联　想

网御防火墙 Power V

Web 界面在线手册

VERSION P4.0

声明

- 本手册所含内容若有任何改动，恕不另行通知。
- 在法律法规的最大允许范围内，联想网御科技（北京）有限公司除就本手册和产品应负的瑕疵担保责任外，无论明示或默示，不作其它任何担保，包括（但不限于）本手册中推荐使用产品的适用性和安全性、产品的适销性和适合某特定用途的担保。
- 在法律法规的最大允许范围内，联想网御科技（北京）有限公司对于您的使用或不能使用本产品而发生的任何损坏（包括，但不限于直接或间接的个人损害、商业利润的损失、业务中断、商业信息的遗失或任何其它损失），不负任何赔偿责任。
- 本手册含受版权保护的信息，未经联想网御科技（北京）有限公司书面允许不得对本手册的任何部分进行影印、复制或翻译。

联想网御科技（北京）有限公司
中国北京海淀区中关村南大街 6 号中电信息大厦 8 层

章节目录

表目录

第1章 系统配置

本章主要介绍防火墙的系统配置，由以下部分组成：日期时间，系统参数，系统更新，管理配置，联动，报告设置，入侵检测和产品许可证。

1.1 日期时间

防火墙系统时间的准确性是非常重要的。

可以采取两种方式来同步防火墙的系统时钟

1) 与管理主机时间同步
2) 与网络时钟服务器同步（NTP 协议）

与管理主机时间同步

1. 调整管理主机时钟
2. 点击“时间同步”按钮

与时钟服务器时间同步有两种方式

1. 立即同步
2. 周期性自动同步

立即同步

1. 选中“启用时钟服务器”，输入“时钟同步服务器 IP”
2. 点击“立即同步”按钮

周期性自动同步

1. 选中“启用时钟服务器”，输入“时钟同步服务器 IP”
2. 设定同步周期
3. 点击“确定”按钮系统参数

注意事项：

防火墙的很多操作依赖于系统时间，改变系统时间会对这些操作发生影响，比如更改时间后配置管理界面登录超时等。

1.2 系统参数

在“系统配置>>系统参数”中配置。

系统参数设置防火墙名称和动态域名注册所使用的用户名、密码。

防火墙名称的最大长度是 20 个 ASCII 字符，不能有空格。默认的防火墙名称是 themis，用户可以自己修改这个名称。

动态域名注册所使用的用户名、密码的最大长度是 31 个 ASCII 字符，不能有空格。动态域名的设置在网络配置>>网络设备的物理设备、冗余设备和拨号设备的配置中。

1.3 系统更新

1.3.1 模块升级

防火墙系统升级功能可以快速响应安全需求，保证防火墙功能与安全的快速升级。
模块升级界面包括以下功能

1. 模块升级
2. 导出升级历史
3. 检查最新升级包
4. 重启安全网关

模块升级

1. 点击“浏览”按钮，选择管理主机上的升级包
2. 点击“升级”按钮

点击“重启安全网关”按钮，重启安全网关完成升级

导出升级历史

点击“导出升级历史”按钮，导出升级历史做备份。

检查最新升级包

管理员可以查看”系统当前软件版本”，点击”检查最新升级包”，系统会弹出新的 IE 窗口并连接联想网御安全服务网站（防火墙可以连接 Internet）。

重启安全网关

点击“重启安全网关”按钮，安全网关将重新启动。

注意：重启安全网关前，记住要保存当前配置。“保存”快捷键： 

1.3.2 导入导出

导入导出界面包含以下功能

1. 导出系统配置
2. 导入系统配置
3. 恢复出厂配置
4. 保存配置
5. 查看当前配置

导出配置

点击“导出配置”按钮，导出最后一次保存的所有系统配置到管理主机，管理员的用户名和密码将不会被导出。选中“导出成加密格式”，则加密配置文件。

导入配置

点击“浏览”按钮，在管理主机上选择要导入的配置文件，点击“导入配置”按钮，导入配置文件，系统提示导入成功，重启防火墙，导入的配置生效。注意：导出的配置文件带有防火墙软硬件版本的信息，不能导入到别的版本防火墙中，而且如果同样的配置文件被导入到不同防火墙中，且这些防火墙位于同一网络时，可能会引起配置冲突，如 IP 地址，MAC 地址等。

注意：导入后，**ipsecvpn** 客户端隧道配置中网关地址 需要重新修改连接端口为 **ipsec0**。另外 **ipsecvpn** 模块由于不同版本差异比较大，推荐导入后重新配置一下，否则可能不可用。

恢复出厂配置

点击“恢复出厂配置”按钮，防火墙所有配置丢失，恢复到出厂配置，重启防火墙后生效。

保存配置

点击“保存配置”，保存所有系统配置。也可以按上方保存快捷图标来保存。

查看当前配置

点击“查看当前配置”，可以下载当前配置的页面，该页面以表格的形式显示配置，并可以用来进行打印。

1.4 管理配置

1.4.1 管理主机

管理员只有在管理主机上才能对防火墙进行管理，最多支持 6 个管理主机 IP 和 1 个集中管理主机，至少有 1 个管理主机 IP 不能被删除。

此“系统配置>>管理配置>>管理主机”界面完成以下功能

1. 添加管理主机
2. 删除管理主机
3. 转到“系统配置>>报告设置>>集中管理”界面

添加管理主机

1. 输入管理主机 IP 和子网掩码
2. 在“说明”中，输入描述性文字，此步骤可忽略
3. 点击“确定”按钮完成添加

修改管理主机

1. 从“管理主机 IP”列表中修改要修改的管理主机 IP 或子网掩码
2. 点击“确定”按钮完成修改

删除管理主机

1. 从“管理主机 IP”列表中删除要删除的管理主机 IP
2. 点击“确定”按钮完成删除

转到“系统配置>>报告设置>>集中管理”界面

1. 点击“集中管理主机”链接，可以跳转到“系统配置>>报告设置>>集中管理”页面，进行集中管理设置。

1.4.2 管理员账号

管理员按级别授权管理，说明如下：

表 1-1 管理员级别与授权

管理员级别	授权	备注
超级管理员	增加、删除管理员帐号，不能直接配置管理。	默认管理员帐号与密码为 administrator：administrator。 帐号 administrator 不能删除。
配置管理员	配置系统策略、网络配置、在线帮助。	无默认帐号
策略管理员	配置安全策略、资源定义、在线帮助。	无默认帐号
审计管理员	查看防火墙日志信息、在线帮助。	无默认帐号

默认只能有一个管理员登录防火墙进行配置管理，选择”允许多个管理员同时管理”时，防火墙系统才会允许多个管理员同时登录，但最好不要多个管理员同时进行修改配置。

可完成以下功能

1. 添加管理员账号
2. 编辑管理员账号
3. 删除管理员账号
4. 允许或禁止多个管理员同时管理
5. 设定管理员登录超时时间

添加管理员账号

1. 点击“添加”按钮，打开管理员账号维护界面
2. 输入账号、口令，并选择要添加的管理员账号类型
3. 点击“确定”按钮完成，点击“添加下一条”可以继续添加管理员账号

编辑管理员账号

1. 点击操作栏中“编辑”的快捷图标，打开管理员账号维护界面
2. 修改口令或账号类型
3. 点击“确定”按钮完成

删除管理员账号

1. 点击操作栏中“删除”的快捷图标，弹出删除对话框
2. 点击“确定”按钮完成删除

允许或禁止多个管理员同时管理

选择“允许多个管理员同时管理”时，防火墙系统才会允许多个管理员同时登录。

设定管理员登录超时时间

管理员登录后如果长时间没有操作，配置界面会超时，超时时间也在这里设置，缺省值是 600 秒，最大超时时间可设为 86400 秒（24 小时），0 是非法值。设置后点击“确定”生效。

1.4.3 管理证书

本界面完成主要的证书管理。管理证书为标准的 CA 证书。

无论使用电子钥匙认证，还是直接使用证书认证，均是通过 https 协议访问，即使用管理证书完成 SSL 的加密。

管理员通过电子钥匙认证成功，访问 https://防火墙可管理 IP:8888，登录防火墙配置界面，使用防火墙 web 服务器的服务器端的证书进行信道加密。防火墙出厂时预置了一套证书（CA 中心证书、防火墙证书、防火墙密钥），管理员可以点击 CA 中心证书的链接、防火墙证书的链接进行查看。管理员也可以更新此套证书，按”系统配置>>管理配置>>管理证书”界面提示直接导入即可。

管理员通过 IE 完成证书认证，访问 https://防火墙可管理 IP:8889，登录防火墙配置界面，使用防火墙 web 服务器的客户端的证书进行信道加密。当管理员使用证书方式进行身份认证时，必须在防火墙中导入一套证书（CA 中心证书、防火墙证书、防火墙密钥、管理员证书），并在管理主机的 IE 中导入管理员证书。管理员可以点击 CA 中心证书的链接、防火墙证书的链接进行查看。管理员可以查看导入的管理员证书列表。

此界面包括以下功能

1. 到联想网御 CA 中心下载证书
2. 导入一套证书（CA 中心证书、防火墙证书、防火墙密钥、管理员证书）
3. CA 中心证书、防火墙证书查看
4. 管理员证书维护（生效、删除）

图 1-1 导入和显示管理证书

操作流程：

1. 管理员向 CA 中心申请证书，选择一套匹配的 CA 中心证书、防火墙证书、防火墙密钥”导入”。
2. 管理员要将选择匹配的管理员证书”导入”。点击”生效”，使用相关管理员证书生效。
3. 下次登录防火墙系统前，请将有效管理员证书导入管理主机的 IE 浏览器中，访问 https://防火墙可管理 IP:8889，进入防火墙配置管理界面。

注意：CA 中心证书、防火墙证书、防火墙密钥必须是配套的。只接受 PEM 格式的证书。

下载证书

点击“联想 CA 中心”按钮，打开联想 CA 中心的主页，下载证书

导入证书

点击“浏览”按钮，分别导入一套匹配的 CA 中心证书、防火墙证书、防火墙密钥、管理员证书。CA 中心证书、防火墙证书、防火墙密钥必须同时更换。

管理员证书维护

管理员证书维护包括生效和删除，在“生效”一栏选择要生效的证书，点击“生效”按钮则生效选中的证书。在“操作”一栏中，点击“删除”的图标，删除此证书。

1.4.4 管理方式

防火墙提供 WEB 界面和 CLI 命令行两种管理方式。可以通过网口访问、串口访问，支持拨号(PPP)连接。

WEB 管理方式和串口命令行方式默认打开，不可关闭。

使用 WEB 方式管理防火墙，管理主机必须能通过网络访问防火墙，并且其 IP 地址必须在防火墙上设置（参考：系统配置>>管理配置>>管理主机）。

使用串口命令行方式管理，在关闭 PPP 接入的情况下，管理主机通过串口连接防火墙的 CONSOLE 口登录；如果打开了 PPP 接入方式，则转移到 AUX 口登录。

“启用远程 SSH”后，管理主机可以通过网络连接（通用网口或 PPP 连接均可），利用 secure crt 或 putty 等终端管理软件登录防火墙命令行界面进行管理。

打开”支持拨号(PPP)接入”选项。前提是 Modem 连接到电话线路上，并将防火墙 CONSOLE 口连接 Modem，管理主机通过另外一个 Modem 也接入电话线路，从管理主机向防火墙拨号，拨号成功后，防火墙与管理主机建立了 PPP 连接。此时，可以从管理主机上利用 putty 软件登录防火墙命令行界面（远程 SSH 方式）。

1.5 联动

1.5.1 IDS 产品

支持与 IDS 产品联动，包括支持 PUMA 协议的网御 IDS 系列，启明星辰的天阗系列，中

科网威的天眼系列，支持 **OPSEC** 协议的 **Safemate** 等。

当 IDS 联动产品发现入侵攻击行为时，会通知防火墙。防火墙会按 IDS 产品通知的阻断方式、阻断时间和入侵主机的相关信息，对入侵主机进行阻断。

防火墙阻断方式包括：

- 对”源 IP 地址”阻断
- 对”源 IP 地址、目的 IP 地址、目的端口、协议”阻断、
- 对”源 IP 地址、目的 IP 地址、协议、方向（单向、双向、反向）”阻断

防火墙阻断协议包括：TCP / UDP / ICMP 和所有协议（any）。

图 1-2 IDS 产品

表 1-2 IDS 产品功能说明

域名	说明
启用“网御通用安全协议（PUMA）入侵检测系统”联动	选择正确的密钥文件导入后，启用”网御通用安全协议（PUMA）入侵检测系统”，并指定产品的 IP 地址、防火墙端的服务端口（默认 5000/TCP），防火墙可以与之联动。
启用“天阗入侵检测系统统” 联动	启用” 天阗入侵检测系统”，并指定产品的 IP 地址、防火墙端的服务端口（默认 2000/UDP），防火墙可以与之联动。
启用“天眼入侵检测系统”联动	选择正确的证书导入后，启用”天眼入侵检测系统”，并指定产品的 IP 地址、防火墙端的服务端口（默认 4000/TCP），防火墙可以与之联动。
启用“safemate 入侵检测系统”联动	选择正确的密钥文件导入后，启用”safemate 入侵检测系统”，并指定防火墙端的服务端口（默认 2001/UDP），防火墙可以与之联动。
忽略指定 IP 地址的自动阻断	当管理员不希望一些特别 IP 被防火墙阻断时，可以在”忽略以下 IP 地址的自动阻断”列表中加入这些 IP。如果在配置忽略某 IP 地址的自动阻断之前，已经下了该 IP 的自动阻断规则，

	则需要将这些自动阻断规则清除，才能实现忽略指定 IP 地址的自动阻断。
立即清除所有自动阻断	可以立即清除所有自动阻断。

注意：每个联动请配置不同的联动端口，如配置成同一端口，则只启用界面上顺序靠后的联动系统。

1.5.2 用户认证服务器

为了增强从内网访问外网时的访问控制，提供不受服务种类限制的用户认证系统，可以为包过滤、双向 NAT、代理等访问控制提供用户认证功能。管理员可以启用防火墙本地帐号服务器，也可以启用标准的 RADIUS 服务器。即，防火墙用户认证使用的是 RADIUS 的账号库，并支持 RADIUS 服务器的审计功能。

包括以下功能

1. 配置认证端口和监控端口
2. 选择认证服务器
3. 配置 RADIUS 认证服务器
4. 配置是否记录用户认证连接日志

配置认证端口和监控端口

使用用户认证服务器，管理员必须配置防火墙用户认证模块监听的认证端口、检测用户在线情况的监控端口。

选择认证服务器

管理员可以启用防火墙本地帐号服务器，也可以启用标准的 RADIUS 服务器。

默认使用防火墙本地帐号服务器。本地帐号服务器可以提供更多的控制功能：

- 提供基于角色的用户策略，并与安全规则策略配合完成强访问控制。主要包括：安全策略和授权服务，其中，安全策略是限制用户在什么时间、什么源 IP 地址可以登录防火墙系统，而授权服务则定义了该用户通过认证后能够享有的服务。
- 支持对用户帐号的流量控制和时间控制
- 客户端可以修改密码
- 服务器端检查用户在线状态
- 支持 PAP 和 S/Key 认证协议

配置 RADIUS 认证服务器

启用 RADIUS 认证服务器，需要配置 RADIUS 认证服务器所在的 IP 地址、认证端口、审计端口及与防火墙加密通信的密钥。

配置是否记录用户认证连接日志

在用户在认证后，防火墙可以记录该用户发起的所有连接的日志信息，如果用户发起的连接数目很多，防火墙将会记录很多条这样的日志。该选项可以让管理员决定是否记录这些用户认证连接日志。

1.6 报告设置

1.6.1 日志服务器

防火墙各功能模块提供标准日志记录。

启用日志记录后，默认情况下日志存储在防火墙本地。防火墙也可以将日志发往第三方的日志服务器，

日志服务器可以与防火墙的任意网口连接。

防火墙提供随机日志服务器软件，提供强大的日志存储与审计功能。

提供以下功能

1. 配置日志服务器
2. 转到“系统监控>>日志信息”界面

配置日志服务器

需要管理员配置日志服务器 IP、防火墙与日志服务器通信的协议与端口。防火墙默认使用 syslog 方式向第三方发送日志，端口 514 / 协议 UDP。

转到“系统监控>>日志信息”界面

点击“查看日志”按钮，转到“系统监控>>日志信息”界面

1.6.2 报警邮箱设置

可以设置防火墙的报警邮箱。当有紧急情况发生时，可以用这个事先设定好的报警邮箱给防火墙管理员发报警邮件。

此界面包括以下功能

配置报警邮箱

转到“网络配置>>域名服务器”界面

配置报警邮箱

配置报警邮箱的发件人地址，并指定邮箱密码。

指定该邮箱所在 SMTP 服务器的域名地址或者 IP 地址和端口。

指定收件人地址，最多可以指定三个收件人地址。

启用或者关闭报警邮箱功能。

启用或者关闭日志功能。

转到“网络配置>>域名服务器”界面

点击“修改 DNS 配置”按钮，转到“网络配置>>域名服务器”界面。如果不能正常发邮件，请检查 DNS 配置是否正确。

图 1-3 报警邮箱设置

1.6.3 发送邮件

可以从防火墙上发送电子邮件给收件人，在这部分功能里，发件人以及 smtp 服务器地址和端口的设置，是在报警邮箱设置里面设置好的。

可以填写长度为 100 的邮件主题。

可以填写长度为 1500 的邮件正文，支持中文和任何符号。

可以设置个性签名功能，签名会连接在邮件正文的后面。

可以添加附件，附件名称需为中文，大小不超过 3 兆。

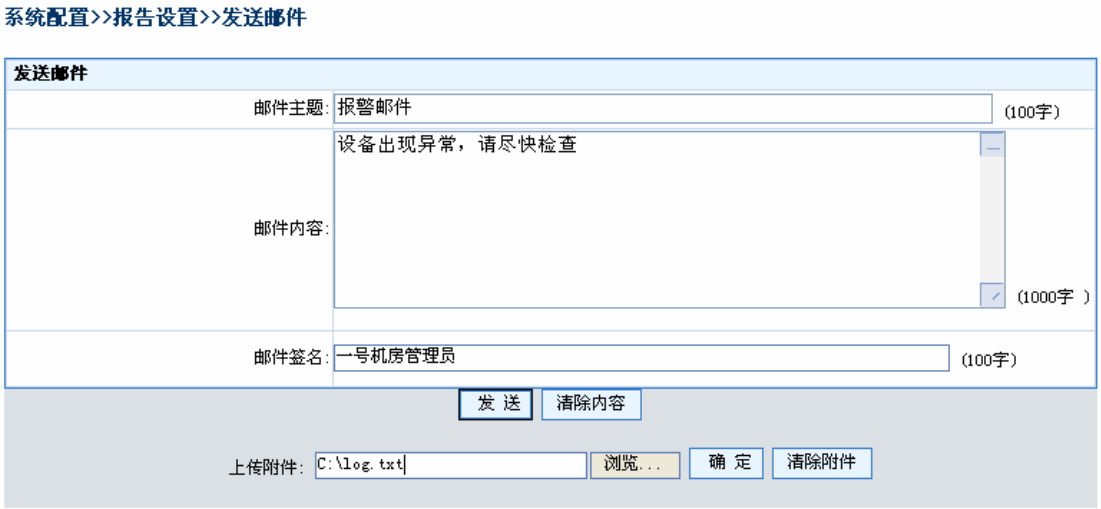


图 1-4 发送邮件界面

1.6.4 集中管理

支持安全网关的集中管理（**SNMP v1,v2**）。安全网关可以与联想网御集中安全管理系统无缝联动。

管理员配置集中管理主机的 **IP**、各项监控信息的阈值和 **SNMP** 团体字串。联想网御集中安全管理系统,通过 **SNMP** 协议从安全网关获取监控信息，包括：系统名字、版本号、序列号、**CPU** 利用率、内存利用率、网络接口状态、网络连通状态等，同时当安全网关运行信息超过阈值后，通过 **SNMP** 协议向集中管理主机发 **Trap** 告警信息。通过 **TRAP** 信息发给集中管理中心，为网络管理人员提供全面、易用、高效的实时监控网络资源使用状况的工具和手段。相关信息也可以在安全网关的“系统监控**>>**网络设备”界面和“系统监控**>>**资源状态”查看。

集中管理的配置页面如下：

表 1-3 集中管理配置元素表

域名	说明
集中管理主机 IP	只有集中管理主机 IP 才能通过 SNMP 访问设备，并接收到 Trap 信息。支持多个集中管理主机 IP，点击“〉〉”添加，“〈〈”删除
安全网关名称	防火墙名称
本机备注	对防火墙的描述
负责人姓名	负责人姓名
负责人电话	负责人电话
CPU 利用率阈值	如果实际利用率超过该值，则向集中管理主机发送报警信息
内存利用率阈值	如果实际利用率超过该值，则向集中管理主机发送报警信息
磁盘利用率阈值	如果实际利用率超过该值，则向集中管理主机发送报警信息
snmp v1&v2	通过此选项控制是否启用 SNMPv1&v2c
只读团体字符串	通过 SNMPv1&v2c 读取设备信息时的认证标识
读写团体字符串	通过 SNMPv1&v2 读/写设备信息时的认证标识
Trap 发送字符串	设备向集中管理主机发送 Trap 报警信息时的标识
snmp v3	通过此选项控制是否启用 SNMPv3
用户名称	SNMP v3 授权用户名
安全选项	选择 SNMP v3 用户访问的安全级别，分为：加密授权认证方式、非加密授权认证方式和非授权认证方式，当选择加密授权认证方式时必须设置认证和加密相关项；当选择非加密授权认证必须设置认证相关项。
认证协议	选择 SNMP v3 用户认证的协议
认证密码	设置 SNMP v3 用户认证的密码
加密协议	选择 SNMP v3 加密协议密码
加密密码	设置 SNMP v3 加密密码

输入以上各域内容，点击“确定”完成集中管理主机配置。同时通过点击“启动 SNMP 代理”/“停止 SNMP 代理”按钮控制安全网关上的 SNMP 代理服务启动或停止。

1.7 入侵检测

防火墙本身主要在链路层进行访问控制，入侵检测技术是防火墙技术的逻辑补偿。作为一种数据通信监视手段，入侵检测技术对于每一个进出数据包都要进行解码分析和模式匹配，如果发现该数据包中含有与已知的攻击方法特征库相匹配的数据，则断定有入侵事件发生，发出警报提醒管理员注意，并可以自动阻断源 IP 地址，及时地将攻击者拒之门外。联想网御防火墙将入侵检测技术无缝地集成到自身当中，极大地提高了防火墙检测数据驱动型攻击的能力。由于防火墙本身部署的特点，只能对通过防火墙的数据包进行检测，如果用户需要对整个网络的潜在攻击进行监控，建议选用联想网御系列入侵检测产品。

入侵检测模块主要功能特点包括：

- **实时网络数据流监控**

实时监视进出防火墙的所有通信流，分析网络通信会话轨迹。信息收集与分析同步进行，快速反应，一旦发现可疑信息，及时报警并响应。

- **网络攻击模式匹配**

预置的已知攻击模式规则库，能检测多种攻击行为，最大限度地防范黑客的入侵和内部用户的非法使用。规则库可以在线升级，确保能够识别最新的黑客攻击手段。

- **针对入侵行为的实时自动响应**

能够自动响应入侵事件，除了报警和写日志外，可以做到实时阻断可疑连接，同时防火墙还可以和其它厂商的 IDS 产品如“天阗”、“天眼”IDS 实现联动，威力强大。

- **灵活的检测策略设置**

内置十六种检测策略，用户可以随意组合使用，做到量体裁衣，突出重点。

- **支持用户添加自定义检测规则**

用户可以根据自己的实际情况和感兴趣的安全事件添加自定义检测规则，体现个性化服务。

- **支持高级用户调整检测规则**

管理员可根据 IDS 保护的网络的具体情况，调整检测策略中的检测规则，将容易引起误报的规则禁用，更好地提高入侵检测的效率。

- **全天候报警方式**

可自动将报警信息传送到管理员的电子邮箱，显现在移动通讯设备上，实现离线监控。

1.7.1 基本配置

首先，登录防火墙配置管理界面后，通过左侧菜单栏的系统配置>>入侵检测，即出现入侵检测的管理界面。

监听网段格式举例：1.1.1.0/24,5.1.1.2/32

基本配置可以设置是否启动入侵检测，及监听的网口和网段。

1.7.2 策略配置

策略配置可以允许管理员选择列表中一项或者多项检测策略并使之生效，以对付入侵。

ids 的报警邮箱设置与整个系统的报警邮箱设置在一起，系统报警邮箱的设置在系统配置-〉报告设置-〉报警邮箱下，

设置好报警邮箱后，ids 系统会在入侵纪录达到 100 条或时间间隔达到 30 秒时，自动发送所有的入侵纪录到此邮箱中。

1.7.3 自定义检测

从列表中可以查看当前的所有的自定义规则，管理员可以生效或失效一条规则，来检测或取消检测某一类入侵事件。

管理员可以添加自定义规则

注意事项：

- 如果正常的网络行为引起某条规则大量误警，可以将该条规则禁用。自动响应功能最好在正常运行一段时间后，当误报已经减少到很低程度时再启用。
- 有时 FTP 服务器或 DNS 服务器会引发扫描报警，这属于误报，可以调整扫描时间阈值或者将这些服务器的 IP 地址添加到忽略扫描报警的地址列表中。
- 有时在检测结果中会看到对外服务器的 IP 出现在攻击者的源地址中，比如从对外服务器的 80 端口到某个外部 IP 地址的高端口，报警信息为发现了 403 forbidden 的特征字符串。这条报警信息并不意味着对外服务器是攻击者，恰恰相反，正是由于某个外部 IP 通过防火墙向对外服务器发起了非法的 web 请求，导致服务器返回“403 禁止访问”的信息，所以攻击者是外部 IP 地址主机。但是由于防火墙的自动响应功能只阻断检测结果中的源 IP 地址，因此为了确保服务器不被阻断，最好将服务器的 IP 地址放入忽略自动阻断的地址列表中。

1.7.4 扫描检测配置

管理员点击“扫描检测配置”，可以将扫描时间阈值由 3 分钟内发现 5 次端口连接调整为 10 秒钟内发现 3 次端口连接。

注意：忽略扫描的源 IP 地址的数量最多为 30 个

1.7.5 自动响应配置

管理员可以启用自动响应功能，并设置阻断时间。

设置完毕后，自动响应功能生效。一旦有触发检测规则的可疑事件发生，出现在检测结果中的源 IP 地址立即被自动列入系统黑名单中，发起者的通信被防火墙阻断，可疑行为将无法继续进行下去。管理员可以自定义阻断时间（以秒为单位），如果不填写时间，则视为永远不解除阻断。

清除已经阻断的 IP 地址，可以清除防火墙系统的所有已经阻断的 IP 地址，包括 ids 联动系统阻断的地址。

注意：攻击者可以伪造地址进行攻击，所以开启该项功能有可能导致对被伪造 IP 的 DOS 攻击或网络通信异常，因此推荐一般情况下不要打开此项功能。

1.7.6 检测结果

管理员点击界面中的“检测结果”，可以查看所有的入侵。

1.8 产品许可证

通过本页面可以将您获取到的防火墙模块的许可证上载，并导入到防火墙。上载成功后，请您重新登录防火墙界面,便可看到防火墙模块已经生效。

第2章 网络配置

本章主要介绍防火墙的网络配置，由以下部分组成：网络设备，域名服务器，默认路由，静态路由，策略路由，UPnP 服务器，DHCP 服务器和 HA（高可靠性）。

2.1 网络设备

联想网御防火墙 Power V 可配置的网络设备有：物理设备，VLAN 设备，桥接设备，VPN 设备，别名设备，冗余设备和拨号设备。下面对各类设备的特点做一简要说明。

物理设备：防火墙中实际存在的网口设备，不能删除，也不能添加。增减网络接口硬件模块会自动在网络配置中显示出来，不需要手动操作。其中第一个物理设备 fe1 是默认的管理设备，它的默认 IP 地址是 10.1.5.254，这个地址允许管理，PING 和 TRACEROUTE。物理设备是其他设备的基础，如果增减网络接口硬件模块，与这个设备相关的其它设备都会受到影响，这一点需要特别注意。

VLAN 设备：是一种在物理设备基础上创建的设备。与交换机的 TRUNK 口相连的防火墙物理设备上可以创建 VLAN 设备，以实现不同 VLAN 之间的互联。它可以工作在路由模式下，也可以工作在透明模式下。同一个物理设备上可以创建 VLAN ID 为 0 至 4094 的 VLAN 设备。同一物理设备上创建的不同 VLAN 设备，VLAN ID 必须不同，用于接收和发送带有相应 VLAN ID 的数据包。不同物理设备上创建的 VLAN 设备的 VLAN ID 可以相同。

桥接设备：是将多个物理设备和 VLAN 设备置于透明模式，并且进行分组的设备。启用此设备的防火墙相当于一个二层交换机，但它同时可以过滤三层的内容。防火墙可以创建多个桥接设备，桥接设备绑定的物理设备或 VLAN 设备必须是启用并且工作在透明模式的设备。这些桥接设备可以和工作在路由模式下的物理设备和 VLAN 设备共存。

VPN 设备：是启用 VPN 功能必须要启用的设备。整个防火墙系统中只能有一个 VPN 设备，但是 VPN 设备的绑定设备可以选择。系统通过绑定的设备来发送和接收加密后的数据包。VPN 设备也可以启用带宽管理功能，但这要求其绑定的设备没有启用带宽管理。VPN 设备的 IP 地址、掩码与它的绑定设备的 IP 地址、掩码一致。

别名设备：用于给物理设备配置多个 IP 地址。每个物理设备可以关联的别名设备是 253 个，这类似于资源定义中地址池的功能，但是在地址池中配置的 IP 不能选择“用于管理”，“允许 PING”，“允许 TRACEROUTE”等属性。同时要注意的是别名设备的 IP 地址不能重复。

冗余设备：是将多个物理设备捆绑在一起而成的虚拟设备。冗余设备捆绑的物理设备共同完成收发工作，组成一个逻辑链路供系统使用。捆绑的物理设备可以相互备份，一个物理设备失效，其它物理设备可接替它的工作。

拨号设备：用于启用 ADSL 拨号功能所必须要启用的设备。系统中只能有一个拨号设备，但是拨号设备绑定的物理设备可以选择。系统通过绑定的设备来发送和接收 PPPoE 的数据包。拨号设备也可以启用带宽管理功能，但这要求其绑定的设备没有启用带宽管理。拨号设备的 IP 地址、掩码每次 ADSL 拨号成功后，自动获得。

配置防火墙的过程中，必须首先配置网络设备，再配置防火墙安全策略。如果网络设备的配置发生了改变，建议对相关的安全策略也进行调整。

2.1.1 物理设备

物理设备初始情况下工作在路由模式，也就是说该设备上绑定有 IP 地址，可以与其它设备进行数据包的路由转发。其中第一个物理设备 fe1 是默认的可管理设备。它的默认 IP 地址是 10.1.5.254，子网掩码为 255.255.255.0，这个地址允许管理，PING 和 TRACEROUTE（默认管理主机的 IP 地址是 10.1.5.200，请参考系统配置>>管理配置>>管理主机）。物理设备也可以切换到透明模式。当桥接设备当中只有一个桥设备 brg0 时，切换到透明模式的物理设备会自动加入到桥接设备 brg0 中；如果把物理设备从透明模式切换到路由模式，系统自动将这个设备从桥接设备的设备列表中删除。

物理设备是其他设备的基础。在 WEB 配置管理界面和 CLI 配置管理界面上可配置的物理设备是在系统启动时能够检测到的设备，如果系统启动时，检测不到相应的设备，那么这个设备在界面上就不会显示。

表 2-1 物理设备上可配置的属性

属性名称	描述
名称	设备名称，不能修改
MAC 地址	设备的 MAC 地址，可以修改。如果忘记了设备最初的 MAC 地址，可以将 MAC 地址置为空值并重启安全网关，防火墙会自动探测出设备的 MAC 地址。
链路工作模式	设备的链路工作模式，有以下三种 1：自适应 2：全双工 3：半双工
链路速度	设备的链路速度，有以下三种 1：10 2：100 3：1000
MTU	设备的 MTU（最大传输单位）。百兆网络设备可设置的范围是 68 到 1504，千兆网络设备可设置的范围是 64 到 16128。
工作模式	设备的工作模式，目前支持的有以下两种 1：路由模式，这是设备默认的工作模式，在路由模式下，必须配置设备的 IP 地址。 2：透明模式，设置为透明模式的设备不能配置 MTU，IP 地址/掩码，不能用于管理，PING 和 TRACEROUTE 等选项也不能选择。
IP 地址获取	IP 地址的获取方式，目前支持的有以下两种 1：静态指定 2：通过 DHCP 获取，即防火墙相应物理设备作为 DHCP 客户端获得 IP 地址。
IP 地址	IP 地址配置只在 IP 地址获取方式为静态指定时可配置
掩码	掩码只在 IP 地址获取方式为静态指定时可配置
开启动态域名	如果选择开启动态域名，则物理设备的 IP 地址和动态域名之间的绑定关系会被注册到特定的服务器上，注册所需的用户

	名、密码可以在 系统设置>>系统参数中设置。此功能用于 IP 地址不固定的 VPN 组网。
动态域名	与设备 IP 地址对应的动态域名
开启 IPMAC 地址绑定	是否开启此设备上的 IPMAC 地址绑定检查功能
允许未绑定的 IPMAC 地址通过	未绑定的 IP 地址是否允许通过
开启 IP 地址欺骗检查	开启此设备上的 IP 地址欺骗检查
开启 TRUNK	是否将设备设置为 TRUNK 口。用于连接交换机或者路由器的 TRUNK 口。配置透明模式下的 TRUNK 功能时，请在”策略配置>>安全选项”页面，选中” 802_2(4) ”选项。
开启带宽管理	是否开启此设备上的带宽管理
设备带宽	此设备支持的带宽。如果设备的速度是 10M，设备带宽的范围是 1-10000 之间；如果设备的速度是 100M，设备带宽的范围是 1-100000 之间；如果设备的速度是 1000M，设备带宽的范围是 1-1000000 之间。
开启 DHCP 中继	是否允许此设备转发 DHCP 中继信息，但是 DHCP 中继功能键不支持在开启 OSPF 启用。
DHCP 服务器地址	此设备将 DHCP 信息中继到哪个服务器上，这是一个 IP 地址的列表，如果有多个 IP 地址，请用英文逗号分隔，中间不能有空格，IP 地址不能重复。
用于管理	此设备的 IP 地址是否能用于管理
允许 PING	此设备的 IP 地址是否允许被 PING 到
允许 TRACEROUTE	此设备的 IP 地址是否允许被 TRACEROUTE 到
是否启用	是否启用此设备

在物理设备中，有一个“允许开启 TRUNK 的物理设备在不同 VLAN 间转发包”的选项，如果选中，则允许配置 TRUNK，工作在透明模式的物理设备，根据规则在不同 VLAN 间转发数据包，如果没有选中，工作在透明模式的物理设备，则不会在不同 VLAN 之间转发数据包。默认是不选中。

2.1.2 VLAN 设备

VLAN 设备是一种在物理设备基础上创建的设备。它可以工作在路由模式下，也可以工作在透明模式下，工作在透明模式时，此设备可加入桥接设备。VLAN 设备可以与其他同 VLAN 的设备通讯，并通过防火墙转发不同 VLAN 之间的通讯。同一个物理设备上可以创建多个不同 VLAN ID 的 VLAN 设备。不同物理设备上的 VLAN 设备的 VLAN ID 可以相同。

VLAN 设备和物理设备上的 TRUNK 属性是防火墙支持 VLAN 应用环境的两种方式。用户可以根据实际情况来选择使用何种方式，但两种方式不能同时使用。

表 2-2 VLAN 设备上可配置的属性

属性名称	描述
选择绑定设备	VLAN 的绑定设备必须是启用的，工作在路由模式下物理设备，并且此物理设备没有开启 TRUNK。

填写 VLAN ID	VLAN ID 是一个 0 到 4094 的无符号整数
工作模式	设备的工作模式，目前支持的有以下两种 1：路由模式，这是设备默认的工作模式 2：透明模式，设置为透明模式的设备 IP 地址/掩码，不能用于管理，PING 和 TRACEROUTE 等选项也不能选择。
IP 地址	设备的 IP 地址，路由模式下必须填写
掩码	设备的掩码，路由模式下必须填写
MAC 地址	设备的 MAC 地址，如果不填，则表示自动获取
开启 IPMAC 地址绑定	是否开启此设备上的 IPMAC 地址绑定检查功能
允许未绑定的 IPMAC 地址通过	未绑定的 IP 地址是否允许通过
开启 IP 地址欺骗检查	开启此设备上的 IP 地址欺骗检查
开启带宽管理	是否开启 VLAN 设备的带宽管理，VLAN 设备的带宽管理和它的绑定设备上的带宽管理相互冲突，不能同时存在
设备带宽	此设备支持的带宽。如果设备的速度是 10M，设备带宽的范围是 1-10000 之间；如果设备的速度是 100M，设备带宽的范围是 1-100000 之间；如果设备的速度是 1000M，设备带宽的范围是 1-1000000 之间。
用于管理	此设备的 IP 是否用于管理
允许 PING	此设备的 IP 是否允许被 PING 到
允许 TRACEROUTE	此设备的 IP 是否允许被 TRACEROUTE 到
是否启用	是否启用此设备

2.1.3 桥接设备

桥接设备是将多个工作在透明模式的物理设备和 VLAN 设备绑定在一起的设备。启用此设备的防火墙相当于一个二层交换机，但它同时可以过滤三层的内容。防火墙可以创建多个桥接设备（最多可以创建八个桥接设备，设备名分别是 brg0, brg1, brg2, brg3, brg4, brg5, brg6, brg7），而且这些桥接设备可以和工作在路由模式下的物理设备和 VLAN 设备共存。在这种情况下，路由信息和桥接设备的信息相互间没有影响。

表 2-3 桥接设备可配置的属性

属性名称	描述
设备名称	桥接设备的设备名称，不能修改
IP 地址	设备的 IP 地址，桥接设备的 IP 地址可以为空。如果它的 IP 地址是空则不能设置管理，PING 和 TRACEROUTE。
掩码	设备的掩码，桥接设备的掩码可以设置为空。
开启 STP	桥接设备是否开启 STP（生成树协议）
允许未绑定的 IPMAC 地址通过	未绑定的 IP 地址是否允许通过
开启 IPMAC 地址绑	是否开启此设备上的 IPMAC 地址绑定检查功能

定	
开启 IP 地址欺骗检查	开启此设备上的 IP 地址欺骗检查
用于管理	此设备的 IP 是否用于管理
允许 PING	此设备的 IP 是否允许被 PING 到
允许 TRACEROUTE	此设备的 IP 是否允许被 TRACEROUTE 到
可选绑定设备列表	桥接设备可选的绑定设备列表。列表包括工作在透明模式的物理设备和 VLAN 设备。
绑定设备列表	被选中的绑定设备列表
是否启用	是否启用此设备

2.1.4 VPN 设备

VPN 设备是启用 VPN 功能所必须要启用的设备。系统中最多可以支持 32 个 VPN 设备，每个 VPN 设备的绑定设备是不同的。每个 VPN 设备都可以启用带宽管理功能，但这要求它的绑定设备没有启用带宽管理。VPN 设备的 IP 地址、掩码与它的绑定设备的 IP 地址、掩码一致。

表 2-4 VPN 设备可配置的属性

属性名称	描述
设备名称	VPN 设备名称，自动生成，不能修改
选择绑定设备	VPN 的绑定设备，包括有 IP 地址的、启用的物理设备、桥接设备或拨号设备
开启带宽管理	开启 VPN 设备的带宽管理
设备带宽	此设备支持的带宽。如果设备的速度是 10M，设备带宽的范围是 1-10000 之间；如果设备的速度是 100M，设备带宽的范围是 1-100000 之间；如果设备的速度是 1000M，设备带宽的范围是 1-1000000 之间。
是否启用	是否启用此设备，如果选择启用，当点击“重新加载设备”按钮时该设备会加载到 VPN 系统中。如果不选择启动，当点击“重新加载设备”按钮时该设备不会加载到 VPN 系统中。

2.1.5 别名设备

别名设备的作用是给物理设备配置多个 IP 地址。每个物理设备可以关联的别名设备是 253 个，这类似于资源定义中地址池的功能，但是在地址池中配置的 IP 不能选择“用于管理”，“允许 PING”，“允许 TRACEROUTE”等属性。同时要注意的是别名设备的 IP 地址不能重复。

表 2-5 别名设备可配置的属性

属性名称	描述
绑定设备名称	绑定设备的名称，可选的绑定设备包括已启用的工作在路由模式下的物理设备和已启用的桥接设备
别名 ID	别名设备的别名 ID，允许值是 0－252
IP 地址	别名设备必须配置 IP 地址
掩码	别名设备必须配置掩码
用于管理	设备的 IP 地址是否能用于管理
允许 PING	是否允许 PING 设备的 IP
允许 TRACEROUTE	是否允许 TRACEROUTE 设备的 IP
是否启用	是否启用设备

2.1.6 冗余设备

通过将几个物理设备捆绑在一起组成一个虚拟的冗余设备。冗余设备的作用有：

- 提高链路可靠性。冗余设备捆绑的物理设备相互动态备份，一个成员的链路中断（网口掉线），其它成员可以迅速接替它的工作，与生成树（STP）不同，对冗余设备之外是不可见，即成员之间的备份只限制所属冗余设备内部，对其它冗余设备无效。
- 增加防火墙带宽。冗余设备的使用可提供一个经济有效的提高防火墙带宽的方法。通过捆绑多个物理设备，可以使防火墙处理更大的带宽，冗余设备带宽理论上等于绑定的物理设备带宽之和。冗余设备按照一定的均衡算法将流量分配给绑定的物理设备，实现链路级的负载分担。

冗余设备的高级设置可以设置冗余设备工作的模式，修改工作模式需要保存并重启防火墙才能生效。

- 轮循方式：冗余设备在绑定设备中采用轮循方式发送数据包
- 热备方式：冗余设备只有一个物理设备转发数据包，其它设备处于备份状态。
- 802.3ad 方式：冗余设备在绑定设备中采用 802.3ad 协议的方式接收发送数据包

表 2-6 冗余设备可配置的属性

属性名称	描述
名称	冗余设备名称，不能修改
工作模式	设备的工作模式，目前支持的有以下两种 1：路由模式，这是设备默认的工作模式，在路由模式下，必须配置设备的 IP 地址。 2：透明模式，设置为透明模式的设备不能配置 MTU，IP 地址/掩码，不能用于管理，PING 和 TRACEROUTE 等选项也不能选择。
IP 地址获取	IP 地址的获取方式，目前支持的有以下两种 1：静态指定 2：通过 DHCP 获取，即防火墙相应物理设备作为 DHCP 客户端获得 IP 地址。
IP 地址	IP 地址配置只在 IP 地址获取方式为静态指定时可配置
掩码	掩码只在 IP 地址获取方式为静态指定时可配置

开启动态域名	如果选择开启动态域名，则物理设备的 IP 地址和动态域名之间的绑定关系会被注册到特定的服务器上，注册所需的用户名、密码可以在 系统设置>>系统参数中设置。此功能用于 IP 地址不固定的 VPN 组网。
动态域名	与设备 IP 地址对应的动态域名
开启 IPMAC 地址绑定	是否开启此设备上的 IPMAC 地址绑定检查功能
允许未绑定的 IPMAC 地址通过	未绑定的 IP 地址是否允许通过
开启 IP 地址欺骗检查	开启此设备上的 IP 地址欺骗检查
开启 DHCP 中继	是否允许此设备转发 DHCP 中继信息
DHCP 服务器地址	此设备将 DHCP 信息中继到哪个服务器上，这是一个 IP 地址的列表，如果有多个 IP 地址，请用英文逗号分隔，中间不能有空格，IP 地址不能重复。
绑定设备选择	供冗余设备捆绑的物理设备（选择了冗余模式的物理设备），冗余设备至少有一个绑定设备
用于管理	此设备的 IP 地址是否能用于管理
允许 PING	此设备的 IP 地址是否允许被 PING 到
允许 TRACEROUTE	此设备的 IP 地址是否允许被 TRACEROUTE 到
是否启用	是否启用此设备

2.1.7 拨号设备

拨号设备用于建立防火墙的 ADSL 连接，目前防火墙只能支持一个 ADSL 连接，它的设备名是 dial0。

表 2-7 拨号设备可配置的属性

属性名称	描述
设备名称	设备名称，是 dial0，不能修改
绑定设备	通过哪个物理设备拨号，拨号前必须先启用此物理设备
用户名	拨号用户名，1 至 15 个 ASCII 字符
密码	拨号密码，1 至 15 个 ASCII 字符
系统启动时拨号	在防火墙启动时拨号，但绑定设备，用户名，密码等参数必须正确
时间调度	定时拨号的时间，需要事先在“资源定义>>时间”处定义，如果没有选择时间，默认是一直保持连接
开启带宽管理	开始此设备的带宽管理，相应的绑定设备上的带宽管理必须去掉
开启动态域名	如果选择开启动态域名，则拨号设备获得的 IP 地址和动态域名之间的绑定关系会被注册到特定的服务器上，注册所需的用户名、密码可以在 系统设置>>系统参数中设置。此功能用

	于 IP 地址不固定的 VPN 组网。
动态域名	与设备 IP 地址对应的动态域名
用于管理	设备的 IP 是否用于管理
允许 PING	设备的 IP 是否允许 PING 到
允许 TRACEROUTE	设备的 IP 是否允许 TRACEROUTE 到
是否启用	是否启用此设备，如果启用此设备，必须选择绑定设备，并配置用户名，密码。

2.1.8 不同设备之间的配置关系

下表说明“物理设备”，“别名设备”，“VLAN 设备”，“桥接设备”，“VPN 设备”，“冗余设备”和“拨号设备”之间的配置关系。

打✔说明横向的设备可以作为竖向设备的绑定设备。

表 2-8 网络设备间的绑定关系

	物理设备	VLAN 设备	桥接设备	VPN 设备	别名设备	冗余设备	拨号设备
物理设备		✔	✔	✔	✔	✔	✔
VLAN 设备			✔	✔	✔		
桥接设备				✔	✔		
VPN 设备							
别名设备							
冗余设备		✔	✔	✔	✔		✔
拨号设备				✔			

2.2 域名服务器

如果管理员设置了邮件代理等服务，则需要配置防火墙的域名服务器，用于防火墙自身向外发数据包时的域名解析。

配置防火墙的域名服务器，可以配置域名服务器 1 和域名服务器 2，其中域名服务器 1 具有较高的优先级。点击“确定”按钮完成配置。

2.3 多默认路由负载均衡

联想网御防火墙提供多个默认路由负载均衡的功能，进行路由选择时，如果没有策略路由、静态路由与当前的数据包匹配，则会选择默认路由，可以通过对默认路由的设置，使默认路由实现负载均衡的功能。

默认路由在系统路由规则中的优先级最低，当数据包到达时，首先与策略路由、静态路由等路由规则进行匹配，如果匹配成功，则对应的策略路由、静态路由被选中，如果匹配不

成功，则进行默认路由。

管理员可以添加、编辑或删除默认路由规则，同时可以开启、关闭对默认路由网关的实时监测功能。

在 web 界面，对默认路由的管理可以分为三个部分，首先是默认路由的状态控制。

在“网络配置>>默认路由”界面中上半部分为状态控制区，可以对默认路由的相关状态进行设置：

1、 启用默认路由均衡：通过设置该项，可以启用/停止系统中多默认路由均衡的功能，当该选项前面的单选框中显示”√”时，该功能为启用状态。只有启用该功能后，该配置页面的其它选项才有意义。

2、 启用网关监测：通过设置该选项，可以设置实时探测/不探测默认路由网关的可连通情况，只有对应的默认路由网关可连通，其对应的默认路由规则才会在系统中生效。如果该项没有被选中(即不对默认网关的可连通情况进行监控)，则系统认为配置的默认路由都是有效的，其默认网关都是可连通的，相应的默认路由规则也会在系统中生效。如果选中该选项，则会对指定的默认路由网关进行实时监测，只有可连通网关对应的默认路由才会在系统中生效。

注意：

对于拨号设备的监控情况，不受该选项的影响，即对拨号设备的监控总在进行，但受下面监测频率的影响。

对于默认网关可连通性的监测，采用 arp 协议与 icmp 协议进行探测，以 icmp 协议的探测为优先，如果 icmp 协议探测失败（失败的原因：可能是对应的默认网关不存在，也可能是对应的默认网关禁用 icmp 协议），则再采用 arp 协议进行探测。如果 icmp 协议与 arp 协议的探测都失败，则表明默认网关是不可达的，否则只要有 icmp 协议或者 arp 协议之一的探测有效，则判定对应的默认网关是可连通的。

3、 监测频率：对指定的默认路由对应网关的监测频率，即多长时间探测一次网关的可连通情况。对于拨号设备，其监测频率受该值的控制。对于其它的设备，如果没有设置“启用网关监测”功能，则该选项无意义。

在“网络配置>>默认路由”界面的下半部分，用以对默认路由进行配置，包括添加、删除、编辑

1、 添加默认路由：

点击“添加”按钮，会出现添加默认路由界面：

添加默认路由参数，请务必保证默认网关地址和选择的网络接口在同一网段内。对于拨号设备，不需要指定其默认网关地址，系统会自动处理。相关参数设置完成后，点击“确定”按钮完成添加。

注意：多默认路由负载均衡功能目前支持的设备类型包括：物理设备、拨号设备、冗余设备、别名设备。

2、 删除默认路由：

点击“操作”一栏中的“删除”图标，弹出删除对话框，点击“确定”按钮完成删除。

3、 编辑默认路由：

点击“操作”一栏中的“编辑”图标，打开“默认路由维护”界面，然后执行修改操作，待相关参数编辑完成后，点击“确定”按钮完成修改。

启用/禁用策略路由规则：
点击“是否启用”一栏中的图标，

如果原来是✔，点击后变成✘，表示由启用状态变成禁用，，如果原来是✘，点击后变成✔，表示由禁用状态变成启用。

表 2-9 添加和编辑默认路由参数说明：

域名	说明	和其他界面的关系
网关地址	默认路由的网关地址，该地址应该与该默认路由的出口在同一子网中	
权重值	该默认路由分配的权重值，系统会根据该权重值来自动调配默认路由的使用频率	
网络接口	接口和默认网关地址须在同一网段内	从网络配置>>网络设备中选取接口
是否启用	是否将该默认路由应用到系统中	

对默认路由的监控，系统会实时显示其监控信息，默认路由的监控页面在 系统监控>>路由监控页面中。

如果对应默认路由的网关地址可达，则对应“是否有效栏”显示为“有效”，该默认路由信息将会在系统中生效，否则，如果对应默认路由的网关地址不可达，则对应“是否有效”栏显示为“无效”，该默认路由规则将不会出现在系统默认路由信息中。

2.4 静态路由

联想网御防火墙提供静态路由和策略路由功能，本节介绍静态路由的使用，下一节介绍策略路由。

防火墙静态路由支持按目的地址的路由，即按数据包中的目的 IP 地址来决定下一跳地址。修改网络设备的 IP 地址可能会影响到相应的路由规则。建议首先配置网络设备的地址，再配置路由规则。

管理员可以添加，编辑，删除，启用或者禁用静态路由规则。静态路由规则的参数包括目的地址、掩码、下一跳地址和网络接口。下一跳地址应该和相应的网络接口在同一网段内。

防火墙的默认路由（默认路由即界面上的默认网关）也是在这里手工添加的，也可以删除，修改和启用，禁用默认路由。默认路由只能有一个生效。

一般拨号设备在拨号成功时，会自动从运营商获得默认路由，因此在使用拨号设备之前，建议最好在这里删除默认路由，而使用自动获取的。同样，DHCP 协议会自动获取默认路由，所以在使用 DHCP 服务时，建议最好在这里删除默认路由，使用自动获取的。否则有可能造成不能连接网络的问题。

在“网络配置>>静态路由”界面中可以完成以下功能：

1. 添加静态路由
2. 编辑静态路由
3. 删除静态路由
4. 启用/禁用静态路由规则

添加静态路由

1. 点击“添加”按钮，进入“静态路由维护”
2. 添加静态路由参数
3. 点击“确定”按钮完成添加

编辑静态路由

1. 点击“操作”一栏中的“编辑”图标，打开“静态路由维护”界面
2. 执行修改操作
3. 点击“确定”按钮完成修改

表 2-10 添加和编辑时参数说明

域名	说明	和其他界面的关系
目的地址和掩码	设置目的 IP 地址，可以设置 IP 地址/子网掩码	
下一跳地址	设置网关的 IP 地址	
网络接口	接口和下一跳地址须在同一网段内	从网络配置>>网络设备中选取接口

删除静态路由

1. 点击“操作”一栏中的 “删除”图标，弹出删除对话框
2. 点击“确定”按钮完成删除

启用/禁用静态路由规则

点击“是否启用”一栏中的图标，如果原来是✔，点击后变成✘，表示由启用状态变成禁用，，

如果原来是✘，点击后变成✔，表示由禁用状态变成启用。

2.5 策略路由

联想网御防火墙提供策略路由功能，进行路由选择时不仅根据数据包的目的地址，而且可以根据数据包的源地址进行路由选择。

策略路由的优先级高于静态路由，即数据包到达时，首先根据源地址匹配策略路由规则，如果找到匹配的规则，则根据规则进行策略路由，如果找不到，则进行静态路由。

管理员可以添加、编辑或删除策略路由规则。策略路由规则的参数包括源 IP 地址、源掩码、目的 IP 地址、目的掩码、下一跳地址和网络接口。下一跳地址应和网络接口在同一网段内。

在“网络配置>>策略路由”界面可以完成以下功能：

1. 添加策略路由
2. 编辑策略路由
3. 删除策略路由
4. 启用/禁用策略路由规则

添加策略路由

2. 点击“添加”按钮，进入“策略路由维护”
3. 添加策略路由参数，请务必保证下一跳地址和选择的网络接口在同一网段内。
4. 点击“确定”按钮完成添加

编辑策略路由

2. 点击“操作”一栏中的“编辑”图标，打开“策略路由维护”界面
3. 执行修改操作
4. 点击“确定”按钮完成修改

删除策略路由

1. 点击“操作”一栏中的“删除”图标，弹出删除对话框
2. 点击“确定”按钮完成删除

启用/禁用策略路由规则

点击“是否启用”一栏中的图标，

如果原来是✔，点击后变成✘，表示由启用状态变成禁用，，如果原来是✘，点击后变成✔，表示由禁用状态变成启用。

表 2-11 添加和编辑时参数说明：

域名	说明	和其他界面的关系
源地址和掩码	设置源 IP 地址，可以使用 IP 地址/子网掩码	
目的地址和掩码	设置目的 IP 地址，可以使用 IP 地址/子网掩码	
下一跳地址	设置网关的 IP 地址	
网络接口	接口和下一跳地址须在同一	从网络配置>>网络设备中选

	网段内	取接口

2.6 动态路由

联想网御防火墙的动态路由支持 OSPF 和 PIM-SM 协议。 在配置动态路由之前应确认已完成相关网络接口的配置。OSPF 网络接口仅限制为以太网接口（如 fe1 等）。

2.6.1 OSPF 协议配置

开放最短路径优先协议（OSPF）是一种链路状态路由选择协议。链路状态协议使用最短路径优先（SPF）算法来计算路由。OSPF 配置比较复杂，需要以下五个步骤：

第一步 启动关闭 OSPF

点击屏幕右上命令按钮即可启动或关闭 OSPF。在配置 OSPF 时，无需将 OSPF 重新启动。

第二步 配置路由器 ID 和重发布（可选）

用户根据需要配置路由器 ID 及重发布路由类型。

表 2-12 路由器 ID 和重发布参数说明

域名	说明	和其他界面的关系
路由器 ID	静态设置路由器 ID(RID)，设置成 IP 地址格式	
连接的	重发布连接路由	
RIP	重发布 RIP 路由	
静态	发布静态路由	
BGP	发布 BGP 路由	

第三步 标识区域分配

OSPF 通过采用特定路由器类型控制下的区域来实现分层网络设计的目标。这里支持的路由器类型分为三种：regular, STUB, NSSA。

Regular：包括主干区域（Backbone area，或称 Area 0）及非主干区域（Nonbackbone），非存根区域（Nonstub area）；

STUB：是一个只有单一出口的区域；

NSSA：Not-so-stub 区域，该区域在保留 Stub 区域特性的基础上允许外部路由通过重发布进入该区域。

在配置区域的同时，可以根据需要指定认证方式。认证方式有两种类型，一种是明文形式的认证，一种是 MD5 加密校验和的认证方式。OSPF 认证方式配置分为两个步骤：

1， 在区域配置中指定认证方式；

2， 在接口配置输入认证方式的密码，在后面介绍接口配置时将介绍配置认证密码详细内容。

在配置区域的界面中，用户还可以配置虚拟路径的远端路由。

注意，如果要删除区域，应首先删除网络中相关记录。

表 2-13 区域配置参数说明

域名	说明	和其他界面的关系
区域 ID	区域，设置成 IP 地址格式	
类型	指定该区域路由器类型： Regular;（缺省） STUB; NSSA	
认证	认证方式： none； text： MD5	？
远端路由	虚拟路径的远端路由 ID	

第四步 配置网络到指定区域

配置网络必须确保已完成了相关区域的配置。

表 2-14 网络配置参数说明

域名	说明	和其他界面的关系
网络	正向掩码	
区域	区域 ID	

第五步 配置接口认证机制及计时（可选）

表 2-15 OSPF 配置参数说明

域名	说明	和其他界面的关系
接口名称	定义接口名称	
接口	指定某一以太网接口	
IP	指定端口的 IP 地址，无需输入	
认证方式	None：无认证，缺省； Text: 明文方式； MD5：信息摘要 5 加密校验和认证方式	
明文密码	最大 15 个字节	
MD5 密钥 ID	最大 255	
MD5 密钥	最大 16 个字节	
Hello 时间间隔	缺省值为 10	
Dead 时间间隔	缺省值为 40	

2.6.2 PIM-SM 协议配置

稀疏模式独立组播协议 PIM-SM（Protocol Independent Multicast--Sparse Mode）配置需要三个步骤：

第一步 开启关闭 PIM-SM 服务

第二步 配置静态集合点 RP（Rendezvous Point）

表 2-16 静态集合点配置参数说明

域名	说明	和其他界面的关系
rp	配置汇合点	

第三步 配置多播接口

表 2-17 多播接口配置参数说明

域名	说明	和其他界面的关系
接口	支持多播协议接口。包括以太网接口和 Vlan 子接口	
模式	只支持稀疏模式	
RP 候选者：是否启动	配置是否启动该接口为 rp 候选者	
RP 候选者：优先级	<0－255>配置 rp 候选者优先级	
DR 优先级	<0－4294967294>配置 dr（制定路由器）优先级	

注：
DR 优先级：在多路访问网络中 **PIM** 需要进行 **DR** 选举，**DR** 优先级设定值越大优先级越高。

2.7 UPnP 服务器

本节介绍 UPnP 服务的配置和使用。

UPNP 协议即 Universal Plug and Play，是微软提出的，目的是在网关上建立对动态应用的一种通用的解决方案，在该版本中，我们提供 UPnP 服务，提供与地址转换有关的动态端口支持工作。

UPnP 服务的配置包括三部分内容：UPnP 接口设置，UPnP 规则维护和 UPnP 启动/停止。

UPnP 接口设置：设置 UPnP 服务使用的接口。

UPnP 规则维护：添加、删除、修改可以使用 UPnP 的 IP 地址或地址段。

UPnP 启动/停止：启动和停止 UPnP 服务。

2.7.1 接口设置

本节设置 UPnP 服务使用的接口。

UPnP 服务使用两个接口，外部接口和内部接口。外部接口和内部接口不能相同。

在“网络配置>>UPnP 服务器>>接口设置”界面中可以完成设置 UPnP 接口的功能。

界面开始显示的是当前的接口配置，如果要重新设置，选择新的接口后，点击“确认”按钮完成修改。外部接口和内部接口不能选择同一个接口。

表 2-18 设置时参数说明

域名	说明	和其他界面的关系
外部接口	UPnP 服务使用的外部接口	从网络配置>>网络设备中选取接口
内部接口	UPnP 服务使用的内部接口	从网络配置>>网络设备中选取接口

2.7.2 规则维护

本节用来设置可以使用 UPnP 服务的 IP 地址或地址段。

UPnP 服务可以自动打开通道，默认对所有 IP 都是不允许使用的，只有在这里设置的 IP 地址，才可以使用 UPnP 服务。

在“网络配置>>UPnP 服务器>>规则维护”界面中可以完成以下功能：

1. 添加可以使用 UPnP 的地址
2. 编辑可以使用 UPnP 的地址
3. 删除可以使用 UPnP 的地址

添加可以使用 UPnP 的地址

1. 点击“添加”按钮，进入“UPnP 维护”
2. 添加地址和注释
3. 点击“确定”按钮完成添加

编辑可以使用 UPnP 的地址

1. 点击“操作”一栏中的“编辑”图标，打开“UPnP 维护”界面
2. 执行修改操作
3. 点击“确定”按钮完成修改

删除可以使用 UPnP 的地址

1. 点击“操作”一栏中的“删除”图标，弹出删除对话框
2. 点击“确定”按钮完成删除

表 2-19 添加和编辑时参数说明

域名	说明	和其他界面的关系
名称	地址的名称。必须是 1－20 位字母、数字、减号、下划线的组合。	
地址/掩码	设置 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码	
注释	设置地址规则的注释	

2.7.3 启动/停止

本节用来启动和停止 UPnP 服务。

在 UPnP 服务处于停止状态时，页面显示“启动 UPnP 服务”，点击此按钮，可以启动 UPnP 服务；在 UPnP 服务处于运行状态时，页面显示“停止 UPnP 服务”，点击此按钮，可以停止 UPnP 服务；

只有在“网络配置>>UPnP 服务器>>接口设置”进行了接口设置，才可以启动 UPnP 服务。

2.8 DHCP 服务器

防火墙可以通过 DHCP 协议对局域网其他主机提供动态获取 IP 地址的服务，称为 DHCP 服务器，配置使用方法如下。

配置 DHCP 服务器。使用 DHCP 协议动态分配的 IP 地址可以分为两种情况：由服务器自行决定为某台提出申请的主机分配什么地址；由用户指定为某台主机分配固定的 IP 地址。对于前者，用户必须定义 DHCP 域，即一段 IP 地址，当有主机提出 IP 地址申请时，服务器自动从 DHCP 域中选择一个分配给该主机；对于后者，用户必须指定为某主机分配什么 IP 地址。

DHCP 协议会自动获取默认路由，所以在使用 DHCP 服务时，建议最好删除静态路由中配置的默认路由，而使用自动获取的。

2.8.1 配置 DHCP 域

进入“网络配置>>DHCP 服务器>>DHCP 域配置”中“添加”DHCP 域。

表 2-20 添加和编辑 DHCP 域时参数说明

域名	说明
网络地址	必填项，和“网络掩码”一起决定为哪个子网提供 DHCP 服务。注意，网络地址必须是网段的地址，而不能是主机地址。另外网络地址至少有一个是和安全网关的网络设备是同一网段，否则 DHCP 服务器启动会失败。如果修改了相应网络设备的地址，则必须重新配置和启动 DHCP 服务器。
网络掩码	必填项，和网络地址一起决定子网地址
网关地址	可选项，为 DHCP 客户端配置网关地址
域名	可选项，为 DHCP 客户端配置域名（注意域名中不能有“.”，否则 DHCP 服务器会启动失败）
DNS 服务器	可选项，为 DHCP 客户端配置 DNS 服务器地址
地址范围	必填项，首先必须在地址列表资源中定义地址段（注意，必须是地址段，而非掩码地址或反地址，参考：“资源定义>>地址>>地址列表”），然后在这里选择
备注	可选项，一些说明
VPN 客户端 DHCP over	在客户端和安全网关建立隧道后，一般都会需要指定一个内部 IP 地址，以便于通信和管理，这个 IP 地址就是所谓的虚拟 IP。虚拟 IP 最

IPSec	简单的方法是手工在客户端指定，但这种方法用户很容易会把两个客户端设成同样的虚拟 IP，这样会对正常通信造成影响。因此最好的办法是通过安全网关端的 DHCP 服务器获得虚拟 IP，这时 DHCP 数据交换实际发生在客户端和网关端的 IPSec 隧道内，这就是所谓的“DHCP Over IPSec”。如果不在隧道里使用 DHCP，就不要开启“DHCP Over IPSec”。
VPN 客户端掩码	VPN 客户端虚拟 IP 得子网掩码。

2.8.2 配置静态 IP 地址

进入“网络配置>>DHCP 服务器>>静态 IP 地址”中“添加”静态分配的 IP 地址。

表 2-21 添加和编辑静态 IP 地址时参数说明

域名	说明
主机名称	必填项，要分配固定 IP 地址的主机名称
MAC 地址	必填项，主机的 MAC 地址
IP 地址	必填项，要分配给该主机的 IP 地址。静态分配的 IP 地址生效的前提条件是：设置的主机 IP 地址和该主机对应的物理接口或其别名设备的 IP 地址在同一网段。
备注	可选项，一些说明

2.8.3 控制 DHCP 服务器

进入“网络配置>>DHCP 服务器>>启动/停止服务器”控制 DHCP 服务器。

如果服务器当前未启动，则按钮上显示“启动 DHCP 服务器”按钮，反之显示“停止 DHCP 服务器”。点击按钮完成相应的动作，弹出的对话框提示操作是否正确完成。如果启动失败，请检查定义的 DHCP 域是否正确。

选中“系统启动时即启动 DHCP 服务器”，则防火墙启动时 DHCP 服务器也随之启动。

2.9 HA

联想网御防火墙支持双机热备，负载均衡和会话保护三种工作模式。

双机热备（主动-被动模式）：集群中所有节点的任意对应的业务网口 IP 和 MAC 地址都分别相同。其中一台防火墙（优先级=1）为主节点，处于主动工作中，负责处理所有的网络数据流以及整个集群的控管；其它防火墙节点为从节点，处于热备中，不处理网络数据（但处理主节点广播发出的同步状态表信号）。一旦主节点发生故障，优先级次之的从节点升为主节点，接管原来主节点的工作，保证网络正常通信。

注意：HA 在双机热备模式下，使用透明模式，桥设备的 STP 不能打开。

负载均衡（主动-主动模式）集群中所有节点的任意对应的业务网口 IP 和 MAC 地址都

分别相同，各节点协同工作。其中一台防火墙（优先级=1）是主节点，处于工作中，负责处理部分网络流量以及整个集群的控管；其它防火墙节点为从节点，也处于主动工作中，和主节点一起分担网络流量。一旦某一防火墙节点发生故障后，其负载可以迅速切换到集群中其它防火墙上，保证网络正常通信。

会话保护模式：此模式不同于上面所说的主动－主动模式，主动－被动模式，本模式的各个防火墙分别独立工作，对应的业务口 IP 和 MAC 地址是不同的，节点的优先级也没有主从之分。此模式的防火墙只启用会话保护协议，使得各个节点之间可以进行包过滤状态同步，保证会话状态的相互备份。此模式由于只启用会话保护，因此不具备配置同步、路径监控等功能。本模式主要用于一些不对称的网络环境和冗余网络环境使用。

详细内容请参考手册章节：HA 概念和范例。

2.9.1 HA 基本参数

HA 基本参数包含以下功能

1. 配置 HA 网口参数
2. 配置 HA 基本参数
3. 查看 HA 状态

表 2-22 网口参数说明

属性名称	描述
启用 HA 网口	是否启用 HA 网口，默认是 fe2
启用状态同步	是否启用防火墙包过滤的状态同步功能
HA 网口 IP	HA 网口使用的 IP，集群各个节点的 IP 必须唯一，系统默认使用 fe2 做为 HA 网口，当 HA 网口启用后，网络设备中的 fe2 就为 HA 专用
掩码	IP 掩码

配置 HA 网口地址

1. 输入 HA 网口 IP 地址，选择掩码
2. 点击“确定”按钮完成配置

只配置 HA 网口和选择状态同步不配置 HA 基本参数，也是防火墙 HA 工作模式的一种，即会话保护模式，只进行两台防火墙之间的包过滤状态同步。

注意事项：

HA 网口将使用物理设备 fe2，请在设置 HA 网口前，先确定 fe2 设备是否工作在路由模式下。若 fe2 工作在透明方式下，请先将 fe2 从桥设备中剥离；若 fe2 工作在路由模式，请不要让 fe2 在被 VLAN 设备、VPN 设备等其它设备使用并且不要被防火墙的各种策略和规则使用，以保证 fe2 的专用性，否则会产生功能问题。

配置 HA 基本参数

表 2-23 配置 HA 基本参数

属性名称	描述
启用 HA	是否启用 HA

HA 标识符	1～255，同一集群中的各节点 HA 标识符必须相同
工作模式	双机热备或负载均衡，同一集群中的各节点工作模式必须相同
节点	节点序号，同一集群中节点序号必须唯一

注意：HA 基本参数需要先配置好 HA 网口

查看 HA 状态
点击“查看 HA 状态”按钮，可以查看 HA 状态。

2.9.2 探测网口

提供按 IP 地址和网口进行链路探测的功能。根据探测结果可以调整集群防火墙的失效状态，均衡负载。

探测网口完成以下功能
1. 设置需要探测的网口
2. 查看被探测网口状态

设置需要探测的网口
1. 选择要探测的网口
2. 点击“确定”按钮完成

查看网口状态
1. 点击“查看网口状态”按钮
2. 打开“HA 网口状态列表”界面：

表 2-24 查看网口状态基本参数

属性名称	描述
探测网口	正在探测的网络接口
连接失败节点失效	若探测网络接口连接是失败状态，是否使本防火墙节点失效
网络连接状态	网络接口连接状态

2.9.3 探测周边设备 IP

如果探测周边设备 IP 列表中所有探测失败的 IP 的权重之和达到指定阈值，则此防火墙被自动设为失效状态，便于防火墙双机热备和负载均衡模式下工作状态的切换。

探测周边设备 IP 完成以下功能
1. 指定失效阈值
2. 添加探测周边设备 IP
3. 编辑探测周边设备 IP

4. 删除探测周边设备 IP
5. 查看探测周边设备 IP 状态

指定失效阈值

1. 输入阈值，可以为 1-100 的整数
2. 点击“确定”按钮完成

添加探测周边设备 IP

点击“确定”按钮

各域说明如下

表 2-25 添加、编辑探测 IP 基本参数

域名	说明
探测周边设备 IP	探测周边设备 IP
权重	在所有探测周边设备中的权重
从该网口探测	从哪个网络接口探测

配置各域后，点击“确定”按钮完成

注意事项：需要探测的 IP 和网口要在同一网段。探测的 IP 指的是双机热备机器以外的地址（不包括双机热备机器的地址）。

编辑探测周边设备 IP

1. 点击“操作”一栏中的“编辑”图标，打开探测周边设备 IP 维护界面
2. 执行修改操作
3. 点击“确定”按钮完成修改

删除探测周边设备 IP

1. 点击“操作”一栏中的“删除”图标，弹出删除对话框
2. 点击“确定”按钮完成删除

查看探测周边设备 IP 状态

点击“查看探测周边设备 IP 状态”按钮，打开“探测周边设备 IP 状态”

第3章 策略配置

本章是防火墙配置的重点。制定符合安全需求的策略是保证防火墙真正起到“防火”作用的基础。 配置错误的安全规则不仅会使防火墙形同虚设，甚至有可能妨碍对网络正常功能的使用。

3.1 安全选项

安全选项提供防火墙可设置的一些全局安全策略，包括包过滤策略、抗攻击策略、IP/MAC 检查开关和是否允许除 IP 和 ARP 之外的其他非 IP 协议通过。这些参数对整个防火墙生效。

3.1.1 包过滤策略

包过滤缺省允许策略：包过滤缺省策略的设置，选中为允许，不选为禁止。包过滤缺省策略是当所有的用户添加的包过滤规则都没有被匹配时所使用的策略。如果包过滤缺省策略是禁止，用户添加的包过滤规则应该是允许哪些连接可以通过；如果包过滤缺省策略是允许，用户添加的包过滤规则应该是禁止哪些连接不能通过。

严格的状态检测：选中为启用，不选为禁止。仅针对 TCP 连接。如果启用，只为 SYN 标志的数据包创建连接状态，除此之外的任何 TCP 数据包都不创建状态。此外，启用严格的状态检测，还可以防止 ACK 扫描攻击，建议用户选中。需要使用“策略配置>>安全规则>>包过滤规则”中的“长连接”属性，设置连接建立的时间时，就必须选中此项属性“策略配置>>安全规则>>包过滤规则”。在特殊网络环境下，如单边路由的环境下，防火墙可能无法收到所有三次握手的数据包，此时就不能选中严格的状态检测。

包过滤策略中还包括一项高级设置：规则配置立即生效：启用后为规则优先（缺省是状态优先）。如果不启用，当一个连接在防火墙上的建立起来后，设置了与原有的规则相反的规则，则此时数据包仍能够根据建立的状态表通过防火墙；如果启用，则此时数据包根据设定的规则将无法通过防火墙。重新设置规则可能会造成已有连接中断。建议不启用。

3.1.2 抗攻击

设定全局的抗攻击选项，包括抗地址欺骗攻击，抗源路由攻击，抗 Smurf 攻击，抗 LAND 攻击，抗 Winnuke 攻击，抗 Queso 扫描，抗 NMAP 扫描，抗 NULL 扫描，抗圣诞树攻击，和抗 FIN 扫描。选中后，防火墙将对所有流经的数据包进行抗攻击检查。

表 3-1 10 种攻击的名词解释

名称	解释
地址欺骗攻击	修改数据包的包头，以使它看起来是从一个可信任的主机发起的，从而使之可通过路由器或防火墙。
源路由攻击	修改数据包包头的路由选项，把数据包路由到它可以控制的路由

	器上，从而进行路由欺骗或者得到该数据包的返回信息。
Smurf 攻击	收到包的 IP 地址都是目标网络的广播地址，如果网内存在大量主机的 ICMP 的请求回应的包。这种洪水般的广播流量会耗费掉所有可用带宽，使得通信中断。
LAND 攻击	构造错误的 SYN 请求连接包，使得目标主机发送的 ACK 应答确认包发给自己本身，形成重复的循环过程。
Winnuke 攻击	利用 Windows 9X 的 NetBIOS 中一个 OOB(Out of Band)的漏洞而进行的，原理是通过 TCP/IP 协议传递一个 Urgent 数据包到计算机的 137、138 或 139 端口，当计算机收到这个数据包之后就会瞬间死机或蓝屏，不重新启动计算机就无法继续使用 TCP/IP 协议来访问网络。
Queso 扫描	Queso 是由 savage@apostols.org 提供的免费端口扫描工具。这里的抗 Queso 扫描是指抗利用 Queso，通过 TCP/IP 堆栈特征探测远程操作系统的扫描。
SYN/FIN 扫描	SYN/FIN 扫描向目标发送 SYN/FIN 标记的 TCP 包，用以探测开启端口和操作系统特征，扫描工具 NMAP 常使用此方法进行扫描活动。
NULL 扫描	TCP Null 扫描是 FIN 扫描的变种。Null 扫描关闭 TCP 包所有标记。当一个这种数据包到达一个关闭的端口，数据包会被丢掉，并且返回一个 RST 数据包。否则，若是打开的端口，数据包只是简单的丢掉，不返回 RST。
圣诞树攻击	TCP Xmas 扫描是 FIN 扫描的变种。Xmas 扫描打开 FIN，URG 和 PUSH 标记。当一个这种数据包到达一个关闭的端口，数据包会被丢掉，并且返回一个 RST 数据包。否则，若是打开的端口，数据包只是简单的丢掉，不返回 RST。
FIN 扫描	扫描器向目标主机端口发送 FIN 包。当一个 FIN 数据包到达一个关闭的端口，数据包会被丢掉，并且返回一个 RST 数据包。否则，若是打开的端口，数据包只是简单的丢掉，不返回 RST。

3.1.3 IP/MAC 检查

开启全局的 IPMAC 绑定检查。此选项需要和设备上的 IPMAC 绑定检查同时启用才能生效 IPMAC 绑定检查功能。

3.1.4 允许所有非 IP 协议

通过该界面，您可以控制所有非 IP 协议都通过；列出的 40 种协议是否通过、自定义协议是否通过、未列出的协议是否通过，。

设定是否允许除 IP 和 ARP 外的以太网协议通过。协议类型包括 42 种固定协议（其中 IP 和 ARP 不可编辑）和 5 种自定义协议。自定义协议的维护界面如下图示：

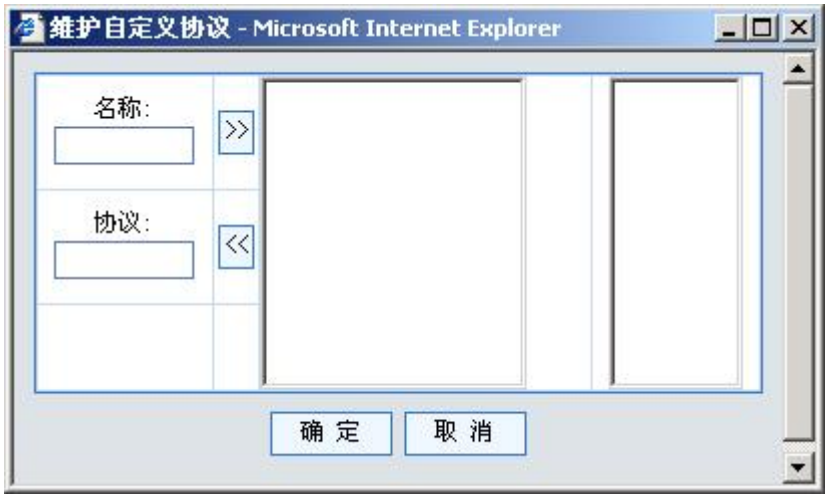


图 3-1 安全选项的自定义协议配置

其中：名称是 8 位字母和数字的组合，协议号范围是 1-65535，且 3 保留。
还可以设定除以上协议外，是否允许其他类型的数据包通过。

表 3-2 42 种已定义非 IP 协议表

名称（协议号）	说明
LOOP(96)	Ethernet Loopback packet
PUP(512)	Xerox PUP packet
PUPAT(513)	Xerox PUP Addr Trans packet
IP(2048)	Internet Protocol packet
X25(2053)	CCITT X.25
ARP(2054)	Address Resolution packet
BPQ(2303)	G8BPQ AX.25 Ethernet Packet
IEEEPUP(2560)	Xerox IEEE802.3 PUP packet
IEEEPUPAT(2561)	Xerox IEEE802.3 PUP Addr Trans packet
DEC(24576)	DEC Assigned proto
DNA_DL(24577)	DEC DNA Dump/Load
DNA_RC(24578)	DEC DNA Remote Console
HDLC(25)	HDLC frames
LAT(24580)	DEC LAT
DIAG(24581)	DEC Diagnostics
CUST(24582)	DEC Customer use
SCA(24583)	DEC Systems Comms Arch
RARP(32821)	Reverse Addr Res packet
CONTROL(22)	Card specific control frames
LOCALTALK(9)	Localtalk pseudo type
MOBITEX(21)	Mobitex
IPX(33079)	IPX over DIX
IPV6(34525)	IPv6 over bluebook

AX25(2)	Dummy protocol id for AX.25
802_2(4)	802.2 frames
EDP2(34978)	Coraid EDP2
802_3(1)	Dummy type for 802.3 frames
SNAP(5)	Internal only
PPP_DISC(34915)	PPPoE discovery messages
ATMMPOA(34892)	MultiProtocol Over ATM
DDCMP(6)	DEC DDCMP: Internal only
AARP(33011)	Appletalk AARP
ATMFATE(34948)	Frame-based ATM Transport over Ethernet
WAN_PPP(7)	Dummy type for WAN PPP frames
PPP_MP(8)	Dummy type for PPP MP frames
ECONET(24)	Acorn Econet
TR_802_2(17)	802.2 frames
IRDA(23)	Linux-IrDA
DNA_RT(24579)	DEC DNA Routing
PPP_SES(34916)	PPPoE session messages
ATALK(32923)	Appletalk DDP
PPPTALK(16)	Dummy type for Atalk over PPP

3.2 安全规则

安全规则提供对以下规则的配置管理：

- 代理规则
- 端口映射规则
- IP 映射规则
- NAT 规则
- 包过滤规则

防火墙的基本策略：防火墙的缺省策略是没有明确被禁止的行为都是被**允许**的。在安全选项中可以修改包过滤的缺省策略。

安全策略是核心：根据管理员定义的安全规则完成数据包控制，策略包括“允许通过”、“禁止通过”、“代理方式通过”、“NAT 方式通过”、“端口映射方式通过”、“IP 映射通过”防火墙。

用户策略是辅助：根据管理员定义的基于角色控制的用户策略，并与安全规则策略配合完成强制访问控制，包括限制用户在什么时间、什么 IP 地址可以登录防火墙系统，以及该用户通过认证后能够使用的服务。

状态检测是主线：安全策略规则与防火墙状态表紧密结合，共同完成对数据包的动态过滤。

资源定义是关键：提供基于资源定义的安全策略配置。资源包括地址和地址组、NAT 地址池、服务器地址、服务（源端口、目的端口、协议）和服务组、时间和时间组、用户和用户组（包括用户策略：如登录时间与地点，源 IP/目的 IP、目的端口、协议等）、URL 过

滤策略。最大限度提供方便性与灵活性。

用户认证、时间控制：双向 NAT（网络地址转换 NAT、端口映射 PAT、IP 映射 VIP），通过包过滤规则支持用户认证、时间调度。因此，下一条端口映射、IP 映射、NAT 规则（代理规则除外），必须再下一条相应的包过滤规则才能生效。

防火墙按顺序匹配规则列表：防火墙规则根据作用顺序分为代理、端口映射、IP 映射、包过滤、NAT 规则五类。其中代理规则是最优先生效的规则，最后为 NAT，这几类规则在界面上排列的顺序也体现了这一顺序，（需要注意的是，端口映射与 IP 映射中的隐藏内部主机规则，要比代理规则优先生效）。匹配了某类规则后，是否再匹配其它类型规则如下图所示，数据包匹配了代理规则，则根据代理规则对数据包进行相应处理，而不再匹配其他类型的规则；如果没有匹配代理，则去匹配端口映射和 IP 映射规则。而无论数据包是否匹配端口映射和 IP 映射的规则，都会去匹配包过滤规则，根据包过滤规则的设置，若允许（包括包过滤规则允许，包过滤认证通过和包过滤 IPSEC 通过，或没有匹配任何包过滤规则，而在“策略配置>>安全选项”中“包过滤策略”中选中包过滤缺省允许）则去匹配 NAT 规则。如果匹配到 NAT 规则则进行 NAT，否则数据包通过防火墙。

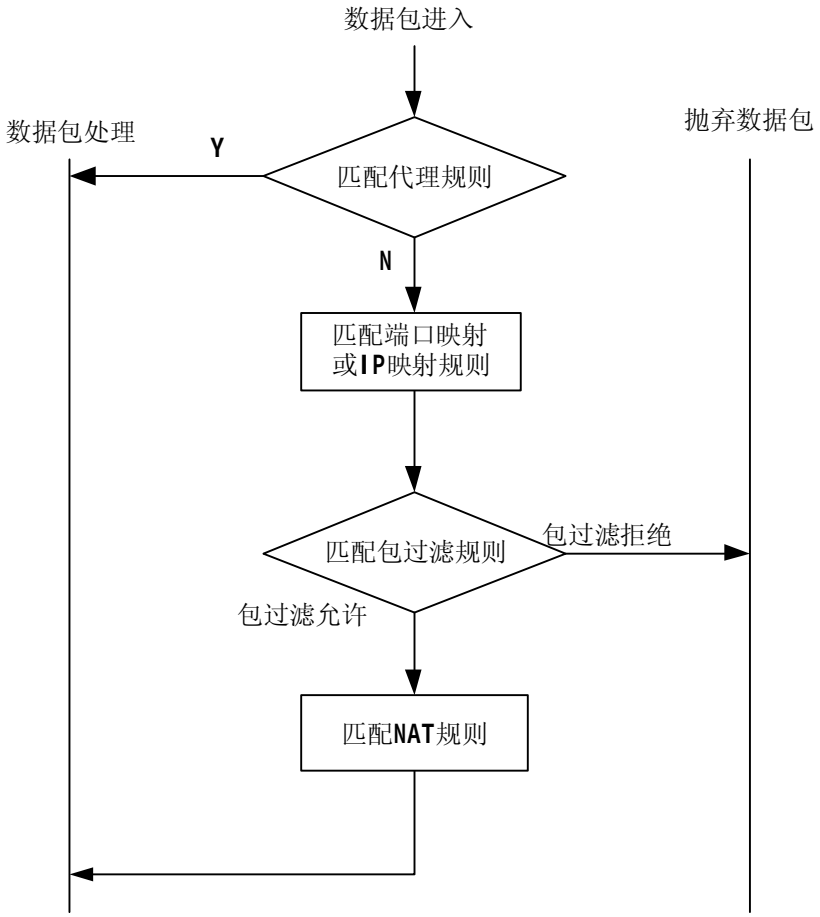


图 3-2 规则生效顺序

每类中的规则根据规则的顺序生效，当匹配了某类型规则中的一条规则时，将根据该条规则对包进行处理，而不会匹配该类规则中其他规则。

提供基于物理设备的安全功能控制：可以根据用户需求，将防火墙的安全功能定义在防

火墙各个网络接口上。当该网口接收数据包时，可以按管理员配置策略进行过滤，如工作模式选择、VLAN 及 TRUNK 支持等。

表 3-3 安全规则图标说明 1

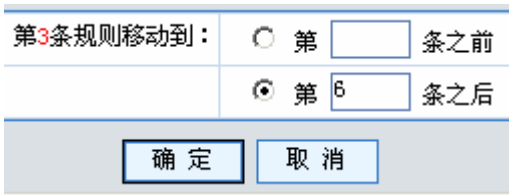
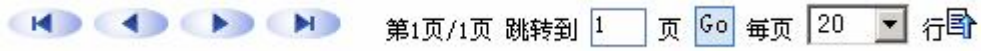
域名	说明
	包过滤规则，允许访问
	包过滤规则，禁止访问
	具有记录日志功能
	生效状态，如果点击该图标，则改变该条规则状态，即变成无效状态
	无效状态，如果点击该图标，则改变该条规则状态，即变成生效状态
	编辑，一次只能编辑一条规则
	复制，一次只能复制一条规则
	规则的顺序非常重要，有时，需要把一条现有的规则移动更合适的位置，因此提供了“移动”按钮。 操作流程： 1. 选中希望移动的规则（只能选中一条） 2. 点击“移动”按钮 3. 弹出移动对话框，如图所示：  4. 填入希望移到的位置 5. 点击“确定”即可 注意： 1. 如果希望移动到的位置大于当前最大序号，则移动到最后。 规则移动以后，其它规则相应调整位置，以保证规则的顺序和连续
	删除，可以选择删除一条或多条规则

表 3-4 安全规则图标说明 2

域名	说明

代理规则	设置代理规则
端口映射规则	设置端口映射规则
IP 映射规则	设置 IP 映射规则
包过滤规则	设置包过滤规则
NAT 规则	设置 NAT 规则

分页显示工具条，如下图：



详细说明请参见本手册“资源定义通用功能介绍”。

表 3-5 安全规则数据域说明

域名	说明
序号	已定义规则的序号，表示规则的先后顺序
规则名	已定义规则的名称
源地址	规则的源地址
目的地址	规则的目的地址
服务	规则的服务
类型	安全规则的访问控制类型， 包括： （1） 代理 （2） 端口映射 （3） IP 映射 （4） 包过滤 禁止 （5） 包过滤 允许 （6） 包过滤 认证 （7） 包过滤 IPSEC （8） NAT 规则（网络地址转换）
选项	安全规则是否记录日志的选项功能： 如果记录日志，则显示图标
生效	表示该规则为生效状态，点击 以后该规则变成无效状态 表示该规则为无效状态，点击 以后该规则变成生效状态

3.2.1 代理规则

其中的 HTTP 代理，FTP 代理，Telnet 代理，POP3 代理是透明的代理规则，即源地址/目的地址之间的信息会自动地由运行在防火墙上的代理程序转发，所以在客户端浏览网页时不必指定所使用的代理服务器（即防火墙）地址。其它代理都需要在客户端上指定代理服务器的地址。配置代理规则时，请先确认相应的代理服务器是否已经启用。使用代理服务，可以监控源地址/目的地址间的信息，并进行相应的访问控制和内容过滤。同时，代理服务由于处理的内容多，所以传输效率也不如相应的包过滤规则高。

注意：代理规则优先于包过滤规则，如果配置了代理规则，就意味着地址、端口、协议完全相同的包过滤规则失去了作用。所以在配置代理规则时请考虑防火墙整体的安全策略。

代理类型包括：HTTP 代理，FTP 代理，Telnet 代理，SMTP 代理，POP3 代理，SOCKS 代理，DNS 代理，ICMP 代理，MSN 代理，以及自定义代理。各种类型代理的启用状态在“策略配置>>代理服务”中配置。配置了启用代理后，还需要在“策略配置>>安全规则>>代理规则”中设置相应的规则，才可以使用代理服务。

表 3-6 代理规则配置项说明

域名	说明
规则名	安全规则的名称。 规则名必须是 1－20 位字母、数字、减号、下划线的组合。 规则名可以重复。 默认规则名为“proxy”+ 默认序号。 如果把规则名置空，则使用默认规则名“proxy”
序号	输入新增策略规则的序号。 防火墙按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。 若该数字与已定义的规则序号有重复，则防火墙会自动将原策略规则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。 若不修改界面中序号，即为添加到最后。 如果序号大于已有规则总数加 1，即为添加到最后。
源地址	可选内容包括：“资源定义>>地址>>地址列表”和“资源定义>>地址>>地址组”中定义的所有资源，及”自定义”。 当选择“自定义”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。 默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0，以此来表示任意地址。
目的地址	形式同源地址
源端口	源端口可以用英文逗号,分割表示多个端口，或者用英文冒号:分割表示端口段。 两种分割方式不能同时使用。
源 MAC	源 MAC 地址，格式为 aa:bb:cc:dd:ee:ff，其中用英文冒号:分割
流入网口	限制网络数据包的流入网口，可以防止 IP 欺骗。 可选内容包括：any 和所有已激活的网口。 默认值为 any，表示不限制接收网口。

	如果工作在透明模式，必须选择相应的物理网口如 fe1 如果不能确定流入网口或工作在混合模式，建议选择 any
代理类型	当策略为“代理”时，必须选择该项。 可选择内容包括：http 代理、ftp 代理、telnet 代理、smtp 代理、pop3 代理、socks 代理、DNS 代理、ICMP 代理、MSN 代理、自定义代理。各类型的代理在“策略配置>>代理服务”中配置。
时间调度	生效的安全规则将在指定的时间段内为生效状态且在其它时间段为失效状态，可选内容包括：“资源定义>>时间>>时间列表”和“资源定义>>时间>>时间组”中定义的所有资源。
服务	可选内容包括：any，在“资源定义>>服务>>服务列表”中配置的基本服务、ICMP 服务、动态服务，以及“资源定义>>服务>>服务组”。 默认值为 any，表示源端口任意、目的端口任意、协议任意。
日志记录	强制要求匹配该条规则的数据包是否需要记录日志
备注	规则注释

3.2.2 端口映射规则

提供对外公开的服务，将用户对该服务公开地址的访问转换到内部网络上另一个内部地址的某个端口。

当管理员配置多个服务器时，提供针对服务器的负载均衡。

注意：设置一条端口映射规则，如果没有选择“包过滤缺省策略通过”， 还必须再设置一条相应的包过滤规则才能生效。方法如下：包过滤规则的源地址是端口映射规则的源地址，包过滤规则的目的地址是端口映射规则的内部地址。服务是端口映射规则的内部服务。

端口映射规则的含义如下：

把客户端对防火墙对“公开地址”，“对外服务”的访问，转换成对“内部地址”，“内部服务”的访问。同时，源地址可以转换成防火墙的某个接口地址，当然，也可以选择“不转换”。在配置端口映射规则时，还可以选择客户端到“公开地址”的“流入网口”和它的“源端口”。如果选择了做“源地址”转换，还可以选择源地址转换后的“流出网口”。

表 3-7 端口映射规则配置项说明

域名	说明
规则名	安全规则的名称。 规则名必须是 1－20 位字母、数字、减号、下划线的组合。 规则名可以重复。 默认规则名为“pnat”+ 默认序号。 如果把规则名置空，则使用默认规则名“pnat”
序号	输入新增策略规则的序号。 防火墙按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。 若该数字与已定义的规则序号有重复，则防火墙会自动将原策略规则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。 若不修改界面中序号，即为添加到最后。 如果序号大于已有规则总数加 1，即为添加到最后。

源地址	可选内容包括：“资源定义>>地址>>地址列表” 中的地址资源、“资源定义>>地址>>地址组”中的地址资源，及“自定义”。 当选择“自定义”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。 默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0，以此来表示任意地址。
源地址转换	可选内容包括：不转换，“资源定义>>地址池”中的地址资源和“网络配置>>网络设备”中的防火墙 IP 地址。
源端口	源端口可以用英文逗号,分割表示多个端口，或用英文冒号:分割表示端口段。 两种分割方式不能同时使用。
公开地址	用户可以访问的 IP 地址，即指定可以访问的目的 IP 地址。 必须是单个 IP 地址，不能是网段。 可选内容包括：“网络配置>>网络设备”中的防火墙 IP 地址。
内部地址	用户实际访问的 IP 地址，即指定实际访问的目的 IP 地址。 一般是单个 IP 地址。当是多个 IP 地址或网段时，一般用于服务器的负载均衡。在不同的源地址访问中，映射的服务器地址采用轮循算法。对相同源地址只采用同一个服务器处理，即源地址相同的不同连接并不采用轮循算法。 可选内容包括：“资源定义>>地址>>服务器地址”中的地址资源。 参考“资源定义>>地址>>服务器地址”中的配置。
对外服务	用户可以访问的服务，即指定可以访问的目的端口。 可选内容包括：“资源定义>>服务>>服务列表”中的基本服务、ICMP 服务、动态服务。 参见表 5-8：对外服务与内部服务选择的服务资源要严格遵守的约定。
内部服务	用户实际访问的服务，即指定实际访问的目的端口。 可选内容包括：“资源>>服务>>服务列表”中的基本服务、ICMP 服务、动态服务。 参见表 5-8：对外服务与内部服务选择的服务资源要严格遵守的约定。
流入网口	检查流入网口可以防止 IP 欺骗。 可选内容包括：所有已激活的网口，或者不选择代表全部接口。 默认值为 any，表示不限制接收网口。 如果工作在透明模式，必须选择相应的桥设备如 brg0 如果不能确定流入网口或工作在混合模式，建议选择 any
流出网口	流出网口检查，当选择源地址转换时才能选择。 在透明模式下请选择桥设备。 如果不能确定流出网口或工作在混合模式，建议选择 any
允许通过	指的是数据包通过端口映射规则，但不做任何地址转换。
日志记录	强制要求数据包是否需要记录日志
隐藏内部地址	如果取消选中，既能通过公开地址和端口访问内部服务器，也可以直接访问服务器；如果选中，只能通过公开地址和端口访问内部服务器。
备注	规则注释

注意：端口映射中的隐藏内部主机规则，要比代理规则优先生效。

表 3-8 公开服务与内部服务选择的服务资源要严格遵守的约定

资源定义中的服务资源		
服务		服务组
基本服务	只能使用一个服务条目 协议类型必须同为 TCP 或同为 UDP 内部服务的目的端口只能用一个	不支持
动态服务	协议类型一致，但不支持 RTSP	
ICMP	N/A	

3.2.3 IP 映射规则

提供对外公开的服务，将用户对某个外部公开地址的访问转换到另一个内部地址。

当管理员配置多个服务器时，提供针对服务器的负载均衡。

注意：下一条 IP 映射规则，如果没有选择“包过滤缺省策略通过”，还必须再下一条相应的包过滤规则才能生效。方法如下：包过滤规则的源地址是 IP 映射规则的源地址，包过滤规则的目的地址是 IP 映射规则的内部地址。

注意：如果源地址包含管理主机，公开地址是防火墙的管理 IP，该管理主机将不能管理防火墙。

IP 映射规则与端口映射规则类似，它的含义如下：

把客户端对防火墙“公开地址”的访问转换成对“内部地址”的服务器的访问。同时，源地址可以转换成防火墙的某个接口地址，当然，也可以选择“不转换”。在配置 IP 映射规则时，可以选择客户端到公开地址的“流入网口”，如果选择了做“源地址”转换，还可以选择源地址转换后的“流出网口”。

IP 映射规则和端口映射规则属于目的地址转换。它们的区别是：端口映射只对指定端口的连接做地址转换，而 IP 映射对特定 IP 地址的所有端口都做转换。

表 3-9 IP 映射规则配置项说明

域名	说明
规则名	安全规则的名称。 规则名必须是 1－20 位字母、数字、减号、下划线的组合。 规则名可以重复。 默认规则名为“vip”+ 默认序号。 如果把规则名置空，则使用默认规则名“vip”
序号	输入新增策略规则的序号。 防火墙按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。 若该数字与已定义的规则序号有重复，则防火墙会自动将原策略规则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。 若不修改界面中序号，即为添加到最后。 如果序号大于已有规则总数加 1，即为添加到最后。
源地址	可选内容包括：“资源定义>>地址>>地址列表” 中的地址资源、“资源定义>>地址>>地址组”中的地址资源，及“自定义”。 当选择“自定义”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。 默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0，以此来表示任意地址。

源地址转换	可选内容包括：不转换，“资源定义>>地址池”中的地址资源、“网络配置>>防火墙 IP”中的 IP 地址资源。
公开地址	用户可以访问的 IP 地址，即指定可以访问的目的 IP 地址。 必须是单个 IP 地址，不能是网段。 可选内容包括：“网络配置>>网络设备”中的防火墙 IP 地址。
内部地址	用户实际访问的 IP 地址，但用户并不知道这个 IP 地址。由防火墙系统将针对公开地址的访问转换为向内部地址的访问。 一般是单个 IP 地址。当是多个 IP 地址或网段时，一般用于服务器的负载均衡。 可选内容包括：“资源定义>>地址>>服务器地址”中的地址资源。 具体内容请参考“资源定义>>地址>>服务器地址”中的配置。
流入网口	检查流入网口可以防止 IP 欺骗。 可选内容包括：所有已激活的网口，或者不选择代表全部接口。 默认值为 any，表示不限制接收网口。 如果工作在透明模式，必须选择相应的桥设备如 brg0 如果不能确定流入网口或工作在混合模式，建议选择 any
流出网口	流出网口检查，当选择源地址转换时才能选择。 在透明模式下请选择桥设备。 如果不能确定流出网口或工作在混合模式，建议选择 any
允许通过	指的是数据包通过 IP 映射规则，但不做任何地址转换。
日志记录	是否要求记录日志
隐藏内部地址	如果取消选中，既能通过公开地址访问内部服务器，也可以直接访问服务器； 如果选中，只能通过公开地址访问内部服务器。
备注	规则注释

注意：IP 映射中的隐藏内部主机规则，要比代理规则优先生效。

3.2.4 包过滤规则

提供基于状态检查的动态包过滤。包过滤规则决定了特定的网络包能否通过防火墙。同时它也提供相关的选项以保护网络免受攻击。它支持的协议包括基本协议（如 HTTP，Telnet，SMTP 等）、ICMP、动态协议（如 H.323，FTP，SQLNET 等）。

表 3-10 包过滤规则配置项说明

域名	说明
规则名	安全规则的名称。 规则名必须是 1－20 位字母、数字、减号、下划线的组合。 规则名可以重复。 默认规则名为“pf”+ 默认序号。 如果把规则名置空，则使用默认规则名“pf”
序号	输入新增策略规则的序号。 防火墙按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。

	若该数字与已定义的规则序号有重复，则防火墙会自动将原策略规则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。 若不修改界面中序号，即为添加到最后。 如果序号大于已有规则总数加 1，即为添加到最后。
源地址	可选内容包括：“资源定义>>地址>>地址列表”和“资源定义>>地址>>地址组”中定义的所有资源，及”自定义”。 当选择“自定义”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。 默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0，以此来表示任意地址。
目的地址	形式同源地址
源端口	源端口可以用英文逗号分割表示多个端口，或用英文冒号分割表示端口段。两种分割方式不能同时使用。如果资源定义中定义的服务资源也包含了源端口，则以此处规则定义的源端口为准。
源 MAC	源 MAC 地址
流入网口	限制网络数据包的流入网口，可以防止 IP 欺骗。 可选内容包括：any 和所有已激活的网口。 默认值为 any，表示不限制接收网口。 如果工作在透明模式，必须选择相应的物理网口如 fe1 如果不能确定流入网口或工作在混合模式，建议选择 any
流出网口	流出网口检查，当选择源地址转换时才能选择。 在透明模式下请选择桥设备。 如果不能确定流出网口或工作在混合模式，建议选择 any
动作	匹配到本条安全规则的数据包可以执行四种过滤策略：“允许”，“禁止”，“IPSec”。 动作为 IPSec 的规则首先允许符合该规则的数据包通过，同时允许符合该规则的数据包被加密，是否加密仍然依赖于 VPN 隧道的配置。
时间调度	生效的安全规则在指定的时间段内为生效状态，在其它时间段为失效状态，可选内容包括：“资源>>时间>>时间列表”和“资源>>时间>>时间组”中定义的所有资源。
服务	可选内容包括：any，在“资源定义>>服务>>服务列表”中配置的基本服务、ICMP 服务、动态服务，以及“资源定义>>服务>>服务组”。 默认值为 any，表示源端口任意、目的端口任意、协议任意。
长连接	设定该条规则可以支持的长连接时间。0 为不限时，限时的有效范围是 30-288000 分钟。如果希望在指定的时间之后断开连接，请启用“安全策略>>安全选项”中的“严格的状态选择”。
深度过滤	生效的安全规则（动作只能为“允许”、“IPSEC”）执行深度过滤，可选择在“资源定义>>深度过滤”中已定义的深度过滤策略对数据包进行应用层过滤。 对数据包进行应用层过滤会影响系统的处理性能，建议一般情况下不要启用深度过滤。可以在下拉框中选择“无”，从而不启用深度过滤。
认证用户组	对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到防火墙上进行认证，则丢弃该包，否则让该包通过。
P2P 过滤	对满足条件的数据包进行 BT 过滤，Emule 和 Edonkey 过滤,只在包过滤允

	许的情况下可用，至少选择 BT 过滤，Emule 和 Edonkey 过滤其中的一个时，才可以选择纪录 P2P 过滤日志.
包过滤日志	强制要求匹配该条规则的数据包是否需要记录包过滤日志
抗攻击	包括四种抗攻击。注意：TCP 服务可以选择抗 Syn Flood 攻击；UDP 服务可以选择抗 UDP Flood 攻击；ICMP 服务可以选择 ICMP Flood 和 Ping of Death 攻击。也可以在一条规则中，设置符合此规则服务的多个抗攻击选项。针对四种抗攻击，详细说明如下： 当允许 **TCP** 规则时，选择了抗 **Syn Flood** 攻击，防火墙会对流经的带有 **Syn** 标记的数据进行单独的处理。抗 **Syn Flood** 攻击之后的输入框填写的数值的具体含义如下：个位数为保留数字，**0-9** 分别代表抗攻击强度，从弱到强。设置数字的位数如果超过两位，则该数字减去个位的数字表示限制每秒通过的能够真正建立 **TCP** 连接的带有 **Syn** 标志数据包的个数，此个数是真正可以建立 **TCP** 连接的数目。如果设置为 **0**，表示每秒通过的带有 **Syn** 标志的数据包大于 **90**，才进行能否真正建立 **TCP** 连接；如果设置为 **1**，表示每秒通过的带有 **Syn** 标志的数据包大于 **80**，才进行能否真正建立 **TCP** 连接；如果设置为 **9**，表示通过的带有 **Syn** 标志的数据包都经过了防火墙的判断，确认是可以建立真正 **TCP** 连接的数据包。 当允许 **UDP** 规则时，选择了抗 **UDP Flood** 攻击，防火墙会对流经的 **UDP** 数据进行单独的处理。抗 **UDP Flood** 攻击之后的输入框填写的数值的具体含义是限制每秒通过的 **UDP** 数据包的个数。 当允许 **ICMP** 规则时，选择了抗 **ICMP Flood** 攻击，防火墙会对流经的 **ICMP** 数据包进行单独的处理。抗 **ICMP Flood** 攻击之后的输入框填写的数值的具体含义是限制每秒通过的 **ICMP** 数据包的个数。 当允许 **ICMP** 规则时，选择了抗 **Ping of Death** 攻击，防火墙会对流经的 **ICMP** 数据包进行单独的处理。含有 **Ping of Death** 攻击特征类型的数据包将被过滤掉。
备注	规则注释

3.2.5 NAT 规则

NAT 实现内部网络地址转换为外部网络 **IP** 地址，将内部网络和外部网络隔离开，内部用户可通过一个或多个外部 **IP** 地址与外部网络通信。

用户可通过安全规则设定需要转换的源地址（支持网络地址范围）、源端口。此处的 **NAT** 转换通信的源地址，因此也被称作正向 **NAT**，用于区别转换目的地址的 **IP** 映射和端口映射。正向 **NAT** 也可以是动态 **NAT**，即通过系统“资源定义>>地址>>地址池”定义的 **NAT** 地址池，支持多对多，多对一，一对多的地址转换关系。

注意：设置一条 NAT 规则，必须再设置一条相应的包过滤规则才能生效。方法如下：包过滤规则的源地址是 NAT 规则的源地址，包过滤规则的目的地址是 NAT 规则的目的地址。

表 3-11 NAT 规则配置项说明

域名	说明
规则名	安全规则的名称。 规则名必须是 1－20 位字母、数字、减号、下划线的组合。

	规则名可以重复。 默认规则名为“nat”+ 默认序号。 如果把规则名置空，则使用默认规则名“nat”
序号	输入新增策略规则的序号。 防火墙按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。 若该数字与已定义的规则序号有重复，则防火墙会自动将原策略规则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。 若不修改界面中序号，即为添加到最后。 如果序号大于已有规则总数加 1，即为添加到最后。
动作	动作可选“源地址转换”，“伪装”或“允许通过”。如果选“源地址转换”，可以手动选择“源地址转换为”；如果选择“伪装”，系统根据路由自动选择转换后的地址；如果选择“允许通过”， 则数据包通过 IP 映射规则，但不做任何地址转换。 注意：在透明模式下选择伪装必须给桥设备配置同网段 IP 地址。如果目的地址不是同网段地址，还必须给系统配置相应的路由信息，并且此路由必须基于桥设备，否则无法完成伪装，只能使用源地址转换功能，指定转换后的地址。
源地址	可选内容包括：“资源定义>>地址>>地址列表” 中的地址资源、“资源定义>>地址>>地址组”中的地址资源，及“自定义”。 当选择“自定义”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。 默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0，以此来表示任意地址。
源地址转换	可选内容包括：“资源定义>>地址池”中的地址资源和可选内容包括：“网络配置>>网络设备”中的防火墙 IP 地址。 注意：当防火墙地址发生了变化，规则不会自动更新，请重新刷新一下。
目的地址	形式同源地址
服务	可选内容包括：any，“资源定义>>服务>>服务列表”中的基本服务、ICMP 服务、动态服务，以及“资源定义>>服务>>服务组”中的服务资源。 默认值为 any，表示源端口任意、目的端口任意、协议任意。
流出网口	流出网口检查，当选择源地址转换时才能选择。 在透明模式下请选择相应的物理设备。 如果不能确定流出网口或工作在混合模式，建议选择 any
日志记录	强制要求是否需要记录日志
备注	规则注释

注意：如果使用拨号设备上 internet，则配置 NAT 规则时，请选择“伪装”，系统根据路由自动选择转换后的地址。如果 NAT 规则引用拨号设备地址，防火墙重启后，如没有拨号，则 NAT 规则仍使用原拨号设备地址进行 NAT。

3.2.6 按条件查询功能

通过点击界面右侧的按条件查询这个超级链接，可以转到相应的查询页面，代理规则，端口映射规则，**IP** 映射规则，包过滤规则，**NAT** 规则都有自己的相应的查询页面。

由于每一类规则在添加的时候，添加的参数有很大的差异，所以每一类规则在查询的时候，查询条件也是相应不一样的。所有的查询条件的说明请参考本手册 **5.2.1-5.2.5** 的每一类规则的规则配置项表。

就拿包过滤规则查询来说，查询包含了按照序号、规则名、源地址、目的地址、服务、用户认证组、动作、备注这个查询的条件，其中，如果选择了序号查询，则其他的条件全部置成不能够输入的状态，因为根据序号可以明确的指定一条规则，如果没有输入序号，规则名、源地址、目的地址、备注，这几项采用了模糊匹配查询的原则，而服务和动作，则只能够分别从下拉列表中选择和单选钮中选择。如果采用了非序号的查询方式，查询的结果是根据满足规则名、源地址、目的地址、服务、用户认证组、动作、备注所有输入条件的情况下输出结果的。规则名、源地址、目的地址、服务、用户认证组、动作、备注都是可选择的输入，如果哪一项没有输入，就不把那一项当作查询条件。

其他的代理规则，端口映射规则，**IP** 映射规则，**NAT** 规则的查寻和包过滤规则的查询是一样的，只不过查询条件有一定的差异，但是查询的过程和操作都是一样的，这里不再叙述。

点击下面的查找按钮，则会回到相应的规则界面。所有显示的内容都是根据条件查询出来的数据。

3.2.7 地址列表、服务列表详细说明

由于在显示规则的时候，源地址，目的地址和服务，显示的都是各自的名称，用户可能无法记得名称所对应的地址和服务具体是什么，为此还要到资源定义中相应的模块去查询，这样给用户造成了很大的不方便，为了方便用户使用，我们对源地址，目的地址和服务加入了提示的功能，在界面显示的时候，这三项对应的数据的颜色将显示为蓝色，并且当鼠标移动到它们上面的时候将呈现出手的形状，点击后会弹出一个提示框，提示框中列出了相应的地址名或者服务名所对应的具体的地址或者服务信息。

注意：如果源地址，目的地址和服务选择的是任意的话，则相应的数据上面的颜色不会变色，并且当鼠标点击它们的时候也不会弹出提示框，只有源地址，目的地址是在资源定义模块中地址资源里面定义的才可以点击并弹出提示框，服务只有在资源定义模块中服务里面定义的才可以点击并弹出提示框。

点击关闭按钮，相应的提示框将会关闭。

3.3 代理服务

3.3.1 预定义代理

预定义代理可以完成以下代理：HTTP 代理、FTP 代理、TELNET 代理、SMTP 代理、POP3 代理、SOCKS 代理、DNS 代理、ICMP 代理、MSN 代理的配置。

配置系统时首先需要在“策略配置>>代理服务”处设定代理程序是否启用，再在“策略配置>>安全规则>>代理规则”处设定代理规则，允许哪些情况可以使用这些代理。其中的 HTTP 代理，FTP 代理，Telnet 代理，POP3 代理是透明代理，其余代理是不透明的代理，需要在客户端知道代理服务器的地址。

HTTP 代理能够对 Java、JavaScript、ActiveX 进行过滤；FTP 代理能够对多线程和 FTP 命令进行过滤；SMTP 能对邮件大小、最多接收人数进行过滤；POP3 能够对邮件大小进行过滤；SMTP 和 POP3 都能够对邮件内容进行过滤。

配置 SMTP 代理时注意：如果仅需内部网邮件代理，只需要设置“将域名为  的邮件，转发到内部邮件服务器  ”这两项即可；如果需要代理内网和 Internet 的邮件，除了设置上述两项外，还需要设置“代理域名为  的邮件(多个用英文逗号分割)，SMTP 服务器的真实域名  ”。其中，第一项为需要代理的所有邮件的域名，第二项为邮件服务器注册的域名，该域名和服务器的真实 IP 地址必须能够被 Internet 的 DNS 服务器解析。此外，必须将防火墙“网络配置>>域名服务器”设置的域名服务器指向 Internet 的有效 DNS 服务器地址。

SMTP 代理提供防止垃圾邮件的功能。可以设置每个发信人地址每  分钟（1-1440）最多发送  封（1-144000）邮件。SMTP 和 POP3 代理还提供针对发件人，收件人，邮件主题，邮件内容，邮件附件名称的过滤。

SOCKS 代理只支持对 TCP 协议进行 SOCKS V5 的代理，并且不是透明代理，客户端需要将 SOCKS 服务器的地址指向防火墙。

MSN 代理支持 MSN Messenger 的语音和文件传输功能。如果需要支持 MSN 的视频，远程协助等功能，还需要手工配置“安全策略>>安全规则”，来打开相应端口。

注意：各代理设置的端口（如：  ）均为该代理的工作端口，即该代理在该端口监听。如果修改了某代理的工作端口，请重新生效该代理对应的代理规则，否则代理服务无法使用。

设置 SMTP 代理内容过滤

操作步骤：

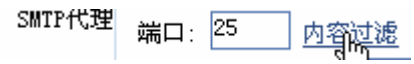
1. 点击“SMTP 代理”行的“内容过滤”链接（如图：  ），将弹出窗口
2. 设置各项值
3. 点击“确定”即可。

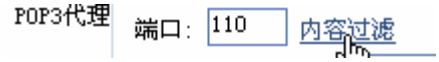
图 3-3 SMTP 代理内容过滤配置

表 3-12 SMTP 代理内容过滤配置项说明

值域	说明
复选框	表示是否启用该项检查。
关键字	邮件内容最多可输入 2048 个字符，多个关键字之间用英文逗号分隔，每项最多可输入 255 个字符； 其他关键字内容最多可输入 255 个字符，多个关键字之间用英文逗号分隔，每项最多可输入 255 个字符。

设置 POP3 代理内容过滤

操作步骤：

1. 点击“POP3 代理”行的“内容过滤”链接（如图： 

），将弹出窗口
2. 设置各项值
3. 点击“确定”即可。

表 3-13 POP3 代理内容过滤配置项说明

值域	说明

复选框 	表示是否启用该项检查。
关键字	邮件内容最多可输入 2048 个字符，多个关键字之间用英文逗号分隔，每项最多可输入 255 个字符； 其他关键字内容最多可输入 255 个字符，多个关键字之间用英文逗号分隔，每项最多可输入 255 个字符。

3.3.2 自定义代理

自定义代理目前只支持 TCP 协议的代理。端口范围为：1 － 65535。使用时与预定义代理类似，也是首先定义并启用自定义代理，再在“策略配置>>安全规则>>代理规则”处设置需要的代理规则。

3.4 地址绑定

IP/MAC 地址绑定用于解决网络管理中 IP 地址盗用的现象。

如果“安全策略>>安全选项”中的 IP/MAC 检查启用，当防火墙接收数据包时，将根据数据包中的源 IP 地址与源 MAC 地址，检查管理员设置好的 IP/MAC 地址绑定表。如果地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按缺省策略（“安全策略>>安全选项”中是否选中“允许未绑定 IP/MAC 对的包通过”）执行。

“策略配置>>地址绑定”可以完成以下功能：

- 探测 IP/MAC 地址对。其中，探测方式有两种：
  （1） 按网口探测
  （2） 按 IP 探测
- 绑定 IP/MAC 地址对。其中，绑定方式有两种：
  （1） 探测 IP/MAC 地址对后选择并绑定
  （2） 手工输入 IP 与 MAC 对。

探测 IP/MAC 地址对

图 3-4 IP/MAC 地址探测

表 3-14 IP/MAC 地址探测项说明

域名	说明
按网口探测	IP/MAC 地址探测方式。

fe1 等网口	当前已激活的网口列表 管理员根据需求指定要做 IP/MAC 探测的网口，可以多选
按 IP 探测	IP/MAC 地址探测方式
输入框	输入 IP 地址或网段
探测	点击后，对指定网口进行 IP/MAC 地址对的探测 探测完成时，指定网口前的选择中符号消失，管理员可以点击“探测到的 IP/MAC 对”进行查看。
探测到的 IP/MAC 对	点击后，显示当前探测到的 IP，MAC 和网口的列表。

按网口探测 **IP/MAC** 地址对的操作步骤：

3. 点击“策略配置>>地址绑定”菜单，弹出“策略配置>>地址绑定”界面。
4. 选择“按网口探测”，可以指定要做 IP/MAC 探测的网口（可以多选）。
5. 点击“探测”，系统对指定网络设备进行 IP/MAC 地址对的探测。界面将提示“正在探测，请稍候…”，根据应用环境的不同，可能需要几十秒钟的时间。
6. 当出现提示“探测完毕，请点击按钮<探测到的 IP/MAC 对>查看探测结果。”点击“确定”后，点击“探测到的 IP/MAC 对”，
7. 弹出”探测到的 IP/MAC 地址对”界面，显示在指定网口当前探测到的 IP、MAC、网口，管理员可以根据探测到的 IP/MAC 地址对，完成绑定功能。详见“探测到的 IP/MAC 对”界面的操作说明。

按 **IP** 探测 **IP/MAC** 地址对的操作步骤：

1. 点击“策略配置>>地址绑定”菜单，弹出“策略配置>>地址绑定”界面
2. 选择“按 IP 探测”，在输入框中输入待探测的主机 IP 地址。
3. 点击“探测”，系统对指定网络设备进行 IP/MAC 地址对的探测。界面将提示“正在探测，请稍候…”，根据应用环境的不同，可能需要几十秒钟的时间。
4. 当出现提示“探测完毕，请点击按钮<探测到的 IP/MAC 对>查看探测结果。”点击“确定”后，点击“探测到的 IP/MAC 对”，
5. 弹出“探测到的 IP/MAC 地址对”界面，显示在指定网口当前探测到的 IP、MAC、网口，管理员可以根据探测到的 IP/MAC 地址对，完成绑定功能。详见“探测到的 IP/MAC 对” 界面的操作说明。

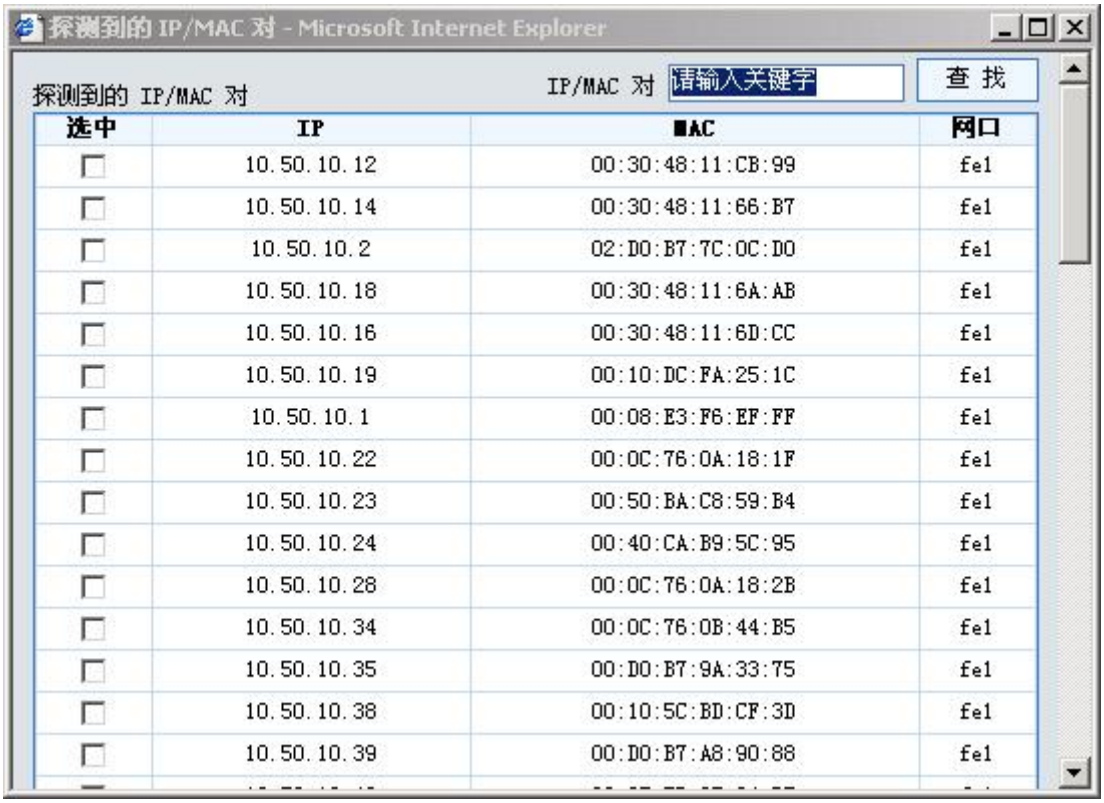


图 3-5 探测到的 IP/MAC 对显示

表 3-15 绑定 IP/MAC 对配置项说明

域名	说明
IP/MAC 对	输入要查找的 IP/MAC 对
查找	点击后，在该界面列表项中查找指定的地址对
选中	选中该 IP/MAC 对，可以根据选择进行删除或绑定操作
IP 地址	探测到的 IP 地址，不能是组播地址
MAC 地址	探测到的 MAC 地址，不能是组播地址
网口	IP/MAC 对是该网口探测到的
全选	全部选中探测到的 IP/MAC 对，可以根据选择进行删除或绑定操作
唯一性检查	当用户选择“唯一性检查”时，IP 与 MAC 建立一一对应，不选择“唯一性检查”时，一个 MAC 可以绑定多个 IP. 如果地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按缺省策略（允许或禁止）执行。
删除	从当前列表中删除选中的 IP/MAC 地址对
绑定	将选中列表项中的 IP/MAC/网口进行绑定，绑定成功后的 IP/MAC 对将显示在已绑定 IP/MAC 对的列表中
取消	取消本次操作

探测到的 IP/MAC 对界面操作说明：

1. 管理员可以根据情况选中相应地址对表项，也可以点击“全选”选中所有地址对表项。
2. 选择唯一性检查时，选中的地址对表项都进行唯一性检查。

3. 针对选中的地址对表项，点击删除，则地址对从当前的列表中清除；点击绑定，则地址对完成绑定功能，绑定成功后界面关闭。

二、绑定 IP/MAC 地址对

图 3-6 添加地址绑定

表 3-16 添加地址绑定项说明

域名	说明
IP 地址	要绑定的 IP 地址
MAC 地址	要绑定的 IP 地址，不能是组播地址。
唯一性检查	当用户选择“唯一性检查”时，IP 与 MAC 建立一一对应，不选择“唯一性检查”时，一个 MAC 可以绑定多个 IP. 如果在地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按缺省策略（允许或禁止）执行。

手工添加 IP/MAC 地址对绑定规则的操作流程：

1. 点击“策略配置>>地址绑定”菜单，弹出“策略配置>>地址绑定”界面
2. 在已绑定 IP/MAC 地址对栏中，点击“添加”，弹出“地址绑定维护”界面
3. 在该界面添加已知的需要进行绑定的 IP/MAC 地址对，点击“确定”，则添加本条规则成功后关闭本窗口；如果点击“添加下一条”，则添加本条规则成功后窗口仍旧打开，可以继续添加下一条规则。

3.5 带宽管理

本节用来设置带宽管理的规则。防火墙会根据这里设置的带宽规则，进行带宽使用的保证和限制。

带宽管理支持基于源 IP 地址，目的地址、服务、接口的带宽管理，支持 VPN 带宽的管理，能够对 VPN 中的封装信息进行基于 IP 地址、服务的带宽管理。每条带宽管理策略可以支持最小保证带宽，最大限制带宽，可以支持带宽优先级的设定，不同的通讯具有不同的带宽使用优先级，优先级高的通讯可以最大量的获得防火墙空余的带宽。

此“策略配置>>带宽管理”界面可以完成以下功能：添加带宽管理规则，编辑带宽管

理规则，启用/禁用带宽管理规则和删除带宽管理规则。

添加带宽管理规则的操作步骤：

1. 点击“添加”按钮，进入“带宽管理规则维护”
2. 添加带宽管理规则参数
3. 点击“确定”按钮完成添加

编辑带宽管理规则的操作步骤：

1. 点击“操作”一栏中的“编辑”图标，打开“带宽管理规则维护”界面
2. 执行修改操作
3. 点击“确定”按钮完成修改

删除带宽管理规则的操作步骤：

1. 点击“操作”一栏中的“删除”图标，弹出删除对话框
2. 点击“确定”按钮完成删除

启用/禁用带宽管理规则的操作步骤：

点击“是否启用”一栏中的图标，如果原来是 ，点击后变成 ，表示由启用状态变成禁用，如果原来是 ，点击后变成 ，表示由禁用状态变成启用。

表 3-17 添加和编辑时参数说明：

域名	说明
规则名	带宽管理规则的名字
序号	输入新增策略规则的序号。 防火墙按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。 若该数字与已定义的规则序号有重复，则防火墙会自动将原策略规则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。 若不修改界面中序号，即为添加到最后。 如果序号大于已有规则总数加 1，即为添加到最后。
源地址	可选内容包括：“资源定义>>地址>>地址列表”和“资源定义>>地址>>地址组”中定义的所有资源，及”自定义”。 当选择“自定义”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。 默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0，以此来表示任意地址。
目的地址	形式同源地址
源端口	源端口可以用英文逗号分割表示多个端口，或用英文冒号分割表示端口段。两种分割方式不能同时使用。如果资源定义中定义的服务资源也包含了源端口，则以此处规则定义的源端口为准。
流入网口	限制网络数据包的流入网口，可以防止 IP 欺骗。 可选内容包括：any 和所有已激活的网口。 默认值为 any，表示不限制接收网口。

	如果工作在透明模式，必须选择相应的物理网口如 fe1 如果不能确定流入网口或工作在混合模式，建议选择 any
时间调度	生效的安全规则在指定的时间段内为生效状态，在其它时间段为失效状态，可选内容包括：“资源>>时间>>时间列表”和“资源>>时间>>时间组”中定义的所有资源。
服务	可选内容包括：any，在“资源定义>>服务>>服务列表”中配置的基本服务、ICMP 服务、动态服务，以及“资源定义>>服务>>服务组”。 默认值为 any，表示源端口任意、目的端口任意、协议任意。
P2P 过滤	对满足条件的数据包进行 BT 过滤，Emule 和 Edonkey 过滤
带宽组资源	从资源定义>>带宽列表>>带宽资源组中选取，匹配上述条件的数据流受带宽资源的限制。
备注	规则注释

3.6 黑名单

提供黑名单阻断的功能，防火墙可以永久或在某一时段内阻断源地址在黑名单上的所有数据包。

黑名单与包过滤规则的不同之处在于：1）黑名单阻断优先于包过滤规则；2）被包过滤拒绝的源地址请求连接时会被拒绝，但是如果未启用规则优先的安全选项，则添加规则前已建立的连接不会被中断；而黑名单上的地址，无论下规则前是否已建立连接，都会被立即阻断。

注意：黑名单规则添加后不能修改，如果需要修改，请删除旧规则，增加一条新的规则。

表 3-18 黑名单添加项说明

域名	说明
地址	阻断的地址
阻断时间	表示从当前开始阻断的分钟，0 为永久阻断
备注	缺省显示开始阻断的时间

3.7 连接管理

目前主流的防火墙都是基于状态检测的防火墙，其主要实现特点是将通讯连接状态保存在内存的连接状态表里，以提高包过滤的安全性和速度。状态表中连接状态的建立主要取决于规则，但不能具体限制每个地址可以建立连接状态的数量。近年蠕虫病毒横行，感染了病毒的内网主机就会在内网不断地进行扫描，试图建立大量的连接，影响了正常网络的通讯。如果能够尽早发现发起大量连接数的主机，可以较早地发现蠕虫病毒感染的主机，减少中毒主机对网络的危害。另外，BT 软件是近年来流行使用的 P2P 下载软件，由于该软件建立大量的连接用于下载使用，导致网络正常的工作或学习使用的带宽资源被严重占用。禁止使用 BT 虽然可以解决此问题，但确实也会影响正常的下载需求。通过限制 IP 地址并发连接数的方法，可以防止 BT 软件建立过多的连接，起到减少 BT 大连接影响的作用。

基于上面需求，联想网御防火墙开发了连接管理功能，此功能可以对地址并发连接进行

有效的统计和管理。

3.7.1 基本参数

选择“启用连接管理”，点确定按钮，则启动连接管理功能；不选择“启用连接管理”，点确定按钮，则关闭连接管理模块。管理连接管理模块，内存中的连接状态和连接排行榜数据将会被清空。

选择会话统计方式，系统对动态协议（如 FTP）的连接将不统计动态生成的连接，否则统计动态生成的连接。

在开启动态学习后，系统会检查记录非连接规则中 IP 地址的连接状态，检查参数根据界面设置的源连接检查类型、源连接阈值、目的连接检查类型、目的连接阈值，学习产生的连接状态类型一律为 dynamic。关闭动态学习，系统将只根据连接规则进行连接状态的记录。

源连接检查类型、源连接阈值、目的连接检查类型、目的连接阈值的含义见连接规则中的说明。

3.7.2 连接规则

连接规则是连接管理模块针对指定的 IP 地址进行并发连接数统计和控制的规则。以 IP 地址为源发起的连接为源连接计数，以 IP 地址为目的发起的连接为目的连接。可以连接数设定相应阈值用于控制。

点击策略配置->连接管理->连接规则，可查看所有的连接规则

单击“添加”按键，可添加连接规则。

表 3-19 添加连接规则说明

域名	说明
地址	连接规则的 IP 地址，可填单 IP 地址或 C 类网段的地址范围，例如 1.1.1.1-1.1.1.254
源连接检查类型	有 5 种类型供选择 u 不统计连接数 -no u 统计连接数，无限制-chk u 统计连接数，超过阈值通过并记录日志-exlog u 统计连接数，超过阈值丢弃，不记录日志-exdrop u 统计连接数，超过阈值丢弃，不记录日志-exdroplog
源连接阈值	源连接检测的阈值，应为正整数
目的连接检查类型	有 5 种类型供选择 u 不统计连接数 -no u 统计连接数，无限制-chk u 统计连接数，超过阈值通过并记录日志-exlog u 统计连接数，超过阈值丢弃，不记录日志-exdrop u 统计连接数，超过阈值丢弃，不记录日志-exdroplog
目的连接阈值	目的连接检查的阈值，应为正整数
备注	备注说明，输入不超过 20 个英文字符或 10 个汉字

注意：

连接规则的源连接检查和目的连接检查可以只选其一，即只统计源连接或只统计目的连接；也可以同时检查源连接和目的连接。

连接规则会产生类型是“静态类型”的连接状态项，连接规则对 IP 的限制不受动态学习参数的影响，即当规则与动态学习参数有交叉时，以规则限制为准。

添加规则 IP 地址是必填选项，其它选项不添则默认从动态学习的参数选择参数做设置。

添加连接阈值的上限为 2147483647，超过此数值的系统一律取 2147483647。

3.7.3 连接状态

查看连接管理的连接状态需要先输入查询条件才能查看连接状态。

查询条件有三种方式供选择：

- 按 IP 查询
- 按类型查询
- 按连接数查询

按 IP 查询

输入 IP 地址，查询此 IP 地址的连接状态

示例：查找 IP 10.1.1.2 的连接状态，输入 IP 地址 10.1.1.2 点击查询按钮

按类型查询

连接管理有两种类型的连接状态：静态类型和动态类型。静态类型的连接状态是由连接规则产生；动态类型的连接状态是由动态学习产生的，例如 FTP 的数据连接就属于动态学习产生的连接，而 FTP 控制连接则属于静态连接。某动态连接状态，其源连接数或目的连接数至少有一项不为 0，若两者都为 0，则此动态连接状态将会自动被清除。

示例：

查询静态类型，选择按类型查询、选择静态类型，点击查询按钮

查询动态类型，选择按类型查询、选择动态类型，点击查询按钮

查询所有类型，选择按类型查询、选择静态和动态类型，点击查询按钮

按连接数查询

可以根据连接数的表达式进行查找连接状态。

示例：查询源连接数大于 100 且小于 500 的连接状态

选择按连接数查询，选择源连接“大于”100，选择“与”，选择“小于”500，点击查询按钮。

示例：查询源连接小于 20，目的连接大于 2000 的连接状态

选择按连接数查询，选择源连接“小于”20，选择“空”；选择目的连接“大于”2000，点击查询按钮。

表 3-20 连接状态表项说明

域名	说明
序号	连接状态 ID 号
IP	IP 地址
源连接数	以 IP 地址为源的并发连接数
目的连接数	以 IP 地址为目的的并发连接数

源类型	源连接检查类型
源阈值	源连接检查的阈值
目的类型	目的连接检查类型
目的阈值	目的连接检查的阈值
类型	Static 静态类型；dynamic 动态类型
类型转换	可将动态类型转换为静态类型

注意：

连接管理的连接数，是对经过防火墙转发的连接状态的统计，访问防火墙本地服务的不计算在内；连接是经过防火墙源地址转换的，源连接计数是地址转换前的源地址；连接经过反向 NAT 转换的，目的连接计数是地址转换后的目的地址。连接管理具有限制并发连接的功能，但他不能替代抗 synflood 攻击功能，抗 synflood 攻击在连接管理前面执行，两者可联合使用。并发连接数的增加减少与防火墙状态的新增和超时一致，即增加一个连接状态计数加 1，一个连接状态超时计数减一。

3.7.4 连接排行榜

启动连接管理模块，可产生源连接排行榜和目的连接排行榜。可显示最多 TOP10 的排行情况，根据这些情况可以监控并发连接的情况，及时发现突发大连接的事件。

第4章 VPN 配置

联想网御防火墙的 VPN（虚拟私有网络）功能模块使得用户可以在 Internet 上构建基于 IPSec（IP 数据包加密）技术或者 SSLVPN 的一系列加密认证技术以及密钥交换方案，使得在公共网络上组建的 VPN，具有同本地私有网络一样的安全性、可靠性和可管理性等特点，同时大大降低了建设远程私有网络的费用。VPN 模块支持 IPSec 协议和 SSL 协议，提供网络层报文的身份鉴别、加密和完整性认证等功能。

联想网御防火墙的 VPN 系统能提供“IPSec”、以及“远程 PPTP/L2TP（点对点隧道协议/第二层隧道协议）拨号”和“SSLVPN”这三种形式的隧道。为了建立这三种隧道，提供如下界面管理：自身 VPN 的基本配置，远程 VPN 的配置，网关－网关隧道配置，网关－客户端隧道配置，隧道监控和证书管理。每次创建一条新的网关隧道或客户端隧道，都需要首先通过“VPN>> IPSec>>远程 VPN”页面设定远程 VPN 的基本信息，包括名称，认证方式，认证数据，类型，IKE 加密算法等。随后根据新建 VPN 隧道的不同类型，分别在“网关隧道配置”、“客户端隧道配置”其中一个页面对新的隧道的子网信息、IPSec 算法、数据包认证方式等信息进行设置。最后在“VPN>>IPSec >>隧道监控”界面对新建的隧道进行启动操作，就可以马上启动新建立的隧道了。同时“VPN>>隧道监控>>L2TP/PPTP”界面，可以监控拨号用户建立的 VPN 隧道。隧道两端都必须进行相应的配置，才可以正常地建立起隧道。

如果在设置远程 VPN 时， “认证方式”设置为“证书”方式，就必须首先通过“证书管理”目录下的配置界面对 CA（认证中心）证书、本地证书、对方证书进行一系列的导入后，才可以建立使用证书方式进行认证的隧道。

在“VPN>>IPSec>>基本配置”界面中包括了对自身 VPN 的基本设置，有 IPSec 协议的基本配置和 L2TP/PPTP 的基本设置。

在“SSLVPN”的配置界面中包括了对 SSLVPN 的参数配置，SSLVPN 的用户管理，隧道监控。

下面就针对：“IPSec”、“L2TP/PPTP”、“SSLVPN”的具体配置方法和参数进行详细的介绍和说明。

4.1 IPSEC

4.1.1 远程 VPN

在建立 VPN 隧道之前，必须明确每条隧道都要有两个端点。其中一个端点是正在配置的 VPN，另外一个端点是远程 VPN。隧道两端都必须进行相应的配置，才可以正常地建立起隧道。用户首先要输入其要建立隧道的对端信息。对端是隧道的终点，由它来负责数据包的加密和解密。远程 VPN 有两种类型，一种是网关，一种是客户端；前者通常就是远程防火墙或者 VPN 网关，后者指客户主机，通常是一台台式机或笔记本电脑。

远程 VPN 数据域说明：

表 4-1 远程 VPN 数据域说明

域名	说明

远程 VPN 名称	远程 VPN 名称，唯一标识，符合命名规则（1－20 个字母、数字、减号、下划线组合）
远程 VPN 地址形式	IP 地址或者域名
远程 VPN 地址	远程 VPN 的 IP 地址或域名
认证方式	与远程 VPN 进行相互认证的方式，预共享密钥或者是证书
认证数据	当认证方式为预共享密钥，则此处显示为预共享密钥的值， 当认证方式为证书，此处显示为 localcert：本地证书名 cert：对方证书名
类型	网关或者客户端

添加远程 VPN

添加远程 VPN 时，需要根据实际情况选择合适的的类型和认证方式。当用户选择的是客户端类型，或远程 VPN 地址为“0.0.0.0”，且“认证模式”为“主模式”，“认证方式”为“预共享密钥”认证，则系统使用缺省的预共享密钥进行认证（缺省的预共享密钥在”VPN>>IPSec>>基本配置”中设置）。当用户选择“认证方式”为“证书认证”时，需要指定相应的本地证书和对方证书。

1. 点击“添加”按钮，弹出远程 VPN 的设置窗口。
2. 输入完成后，点击“确定”按钮，或点击“添加下一条”按钮，添加下一个远程 VPN。

远程 VPN 添加数据域说明：

表 4-2 VPN 添加编辑数据域说明

域名	说明
远程 VPN 名称	远程 VPN 名称，唯一标识，符合命名规则，必须是 1－20 位字母、数字、减号、下划线的组合，不能为空。
远程 VPN 地址形式	选择远程 VPN 的地址表示形式，可选内容为“IP 地址”或“域名”。
IP 地址/域名	当远程 VPN 地址形式为“IP 地址”，此处输入远程 VPN 的 IP 地址，当远程 VPN 地址形式为“域名”，此处输入远程 VPN 的域名。
认证方式	与远程 VPN 进行相互认证的方式，可选内容为“预共享密钥”或“证书”
预共享密钥	当认证方式为“预共享密钥”，此处输入预共享密钥的值。缺省为“VPN>>IPSec>>基本配置”中设置的预共享密钥的值。
本地证书	当认证方式为“证书”时，在此处选择本地证书，可选内容为：在“VPN>>IPSec>>证书管理>>本地证书”中生成的证书。
对方证书	当认证方式为“证书”时，在此处选择对方证书，可选内容为：在“VPN>>IPSec>>证书管理>>对方证书”中生成的证书。
IKE 算法组件	IKE 协商第一阶段加密和认证算法选择。左边窗口为加密算法，默认为 3des，可选算法为：3des，des，aes128。右边窗口为认证算法，默认为 md5，可选算法为：md5, sha1, sha2-256, sha2-512
认证模式	IKE 协商第一阶段的认证模式，可选内容为“主模式”和“野蛮模式”。主模式需要三个交换完成 IKE SA（安全联盟）的建立，提供交换双方的身份保护。野蛮模式只需要一个交换就可以完成 IKE SA 的建立，不提供身份保

	护
本地 ID	本地网关的设备 ID，必须是 1－16 位字母、数字、减号、下划线的组合，不能为空
对方 ID	远程网关的设备 ID，必须是 1－16 位字母、数字、减号、下划线的组合，不能为空
类型	可选内容为：“网关”和“客户端”
启用扩展认证	可选内容为：“是”和“否”。在 VPN 客户端远程访问时，可以提供除 IPSec 的预共享密钥或证书认证外的 Radius 加强认证。只有客户端类型，而且是主模式的网关才能启用扩展认证。

编辑远程 VPN

1. 点击想要对其进行编辑的远程 VPN 的“编辑”图标，弹出远程 VPN 的设置窗口。
2. 修改完成后，点击“确定”按钮。

数据域说明，同“添加远程 VPN”。

注意：只有在“VPN>>IPSec >>隧道监控”中重新启动相应的隧道后，修改的远程 VPN 信息才会生效。

删除远程 VPN

3. 点击想要进行删除的远程 VPN 的“删除”图标，在弹出的对话框中点击“确认”。
4. 出现“删除成功”提示框，点击“确定”。

注意：当删除远程 VPN 时，将删除所有的和此远程网关相关的隧道。

4.1.2 网关隧道配置

隧道是在两个远程网关之间建立的加密通道，这个通道只加密符合隧道规则的数据包，即 “策略配置>>安全规则>>包过滤规则”中动作选择了 IPSec 的规则匹配的数据包。隧道根据远程网关的类型可以分为两类，一种是网关类型和网关类型的远程网关之间建立的隧道，用于保护两个子网之间的数据通信，一种是网关类型的远程网关和客户端之间建立的隧道，用于保护子网和远程主机之间的数据通信。

图标说明：

表 4-3 VPN 网关隧道配置图标说明

域名	说明
	启用状态，表示已启用
	启用状态，表示未启用
	编辑本条记录

	删除本条记录

数据域说明：

表 4-4 VPN 网关隧道配置数据域说明

域名	说明
隧道名称	网关隧道名称，唯一标识，符合命名规则
本地网关	自动读取防火墙 IP
本地保护子网	本地需要保护的子网网段
远程网关地址	要建立隧道的对方网关地址
远程保护子网	远程需要保护的子网网段
缺省策略	本隧道的缺省防火墙规则：允许和包过滤 隧道的缺省策略用于控制隧道内的数据包是否需要进行包过滤控制。在隧道的缺省策略是允许的情况下，防火墙将不对隧道内的数据包进行过滤，这时隧道保护的两个子网之间是可以相互间任意访问的。当缺省规则是包过滤时，需要添加合适的包过滤策略，来控制隧道内数据包的流动。包过滤规则是有方向性的，因此如果需要隧道两端的子网可以相互通信，则至少需要添加对应的两条包过滤规则（源地址和目的地址正好相反）。
是否启用	是否已启用了本隧道

添加网关隧道

在添加网关－网关之间的隧道时，请选择本地出口，合适的缺省策略，并选择是否启用。当隧道的缺省策略是包过滤时，用户应该添加合适的包过滤策略，允许指定的数据包通过。当选择隧道启用时，隧道会在防火墙重启时自动加载建立。注意新添加网关隧道或者修改了网关隧道的配置信息，请到隧道监控中重新启动该网关隧道。

1. 点击“添加”按钮，弹出网关隧道的设置窗口。
2. 输入完成后，点击“确定”按钮，或“添加下一条”按钮，添加下一个网关隧道。

VPN 网关隧道添加数据域说明：

表 4-5 VPN 网关隧道添加编辑数据域说明

域名	说明
隧道名称	网关隧道名称，唯一标识，符合命名规则，必须是 1－20 位字母、数字、减号、下划线的组合，不能为空。
本地出口	本地网关与远程网关建立隧道，所使用的网络接口。
本地保护子网	本地需要保护的子网 IP
本地保护子网掩码	本地保护子网掩码

远程 VPN	要建立隧道的对方名称，可选内容为：在“VPN>>IPSec>>远程 VPN”中配置的类型为“网关”的远程 VPN 名称。
远端保护子网	远端需要保护的子网 IP
远端保护子网掩码	远端保护子网掩码
IPSec 算法组件	数据通信用的加密算法和认证算法。左边窗口为加密算法，默认为 3des，可选算法为：3des，des，aes128，null，专用算法。右边窗口为认证算法，默认为 md5，可选算法为：md5, sha1, sha2-256, sha2-512。 “专用算法”指的是国家批准的专用算法，该算法需要特殊加密卡的支持，除非产品特别指明，不包含加密卡的产品不能使用该算法。
完美前向保密	是否选用完美前向保密方式，隧道两端该参数的选择应该一致，否则无法建立隧道。
数据包认证方式	可选内容为：“ESP”，“AH”。AH 协议提供无连接的完整性、数据源认证和抗重放保护服务，ESP 提供和 AH 类似的服务，并增加了数据保密和有限的数据流保密服务。Ah 不支持 NAT 穿越和 null 算法。
缺省策略	本隧道的缺省防火墙规则（允许/包过滤）。 隧道的缺省策略用于控制隧道内的数据包是否需要进行包过滤控制。在隧道的缺省策略是允许的情况下，防火墙将不对隧道内的数据包进行过滤，这时隧道保护的两个子网之间是可以相互间任意访问的。当缺省规则是包过滤时，需要添加合适的包过滤策略，来控制隧道内数据包的流动。包过滤规则是有方向性的，因此如果需要隧道两端的子网可以相互通信，则至少需要添加对应的两条包过滤规则（源地址和目的地址正好相反）。
DPD 周期	DPD 功能用来探测建立隧道的对端主机的状态。DPD 周期表示探测的周期时间长度，单位为秒，允许配置的时间范围[5，180]。0 表示不启用 DPD。
DPD 超时	在发出探测后，如果超过这个时间还未收到回应，则认为隧道对端主机已经离线。单位为秒，允许配置的时间范围[5，600]。0 表示不启用 DPD。
是否主动连接	网络中间如果有 NAT 设备，导致本地网关不能主动与对方网关建立连接，就必须选择“否”，能主动与对方网关建立连接的必须选择“是”。默认为“是”
是否启用	是否已启用了本隧道

注意：网络中间如果有 NAT 设备，则数据包认证方式无法使用 AH 协议，国际标准不支持 AH 数据报穿越 NAT。

编辑网关隧道

1. 点击想要对其进行编辑的网关隧道的“编辑”图标，弹出网关隧道的设置窗口。
2. 修改完成后，点击“确定”按钮。

数据域说明，同“添加网关隧道”。

注意：只有在“V VPN>>IPSec >>隧道监控”中重新启动相关联的隧道后，修改的网关隧道信息才会生效。

删除网关隧道

1. 点击想要进行删除的网关隧道“删除”图标，在弹出的对话框中点击“确认”。

2. 出现“删除成功”提示框，点击“确定”。

4.1.3 客户端隧道配置

图标说明：

表 4-6 VPN 客户端隧道配置图标说明

域名	说明
	启用状态，表示已启用
	启用状态，表示未启用
	编辑本条记录
	删除本条记录

数据域说明：

表 4-7 VPN 客户端隧道配置数据域说明

域名	说明
隧道名称	客户端隧道网关名称，唯一标识，符合命名规则
本地网关地址	自动读取防火墙 IP
本地保护子网	本地需要保护的子网网段
客户端地址	要建立隧道的对方客户端地址
客户端虚拟 IP 地址	客户端需要保护的虚拟 IP 地址
缺省策略	本隧道的缺省防火墙规则（允许/包过滤）。 隧道的缺省策略用于控制隧道内的数据包是否需要进行包过滤控制。在隧道的缺省策略是允许的情况下，防火墙将不对隧道内的数据包进行过滤，这时隧道保护的两个子网之间是可以相互任意访问的。当缺省规则是包过滤时，需要添加合适的包过滤策略，来控制隧道内数据包的流动。包过滤规则是有方向性的，因此如果需要隧道两端的子网可以相互通信，则至少需要添加对应的两条包过滤规则（源地址和目的地址正好相反）。
是否启用	是否已启用了本隧道。

添加客户端隧道

当添加网关－客户端之间的隧道时，请选择本地出口，合适的缺省策略，并选择是否启用。当隧道的缺省策略是包过滤时，用户应该添加合适的包过滤策略，允许指定的数据包通过。当选择隧道启用时，隧道会在防火墙重启时自动加载建立。注意新添加隧道或者修改了

隧道的配置信息，请到隧道监控中重新启动该隧道。

1. 点击“添加”按钮，弹出客户端隧道的设置窗口。
2. 输入完成后，点击“确定”按钮，或点击“添加下一条”按钮，添加下一个客户端隧道。

客户端隧道配置添加数据域说明：

表 4-8 VPN 客户端隧道配置添加编辑数据域说明

域名	说明
隧道名称	客户端隧道名称，唯一标识，符合命名规则，必须是 1－20 位字母、数字、减号、下划线的组合，不能为空。
本地出口	本地网关与远程客户端建立隧道，所使用的网络接口。
远程网关	要建立隧道的对方名，可选内容为：在“VPN>>IPSec>>远程 VPN”中配置的类型为“客户端”的远程 VPN 名称。
客户端虚拟 IP 地址类型	可选内容为：“any”，“单个 IP”和“某一范围”，any 表示 IP 地址为任意
客户端虚拟 IP 地址	当客户端虚拟 IP 地址类型为 any 时，默认为 0.0.0.0。当客户端虚拟 IP 地址类型为“单个 IP”或“某一范围”时，要输入具体的 IP 地址。
客户端虚拟 IP 掩码	客户端虚拟 IP 掩码
客户端可访问子网	客户端可访问的本地子网 IP
客户端可访问子网掩码	客户端可访问子网掩码
数据包认证方式	可选内容为：“ESP”，“AH”。AH 协议提供无连接的完整性、数据源认证和抗重放保护服务，ESP 提供和 AH 类似的服务，并增加了数据保密和有限的数据流保密服务。Ah 不支持 NAT 穿越和 null 算法。
缺省策略	本隧道的缺省防火墙规则（允许/包过滤）。 隧道的缺省策略用于控制隧道内的数据包是否需要进行包过滤控制。在隧道的缺省策略是允许的情况下，防火墙将不对隧道内的数据包进行过滤，这时隧道保护的两个子网之间是可以相互间任意访问的。当缺省规则是包过滤时，需要添加合适的包过滤策略，来控制隧道内数据包的流动。包过滤规则是有方向性的，因此如果需要隧道两端的子网可以相互通信，则至少需要添加对应的两条包过滤规则（源地址和目的地址正好相反）。
DPD	对于客户端如果采用 DPD 功能，可能会导致客户端被断开，因此对于客户端隧道 DPD 的设置是没有用的。
是否启用	是否已启用了本隧道。

注意：网络中间如果有 NAT 设备，则数据包认证方式无法使用 AH 协议，国际标准不支持 AH 数据报穿越 NAT。

编辑客户端隧道

1. 点击想要对其进行编辑的客户端隧道的“编辑”图标，弹出客户端隧道的设置窗口。

2. 修改完成后，点击“确定”按钮。

数据域说明，同“添加客户端隧道”。

注意：只有在“VPN>>IPSec >>隧道监控”中重新启动相关联的隧道后，修改的客户端隧道信息才会生效。

删除客户端隧道

1. 点击想要进行删除的客户端隧道的“删除”图标，在弹出的对话框中点击“确认”。
2. 出现“删除成功”提示框，点击“确定”。

4.1.4 证书管理

4.1.4.1 文件证书

证书分为三类： CA 证书，本地证书和对方证书。CA 证书是进行认证的基础，利用他验证对方证书是否可信。本地证书是防火墙的证书，防火墙利用本地证书与远程 VPN 交换身份信息，进行认证。防火墙使用对方证书或对方证书主题判断对方证书身份是否合适。

用户应该首先添加合适的 CA 证书，其次再添加该 CA 证书签发的本地证书和对方证书。可以通过“VPN>>证书管理>>CA 证书”，“VPN>>证书管理>>对方证书”和“VPN>>证书管理>>本地证书”与 CA 软件相配合，来生成和导出证书。

- CA 证书

CA 证书数据域说明：

表 4-9 VPN CA 证书数据域说明

域名	说明
名称	证书的名称，唯一标识，符合命名规则
颁发者	签发该证书的实体的惟一名（DN）
主题	被授予该证书的实体的惟一名（DN）
有效期起始时间	证书有效期开始的日期
有效期终止时间	证书有效期结束的日期

功能说明：

表 4-10 VPN CA 证书功能说明

域名	说明
	选定所有的 CA 证书，或取消所有的 CA 证书的选定
	导入 CA 证书。可以使用证书管理器导出 CA 根证书，然后在此导入。如果使用第三方 CA，则导入第三方 CA 证书。
	删除选定的 CA 证书

导出证书	导出选定的 CA 证书

- 对方证书

添加对方证书有两种方法，添加主题方式和导入方式。添加主题就是根据对方证书设置各种信息。防火墙认证对方身份时，判断对方证书是否和您在此添加的主题信息相符合。导入方式是把对方证书导入到防火墙，取出证书的主题，用主题来判断对方身份。

对方证书数据域说明：

表 4-11 VPN 对方证书数据域说明

域名	说明
名称	证书的名称，唯一标识，符合命名规则
颁发者	签发该证书的实体的惟一名（DN）
主题	被授予该证书的实体的惟一名（DN）
有效期起始时间	证书有效期开始的日期
有效期终止时间	证书有效期结束的日期

功能说明：

表 4-12 VPN 对方证书功能说明

域名	说明
全选	选定所有的对方证书，或取消所有的对方证书的选定
添加主题	添加主题。防火墙认证对方身份时，判断对方证书是否和您在此添加的主题相符合。
导 入	导入对方证书。将对方证书导入到防火墙，取出证书的主题，用此主题判断对方身份。
删 除	删除选定的对方证书
导出证书	导出选定的对方证书

添加主题数据域说明：

表 4-13 VPN 对方证书添加主题数据域说明

域名	说明
证书名称	证书的名称，唯一标识，符合命名规则
国家	证书被授予者所在的国家代码
省	证书被授予者所在的省的代码
市区	证书被授予者所在的市或区的代码
组织	证书被授予者所在的组织的代码

部门	证书被授予者所在的部门代码
公共名主题	证书被授予者的通用名或常用名
邮件	证书被授予者的电子邮箱地址

▌ 本地证书

有两种添加本地证书的方法：密钥本地生成、密钥外部生成。一般情况下使用密钥本地生成。

使用密钥本地生成，防火墙内部随机生成公、私钥对，然后用公钥和您输入的请求信息生成证书请求文件。您将此证书请求文件导出后，可以在另外的证书管理器软件中签发，也可以用第三方 CA 签发。签发后将生成证书文件，将此证书文件导入到防火墙就完成了本地证书生成的过程。

使用密钥外部生成，您可以将其他 CA 生成的证书、私钥导入到防火墙。

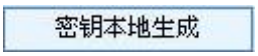
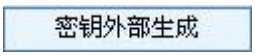
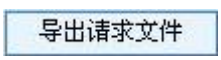
本地证书数据域说明：

表 4-14 VPN 本地证书数据域说明

域名	说明
名称	证书的名称，唯一标识，符合命名规则
颁发者	签发该证书的实体的惟一名（DN）
主题	被授予该证书的实体的惟一名（DN）
有效期起始时间	证书有效期开始的日期
有效期终止时间	证书有效期结束的日期

功能说明：

表 4-15 VPN 本地证书功能说明

域名	说明
	选定所有的 CA 证书，或取消所有的 CA 证书的选定
	如果密钥是在本地生成的，点击此按钮生成请求文件
	如果密钥是在外部生成的，点击此按钮导入证书及密钥
	选定相应的请求文件前的复选框，点击此按钮导入本地证书
	删除选定的本地证书
	导出选定的本地证书，如果选定的是请求文件，则该按钮不起作用
	导出选定的请求文件，如果选定的是密钥外部生成的证书，则该按钮不起作用

密钥本地生成

本地证书密钥本地生成数据域说明：

表 4-16 VPN 本地证书密钥本地生成数据域说明

域名	说明
证书名称	证书的名称，唯一标识，符合命名规则
国家	证书被授予者所在的国家代码
省	证书被授予者所在的省的代码
市区	证书被授予者所在的市或区的代码
组织	证书被授予者所在的组织的代码
二级组织	证书被授予者所在的二级组织的代码
公共名主题	证书被授予者的通用名或常用名
邮件	证书被授予者的电子邮箱地址

4.1.5 基本配置

IPSec 数据域说明：

表 4-17 VPN IPSec 基本配置数据域说明

域名	说明
启用 IPSec 功能	用来启动或停止 VPN 系统。
IKE 密钥周期	IKE 生命周期，单位为秒，必须在［1200,86400］之间
IPSec 密钥周期	IPSec 生命周期，单位为秒，必须在［1200,28800］之间
预共享密钥	预共享密钥，在此处更新了预共享密钥后，需要在远程 VPN 中重新编辑用到预共享密钥的记录。
启用 DHCP over IPSec	选择后可以为 VPN 客户端动态分配 IP 地址。
DHCP 中继地址	为 VPN 客户端动态分配地址的 DHCP 服务器地址。
DHCP 中继设备	从安全网关到达 DHCP 服务器的网口，如果使用安全网关的 DHCP 服务器，中继设备就是“lo”。

4.1.6 隧道监控

IPSec 隧道数据域说明：

表 4-18 VPN 隧道监控 IPSec 隧道数据域说明

域名	说明
隧道名称	隧道名称，唯一标识，符合命名规则
隧道类型	隧道类型，有以下两种类型：网关－网关、 客户端－网关
本地保护子网	隧道本地端的保护子网网段地址
本地网关	隧道本地网关的地址

对端网关	隧道对端网关的地址
对端保护子网	隧道对端保护子网网段地址
发送流量（字节）	发送了多少字节的数据
接收流量（字节）	接收了多少字节的数据
SA 建立时间（秒）	SA 建立的时间
状态	隧道当前的状态，有以下四种状态：未启动、已经建立、正在建立、信息错误。
操作	启动或停止该隧道

功能说明：

表 4-19 VPN 隧道监控 IPSec 隧道功能说明

域名	说明
隧道同步	隧道同步
刷 新	刷新当前隧道状态

启动 IPSec 隧道

1. 点击想要启动的隧道的“启动”链接，点击后，启动会变为停止链接，同时状态栏中显示隧道的状态。

停止 IPSec 隧道

1. 点击想要停止的隧道的“停止”链接，点击后，“停止”会变为“启动”链接，同时状态栏中显示隧道的状态。

隧道同步

1. 点击“隧道同步”按钮。

刷新

1. 点击“刷新”按钮。

注意：当对“远程 VPN”、“网关隧道配置”、“客户端隧道配置”等进行了修改，必须在“VPN>>IPSec >>隧道监控”中重新启动相应的隧道，所做的修改才会生效。

4.2 L2TP/PPTP

4.2.1 拨号用户

远程拨号用户图标说明：

表 4-20 VPN 远程拨号用户图标说明

域名	说明
	编辑本条记录
	删除本条记录

数据域说明：

表 4-21 VPN 远程拨号用户数据域说明

域名	说明
用户名称	用户名称，唯一标识，符合命名规则
备注	用户的详细描述。

添加远程拨号用户

1. 点击“添加”按钮，弹出远程拨号用户的设置窗口。
2. 输入完成后，点击“确定”按钮，或“添加下一条”按钮，添加下一个远程拨号用户。

远程拨号用户添加数据域说明：

表 4-22 VPN 远程拨号用户添加编辑数据域说明

域名	说明
用户名称	用户名称，唯一标识，符合命名规则，必须是 1－20 位字母、数字、减号、下划线的组合，不能为空。
密码	用户的密码
备注	用户的详细描述。

编辑远程拨号用户

1．点击想要对其进行编辑的远程拨号用户的“编辑”图标，弹出远程拨号用户的设置窗口。
2．修改完成后，点击“确定”按钮。

数据域说明，同“添加远程拨号用户”。

删除远程拨号用户

1. 点击想要进行删除的远程拨号用户的“删除”图标，在弹出的对话框中点击“确认”。
2. 出现“删除成功”提示框，点击“确定”。

4.2.2 参数配置

PPTP/L2TP 客户端可以使用 Windows XP 和 Windows 2000 系列操作系统自带的系统程序来配置。具体配置方法，请参考 Windows 的使用说明。

PPTP/L2TP 数据域说明：

表 4-23 VPN PPTP/L2TP 基本配置数据域说明

域名	说明
启用	表示启动或者停止拨号服务器
IP 地址范围	拨号服务器提供的 IP 地址范围。要求起始地址与终止地址在同一个 C 类地址段内，并且 IP 个数在 3—200 个以内。例如：10.10.10.1-10.10.10.100
加密强度	high 表示比较高的加密等级(128 位)，low 表示比较低的加密等级(40 位)。
认证协议	支持的认证协议，可以多选

4.2.3 隧道监控

PPTP/L2TP 隧道数据域说明：

表 4-24 VPN 隧道监控 PPTP/L2TP 隧道数据域说明

域名	说明
用户名	名称，唯一标识，符合命名规则
登录时间	用户登录的时间
本地分配地址	本地地址
远程网络地址	远程网络地址
加密强度	high 表示比较高的加密等级(128 位)，low 表示比较低的加密等级(40 位)。NONE 表示未加密。

功能说明：

表 4-25 VPN 隧道监控 PPTP/L2TP 隧道功能说明

域名	说明

刷 新	刷新当前隧道状态

4.3 GRE

图标说明：

表 4-26 GRE 图标说明

域名	说明
	编辑本条记录
	删除本条记录

数据域说明：

表 4-27 GRE 数据域说明

域名	说明
隧道名称	GRE 隧道名称，唯一标识，符合命名规则。名称必须以 GRE_开头。
本地网关	GRE 隧道使用的本地物理设备名称。
远程网关	GRE 隧道使用的远程网关域名或者 IP 地址
GRE 设备 IP	GRE 隧道设备的 IP 地址
对端设备 IP	对端 GRE 隧道设备的 IP 地址
是否启用	 表示该规则为生效状态，点击  以后该规则变成无效状态   表示该规则为无效状态，点击  以后该规则变成生效状态 

添加 GRE 隧道

1. 击“添加”按钮，弹出 GRE 隧道的设置窗口。
2. 输入完成后，点击“确定”按钮，或“添加下一条”按钮，添加下一个 GRE 隧道。

数据域说明：

表 4-28 GRE 隧道添加编辑数据域说明

域名	说明
隧道名称	GRE 隧道名称，唯一标识，符合命名规则
本地网关	GRE 隧道使用的本地物理设备名称。
远程网关	GRE 隧道使用的远程网关域名或者 IP 地址
GRE 设备 IP	GRE 隧道设备的 IP 地址
对端设备 IP	对端 GRE 隧道设备的 IP 地址
是否启用	是：启用隧道　　否：停用隧道

编辑 GRE 隧道

1．点击想要对其进行编辑的 GRE 隧道的“编辑”图标，弹出 GRE 隧道的设置窗口。
2．修改完成后，点击“确定”按钮。

数据域说明，同“添加 GRE 隧道”。

删除 GRE 隧道

1． 想要进行删除的 GRE 隧道的“删除”图标，在弹出的对话框中点击“确认”。
2． 出现“删除成功”提示框，点击“确定”。

GRE 隧道重起

点击 GRE 隧道重起按钮，防火墙将把所有已经启用的隧道重新启动一遍。

4.4 SSLVPN

4.4.1 参数配置

数据域说明：

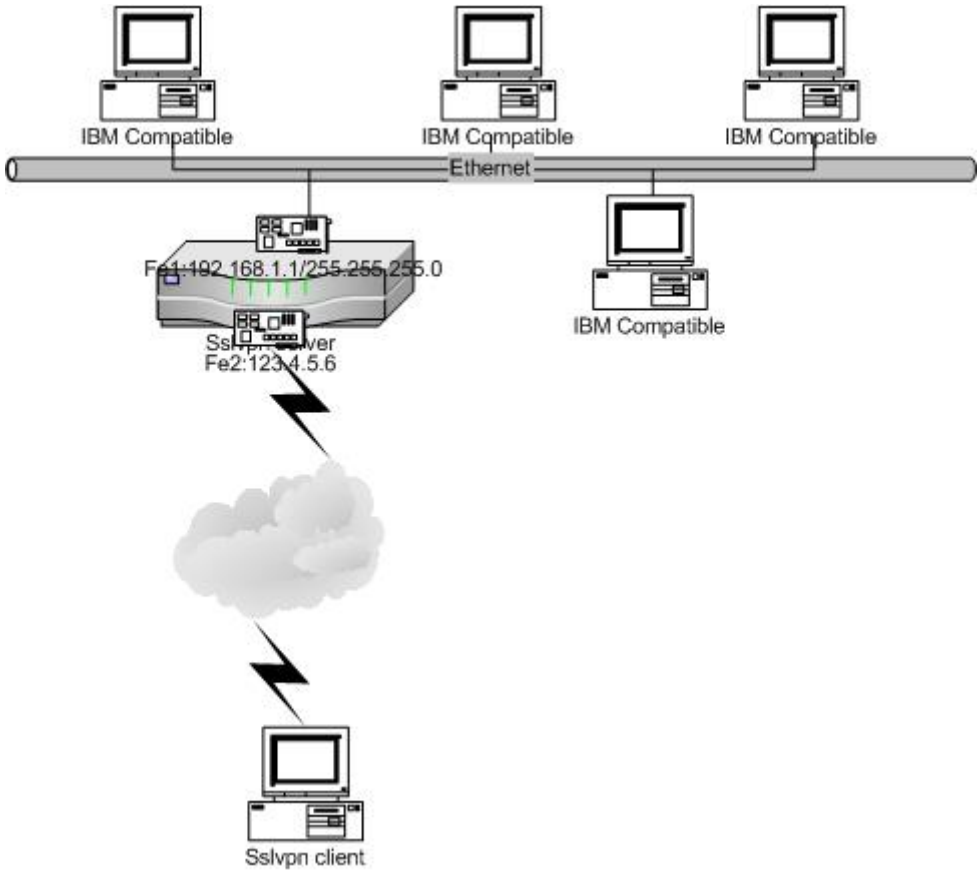
表 4-29 SSLVPN 参数配置数据域说明

域名	说明
启动 SSLVPN 功能	该选项表示是否启动 SSLVPN 功能。选中后，点击“确定”按钮 SSLVPN 功能就会被启动。
用户登录页面显示文字	设置此属性，可以在移动用户通过 web 页面进行连接时，给用户提供一定的提示信息，例如公司名称等。最多可以输入 25 个汉字。
SSLVPN 服务端口	SSLVPN 服务使用的端口。默认 2299。
协议	SSLVPN 连接使用的协议，tcp 或者 udp，选择 udp 时，无法穿越
允许接入设备	允许用户从哪些设备建立 SSLVPN 连接，通常选择与公网连接的设备。
保护子网	建立 SSLVPN 连接的用户可以访问的子网，最多可以加入 5 个保护子网。
客户端 DNS	设置该属性后，当用户建立 SSLVPN 连接后，用户本地机器的 DNS 服务器就会被设置为该处配置的 IP。
客户端 WINS	设置该属性后，当用户建立 SSLVPN 连接后，用户本地机器的 WINS 服务器就会被设置为该处配置的 IP。
探测周期	在建立 SSLVPN 连接后，网关会按照设定的周期探测建立连接的用户主机是否仍然存在。
超时时间	在探测失败后，超过超时时间后，SSLVPN 连接则被认为已经断开。
加密算法	SSLVPN 连接建立后，采用的加密算法。
摘要算法	SSLVPN 连接建立后，采用的摘要算法。
客户端可以互相访问	选择该项后，与 SSLVPN 建立建立连接的用户主机之间可以互相访问。
支持压缩	选择该项后，通信过程中，会对数据包先进行压缩再发送。
路由地址空间	SSLVPN 用户建立 SSLVPN 连接后的地址范围，最小一个 C 类子网，最大一个 B 类子网。

客户端接入方式	移动用户接入时，通过域名连接还是 IP 连接。
客户端接入地址	输入移动用户连接时要连接的地址，可以是 ip 或者域名。IP 通常是一个公网地址。
密码允许错误次数	最多用户允许输错几次密码，超过后，用户被锁定。
用户锁定时间	用户被锁定后，多长时间自动解锁。

在配置完各项内容后，点击“确定”按钮，设置内容就会生效。如果选择了启动 SSLVPN，SSLVPN 模块就会被启动。

配置示例：



在以上网络拓扑示例中，保护子网是 192.168.1.0/24，客户接入地址是 123.4.5.6，sslvpn 客户端从路由地址空间中分配虚拟地址来访问保护子网。

4.3.2 SSLVPN 内网资源定义

用户通过 SSLVPN 可以访问内部网络资源，但是通常有些用户不知道自己访问的资源在哪里。通过内网资源定义，可以帮助这些用户方便的访问内网资源。

定义内网资源后，用户连接 SSLVPN 后，就会在页面上看到可以访问的内网资源，对于 http、ftp 等资源可以直接在浏览器访问。图 6-20 中定义了三个内网资源。

图 4-1 SSLVPN 用户管理

表 4-30 SSLVPN 内网资源说明

域名	说明
	编辑本条记录
	删除本条记录

点击“添加”按钮可以定义新的内网资源。

图 4-2 SSLVPN 用户管理

表 4-28 SSLVPN 内网资源添加编辑数据域说明

域名	说明
资源名称	内网资源名称，唯一标识，符合命名规则，必须是 1－20 位字母、数字、减号、下划线的组合，不能为空。
资源 IP 地址	内网资源 IP 地址。
资源类型	资源类型，ftp、http、https 类型的资源在 IE 中就可以直接访问。其它的类型只有参考意义。
备注	内网资源定义的详细描述。

4.3.3 用户管理

图标说明：

表 4-31 SSLVPN 用户图标说明

域名	说明
	编辑本条记录
	删除本条记录

数据域说明：

表 4-32 SSLVPN 用户数据域说明

域名	说明
用户名称	用户名称，唯一标识，符合命名规则
备注	用户的详细描述。

添加 SSLVPN 用户

3. 点击“添加”按钮，弹出 SSLVPN 用户的设置窗口。
4. 输入完成后，点击“确定”按钮，或“添加下一条”按钮，添加下一个 SSLVPN 用户。

数据域说明：

表 4-33 SSLVPN 用户添加编辑数据域说明

域名	说明
用户名称	用户名称，唯一标识，符合命名规则，必须是 1－20 位字母、数字、减号、下划线的组合，不能为空。
密码	用户的密码
虚拟 IP 地址	用户建立 VPN 连接时，给用户分配的地址。可以不指定。（当修改或添加虚拟 IP 后，SSLVPN 功能需要重新启动。）
备注	用户的详细描述。

添加用户时，在页面的最下部有一个“启用”选项，只有启用后，该用户才能够连接。

编辑 SSLVPN 用户

1．点击想要对其进行编辑的 SSLVPN 用户的“编辑”图标，弹出 SSLVPN 用户的设置窗口。
2．修改完成后，点击“确定”按钮。

数据域说明，同“添加 SSLVPN 用户”。

删除 SSLVPN 用户

1．点击想要进行删除的 SSLVPN 用户的“删除”图标，在弹出的对话框中点击“确认”。
2．出现“删除成功”提示框，点击“确定”。

4.3.4 隧道监控

数据域说明：

表 4-34 SSLVPN 隧道监控数据域说明

域名	说明
用户名	名称，唯一标识，符合命名规则
连接地址	连接用户的来源 IP 地址
虚拟地址	为连接用户分配的虚拟 IP 地址
登录时间	用户建立连接的时间
发送流量	移动用户发送的流量
接收流量	移动用户收到流量

功能说明：

表 4-35 SSLVPN 隧道监控隧道功能说明

域名	说明
刷 新	刷新当前隧道状态

第5章 资源定义

为了简化防火墙安全规则的配置和维护工作，引入了资源定义。联想网御防火墙系统可以定义以下资源：

- 地址：地址、地址组、NAT 地址池、服务器地址、域名地址
- 服务：服务、服务组
- 用户：用户、用户组
- 时间：时间、时间组、一次性调度和周循环调度
- 带宽：带宽
- 深度过滤：url 组、关键字组、文件名组、邮件地址组、蠕虫过滤、过滤策略、基本配置
- VLAN ID

5.1 资源定义通用功能介绍

对于各项资源，操作基本相同，通常提供如下操作：

- 分页显示
- 查找
- 排序
- 添加资源
- 编辑资源（修改）
- 删除资源

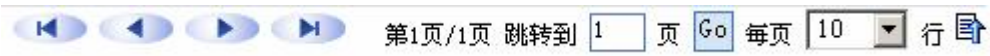
还有一些需要注意的地方，适用于所有规则，比如：

- 名称的限制
- 备注的限制

下面对这些共同的功能做一个介绍。

5.1.1 分页显示

各列表界面均有“分页功能”，其工具条通常位于表格的下方，如下图所示：



例如，点击“资源定义>>地址>>地址列表”，显示地址列表页面，就能看到上述工具条。实际上，所有资源的列表页面都有该项功能。

具体如下：

表 5-1 资源定义分页功能列表

功能	说明

	第一页
	前一页
	后一页
	最后一页
第1页/1页	当前页面/总页码
跳转到 1 页 Go	当有很多页时，可以直接跳转。输入希望跳转的页码，点击 Go 即可。 页码框只接受正整数。 如果输入页面大于总页码，则跳转到最后一页。
每页 10 行 10 20 50 100 全部	每页显示的行数
	如果出现竖向滚动条，则点击  可以回到该页页首。

5.1.2 查找

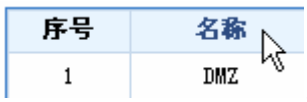
为便于查找已经定义过的资源，各列表界面均提供了查找功能，通常位于标题和列表之间，靠右排列。如下图所示：

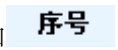
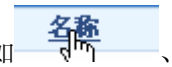
功能	说明
查找	通常为按“名称”和“备注”进行查找。 在输入框中输入待查找的关键词，点击“查找”即可。 如果输入框中为空或者默认值，则不进行筛选，列出所有资源。

5.1.3 排序

为便于查看比较资源，各列表界面均提供了排序功能。

具体如下：

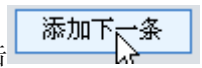
功能	说明
排序	在列表的标题部分，有两种不同的字体，如图所示  ，蓝粗体（如 名称 ）表示可以进行排序，黑

	粗体（如  ）则不能进行排序。用鼠标点击（如  ）则进行排序，升序降序交替进行，如前一次为升序排序，则下一次为降序排序。 通常按照字符串顺序进行排序（如  、  ，如果为数字项，则按数字大小进行排序（如  ）。

5.1.4 添加

各项资源最重要的功能之一就是能够添加资源，  按钮都排列在在各列表最下方的正中位置。

添加资源的操作步骤：

8. 在相应的资源列表页面中，点击  ，将弹出添加界面；
9. 给弹出界面的各域选择或者输入相应的值；
10. 点击  ，则成功添加本条规则后关闭本窗口；如果点击  ，则添加本条规则成功后刷新列表页码，本窗口不关闭，以便继续添加下一条。

点击  后弹出界面中最下方通常有三个按钮，如图所示：

功能	说明
添加下一条	点击“添加下一条”，则进行添加资源的动作，如果通过有效性检查，添加成功，则刷新列表界面，本窗口继续存在，可以继续添加其它资源。“添加下一条”通常用在同时添加若干资源的情况，不用再点击列表界面的“添加”按钮了，简化了操作过程。 在修改资源时，弹出窗口中只有“确定”和“取消”按钮，无“添加下一条”按钮。
确定	点击“确定”，则进行添加资源的动作，如果通过有效性检查，添加成功，则关闭弹出窗口，刷新列表界面。“确定”为默认操作。
取消	点击“取消”，则关闭弹出窗口，即为取消本次操作。

5.1.5 编辑

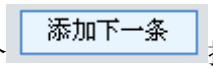
各项资源，不管是否被引用，均能随时修改。名称不能改变，其余属性可以修改。

编辑资源的操作步骤：

1. 在相应的资源列表页面中，点击对应的编辑图标（如图： 

），将弹出编辑界面
2. 输入相应的值，或者指定相应的成员（对于各项资源，值的限制不同，在各资源中进行介绍，可参考具体资源的帮助或者手册）
3. 点击 

，修改成功后关闭本窗口。

功能	说明
编辑（修改）	 点击对应资源的后，将弹出编辑框，通常，编辑框比添加框少一个  按钮，其它各项相同。 需要注意以下三点： （1） 修改时，**不能修改资源的名称**，其它各项值，均可修改。 （2） **所有资源可以随时进行修改**。例如，有一个地址“DepA”，不管它是否被安全规则等使用了，都可以进行修改。 （3） 修改成功以后**立刻生效**了。即用到了该地址的所有规则都自动更新。

5.1.6 删除

资源可以被删除，但是正在被规则引用的资源不能被删除。
删除资源的操作步骤如下：

1. 在相应的资源列表界面，点击对应的删除图标（如图： 

）
2. 弹出确认框，如图：

3. 点击 

则进行删除动作，如果该资源不能被删除，则报错；如果点击“取消”，则取消本次操作。

注意：被引用的资源不能被删除。
有两种引用方式：
被规则引用：即规则中使用了该资源

被组引用：即该资源为资源组的成员

例如，有一个地址“DepA”，如果其被安全规则等使用了，则不能进行删除。又例，地址“DepA”是地址组“GrpA”的成员，则不能删除地址“DepA”，要删除地址“DepA”，必须先到地址组“GrpA”中移出该成员。

如果确实需要删除该地址，则必须先清除所有对该资源的引用。

5.1.7 名称和备注

值域	说明
名称	所有资源都有名称，名称为必填项。 名称不能被修改。如果确实需要修改名称，则只能先删除该资源，再重新添加。 名称必须满足：1-15 字母、数字、减号、点、下划线组合，并以字母开头。 相同类型中不能重名，比如不能在地址列表中同时出现两个名称为“AAA”的地址，也不能在地址列表和地址组中出现同名。
备注	所有资源都有备注，备注为可选项。 备注中不像名称那样对输入字符串进行了严格的限制，备注中可以输入任何字符，但是必须小于 48 个字节，即 48 个英文字符或者 24 个汉字。

5.2 地址

在定义“安全策略>>安全规则”之前，一般需要按照特定的原则（比如：按部门、按人员等）定义地址资源，这样制定的安全规则比较容易阅读和理解。当部门或者人员的 IP 地址发生变化时，只需在本列表中更新即可，无需再更改安全规则。

注意：添加地址资源时最好不要超过 512 条，否则对系统性能影响较大。

5.2.1 地址列表

地址用于“策略配置>>安全规则”和“资源定义>>用户”。

可以按三种方式来定义地址：

（1） IP 地址/掩码

（2） 反 IP 地址/掩码

（3） 地址范围 IP1 － IP2。

注意：在修改地址资源时，不能修改地址的类型。

表 5-2 地址类型列表

值域	说明
IP/MASK 地址	用 IP 和掩码表示一个网段 自动用 IP 和掩码进行运算，添加成功的为一个网段。例如：输入 192.168.25.22/255.255.255.0 ，则添加成功后变为

	192.158.25.0/255.255.255.0。 如果希望指定一台主机，请选择掩码为 255.255.255.255
反 IP/MASK 地址	定义 IP 和掩码表示的网段之外的所有地址
IP1-IP2 地址段	IP1 必须小于或等于 IP2 如果只指定一台主机，可以让 IP1 和 IP2 相等

5.2.2 地址组

地址组用于“策略配置>>安全规则”和“资源定义>>用户”。
地址组的成员只能为“资源定义>>地址>>地址列表”中已经定义过的地址。

在“资源定义>>地址>>地址组”，点击 

，进行地址组添加。

表 5-3 地址组添加元素表

值域	说明
地址列表	列出所有在“资源定义>>地址>>地址列表”中定义的地址，“服务器地址”和“NAT 地址池”不能作为地址组的成员。 属于地址的成员将被移动到成员列表中，不再显示于本列表中。
地址组成员	该地址组的所有成员，成员只能是在“资源定义>>地址>>地址列表”中定义的地址。 地址组至少要有一个成员。

操作	说明
	添加成员，点击  把选中的地址移动到成员列表
	删除成员，点击  把选中的成员移动到地址列表中

5.2.3 地址池

“地址池”用于在一个网络接口上绑定多个 ip 地址。

在“资源定义>>地址>>地址池”，点击 

，进行地址池添加.

表 5-4 地址池添加元素表

值域	说明
地址	IP1 到 IP2 的一段地址范围，一个 NAT 地址池最多支持 254 个 IP 地址，IP 地址不能跨网段，计算时，A 类地址掩码为 255.0.0.0，B 类地址掩码

	为 255.255.0.0，C 类地址掩码为 255.255.255.0 IP1 必须小于等于 IP2 IP1 和 IP2 相等表示一台主机 不同的地址池之间不能有相同的 IP 地址
网络接口	地址中指定的所有地址虚拟绑定在该网络接口上。

5.2.4 服务器地址

“服务器地址”用于指定一组内部服务器地址。

在“资源定义>>地址>>服务器地址”，点击 

，进行服务器地址添加。

表 5-5 服务器地址添加元素表

值域	说明
服务器地址	填写受保护的内部服务器的 IP 地址，多个服务器提供相同服务。 最多可同时支持 8 个服务器。

5.2.5 域名地址

“域名地址”是使用域名做为安全规则中源地址和目的地址的选项。

注： 图标代表刷新域名地址的自动解析记录。域名地址支持定时自动刷新，也可以在启用“自动解析”的情况下，手工刷新域名地址对应的 IP 地址。

在“资源定义>>地址>>域名地址”，点击 

，进行域名地址添加

表 5-6 域名地址参数说明

值域	说明
名称	域名地址资源名称
域名	完整、合法的域名地址，不支持通配符
静态 IP 列表	手动添加的域名地址的 IP 地址列表。选择 IP 地址并点击“删除“，可以将 IP 地址从列表中删除；点击“清空”可以将 IP 列表清空。接着点击“确定”，可以使之生效。
静态 IP 地址	输入 IP 地址，然后点击“添加”，就可以将 IP 地址加入静态 IP 列表，接着点击“确定”，就可以使之生效
最大记录数	一个域名可以对应的静态 IP 地址和动态 IP 地址的最大数目，如果超出这个值，动态解析的 IP 地址会自动删除最旧的地址，输入范围是 1-128
自动解析	是否自动解析域名地址对应的 IP 地址，自动解析只有在开启自动解析服

	务的情况下才有效，如果关闭自动解析服务而开启或关闭自动解析都会出现错误，所以，请在开启自动解析服务时开启自动解析；在关闭所有的自动解析之后关闭自动解析服务
解析记录	自动解析域名地址对应的哪些记录，A 记录（DNS 主机记录），MX 记录（DNS 邮件交换记录）
自动解析间隔	自动解析启用的时间间隔，输入范围是 1-525600 分钟
自动解析记录失效间隔	自动解析的记录多长时间失效，这个值用自动解析间隔的倍数来表示，输入范围是 1-525600 分钟
主 DNS 服务器	主 DNS 服务器
次 DNS 服务器	次 DNS 服务器
动态 IP 列表	自动解析的 IP 地址列表，不能添加和删除
备注	域名地址的说明

注意：在 NAT 规则中使用域名地址后，在访问其它页面时要加上所有的域名。如：新浪首面的域名地址为 www.sina.com.cn，新闻页面的域名地址为 news.sina.com.cn。

5.3 服务

服务用于指定“协议 + 源端口 + 目的端口”， 可以定义四种服务：

（2） 动态服务：目前支持 H323、FTP、SQLNET、IRC、RSTP、TFTP 等动态协议

（3） ICMP 服务：可指定 type 和 code。

（4） 基本服务：可以“协议 + 源端口 + 目的端口”

（5） 服务组：把以上服务组合起来，形成一个服务组。

以下两处用到服务资源：

（1） “策略配置”下的：包过滤规则、NAT 规则、端口映射规则

（2） “资源定义”下的：用户、用户组

5.3.1 预定义服务

预定义服务定义了一些常用的服务，不可以修改，删除，只可以被引用。

5.3.2 动态服务

动态服务列表中列出了当前已定义的所有动态服务。

选中点击 

，将弹出以下界面：

图 5-1 动态服务维护

值域	说明
协议	选择要修改的动态协议类型,可以是 ftp，h323，tftp，irc，rstp，sqlnet，mms， xdmcp,h323_gk,sip
端口	协议使用的端口

5.3.3 ICMP 服务

服务列表显示当前的 ICMP 服务。

添加窗口为：

图 5-2 icmp 服务添加

值域	说明
类型（type）	ICMP 服务类型
代码（Code）	ICMP 服务代码

5.3.4 基本服务

列表中显示了当前已定义的所有基本服务。

点击 

，进行基本服务添加。

表 5-7 基本服务添加元素表

值域	说明
源端口	指定该服务请求者的端口 从低端口到高端口的一段地址范围，如果只想表示一个端口，则把低端口和高端口设成相同。 低端口小于等于高端口 端口的取值范围为 0 到 65535 源端口通常设为 0-65535，表示所有端口

目的端口	指定提供该服务的端口 从低端口到高端口的一段地址范围，如果只想表示一个端口，则把低端口和高端口设成相同的数字。 低端口小于等于高端口 端口的取值范围为 0 到 65535 目的端口通常有限的一个或者几个端口，例如 80 － 80
协议	可以设置 TCP、UDP 和其它协议。 TCP 和 UDP 协议必须指定端口，低端口和高端口必须成对出现，若低端口和高端口都没出现，则默认为 0-65535，表示所有端口。 其它协议需要指定协议号，协议号范围为 0-255，若该协议有端口的概念，则同 TCP 和 UDP；若该协议无端口的概念，则无需填写源端口和目的端口，系统默认使用 0-65535。

一个服务最少需要 1 对“协议＋源端口＋目的端口”，最多同时支持 8 对，通常少于 8 个，则依次靠前填写，剩下各行均不填写即可。

5.3.5 服务组

服务组用于“策略配置>>安全规则”和“资源定义>>用户>>用户组”。

服务组的成员可以是“资源定义>>服务>>服务列表”中已经定义过的基本服务、动态服务和 ICMP 服务。

在“资源定义>>服务>>服务组”，点击 

，进行服务组添加。

表 5-8 服务组添加元素表

值域	说明
服务列表	列出所有在“资源定义>>服务>>服务列表”中定义的所有服务，包括“预定义服务”“基本服务”“动态服务”“ICMP”。 本服务的成员将被移动到成员列表中，不再显示于本列表中。
服务组成员	列出本组的所有成员。

操作	说明
	添加成员，点击  把选中的服务移动到成员列表
	删除成员，点击  把选中的成员移动到服务列表中

5.4 用户

用户认证与“策略配置>>安全规则”配合使用，在安全规则中选中“用户认证”，则被

安全规则“允许”或者“代理”的连接必须需要经过认证才能被“允许”或者“代理”。

认证服务器在“系统配置>>联动>>用户认证服务器”中设置，支持两种认证方式：

（1） RADIUS 认证

（2） 本地认证

注意：在此“资源定义>>用户”界面中定义的用户和用户组均为本地用户认证库，只能为本地认证使用。

如果使用 RADIUS 认证方式，则用户的信息在 RADIUS 认证服务器上进行设置。

如果需要使用用户认证，必须定义用户库。在本地用户认证库中，提供了两种形式：

（1） 用户：通常指单个人，如小王、小李。

（2） 用户组：通常指有共性的人，比如同一个部门，同一种职位，等等。

注意：

（1） 用户可以不属于任何一个用户组：如刚来的新员工，还不属于任何一个部门

（2） 用户组中可以没有任何一个用户：如要成立一个新部门，还没有任何员工；又如，有一种职位，还没有任何员工

（3） 同一用户只能属于一个组。

（4） 如果用户属性和组属性发生冲突，以用户属性为准

通常，推荐先定义用户组，再定义用户。

5.4.1 用户列表

表 5-9 用户添加元素列表

值域	说明
用户名	名称必须唯一
口令	该用户用于认证的口令
生存时间	表示该用户从创建时间开始算起，可以有效使用的天数
是否允许登录	是否启用本帐号

点击相应的“编辑”按钮，弹出以下界面：

图 5-3 用户维护

界面中，显示了一些用户的状态信息。

5.4.2 用户组

表 5-10 用户组维护元素表

值域	说明
名称	名称必须唯一
分配流量	给该用户组中每个用户分配的流量 分配流量使用完毕后用户帐号将无法登录，重置后才能恢复使用 0 表示没有限制
分配时间	给该用户组中每个用户分配的时间 分配时间使用完毕后用户帐号将无法登录，重置后才能恢复使用 0 表示没有限制
本组用户	左边的列表框列出了在“用户”中定义的所有用户。 右边的列表框列出了属于本组的用户 用户组可以无任何成员

5.5 时间

很多访问控制和时间有紧密的关系。比如，上班时间不能上网浏览新闻，但是，下班时间可以。这样，就需要有时间调度策略。在“资源定义>>时间”中，可以定义灵活的时间调度方式。可以按照一次性调度和周循环调度两种方式，来定义时间。还可以把时间组合成时间组。

定义的时间和时间组在以下几处应用：

（1） 安全规则：包过滤规则、NAT 规则、端口映射规则、IP 映射规则

（2） 本地用户认证：用户、用户组的安全策略和可使用服务

（3） 拨号设备中设置自动拨号

5.5.1 时间列表

可以按照一次性调度和周循环调度两种方式，来定义时间。

表 5-11 时间资源维护元素表

值域	说明
一次性调度	指定起始和终止 年月日 时分秒 例如：2004/10/01 00:00:00 至 2004/10/07 23:59:59 为放假时间，禁止所有内部主机访问外部 INTERNET。则可在时间定义中定义一条一次性时间，再到安全规则中定义相应的规则即可。
周循环调度	每周七天，每天都可以指定起始时间和终止时间，指定 时分秒 例如：需要实现这样的功能：在工作时间禁止所有 WEB 浏览。则可以设置一条安全规则，源地址和目的地址均设为“any”，服务选择“HTTP”，时间段选择按上图设置“worktime”，其它各项使用默认值，即可。

5.5.2 时间组

时间组维护：

表 5-12 时间组资源维护元素表

值域	说明
时间列表	列出所有在“资源定义>>时间>>时间列表”中定义的时间。 时间组成员不再显示于本列表中。
时间组成员	该时间组的所有成员。

表 5-13 时间组资源操作元素表

操作	说明
	添加成员，点击  把选中的时间移动到成员列表
	删除成员，点击  把选中的成员移动到时间列表中

5.6 带宽列表

由于可供用户使用的线路带宽总是有限的，为了协调资源，优先保障重要服务，有必要进行带宽控制。

可以定义三种类型的带宽资源，非共享带宽，共享带宽和带宽资源组，只有先定义了非共享带宽后，才可以定义共享带宽，而带宽资源组是不同接口下的共享带宽的组合。

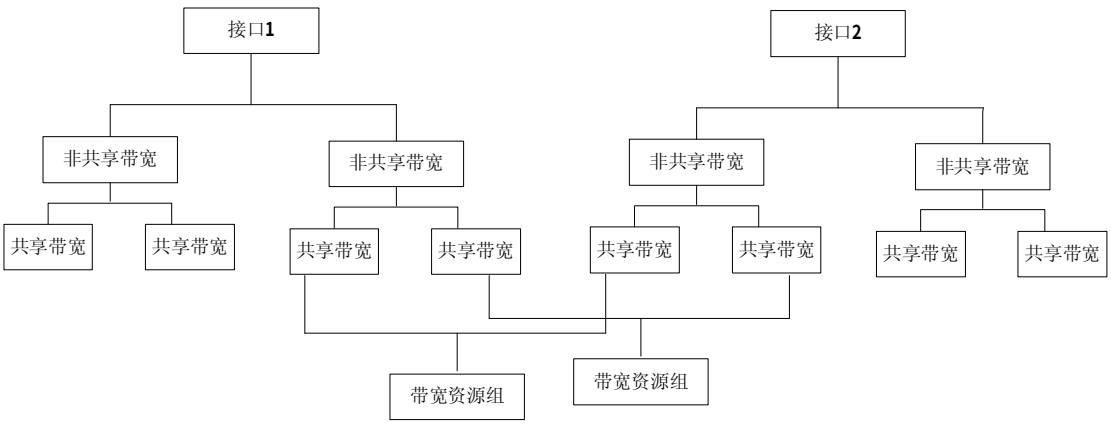


图 5-4 带宽资源关系图

定义的带宽资源组在“策略配置>>带宽管理”中被引用。

5.6.1 非共享带宽

可以增加，删除，修改非共享带宽。

表 5-14 带宽列表维护元素表

值域	说明
名称	非共享带宽的名称
接口	非共享带宽限制的接口，同一个接口下可以建立多个非共享带宽，各个非共享带宽之间不可相互借用。不能修改已经定义好的一条带宽资源的接口.
最大带宽	最大能够使用的带宽，范围为 0~1048576K，必须大于保证带宽。

5.6.2 共享带宽

可以增加，删除，修改共享带宽。

表 5-15 带宽列表维护元素表

值域	说明
名称	共享带宽的名称
优先级	当各项服务竞争带宽资源时，总是首先保障优先级高的服务，优先级那一项对应的数字越高，说明它的优先级越低。
保证带宽	保证带宽，范围为 0~1048576K。
最大带宽	最大能够使用的带宽，范围为 0~1048576K，必须大于保证带宽。
父带宽	在非共带宽中已经定义好的带宽资源，相同父带宽下的共享带宽可以相互借用带宽资源。

5.6.3 带宽资源组

可以增加，删除，修改带宽资源组。

表 5-16 带宽列表维护元素表

值域	说明
名称	带宽资源组名称，将在策略配置>>带宽管理中被引用，请保证名称不重复。
接口下的带宽	每个接口只能选择一个共享带宽作为组的成员。

5.7 深度过滤

深度过滤模块对应用层数据进行过滤，支持的协议包括 HTTP 协议、FTP 协议、SMTP 协议等。实现的功能包括 URL 过滤、网页关键字过滤、FTP 文件下载过滤、FTP 文件上传过滤、SMTP 收件人过滤、SMTP 发件人过滤、邮件主题过滤、反邮件中转过滤、Internet 蠕虫过滤等。

使用深度过滤功能，需要在**资源定义>>深度过滤**定义深度过滤资源。首先，在**资源定义>>深度过滤>>基本配置**启用深度过滤，然后定义 URL 组、关键字组、文件名组、邮件地址组等预先定义的资源，之后定义深度过滤策略，根据起用的功能点，选择不同的预先定义的资源，同时设置是否记录日志等选项。

使用蠕虫过滤功能时，在蠕虫过滤界面选择需要过滤的蠕虫，设置记录日志选项。根据设置的结果，会形成一条针对蠕虫过滤的深度过滤策略。

定义好的深度过滤策略，可以在**策略配置>>安全规则**和**资源定义>>用户>>用户组**部分选择使用。

5.7.1 URL 组

可以定义多组 URL，用于过滤策略的 URL 过滤设置。

表 5-17 URL 组维护操作列表

功能	说明
添 加	把关键词添加到关键词列表中，最多添加 50 个 URL，每个关键词不能超过 100 个字符。
删 除	删除关键词列表中选定的关键词
清 空	删除关键词列表中所有内容
导 出	到关键词列表导出成一个文本文件，每行一个关键词
导 入	把文本文件（*.txt）导入到关键词列表中，文件格式为每行一个关键词
确 定	在添加或删除或清空关键字后，生效改变

5.7.2 关键字组

可以定义多组关键字，用于过滤策略的网页关键字过滤和邮件主题过滤设置。

表 5-18 关键字组维护操作列表

功能	说明
添 加	把关键词添加到关键词列表中，最多添加 50 个关键词，每个关键词不能超过 100 个字符。

删 除	删除关键词列表中选定的关键词
清 空	删除关键词列表中所有内容
导 出	把关键词列表导出成一个文本文件，每行一个关键词
导 入	把文本文件（*.txt）导入到关键词列表中，文件格式为每行一个关键词
确 定	在添加或删除或清空关键字后，生效改变

5.7.3 文件名组

可以定义多组文件名关键字，用于过滤策略的 FTP 下载过滤和 FTP 上传过滤设置。

表 5-19 文件名组维护操作列表

功能	说明
添 加	把关键词添加到关键词列表中，最多添加 50 个文件名关键词，每个关键词不能超过 100 个字符。
删 除	删除关键词列表中选定的关键词
清 空	删除关键词列表中所有内容
导 出	把关键词列表导出成一个文本文件，每行一个关键词
导 入	把文本文件（*.txt）导入到关键词列表中，文件格式为每行一个关键词
确 定	在添加或删除或清空关键字后，生效改变

5.7.4 邮件地址组

可以定义多组邮件地址关键字，用于过滤策略的 SMTP 收件人过滤、发件人过滤、反邮件中转过滤设置。

表 5-20 邮件地址组维护操作列表

功能	说明
添 加	把关键词添加到关键词列表中，最多添加 50 个邮件地址关键词，每个关键词不能超过 100 个字符。
删 除	删除关键词列表中选定的关键词

清 空	删除关键词列表中所有内容
导 出	把关键词列表导出成一个文本文件，每行一个关键词
导 入	把文本文件（*.txt）导入到关键词列表中，文件格式为每行一个关键词
确 定	在添加或删除或清空关键字后，生效改变

5.7.5 蠕虫过滤

选择需要防范的蠕虫，设置记录日志选项。可以根据需要启用或停止蠕虫过滤。蠕虫过滤会消耗较多的系统资源，除非必要，建议一般情况下不启用蠕虫过滤。

表 5-21 蠕虫过滤数据域说明

域名	说明
名称	蠕虫的名称
描述	关于蠕虫特性的描述
生效	表示该蠕虫过滤为生效状态，点击  以后不对该蠕虫过滤变成 表示不对该蠕虫过滤，点击  以后该蠕虫过滤变成生效状态
启用蠕虫过滤	选中时，启用蠕虫过滤功能。否则，停止蠕虫过滤功能。
记录日志	强制要求对蠕虫过滤模块过滤的攻击数据包是否需要记录日志

5.7.6 过滤策略

定义深度过滤策略，使用时在**策略配置>>安全规则**设置和**资源定义>>用户>>用户组**设置中选择定义好的策略。其中，蠕虫过滤策略是在**资源定义>>深度过滤>>蠕虫过滤**定义的用于蠕虫过滤的特殊策略，不允许在此修改和删除。在每条策略的设置界面，分别定义 HTTP 协议、FTP 协议、SMTP 协议过滤的具体过滤项。最多可以定义 50 条深度过滤策略。

表 5-22 深度过滤数据域说明

域名	说明
启用 URL 过滤	选中时，启用 URL 过滤。可以选择在**资源定义>>URL 组**定义的 URL 组。
白名单方式	URL 过滤时，如果选择白名单方式，只有匹配的数据包允许通过；未被匹配的数据包禁止通过。
黑名单方式	URL 过滤时，如果选择黑名单方式，匹配的数据包禁止通过；未被匹配的数据包允许通过。
允许通过记录日志	URL 过滤时，在黑名单方式下，选中该项，则匹配的数据包允许通过，并且记录日志。
启用网页关键	选中时，启用网页关键字过滤。可以选择在**资源定义>>关键字组**定义的网

字过滤	页关键字组。
启用文件下载过滤	选中时，启用文件下载过滤。根据定义的文件名关键字，对 FTP 下载的文件进行文件名匹配过滤。可以选择在**资源定义>>文件名组**定义的文件名关键字组。
启用文件上传过滤	选中时，启用文件上传过滤。根据定义的文件名关键字，对 FTP 上传的文件进行文件名匹配过滤。可以选择在**资源定义>>文件名组**定义的文件名关键字组。
启用禁止下载	选中时，启用禁止下载，将禁止所有文件的下载，如果没有选中，则禁止下载那些匹配文件名的文件。
启用禁止上传	选中时，启用禁止上传，将禁止所有文件的上传，如果没有选中，则禁止上传那些匹配文件名的文件。
启用收件人地址过滤	选中时，启用收件人地址过滤。可以选择在**资源定义>>邮件地址组**定义的邮件地址关键字组。
启用发件人地址过滤	选中时，启用发件人地址过滤。可以选择在**资源定义>>邮件地址组**定义的邮件地址关键字组。
启用邮件主题过滤	选中时，启用邮件主题过滤。可以选择在**资源定义>>关键字组**定义的邮件主题关键字组。
启用反邮件中转过滤	选中时，启用反邮件中转过滤。只要收件人或发件人地址含指定的域名关键字，允许该邮件通过；否则，禁止通过。可以选择在**资源定义>>邮件地址组**定义的用于反邮件中转的域名关键字组。
记录日志	强制要求对深度过滤模块过滤的网络数据包是否需要记录日志

5.7.7 基本配置

深度过滤的启用消耗比较多的系统资源，会影响系统的性能，建议一般情况下不启用。通过“深度过滤控制”，可以启用或者停止深度过滤模块的运行。

对应用层数据过滤时，可以指定过滤的应用层服务端口。

表 5-23 深度过滤基本配置数据域说明

域名	说明
HTTP	设置 HTTP 协议过滤的端口，最多可以定义 5 个端口
FTP	设置 FTP 协议过滤的端口，最多可以定义 5 个端口
SMTP	设置 SMTP 协议过滤的端口，最多可以定义 5 个端口
深度过滤控制	启用或者停止深度过滤模块的运行。

5.8 VLAN ID

VLAN 的 ID 号可以通过系统自己学习获得，也可以通过用户手工配置得到，此处只显示用户配置的节点。

在 VLAN ID 中输入节点号，支持段定义，例如 3-10 代表 3、4、5、6、7、8、9、10

节点。

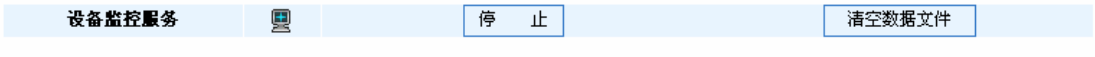
第6章 系统监控

系统监控能够显示防火墙当时的工作状态，为防火墙管理员提供了功能强大的监控工具。与联想网御集中管理软件共同使用，可以搭建全面的安全管理平台。

6.1 网络设备

网络设备监控的是启用的物理设备收发包的情况。

其中的网络设备是当前有效的物理设备，状态图标  表示设备处于启用状态，图标  表示设备处于停止状态。流量栏中显示了当前设备总发送和总接收的字节数。点击“当前状态”可以查看设备更详细的信息，点击“统计图”可以查看设备收发数据的统计图示。
如果要查看设备一段时间内的监控信息，必须先启用设备监控服务，如下图：



图标  表示监控服务正在运行，图标  表示监控服务已经停止。点击“停止”按钮可以停止监控服务，点击“启动”按钮可以启动监控服务。启动监控服务后，才可以在统计图中查看到统计数据；停止监控服务后，仍然可以查看当前设备收发数据的情况，但是无法查看历史数据。如果要清除以前的统计数据，可以点击“清空数据文件”将之清除。

点击“当前状态”后，显示设备的详细信息。

点击“统计图”后，显示统计信息，其中显示了设备“5 分钟”，“30 分钟”，“3 小时”，“一天”之内的流量统计信息，每个设备都有自己的统计图。流量的单位是兆字节，如果选择最近 5 分钟的数据，则系统每 10 秒钟记录一次流量信息，如果选择查看的时间较长，则系统记录流量信息的间隔也相应增大。如果单位时间内流量一直小于 1 兆字节，则绘制的曲线会比较贴近横坐标，不很醒目。

6.2 HA 状态

如果启用了 HA 功能，则可以进行 HA 状态监控。

在主防火墙的监控界面上，可以监控集群内所有防火墙的 HA 状态。包括：配置同步的情况，节点优先级，网口状态列表和探测周边设备状态列表。

点击详细可看到该节点的详细信息
其中主节点的“优先级”应为 1，其余从节点的“优先级”依次为 2，3，4（目前支持 4 个节点的 HA 工作模式）。节点“配置同步”的状态如果是“已同步”，则说明主节点的配置已经同步到从结点。如果没有成功同步请检查同步网口的物理和逻辑设置。从网口状态列表中可以看到各个网口连接的状态。如果设置了连接失败则节点失效，防火墙会在发现节点的一个相应网口连接失败后，将自身设置为失效，及时将网络负载切换到其它节点。探测周边设备 IP 状态列表可以使得多个连接失败后，再将自身设置为失效。

6.3 资源状态

表显示当前 CPU、内存和磁盘的利用率。

点击对应的详细信息可以查看详细的使用情况。

点击对应的“统计图”链接，可以查看相应的统计信息。

点击“启用”或“停止”按钮可以启动或关闭资源统计服务，当资源统计文件超过一定大小（400K）时，自动进行空间清理；用户也可以点击”清空数据文件“，强制删除后台统计数据存储文件。

6.4 日志信息

6.4.1 日志查看

防火墙上各功能模块均记录了详细的日志信息。

日志信息有两种处理方式：

（1） 发送给日志服务器处理：日志服务器上需安装相应的日志服务器程序。日志服务器程序提供丰富的查询、统计、报表功能，可以保存数量庞大的日志信息（受日志服务器上硬盘容量限制）。

（2） 防火墙上保留的日志：由于受到资源的限制，防火墙上最多保存 2M 日志。日志信息不能保存，断电即丢失。查询功能有限，只能按日志类型、日志级别和关键词进行查找。

推荐使用日志服务器来接收、保存、查询、统计日志信息，即配置“系统配置>>报告设置>>日志服务器”中的日志服务器 IP 和端口。 点击“设置日志服务器”链接，即可转到“系统配置>>报告设置>>日志服务器”页面，进行日志服务器的设置。

日志类型包括：包过滤，代理，入侵检测，用户认证，内容过滤，设备状态，设备管理，其它以及所有。日志级别包括：警报（紧急，一般和临界），事件（错误，警告，注意，信息和调试）和所有。NAT 日志包含在包过滤日志类型中。

注意：

1. 选中类型和级别后，需要点击“查找”按键才可以进行查找。
2. 如果关键词输入框中有内容，则同时按关键词进行查找，如果没有内容，则不按关键词查找。

6.4.2 包过滤日志报表

为了增加日志的可读性，可以对包过滤日志以表格的形式进行察看。

6.4.3 P2P 报表

可以对 P2P 日志以表格的形式进行察看。

6.4.4 深度过滤报表

可以对深度过滤日志以表格的形式进行察看。

6.5 用户信息

使用了用户认证功能，可以在本页面监控所有在线用户，登录 IP、已用时间、已用流量、组 ID、组名称、创建时间和有效时间。

管理员可以根据监控到的用户情况，通过选中待删除用户对应的复选框，点击“中断”按键，来中断该用户的连接。

6.6 连接状态

连接状态可以显示防火墙上当前的所有连接，包括协议类型、源地址、目的地址、源端口、目的端口、超时时间、状态等属性，通过“按条件查询”可以显示特定的连接。

“刷新”按钮可以按照当前查询条件，重新读取连接状态。

“全部显示”将显示全部连接，而不是查询条件限定的部分连接。

在连接状态查询界面内，可以通过协议，源地址，目的地址，源端口，目的端口来查询特定的连接。

在“滤掉以下目的地址对的连接”中输入的目的地址对将被过滤掉，不会出现在查询结果中，例如：当用户不想看到用于管理的连接时，可以输入:10.50.10.181:8888 此时，所有管理连接都被屏蔽掉了。

6.7 连接统计

系统监控的连接统计显示，可以显示防火墙状态表里的状态统计信息，包括当前并发连接数，TCP、UDP、ICMP 的连接数，TCP 连接的处于各状态的连接数，ICMP 处于非应答状态的连接数

6.8 深度过滤

系统监控的深度过滤状态显示，可以显示被防火墙深度过滤模块禁止的网络数据包统计信息，包括总统计数、HTTP 网络数据包、FTP 网络数据包、SMTP 网络数据包、蠕虫过滤攻击包的统计值。

6.9 带宽监控

联想网御防火墙提供带宽监控的功能。本页用来设置带宽监控的参数。
带宽监控能够以表的形式，显示网络接口和带宽资源的实际使用情况。

表 6-1 可监控的参数说明

域名	说明	和其他界面的关系
监控网口	要监控的网络接口，合法的接口为启用带宽管理的接口	从网络配置>>网络设备中选取接口,并设置启用接口的带宽管理
共享带宽资源	要监控的带宽资源，	从资源定义>>带宽列表>>共享带宽中选取接口
刷新时间	数据更新时间	

选择“开始监控”进入系统监控>>带宽监控>>监控状态页面。

表 6-2 监控的属性说明：

监控对象	域名	说明
网口	标定流速	接口的标准带宽
网口	实际流速	接口的实际带宽
网口	发送包数	接口当前发送的数据包数
网口	发送字节数	接口当前发送的字节数
网口	丢弃	丢弃的数据包
网口	溢出次数	溢出次数
带宽资源	标定流速	资源的设定带宽
带宽资源	实际流速	资源实际被使用的带宽
带宽资源	发送包数	资源被使用发送的数据包数
带宽资源	发送字节数	资源被使用发送的字节数
带宽资源	丢弃	资源被使用丢弃的数据包
带宽资源	溢出次数	资源被使用溢出的次数
带宽资源	借入	借用其他带宽资源发送的数据报数
带宽资源	借出	借给其他带宽资源发送的数据报数

6.10 网络调试工具

联想网御百兆防火墙提供网络调试工具，可以选择网络调试工具和参数。

表 6-3 调试工具及参数说明

调试工具名称	说明	参数	说明
ping	检测一帧数据从当前主机传送到目的主机所需要的时间	IP 地址	目的主机
traceroute	判定数据包到达目的主机所经过的路径	IP 地址	目的主机

tcpdump	检测经过防火墙的数据包	网络接口	检测的网络接口
arp	检查防火墙所能得到的 IP 与 MAC 地址对	无	
routeshow	**检查各种路由信息，包括连接路由、静态路由、动态路由、策略路由等等**	无	

选择“开始调试”进入系统监控>>网络调试工具>>调试结果。

6.11 批处理工具

联想网御百兆防火墙提供对命令行进行批处理。该页提供的功能如下：

1） 导出配置命令，批处理部分策略导出了包过滤规则和资源两个部分的命令。其中资源包括所有资源定义里的地址资源和服务资源。导出是以命令的格式导出的，可以直接导入导系统中。根据配置分类选择导出资源定义还是包过滤规则，然后点击右侧的导出按钮既可导出配置命令。直接在后台调用命令的话，包过滤默认导出到/tmp/pf.log 下面，资源定义默认导出到/tmp/addserver.log 下面。

2） 查看防火墙上执行命令行的历史记录。

3） 清空防火墙上执行命令行的历史记录，点击”清空”按钮。

4） 下载防火墙上执行命令行的历史记录，点击”导出”按钮。

5） 编辑将要执行的命令行批处理文件，在编辑框中输入想要执行的命令行语句，每一个命令行为一行，并可加入 sleep 和 beep 语句，点击”重写”按钮，可进行重新编辑，编辑完成的命令，将以黑色显示，提示用户这些命令尚未提交至防火墙。点击”提交”按钮，提交所编辑好的命令行批处理文件。

6） 上载已有的命令行批处理文件，点击”浏览”按钮，选择将要上载的命令行批处理文件，点击”导入”按钮，将该文件上载至防火墙。

7） 执行已经提交或上载了的命令行批处理文件。当已经提交或上载了批处理文件，但尚未执行时，批处理编辑框中的命令将以蓝色显示，提示用户这些命令尚未执行。点击”执行批处理”按钮，将执行批处理。

7）执行过程中，如果要中断批处理执行，请点击弹出窗口中的”取消执行”按钮。

注意：

1.在批处理执行过程中，请不要关闭弹出的窗口，也不要刷新该弹出窗口。

2.每一个命令行请顶格写，前面不要有空格。

3.sleep 和 beep 命令的格式为关键字 + 空格 + 秒数， 如：sleep 2。

4.先导出资源，后导出规则，因为规则引用了资源，因此如果先导入规则，后导入资源，则批处理时可能会失败，提示 fail。

6.12 路由监控

联想网御百兆防火墙提供对多默认路由的系统监控。本页用来显示默认路由可用的信息。

表 6-4 默认路由监控的参数说明

域名	说明
网关地址	对应默认路由默认网关的 IP 地址
权重值	对应默认路由分配的权重值
网络接口	对应的默认路由的本地网络接口名
是否有效	对应的默认路由的默认网关是否可达

注意：如果对应的默认路由的网络接口设备为拨号设备，则只有当该默认路由有效（即：拨号设备可用）时，其默认路由信息才会在该路由监控页面中出现，否则将不出现。即：对拨号设备的默认路由的有效信息是动态显示的。

6.13 动态路由监控

通过点击刷新按钮可获得当前的 OSPF 路由表。

第7章 在线支持

7.1 在线注册

在线注册直接连接到联想网御的信息安全网站 http://www.leadsec.com.cn/，用户可以在网站上注册防火墙。

7.2 技术支持

当您在使用防火墙时，如果遇到了什么问题，您可以选择“技术支持”，将为您提供几种解决问题的办法。

1. 参考随机的防火墙帮助手册
2. 登录到联想网御的防火墙支持网站 http://www.leadsec.com.cn/寻求帮助
3. 给联想的防火墙支持人员打电话寻求帮助，热线电话是：010-82167766 400-810-7766

7.3 关于

选择“关于”，出现网御防火墙 Power V 的简单说明。