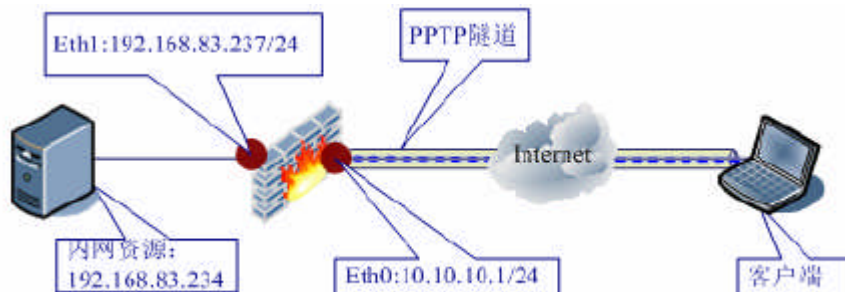


PPTP 隧道

举例如下

远程客户端与防火墙建立 PPTP VPN 隧道，安全访问内网资源。



图例： 远程用户通过 PPTP 隧道访问内网示意图

本例中防火墙的 Eth0 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

- 1、配置远程用户
- 2、开放相关接口的 PPTP 服务
- 3、配置 PPTP 服务
- 4、配置 PPTP 客户端
- 5、配置 PPTP 的访问控制

WebUI 配置步骤

1) 配置远程用户。包括添加远程用户、启动内部 basic 认证服务器并设置用户角色。

a) 选择 用户认证 > Basic 认证，选择“用户列表”页签，点击“增加用户”添加类型为“远程用户”的新用户 pptpuser。该用户用于 PPTP 用户的身份认证。



b) 防火墙作为认证服务器接受 PPTP 用户的认证请求，需要在防火墙上启动内部认证服务器（默认为停止状态）。

选择 用户认证 > Basic 认证，并选择“Basic 认证服务器”页签，点击“启动”按钮启动内置认证服务器。

Basic认证服务器 | 用户列表 | 用户角色 | 活动用户

内置Basic服务器属性

内置Basic服务器：

认证服务器名称：

运行状态：

保活时间： [不小于60秒]

c) 将 PPTP 用户设置所属用户角色。不属于任何用户角色的用户无法通过认证服务器的认证。而且可以通过设置对用户角色的访问控制规则来实现对 PPTP 用户的访问控制。选择 用户认证 > Basic 认证，并选择“用户角色”页签，点击“添加”按钮，设置包含 PPTP 远程用户的用户角色。

Basic认证服务器 | 用户列表 | 用户角色 | 活动用户

用户角色属性

角色名称： *

所属服务器：

所有用户：☐

指定用户：☒

已有的用户列表

所有用户

点击“确定”，完成用户角色设置。界面如下图所示。

Basic认证服务器 | 用户列表 | 用户角色 | 活动用户

用户角色

[添加] [清空]

用户角色名称	认证服务器	用户名列表	修改	删除
bbb1	basic			
pptp_group	basic	pptpuser		

2) 开放 Eth0 口的 PPTP 服务。

a) 选择 资源管理 > 区域，设置区域 intranet、dmz 分别和属性 eth0、eth1 绑定，权限为允许访问。

区域 [添加] [清空]					
名称	绑定属性(可多选)	权限	注释	修改	删除
area_eth0	eth0	允许			
area_eth1	eth1	允许			
area_eth2	eth2	允许			
adsl-a	adsl	允许			
intranet	eth0	允许			
dmz	eth1	允许			

b) 选择 系统管理 > 配置 菜单，并选择“开放服务”页签，开放该区域的 PPTP 服务服务。

开放服务 [添加]				
服务名称	控制区域	控制地址	修改	删除
gui	area_eth0	any		
ssh	area_eth0	any		
ping	area_eth0	any		
webui	area_eth0	any		
telnet	area_eth0	any		
auth	area_eth1	any		
webui	area_eth1	any		
gui	area_eth1	any		
ping	area_eth1	any		
ssh	area_eth1	any		
auth	area_eth0	any		
monitor	area_eth0	any		
snmp	area_eth0	any		
snmp	area_eth1	any		
update	area_eth0	any		
ntp	area_eth0	any		
rip	area_eth0	any		
dhcp	area_eth0	83.234		
dhcp	area_eth1	any		
pptp	intranet	any		

3) 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。

PPTP设定

PPTP端口：1723 *

本地地址：172.16.100.1 *

起始地址：172.16.200.101 *

结束地址：172.16.200.200 *

PPTP状态

```
pptpd is not running.
```

启动

停止

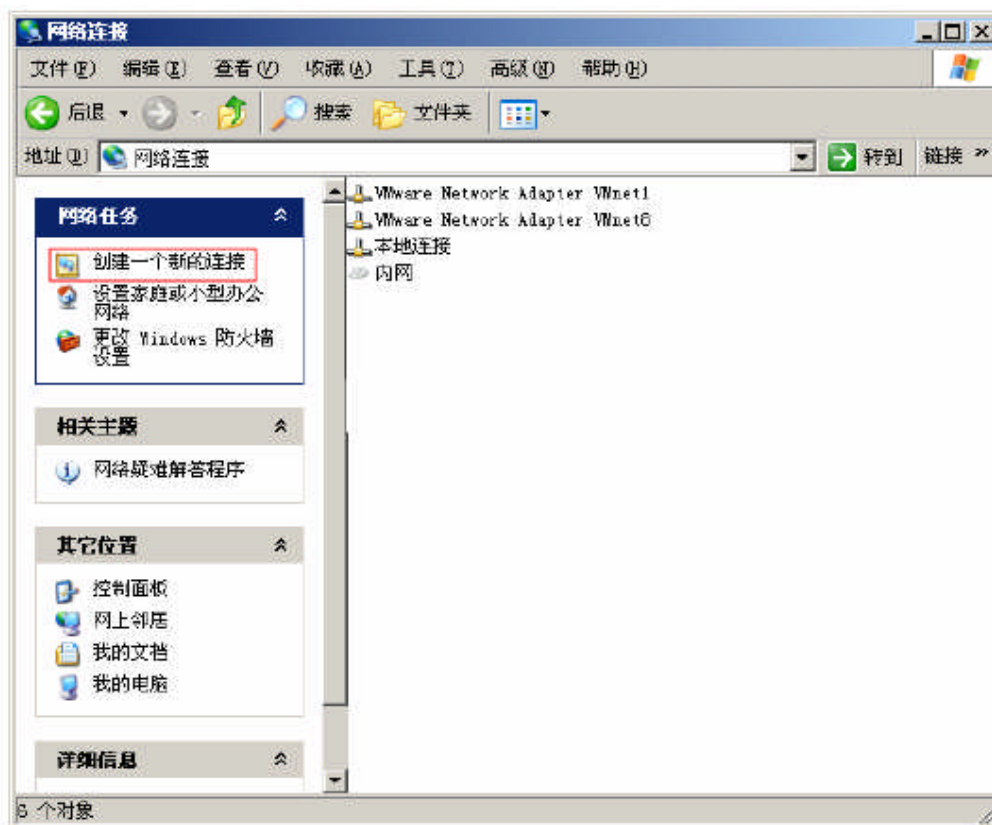
应用

需要注意的是：PPTP 服务器的起始地址和结束地址必须和本地地址（服务器的虚拟 IP）在同一个网段。

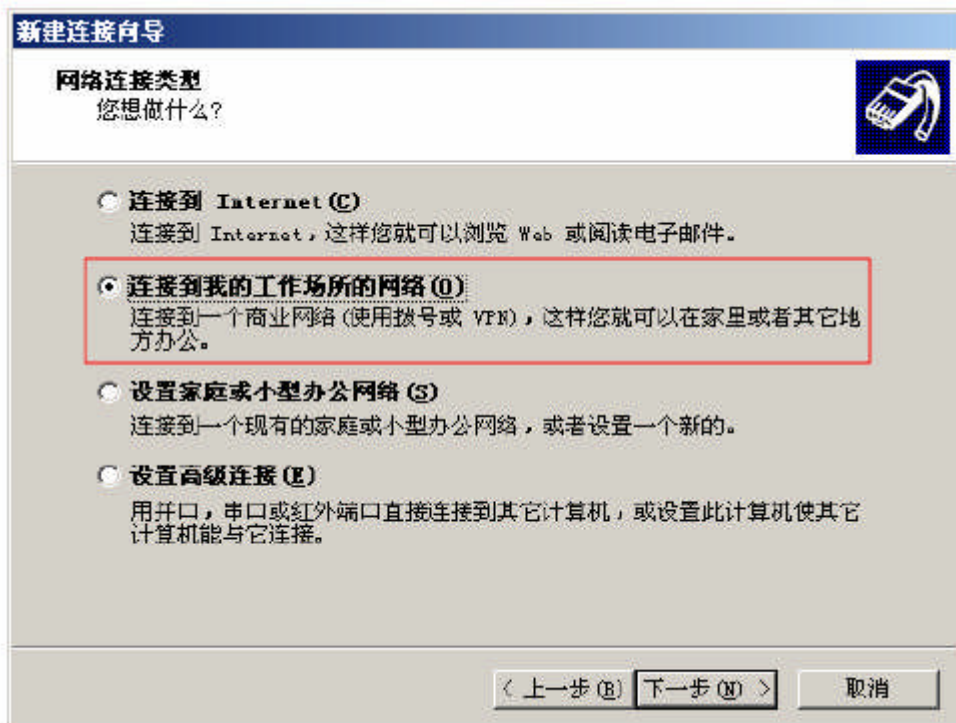
点击“启动”，成功后进入等待远程 PPTP 客户端的连接。

4) 配置 PPTP 客户端（以 windows 2000 为例）

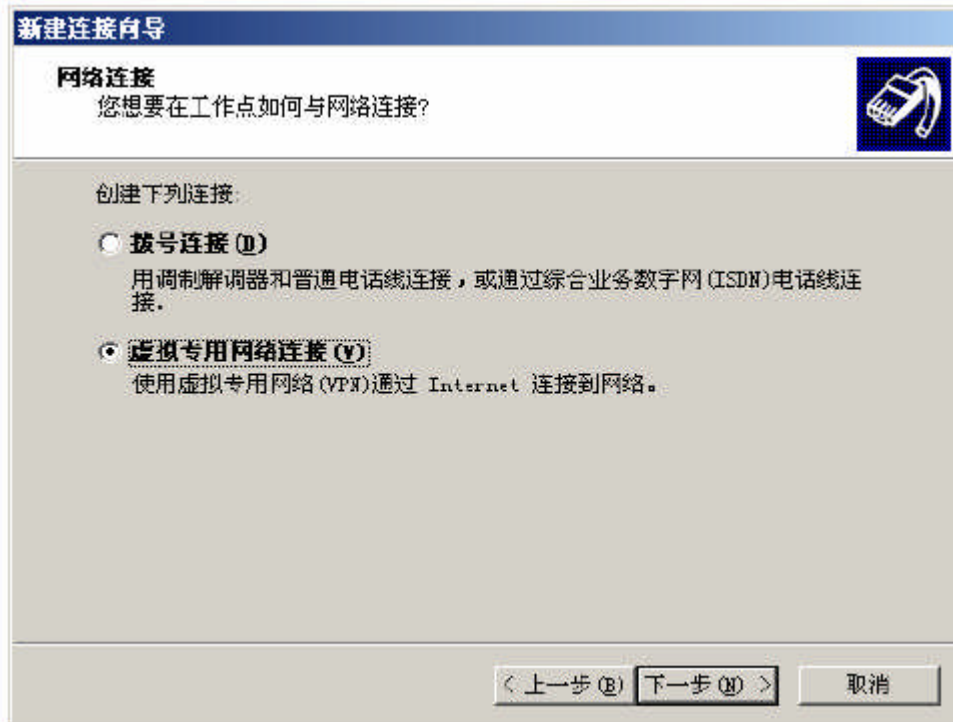
需要确认 PPTP 客户端可以访问防火墙的 Eth0 接口。在控制面板中打开网络连接



点击“创建一个新连接”，新建一个连接（VPN）。



选择网络连接类型为“连接到我的工作场所的网络”。



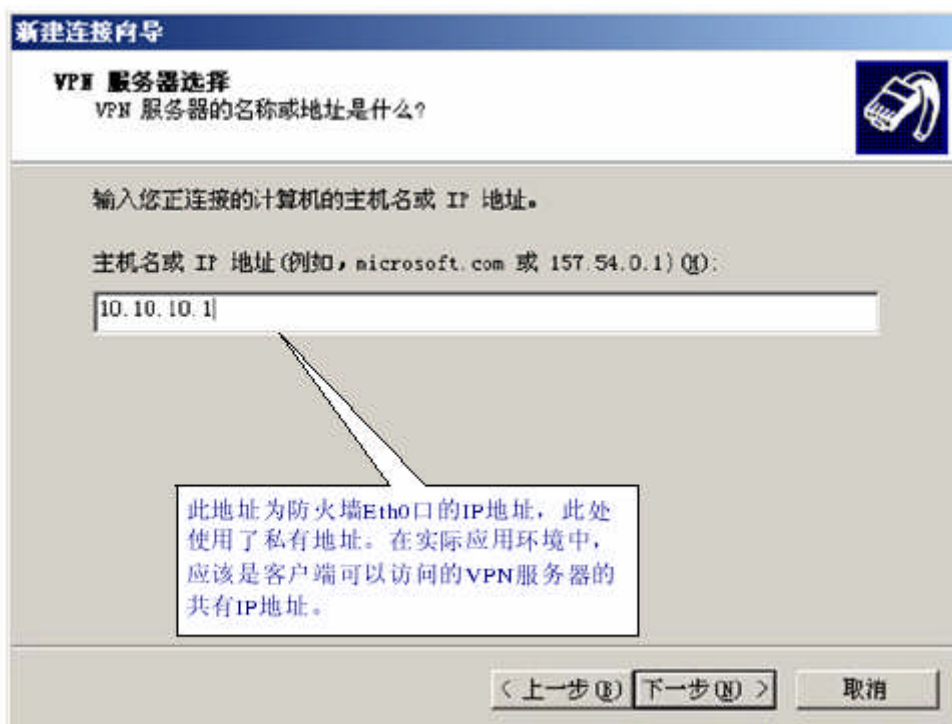
选择创建“虚拟专用网连接”。



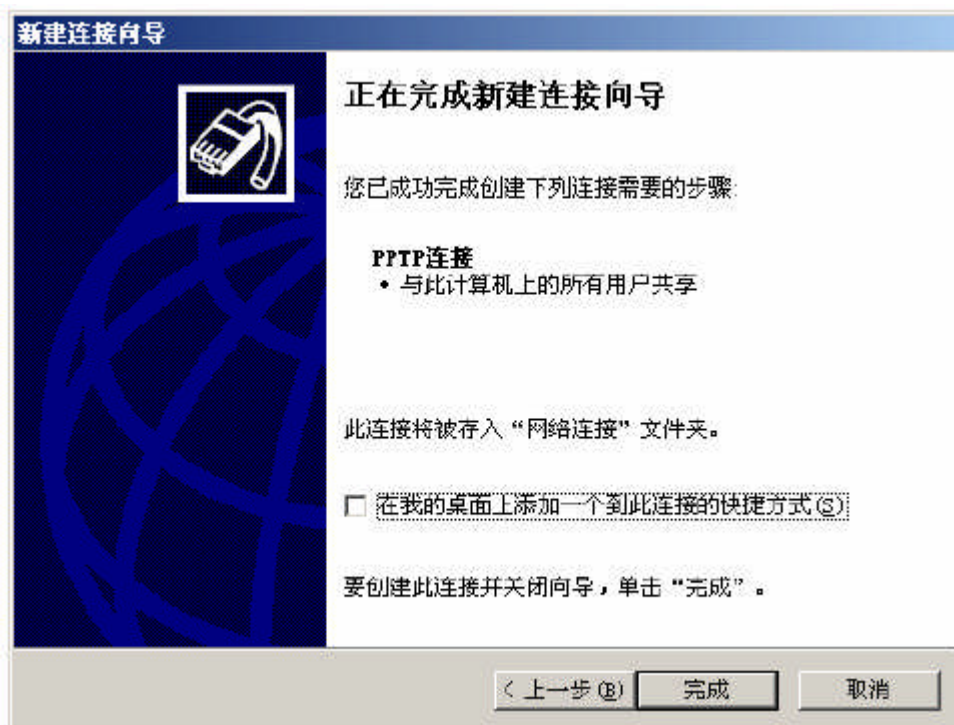
输入为此 VPN 连接定义的名字 (例如 PPTP 连接)。



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。

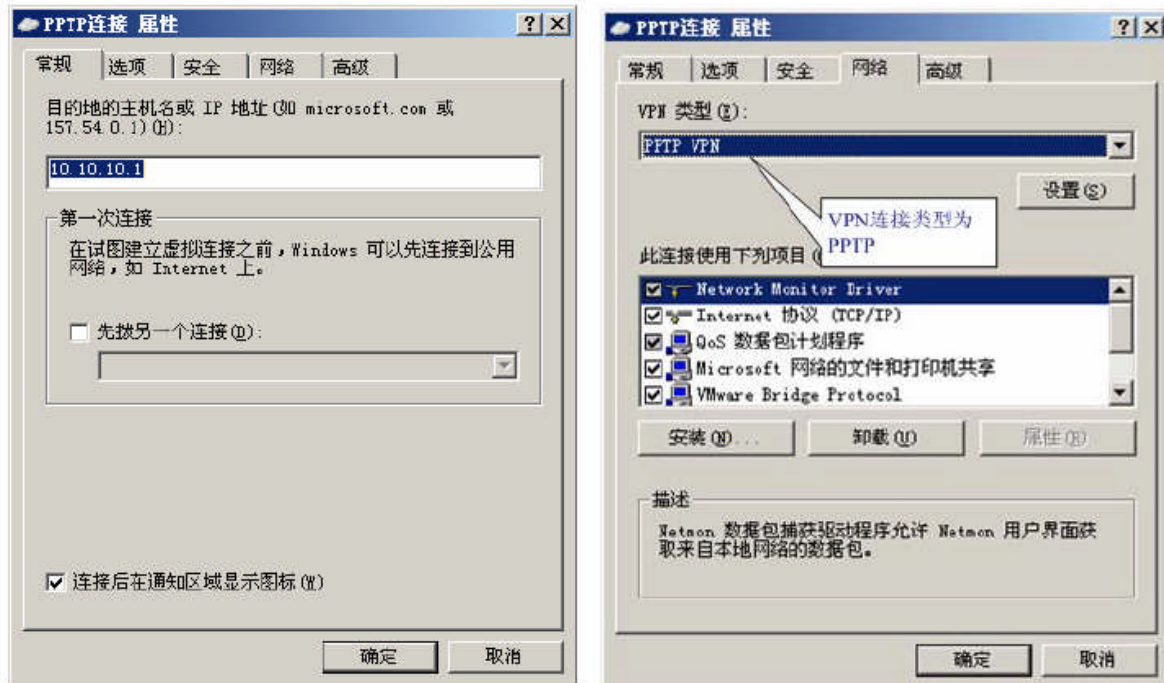


输入防火墙上开放 PPTP 服务的接口的 IP 地址,此例中为 10.10.10.1,如上图所示。

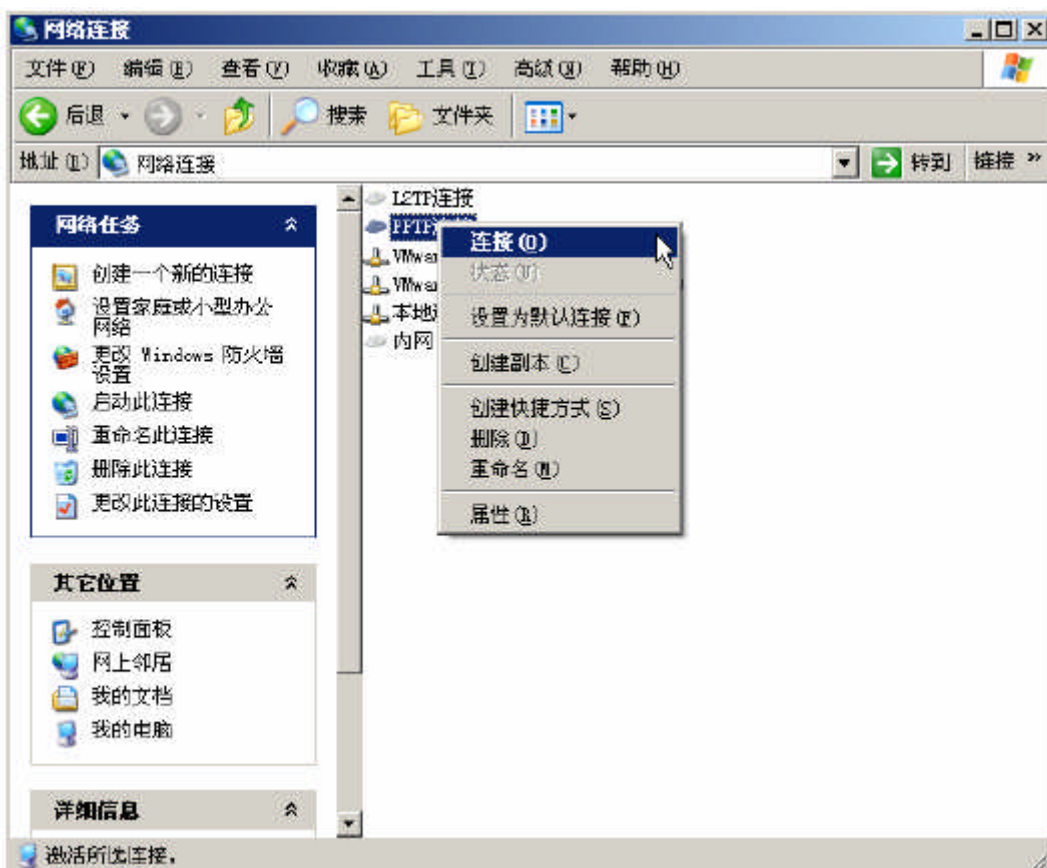


点击“完成”完成设置，会出现该连接，右键修改其属性。





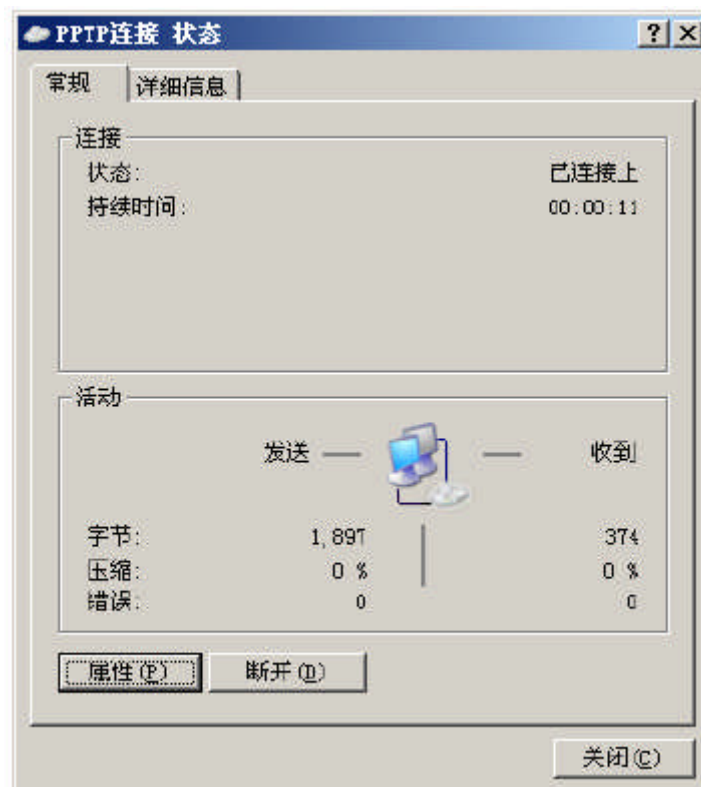
5) 建立 PPTP VPN 隧道



输入已在防火墙上设好的远程用户的用户名（pptpuser@basic）和密码，点击连接按钮。



连接成功后如下图。



6) 设置内网资源对象。

选择 资源管理 > 地址，并选择“主机”页签添加内网资源对象 83.234。

主机 | 范围 | 子网 | 地址组

主机地址

[添加] [清空]

名称	IP地址	修改	删除
83.234	192.168.83.234		
172.16.1.2	172.16.1.2		

7) 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。

a) 通过对 PPTP 区域的控制完成访问控制。

选择 资源管理 > 区域, 添加区域 pptp_area 并和 pptp 属性绑定, 权限为默认权限“允许”。pptp_area 区域可以作为源或目的区域在访问控制规则中使用。

区域

[添加] [清空]

名称	绑定属性(可多选)	权限	注释	修改	删除
area_eth0	eth0	允许			
area_eth1	eth1	允许			
area_eth2	eth2	允许			
adsl-a	adsl	允许			
intranet	eth0	允许			
dmz	eth1	允许			
pptp_area	pptp	允许			

“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。

选择 防火墙 > 访问控制, 点击“添加”按钮设置新的访问控制规则。

访问控制规则

[添加] [清空]

源区域 目的区域 地址 服务 查找

所有区域 所有区域

ID	控制	源	目的	服务	时间	日志	选项	修改	移动	插入	删除
8157	✓	(pptp_area)	(dmz) 转换前目的:83.234								

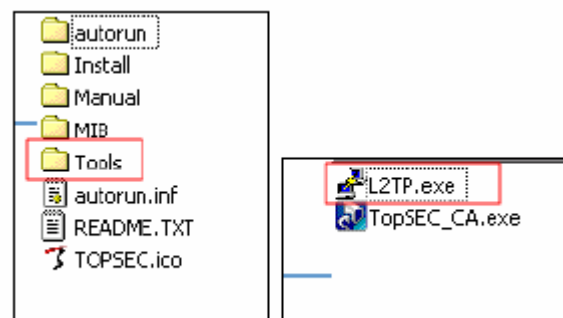
b) 通过基于认证用户角色的访问控制来实现对 PPTP 用户的访问控制。

选择 防火墙 > 访问控制, 点击“添加配置”按钮设置新的访问控制规则。



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，该程序在防火墙随机光盘和 TOPSEC 的网站上均可获取。光盘位置如下图所示：

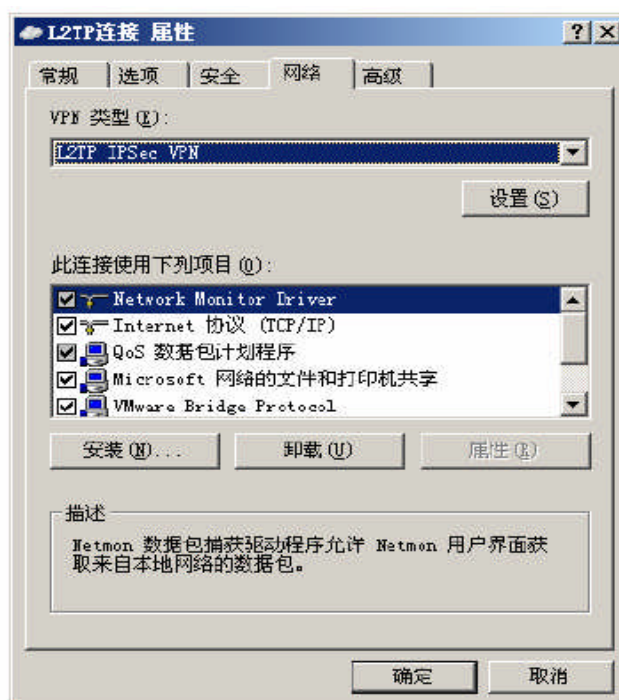


安装该程序后，必须重启系统才可以生效。运行该程序，如下图。



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。

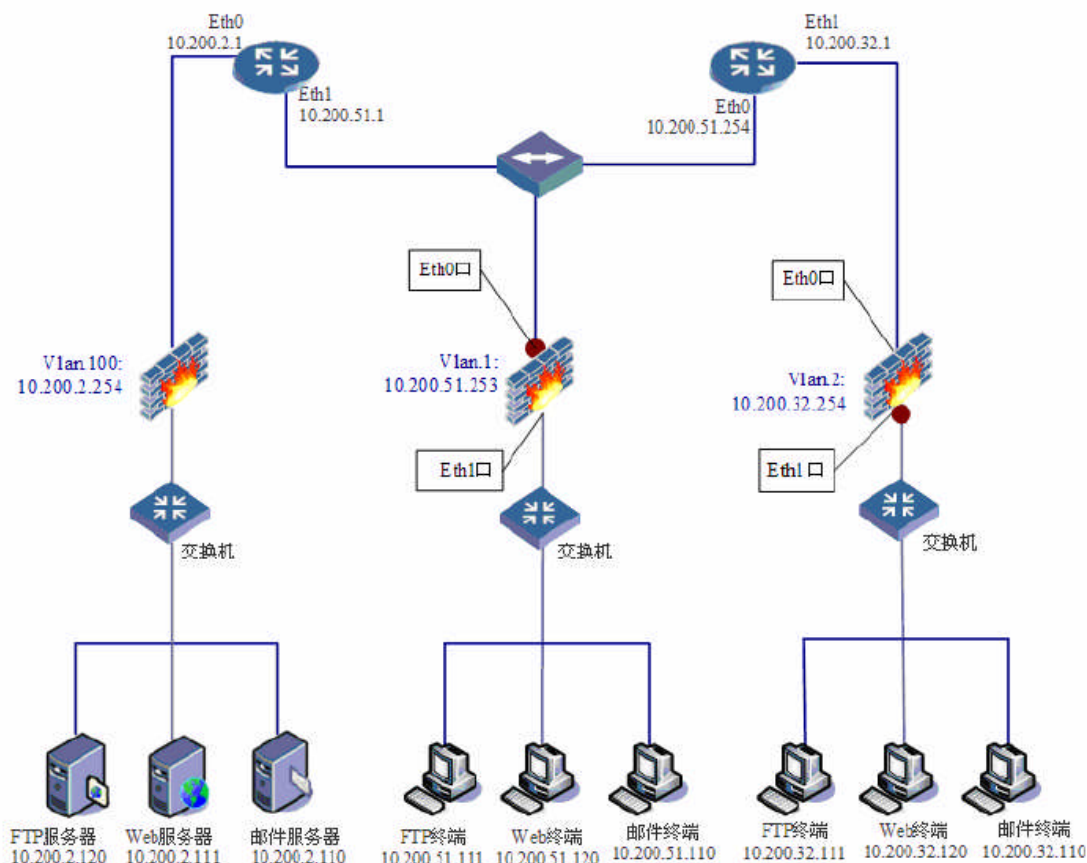


详细配置请参考 PPTP 案例。

带宽管理 QoS

QoS（服务质量），是 Quality of Service 的缩写。通过 QoS 管理，用户可以根据实际用户网络规划，方便、灵活地定制带宽策略，防止带宽滥用现象，并确保关键应用的带宽需求。

网络卫士防火墙的带宽策略采用了分层的带宽管理机制，用户可以通过设置细粒度的带宽规则来实现基于源和目的 IP 地址（或地址段）、服务的带宽的集中管理。同时，同层的带宽策略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。



图例： 防火墙分层带宽管理示意图

图中的防火墙工作在纯透明模式（即所有接口均工作在交换模式下，且属于同一个VLAN），只起到限制带宽的作用，不做任何访问策略配置。防火墙的初始配置不需要用户进行修改。

上传带宽管理

基本需求

子网 1（10.200.51.0/24）向网段 10.200.2.0/24 上传数据，防火墙为其分配 7K（如果没有特殊说明单位均为字节/秒）的限制带宽，7K 的保证带宽。并对不同的应用设置不同的优先级控制以及带宽优化：

- 1、ICMP 为最高优先级，保证带宽为 1K（最大限制带宽为 7K）
- 2、数据库为第二优先级，保证带宽为 2K（最大限制带宽为 7K）
- 3、FTP 为第三优先级，保证带宽为 2K（最大限制带宽为 7K）
- 4、SMTP 为最低优先级，保证带宽为 1K（最大限制带宽为 7K）

配置要点

带宽策略的设置包括以下方面：

- 1、设置采用 QoS 的物理接口。
- 2、在接口下设置一到多个类及其子类。
- 3、在类下设置数据流的匹配规则。

WEBUI 配置步骤

1) 设置采用 QoS 的物理接口。

选择 网络管理 > 流量管理，在“带宽控制”页面点击“添加接口”，添加采用上传带宽配置策略的物理接口 eth0。接口的配置原则是以数据流流向为准，在数据流出防火墙的物理接口上配置才能生效。本例中即 eth0 接口。

The screenshot shows a dialog box titled "带宽控制 | 流量统计" (Bandwidth Control | Traffic Statistics). Inside, there is a section "添加接口" (Add Interface). Below this, there is a label "接口:" (Interface:) followed by a text input field containing "eth0". At the bottom of the dialog, there are two buttons: "确定" (Confirm) and "取消" (Cancel).

点击“确定”，则新添加的接口显示在右侧界面中，如下图所示。

The screenshot shows the "带宽管理" (Bandwidth Management) section of the "带宽控制 | 流量统计" (Bandwidth Control | Traffic Statistics) interface. It includes a "[添加接口]" (Add Interface) button. Below is a table with the following data:

类型	名称	上级	属性	下级	修改	删除
Dev	eth0					

2) 在物理接口下设置上传类及其四个子类：ICMP 上传、Web 上传、FTP 上传、邮件上传。

a) 点击接口 eth0 对应的“下级”，添加 eth0 口的上传带宽类“上传类”。

The screenshot shows the "带宽规则" (Bandwidth Rule) configuration dialog box. It contains the following fields and options:

- 类型 (Type): class (dropdown menu)
- 名称 (Name): 上传类 (text input)
- 父带宽 (Parent Bandwidth): eth0 (text input)
- 优先级 (Priority): 0 (dropdown menu)
- 保证带宽 (Guaranteed Bandwidth): 7K (text input) [M, K, 默认为：字节每秒]
- 限制带宽 (Limited Bandwidth): 7K (text input) [M, K, 默认为：字节每秒]

At the bottom, there are two buttons: "确定" (Confirm) and "取消" (Cancel).

点击“确定”，则新添加的类显示在接口 eth0 下，如下图所示。

带宽控制 流量统计						
带宽管理				[添加接口]		
类型	名称	上级	属性	下级	修改	删除
Dev	eth0					
class	上传类	eth0	优先级:0 保证带宽:7Kbps, 限制带宽:7Kbps			

b) 点击“上传类”所在行的“下级”图标，添加上传业务带宽子类，共分为 4 个优先级。

“ICMP 上传”为最高优先级 0，保证带宽为 1K（最大限制带宽为 7K）

“Web 上传”为第二优先级 1，保证带宽为 2K（最大限制带宽为 7K）

“FTP 上传”为第三优先级 2，保证带宽为 2K（最大限制带宽为 7K）

“邮件上传（SMTP）”为最低优先级 3，保证带宽为 1K（最大限制带宽为 7K）

设置完成后界面如下图所示。

带宽控制 流量统计						
带宽管理				[添加接口]		
类型	名称	上级	属性	下级	修改	删除
Dev	eth0					
class	上传类	eth0	优先级:0 保证带宽:7Kbps, 限制带宽:7Kbps			
class	ICMP上传	上传类	优先级:0 保证带宽:1Kbps, 限制带宽:7Kbps			
class	Web上传	上传类	优先级:1 保证带宽:2Kbps, 限制带宽:7Kbps			
class	FTP上传	上传类	优先级:2 保证带宽:3Kbps, 限制带宽:7Kbps			
class	邮件上传(SMTP)	上传类	优先级:3 保证带宽:1Kbps, 限制带宽:7Kbps			

需要注意的是：子类的保证带宽之和不能大于父类的保证带宽。每个类中的保证带宽不能大于限制带宽。

3) 设置带宽管理策略。

点击“ICMP 上传”所在行的“下级”图标，添加 ICMP 上传业务带宽规则（ICMP-rule）。

带宽控制 | 流量统计

带宽规则

类型: rule
 名称: ICMP-rule
 父带宽: ICMP上传
 优先级: 0
 策略源: --任意--
 策略目的: --任意--
 服务类型: PING (ICMP:8)
 时间: 工作时段内

确定 取消

图中的“时间对象”用户可以通过 资源管理 > 时间，并根据自己的需求进行设置。
点击“Web 上传”所在行的“下级”图标，添加 Web 上传业务带宽规则（Web-rule）。

带宽控制 | 流量统计

带宽规则

类型: rule
 名称: Web-rule
 父带宽: Web上传
 优先级: 0
 策略源: --任意--
 策略目的: --任意--
 服务类型: HTTP (TCP:80)
 时间: 工作时段内

确定 取消

点击“FTP 上传”所在行的“下级”图标，添加 FTP 上传业务带宽规则（FTP-rule）。

带宽控制 | 流量统计

带宽规则

类型: rule
 名称: FTP-rule
 父带宽: FTP上传
 优先级: 0
 策略源: --任意--
 策略目的: --任意--
 服务类型: FTP (TCP:21)
 时间: 工作时段内

确定 取消

点击“邮件上传（SMTP）”所在行的“下级”图标，添加邮件上传业务带宽规则（SMTP-rule）。

带宽控制 | 流量统计

带宽规则

类型: rule
 名称: SMTP-rule
 父带宽: 邮件上传（SMTP）
 优先级: 0
 策略源: --任意--
 策略目的: --任意--
 服务类型: SMTP (TCP:25)
 时间: 工作时段内

确定 取消

4) 设置完成后，单击“确定”按钮。
配置好 QoS 策略的界面如下图所示。

带宽控制 | 流量统计

带宽管理

[添加接口]

类型	名称	上级	属性	下级	修改	删除
Dev	eth0					
class	上传类	eth0	优先级:0 保证带宽:7KBps, 限制带宽:7KBps			
class	ICMP上传	上传类	优先级:0 保证带宽:1KBps, 限制带宽:7KBps			
rule	ICMP-rule	ICMP上传	优先级:0 源:任意, 目的:任意 服务:PING, 时间:工作时段内			
class	Web上传	上传类	优先级:1 保证带宽:2KBps, 限制带宽:7KBps			
rule	Web-rule	Web上传	优先级:0 源:任意, 目的:任意 服务:HTTP, 时间:工作时段内			
class	FTP上传	上传类	优先级:2 保证带宽:3KBps, 限制带宽:7KBps			
rule	FTP-rule	FTP上传	优先级:0 源:任意, 目的:任意 服务:FTP, 时间:工作时段内			
class	邮件上传(SMTP)	上传类	优先级:3 保证带宽:1KBps, 限制带宽:7KBps			
rule	SMTP-rule	邮件上传(SMTP)	优先级:0 源:任意, 目的:任意 服务:SMTP, 时间:工作时段内			

5) 点击规则所在行的“修改”图标可以完成对已添加规则的修改。

6) 对于已经添加的类，则：

如果该类没有子类，可以直接点击“修改”图标进行修改。如果该类有子类，则必须首先删除子类，然后才能点击“修改”图标进行修改。

7) 删除一个接口或类时，必须先删除该接口或类的所有子类和规则。

注意事项

1) Windows 的文件共享服务首先通过 TCP: 139 端口进行连接，如果连接不成功，会使用 TCP: 445 端口，故针对 Windows 文件共享服务做 QoS 策略时，还需添加一条针对 TCP: 139 端口的 QoS 策略，具体配置：先在自定义服务（选择 资源管理 > 服务，选择“自定义服务”页签）中添加 TCP: 139 端口这样一条服务，再在 QoS 策略中的设置一条针对该服务的带宽控制规则。

2) 在设置带宽控制规则时，策略源、策略目的和服务均不可选择“任意”，最好选择“any”地址对象或者根据需要定义的地址范围、子网、或者用户组对象。

3) 流量控制配置上传和下载的策略源和策略目的是相反的，如 FTP，在控制上传配置时，策略源是 FTP 客户端，策略目的是 FTP 服务器；而在控制下载配置时，策略源则是 FTP 服务器，策略目的是 FTP 客户端。

4) 在修改了 QoS 策略后，需要在管理器右上角点击“刷新连接”，进行“刷新连接”操作，使修改的配置生效。并且对于以前已经建立的连接如 FTP、文件共享等，则需要重新连接后才能应用新的 QoS 策略。

下载带宽管理

基本需求

子网 1 (10.200.51.0/24) 需要从网段 10.200.2.0/24 下载数据，防火墙为其分配 7K（如果没有特殊说明单位均为字节/秒）的限制带宽，7K 的保证带宽。并对不同的应用设置不同的优先级控制以及带宽优化：

- 1、ICMP 为最高优先级，保证带宽为 1K（最大限制带宽为 7K）
- 2、Web 为第二优先级，保证带宽为 2K（最大限制带宽为 7K）
- 3、FTP 为第三优先级，保证带宽为 2K（最大限制带宽为 7K）
- 4、SMTP 为最低优先级，保证带宽为 1K（最大限制带宽为 7K）

配置要点

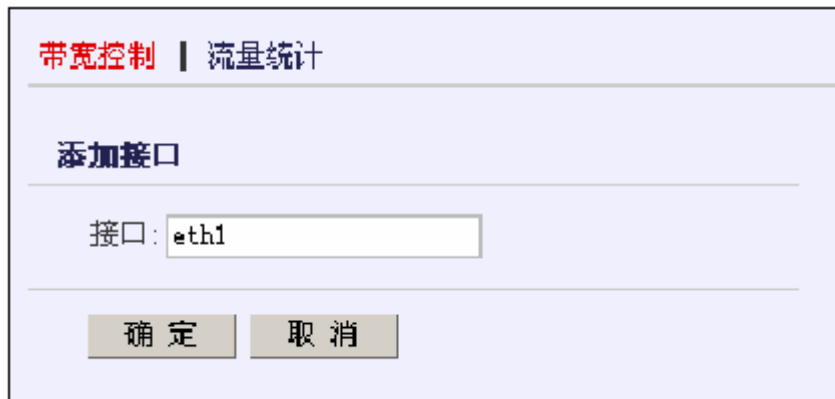
带宽策略的设置包括以下方面：

- 1、设置采用 QoS 的物理接口。
- 2、在接口下设置一到多个类及其子类。
- 3、在类下设置数据流的匹配规则

WEBUI 配置步骤

- 1) 设置采用 QoS 的物理接口。

选择 网络管理 > 流量管理，在“带宽控制”页面点击“添加接口”按钮，添加要应用下载带宽控制策略的物理接口 eth1，接口的配置原则是以数据流流向为准，在数据流出防火墙的物理接口上配置才能生效。本例中即 eth1 接口。



点击“确定”，则新添加的接口显示在右侧界面中。

- 2) 点击接口 eth1 对应的“下级”，在物理接口 eth1 口下设置“下载类”及其四个子类：ICMP 下载、Web 下载、FTP 下载、邮件下载。

- a) 添加下载带宽类“下载类”

带宽控制 | 流量统计

带宽规则

类型:
 名称:
 父带宽:
 优先级:
 保证带宽: [M, K, 默认为: 字节每秒]
 限制带宽: [M, K, 默认为: 字节每秒]

点击“确定”，则新添加的类显示在接口 eth1 下，如下图所示。

带宽控制 | 流量统计

带宽管理 [添加接口]

类型	名称	上级	属性	下级	修改	删除
Dev	eth0					
class	上传类	eth0	优先级:0 保证带宽:7KBps, 限制带宽:7KBps			
class	ICMP上传	上传类	优先级:0 保证带宽:1KBps, 限制带宽:7KBps			
rule	ICMP-rule	ICMP上传	优先级:0 源:任意, 目的:任意 服务:PING, 时间:工作时段内			
class	Web上传	上传类	优先级:1 保证带宽:2KBps, 限制带宽:7KBps			
rule	Web-rule	Web上传	优先级:0 源:任意, 目的:任意 服务:HTTP, 时间:工作时段内			
class	FTP上传	上传类	优先级:2 保证带宽:3KBps, 限制带宽:7KBps			
rule	FTP-rule	FTP上传	优先级:0 源:任意, 目的:任意 服务:FTP, 时间:工作时段内			
class	邮件上传(SMTP)	上传类	优先级:3 保证带宽:1KBps, 限制带宽:7KBps			
rule	SMTP-rule	邮件上传(SMTP)	优先级:0 源:任意, 目的:任意 服务:SMTP, 时间:工作时段内			
Dev	eth1					
class	下载类	eth1	优先级:0 保证带宽:7KBps, 限制带宽:7KBps			

b) 点击“下载类”所在行的“下级”图标，添加下载业务带宽子类，共分为 4 个优先级。

“ICMP 下载”为最高优先级 0，保证带宽为 1K（最大限制带宽为 7K）。

“Web 下载”为第二优先级 1，保证带宽为 2K（最大限制带宽为 7K）。

“FTP 下载”为第三优先级 2，保证带宽为 2K（最大限制带宽为 7K）。

“邮件下载（POP3）”为最低优先级 3，保证带宽为 1K（最大限制带宽为 7K）。
设置完成后界面如下图所示。

Dev	eth1					
class	下载类	eth1	优先级:0 保证带宽:7KBps, 限制带宽:7KBps			
class	ICMP下载	下载类	优先级:0 保证带宽:1KBps, 限制带宽:7KBps			
class	Web下载	下载类	优先级:1 保证带宽:2KBps, 限制带宽:7KBps			
class	FTP下载	下载类	优先级:2 保证带宽:3KBps, 限制带宽:7KBps			
class	邮件下载 (SMTP)	下载类	优先级:3 保证带宽:1KBps, 限制带宽:7KBps			

需要注意的是：子类的保证带宽之和不能大于父类的保证带宽，每个类中的保证带宽的值不能大于限制带宽的值。

3) 设置带宽管理策略。

点击“ICMP 下载”所在行的“下级”图标，添加 ICMP 下载业务带宽规则（ICMP-down）。

带宽控制 | 流量统计

带宽规则

类型：

rule

名称：

ICMP-down

父带宽：

ICMP下载

优先级：

0

策略源：

--任意--

策略目的：

--任意--

服务类型：

PING (ICMP:8)

时间：

工作时段内

确定

取消

图中的“时间对象”用户可以通过 资源管理 > 时间，并根据自己的需求进行设置。
点击“Web 下载”所在行的“下级”图标，添加 Web 下载业务带宽规则（Web-down）。

带宽控制 | 流量统计

带宽规则

类型: rule
名称: Web-down
父带宽: Web下载
优先级: 0
策略源: --任意--
策略目的: --任意--
服务类型: HTTP (TCP:80)
时间: 工作时段内

确定

取消

点击“FTP 下载”所在行的“下级”图标，添加 FTP 下载业务带宽规则（FTP-down）。

带宽控制 | 流量统计

带宽规则

类型: rule
名称: FTP-down
父带宽: FTP下载
优先级: 0
策略源: --任意--
策略目的: --任意--
服务类型: FTP (TCP:21)
时间: 工作时段内

确定

取消

点击“邮件下载 (POP3)”所在行的“下级”图标，添加邮件下载业务带宽规则（POP3-down）。

带宽控制 | 流量统计

带宽规则

类型: rule
 名称: POP3-down
 父带宽: 邮件下载 (POP3)
 优先级: 0
 策略源: --任意--
 策略目的: --任意--
 服务类型: POP3 (TCP:110)
 时间: 工作时段内

确定 取消

4) 设置完成后, 单击“确定”按钮。
配置好 QoS 策略的界面如下图所示。

带宽控制 | 流量统计

带宽管理 [添加接口]

类型	名称	上级	属性	下级	修改	删除
Dev	eth1					
class	下载类	eth1	优先级:0 保证带宽:7KBps, 限制带宽:7KBps			
class	ICMP下载	下载类	优先级:0 保证带宽:1KBps, 限制带宽:7KBps			
rule	ICMP-down	ICMP下载	优先级:0 源:任意, 目的:任意 服务:PING, 时间:工作时段内			
class	Web下载	下载类	优先级:1 保证带宽:2KBps, 限制带宽:7KBps			
rule	Web-down	Web下载	优先级:0 源:任意, 目的:任意 服务:HTTP, 时间:工作时段内			
class	FTP下载	下载类	优先级:2 保证带宽:3KBps, 限制带宽:7KBps			
rule	FTP-down	FTP下载	优先级:0 源:任意, 目的:任意 服务:FTP, 时间:工作时段内			
class	邮件下载 (POP3)	下载类	优先级:3 保证带宽:1KBps, 限制带宽:7KBps			
rule	POP3-down	邮件下载 (POP3)	优先级:0 源:任意, 目的:任意 服务:POP3, 时间:工作时段内			

5) 点击规则所在行的“修改”图标可以完成对已添加规则的修改。

6) 对于已经添加的类，则：

如果该类没有子类，可以直接点击“修改”图标进行修改。

如果该类有子类，则必须首先删除子类，然后才能点击“修改”图标进行修改。

7) 删除一个接口或类时，必须先删除该接口或类的所有子类和规则。

注意事项

1) Windows 的文件共享服务首先通过 TCP: 139 端口进行连接，如果连接不成功会使用 TCP: 445 端口，故针对 Windows 文件共享服务做 QoS 策略时，还需添加一条针对 TCP: 139 端口的 QoS 策略，具体配置：先在自定义服务（选择 资源管理 > 服务，选择“自定义服务”页签）中添加 TCP: 139 端口这样一条服务，再在 QoS 策略中的设置一条针对该服务的带宽控制规则。

2) 在设置带宽控制规则时，策略源、策略目的和服务均不可选择“任意”，最好选择“any”地址对象或者根据需要定义的地址范围、子网、或者用户组对象。

3) 流量控制配置上传和下载的策略源和策略目的是相反的，如 FTP，在控制上传配置时，策略源是 FTP 客户端，策略目的是 FTP 服务器；而在控制下载配置时，策略源则是 FTP 服务器，策略目的是 FTP 客户端。

4) 在修改了 QoS 策略后，需要在管理器右上角点击“刷新连接”，进行“刷新连接”操作，使修改的配置生效。并且对于以前已经建立的连接如 FTP、文件共享等，则需要重新连接后才能应用新的 QoS 策略。

FTP 带宽管理

QoS（服务质量），是 Quality of Service 的缩写。通过 QoS 管理，用户可以根据实际用户网络规划，方便、灵活地定制带宽策略，防止带宽滥用现象，并确保关键应用的带宽需求。

网络卫士防火墙的带宽策略采用了分层的带宽管理机制，用户可以通过设置细粒度的带宽规则来实现基于源和目的 IP 地址（或地址段）、服务的带宽的集中管理。同时，同层的带宽策略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、用户分配带宽资源。

基本需求

为公司市场部的人员设置可用的 FTP 下载带宽

- 1、市场部经理保证带宽为 2M（最大限制带宽为 4M）
- 2、市场部员工保证带宽为 1M（最大限制带宽为 3M）
- 3、市场部配置保证带宽为 2M（最大限制带宽为 5M）

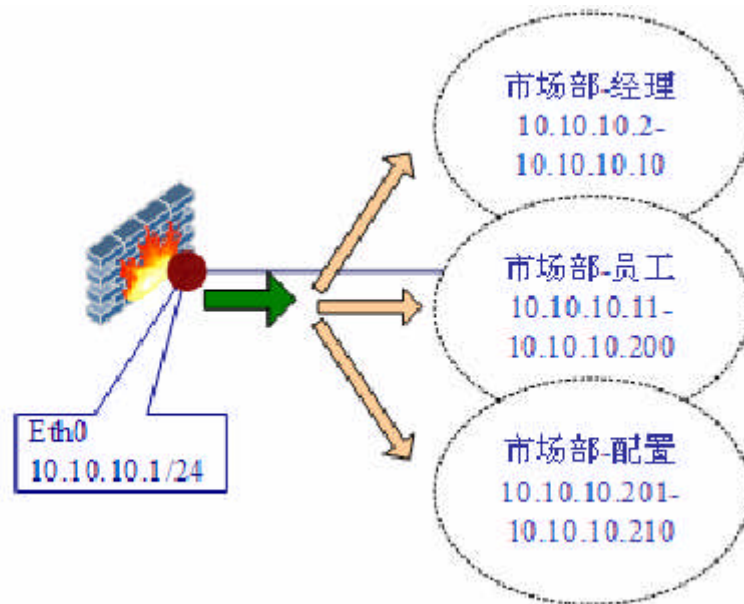


图 12 FTP 带宽管理示意图

配置要点

- 1、配置地址对象
- 2、配置带宽策略

WebUI 配置步骤

1) 配置地址对象

选择 资源管理 > 地址，选择“范围”页签，添加相应的地址范围。

主机 范围 子网 地址组							
地址范围				[添加] [清空]			
名称	起始地址	终止地址	除去地址	并发连接数	修改	删除	
any	0.0.0.0	255.255.255.255					
市场部-经理	10.10.10.2	10.10.10.10					
市场部-员工	10.10.10.11	10.10.10.200					
市场部-配置	10.10.10.201	10.10.10.210					

2) 配置带宽策略

选择 网络管理 > 流量管理，并点击“带宽控制”页签，添加接口 eth0。

带宽控制 | 流量统计

添加接口

接口:

确定

取消

添加 eth0 口的总带宽类 (ftp1)。注意：在接口下的一级子类的保证带宽和限制带宽必须相等。

带宽控制 | 流量统计

带宽规则

类型:

名称:

父带宽:

优先级:

保证带宽: [M, K, 默认为: 字节每秒]

限制带宽: [M, K, 默认为: 字节每秒]

确定

取消

添加市场部经理带宽子类 (ftp1-1)

带宽控制 | 流量统计

带宽规则

类型: class
 名称: ftp1-1
 父带宽: ftp1
 优先级: 0
 保证带宽: 2M [M, K, 默认为: 字节每秒]
 限制带宽: 4M [M, K, 默认为: 字节每秒]

确定 取消

添加市场部经理带宽规则 (ftp1-1rule)

带宽控制 | 流量统计

带宽规则

类型: rule
 名称: ftp1-rule
 父带宽: ftp1-1
 优先级: 0
 策略源: any [范围]
 策略目的: 市场部-经理 [范围]
 服务类型: FTP (TCP:21)
 时间: 工作时段内

确定 取消

图中的“时间对象”用户可以通过 资源管理 > 时间，并根据自己的需求进行设置。
添加市场部员工带宽子类 (ftp1-2)

带宽控制 | 流量统计

带宽规则

类型: class
 名称: ftp1-2
 父带宽: ftp1
 优先级: 0
 保证带宽: 1M [M, K, 默认为: 字节每秒]
 限制带宽: 3M [M, K, 默认为: 字节每秒]

确定 取消

添加市场部员工带宽规则 (ftp1-2rule)

带宽控制 | 流量统计

带宽规则

类型: rule
 名称: ftp1-2rule
 父带宽: ftp1-2
 优先级: 0
 策略源: any [范围]
 策略目的: 市场部-员工 [范围]
 服务类型: FTP (TCP:21)
 时间: 工作时段内

确定 取消

添加市场部配置带宽子类 (ftp1-3)

带宽控制 | 流量统计

带宽规则

类型: class
名称: ftp1-3
父带宽: ftp1
优先级: 0
保证带宽: 2M [M, K, 默认为: 字节每秒]
限制带宽: 5M [M, K, 默认为: 字节每秒]

确定

取消

添加市场部配置带宽规则 (ftp1-3rule)

带宽控制 | 流量统计

带宽规则

类型: rule
名称: ftp1-3rule
父带宽: ftp1-3
优先级: 0
策略源: any [范围]
策略目的: 市场部-配置 [范围]
服务类型: FTP (TCP:21)
时间: 工作时段内

确定

取消

配置好的界面如下图。

Dev	eth0					
class	ftp1	eth0	优先级:0 保证带宽:5Mbps, 限制带宽:5Mbps			
class	ftp1-1	ftp1	优先级:0 保证带宽:2Mbps, 限制带宽:4Mbps			
rule	ftp1-rule	ftp1-1	源: any, 目的: 市场部-经理 服务: FTP, 时间: 工作时段内			
class	ftp1-2	ftp1	优先级:0 保证带宽:1Mbps, 限制带宽:3Mbps			
rule	ftp1-2rule	ftp1-2	源: any, 目的: 市场部-员工 服务: FTP, 时间: 工作时段内			
class	ftp1-3	ftp1	优先级:0 保证带宽:2Mbps, 限制带宽:5Mbps			
rule	ftp1-3rule	ftp1-3	源: any, 目的: 市场部-配置 服务: FTP, 时间: 工作时段内			

子类的保证带宽之和不能大于父类的保证带宽。

Dev	eth0					
class	ftp1	eth0	优先级:0 保证带宽:5Mbps, 限制带宽:5Mbps			
class	ftp1-1	ftp1	优先级:0 保证带宽:2Mbps, 限制带宽:4Mbps			
rule	ftp1-rule	ftp1-1	源: any, 目的: 市场部-经理 服务: FTP, 时间: 工作时段内			
class	ftp1-2	ftp1	优先级:0 保证带宽:1Mbps, 限制带宽:3Mbps			
rule	ftp1-2rule	ftp1-2	源: any, 目的: 市场部-员工 服务: FTP, 时间: 工作时段内			
class	ftp1-3	ftp1	优先级:0 保证带宽:2Mbps, 限制带宽:5Mbps			
rule	ftp1-3rule	ftp1-3	源: any, 目的: 市场部-配置 服务: FTP, 时间: 工作时段内			

上图中，市场部-经理使用 FTP 进行下载的最大速率不会超过 4Mbps。

#	Item Name	Addr...	<->	Size	Progress	Local	Speed	Elapsed
F	✓ Norton Anti...	192....	←	294.73 ...	100%	F:\Norto...	30.18 mbs	0:01:18

3) 验证

上图是 10.10.10.2（属于市场部-经理地址段）通过 cuteftp 下载一个文件时的截图，可以看到下载速度是 30.18mbs，此处显示的速率是兆比特/秒，换算成兆字节/秒后的值为 3.7725（一字节等于八比特），小于市场部-经理的限制带宽（4M），大于其保证带宽（2M）。说明该子类在其他子类（如 ftp1-2 或 ftp1-3）没有 FTP 流量的前提下，“借用”了它们的带宽。

至此，FTP 带宽控制策略配置完成。

注意事项

- 1) 防火墙带宽单位是字节/秒，防火墙的带宽单位 bps 指的是字节/秒，不是通常的比

特/秒。

- 2) 防火墙的带宽管理指的是出口带宽只能对防火墙转发的流量作限制。
- 3) 防火墙的带宽管理具有与接口无关性指物理接口，不关心路由、交换等工作模式。
- 4) 注意打开相关协议的端口绑定

对于有子连接的协议，需要在 **内容过滤 > 应用端口绑定** 中打开端口绑定，如 **FTP** 等,否则不能对该协议进行带宽管理。

模块列表

SIP支持服务：

启动

停止

应用协议端口绑定

[添加][重置][清空]

应用协议类型	协议	端口	目的子网	子网掩码	启用	修改	删除
ftp	tcp	21	0.0.0.0	0.0.0.0	yes		
smtp	tcp	25	0.0.0.0	0.0.0.0	yes		
tftp	udp	69	0.0.0.0	0.0.0.0	yes		
http	tcp	80	0.0.0.0	0.0.0.0	yes		
pop3	tcp	110	0.0.0.0	0.0.0.0	yes		
sqlnet	tcp	1521	0.0.0.0	0.0.0.0	yes		
telnet	tcp	23	0.0.0.0	0.0.0.0	yes		

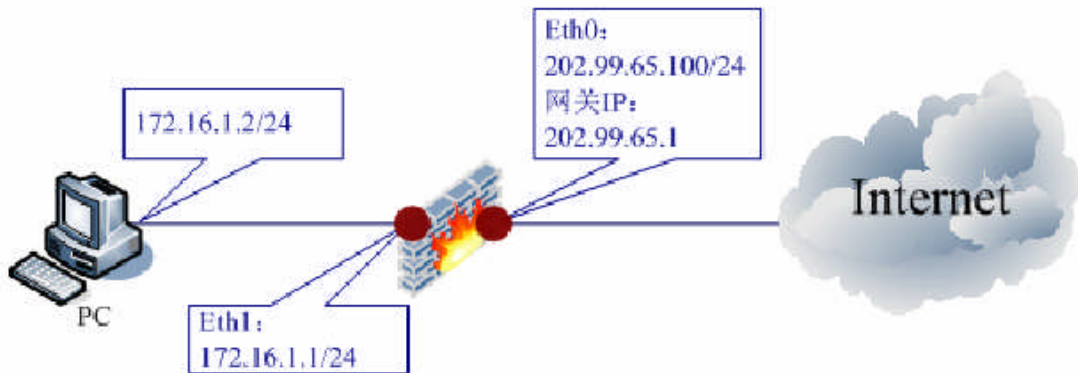
对于上述协议如果使用了非标准端口，需要添加自定义服务，并进行绑定。

应用程序识别

一、应用程序过滤（以 QQ 举例）

基本需求

禁止内网用户（172.16.1.2/24）通过防火墙登录 QQ 服务器。



图例 应用层访问过滤示意图

本例中网络卫士防火墙的 Eth0 连接外网，其 IP 地址为 202.99.65.100/24，网关地址为 202.99.65.1；Eth1 连接内网 172.16.1.0/24，其 IP 地址为 172.16.1.1；内网主机 172.16.1.2 通过 Eth0 访问外网。

配置要点

- 1、配置内容过滤的应用程序识别策略（用于禁止 QQ 登录）
- 2、配置被禁止登录 QQ 服务器的主机地址对象
- 3、配置访问控制规则并启用禁止 QQ 登录的应用程序识别策略

WebUI 配置步骤

- 1) 配置内容过滤的应用程序识别策略（用于禁止 QQ 登录）

选择 内容过滤 > 应用程序识别

The screenshot shows the WebUI configuration interface for application identification. The left sidebar contains a navigation menu with the following items: 系统管理, 网络管理, 资源管理, 用户认证, 防火墙, 内容过滤 (selected), PKT管理, 虚拟专网, 入侵防御, 病毒防御, 高可用性, 日志与报警, and 退出系统. The '内容过滤' section is expanded, showing '过滤对象', '应用端口绑定', '过滤策略', and '应用程序识别' (selected). The main area displays the configuration for '应用程序识别'. It includes a table with the following data:

名称	策略内容	修改	删除
forbid_qq	协议:qq 处理动作:拒绝		

Below the table, there is a section for '协议扩展' (Protocol Expansion) with a '选择文件:' label and a '浏览...' button. There is also an '上传' button and a link '[增加其它协议支持]'. At the bottom, there is a table showing the version of the protocols:

协议	版本
BT	0.0.3
edonkey	0.0.1
msn	0.0.1
qq	0.0.1
skype	0.0.1

- 2) 配置被禁止登录 QQ 服务器的主机地址对象
选择 资源管理 > 地址，然后激活“主机”页签



- 3) 配置访问控制规则
选择 防火墙 > 访问控制，添加一条访问控制规则。



配置完成。

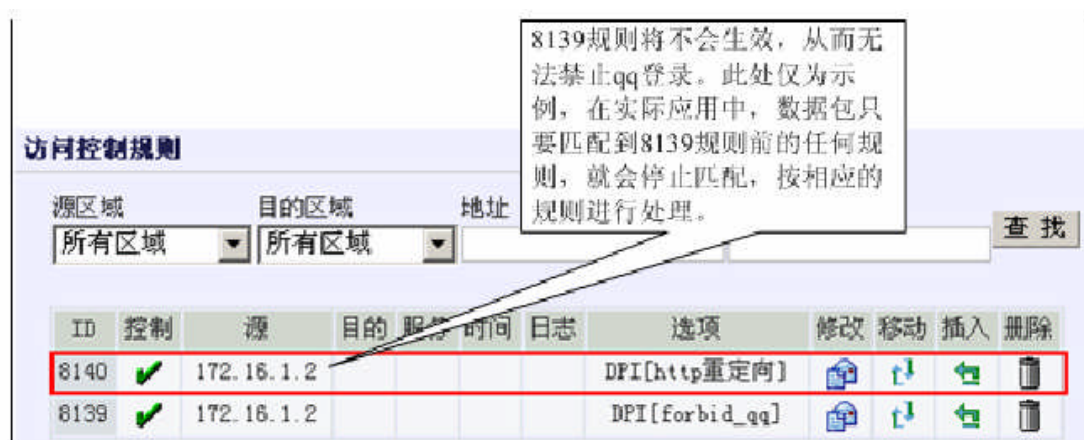
- 4) 验证

使用内网主机（172.16.1.2/24）登录 QQ 服务器，QQ 客户端登录失败。

注意事项

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。如下图所示。

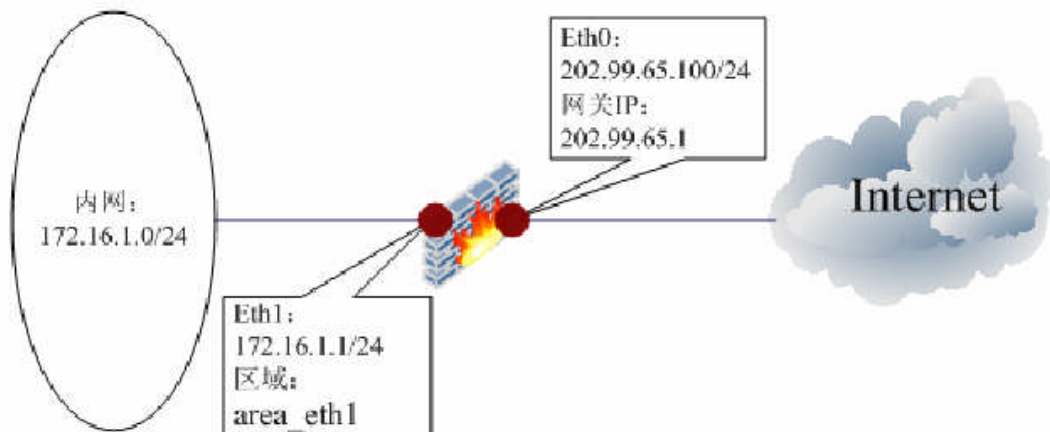


所以，启用应用程序识别策略的访问控制规则应尽可能的精确、前置。

二、应用程序限制（BT 流量的带宽限制为例）

基本需求

限制内网 172.16.1.0/24 的用户在上班时间（09:01—17:30）不能使用 BT 登录，可以在下班时间使用，但是上传带宽和下载带宽均不能超过 100KBps。



图例 应用层访问过滤示意图

本例中网络卫士防火墙的 Eth0 连接外网，其 IP 地址为 202.99.65.100/24，网关地址为 202.99.65.1；Eth1 连接内网 172.16.1.0/24，其 IP 地址为 172.16.1.1；内网 172.16.1.0/24 的用户通过 Eth0 访问外网。

配置要点

- 1、配置时间对象（工作时段内）
- 2、配置上传 QoS 和下载 QoS
- 3、配置两条内容过滤的应用程序识别策略（用于禁止使用 BT、限制 BT 流量）
- 4、配置被限制或禁止 BT 流量的子网对象
- 5、配置两条访问控制规则并分别启用禁止、限制 BT 流量的应用程序识别策略（工作时段外/工作时段内）

WebUI 配置步骤

- 1) 配置时间对象（工作时段内）

选择 资源管理 > 时间，然后激活“时间多次”页签，添加时间对象

系统管理

网络管理

资源管理

地址

属性

区域

时间

服务

时间多次 | 时间单次

时间多次循环 [添加][清空]

名称	星期	每日开始	每日结束	修改	删除
工作时段内	12345	09:01	17:30		

2) 配置上传 QoS 和下载 QoS

选择 网络管理 > 流量管理，然后激活“带宽控制”页签，添加上传 QoS (up_bt) 和下载 QoS (down_bt)

带宽控制 | 流量统计

带宽管理 [添加接口]

类型	名称	上级	属性	下级	修改	删除
Dev	eth0					
class	class1	eth0	优先级:0 保证带宽:100KBps, 限制带宽:100KBps			
dyn-rule	up_bt	class1	优先级:0 时间:任意			
Dev	eth1					
class	class2	eth1	优先级:0 保证带宽:100KBps, 限制带宽:100KBps			
dyn-rule	down_bt	class2	优先级:0 时间:任意			

3) 配置内容过滤的应用程序识别策略（用于禁止使用 BT、限制 BT 流量）

选择 内容过滤 > 应用程序识别，添加两个应用程序识别策略

应用程序识别 [添加] [清空]

名称	策略内容	修改	删除
forbid_bt	协议:BT 处理动作:拒绝		
limit_bt	协议:BT 处理动作:带宽控制 下载Qos:down_bt 上传Qos:up_bt		

协议扩展

选择文件: 浏览...

上传 [增加其它协议支持]

4) 配置被限制或禁止 BT 流量的子网对象

选择 资源管理 > 地址，然后激活“子网”页签

主机 | 范围 | 子网 | 地址组

子网 [添加] [清空]

名称	IP地址	掩码地址	除去地址	并发连接数	修改	删除
subnet_bt	172.16.1.0	255.255.255.0				

5) 配置访问控制规则

选择 防火墙 > 访问控制，添加两条访问控制规则。



配置完成。

6) 验证

在内网主机（172.16.1.2/24）上使用 BT 客户端软件进行下载，工作时间内（09:00-17:30）无法进行 BT 软件下载；工作时间外（00:00-09:00，17:30-23:59）可以进行 BT 软件下载，但是最大上传/下载带宽均不能超过 100KBps。

注意事项

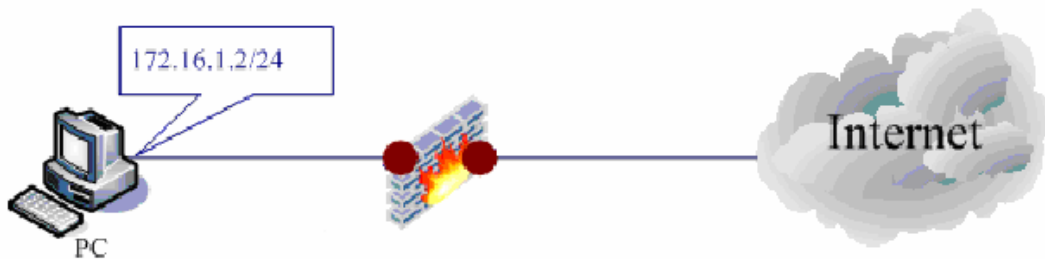
注意访问控制规则的顺序匹配

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。

并发连接数限制

基本需求

设置内网用户（172.16.1.2/24）与公网的连接数为 50



图例

本例中网络卫士防火墙的 Eth0 连接外网，其 IP 地址为 202.99.65.100/24，网关地址为 202.99.65.1；Eth1 连接内网 172.16.1.0/24，其 IP 地址为 172.16.1.1；内网主机 172.16.1.2 通过 Eth0 访问外网。

配置要点

- 1、配置需要做限制的地址对象
- 2、配置限制对象的连接数

WebUI 配置步骤

- 1) 配置需要做限制的地址对象

选择 资源管理 > 时间，在主机页签中添加地址对象

The screenshot shows the '主机属性' (Host Properties) dialog box in the WebUI. It has two input fields: '名称:' (Name) with the value '172.16.1.2' and a red asterisk, and 'IP地址:' (IP Address) with a dropdown menu showing '172.16.1.2'. To the right of the dropdown are '<' and 'x' buttons, followed by another input field containing '172.16.1.2'. At the bottom are '确定' (OK) and '取消' (Cancel) buttons.

- 2) 配置限制对象的连接数

选择 入侵防御 > 主机防护，在 172.16.1.2 这个对象中点击修改，设置连接数 50，确定

防护主机属性

地址: 172.16.1.2 [主机] ▼

SYN代理: 否 ▼

并发连接数: 50

并发半连接数: 0

确 定**取 消**

配置完成

VPN 配置

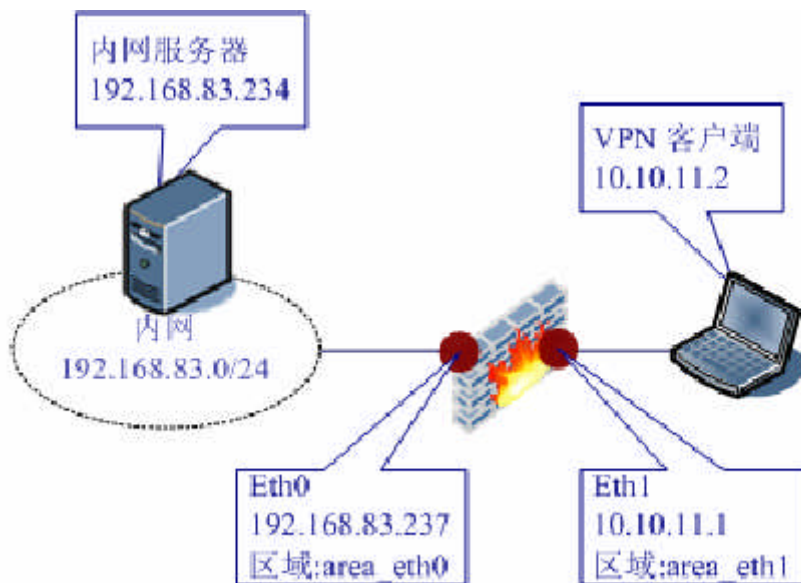
天融信 IPSec VPN 支持标准的 IKE 和 IPSec 协议，也就是说，该 IPSec VPN 不可以和天融信的 IPSec VPN 建立隧道，也可与其他支持 IKE 标准协议的 VPN 设备协商并建立标准的 IPSec VPN 隧道。安装天融信 IPSEC VPN 引擎的网络卫士防火墙，具备一切 VPN 网关的功能，可作为一台标准的 VPN 网关使用。同时，移动远程用户（VRC，VPN RomoteClient）可以通过 VPN 远程客户端与网络卫士防火墙建立 VPN 隧道。

一、远程用户本地认证（点到端模式）

远程用户经过网络卫士防火墙认证以后与防火墙建立 VPN 隧道连接。

基本需求

移动用户经防火墙本地证书认证后通过 VPN 隧道访问内网资源（192.168.83.234）用户lisi 采用用户名+口令的认证方式



图例 远程用户本地认证示意图

配置要点

- 1、配置防火墙开放服务
- 2、配置 VRC 功能
- 3、配置 VRC 客户端
- 4、验证

WebUI 配置步骤

- 1) 开放 Eth1 口的 IPSecVPN 服务，绑定虚接口。
设置 Eth0、Eth1 所属区域，缺省访问权限为“允许”。
资源管理 > 区域

+

系统管理

+

网络管理

+

资源管理

+

地址

+

属性

+

区域

+

时间

+

服务

+

用户认证

区域

[添加] [清空]

名称	绑定属性(可多选)	权限	注释	修改	删除
area_eth0	eth0	允许			
area_eth1	eth1	允许			
area_eth2	eth2	允许			
area_eth3	eth3	允许			

开放 Eth1 口相关服务

系统管理 > 配置，然后激活“开放服务”页签

+

系统管理

+

网络管理

+

资源管理

+

用户认证

+

防火墙

+

内容过滤

+

PKI管理

+

虚拟专网

+

入侵防御

+

病毒防御

+

高可用性

+

日志与报警

+

退出系统

系统参数 | 开放服务 | 时间

监控服务:

启动

停止

SSH服务:

启动

停止

TELNET服务:

启动

停止

HTTP服务:

启动

停止

NTP服务:

启动

停止

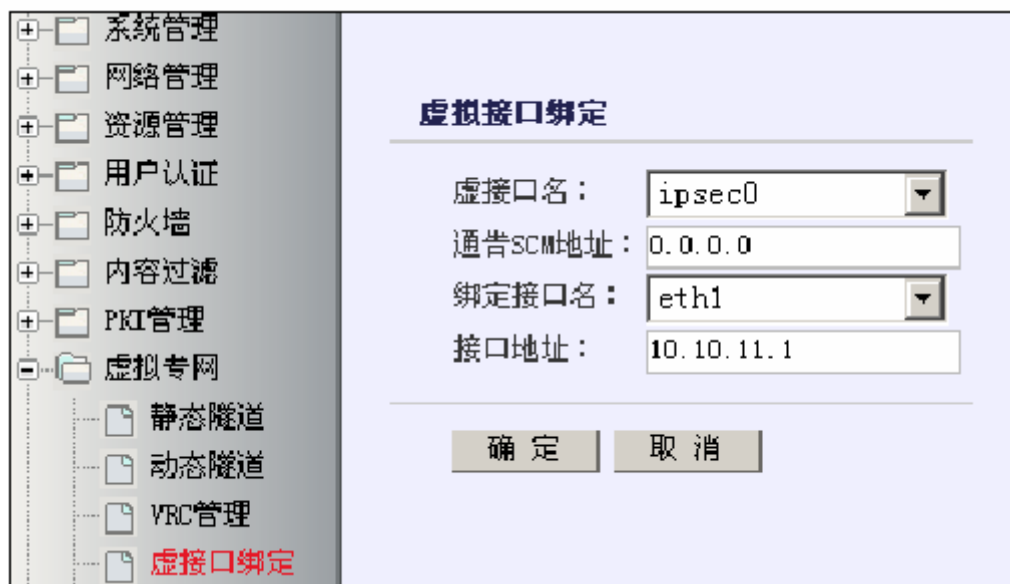
开放服务

[添加]

服务名称	控制区域	控制地址	修改	删除
webui	area_eth0	any		
ssh	area_eth0	any		
telnet	area_eth0	any		
auth	area_eth1	any		
ssh	area_eth1	any		
webui	area_eth1	any		
auth	area_eth0	any		
gui	area_eth0	any		
gui	area_eth1	any		
ipsecvpn	area_eth1	any		

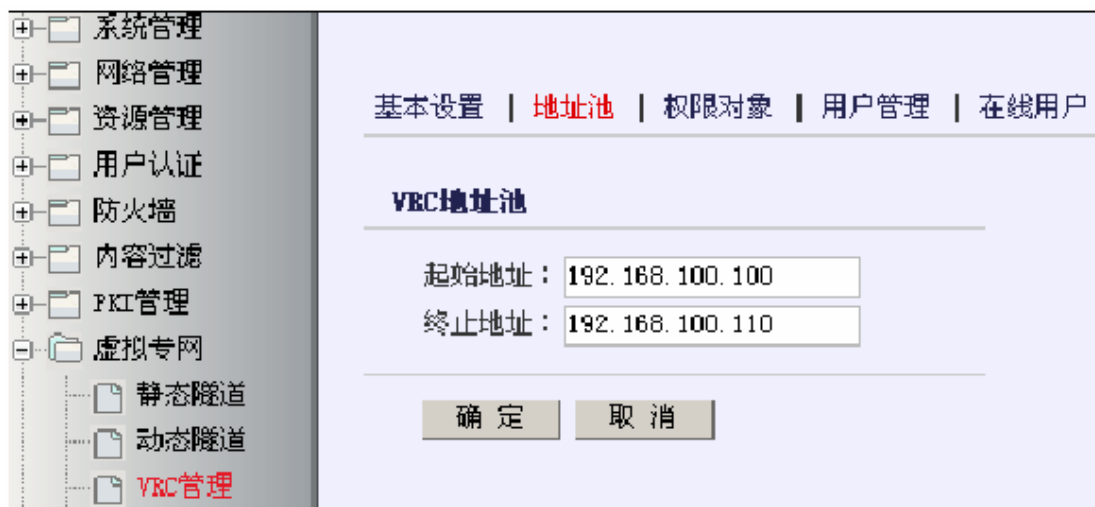
绑定虚接口为 Eth1

虚拟专网 > 虚接口绑定，点击“添加”。



2) 配置 VRC 功能

a) 选择 虚拟专网 > VRC 管理，然后激活“地址池”页签，设置为 VRC 用户分配的地址池，需要注意的是，地址池的选择一定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。



b) 设置 VRC 用户的默认权限，选择 虚拟专网 > VRC 管理，然后激活“权限对象”页签，如图所示。

+

系统管理

+

网络管理

+

资源管理

+

用户认证

+

防火墙

+

内容过滤

+

PKI管理

+

虚拟专网

+

静态隧道

+

动态隧道

+

VRC管理

+

虚接口绑定

基本设置 | 地址池 | 权限对象 | 用户管理 | 在线用户

权限对象

[添加]

名称	控制(a/d)	协议	目的端口范围	IP	掩码	修改	删除
234	允许	all	所有端口	192.168.83.234	255.255.255.255		

默认权限

[添加]

名称	上移	下移	删除
234			

默认权限可以添加一个或多个权限对象。

c) 选择 虚拟专网 > VRC 管理，然后激活“用户管理”页签，设置 VRC 用户。

基本设置 | 地址池 | 权限对象 | 用户管理 | 在线用户

添加本机用户

用户名: [只能输入字母、数字、'-'、'_'、'.'和'@']

用户状态:

需要证书认证:

需要密码认证:

密码: [最长32个字符]

用户权限控制:

硬件特征码绑定控制:

硬件特征码: [32个16进制数]

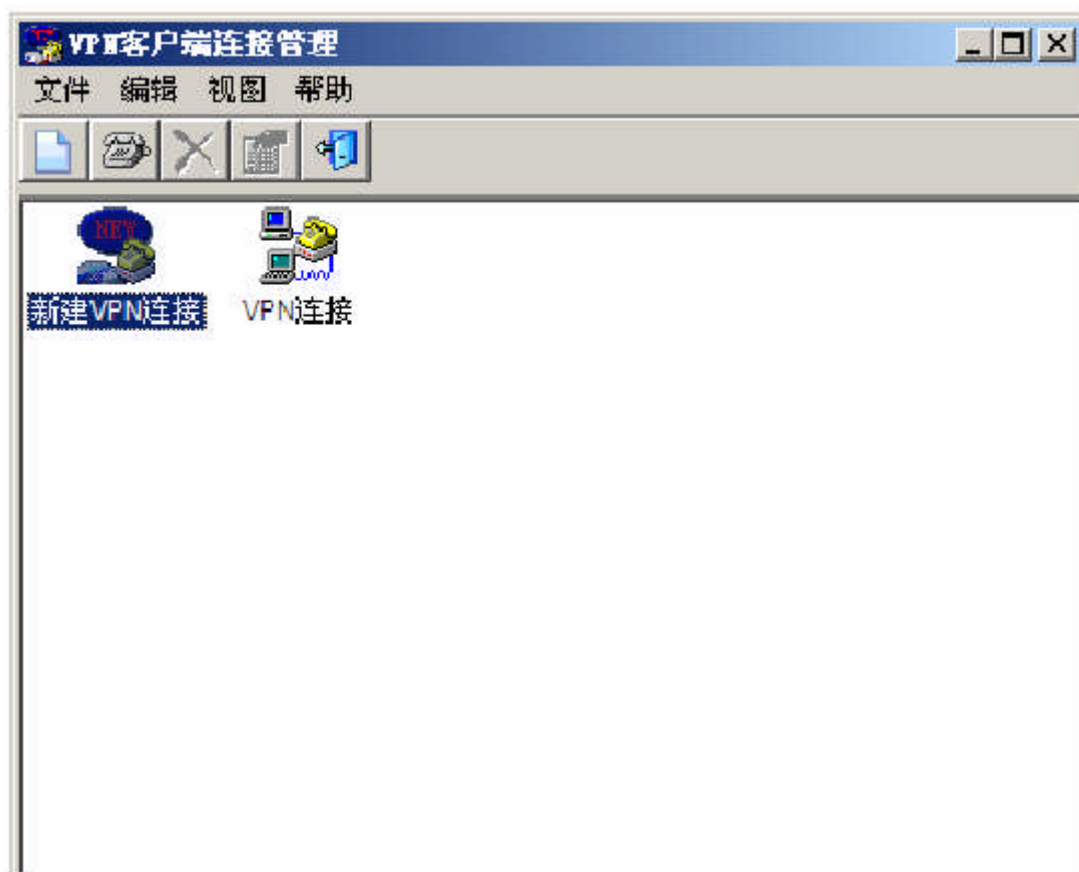
指定虚IP: ☐

确定

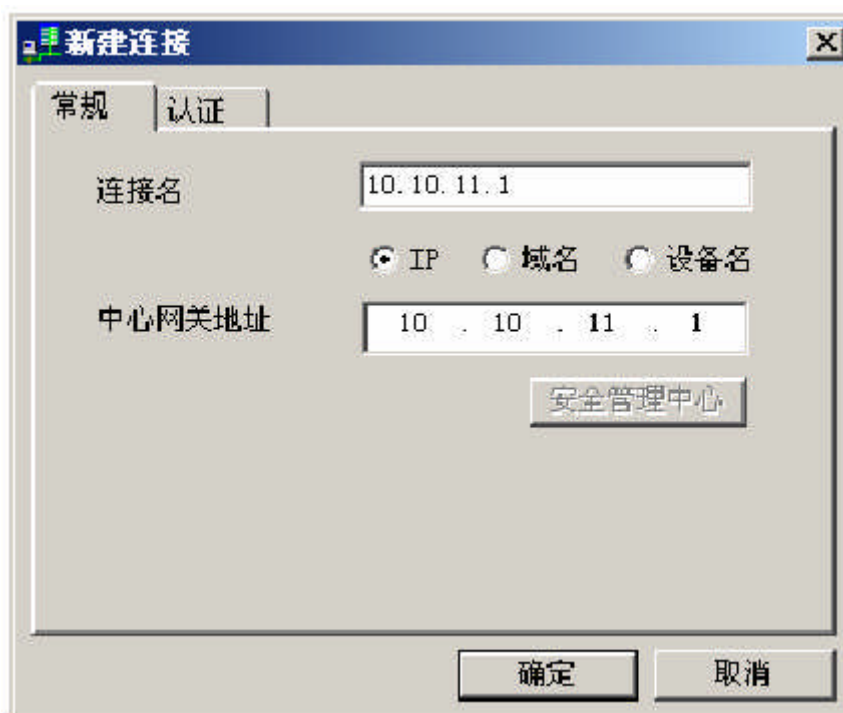
取消

3) 在远程 VRC 客户机器上安装并配置 VRC 远程客户端，客户端主机上会添加一 IPSec VPN 虚拟网卡。

打开 VPN 客户端，点击“新建 VPN 连接”。

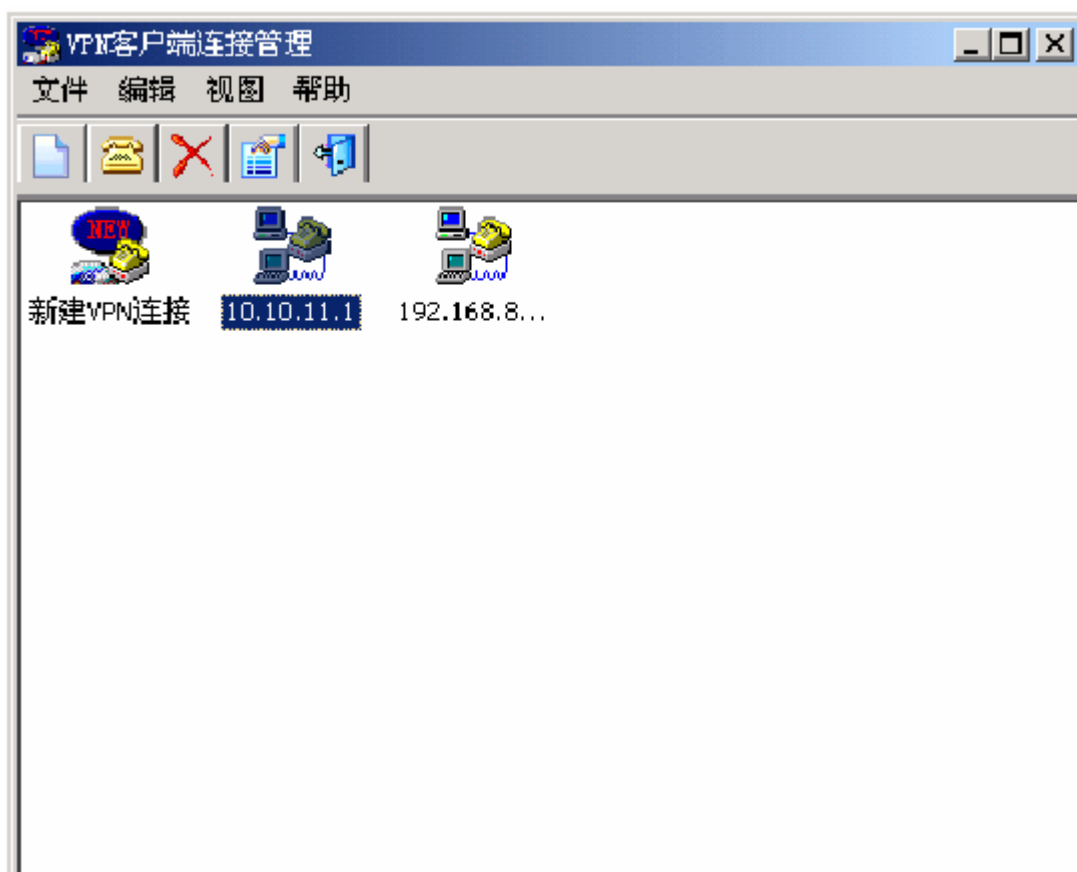


网关地址设为防火墙 Eth0 接口的地址（10.10.11.1），连接使用 IP。



4) 验证

a) 启动 VPN 客户端



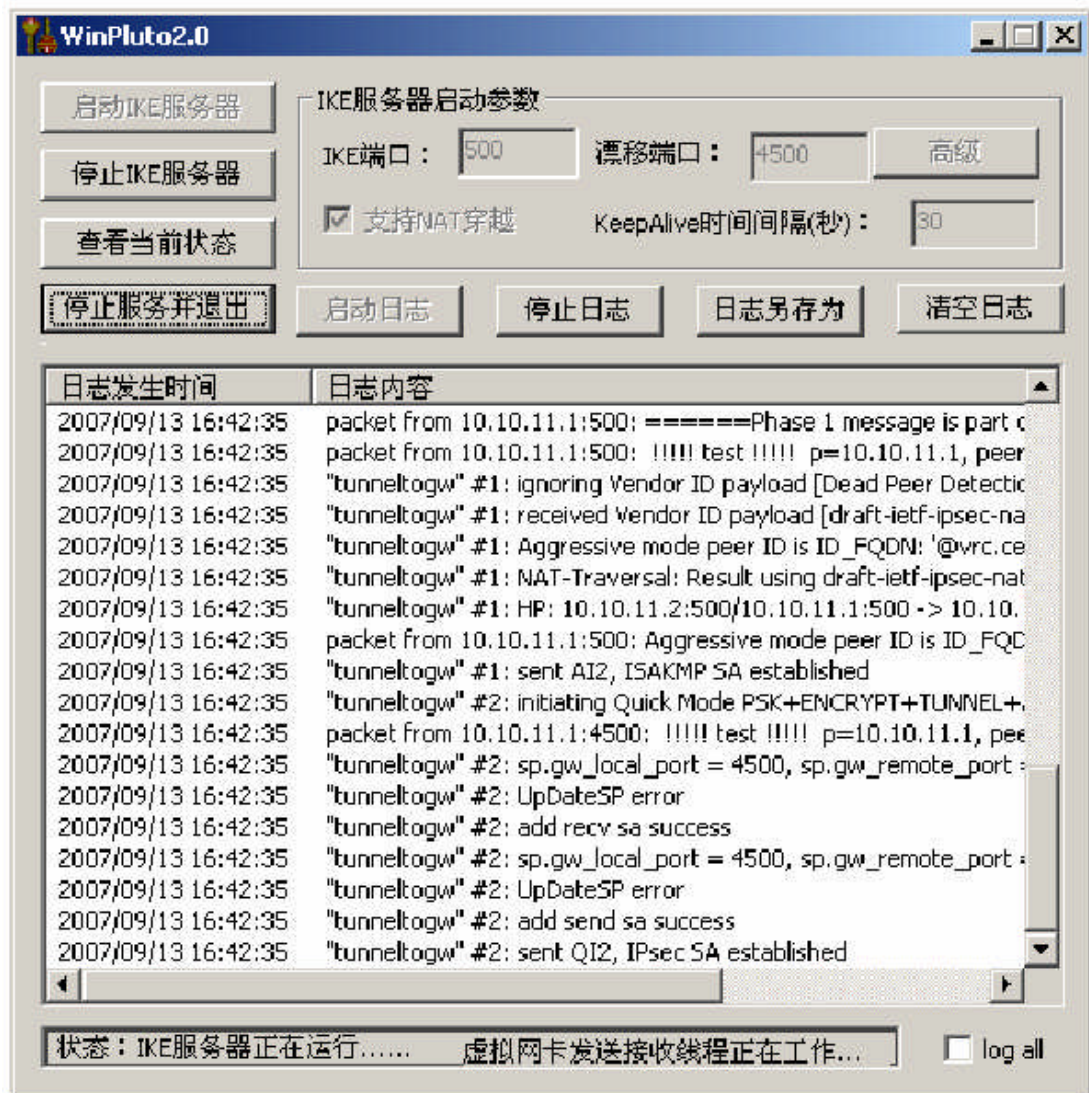
在鼠标右键菜单点击连接，在下图中输入 VRC 用户名和口令，点击“连接”。



如果连接成功则界面如下图所示。



在“VPN 客户端属性”界面中选中“显示 IKE 协商进程”前的复选框，则客户端弹出如下窗口。可以查看隧道是否协商成功。



b) 用 ipconfig /all 命令查看本地 IP 配置。

```
Ethernet adapter 本地连接 25:

Connection-specific DNS Suffix . : 
Description . . . . . : OCS UPeN Adapter
Physical Address. . . . . : 08-00-58-00-00-05
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.100.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
DHCP Server . . . . . : 192.168.100.1
Lease Obtained. . . . . : 2007年9月13日 16:42:29
Lease Expires . . . . . : 2007年9月13日 18:24:53
```

c) 选择 网络管理 > 路由，然后激活“静态路由”页签，查看防火墙上的路由信息。



注意事项

1) VRC 用户必须访问启用了 IPSEC 功能的接口 IP。

防火墙的默认路由的相关接口是 IPSEC 口，本例中，为 Eth0 口（10.10.11.1/24）。对于 TOS 来说不是所有的网口的所有 IP 都能参与 VPN 通信，必须由管理员指定 VPN 通信使用的接口及 IP，即虚接口。防火墙的一个接口可能有多个 IP 地址，默认路由中的网关只能是虚接口 IP 地址同网段的 IP。

2) VRC 客户端与 VPN 网关 VPN 参数设置。

VRC 客户端与防火墙的协商模式加密算法等无须用户设置。

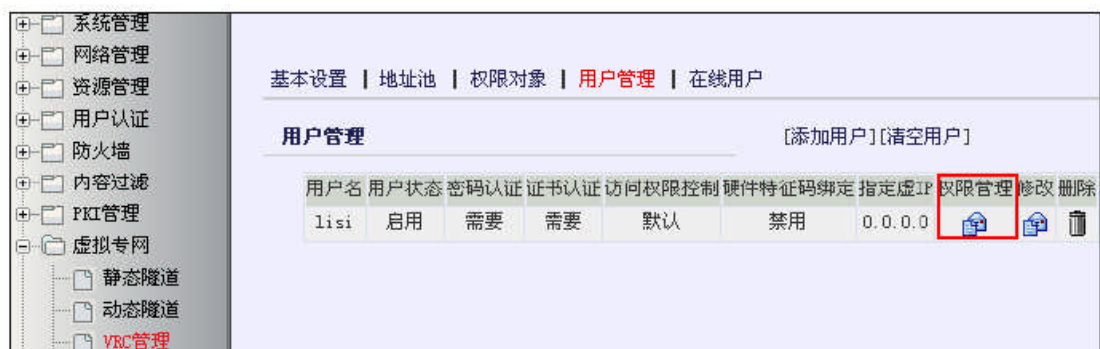
3) 本地认证的 VRC 用户权限分配。

本地认证的 VRC 用户权限比较灵活，对于每个 VRC 用户，既可以使用默认权限，也可以使用自定义权限。

默认权限的设置：虚拟专网 > VRC 管理，然后激活“权限对象”页签。



自定义权限的设置：虚拟专网 > VRC 管理，然后激活“用户管理”页签。



如果指定使用了默认权限，上图中设置的权限将无效。

4) 限制 VRC 用户从特定机器使用 VPN 功能。

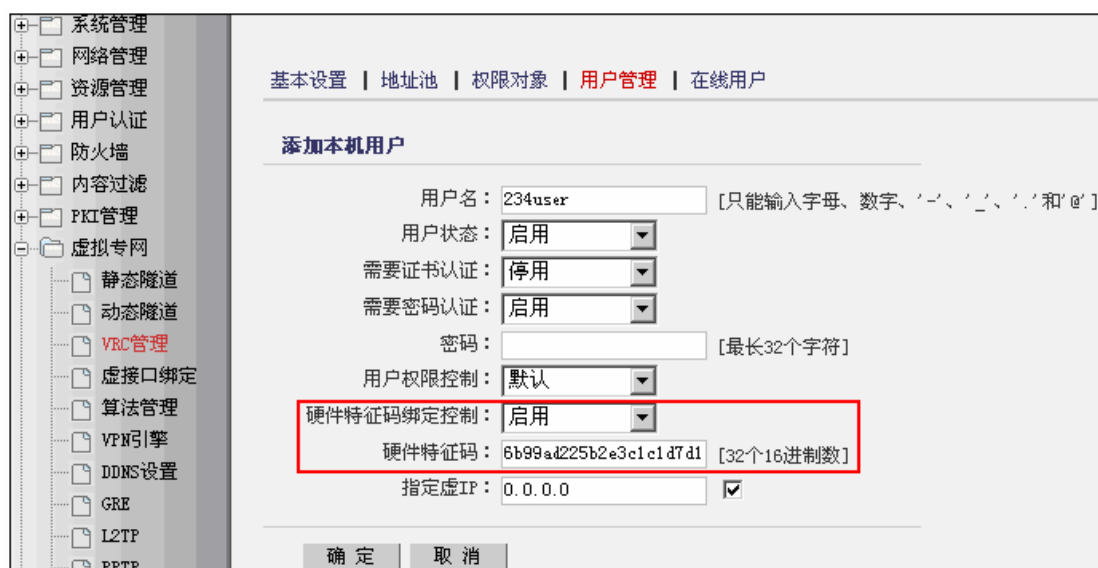
特征码是按照特定计算机硬件计算出来的特征值，不同计算机特征码不同。防火墙可以根据客户端提供的特征码将用户名和特定机器绑定在一起，减少内网资源被非授权访问的风险。

a) 获取客户端特征码。



b) 在防火墙上设置特征码绑定。

虚拟专网 > VRC 管理，然后激活“用户管理”页签



5) 如需要绑定用户和虚 IP，可以进行如下设置。

虚拟专网 > VRC 管理，然后激活“用户管理”页签

系统管理

网络管理

资源管理

用户认证

防火墙

内容过滤

PKI管理

虚拟专网

静态隧道

动态隧道

VRC管理

虚接口绑定

算法管理

VPN引擎

DDNS设置

GRE

L2TP

PPTP

基本设置 | 地址池 | 权限对象 | 用户管理 | 在线用户

添加本机用户

用户名: lisi [只能输入字母、数字、'-'、'_'、'.'和'@']

用户状态: 启用

需要证书认证: 启用

需要密码认证: 启用

密码: [最长32个字符]

用户权限控制: 默认

硬件特征码绑定控制: 停用

硬件特征码: 00000000000000000000 [32个16进制数]

指定虚IP: 192.168.100.25 ☒

确定 取消

二、VPN 隧道（端到端模式）

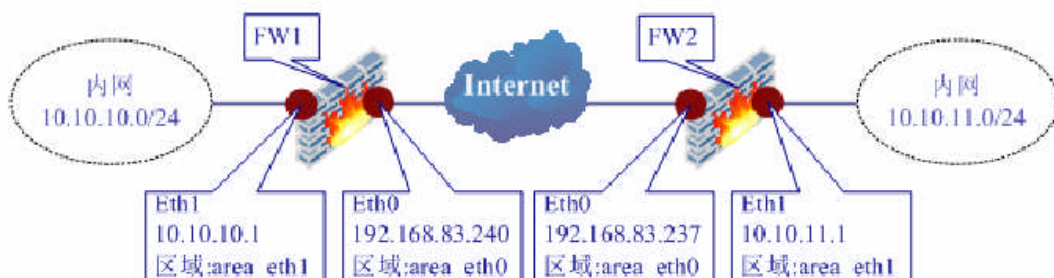
基本需求

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。

FW1 的 Eth0 口和 FW2 的 Eth0 口参与 VPN 隧道的协商和建立

FW1 保护子网 10.10.10.0/24

FW2 保护子网 10.10.11.0/24



图例 VPN 静态隧道构建示意图

配置要点

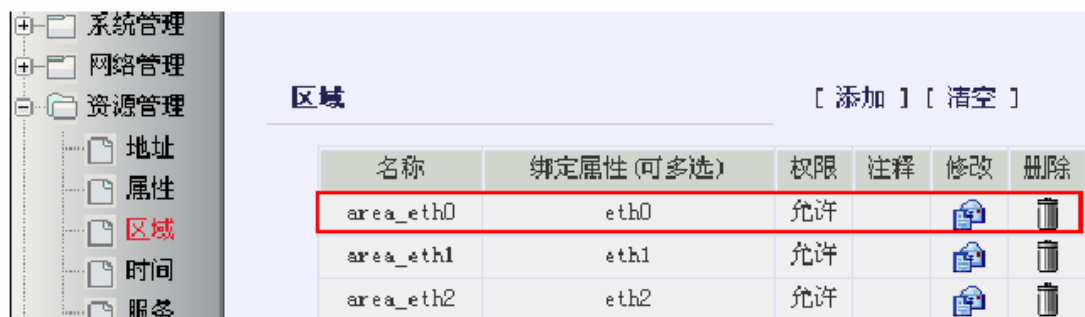
- 1、配置防火墙开放服务
- 2、配置防火墙 VPN 功能

WebUI 配置步骤

1) 开放 FW1 的 Eth0 口的 IPSecVPN 服务，绑定虚接口。

设置 Eth0 所属区域

资源管理 > 区域



名称	绑定属性 (可多选)	权限	注释	修改	删除
area_eth0	eth0	允许			
area_eth1	eth1	允许			
area_eth2	eth2	允许			

开放 Eth0 口相关服务

系统管理 > 配置，然后激活“开放服务”页签



系统参数 | **开放服务** | 时间

监控服务：

SSH服务：

TELNET服务：

HTTP服务：

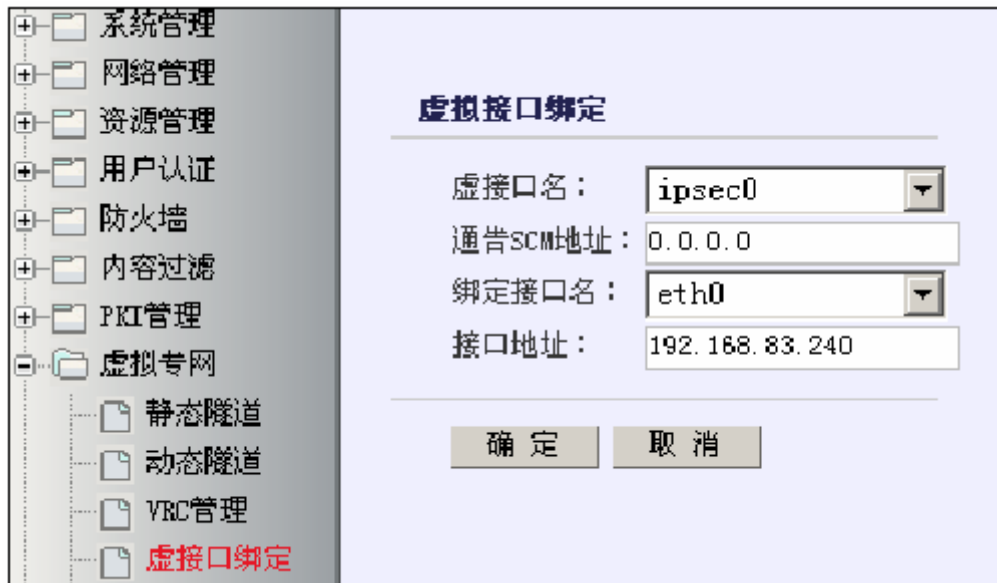
NTP服务：

开放服务 [添加]

服务名称	控制区域	控制地址	修改	删除
gui	area_eth0	any		
ssh	area_eth0	any		
ping	area_eth0	any		
webui	area_eth0	any		
telnet	area_eth0	any		
gui	area_eth1	any		
auth	area_eth0	any		
update	area_eth0	any		
ipsecvpn	area_eth0	any		

绑定虚接口为 Eth0

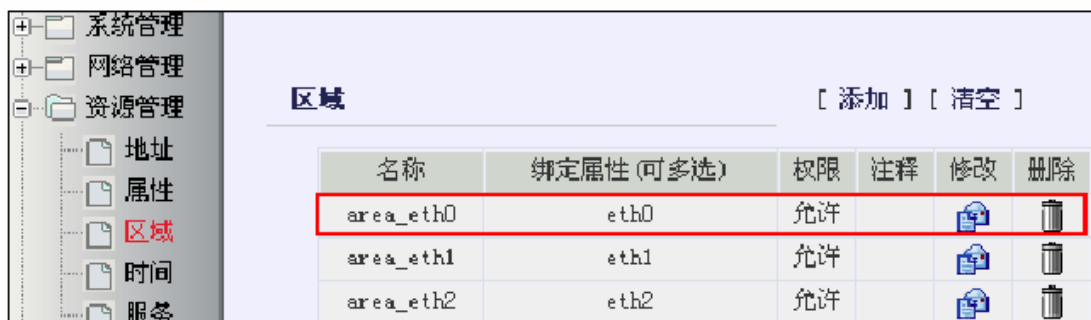
虚拟专网 > 虚接口绑定，点击“添加”。



2) 开放 FW2 的 Eth1 口的 IPsecVPN 服务，绑定虚接口。

设置 Eth0 所属区域

资源管理 > 区域



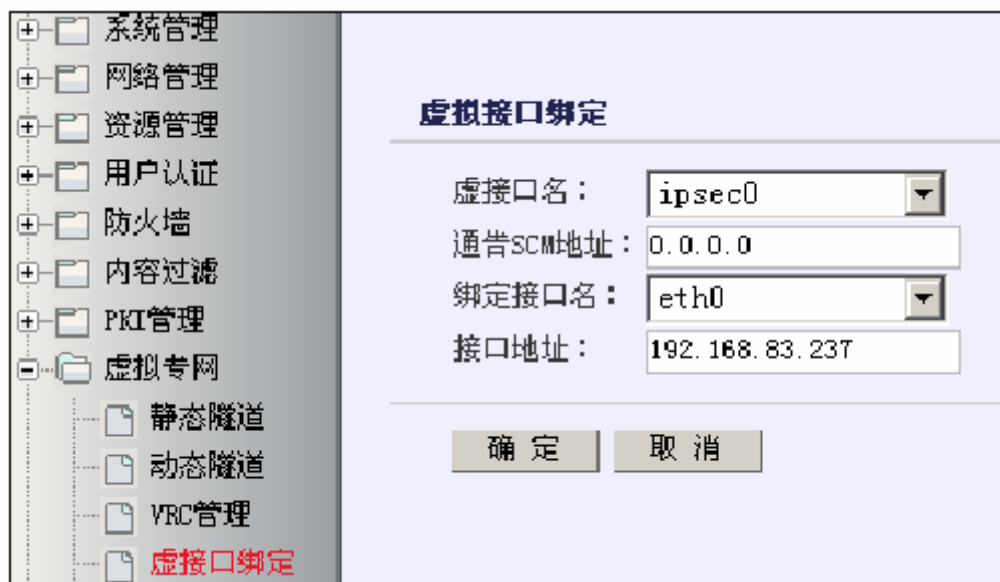
开放 Eth0 口相关服务

系统管理 > 配置，然后激活“开放服务”页签



绑定虚接口为 Eth0

虚拟专网 > 虚接口绑定，点击“添加”。



3) 设置 FW1 的 VPN 功能

虚拟专网 > 静态隧道，点击“添加隧道”。

点击“第一阶段协商”页签，然后设置第一阶段协商参数，如下图所示。

隧道设置

第一阶段协商 | **第二阶段协商**

隧道名: 240-237 * [只能输入字母、数字、'-'和'_']

认证方式: 预共享密钥

预共享密钥: ●●●●●● *

本地标识: 240@topsec [填写格式: @XXX或者XXI@XX, XXX为字母或者数字]

对方标识: 237@topsec [填写格式: @XXX或者XXX@XX, XXI为字母或者数字]

对方地址或域名: 192.168.83.237 *

☒ 高级配置

隧道描述:

IKE协商模式: 主模式

选择IPSEC隧路: ipsec0

主动发起隧道协商: 是

SA协商重试次数: 3 [范围: 1~100, 缺省: 3]

ISAKMP-SA存活时间: 3600 [单位: s, 最大: 86400, 缺省: 3600]

ISAKMP-SA的安全策略属性: 3des-md5 3DES SHA1

DH1

确定 取消

点击“第二阶段协商”页签，然后设置第二阶段协商参数，如下图所示。

隧道设置

第一阶段协商 | **第二阶段协商**

本地子网: 10.10.10.0

本地掩码: 255.255.255.0

对方子网: 10.10.11.0

对方掩码: 255.255.255.0

☒ 高级配置

IPSEC-SA存活时间: 28800 [单位: s, 最大: 86400, 缺省: 28800]

IPSEC-SA的算法提议列表: 加密算法 3DES 校验算法 MD5

IPSEC-SA的安全策略属性: ☐ pfs ☒ tunnel ☐ compress ☒ encrypt ☐ authenticate

DPD间隔: 10 [单位: s, 范围: 1~3600, 缺省: 30]

DPD超时时间: 300 [单位: s, 范围: 1~28800, 缺省: 300]

DPD失败隧道操作: clear [缺省: clear]

NAT-T的KEEP-ALIVE间隔: 20 [单位: s, 范围: 1~40, 缺省: 20]

metric值: 100

确定 取消

4) 设置 FW2 的 VPN 功能

虚拟专网 > 静态隧道，点击“添加隧道”。

点击“第一阶段协商”页签，然后设置第一阶段协商参数，如下图所示。

隧道设置

第一阶段协商 第二阶段协商

隧道名: 237-240 * [只能输入字母、数字、'-'和'_']

认证方式: 预共享密钥

预共享密钥: ●●●●●● *

本地标识: 237@topsec [填写格式: @XXX或者XIX@XXX, XXX为字母或者数字]

对方标识: 240@topsec [填写格式: @XXX或者XIX@XXX, XXX为字母或者数字]

对方地址或域名: 192.168.83.240 *

☒ 高级配置

隧道描述:

IKE协商模式: 主模式

选择IPSEC策略: ipsec0

主动发起隧道协商: 是

SA协商重试次数: 3 [范围: 1~100, 缺省: 3]

ISAKMP-SA存活时间: 3600 [单位: s, 最大: 86400, 缺省: 3600]

ISAKMP-SA的安全策略属性: 3des-md5 < 3DES - SHA1 -

DH1

确定 取消

点击“第二阶段协商”页签，然后设置第二阶段协商参数，如下图所示。

隧道设置

第一阶段协商 第二阶段协商

本地子网: 10.10.11.0

本地掩码: 255.255.255.0

对方子网: 10.10.10.0

对方掩码: 255.255.255.0

☒ 高级配置

IPSEC-SA存活时间: 28800 [单位: s, 最大: 86400, 缺省: 28800]

IPSEC-SA的算法提议列表: 加密算法 3DES 校验算法 MD5

IPSEC-SA的安全策略属性: ☐ pfs ☒ tunnel ☐ compress ☒ encrypt ☐ authenticate

DPD间隔: 10 [单位: s, 范围: 1~3800, 缺省: 30]

DPD超时时间: 300 [单位: s, 范围: 1~28800, 缺省: 300]

DPD失败隧道操作: clear [缺省: clear]

NAT-T的KEEP-ALIVE间隔: 20 [单位: s, 范围: 1~40, 缺省: 20]

metric值: 100

确定 取消

上述参数配置成功后，隧道会自动协商。



当“状态”显示为“第二阶段协商成功”，表示隧道成功建立，可以使用。

5) 验证

防火墙 FW2 的静态路由表中会添加到 FW1 保护子网（10.10.10.0/24）的路由，如下图所示。



防火墙 FW1 的静态路由表中会添加到 FW2 保护子网（10.10.11.0/24）的路由，如下图所示。

系统管理

网络管理

接口

二层网络

路由

DHCP

SNMP

ADSL

流量管理

域名解析

资源管理

用户认证

静态路由 | 策略路由 | 动态路由OSPF | 动态路由RIP | 多播路由

静态路由表 [添加][清空]

目的	网关	标记	Metric	接口	删除
192.168.83.240/32	0.0.0.0	UL	1	lo	
192.168.83.0/24	0.0.0.0	UC	10	eth0	
192.168.83.0/24	0.0.0.0	UC	100	ipsec0	
10.10.11.0/24	192.168.83.240	UGI	100	ipsec0	
0.0.0.0/0	192.168.83.1	UGS	1	eth0	

防火墙 FW2 保护子网中的主机（10.10.11.2/24）可以访问防火墙 FW1 子网中的主机（10.10.10.22/24）：

```
C:\Documents and Settings\guest001>ping 10.10.10.22

Pinging 10.10.10.22 with 32 bytes of data:

Reply from 10.10.10.22: bytes=32 time<10ms TTL=126
Reply from 10.10.10.22: bytes=32 time<10ms TTL=126
Reply from 10.10.10.22: bytes=32 time<10ms TTL=126
Reply from 10.10.10.22: bytes=32 time<10ms TTL=126
```

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”。