP”，然后在用户界面中点击“ftp_220”链接，自动弹出 CutpFTP 客户端，在客户端界面中输入主机地址、用户名和密码后点击连接图标“ ”，如下图所示。



稍候，远程用户通过 CuteFTP 客户端登录到 FTP 服务器“192.168.83.220”，如下图所示。



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。

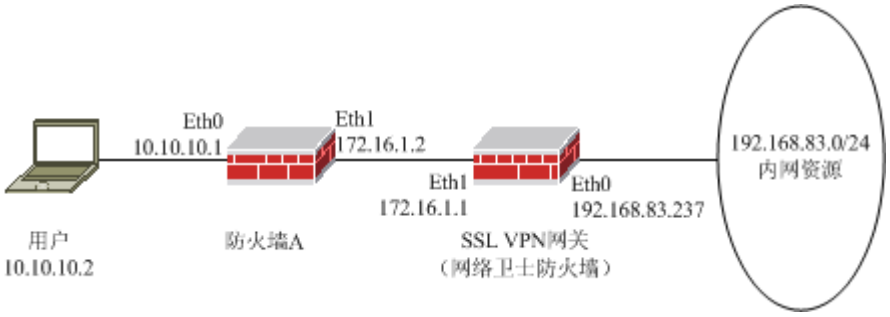


图 30 本地证书认证的网络部署图

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。

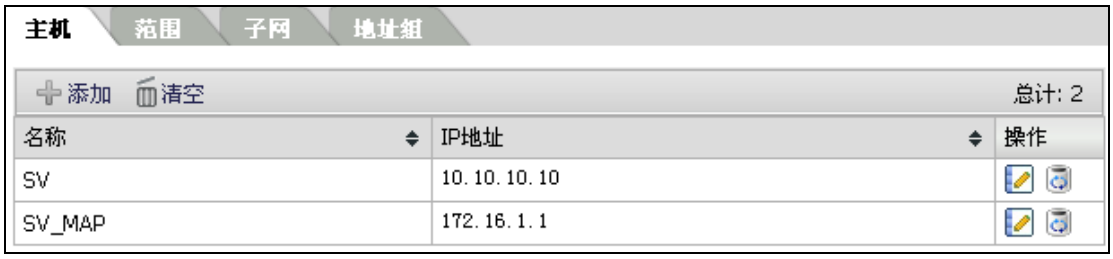
防火墙 A 的配置步骤

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。

2）定义访问控制规则，如下图所示。

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。



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

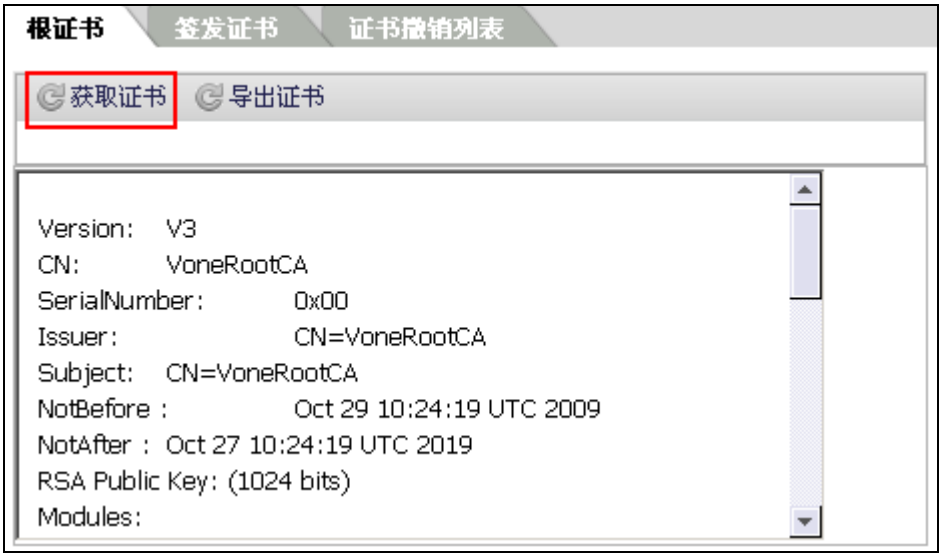
1．开启 Eth1 所属区域的 SSLVPN 服务。

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。

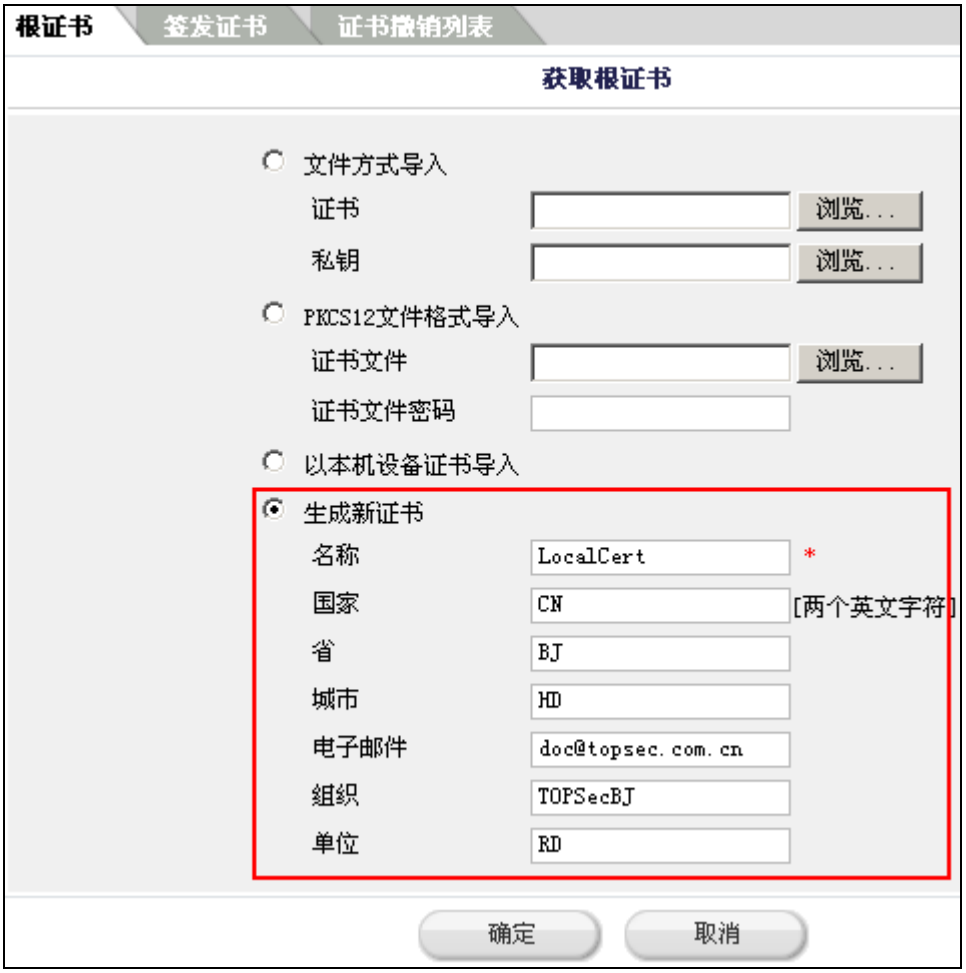
参数设置完成后，点击“确定”按钮即可。

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。



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。



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。

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。

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。

参数设置完成后，点击“确定”按钮使配置生效。

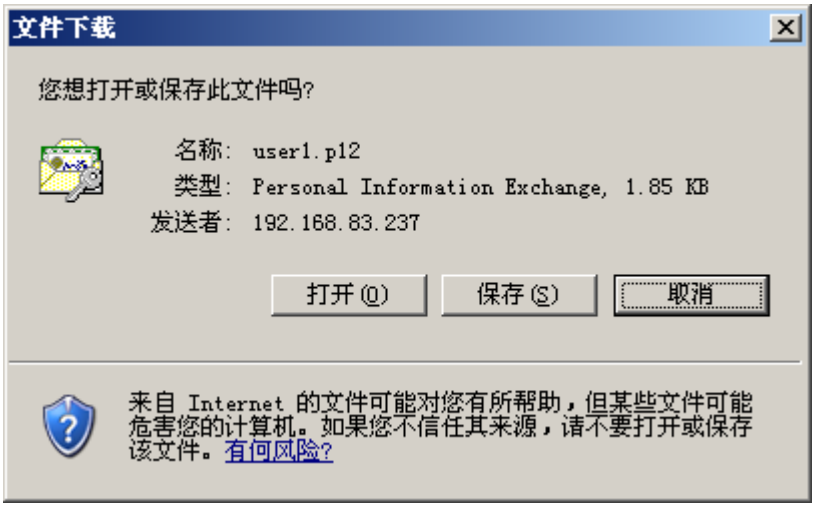
两种移动用户的区别在于“单位（OU）”项的内容不同。根据该项的区别，SSL VPN 网关将在移动用户登录时判断身份，然后把用户归类入不同的角色中。

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。

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。

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。



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。

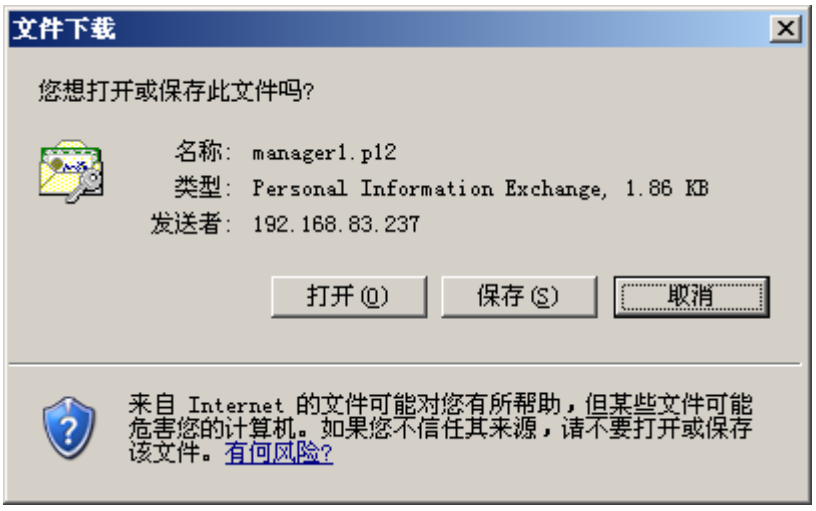
5）将“manager1”的证书保存到本地。

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。

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。

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。



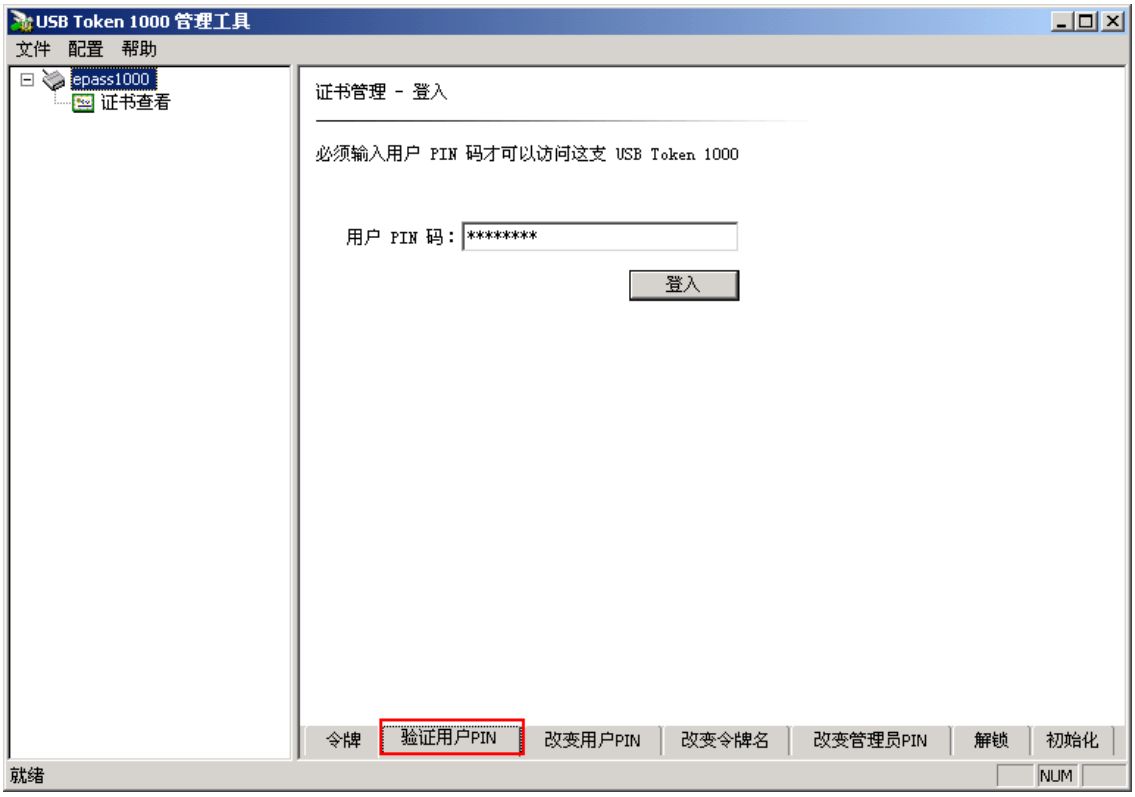
④ 点击“保存”按钮，在文件保存窗口中为证书文件指定保存路径后，点击“保存”按钮即可。

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。

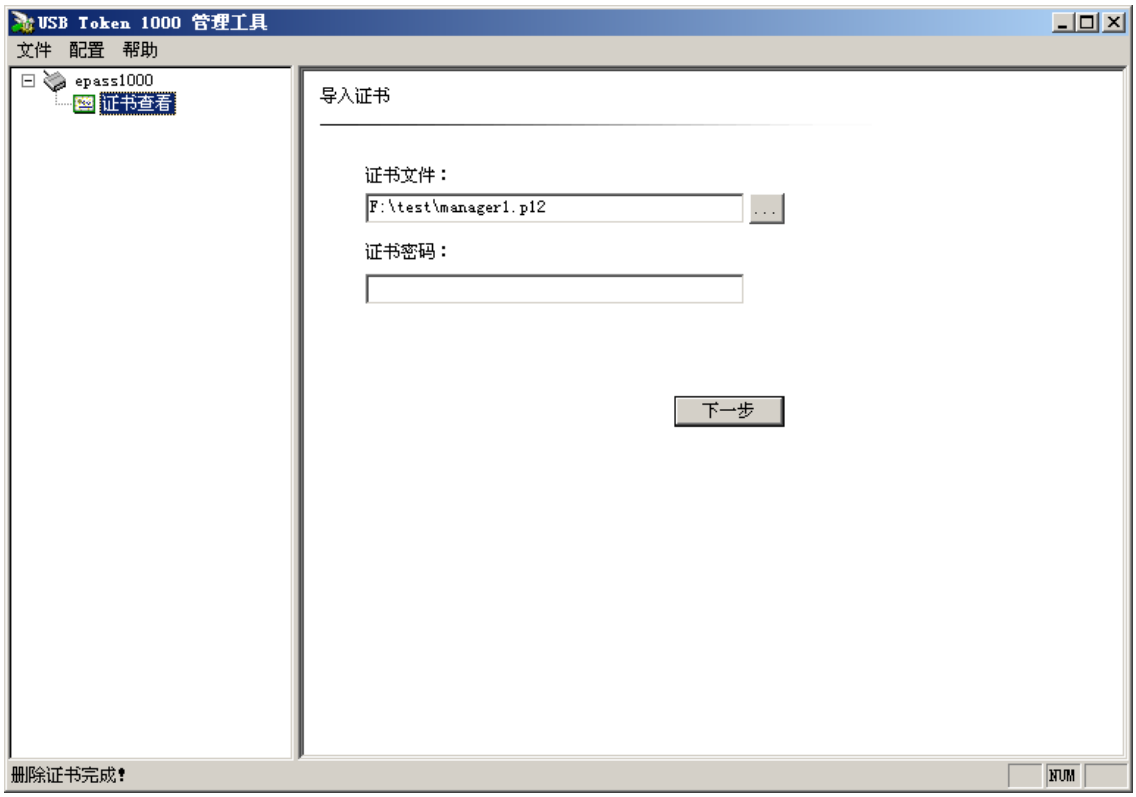
c）双击证书写入工具“ePassMgr.exe”，进入“USB Token 1000 管理工具”界面，激活右侧界面下方的“验证用户 PIN”，然后输入正确的 PIN 码，如下图所示。



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。

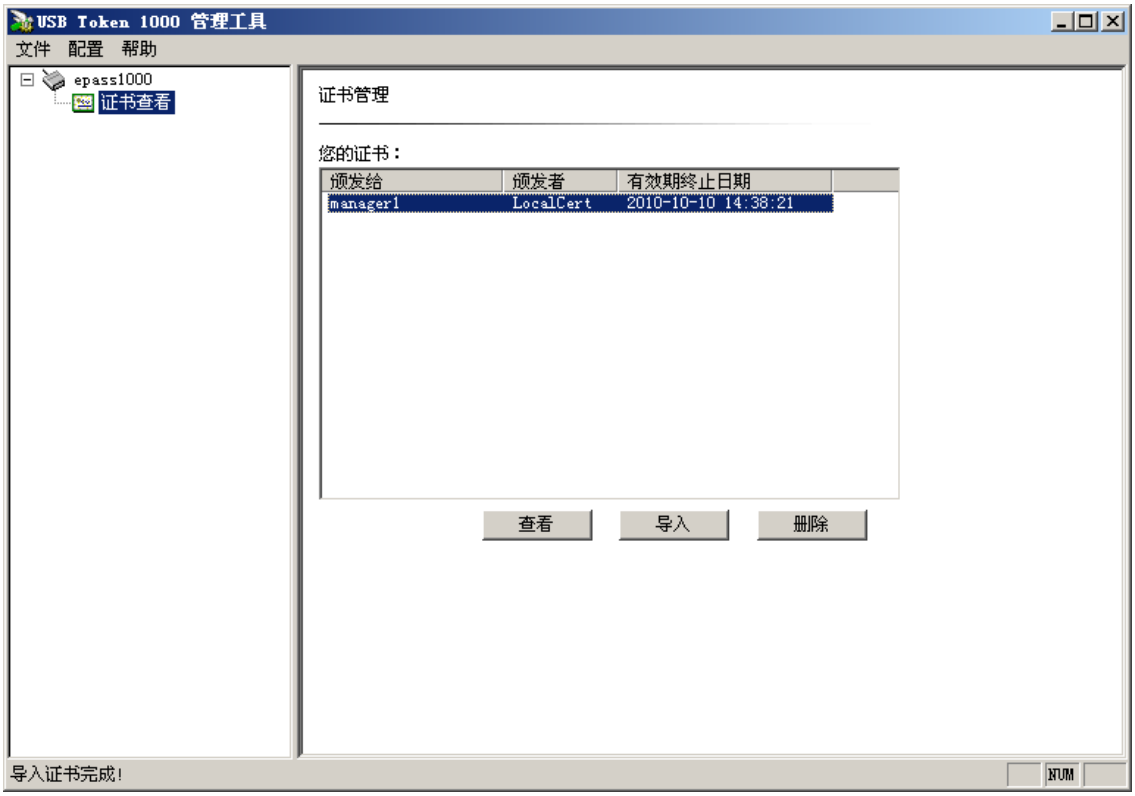
点击“确定”按钮后，导入证书的界面如下图所示。

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。



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，如下图所示。



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。

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。

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

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。

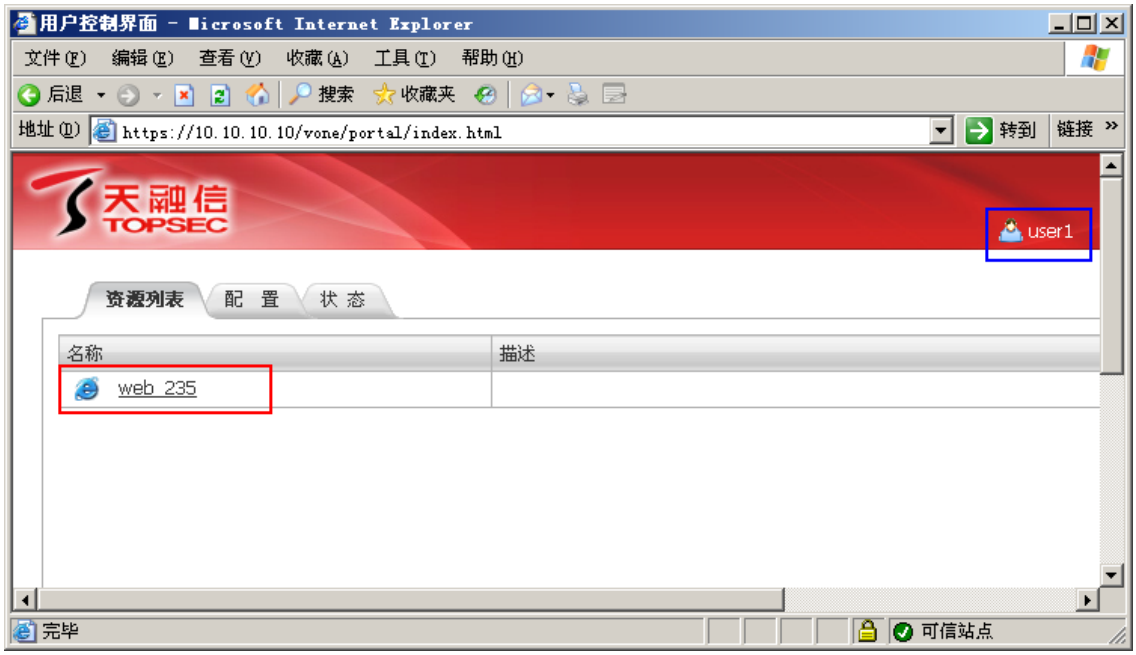
1）用户“user1”采用文件方式证书登录 SSL VPN 网关（对外 IP 为 10.10.10.10）。

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。

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。

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。



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。

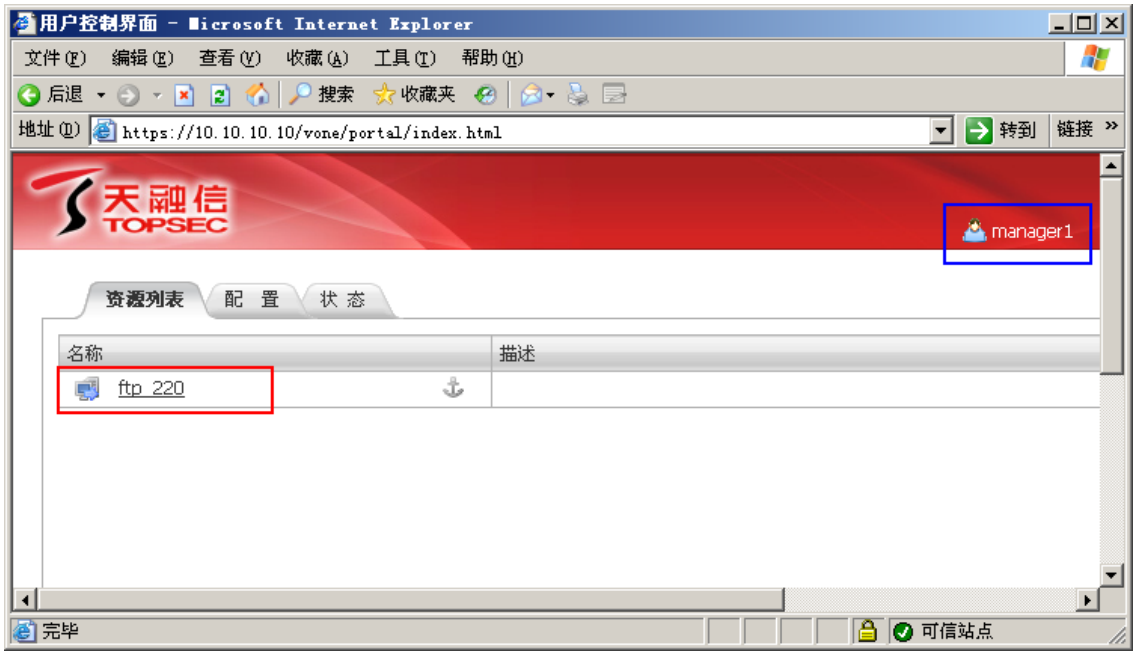
b）将装有证书的 epass1000 插入主机的 USB 接口。

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。

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。

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。

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。



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。

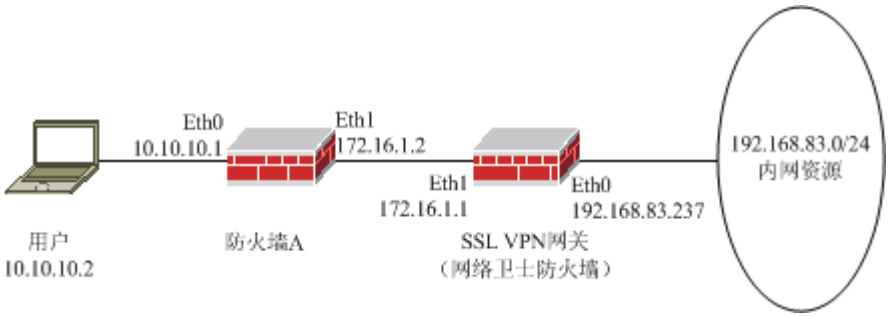


图 31 第三方证书认证的网络部署图

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。

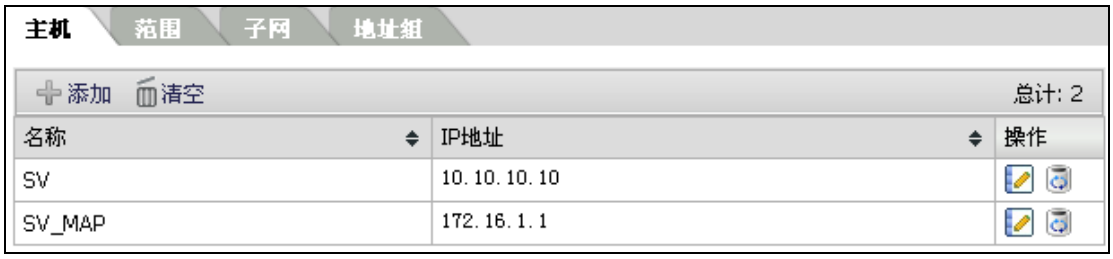
防火墙 A 的配置步骤

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。

2）定义访问控制规则，如下图所示。

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。



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

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。

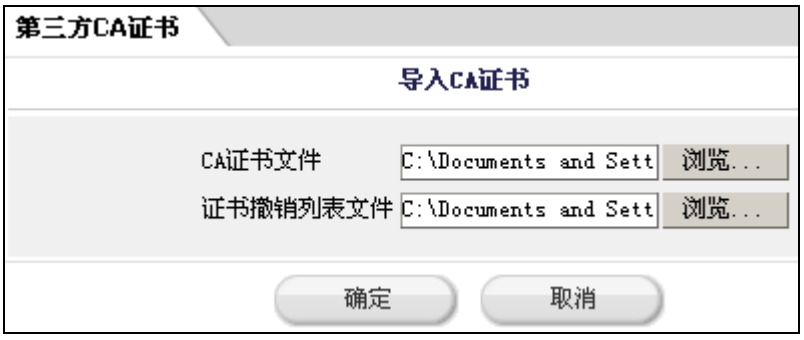
选择 **系统管理 > 配置**，激活“开放服务”页签，然后点击“添加”，开放 Eth1 口所属区域的 SSLVPN 服务，如下图所示。

参数设置完成后，点击“确定”按钮即可。

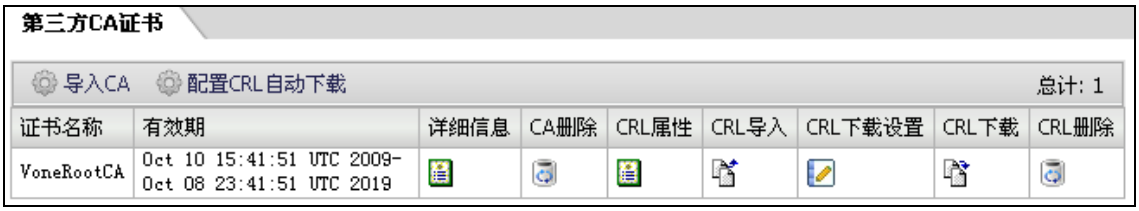
2．导入第三方 CA 根证书和 CRL 列表文件。

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。



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。



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。

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。

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

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。

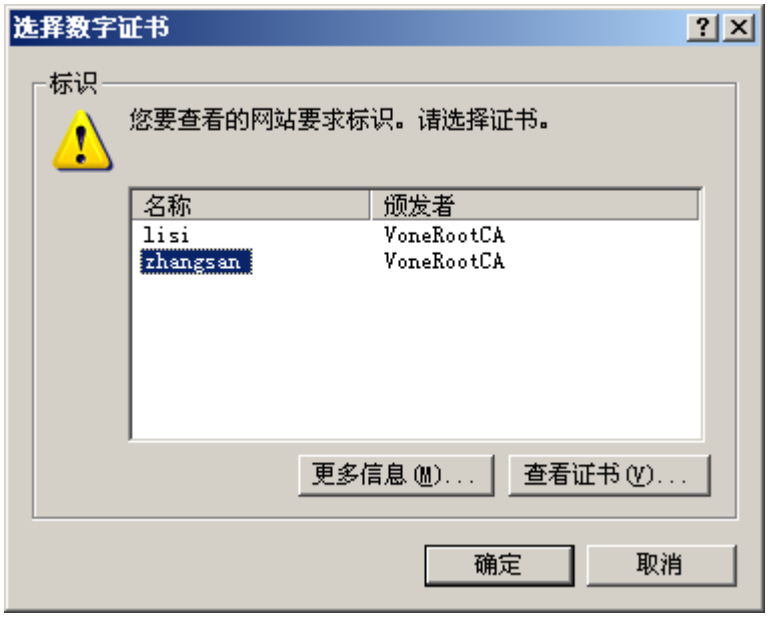
假设外部证书用户“zhangsan”和“lisi”使用同一主机“10.10.10.2”登录，并且该主机已经下载完所有的控件。

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）。

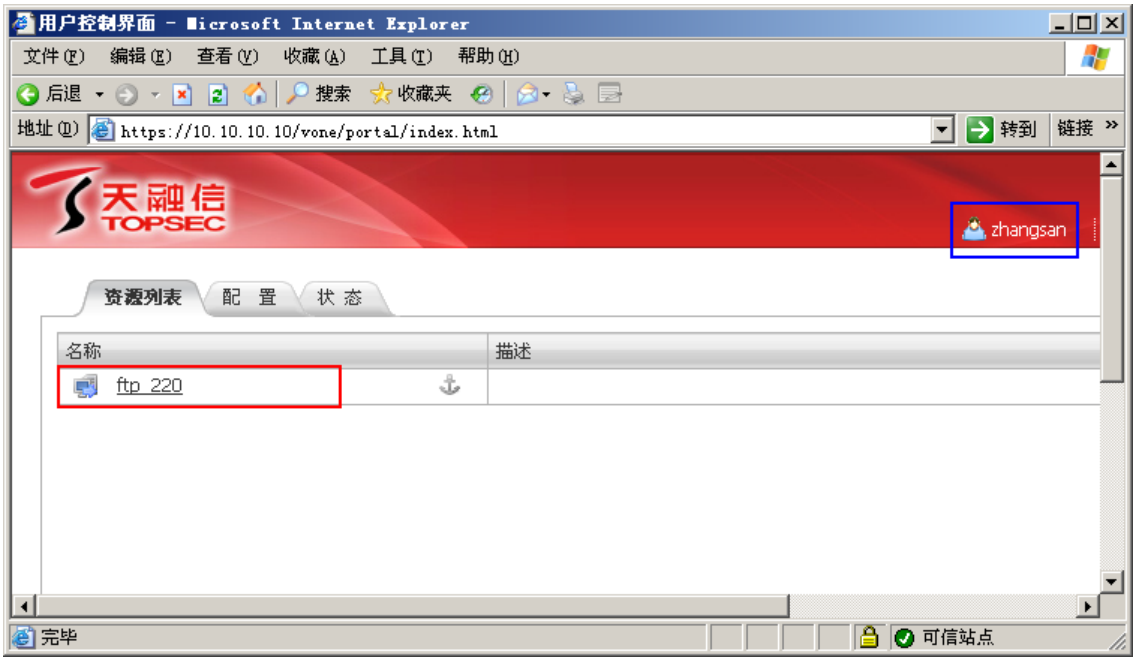
a）双击用户“zhangsan”的文件证书，根据提示将客户端证书安装到本机中。

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。

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。



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。

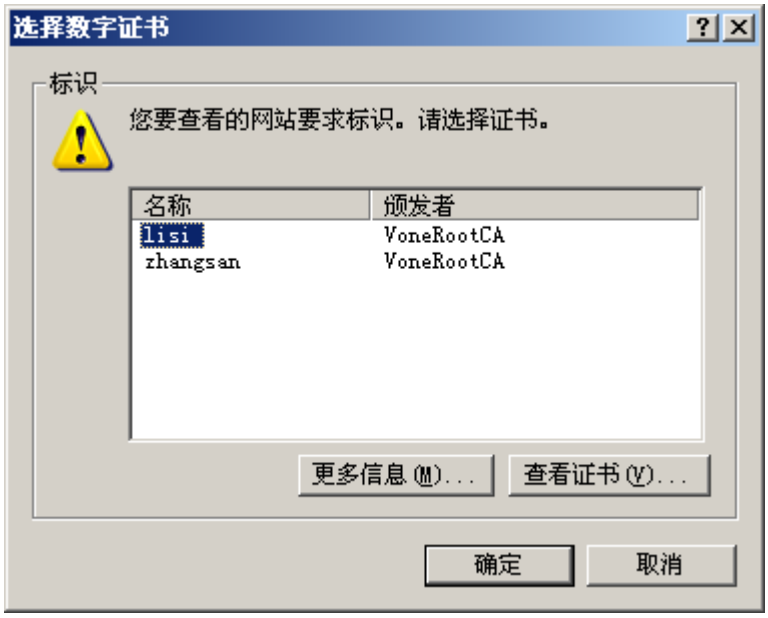


2）用户“lisi”采用文件方式证书登录 SSL VPN 网关（对外 IP 为 10.10.10.10）。

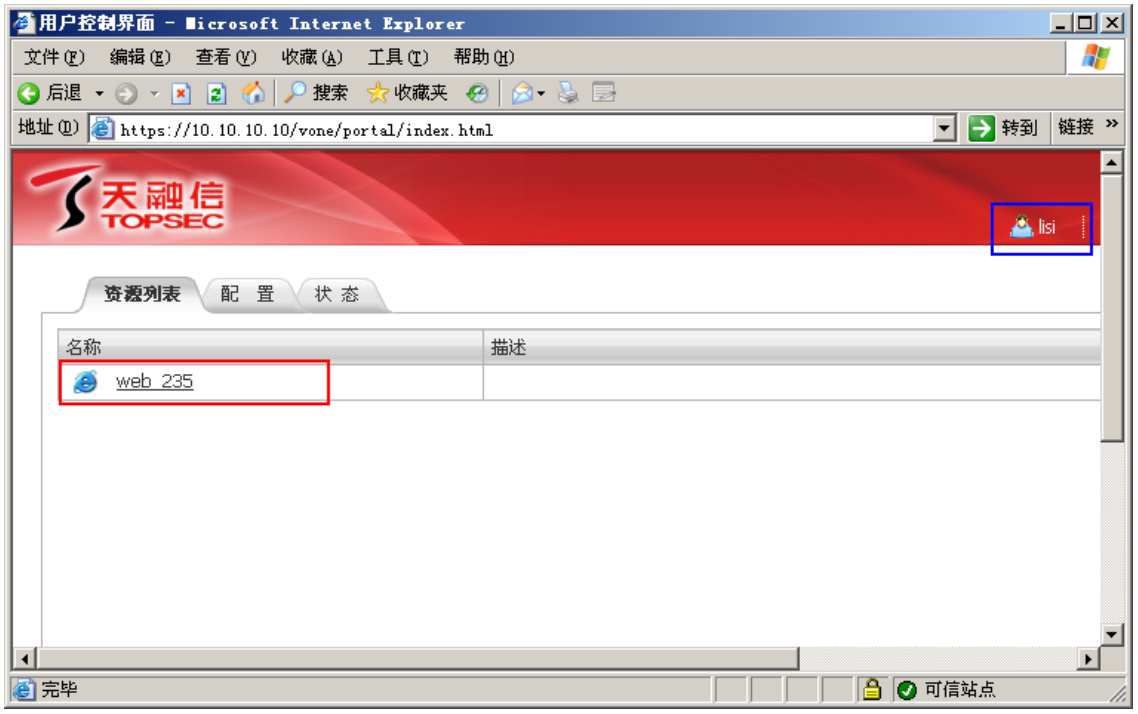
a）双击用户“lisi”的文件证书，根据提示将客户端证书安装到本机中。

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。

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。



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。



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。

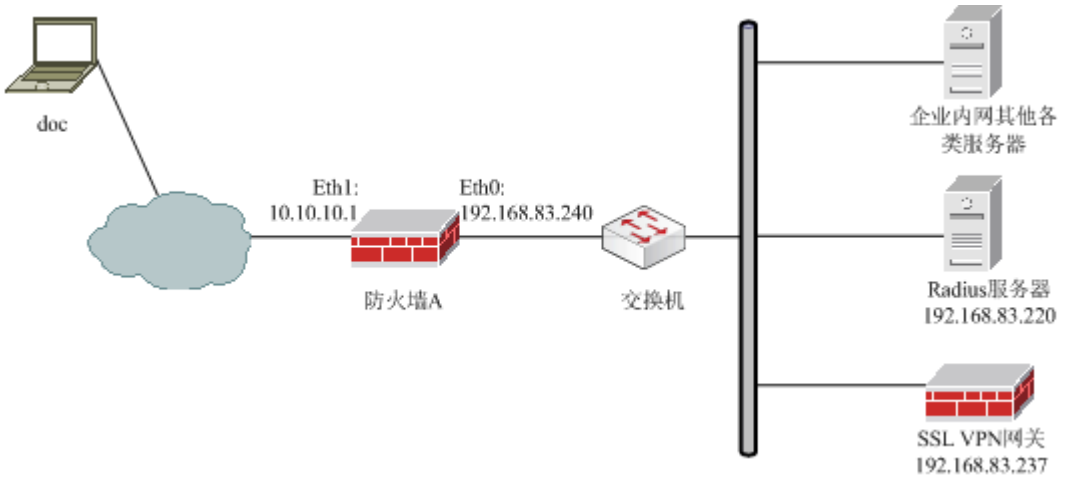


图 32 SSL VPN 网关 Radius 认证示意图

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。

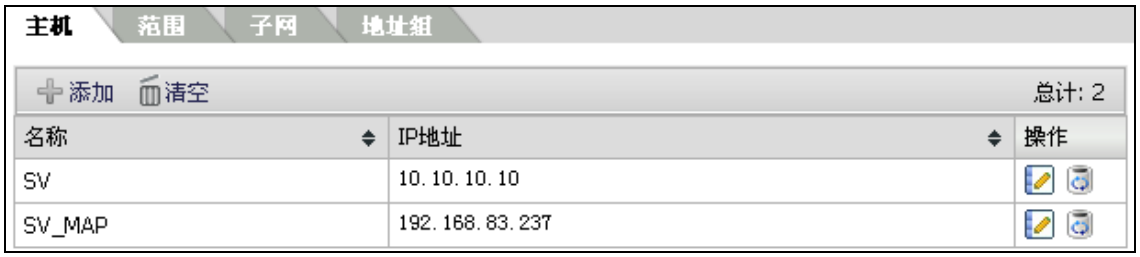
防火墙的配置步骤

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。

2）定义访问控制规则，如下图所示。

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。



4）配置双向地址转换（到 SSL VPN 网关的映射），如下图所示。

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。

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。

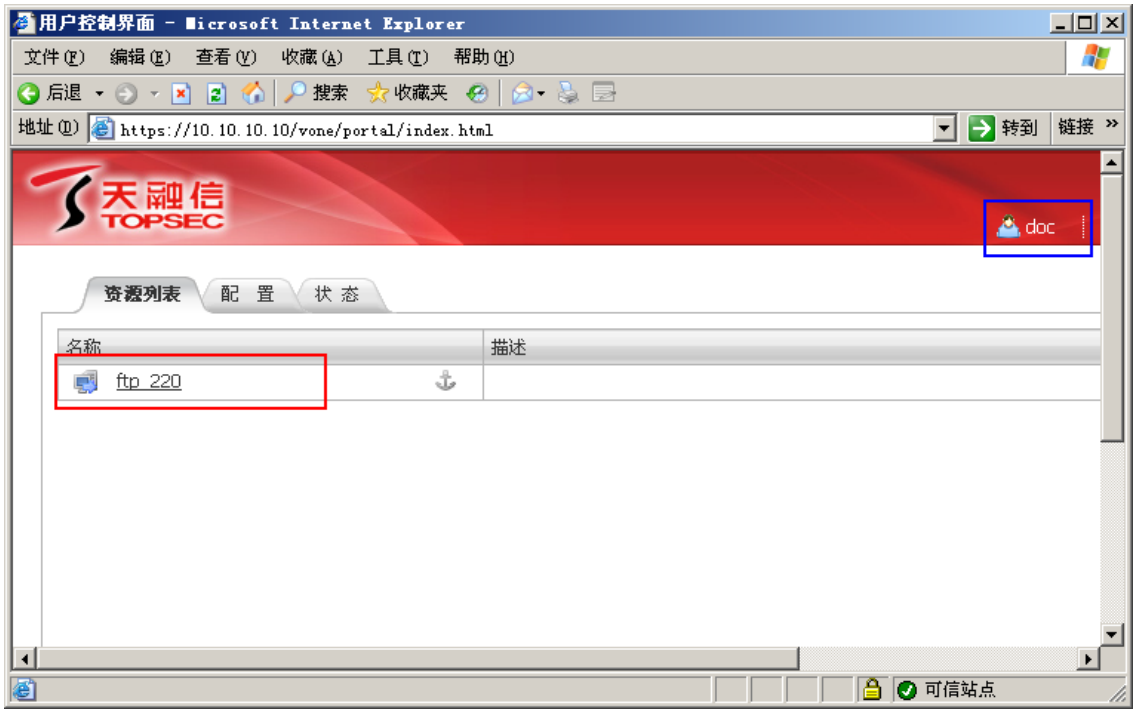
参数设置完成后，点击“确定”按钮。

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。

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。



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。

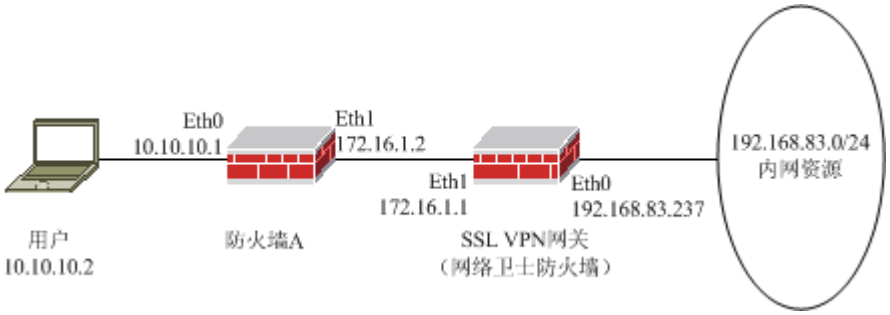


图 33 本地证书认证的网络部署图

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。
- 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。

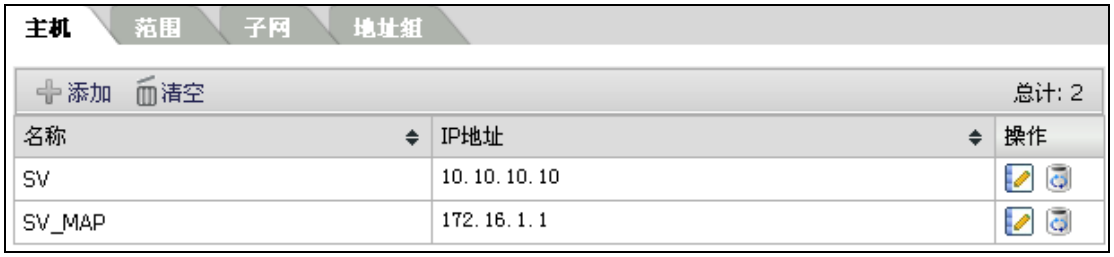
防火墙 A 的配置步骤

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。

2）定义访问控制规则，如下图所示。

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。



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。

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。

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。

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。

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。

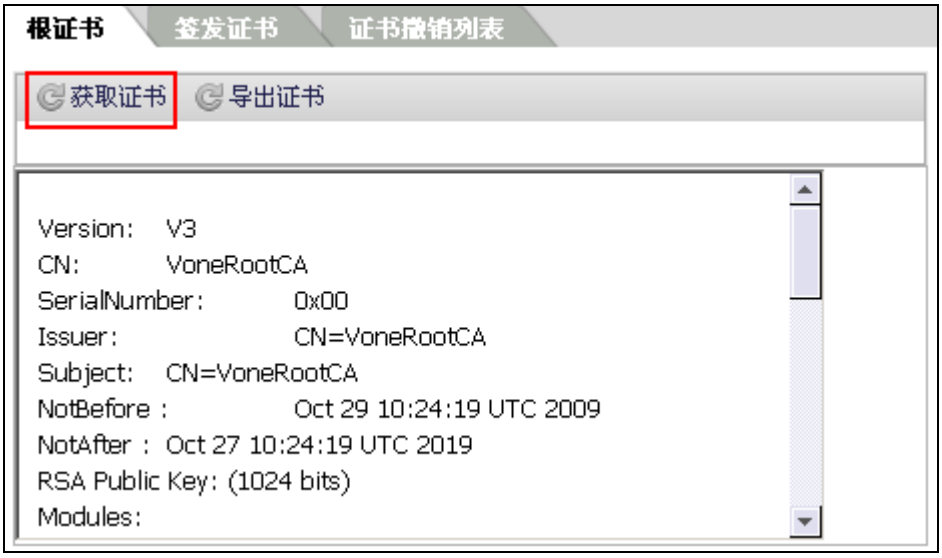
将所有证书用户全部映射到角色“cert_role”。

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。

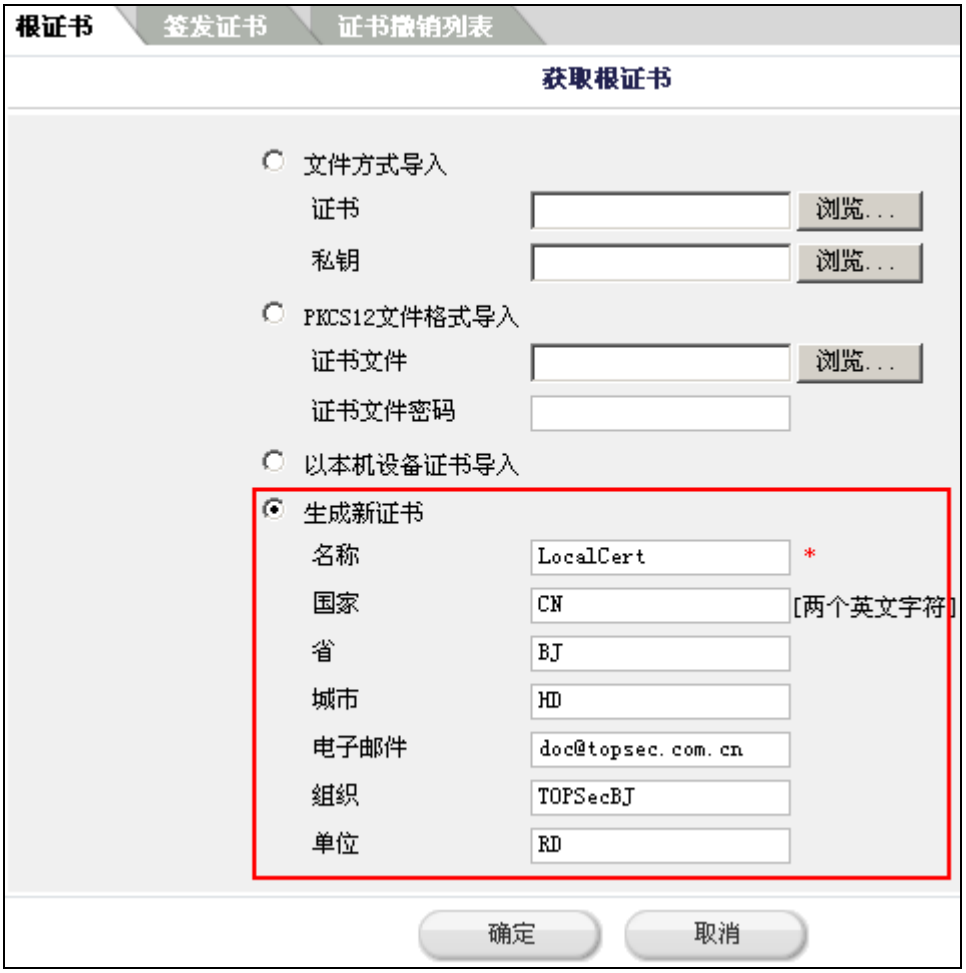
2）参数设置完成后，点击“确定”按钮。

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。



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。



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”。

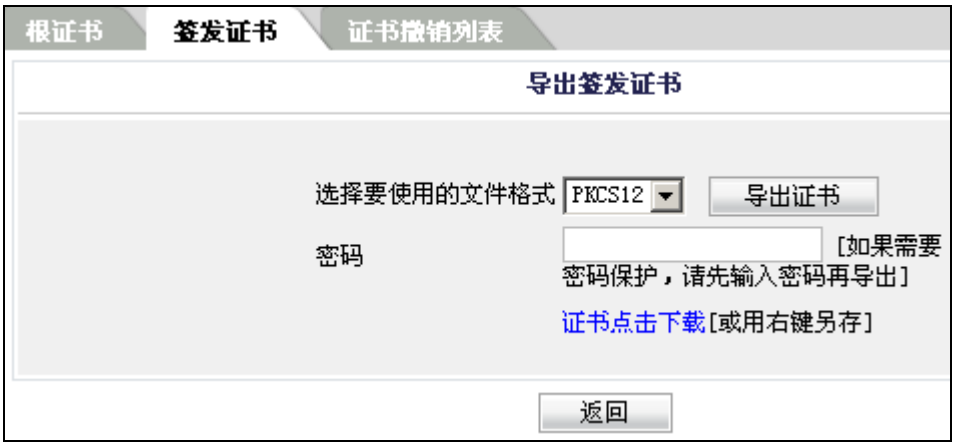
2）配置远程用户“test”的用户证书，如下图所示。

参数设置完成后，点击“确定”按钮使配置生效。

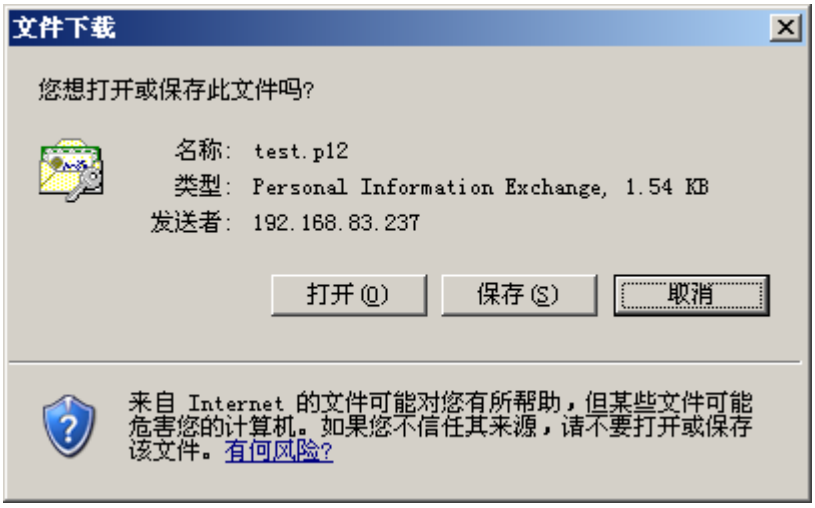
3）将“test”的证书保存到本地。

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。



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。



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。

9．配置 ACL 规则。

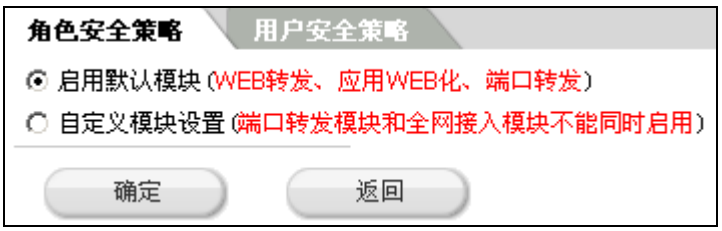
点击导航菜单 **SSLVPN > ACL 管理**，默认禁止远程用户访问内网资源，然后配置三条 ACL 规则，分别允许访问内网资源“ftp_220”、“ftp_235”和“ftp_234”，如下图所示。

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”。

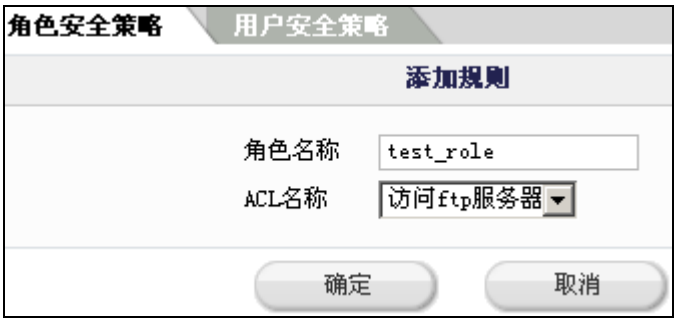
a）点击导航菜单 **SSLVPN > 安全策略**，然后选择“角色安全策略”页签，点击角色“test_role”条目右侧的“安全策略设置”图标。

b）勾选“启用默认模块”，如下图所示。

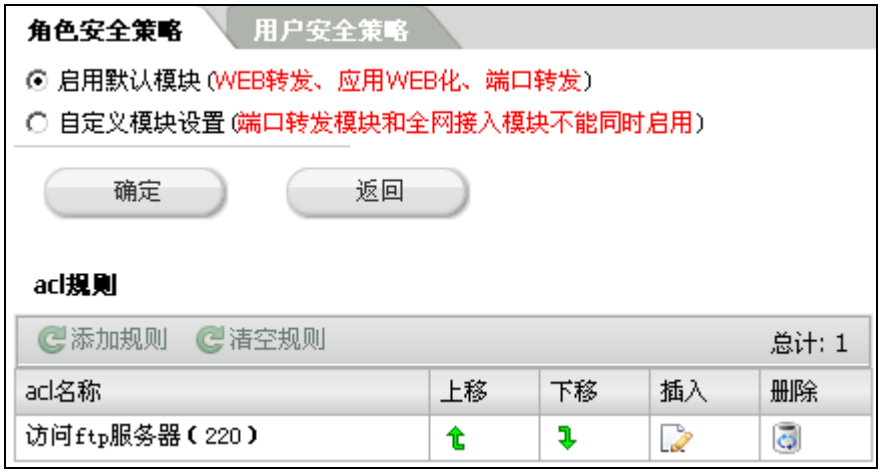


设置完成后，点击“确定”按钮使配置生效。

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。



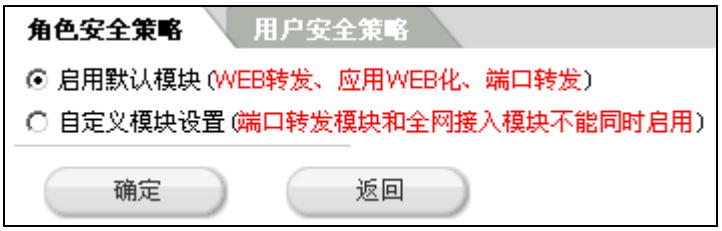
参数设置完成后，点击“确定”按钮，如下图所示。



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。

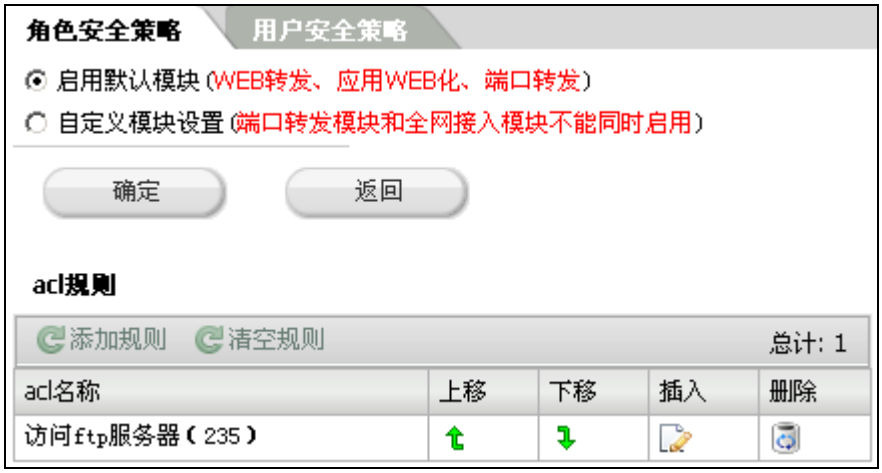
b）勾选“启用默认模块”，如下图所示。



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。

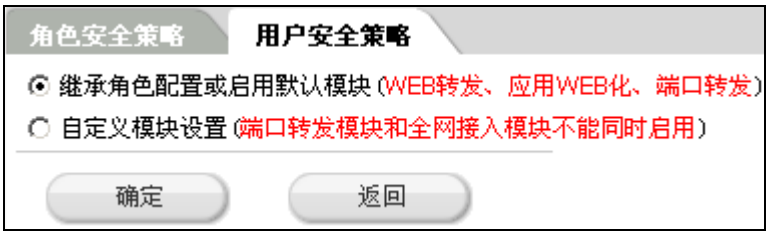
参数设置完成后，点击“确定”按钮，如下图所示。



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。

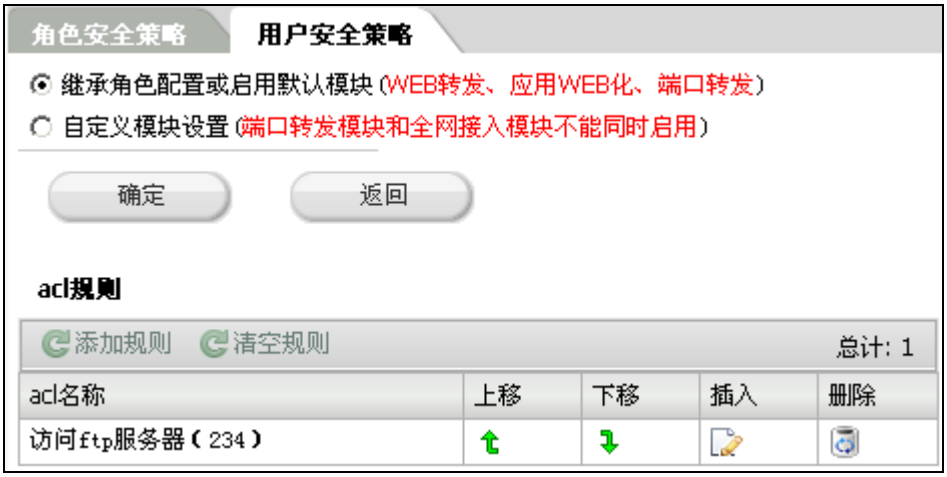
b）勾选“继承角色配置或启用默认模块”，如下图所示。



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。

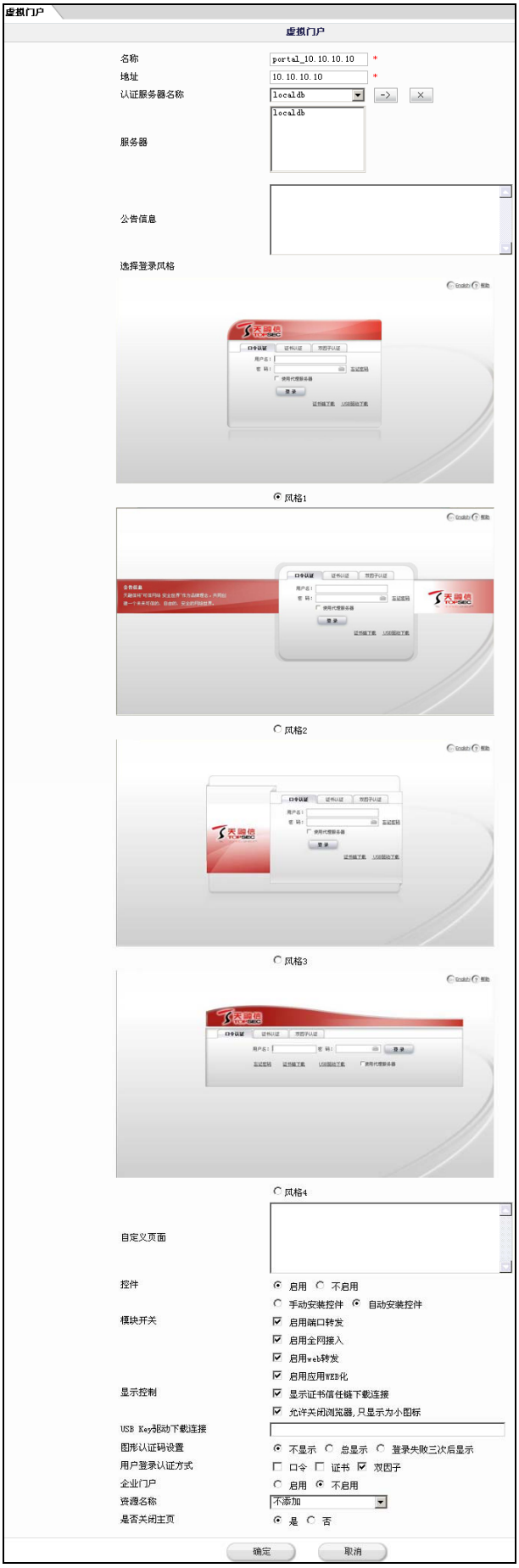
参数设置完成后，点击“确定”按钮，如下图所示。



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
名称
portal_10.10.10.10
地址
10.10.10.10
认证服务器名称
localdb
服务器
localdb
公告信息
选择登录风格
风格1
风格2
风格3
风格4
自定义页面
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驱动下载连接
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
不启用
资源名称
不添加
是否关闭主页
是
否
确定
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。

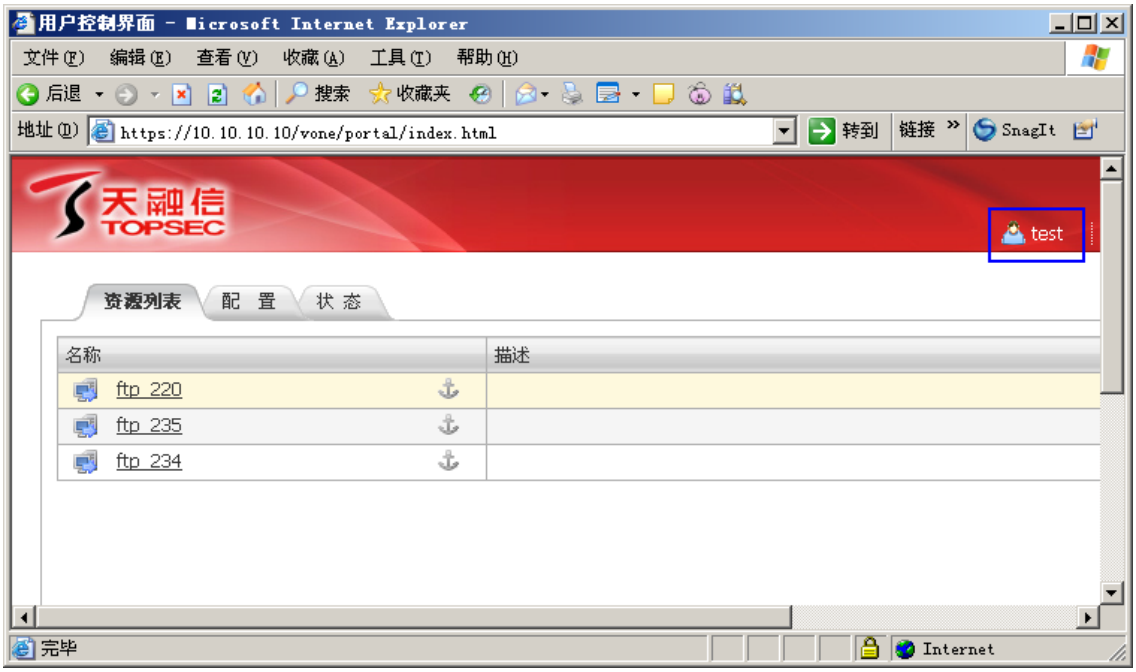
假设用户“test”等登录主机已经下载完所有的控件，用户“test”采用文件方式证书登录 SSL VPN 网关（对外 IP 为 10.10.10.10）。

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。

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。

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。



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。

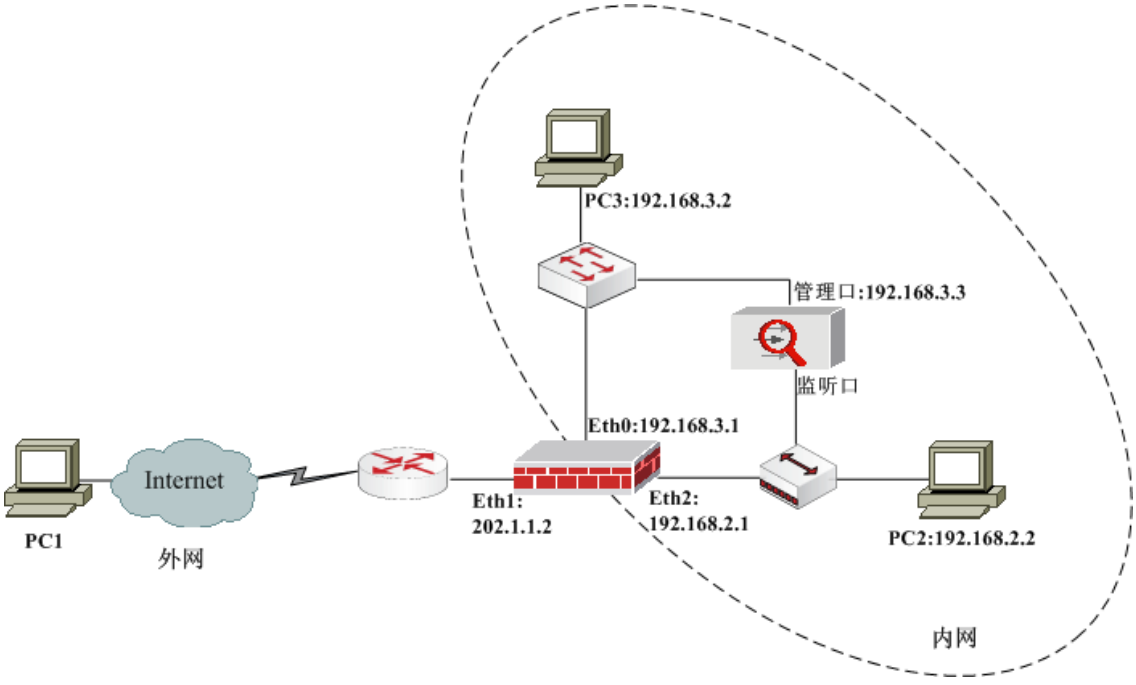


图 34 防火墙与 IDS 联动网络示意图

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。

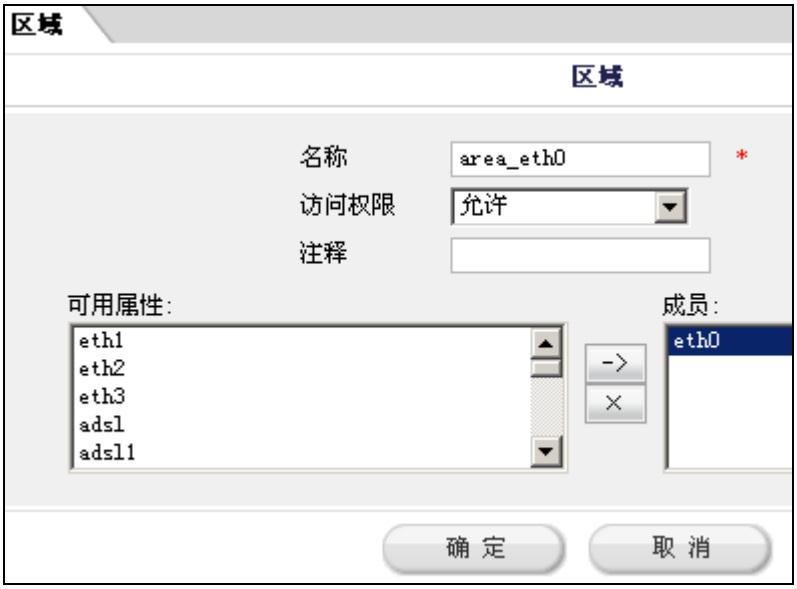
参数设置完成后，点击“确定”按钮即可。

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。



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。

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。

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”。

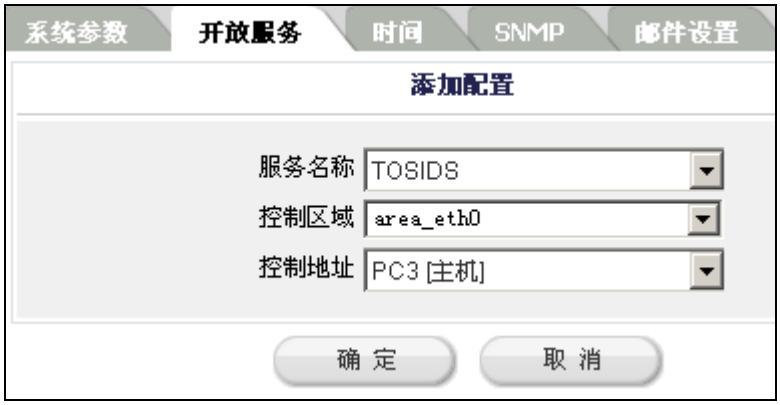
a）配置 IDS 管理主机对象。

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。

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”。

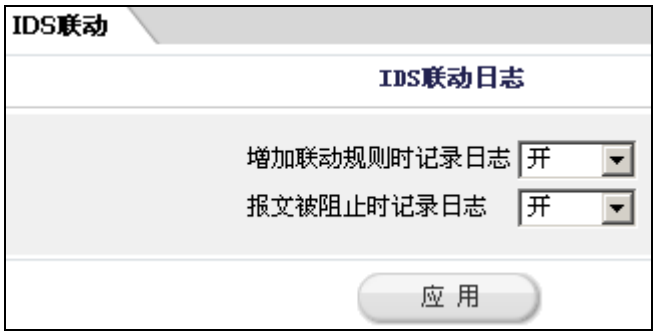
选择 **系统管理 > 配置**，然后激活“开放服务”页签，点击“添加”进行配置，如下图所示。



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。

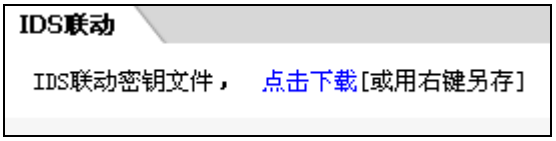
a）选择 **入侵防御 > IDS 联动**，点击“设置”链接，然后打开 IDS 日志开关，如下图所示。



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。

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。



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

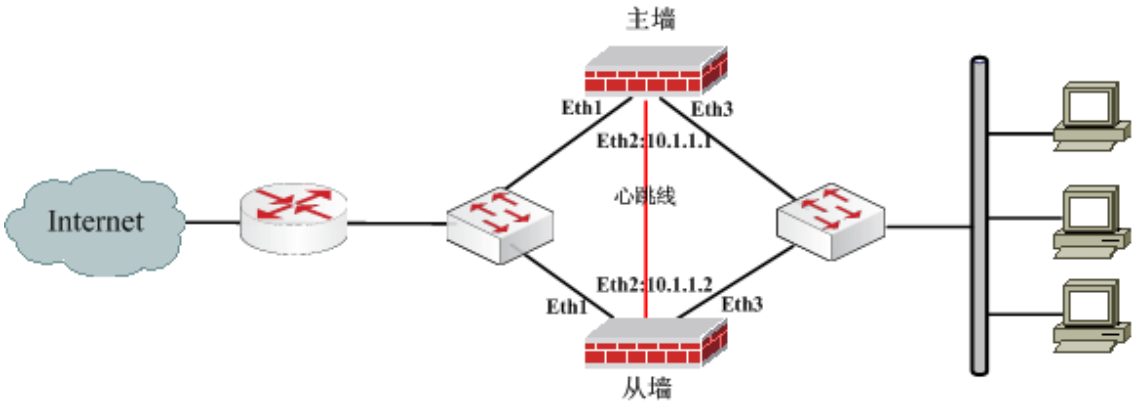


图 35 双机热备模式的网络拓扑图

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。

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。

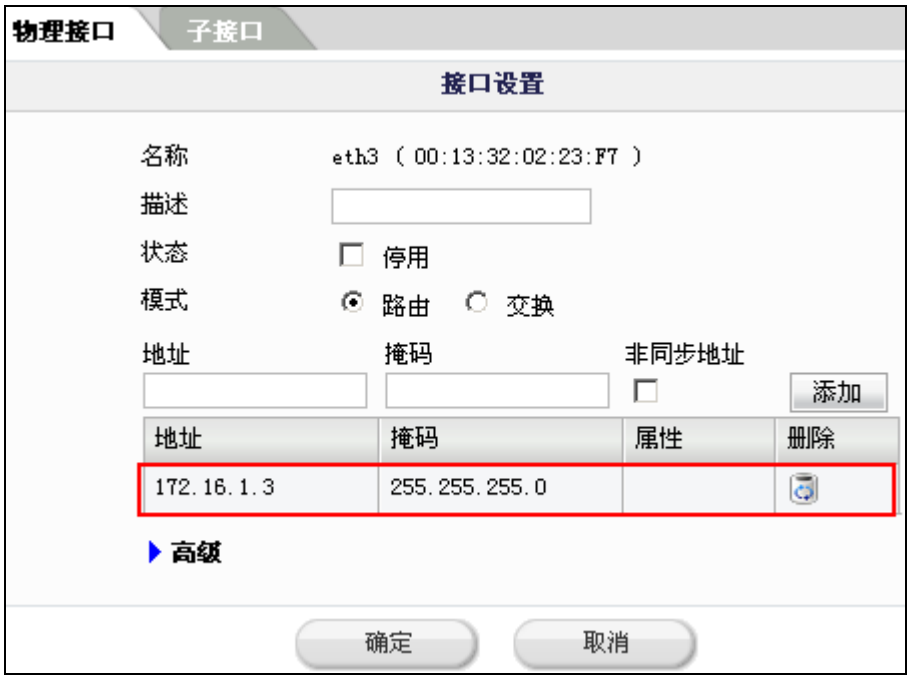
因为需求中要求两台防火墙的 eth1 口互相备份，两条防火墙的 eth3 口互相备份，所以两台防火墙的 eth1 口需要设定相同的 IP 地址和 VRID；两台防火墙的 eth3 口也需要设定相同的 IP 地址和 VRID。

➢ 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。

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。



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

- ✧ 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。

3）配置 HA 功能。

- ➢ 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。

➢ 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。

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
心跳地址
本地
10.1.1.1
对端
10.1.1.2
热备组
热备组
身份
抢占
工作状态
1
主
开启
工作
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
对端机同步到本机
本机同步到对端机

- 从墙

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

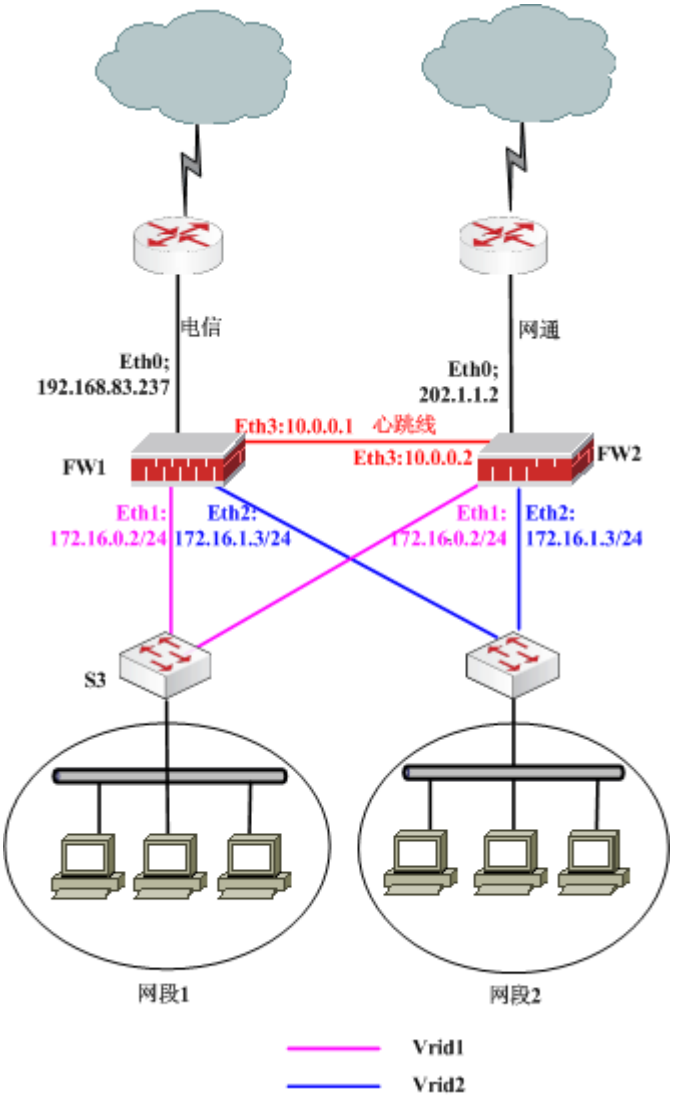


图 36 路由接口下负载均衡模式的网络拓扑图

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 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 条目后的“设置”图标，设定其 IP 地址为“192.168.83.237/24”，如下图所示。

b）参数设置完成后，点击“确定”按钮保存配置。

- 防火墙 2

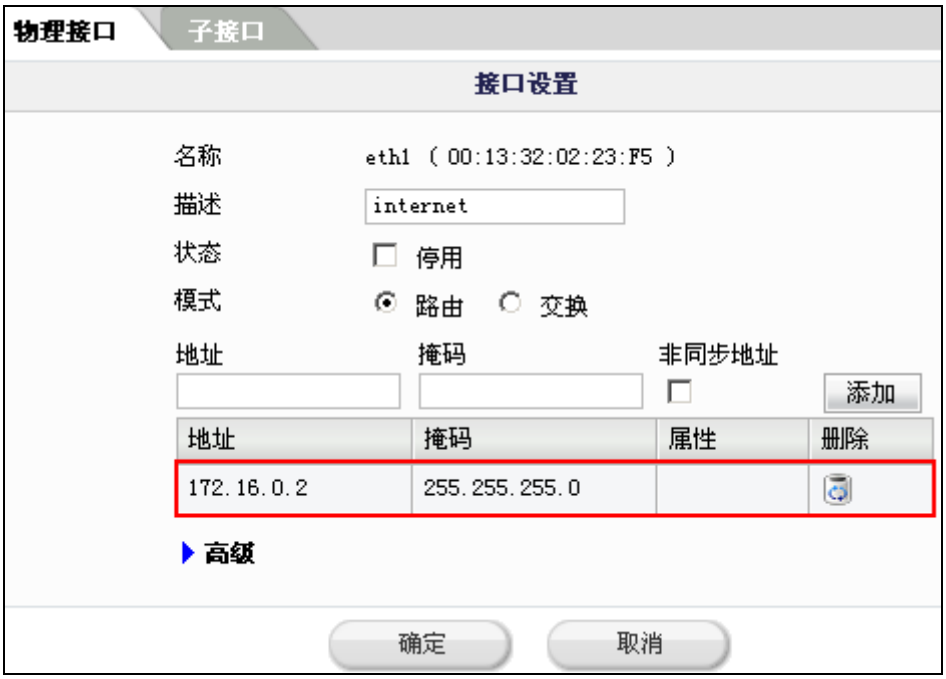
配置防火墙 2 的 IP 地址为“202.1.1.2/24”，具体步骤请参见防火墙 1 的配置。

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。

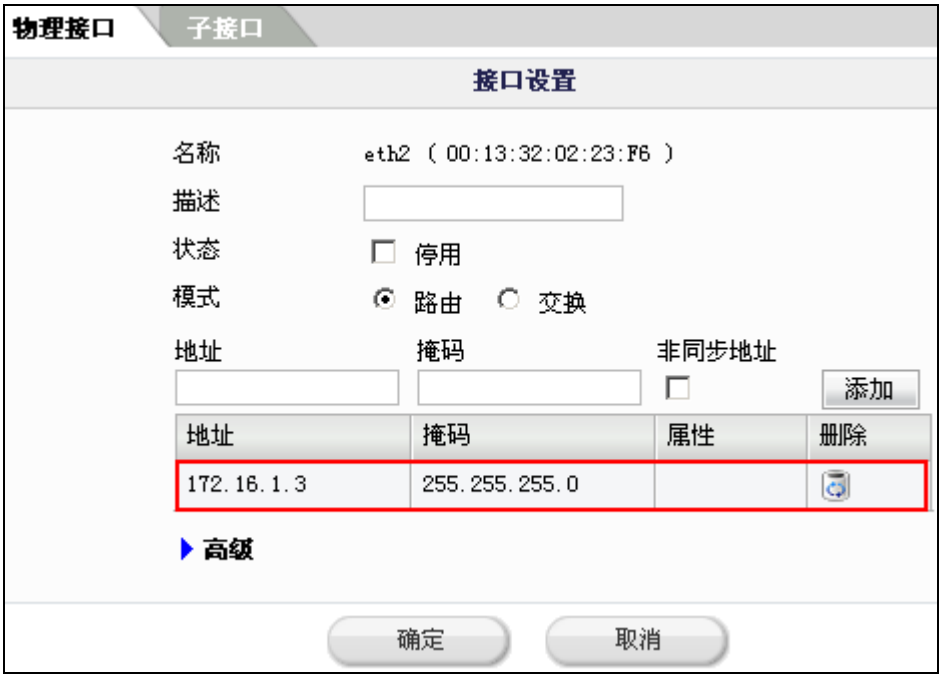
➢ 防火墙 1

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。



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。



参数设置完成后，点击“确定”按钮即可。

➢ 防火墙 2

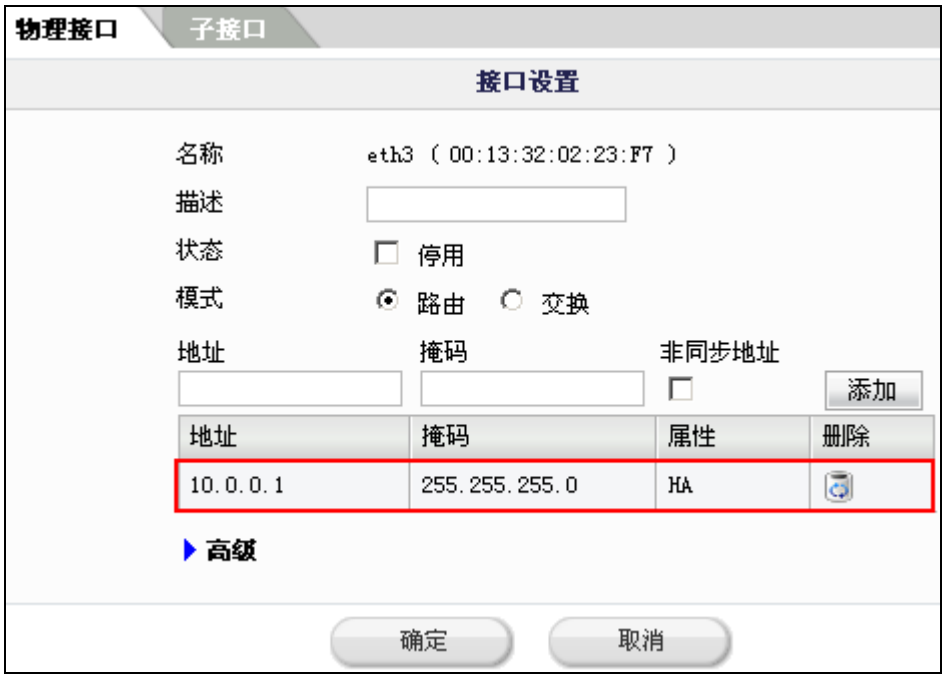
防火墙 2 的配置与防火墙 1 完全一致，具体操作请参见防火墙 1。

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。



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。

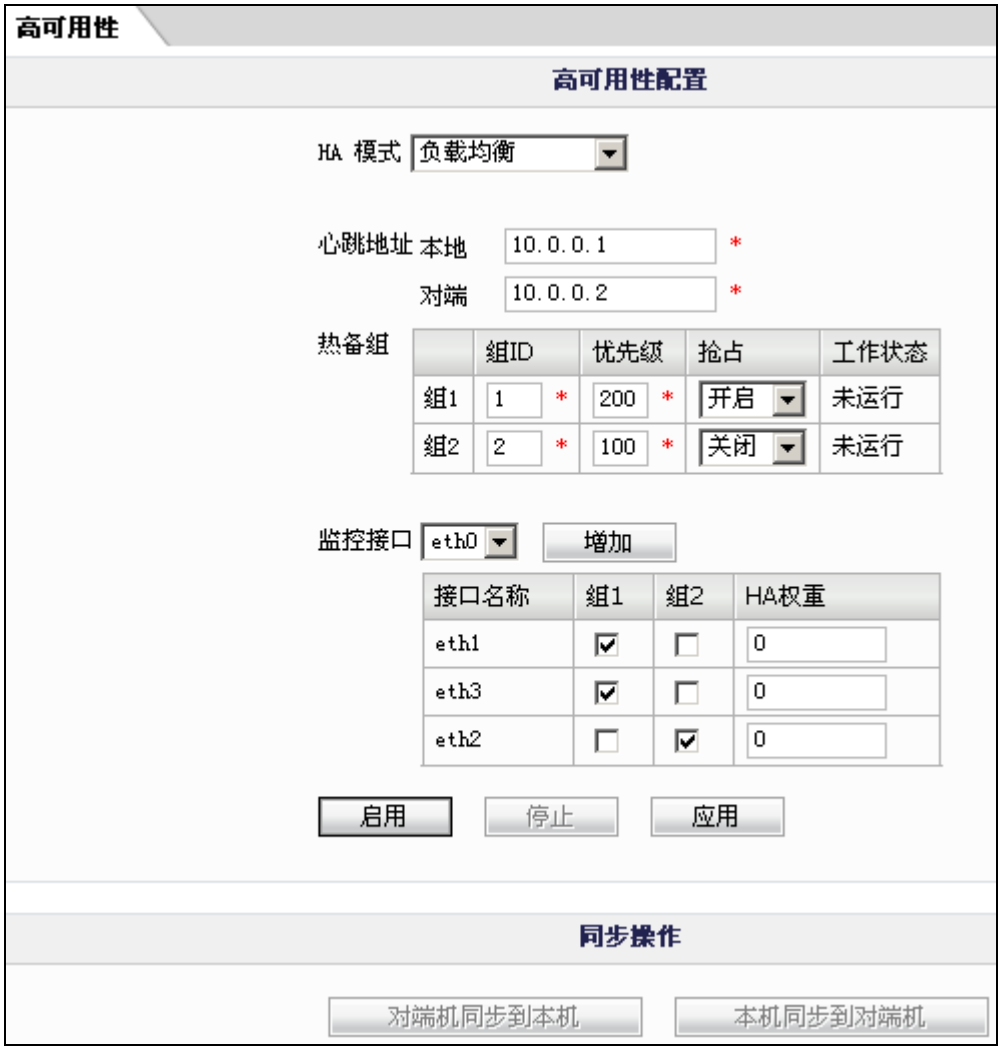
开启主墙的“抢占”模式，即主墙能在失效后，重新恢复正常工作时，重获主墙地位。“抢占”模式，是指主墙宕机后，重新恢复正常工作时，是否重新夺回主墙的地位。只有当主墙与从墙相比有明显的性能差异时，才需要配置主墙工作在“抢占”模式，否则当主墙恢复工作时主从墙的再次切换浪费系统资源，没有必要。

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。

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。

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
eth0
增加
接口名称
组1
组2
HA权重
eth1
0
eth2
0
启用
停止
应用
同步操作
对端机同步到本机
本机同步到对端机

- 防火墙 2


高可用性
高可用性配置
HA 模式
负载均衡
心跳地址
本地
10.0.0.2
对端
10.0.0.1
热备组
组ID
优先级
抢占
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
同步操作
对端机同步到本机
本机同步到对端机

Trunk 口下的负载均衡模式

基本需求

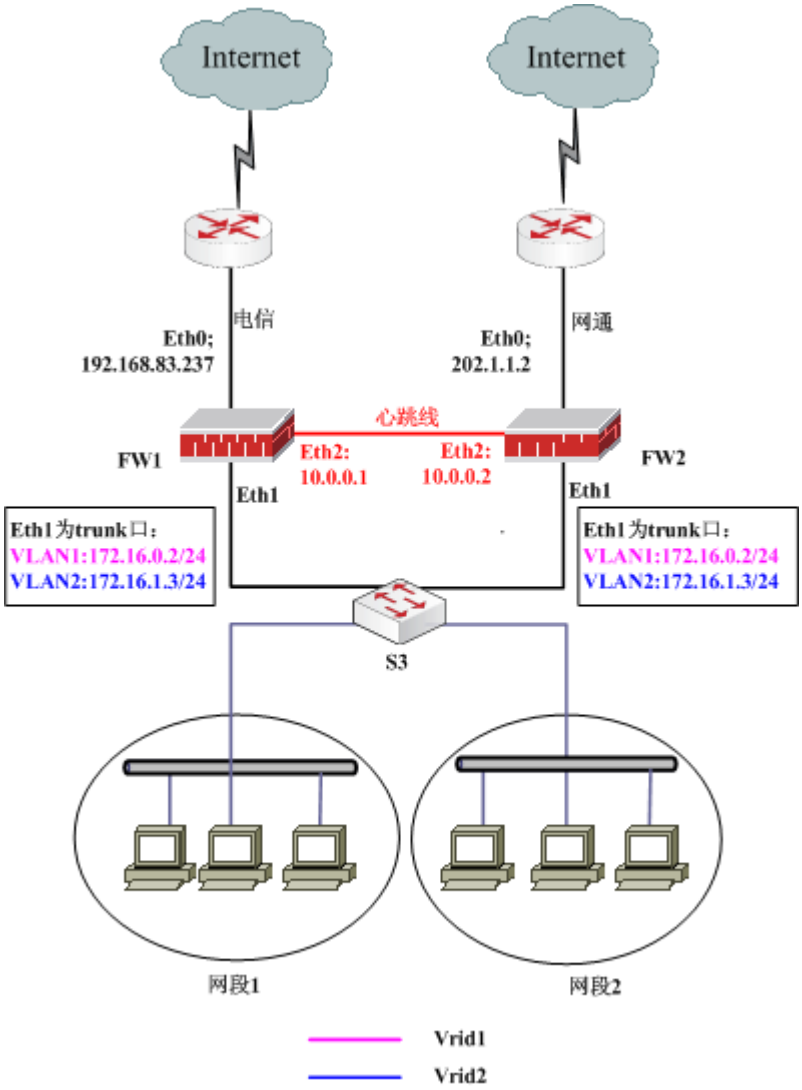


图 37 Trunk 口下负载均衡模式的网络拓扑图

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。

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。

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。

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“ ”，设置 VLAN 虚接口 vlan.0001 的 IP 地址为 172.16.0.2/24，如下图所示。

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“ ”，设置 VLAN 虚接口 vlan.0002 的 IP 地址为 172.16.1.3/24，如下图所示。

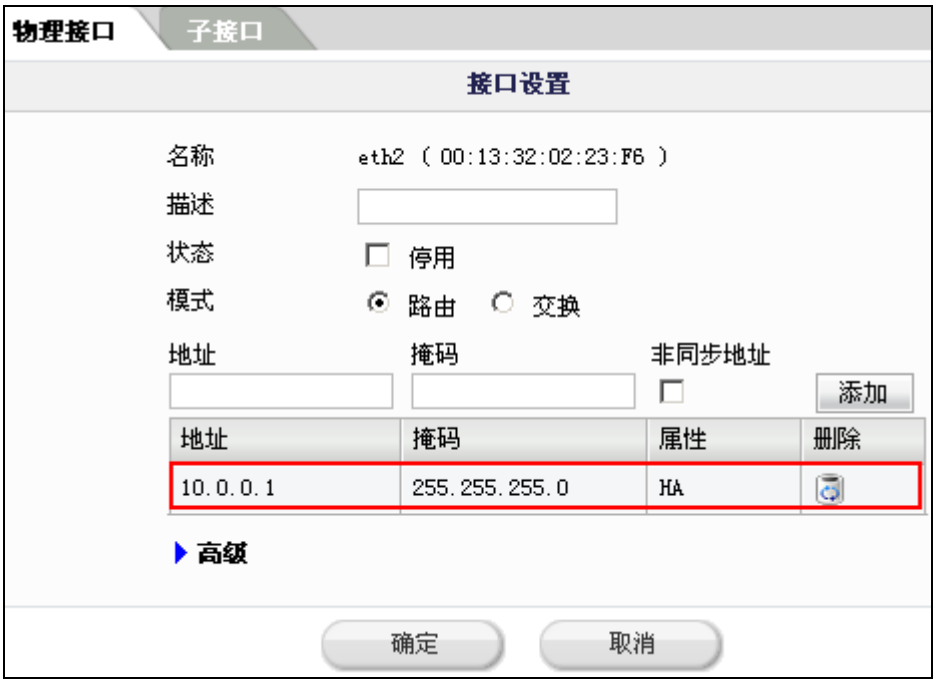
参数设置完成后，点击“确定”按钮即可。

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。



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。

➢ 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。

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
eth0
增加
接口名称
组1
组2
HA权重
vlan.0001
0
vlan.0002
0
启用
停止
应用
同步操作
对端机同步到本机
本机同步到对端机

- 防火墙 2


高可用性
高可用性配置
HA 模式
负载均衡
心跳地址
本地
10.0.0.2
对端
10.0.0.1
热备组
组ID
优先级
抢占
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
vlan.0001
0
vlan.0002
0
启用
停止
应用
同步操作
对端机同步到本机
本机同步到对端机

连接保护模式

基本需求

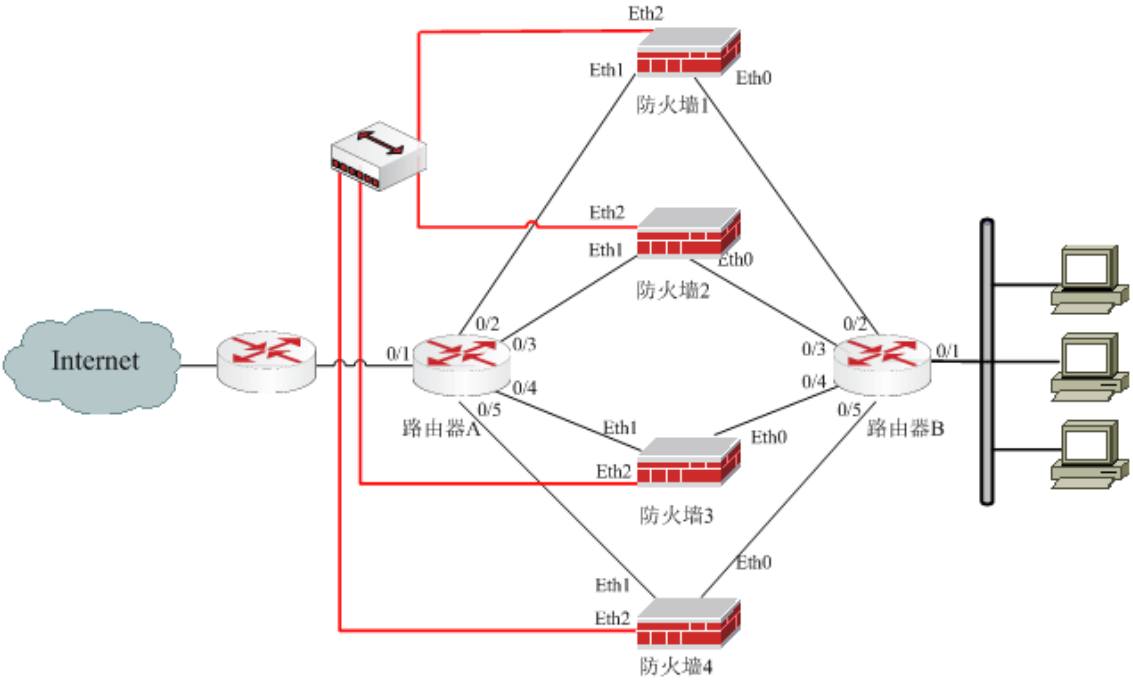


图 38 连接保护模式拓扑图

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

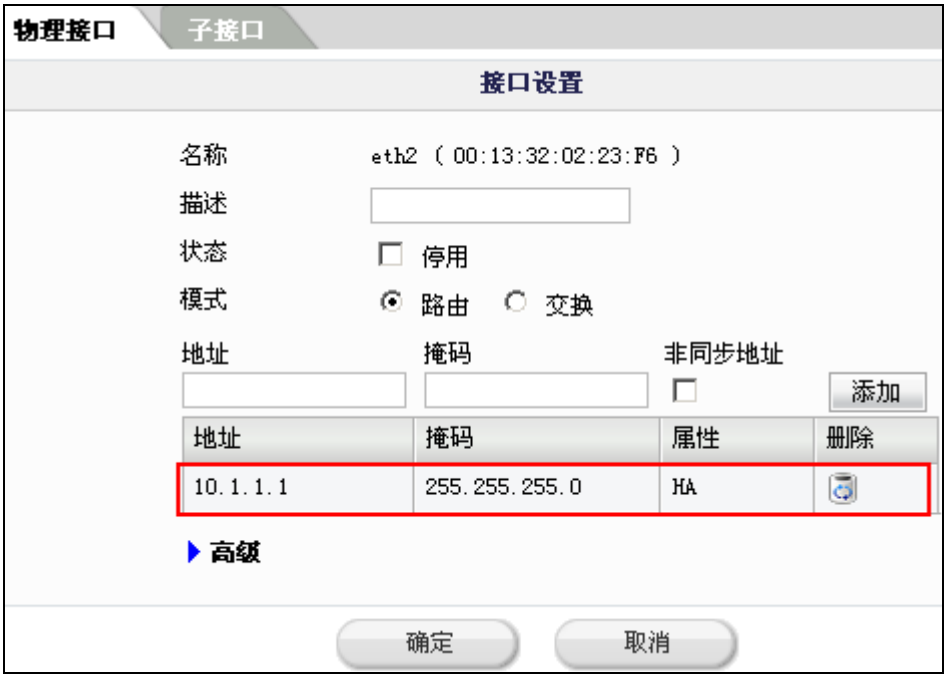
WEBUI 配置步骤

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。



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。

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。

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。

➢ 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。

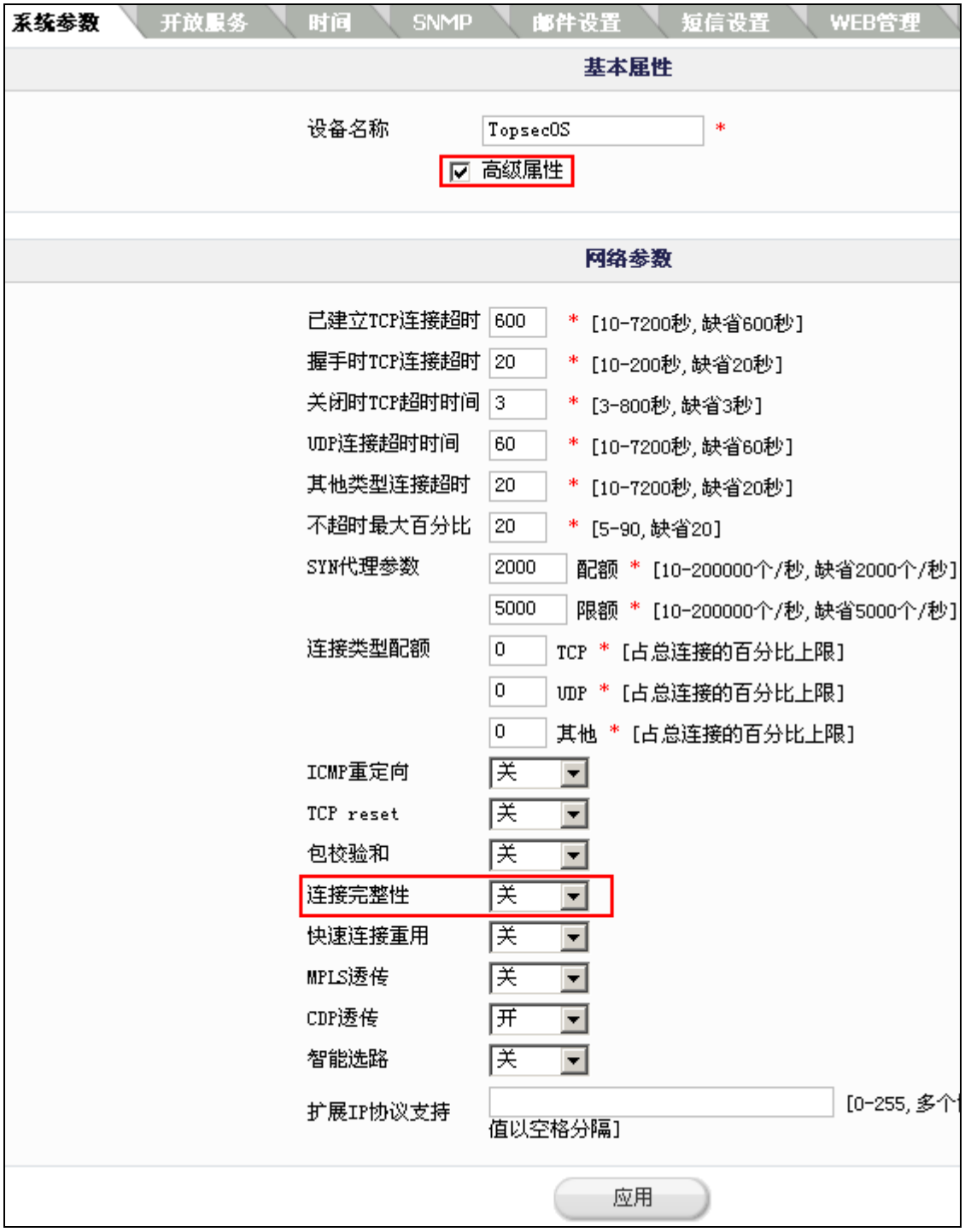
- 防火墙 1、防火墙 2、防火墙 3 和防火墙 4

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。

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。



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

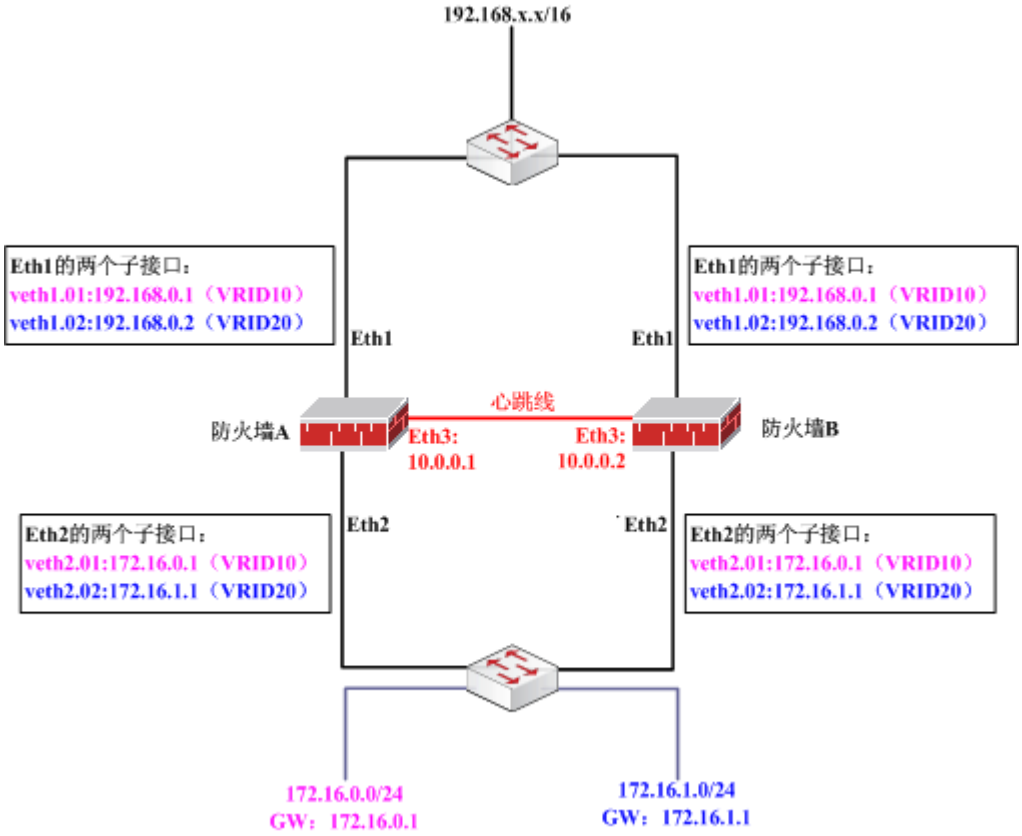


图 39 子接口负载均衡模式的网络示意图

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。

名称	描述	地址	MTU	状态	操作
veth1.01		192.168.0.1/255.255.255.0	1500	启用	
veth1.02		192.168.0.2/255.255.255.0	1500	启用	
veth2.01		172.16.0.1/255.255.255.0	1500	启用	
veth2.02		172.16.1.1/255.255.255.0	1500	启用	

- 防火墙 B

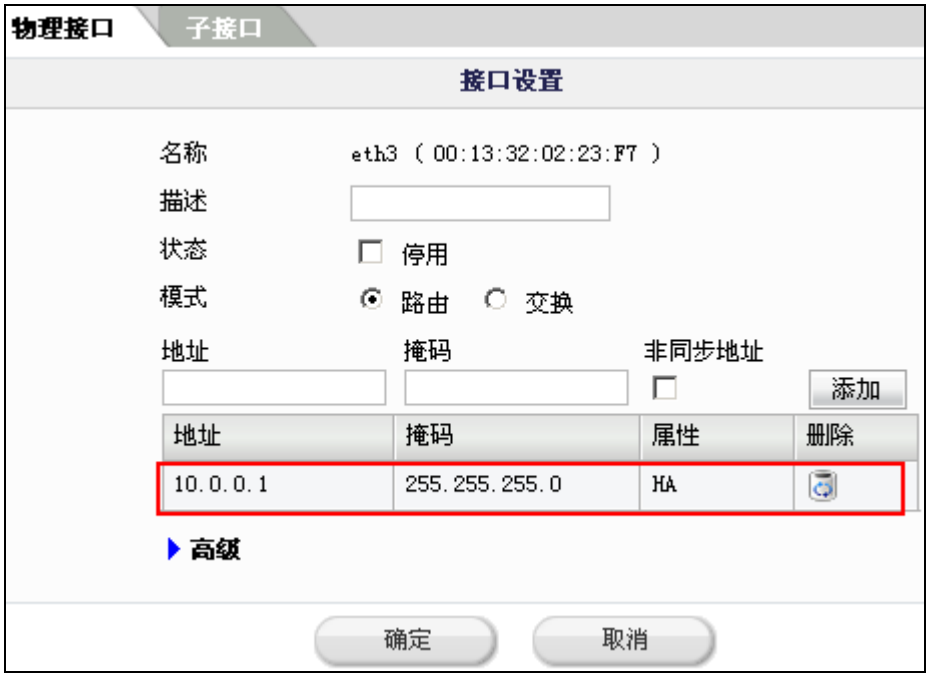
配置防火墙 B 的备份子接口，与防火墙 A 的配置完全相同，此处不再赘述。

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。



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。

➢ 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。

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
抢占
工作状态
组1
10
100
关闭
备份
组2
20
200
开启
工作
监控接口
eth0
增加
接口名称
组1
组2
HA权重
veth1.01
veth2.01
veth1.02
veth2.02
启用
停止
应用
同步操作
对端机同步到本机
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
负载均衡
心跳地址
本地
10.0.0.2
对端
10.0.0.1
热备组
组ID
优先级
抢占
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
增加
接口名称
组1
组2
HA权重
veth1.01
veth2.01
veth1.02
veth2.02
0
启用
停止
应用
同步操作
对端机同步到本机
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。

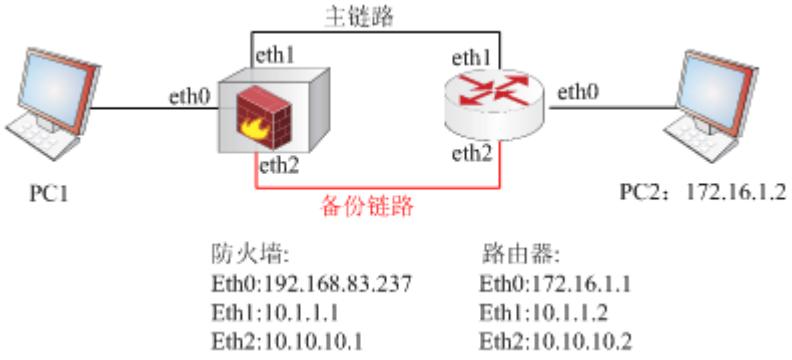


图 40 防火墙链路备份网络示意图

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。

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。

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。

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。

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。

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。

参数设置完成后，点击“确定”按钮即可。

2）配置地址转换策略。

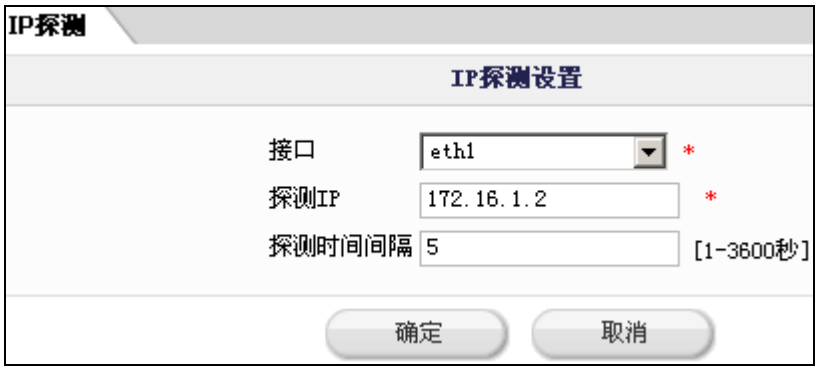
点击 **防火墙 > 地址转换**，点击“添加”，配置两条地址转换策略，如下图所示。

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。

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。



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。

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。

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。

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。

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 | 策略路由 | 动态路由OSPF | 动态路由RIP | 动态路由BGP | 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

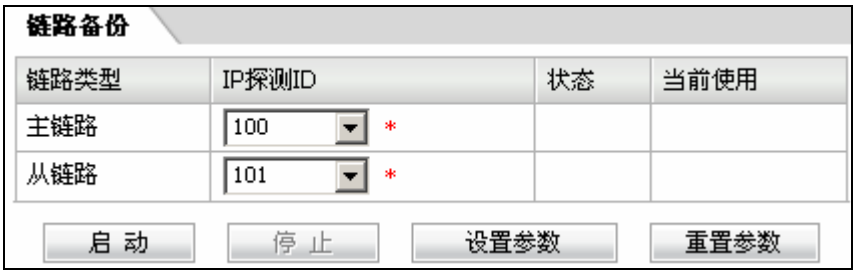
添加 清空 总计：12

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	lo	-	-
192.168.83.237/32	0.0.0.0	ULi	1	1	lo	-	-
10.1.1.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.10.10.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.10.11.0/24	0.0.0.0	UCi	200	1	sslvpn0	-	-
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	-	-
0.0.0.0/0	10.1.1.2	UGSi	1	1	eth1	-	
0.0.0.0/0	10.10.10.2	UGSi	1	1	eth2	-	

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。

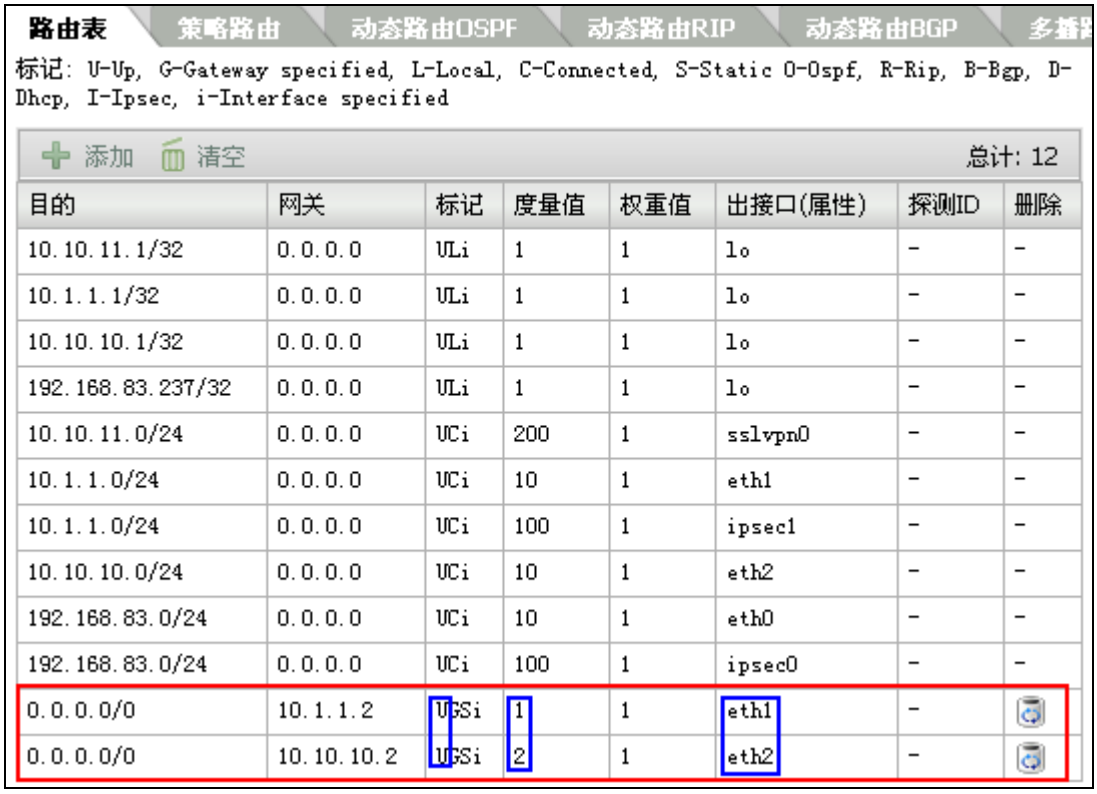


b）点击“设置参数”按钮，将链路备份参数写入系统内存。

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。

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 | 动态路由OSPF | 动态路由RIP | 动态路由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 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	lo	-	-
10.1.1.1/32	0.0.0.0	ULi	1	1	lo	-	-
10.10.10.1/32	0.0.0.0	ULi	1	1	lo	-	-
192.168.83.237/32	0.0.0.0	ULi	1	1	lo	-	-
10.10.11.0/24	0.0.0.0	UCi	200	1	sslvpn0	-	-
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	eth1	-	
0.0.0.0/0	10.10.10.2	UGSi	2	1	eth2	-	

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：

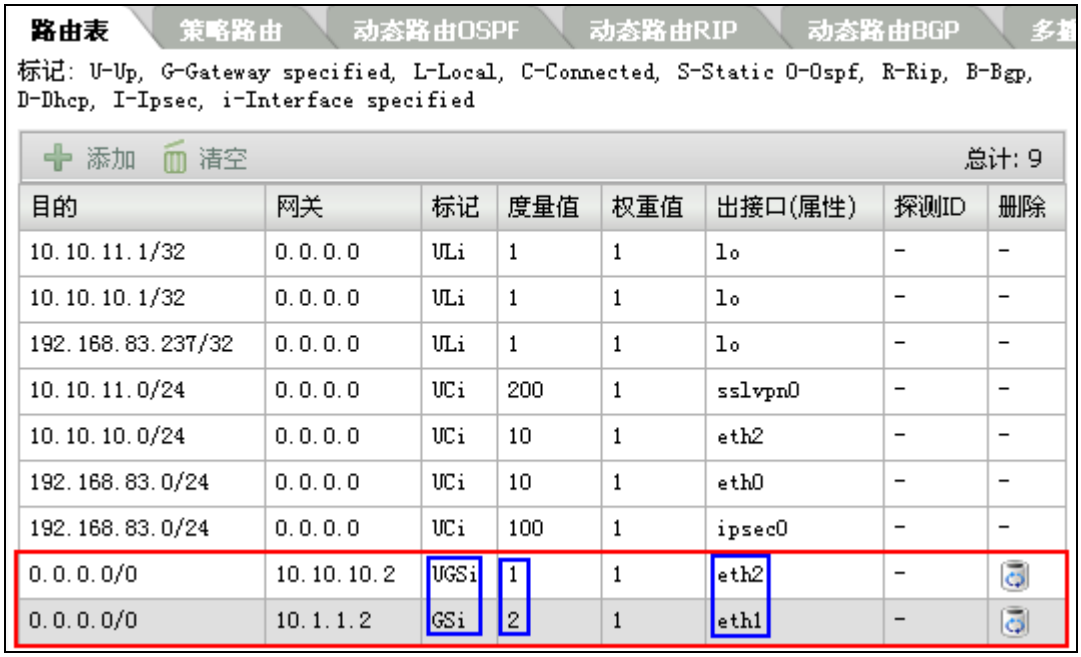
① 界面链路状态显示如下图所示。

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。



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。

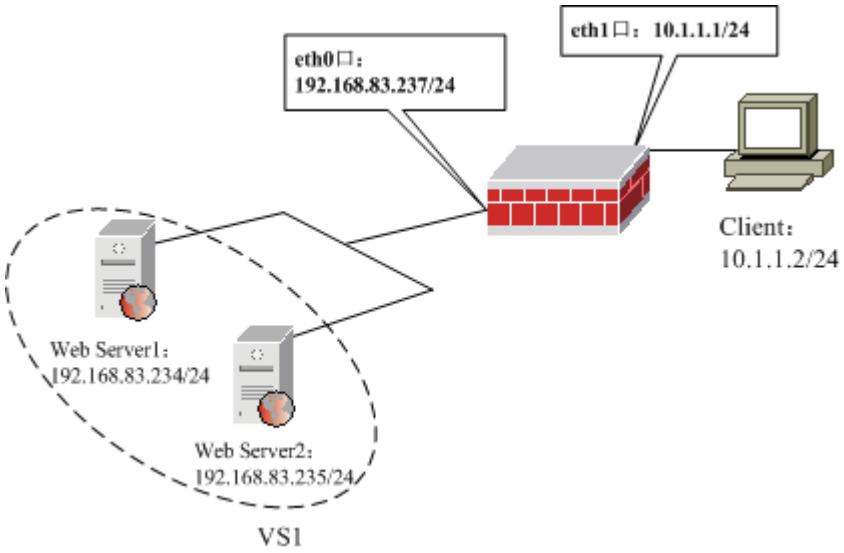


图 41 防火墙负载均衡网络示意图

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。

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。

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。

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。

参数设置完成后，点击“确定”按钮即可。

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。

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。

参数设置完成后，点击“确定”按钮即可。

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。

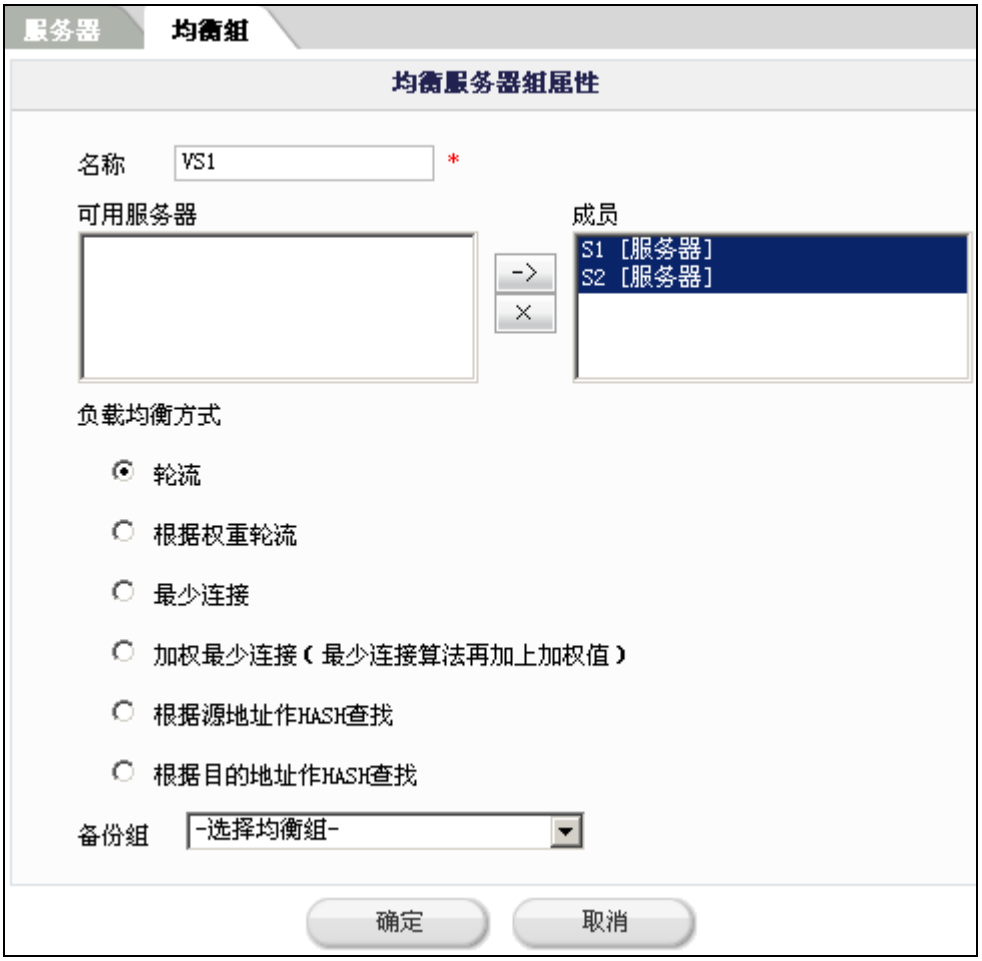
参数设置完成后，点击“确定”按钮即可。

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。

参数设置完成后，点击“确定”按钮即可。

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）参数设置完成后，点击“确定”按钮即可。

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。

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）。

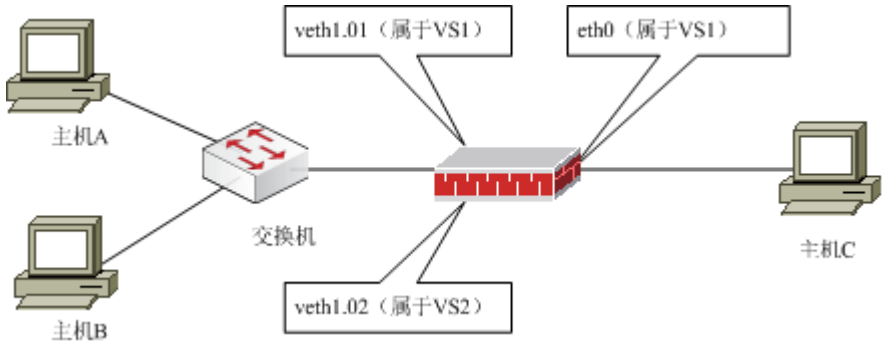


图 42 防火墙虚系统示意图

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。

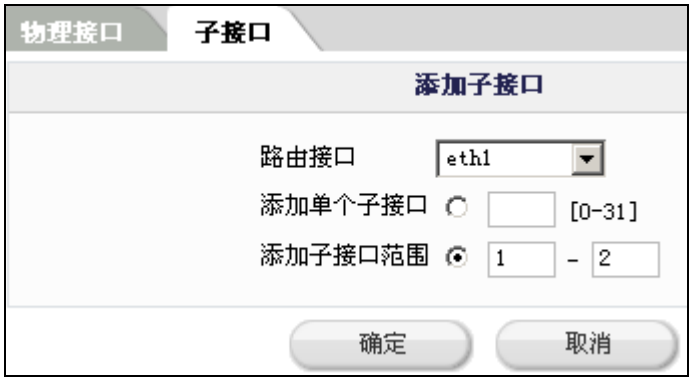
① 点击 **网络管理 > 接口**，然后选择“物理接口”页签，在 eth0 接口后点击“设置”图标，配置 IP 地址为“192.168.83.237”，如下图所示。

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。

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。



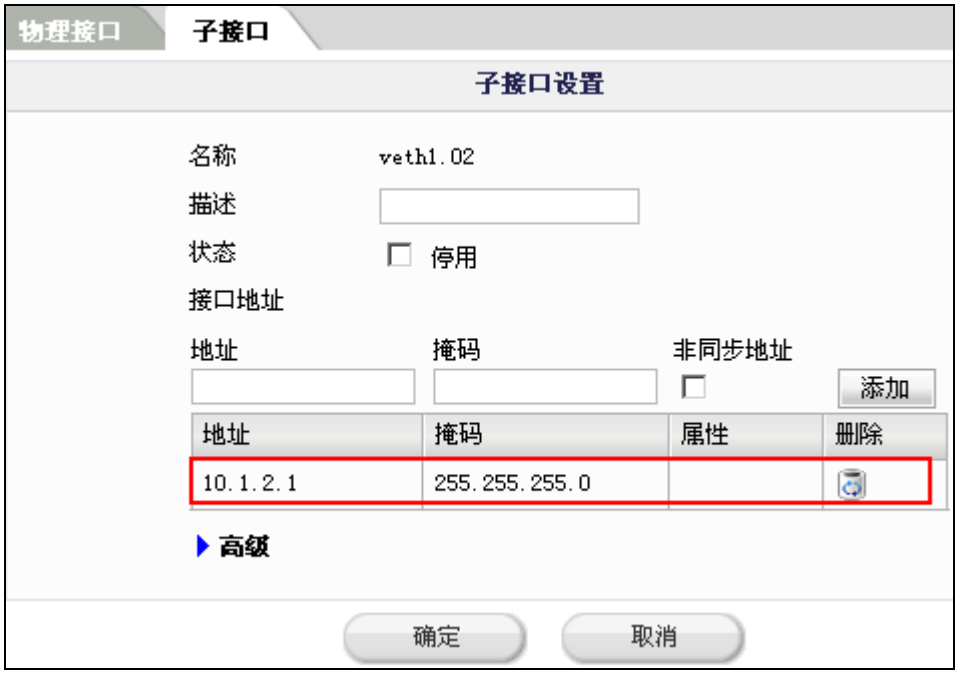
参数设置完成后，点击“确定”按钮即可。

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。

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。

参数设置完成后，点击“确定”按钮即可。

③ 点击 veth1.02 接口右侧的修改图标“ ”，配置该子接口的 IP 地址，如下图所示。

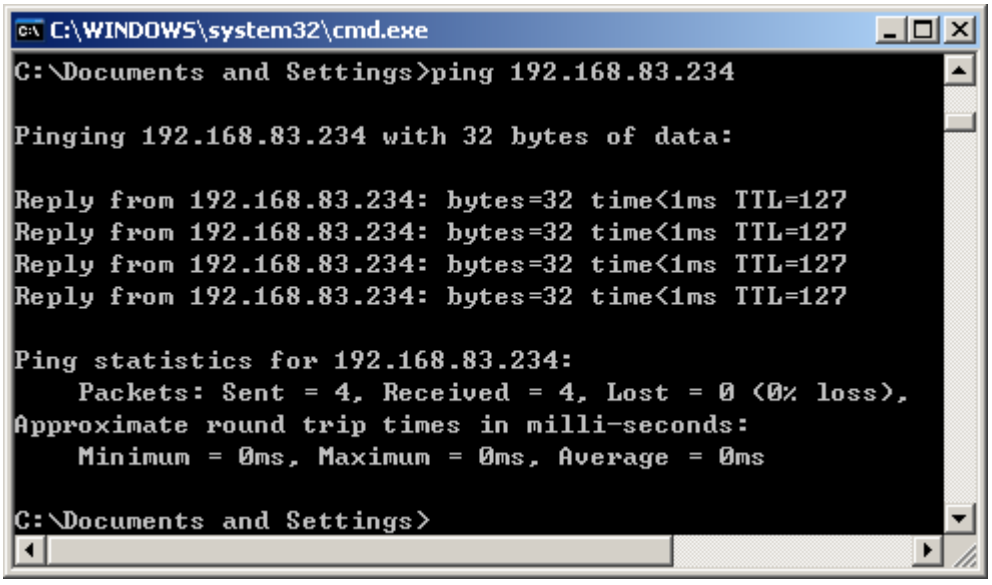


在 veth1.02 接口配置页面，点击“高级”左侧图标，配置该子接口属于 VS2，如下图所示。

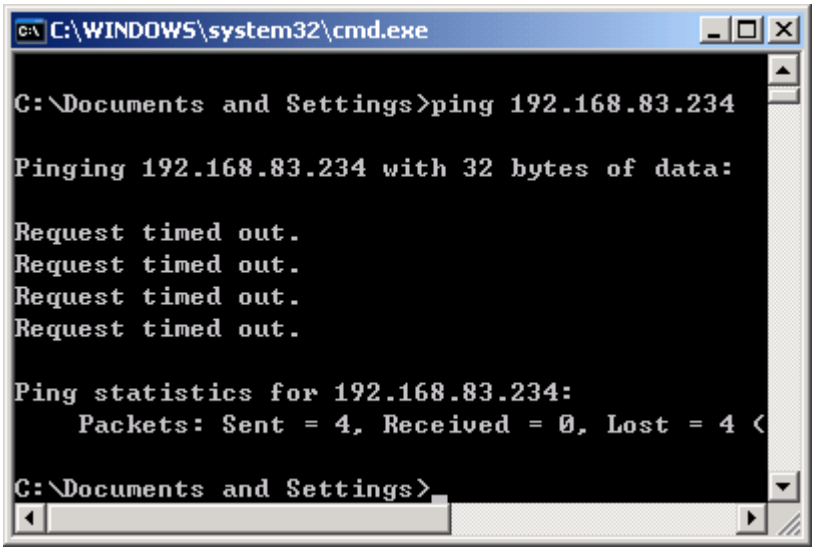
参数设置完成后，点击“确定”按钮即可。

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。

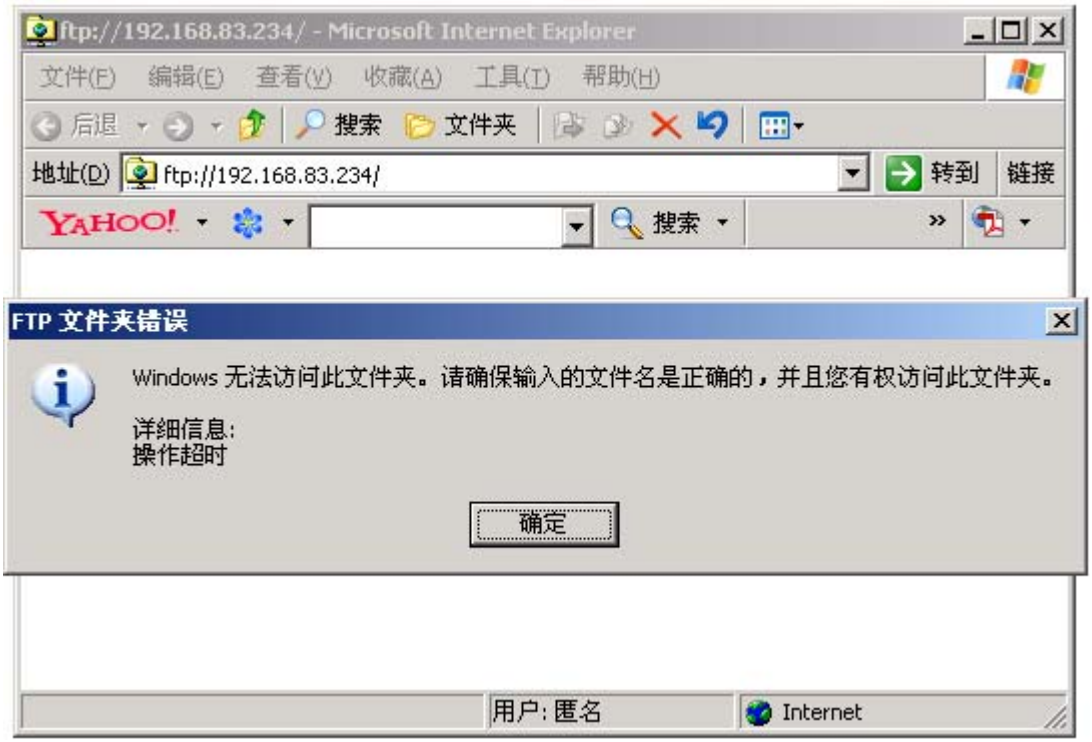


在主机 B 上 ping 主机 C，不能收到主机 C 的 ping 回应，如下图所示。



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。



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。

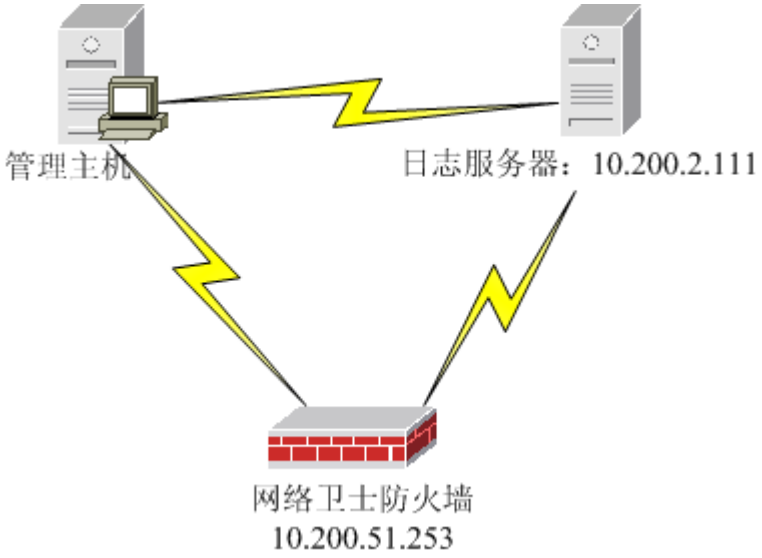


图 43 防火墙与日志系统连接示意图

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

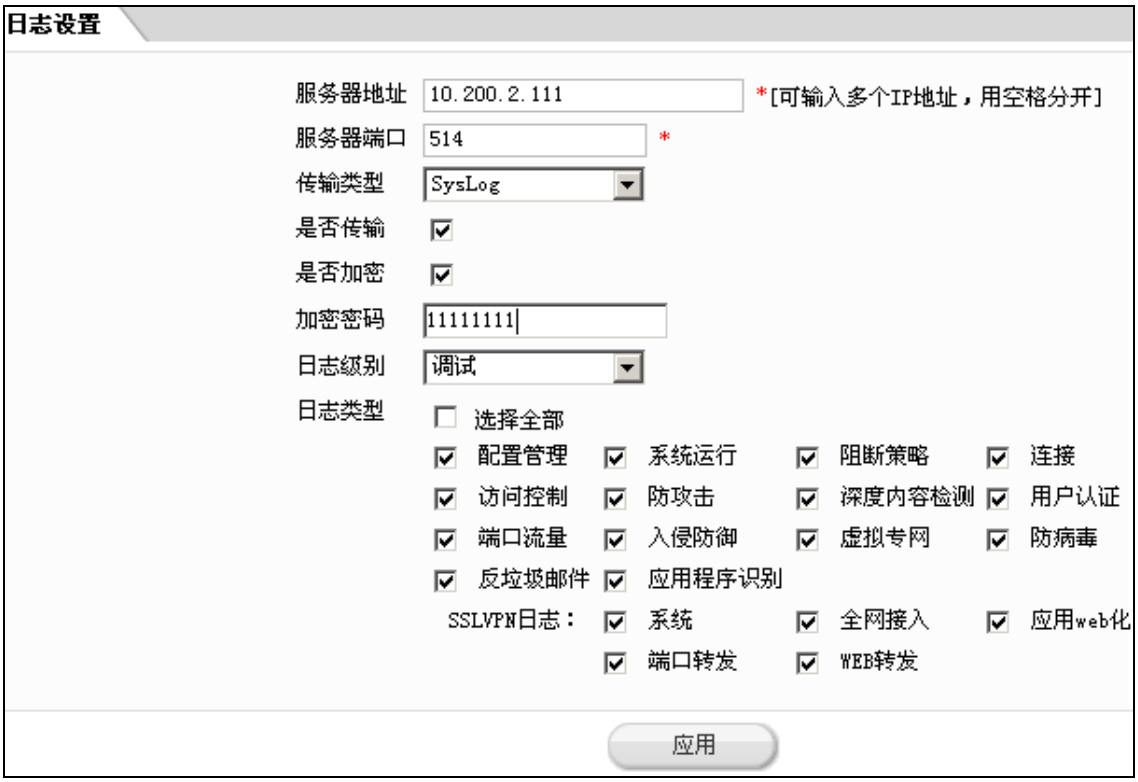
- 在每台需要进行日志分析的网络卫士防火墙上配置日志服务器及相应参数
- 查看防火墙中的日志信息

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。

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。

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。

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。

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。

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。

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。

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。

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。

2. 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。

3. 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。

4. 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。