天工LFW400+防火墙使用说明书

目录

第 1 章 简介 5
1.1 关于天工防火墙 5
1.1.1 病毒防护 5
1.1.2 Web 内容过滤 5
1.1.3 垃圾邮件过滤 6
1.1.4 防火墙 6
1.1.5 VLAN 和域 7
1.1.6 IPS 7
1.1.7 VPN 7
1.1.8 双机热备 7
1.1.9 安全安装，配置和管理 7
1.2 文档约定 8
1.3 天工防火墙文档 8
1.4 客户服务及技术支持 9
第 2 章 防火墙配置方法 10
2.1 连接 PC 和防火墙 10
2.2 登录配置防火墙 11
第 3 章 WEB 管理界面 13
3.1 基于 WEB 的管理页面 13
3.1.2 本手册的组织结构 15
第 4 章 系统管理 状态 16
4.1 状态 16
4.1.1 查看系统状态 16
4.1.2 更改系统信息 18
4.2 会话 18
第 5 章 系统管理 网络 20
5.1 域 20
5.1.1 域的设置 21
5.2 接口 21
5.2.1 接口设置 22
5.3 管理地址 25
5.3.1 管理地址的设置 26
5.4 别名地址 26
5.4.1 别名地址的设置 27
5.5 IP 池 27
5.5.1 IP 池的设置 28
5.6 DNS 29
第 6 章 系统管理 DHCP 31
6.1 服务 31

6.1.1 配置 DHCP 服务 31
6.2 分配范围 32
6.2.1 配置 DHCP 分配范围 32
6.3 排除范围 33
6.3.1 配置排除范围 34
6.4 IP/MAC 绑定 35
6.4.1 配置 IP/MAC 绑定 35
第 7 章 系统管理 配置 36
7.1 时间设置 36
7.2 选项 36
7.3 HTTP 登录端口 37
7.4 高可靠性 38
7.4.1 HA 基本设置 38
7.4.2 HA 节点 39
7.4.3 心跳接口 41
7.4.4 链路检测 42
7.5 SNMP 43
7.5.1 SNMP 代理基本设置 43
7.5.2 配置 SNMP 团体 43
7.6 生成树 45
7.6.1 配置网桥 45
7.6.2 网桥端口 46
7.6.3 配置网桥端口 46
第 8 章 系统管理 管理员设置 48
第 9 章 系统管理 维护 50
9.1 备份与恢复 50
9.1.1 保存配置 50
9.1.2 备份配置 50
9.1.3 恢复配置 51
9.1.4 升级 52
9.1.5 授权文件 52
9.1.6 支持 52
9.1.7 命令检测 52
9.1.8 关机 53
第 10 章 设置用户 54
10.1 用户 54
10.2 RADIUS 服务器 55
10.3 用户组 56
第 11 章 认证用户 58
第 12 章 路由 60
12.1 静态路由 60
12.2 策略路由 61

第 13 章 防火墙 64
13.1 策略 64
13.2 地址 67
13.2.1 地址 67
13.2.2 地址组 69
13.3 服务 70
13.3.1 预定义 70
13.3.2 定制 71
13.3.3 组 72
13.4 时间表 73
13.4.1 单次时间 73
13.4.2 循环时间 74
13.5 保护设置 76
13.6 NAT 策略 77
13.6.1 虚拟 IP 78
13.6.2 NAT 策略的生效 81
13.7 MAC 绑定 81
第 14 章 虚拟专网 83
14.1 IPSEC 83
14.1.1 阶段 1 83
14.1.2 阶段 2 86
14.1.3 手动模式 87
14.1.4 VPN 隧道 89
14.1.5 阶段 1 状态 91
14.1.6 阶段 2 状态 91
14.1.7 IPSec 使用中的特殊情况 92
14.2 PPTP 92
14.2.1 PPTP 分配地址范围 92
14.2.2 PPTP 状态 93
14.3 L2TP 94
14.3.1 L2TP 分配地址范围 94
14.3.2 L2TP 状态 95
14.4 证书 95
14.4.1 本地证书 96
14.4.2 CA 证书 98
第 15 章 入侵防御 99
15.1 特征 99
第 16 章 防病毒 101
16.1 HTTP 设置 101
16.2 SMTP 设置 101
16.3 POP3 设置 102
第 17 章 WEB 防护 104

17.1 HTTP 设置 104
17.2 扩展名 105
17.2.1 例外扩展名 105
17.2.2 禁用扩展名 105
17.3 MIME 类型 106
17.3.1 例外 MIME 107
17.3.2 禁用 MIME 107
17.4 站点过滤 108
17.5 URL 过滤 109
17.6 关键字过滤 110
第 18 章 垃圾邮件过滤 112
18.1 SMTP 设置 112
18.2 POP3 设置 113
18.3 垃圾邮件过滤设置 114
18.4 黑名单 115
18.5 白名单 116
18.6 RBL 列表 117
18.7 关键字 118
第 19 章 日志与报告 120
19.1 日志配置 120
19.1.1 日志设置 120
19.1.2 邮件告警 121
19.1.3 日志过滤 122
19.2 日志访问 124
19.2.1 配置日志 124
19.2.2 事件日志 125
19.2.3 流量日志 127
第 20 章 退出系统 128
第 21 章 附录 A 案例配置 129
第 22 章 注意事项 130

第1章 简介

天工防火墙支持基于网络的应用级的服务部署，包括病毒防护和全面的内容扫描过滤。天工防火墙增强了网络安全性，防止不需要的网络服务的使用，最大程度降低网络风险，确保网络有效地通讯。天工防火墙包括防火墙，IPSec，防病毒等功能服务。

本章将介绍以下内容：

- 关于天工防火墙
- 帮助文档资料
- 最近的帮助文档
- 客户服务及服务热线

1.1 关于天工防火墙

天工防火墙是一个容易管理的网络安全设备，它提供一套完整的，包括各种级别的服务，主要分为两大类：

应用级的服务，如病毒防护和内容过滤等。

网络级的服务，如防火墙策略过滤，VPN，流量控制等。

天工防火墙对事件处理进行优化，采用全新的内容分析技术，明显提高了网络性能、安全性及内容过滤能力。独特的体系架构，实时地监控网络中进出入的数据，最大地保护网络，使公司服务部署在安全的范围之内。

天工防火墙还支持一些高级功能，如 802.1Q 的 VLAN，双机热备等。

1.1.1 病毒防护

天工防火墙病毒防护功能会自动检测通过天工防火墙的网页(HTTP)和电子邮件(SMTP, POP3)的内容。它通过模式匹配找出病毒。如果找到符合特征的病毒，防火墙会根据已设定的规则，对病毒作出相应的动作：或者丢弃，或者放行并给用户提示。

另外，用户通过指定允许通过的文件类型也可以增强病毒防护功能。

1.1.2 Web内容过滤

防火墙的 Web 内容过滤功能能够深入检测 HTTP 的数据流内容，包括站点，网址和网页内容。如果当前的站点或网址已被列入黑名单，或者网页内容中的关键字加权值总和处于被禁止的范围，则该页面不能被访问，取而代之的是防火墙的一个提示警告页面。用户可以配置过滤的站点、网址和关键字。

用户还可以对访问的页面中的包括的文件和 MIME 进行过滤。例外扩展名指定了可以通过的文件类型，禁止扩展名即是不允许通过的文件类型；例外 MIME 表示允许的 MIME 类型，禁止的 MIME 即是不允许的 MIME 类型。除此之外，用户也可以配置上传文件大小，记录 HTTP 请求的日志。

1.1.3 垃圾邮件过滤

防火墙的垃圾邮件过滤能够扫描 POP3，SMTP 电子邮件内容。你可以根据 E-mail 地址，邮件内容来过滤垃圾邮件。垃圾邮件可以被特别提示或者清除。

使用 dcc 和贝耶斯自学习功能能够更加有效地检测垃圾邮件。

如果防火墙发现一封垃圾邮件，它可以在邮件中加入头标记或者重写邮件主题。邮件接收人可以通过他们邮件客户端软件过滤含有这么标记的邮件。防火墙也可以配置成直接删除垃圾邮件。

1.1.4 防火墙

天工防火墙能有效保护你的网络使它免受互联网的威胁。当对防火墙完成基本的配置后，防火墙默认是禁止内部网络的用户直接访问互联网的。你可以按需要很方便地配置各种对互联网的控制访问。

天工防火墙策略可以进行以下控制：

- 控制网络的所有进出入数据
- 对数据进行病毒检查和过滤
- 可以启用或禁用策略
- 当单条策略生效时进行控制
- 接收或禁止指定地址的数据
- 控制已有或自定义的服务及服务组合
- 用户通过认证后才能访问服务
- 在策略中指定连接数限制及流量控制
- 在策略中启用流量日志
- 应用级防护（包括 http、smtp 和 pop3）
- 天工防火墙可以运行在 NAT/路由模式、透明模式以及混合模式下。

1. NAT/路由模式

在防火墙运行在 NAT/路由模式时，它相当于一个三层设备。这意味着每个接口都位于一个不同的 IP 子网，对于其它设备来说，每个接口相当于一个路由设备。这种设置是防火墙最常见的。

在 NAT/路由模式时，你可以创建 NAT 模式策略和路由模式的策略。

NAT 模式时，策略通过地址转换把从安全网络到不安全网络的地址隐藏起来。

路由模式时，策略接受或禁止网络间的连接，但没有进行地址转换。

2. 透明模式

当天工防火墙运行在透明模式时，防火墙没有改变网络的三层拓扑结构。这意味着所有的接口都位于相同的网络，对于别的设备来说，每个接口相当于一个网桥。一般来说，防火墙运行在透明模式时主要用来提供病毒防护和内容过滤功能，而在其之前已经存在另外一个防火墙方案。

透明模式时，防火墙仍然能象 NAT 模式那样为网络提供基本的保护。防火墙会根据策略放行或阻塞它收到的数据包。防火墙可以接入网络的任何一个地方，而且不需

要对网络或者其它设备作改动。然而，一些高级防火墙功能仍然只能在 NAT/路由模式时才起作用。

3. 混合模式

混合模式是同时包含了路由模式和透明模式的配置模式，即同时包含路由接口和二层网桥接口。使用混合模式可以综合透明模式和路由模式的优点，扩展防火墙的工作模式。

1.1.5 VLAN和域

天工防火墙支持 IEEE 802.1Q 兼容的虚拟局域网（VLAN）技术。域可以理解为网络接口的集合，我们可以把网络接口或几个 VLAN 归于一个域中。使用 VLAN 技术，防火墙可以为单个 VLAN 或多个 VLAN（域）提供安全的服务，并能管理不同 VLAN，不同域之间的数据及连接。防火墙能把策略应用域和域之间以及同一个域的内部。防火墙也可以对 VLAN 内部网络进行用户认证，内容过滤和病毒防护。

天工防火墙支持运行在 NAT/路由和透明模式时也支持 VLAN。在 NAT/路由模式时，你可以从 VLAN 子接口中接收和发送数据。

1.1.6 IPS

天工防火墙入侵检测系统（IPS）根据各种入侵特征来防止可能的入侵活动并保护你的系统。你可以对具有特征的数据进行通过、丢弃、重置、重置客户端或重置服务器端等动作，也可以把这些动作记入到日志中。

1.1.7 VPN

虚拟专网（VPN）能为你分布在广域网中的各种办公网络之间建立起安全的网络连接，和安全的通信，在公司外面的用户可以通过 VPN 安全地连接到公司内部网络。

1.1.8 双机热备

天工防火墙支持双机热备功能（HA），为网络提供高可靠性。双机热备是通过 serial 和 udp 的心跳包来检测对端设备（防火墙）的可用性，支持主-从和主-主两种模式。通过心跳包，来检测对端设备的运行状态。任何一台设备出现异常，另外一台设备都可以承载对端设备原来的载荷。

1.1.9 安全安装，配置和管理

当天工防火墙第一次启动时，它已经含有一些 IP 地址及安全策略的基本配置。请连接到 WEB 管理界面，查看系统运行状态，并且根据你的网络的实际情况对它重新配置，完成后防火墙就能对你的网络产生保护作用。使用 WEB 管理界面你能对防火墙进行大多数的高级配置。

你也可以使用命令管理界面（CLI）方式来配置防火墙。

1. WEB界面

在任何一台支持浏览器的电脑上，通过 HTTP 或安全 HTTPS 可以连接到防火墙上，进行配置和管理防火墙。WEB 管理界面目前只支持中文语言。你可以通过配置指定任意一个接口作为 HTTP 或 HTTPS 的管理接口。

通过 WEB 管理界面，你可以对防火墙进行大部分的配置。通过 WEB 界面也能监视防火墙的运行状态。通过 WEB 界面更改配置会立即生效，不需要重启防火墙或重启服务。当你对某个配置满意时，你可以把它下载来。下载下来的配置文件在可以用来防火墙配置的恢复。

2. 命令行界面

通过数据线把一台主机串口连接到防火墙 RS-232 串口控制终端可以进入防火墙的命令行管理界面。在一个网络环境中，你也可以通过 Telnet 或 SSH 连接到防火墙的命令行界面，包括互联网。

正如 WEB 界面那样，命令行界面同样支持对防火墙进行配置和查看系统的运行状态。另外，用命令行界面你能进行 WEB 界面不支持的高级操作。管理员操作手册包含基本和高级的命令的用法，欲需要更详细信息，请参考天工防火墙命令行参考手册。

3. 日志及报告

天工防火墙支持流量及事件的各种级别日志记录。主要功能有：

- 报告与防火墙连接的流量信息
- 报告使用的网络服务
- 报告策略允许的流量
- 报告策略拒绝的流量
- 报告事件，例如配置修改，其它管理员登录，IPSec 隧道流通，病毒检查攻击和阻止页面访问记录
- 报告入侵检查到的攻击
- 发邮件给管理员报告病毒事件，入侵和防火墙或者 VPN 事件或其它非法事件。
- 日志也可以发送到远程日志服务器。

1.2 文档约定

本文档对配置命令的语法采用以下格式：

尖括号<>表示变量

例如：

restore2fm <filename>

你可能输入：

restore2fm myfile.bak

竖线和大括号{ | }用来分隔可替换的、相互的不包含或需要的关键词，例如：

set opmode { nat | transparent }

1.3 天工防火墙文档

请到天工网站下载最新的文档：http://www.lenovonetworks.com

1.4 客户服务及技术支持

请访问天工网站查看最新的服务支持：http://www.lenovonetworks.com

第2章　防火墙配置方法

2.1　连接PC和防火墙

将防火墙接上电源并打开开关加电。检查 power 指示灯，如果未亮，请检查电源连接是否正常；如果已亮，则使用交叉/直连网线将电脑和防火墙的 **E0** 口相连接。然后按以下步骤操作：

检查 E0 口的指示灯，如果已亮转步骤 B；否则检查网线、网卡是否故障。

在计算机网卡上配置 IP 地址和子网掩码，步骤如下：

开始 —> 控制面板 —> 网络连接，左键双击打开网络连接

右键单击其中“本地连接”图标，在弹出的上下文菜单中单击“属性”菜单。

选中“Internet 协议（TCP/IP）”。如图（图 1-1）：

图 1-1

单击“属性”按键，设置计算机的 IP 地址：192.168.1.100，子网掩码：255.255.255.0。然后点击确定，完成网卡设置，如图(图 1-2)：

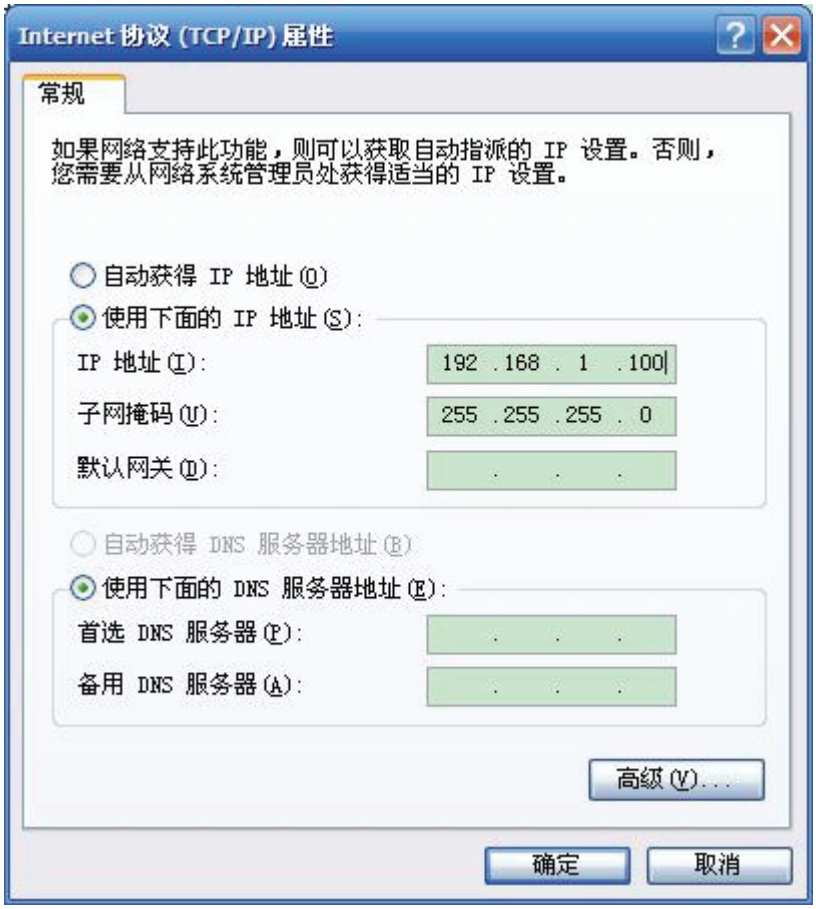


图 1-2

测试计算机与路由器是否连通

开始 —> 运行 —> 键入“cmd” —> 确定

在命令提示符使用 ping 命令测试是否连通。执行：ping 192.168.1.1

如果显示：

Reply from 192.168.1.1: bytes=32 time<10ms TTL=64

表示连接成功，转下一步进入配置，否则表示可能未能正确连接。请检查 TCP/IP 设置是否正确，网线是否故障。

2.2 登录配置防火墙

通过 Web 浏览器（如 Internet Explorer）进行路由器的配置。

打开Internet Explorer浏览器，在地址栏中输入http://192.168.1.1:2000/将会出现登录面(图 1-3)。

图 1-3

输入正确的用户名与密码后即登录（默认的用户名为：admin；密码为：admin）。登录成功后浏览器即会显示具体的配置页面。

第3章 WEB管理界面

在任何一台支持浏览器的电脑上，通过 HTTP 或 HTTPS 可以进入 WEB 管理界面，对防火墙配置管理。目前防火墙只支持中文一种语言。你可以指定防火墙哪一个接口开启 HTTP 或 HTTPS 管理端口。

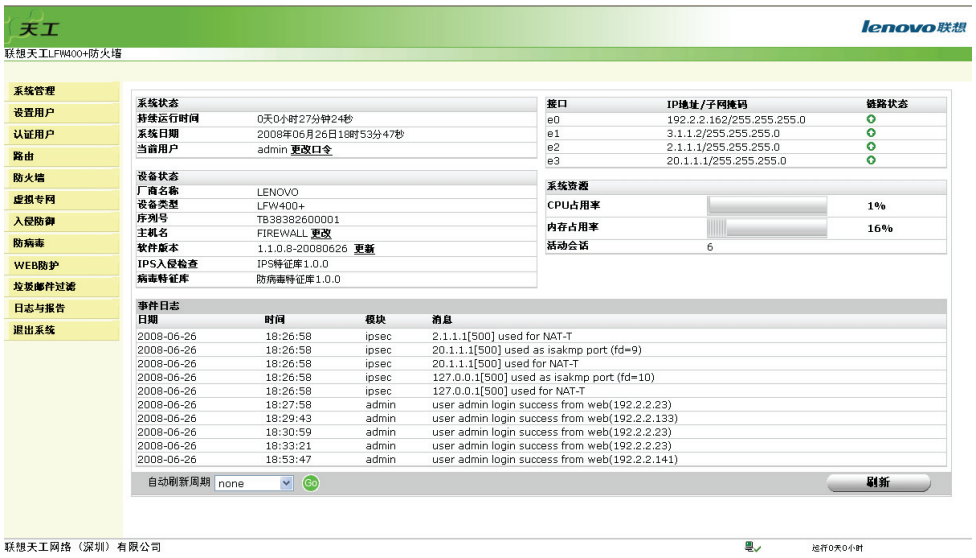


图 WEB 登录初始化页面

通过 WEB 管理界面，你可以对防火墙进行大部分的配置。通过 WEB 界面也能监视防火墙的运行状态。通过 WEB 界面更改配置会立即生效，不需要重启防火墙或重启服务。当你对某个配置满意时，你可以把它下载来。下载下来的配置文件在可以用来防火墙配置的恢复。

3.1 基于WEB的管理页面

基于 WEB 的管理界面由菜单和页面组成，它们一般都含有多个标签。以系统管理为例，它展开后包含几个子菜单。当你选择一个子菜单时，就会打开与之关联页面的第一个标签。如果想查看其它标签，直接点击其它标签的名字。

在本手册中，到一个指定的页面的顺序是：先到打开特定的菜单栏目，再到子菜单和它的标签，如：

1 系统管理 -> 网络 -> 域

图：WEB 管理界面范例。

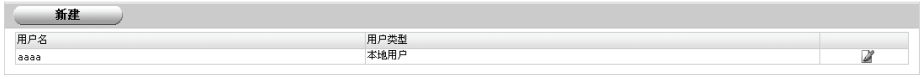
1. WEB管理菜单

本菜单提供了防火墙大部分主要配置的入口：

系统管理	配置系统的网络功能如域和接口，管理地址，DNS，DHCP，时间，管理用户，系统升级维护。
设置用户	创建防火墙策略中需要认证的用户账号、用户组或Radius服务器。
认证用户	配置允许哪个用户组的用户认证。
路由	配置静态路由或策略路由。
防火墙	配置防火墙策略和保护设置，也包含NAT地址转换及MAC地址绑定。
虚拟专网	配置虚拟专网VPN。
入侵防御	配置入侵检查系统。
防病毒	配置病毒防护。
WEB防护	配置WEB防护及内容过滤。
垃圾邮件过滤	配置垃圾邮件过滤。
日志与报告	配置日志与报告。
退出系统	注销退出系统。

2. 列表

很多 WEB 管理页面都是列表形式，如域、接口、防火墙策略，认证用户等等。



图：接口列表

列表显示了项目的一些信息，在列表的最右列，是对项目的可操作图标。在上图中，你可以对单条项目进行删除或编辑操作。

如果想新建一个项目，就点击“新建”按钮。点击“新建”按钮会打开一个对话框，让你填写项目的各种信息。“新建”按钮打开的对话框跟“编辑”图标打开的对话框类似。

3. 图标

WEB 管理界面不但含有按钮，还有不少图标来满足用户和系统的交互。以下是一些

名称	描述
编辑	编辑项目，点击后会出现项目信息对话框。
删除	删除项目，点击后会出现确认删除对话框。
插入	插入项目，点击后会在当前项目前上插入新的项目。
移动	移动项目，点击后会出现移动顺序对话框。
下载	点击后将下载文件。
显示	显示文本项目内容。
开始	开始执行某个动作。
加入组	把处于左边组的可选项目加入到右边组里
从组删除	把位于右边组的项目删除，删除的项目重新出现在左边组里，可以被选择。

WEB 管理界面常见的图标的含义：

4. 状态栏

状态栏就是 WEB 管理界面最下端那栏。

图： 状态栏

状态栏显示：

系统自从上次启动后运行了多长时间。

3.1.2 本手册的组织结构

本手册将照 WEB 管理菜单介绍 WEB 管理页面，每一个系统菜单的项目都有相应的介绍页面。

第4章　系统管理 状态

你可以连接到 WEB 管理界面查看当前的系统状态。状态页面显示了当前系统状态、设备状态、系统资源、接口状态和系统最近 10 条日志及会话情况。

4.1　状态

状态页面就象系统的仪表，通过观察状态页面，我们可以知道当前系统的总体运行情况。系统所有具有读权限的用户都能查看系统状态页面。

具有写权限的用户（配置用户），可以更改状态页面的一些属性如主机名，也可以对升级系统。下面介绍：

查看系统状态

更改系统信息

4.1.1　查看系统状态

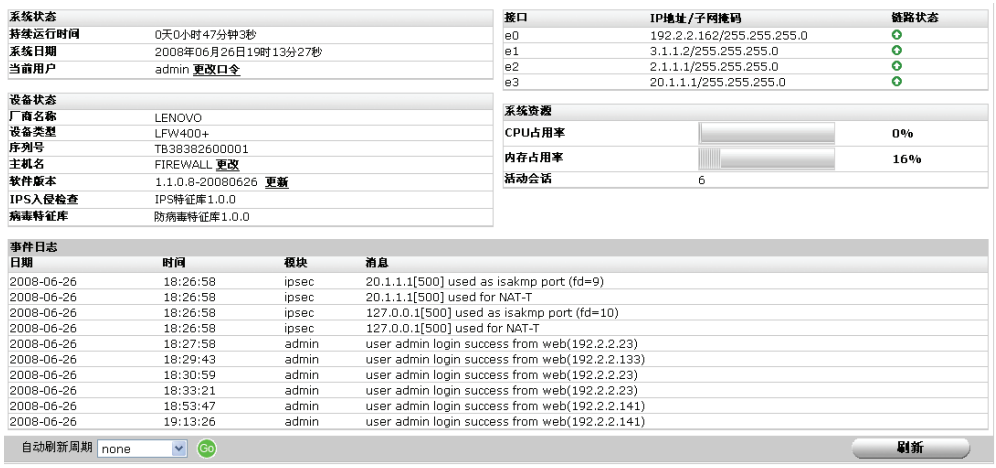


图　系统状态查看页面

1. 系统状态

持续运行时间	系统从上次启动到现在持续运行的时间。
系统日期	防火墙系统当前时间。
当前用户	当前登录的用户。

2. 设备状态

厂商名称	防火墙厂商名称
设备类型	防火墙设备的类型
序列号	防火墙序列号

主机名	防火墙系统的主机名
软件版本	防火墙系统软件版本。
IPS入侵检查	IPS入侵检查软件版本。
病毒特征库	病毒特征库软件版本。
序列号	防火墙序列号标识。

3. 接口状态

接口	显示系统默认接口名称
IP地址/掩码	显示接口的IP地址及掩码，如果接口没配地址即显示为空
链路状态	显示接口的链路状态

4. 系统资源

CPU占用率	系统当前CPU占用率
内存占用率	系统当前内在占用率
活动会话	系统当前活动会话数目。

5. 事件日志

日期	事件日志产生的日期
时间	事件日志产生的时间
模块	事件日志所属的子模块
消息	事件日志消息的具体内容

6. 自动刷新周期

自动刷新周期	启用自动刷新周期后，状态页面可以定时自动刷新。
Go	应用选择的自动刷新时间周期。
刷新	手动刷新状态页面。

4.1.2 更改系统信息

具有读写权限的配置管理员通过状态页面可以更改的信息有：

- 改变主机名称
- 升级系统版本

1. 改变主机名称

防火墙的主机名称在状态页面和命令行界面提示符中都有显示。SNMP 中也使用到主机名称。请参考 SNMP 一章。

默认的主机名是 FIREWARE。

进入系统管理 > 状态 > 系统状态。

在设备状态栏中，找到主机名那行，点更改。

输入新的主机名。

点击 OK 按钮。

改变后的主机名会立即显示在系统状态页面和命令行的提示符里，也会加到 SNMP 系统名里。

2. 升级软件版本

升级版本详细内容请参看“升级”一章：系统管理 > 维护 > 升级。

4.2 会话

会话列表显示当前系统所有的连接会话信息。

图 会话列表查看页面

列项	说明
源IP	设置查找的源IP
源端口	设置查找的源端口
目的IP	设置查找的目的IP
目的端口	设置查找的目的端口
查找	根据查找条件查找会话
	连接的服务协议，如 TCP，UDP 或者 ICMP
有效期	会话有效的时间（单位：秒）

查看会话列表：

系统管理 > 状态 > 会话

WEB 管理界面的会话列表显示所有的活动会话，每页显示 10 个。

通过点击上一页，下一页，首页，尾页图标来查看其它页会话。

通过填写 IP 地址和端口来查找 会话。

第5章 系统管理 网络

系统网络设主要置防火墙与你目前网络的连接和交互。最基本的就是配置防火墙接入你当前的网络和设置 DNS。高级的设置即包括域和 VLAN 子接口的设置。本章主要有：

- 域
- 接口
- 管理地址
- 别名地址
- IP 池
- DNS

5.1 域

域（zone）可以理解为接口的集合。通过域，可以把相关的接口或 VLAN 子接口组合在一起，这样为应用策略提供了方便。例如把一个或多个接口或 VLAN 组合成一个域后，对此域应用策略后，此域下的所有接口或 VLAN 都受到影响，这样比指定单个接口或 VLAN 更实用。

在域列表中，你可以新建、编辑和删除域，更改域名。当你新建一个域后，可以把接口或 VLAN 归于这个域。

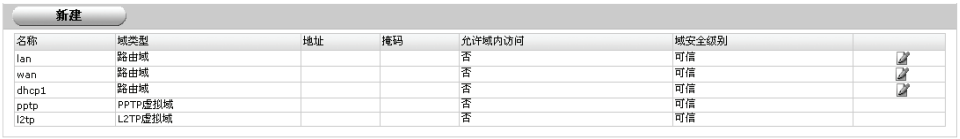


图 域列表查看页面

列项	说明
名称	域的名称。
域类型	域的类型（路由域或透明域）。
地址	域的地址。如果是透明域，IP地址可有可没。
掩码	域的掩码。如果是透明域，掩码可有可无。
允许域内访问	是否允许域内相互访问。
域安全级别	域的安全级别（可信，不可信，DMZ）。
	删除
	编辑/查看

表 域列表选项

5.1.1 域的设置

图 新建域页面

设置项	说明
名称	域的ID，长度必须小于或等于6个字符。
域类型	域的类型（路由域/透明域）
域 /IP地址	透明域我们可以设置域接口地址。
掩码	透明域我们可以设置域接口地址掩码
允许域内访问	选择后域内的接口之间可以相互访问。
域安全级别	标识域的安全等级。

表 新建域配置项

配置过程：

- 进入系统管理 -> 网络 -> 域。
- 点击新建按钮，进入新建域页面
- 输入域的名字。
- 选择域的类型。
- 勾选是否允许域内访问。
- 选择域的安全级别。
- 点击“确定”按钮。

5.2 接口

接口列表显示了防火墙所有的接口（包括物理接口及 VLAN）。物理接口不能新建删除，是预设定的。VLAN 接口可以新建、编辑和删除。通过修改接口参数，可以影响防火墙与网络的连接。

图　接口列表查看页面

列项	说明
名称	物理接口或VLAN接口的名称。
域	接口所属的域。
IP地址	接口的IP地址。
掩码地址	接口地址的掩码。
网络接口状态	接口的开关状态。
访问权限	接口所提供的访问服务。主要有： ☑ HTTPS ☑ PING ☑ HTTP ☑ SSH ☐ SNMP ☑ TELNET 如果想到从WEB管理页面，至少提供HTTP或HTTPS服务。
	删除
	编辑/查看

表　接口列表选项

5.2.1　接口设置

接口部分包括两种类型：一是物理接口；二是 vlan 虚拟接口。对于物理接口，我们只能编辑操作，而 vlan 接口，我们可以新建、编辑和删除。接口设置对话框显示物理接口或 VLAN 子接口的当前设置。通过设置接口对话框，可以新建一个 VLAN 子接口，或者改变物理接口或 VLAN 子接口的设置。

当一个接口起作用时，不能改变接口的名称。

图 编辑物理接口页面

设置项	说明
名称	接口名称，系统预定义
所属域	所属域的名称
地址类型	接口地址类型包括手动指定、pppoe拨号和dhcp获取三种方式
IP地址	当接口类型为自定义时，表示手动指定的接口地址
掩码地址	当接口类型为自定义时，表示手动设定的接口地址掩码
用户	当接口类型为pppoe时，表示pppoe拨号时的用户帐号
密码	当接口类型为pppoe时，表示pppoe拨号时的用户帐号密码
覆盖本地DNS	当接口类型为pppoe或者dhcp时，表示是否覆盖本地的DNS，即自动设置本地dns。
启用ddns	是否启用动态域名注册
Ddns服务器	提供动态域名的服务器
Ddns帐户	Ddns服务器注册帐号
Ddns密码	Ddns服务器注册帐号密码
动态域名	注册的动态域名
Ping服务器	启用ping服务器检测
访问权限	设置接口的访问权限，包括https,ping,http,ssh,snmp,telnet
接口速率	设置物理接口工作速率 
接口模式	当物理接口速率不为“自适应”时，可设置网络接口工作模式为全双工或半双工： 
Mtu值	设置接口mtu值。为了提高网络的传输性能，你可以改变防火墙的数据包的最大传输单元（MTU），这个影响到所有的接口。理想上来说，MTU值必须与防火墙内所有网络及数据包目的地网络的最小MTU值一致。如果防火墙发送的数据包过大，它们就会被分割成较小的片断，这样降低了传输速率。通过实验慢慢减小MTU值，可以找到适合网络的MTU值。 要改变MTU值，先删除默认的MTU值（1500），然后输入新的MTU值。如果地址类型为自定义或DHCP，MTU值可为576~1500字节。 提示：在透明模式时，如果你改变了一个接口的MTU值，你需要改变所有其它接口的MTU值，使它们跟此接口MTU值一致。

表 设置物理接口选项

物理接口配置过程：

- 进入系统管理->网络->接口页面
- 点击编辑，进入编辑接口页面
- 选择接口所属域
- 选择接口地址类型。对于自定义类型，输入 IP 地址/掩码；对于 pppoe 类型，输入认证用户/密码，选择是否覆盖本地 DNS；对于 dhcp 类型，选择是否覆盖本地 DNS。
- 对于 pppoe 或者 dhcp 地址类型，选择是否启用 ddns。如果启用 ddns，输入 ddns 服务器地址、动态域名、注册帐号和注册帐号密码。
- 选择是否启用 ping 服务器。如果启用，输入 ping 服务器地址。
- 选择访问权限。
- 点击“确定”，完成配置。

与编辑物理接口类似，下面是新建 VLAN 部分。

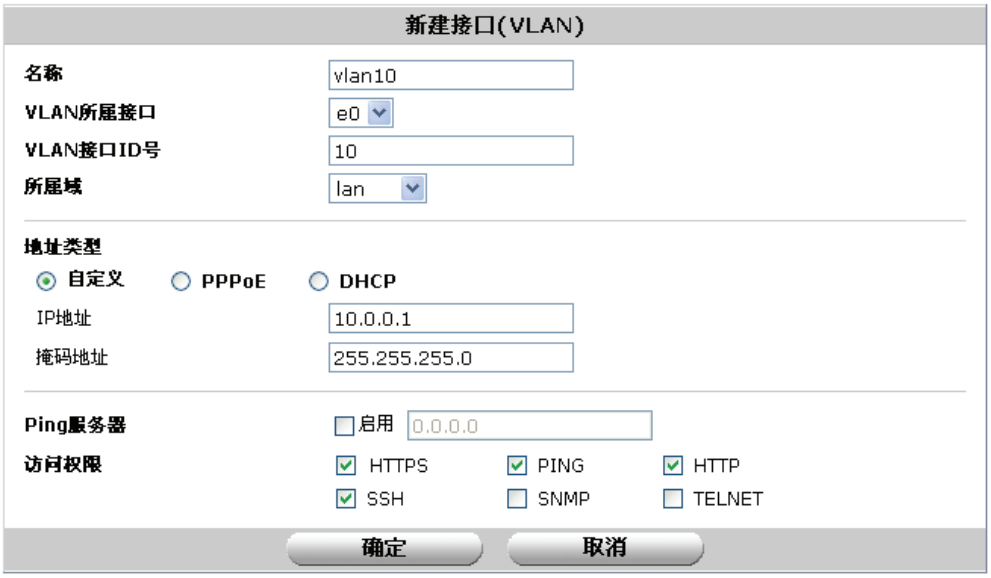


图 新建 VLAN 接口页面

设置项	说明
名称	接口名称，系统预定义
Vlan 所属接口	Vlan接口对应的物理接口
Vlan接口ID	Vlan id号
所属域	所属域的名称（该域可以是路由域或着透明域。当选择的域是透明域时，防火墙可以配置成“网桥模式vlan trunk透传”。应避免某个物理接口和该物理接口所属的vlan都配置为同一个透明域）
地址类型	接口地址类型包括手动指定、pppoe拨号和dhcp获取三种方式

IP地址	当接口类型为自定义时，表示手动指定的接口地址
掩码地址	当接口类型为自定义时，表示手动设定的接口地址掩码
用户	当接口类型为pppoe时，表示pppoe拨号时的用户帐号
密码	当接口类型为pppoe时，表示pppoe拨号时的用户帐号密码
覆盖本地DNS	当接口类型为pppoe或者dhcp时，表示是否覆盖本地的DNS，即自动设置本地dns。
启用ddns	是否启用动态域名注册
Ddns服务器	提供动态域名的服务器
Ddns帐户	Ddns服务器注册帐号
Ddns密码	Ddns服务器注册帐号密码
动态域名	注册的动态域名
Ping服务器	启用ping服务器检测
访问权限	设置接口的访问权限，包括https,ping,http,ssh,snmp,telnet

表　设置 vlan 接口选项

VLAN 接口配置过程：

- 进入系统管理->网络->接口页面
- 点击新建，进入新建 VLAN 页面
- 选择 vlan 所属接口，设置 vlan id
- 选择接口所属域
- 选择接口地址类型。对于自定义类型，输入 IP 地址/掩码；对于 pppoe 类型，输入认证用户/密码，选择是否覆盖本地 DNS；对于 dhcp 类型，选择是否覆盖本地 DNS。
- 对于 pppoe 或者 dhcp 地址类型，选择是否启用 ddns。如果启用 ddns，输入 ddns 服务器地址、动态域名、注册帐号和注册帐号密码。
- 选择是否启用 ping 服务器。如果启用，输入 ping 服务器地址。
- 选择访问权限。
- 点击“确定”，完成配置。

5.3　管理地址

管理地址指可以管理防火墙的 IP 地址，为了安全，你可以设定能连接上管理页面的 IP。防火墙产品出厂默认有一个管理地址。

图　管理地址列表查看页面

列项	说明
接口	管理地址所使用的物理接口。
管理IP	管理地址的IP。
掩码	管理IP的掩码。
	删除
	编辑/查看

表　管理地址列表选项

5.3.1　管理地址的设置

新建一个管理地址：

图 新建管理地址页面

设置项	说明
接口	管理地址所使用的物理接口
管理IP	管理地址的IP
掩码	管理IP的掩码

表 新建管理地址配置项

进入系统管理 -> 网络 -> 管理地址

点击新建按钮

选择管理地址所连接的接口。

填写管理 IP 地址。

填写 IP 地址的掩码。

点击“确定”按钮。

5.4　别名地址

别名地址就是为接口指定一个其它的 IP 地址。

图 别名地址列表查看选项

列项	说明
接口	别名地址的接口。
掩码	别名地址的掩码。
	删除
	编辑/查看

表 别名地址列表选项

5.4.1 别名地址的设置

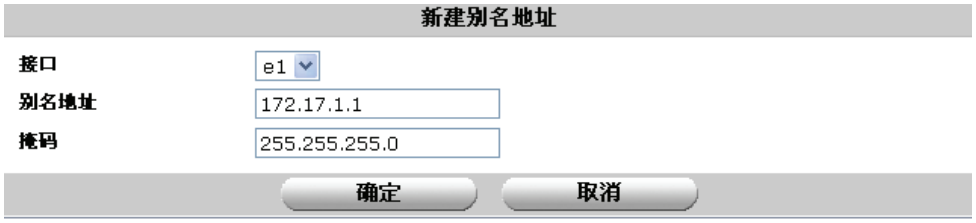


图 新建别名地址页面

设置项	说明
接口	选择别名地址的接口
别名地址	填写别名地址
掩码	填写别名地址的掩码

表 新建别名地址配置项

新建别名地址：

进入系统管理 -> 网络 -> 别名地址

点击新建按钮。

选择别名地址的接口。

填写别名地址。

填写别名地址的掩码。

点击“确定”按钮。

5.5 IP池

IP 池（也称动态 IP 池）指应用在防火墙接口的一个 IP 地址段。当你在防火墙 SNAT 策略中开启池功能后，出口数据包就会从 IP 池中随机地选择一个地址作为 IP 源地址。

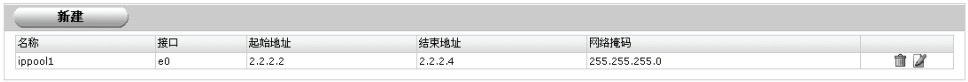


图 IP 地址池列表查看页面

列项	说明
名称	IP池的名称。
接口	IP池的作用接口。
起始地址	IP池的起始地址。
结束地址	IP池的结束地址。
网络掩码	IP池地址掩码，必须为C类以上掩码。
	删除
	编辑/查看

表 IP 地址池列表选项

5.5.1 IP池的设置

图 新建 IP 地址池页面

设置项	说明
名称	IP池的名称。
接口	IP池的作用接口。
起始地址	IP池分配的起始地址。
结束地址	IP池分配的结束地址。
网络掩码	IP池地址的掩码，必须是C类以上掩码，如255.255.255.0

表 新建 IP 地址池配置项

进入系统管理 > 网络 > IP 池。

输入 IP 池的名称。

选择 IP 池的接口。

输入 IP 池的起始地址。

输入 IP 池的结束地址。

输入 IP 池地址的掩码。

点击“确定”按钮。

5.6 DNS

防火墙的不少服务都使用 DNS 服务，比如邮件警告跟 URL 过滤。你可以增加防火墙能连接上的 DNS 地址。DNS 地址一般都是你的 ISP 提供的。

你可以配置你的主 DNS 或备用 DNS 服务器地址，也可以让防火墙自动获取 DNS 服务器地址。为了自动获取 DNS 地址，防火墙至少有一个接口启用了 DHCP 或 PPPoE 服务。参看接口部分。

如果某接口启用了 DNS 转发，此接口相连网络的主机就能把当前接口 IP 地址当作 DNS 服务器地址。发送到此接口的 DNS 请求会转发到你配置的或自取获取的 DNS 服务器地址。

图 DNS 设置页面

设置项	说明
自动获取	DNS服务器地址是自动获取的，当有接口类型选择启用获取dns时生效。
手动设置	手动设置DNS服务器地址。
主DNS地址	手动设置主DNS地址
备用 DNS 地址	手动设置备用DNS地址
启用 DNS 转发	启用DNS地址的转发，需要选择转发的接口。
转发接口	选择启用DNS地址转发的接口。

表 DNS 设置选项

DNS 设置过程：

- 选择 DNS 地址获取模式，自动获取/手动设置

- 对于自动设置方式，需要在接口部分启用 pppoe 或者 dhcp 的接口上启用覆盖本地 DNS。
- 对于手动设置方式，输入主 DNS 地址和备用 DNS 地址
- 如果需要启用 DNS 中继，则选择 DNS 转发选项以及选择转发网络接口
- 点击“确定”完成

第6章　系统管理 DHCP

6.1　服务

你可以对防火墙的任何接口包括 VLAN，配置 DHCP 服务或 DHCP 中继代理服务。防火墙的一个接口完全可以当作一个 DHCP 服务器或 DHCP 中继器来用，但一个接口不能同时提供这两种服务。

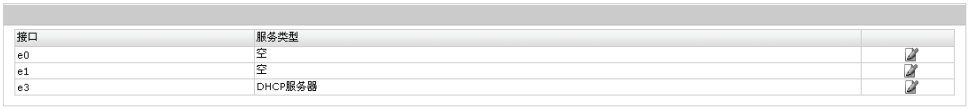


图 DHCP 服务列表查看页面

列项	说明
接口	接口名称
服务类型	选择DHCP服务类型（空、DHCP中继和DHCP服务器）
	编辑/查看

表　dhcp 服务列表选项

6.1.1　配置DHCP服务

图 设置 DHCP 服务页面

设置项	说明
接口	启用dhcp服务的接口名称
服务类型	选择DHCP服务类型（空，DHCP中继，DHCP服务器）。
DHCP 服务器地址	当启用DHCP中继服务时， 填写DHCP服务器的IP。跟接口连接的网络的主机都会使用此DHCP服务器。

表　设置 dhcp 服务选项

配置 DHCP 服务过程：

进入系统管理->DHCP->服务

点击对应接口的编辑选项

选择服务类型。如果选择 DHCP 中继，输入 DHCP 服务器地址

点击“确定”完成。

6.2 分配范围

你可以为防火墙的接口配置 DHCP 分配范围。当接口配置成 DHCP 服务器时，接口会根据分配范围为与它相连的网络主机动态地分配 IP 地址。

图 分配范围列表查看页面

列项	说明
名称	DHCP分配范围名称。
接口	DHCP分配范围的接口。
默认路由	默认的路由地址。
	删除
	编辑/查看

6.2.1 配置DHCP分配范围

图 新建 dhcp 分配范围页面

设置项	说明
名称	分配范围的名称

接口	DHCP服务的接口
域名	填写DHCP服务器指派给客户端的域名。
开始地址	分配范围的开始地址。
结束地址	分配范围的结束地址。
租赁时间	地址的有效租赁时间，单位为分钟。超过租赁时间后客户端需要向服务器重新请求地址，服务器会给客户端分配新的地址。
主DNS服务器地址	主DNS服务器地址。
备用DNS服务器地址	备用DNS服务器地址。
WINS服务器1	WINS服务器1地址。
WINS服务器2	WINS服务器2地址。
地址掩码	分配地址的掩码。
默认路由	服务器分配给客户端的默认路由地址。

表　新建 dhcp 分配范围设置项

新建 DHCP 分配范围过程：

- 进入系统管理 > DHCP > 分配范围
- 点击新建按钮，进入新建 DHCP 分配范围页面
- 输入名称
- 选择接口
- 输入域名
- 输入开始地址
- 输入结束地址
- 输入租赁时间
- 输入主 DNS 服务器地址
- 输入备用 DNS 服务器地址
- 输入 WIN 服务器 1 地址
- 输入 WIN 服务器 2 地址
- 输入地址掩码
- 输入默认路由地址
- 点击“确定”完成

6.3　排除范围

排除范围设定了不能分配到客户端的 IP 地址范围。例如，当我们设定分配范围为 192.168.18.10~192.168.18.20 时，我们想保留地址 192.168.18.16~192.168.18.18

不会分配到客户端，这时就可以把 192.168.18.16~192.168.18.18 设为排除范围。当设定排除范围后，所有的分配范围都不能包括此排除范围的地址。

页面位置 ：网络管理 > DHCP > 排除范围

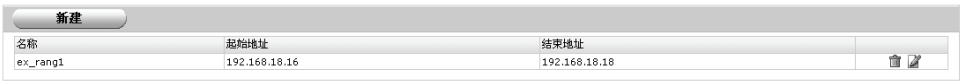


图 排除范围列表查看页面

列表	说明
名称	排除范围的名称。
起始地址	排除范围的起始IP地址。
结束地址	排除范围的结束IP地址。
	删除
	编辑/查看

表 排除范围列表选项

6.3.1 配置排除范围

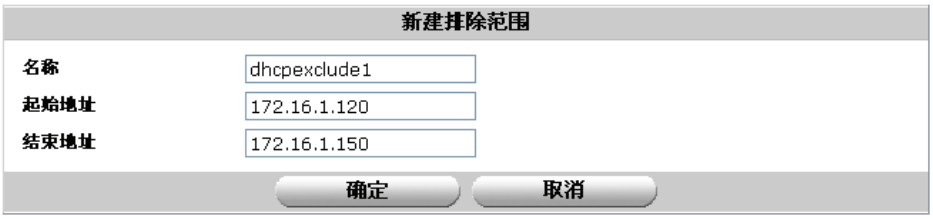


图 新建排除范围页面

设置项	说明
名称	填写排除范围的名称。
起始地址	填写排除范围的起始IP地址。
结束地址	填写排除范围的结束IP地址。结束地址跟起始地址要在同一网段。

表 新建排除范围设置项

新建排除范围过程：

- 进入系统管理 > DHCP > 排除范围。
- 点击新建按钮，进入新建 DHCP 排除范围页面
- 输入名称、起始地址、结束地址
- 点击“确定”完成

6.4 IP/MAC绑定

如果你新建了 DHCP 服务器，你可以用 IP/MAC 绑定，根据设备的 MAC 地址来为网络上的特定设备保留一个 IP 地址。当一个 IP 跟 MAC 地址绑定后，DHCP 服务器会把该 IP 分给该 MAC 地址的设备。IP/MAC 之间的绑定关系对所有的 DHCP 服务器起作用。

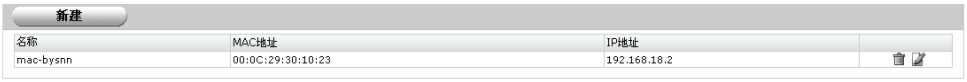


图 IP/MAC 绑定列表查看页面

列项	说明
名称	IP/MAC绑定的名称。
MAC地址	被绑定的设备的MAC地址。
IP地址	被绑定设备的IP地址。
	删除
	编辑/查看

表 DHCP IP/MAC 绑定选项

6.4.1 配置IP/MAC绑定

图 新建 IP/MAC 绑定页面

设置项	说明
名称	IP/MAC绑定的名称。
MAC地址	被绑定的设备的MAC地址。每个网卡都有一个唯一的MAC地址。
IP地址	被绑定设备的IP地址。

表 新建 IP/MAC 绑定选项

新建 IP/MAC 绑定过程：

- 进入系统管理 > DHCP > IP/MAC 绑定
- 点击新建按钮，进入新建 DHCP IP/MAC 绑定页面
- 输入名称、MAC 地址、IP 地址
- 点击“确定”完成

第7章　系统管理 配置

通过配置页面你可以更改很多系统参数及配置。

7.1　时间设置

到系统管理 > 配置 > 时间设置页面，可以配置系统的时区及时间。

图 时间设置页面

设置项	说明
刷新	手动刷新页面，显示系统最新时间。
时区选择	选择所在的时区。北京，上海，香港，乌鲁木齐都采用GMT+8。
时间设置	手动设置时间的年、月、日、时、分、秒。
与NTP服务器同步	系统时间自动与NTP服务器同步。
服务器	选择“与NTP服务器同步”后填写NTP服务器的地址。
同步间隔	选择“与NTP服务器同步”后填写同步的时间间隔，单位为分钟。

表　时间设置选项

系统时间配置过程：

进入系统管理->配置->时间设置

选择时区

在手动时间设置模式下，选择时间选项（年、月、日、时、分、秒）

在时间同步模式下，输入同步时间服务器地址和同步周期

点击“确定”完成

7.2　选项

选项设定系统页面超时时间，语言版本和网关检测等参数。

页面位置：系统管理 > 配置 > 选项。

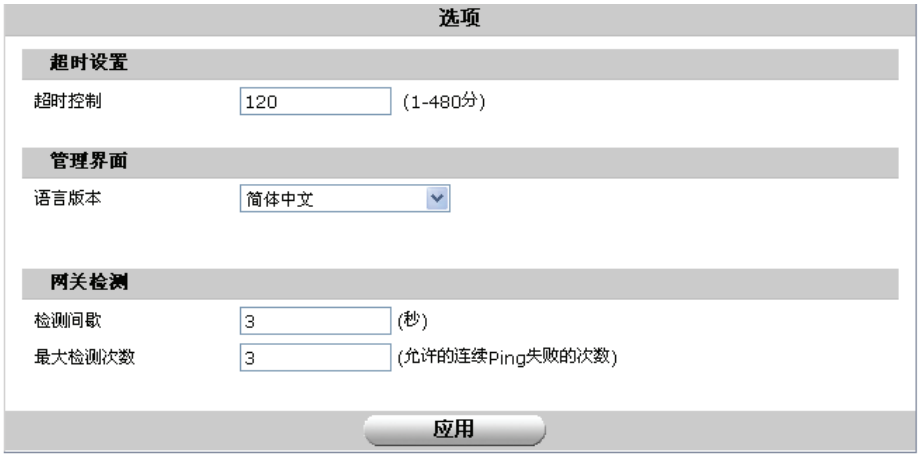


图 系统选项设置页面

设置项	说明
超时控制	设置页面超时退出的时间。当页面无操作、空闲的时间大于此时间后，页面会自动退出，要求重新登录。单位为分钟。
语言版本	选择防火墙的语言版本，目前只支持中文版本。
检测间歇	设定网关检测间隔时间。系统每隔一定时间自动检测网关，以判断与网关的连通性。
最大检测次数	网关检测的最大次数，即是允许的连续Ping失败的次数。当Ping失败次数达到此次数后，会认为网关不可到达。

表 系统选项设置选项

系统选项设置过程：

- 进入系统管理->配置->选项
- 输入超时时间
- 选择语言版本，目前只支持简体中文
- 输入网关检测间隔和网关检测最大检测次数
- 点击“应用”完成

7.3 HTTP登录端口

设定防火墙管理界面的 HTTP 登录端口。

图：HTTP 登录端口

端口号	填写HTTP登录端口，范围1~65535，默认值是2000。

7.4 高可靠性

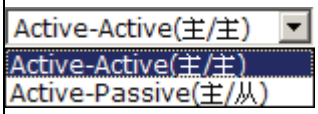
HA 是 high available 缩写，它通过 serial 和 udp 的心跳包来检测对端设备（防火墙）的可用性，支持主-从和主-主两种模式。

通过心跳包，从而检测对端设备的运行状态。在主-从模式下，在两台设备都运行正常的情况下，只有主设备独自工作，从设备处于 holding 状态，只有主设备出现故障时，从设备通过心跳链路检测到主设备的异常，它才会将自己状态改变为 active，将所有资源（地址、连接等）转移到自身，担当起主设备的工作，当主设备恢复正常后，它会再将自身状态置为 holding。而主-主模式下，两台设备都同时运行，任何一台设备出现异常，另外一台设备都可以承载对端设备原来的载荷。

位置：系统管理 > 配置 > 高可靠性

7.4.1 HA基本设置

图 双机热备基本设置页面

设置项	说明
单机模式	单机模式，即防火墙没有工作在双机热备模式下。
高可靠性	两台以上防火墙时，可以开启双机热备功能，即高可靠性。
模式	 选择（主/主）或（主/从）模式。
主设备强占	是否启用主设备强占功能，主从模式下的主设备以及主主模式下的设备都需要开启该项
密码	两防火墙设备互相通信时的密码。

重新输入密码	再输入一次两防火墙设备互相通信时的密码。

表　HA 基本设置选项

HA 基本设置配置过程：

进入系统管理->配置->高可靠性

选择工作模式（单机模式/高可靠性）

在高可靠性模式下，选择 HA 工作模式（主/主模式或者主/从模式）

选择是否主设备强占，工作在主模式下的 HA 节点必须选择该项

输入 HA 节点间通讯密码

点击“应用”完成

7.4.2　HA节点

HA 节点指双机热备的主机节点，一般一台防火墙就可设置为一个节点。

图 HA 节点列表查看页面

列项	说明
名称	HA节点的名称。
类型	类型，可能是主节点、备用节点或虚拟IP。
接口	虚拟IP所在的接口。
接口地址	虚拟IP的地址。
	删除
	编辑/查看

表 HA 节点列表查看选项

1. 配置HA节点

图 新建 HA 节点页面

设置项	说明
名称	HA节点的名称。
节点类型	选择节点的类型（主节点、备用节点）。

表　新建 HA 节点设置项

新建 HA 节点过程：

进入系统管理 > 配置 > 高可靠性

点击新建节点按钮，进入新建 HA 节点页面

输入节点名称，节点名称为 HA 集群中主机名称

选择节点类型

点击“确定”完成

2. 心跳虚拟IP

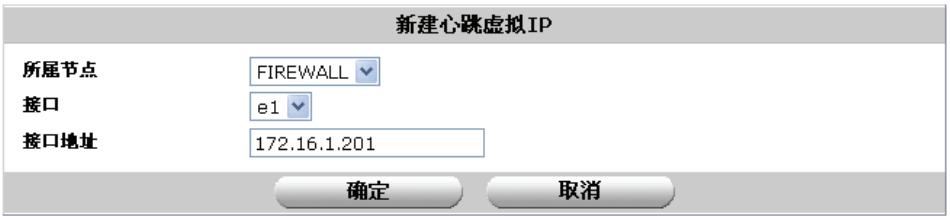


图 新建心跳虚拟 IP 页面

设置项	说明
所属节点	选择虚拟IP所属的节点。
接口	选择虚拟IP所在的接口。
接口地址	虚拟IP的地址。
	删除
	编辑/查看

表 新建心跳虚拟 IP 选项

新建心跳虚拟 IP 配置过程：

进入系统管理->配置->高可靠性

点击新建虚拟 IP 按钮，进入新建虚拟 IP 页面

选择所属节点

选择所属接口

输入虚拟 IP 地址

点击“确定”完成

7.4.3 心跳接口

心跳接口指的是 HA 主机用来发送心跳包的媒介，包括串行口和网络接口。

图 心跳接口列表页面

列项	说明
名称	心跳接口的名称。
类型	接口类型（串行口、单播、多播和广播）。
接口	当接口类型为单播、多播或广播时所应用的接口。
对端地址	对端防火墙的IP地址。
串行端口号	当串口类型为“串行口”时的端口号。
	删除
	编辑/查看

表 心跳接口列表选项

1. 配置心跳接口

图 新建心跳接口页面

设置项	说明
名称	心跳接口的名称。
类型	接口类型（串行口、单播、多播和广播）。
串行端口号	当接口类型为“串行口”时的端口号。
接口	当接口类型为“单播”、“多播”和“广播”时，所应用的接口。
对端地址	当串口类型为“单播”或“多播”时，对端防火墙的地址。

表 新建心跳接口配置项

新建心跳接口配置过程：

- 进入系统管理->配置->高可靠性

- 点击新建心跳接口按钮，进入新建心跳接口页面
- 输入名称
- 选择心跳接口类型。串行口类型下，输入串行端口号；单播模式和多播模式下，选择接口，输入对端地址；广播模式下，选择接口。
- 点击“确定”完成

7.4.4 链路检测

链路用来检测接口连接的线路是连通的或者断开的。

图 链路检测列表查看页面

列项	说明
检测地址	检测的IP地址。
	删除
	编辑/查看

表 链路检测列表选项

1. 配置链路检测地址

图 新建链路检测地址页面

设置项	说明
检测地址	链路检测的IP地址。

表 新建链路检测地址配置项

新建链路检测配置过程：

进入系统管理->配置->高可靠性

点击新建链路检测，进入新建链路检测页面

输入检测地址

点击“确定”完成

7.5 SNMP

SNMP(Simple Network Management Protocol)即简单网络管理协议，包括对网络设备信息的获取和对网络设备管理两部分。

网络信息的获取是指对网络中的节点设备（路由器，防火墙等）的运行状态信息进行查看，如查看网络设备的网络接口信息（地址、流量等）。而对网络设备的管理功能是指对于远程网络设备进行管理配置操作，包括网络接口地址的设定等。

7.5.1 SNMP代理基本设置

图 SNMP 代理基本设置页面

设置项	说明
SNMP代理	选择是否启用SNMP代理功能。
描述	SNMP的描述。
位置	SNMP位置。
联系	SNMP的联系地址。

表 snmp 代理设置选项

SNMP 代理基本设置过程：

进入系统管理->配置->SNMP

选择是否启用 SNMP 代理

输入描述、位置、联系

点击“应用”完成

7.5.2 配置SNMP团体

图 SNMP 团体列表查看页面

列项	说明
团体名称	SNMP团体名称。

查询	是否启用SNMP查询
陷阱	是否启用SNMP陷阱功能。防火墙暂不支持此功能。
启用	选择是否启用该团体。
	删除项
	编辑项

表 snmp 团体列表选项

图 新建 SNMP 团体页面

设置项	说明
团体名	SNMP团体名称。
新建	新建一个管理主机。最多能建立3个管理主机。
IP地址	管理主机的地址格式类似“192.168.1.0/24”这种格式。
删除	删除管理主机。
查询	是否启用SNMP查询
协议	选择查询的协议（v1/v2c）。
启用	选择启用的查询协议。
	删除一个管理主机IP地址。

表 新建 snmp 团体配置项

新建 SNMP 团体过程：

进入系统管理->配置->SNMP

点击新建 SNMP 团体，进入新建 SNMP 团体页面

输入团体名称

新建管理主机地址

选择查询协议版本

点击“确定”完成

7.6 生成树

生成树协议是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。生成树协议可以通过只允许流量通过单一路径抵达网络的其他端口防止在冗余的交换或者桥接网络中出现环路除非必要情况通常在主链路中断时否则所有冗余路径全被阻塞。我们可以使用生成树协议(stp)来实现二层下的双机热备。

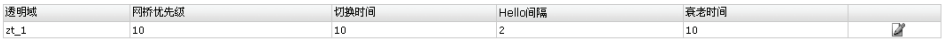


图 生成树网桥列表查看页面

列项	说明
透明域	透明域的名称。
网桥优先级	生成树网桥的优先级。
切换时间	生成树切换时间。
Hello间隔	生成树Hello间隔。
衰老时间	衰老时间。
	编辑/查看

表 生成树网桥列表项

7.6.1 配置网桥

图 设置生成树网桥参数页面

设置项	说明
启用	是否启用生成树网桥。
透明域	网桥所在的透明域的名称。
网桥优先级	生成树网桥的优先级。
切换时间	生成树切换时间。
Hello间隔	生成树Hello间隔。

衰老时间	衰老时间。

表　生成树网桥部分设置项

网桥配置过程：

进入系统管理->配置->生成树

编辑网桥，进入网桥编辑页面

选择启用 STP

输入网桥优先级、切换时间、hello 时间和衰老时间

点击“确定”完成

7.6.2　网桥端口

图 生成树接口列表查看页面

列项	说明
端口	生成树的端口名称。
接口路径耗费	接口的路径耗费值。
接口优先级	接口的优先级。
	编辑/查看

表　生成树接口列表选项

7.6.3　配置网桥端口

页面位置：系统管理 > 配置 > 生成树。

图　设置生成树接口参数页面

设置项	说明
端口	生成树的端口名称。
接口路径耗费	接口的路径耗费值。
接口优先级	接口的优先级。

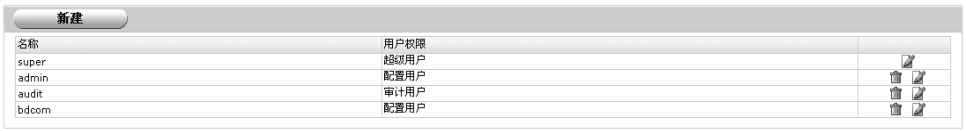
表　设置生成树接口选项

STP 接口配置过程：

- 进入系统管理->配置->生成树
- 编辑 STP 接口，进入接口编辑页面
- 输入接口路径耗费和接口优先级
- 点击“确定”完成

第8章　系统管理 管理员设置

管理员配置主要用来配置系统管理的用户，包括超级管理员（super），配置管理员(admin)和审计管理员(audit)。超级管理员能够新建和修改所有管理员用户信息；配置管理员及审计管理员只能修改自己的密码。以下是超级管理员能看到的管理员用户列表。



图：管理员列表查看页面

列项	说明
名称	管理员账号名称
用户权限	管理员类型（super, admin, audit）。
	删除项
	编辑项

表 管理员列表选项

图　新建管理员账号页面

设置项	说明
名称	管理员账号名称
用户密码	管理员密码。
确认密码	再次输入管理员密码。
用户权限	管理员类型（超级用户，配置用户，审计用户）。 超级用户能新建管理员账号，修改所有管理员信息。但不能配置系统。但不能下载和删除日志。 配置用户不能新建管理员账号，但能修改自己账号密码。还能配置系统。但不能下载和删除日志。 审计用户不能新建管理员账号，但能修改自己账号密码。不能配置系统，但能下载

	和删除日志。

表 新建管理员用户配置项

新建系统管理员过程：

进入系统管理->管理员配置

只有超级管理员有新建权限

点击新建按钮，进入新建管理员页面

输入用户名称、密码

选择用户级别

点击“确定”完成

第9章 系统管理 维护

系统管理包含了防火墙的备份与恢复配置文件、升级、客服支持、命令检测和注销、重启关机等控制。

9.1 备份与恢复

备份允许你把对防火墙当前配置保存起来，或把所有配置文件打包成一个文件下载保存，下次你可以通过恢复配置文件并上传文件就能把防火墙恢复到当前的配置。

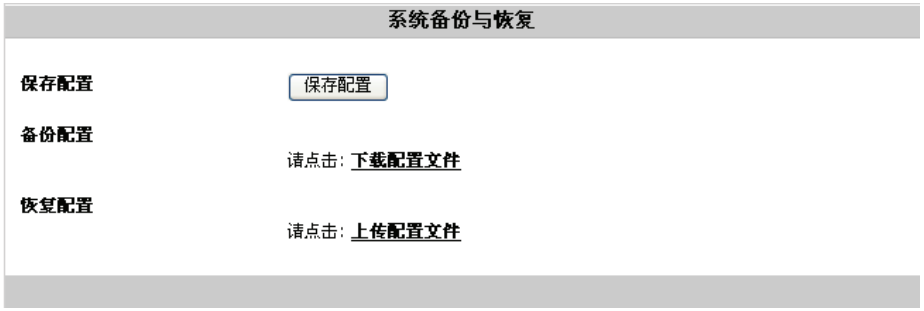


图 系统备份与恢复

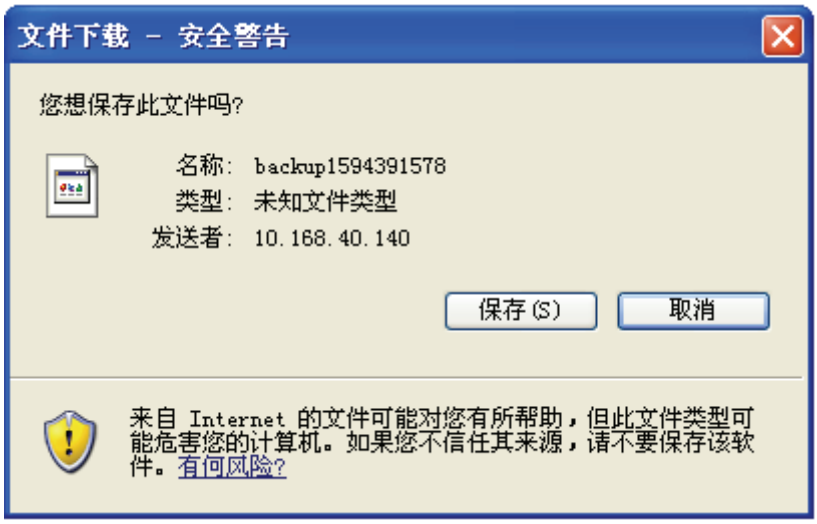
保存配置	让防火墙把当前配置保存起来，下次开机时会读入当前配置。
备份配置	备份当前配置。点击“下载配置文件”再输入密码把当前配置保存，并加密提供打包下载。
恢复配置	通过上传配置文件让系统恢复以前的配置。

9.1.1 保存配置

点击 OK 按钮防火墙开始保存配置，保存时间视系统运行情况而定，一般大概几秒就保存完毕。

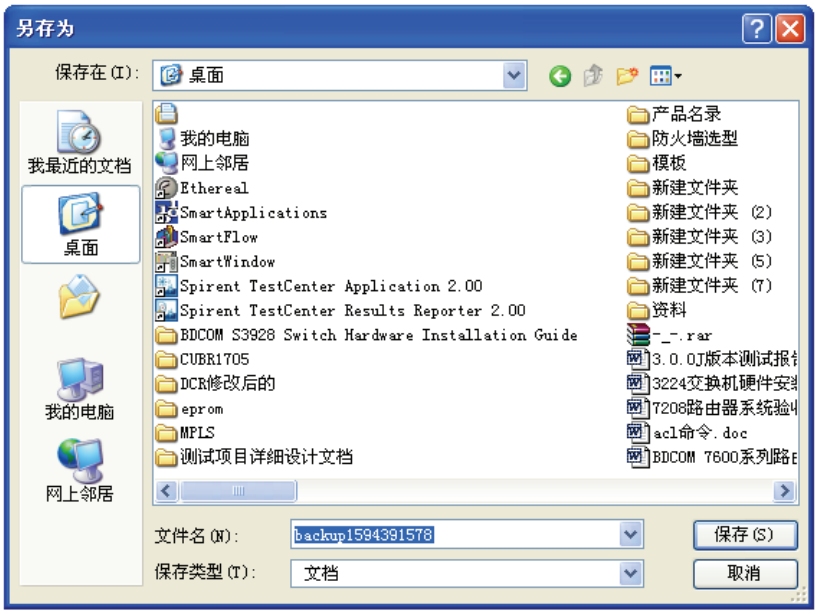
9.1.2 备份配置

图：点击“下载配置文件后”，输入用户自设的密码对配置文件加密。



图：下载文件，如有安全警告，请选择“保存”。

如没有下载文件提示框，请关闭电脑上所装的防火墙软件，或使用标准的 IE 或 FIREFOX 浏览器下载。



图：选择保存的位置，点“保存”，完成配置文件的下载

9.1.3 恢复配置

点击“上传配置文件”，显示如下对话框。

图：上传配置文件。

密码	输入解压密码。此密码跟下载配置时用户自设的密码一致，否则配

	置文件不能被系统解压。
配置文件	点击“浏览”选择需上传的配置文件。

如果密码和配置文件正确，系统会提示“恢复系统配置成功！”。

9.1.4 升级

天工防火墙支持不断更新升级，以保证软件最新最安全。用户可能到天工网站下载最新的升级包来升级。

图：系统升级

上传文件	选择所要上传的升级包。最新升级包可到天工网站下载。

9.1.5 授权文件

授权文件包含了防火墙的设备名称、设备类型及序列号等信息。此处上传授权文件后，在系统状态页面就能看到。

图：上传授权文件

上传文件	选择所要上传的制授权文件

9.1.6 支持

你可以报告防火墙的 BUG 或到天工注册防火墙产品。

图：防火墙支持。

9.1.7 命令检测

命令检测允许你用 PING 等命令来对网络进行简单的检测。

图：命令检测。

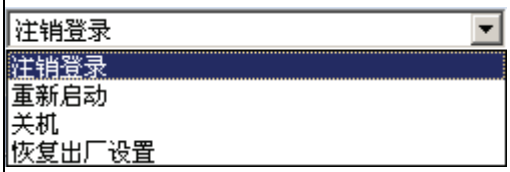
返回的结果如下：

图：Ping 命令返回结果示例。

9.1.8 关机

关机页面包括系统的注销登录，重新启动，关机，恢复出厂设置。

图：关闭系统。

请选择	选择所要的操作：  注销登录：管理员退出当前系统，重新登录。 重新启动：防火墙重新启动。 关机：关闭防火墙。 恢复出厂设置：把防火墙恢复到出厂时的配置。

第10章 设置用户

我们可以定义一系列用户来控制访问特定的资源（包括特定网络和建立 VPN 隧道）。为了使用特定网络（防火墙策略中开启了授权认证选项），访问用户必须首先属于认证用户定义的用户组中，然后输入用户密码认证通过后方可访问对应网络，这部分详见防火墙策略的授权认证部分；对于 VPN 隧道部分，主要被用于 PPTP 和 L2TP 的用户认证部分，只有认证通过用户才可建立 VPN 隧道，这部分详见 PPTP 和 L2TP 部分。

为了方便防火墙策略部分以及 VPN 部分引用，我们将用户定义成对象方式，包括单一的用户和用户组两部分，默认我们指的用户即为单一用户。

用户包括两种：一是本地用户；二是远程用户。本地用户是指在本地指定的用户，包括存放在本地的用户以及本地指定的远程用户两种。本地存放用户是指本地新建的，存放在本地数据库中包括用户密码的帐户；而本地指定的远程用户则是指指定了用户帐户，但该帐户存放在远程服务器中，我们通过需要通过远程认证来验证用户，目前我们支持的为远程 radius 认证。远程用户是指存放在远程服务器上的所有用户，目前我们支持的远程 radius 用户。

用户组是指包含了多个用户的集合。

10.1 用户

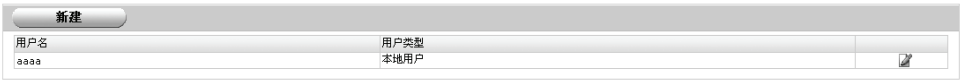


图 本地用户列表查看页面

列项	说明
用户名	用户名称
用户类型	本地用户类型（本地用户/radius用户）
	删除项
	编辑项

表 本地用户列表项

图 新建本地用户页面

配置项	说明
用户名	用户名称
用户类型	选择本地用户类型（本地用户/radius用户）
用户密码	用户类型为本地用户时，本地用户密码
Radius服务器	用户类型为radius用户时，用户所属的radius服务器。

表　新建本地用户配置项

新建本地用户过程：

- 进入设置用户->用户
- 点击新建，进入新建用户页面
- 输入用户名
- 选择用户类型（本地用户/Radius 用户）
- 本地用户类型下，输入用户密码
- Radius 用户类型下，选择 radius 服务器
- 点击“确定”完成

10.2　RADIUS服务器

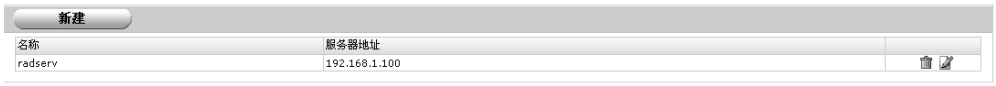


图　radius 服务器列表查看页面

列项	说明
名称	Radius服务器名称
服务器地址	Radius服务器地址
	删除项
	编辑项

表　radius 服务器列表项

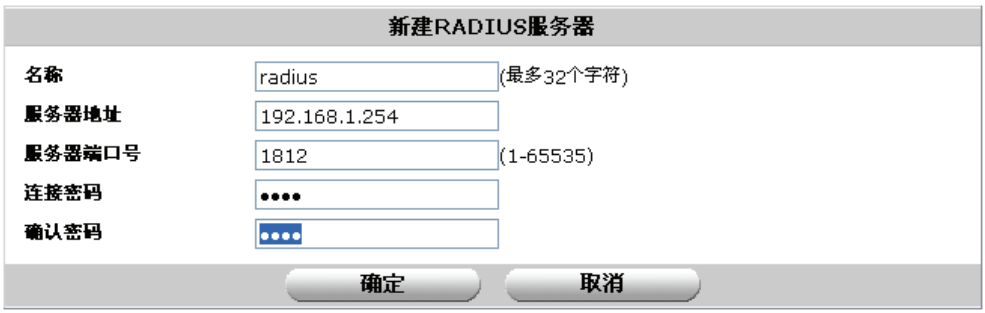


图　新建 radius 服务器页面

配置项	说明
名称	Radius服务器名称
服务器地址	Radius服务器地址
服务器端口号	Radius服务器的连接端口号
连接密码	Radius服务器的连接密码
	删除项
	编辑项

表　新建 radius 服务器配置项

新建 radius 服务器过程：

- 进入设置用户->RADIUS 服务器
- 点击新建按钮，进入新建 Radius 服务器页面
- 输入名称、服务器地址、端口、连接密码
- 点击“确定”完成

10.3　用户组

图　用户组列表查看页面

列项	说明
名称	用户组名称
用户名列表	包含用户名称列表
	删除项
	编辑项

图　新建用户组页面

配置项	说明
组名	用户组名称
可用成员	所有用户
组员	用户组所包含用户
	移入选择用户中
	移出选择用户中

表　新建用户组配置项

新建用户组过程：

- 进入设置用户->用户组
- 点击新建按钮，进入新建用户组页面
- 将需要包含用户移入右边列表中
- 点击“确定”完成

第11章 认证用户

认证用户部分用来设置用于防火墙用户认证的用户组，该用户组在设置用户->用户组部分创建。

认证用户适用于使用了授权认证的防火墙策略，访问用户必须输入该认证用户组，并且认证通过方可访问对应网络。目前我们支持 web 认证方式，用户打开认证页面，输入认证用户、密码认证成功后，方可访问指定网络。

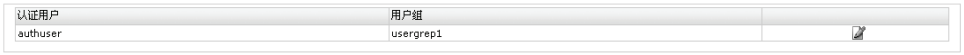


图 认证用户查看页面

列项	说明
认证用户	认证用户名称
用户名	包含用户组列表
	编辑项

表 认证用户列表选项

图 设置认证用户页面

配置项	说明
可选用户组	所有用户组
认证用户成员	认证用户所包含的用户组
	移入选择认证用户中
	移出选择认证用户中

表 设置认证用户选项

设置认证用户过程：

进入认证用户

点击编辑按钮，进入认证用户设置页面

将需要包含用户组移入右边列表中

点击“确定”完成

第12章　路由

路由是用来指定到达目的地址的路径走向。我们可以手动配置静态路由来指定到达目的网络的路径，也可以指定策略路由来指定来自某个网络的数据的走向。

12.1　静态路由

用于手动设置到达目的网络的转发路径。包括指定目的网络地址、出口网络接口和下一跳网关。

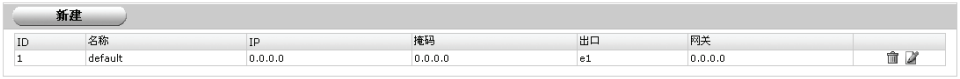


图　静态路由列表查看页面

列项	说明
名称	静态路由名称
IP	目的网络地址
掩码	目的网络掩码
出口	出口网络
网关	下一跳网关地址
	删除项
	编辑项

表 静态路由列表选项

图　新建静态路由配置项

设置项	说明
名称	静态路由名称
目的IP	目的网络地址
目的掩码	目的网络掩码
出口	出口网络
网关	下一跳网关地址

表

表　新建静态路由配置项

新建静态路由配置过程:

- 进入路由->静态路由
- 点击新建按钮，进入新建静态路由页面
- 输入名称
- 输入目的 IP、目的掩码
- 选择出口
- 输入网关地址，网关地址可以为 0.0.0.0。对于不同接口类型，网关地址 0.0.0.0 有不同含义。如果出口为二层透明域或者手动指定地址的接口，表示不指定网关，这是一条接口路由；如果出口为动态获取地址的接口，表示使用动态获取网关。
- 点击“确定”完成

12.2　策略路由

使用策略路由，我们可以基于协议、源接口和源地址来指定数据包的走向。

图　策略路由列表查看页面

列项	说明
名称	策略路由名称
入口	入口网络接口
源地址	源地址
源地址掩码	源地址掩码
目的地址	目的地址
目的地址掩码	目的地址掩码
出口	出口网络接口
	删除项
	编辑项
	插入策略路由
	移动策略路由

表　策略路由列表项

图　新建策略路由页面

设置项	说明
名称	策略路由名称
协议号	协议号(IP:0,tcp:6,udp:17)
入口	数据进入接口
源地址	源地址范围
源地址掩码	源地址掩码

目的地址	目的地址范围
目的地址掩码	目的地址掩码
目的起始端口	目的起始端口
目的结束端口	目的结束端口
出口	数据包出口
网关地址	下一条路由地址

表　新建策略路由配置项

新建策略路由过程：

进入路由->策略路由

点击新建，进入新建策略路由页面

输入名称

输入协议号

选择入口

输入源地址、源地址掩码

输入目的地址、目的地址掩码

输入目的地址起始端口、目的地址结束端口

选择出口

输入网关地址

点击“确定”完成

第13章 防火墙

防火墙策略是防火墙系统中最重要的一个部分，它控制了所有通过防火墙设备的数据流量。当防火墙设备接受到数据报文时，它分析数据报文的源地址、目的地址、来自那个网络接口、去往那个网络接口以及服务等，并根据设定的策略来采用相应的动作。采用的动作包括：允许，丢弃，和重置。

防火墙策略分析数据报文的源地址、目的地址、服务等，采用自上而下查找方式，匹配成功后采取对应策略指定动作。

我们可以在防火墙策略中选择保护设置来进行应用层的防护，包括 HTTP 防护、SMTP 防护、POP3 防护以及 IPS。

我们可以在 NAT 策略部分设置 NAT 策略来进行地址转换，包括 SNAT 转换和虚拟 IP 两部分。

MAC 绑定用来将 IP 与 MAC 地址进行绑定，防止 IP 欺骗。

13.1 策略

策略设置用来对通过防火墙的数据流量进行分析，并根据匹配策略采取相应的动作。

对于到达防火墙的数据包的策略匹配过程，我们采用自上而下一次匹配的原则，匹配成功后，本地匹配结束，不再进行其余的匹配，如果没有查找到匹配策略，默认规则为丢弃。对于策略，我们支持新建、编辑、删除、插入、移动、启用、禁用等操作。

图 防火墙策略列表查看页面

列项	说明
ID	策略标识号
名称	策略名称
源地址	策略的源地址范围
目的地址	策略的目的地址范围
时间表	策略的时间表
服务	策略的服务
动作	策略采取动作
启用	策略的启用状态
	删除项
	编辑项
	插入项
	移动项

表　防火墙策略列表项

图　新建策略页面

设置项	说明
名称	策略名称
源域	选择入口域
源接口	选择入口接口，包括域和该域所属的网络接口，选择域时表示属于该域的所有网络接口。
源地址名	选择源地址名称，该地址在防火墙->地址部分定义，可以为地址或者地址组。
目的域	选择出口域
目的接口	选择出口接口，包括域和该域所属的网络接口，选择域时表示属于

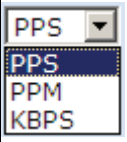
	该域的所有网络接口。
目的地址名	选择目的地址名称，该地址在防火墙->地址部分定义，可以为地址或者地址组。
时间表	选择时间表，该时间表在防火墙->时间表部分定义。
服务	选择服务，该服务在防火墙->服务部分定义，可以为服务和服务组。
动作	策略采取的动作。 
流量日志	选择是否记录网络流量
授权认证	选择是否启用用户认证，即认证通过用户才可匹配该策略。
流量控制	选择是否进行流量控制
基本带宽	流量控制时的保证带宽
最大带宽	流量控制时的最大带宽
优先级	流量控制时选择的优先级，优先级越高越容易获得保证带宽之外的额外带宽以及减小数据报文延迟。
速率控制	选择是否进行速率控制
基本速率	设置基本速率
速率	设置速率。速率单位有： 1．PPS（包/秒） 2．PPM（包/分） 3．KBPS（K字节/秒） 
连接数限制	选择是否启用连接数限制。
TCP最大连接数	设置TCP最大连接数。 当服务选为“ANY”或选TCP类型服务时该文本框可见。
其它最大连接数	设置其它最大连接数。 当服务选为“ANY”或含有UDP类型服务时该文本框可见。
连接掩码	设置连接数控制的网段划分。8表示以8位掩码网络为单位最多拥有最大连接数个连接；16表示以16位掩码网络为单位最多拥有最大连接数个连接；24表示以24位掩码网络为单位最多拥有最大连接数个连接；32表示以32位掩码网络为单位最多拥有最大连接数个连接。
保护设置	选择是否启用保护配置，保护配置在防火墙->保护设置部分定义。

表　新建策略配置项

新建防火墙策略配置过程：

- 进入防火墙->策略
- 点击新建，进入新建防火墙策略页面
- 输入名称
- 选择源域
- 选择源接口
- 选择源地址名，在防火墙->地址部分定义
- 选择目的域
- 选择目的接口
- 选择目的地址
- 选择时间表，在防火墙->时间表部分定义
- 选择服务，在防火墙->服务部分定义
- 选择动作，包括允许/丢弃/重置
- 选择启用流量日志，记录数据流量
- 选择授权认证，开启用户认证部分
- 选择流量控制，设置基本带宽，最大带宽和优先级
- 选择连接数限制，设置连接数限制和连接掩码
- 启用保护设置，选择保护设置选项，保护设置选项在防火墙->保护设置部分定义。

点击“确定”完成

13.2　地址

我们将策略中地址引用部分定义成对象方式，方便策略引用，包括地址和地址组两部分。

13.2.1　地址

地址可以采用掩码方式或者地址范围方式表示。

采用掩码方式格式如下：

x.x.x.x/x.x.x.x，例如 192.168.1.0/255.255.255.0 表示为在地址部分输入 192.168.1.0，在掩码部分输入 255.255.255.0

采用地址范围格式如下：

x.x.x.x-x.x.x.x，例如 192.168.1.1-192.168.1.10 表示在起始地址部分输入 192.168.1.1，在结束地址部分输入 192.168.1.10。

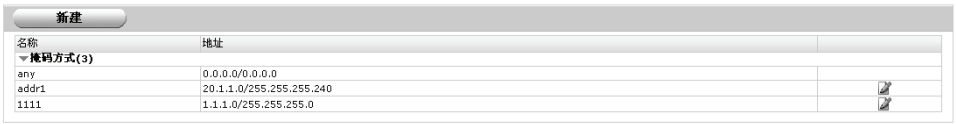


图　地址列表查看页面

列项	说明
名称	网络地址的名称
地址	网络地址
	删除项
	编辑项

表　地址列表选项

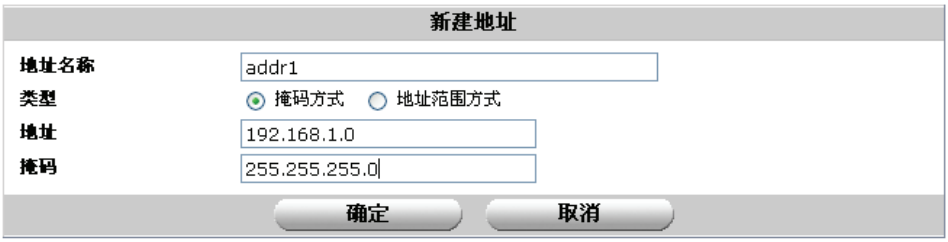


图　新建地址页面

设置项	说明
地址名称	网络地址的名称
类型	网络地址的类型（掩码方式/地址范围方式）
地址	地址类型选择掩码方式时，表示网络地址
掩码	地址类型选择掩码方式时，表示网络掩码
起始地址	地址类型选择地址范围方式时，表示地址范围的起始地址
结束地址	地址类型选择地址范围时，表示地址范围的结束地址。

表　新建地址的配置项

新建地址配置过程：

进入防火墙->地址->地址

点击新建按钮，进入新建地址页面

输入地址名称

选择地址类型(掩码方式/地址范围方式)

对于掩码类型方式，输入地址和掩码

对于地址范围方式，输入起始地址和结束地址

点击“确定”完成

13.2.2 地址组

地址组是指包含多个地址的一个集合。

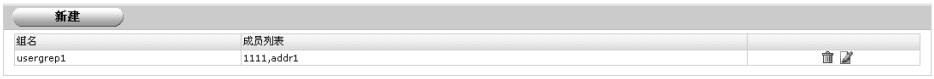


图 地址组列表查看页面

地址组列表项

列项	说明
组名	地址组组名
成员列表	地址组包含地址成员列表
	删除项
	编辑项

图 新建地址组页面

配置项	说明
组名	地址组名称
可用地址	所有地址
成员	地址组包含的地址
	移入地址组成员中
	移出地址组成员中

表 新建地址组配置项

新建地址组配置过程：

- 进入防火墙->地址->地址组
- 点击新建按钮，进入新建地址组页面
- 输入组名
- 将所需地址移入右边列表中
- 点击“确定”完成

13.3 服务

防火墙使用服务来区分通讯类型（如 http,ftp,ping 等），包括单个服务和服务组，以下部分我们把单个服务简称为服务。

服务包括系统预定义的和用户自定义的，包括：协议号、源端口、目的端口。

服务组则是包含若干个服务的集合。

13.3.1 预定义

预定义部分是防火墙系统预先设定的一些常用服务，包括 http，ftp,ping 等。

名称	描述
ANY	all
GRE	ip/47
ESP	ip/50
AH	ip/51
AOL	tcp/5190:5194
BGP	ip/179
DHCP	udp/67:68
DNS	tcp/53 udp/53
FINGER	tcp/79
FTP	tcp/21
GOPHER	tcp/70
HTTP	tcp/80
HTTPS	tcp/443
IKE	udp/500,4500
IMAP	tcp/143
IRC	tcp/6660:6669
L2TP	tcp/1701 udp/1701
LDAP	tcp/389
NETMEETING	tcp/1720
NFS	tcp/111,2049 udp/111,2049
NNTP	tcp/119
NTP	tcp/123 udp/123
FINGER	ip/89
ICMP_ALL	icmp/0
PING	icmp/8

图　系统预定义服务列表查看页面

列项	说明
名称	服务名称
描述	服务描述，如果是tcp,udp协议，显示tcp/dport,udp/dport；如果是icmp，显示icmp/type；如果为其他IP协议，显示为ip/协议号。
	删除项
	编辑项

表　系统预定义服务列表选项

13.3.2　定制

为了更加灵活，我们加入了用户定制部分。定制部分可以允许用户自己定义服务，包括指定协议号、源端口、目的端口。

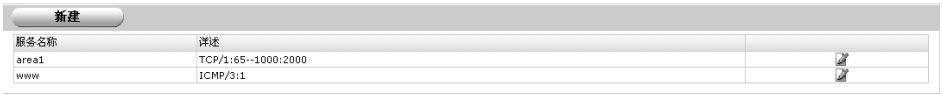


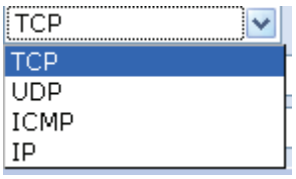
图　定制服务列表查看页面

表　定制服务列表项

列项	说明
服务名称	服务名称
详述	服务描述，如果是tcp,udp协议，显示tcp/sport--dport,udp/sport--dport；如果是icmp，显示icmp/type；如果为其他IP协议，显示为ip/协议号。如果sport,dport为端口范围，表示为startport:endport。
	删除项
	编辑项

表 定制服务列表选项

图　新建自定义服务页面

设置项	说明
名称	自定义服务名称
协议	协议选择 
源端口	当协议选择为tcp或udp时，表示源端口范围

目的端口	当协议选择为tcp或udp时，表示目的端口范围
Icmp类型	当协议选择为icmp时，表示icmp类型
Icmp代码	当协议选择为icmp时，表示icmp代码
协议号	当协议选择为IP时，表示协议号

表　新建自定义服务配置项

新建自定义服务配置过程：

- 进入防火墙->服务->定制
- 点击新建按钮，进入新建定制服务页面
- 输入服务名称
- 选择协议(tcp/udp/icmp/ip)
- 当选择协议为 tcp/udp 时，输入源端口范围和目的端口范围
- 当选择协议为 icmp 时，输入 icmp 类型和 icmp 代码
- 当选择协议为 ip 时，输入协议号(如 50 代表 esp 协议)
- 点击“确定”完成

13.3.3　组

服务组是包含若干个相关服务的集合。

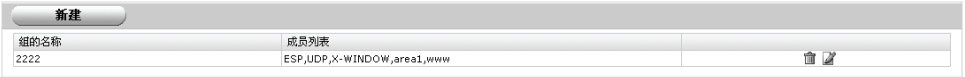


图 服务组列表查看页面

列项	说明
组的名称	服务组名称
成员列表	包含成员显示
	删除项
	编辑项

表　服务组列表选项

图 新建服务组页面

设置项	说明
组的名称	服务组名称
可用服务	可选用的服务列表
成员	该服务组包含的服务列表
	移入服务组成员中
	移出服务组成员中

表 新建服务组配置项

新建服务组配置过程：

- 进入防火墙->服务->组
- 点击新建按钮，进入新建服务组页面
- 将所需服务移入右边成员列表中
- 点击“确定”完成

13.4 时间表

时间表是指按时间启用策略，包括单次时间和循环时间两种，单次时间是指从某个时间开始到某个时间结束，只在这段时间范围内规则才有效；而循环时间用户设置每周固定时间规则生效。

13.4.1 单次时间

单次时间是指设定开始时间和结束时间，限制规则在规定的时间内生效。

图 单次时间列表查看页面

列项	说明

名称	单次时间名称
开始时间	开始时间
停止时间	停止时间
	删除项
	编辑项

表　单次时间列表选项

图 新建单次时间页面

设置项	说明
名称	单次时间名称
开始时间	开始时间，选择年、月、日、时、分
停止时间	停止时间，选择年、月、日、时、分

表　新建单次时间配置项

新建单次时间配置过程：

进入防火墙->时间表->单次时间

点击新建按钮，进入新建单次时间页面

输入单次时间名称

选择开始时间和停止时间

点击“确定”完成

13.4.2　循环时间

循环时间是指设定每周定期生效时间，限制规则在指定时间范围内周期性生效。

图 循环时间列表查看页面

列项	说明
名称	循环时间名称
工作日	生效工作日列表
开始时间	开始时间
停止时间	停止时间
	删除项
	编辑项

表　循环时间列表选项

图　新建循环时间页面

设置项	说明
名称	循环时间名称
工作日选择	选择生效工作日
开始时间	开始时间
停止时间	停止时间

表　新建循环时间配置项

新建循环时间配置过程：

进入防火墙->时间表->循环时间

点击新建按钮，进入新建循环时间页面

输入循环时间名称

选择生效工作日

输入开始时间

输入停止时间

点击“确定”完成

13.5 保护设置

保护设置用于定制应用防护内容，用来对符合规则的流量进行应用层的防护，目前支持(http,smtp,pop3,IPS)。包括病毒检测和内容检测。

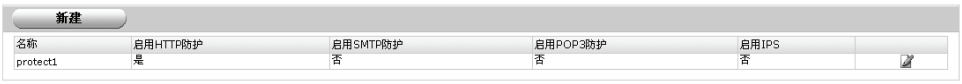


图 保护设置列表查看页面

列项	说明
名称	保护设置名称
启用HTTP防护	是否启用HTTP防护
启用SMTP防护	是否启用SMTP防护
启用POP3防护	是否启用POP3防护
启用IPS	是否启用IPS防护
	删除项
	编辑项

表 保护设置列表选项

图 新建保护设置页面

设置项	说明
名称	保护设置名称
启用HTTP防护	是否启用HTTP防护
启用SMTP防护	是否启用SMTP防护
启用POP3防护	是否启用POP3防护
启用IPS	是否启用IPS防护

表 新建保护设置配置项

新建保护设置配置过程：

- 进入防火墙->保护设置

- 点击新建按钮，进入新建保护设置页面
- 输入名称
- 选择启用 HTTP 防护
- 选择启用 SMTP 防护
- 选择启用 POP3 防护
- 选择启用 IPS
- 点击“确定”完成

13.6 NAT策略

NAT(NETWORK ADDRESS TRANSLATE)，即网络地址转换，包括源地址 N（SNAT）和虚拟 IP（DNAT）两种。

SNAT

SNAT 即源地址转换，一般用户将内部私有地址转换成一个公网地址。

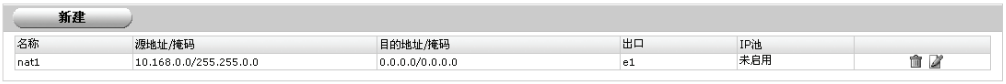


图 SNAT 列表查看页面

列项	说明
名称	SNAT规则名称
源地址/掩码	源地址/掩码
目的地址/掩码	目的地址/掩码
出口	出口接口
IP池	是否启用IP池
	删除项
	编辑项

表 SNAT 列表选项

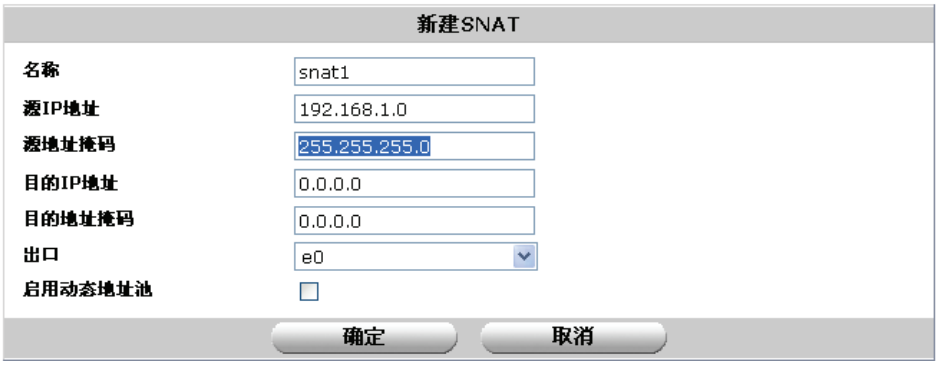


图 新建 SNAT 页面

设置项	说明
名称	SNAT规则名称
源地址/掩码	源地址/掩码
目的地址/掩码	目的地址/掩码
出口	出口接口
启用动态地址池	是否启用IP池
地址池	启用动态地址池后，选择地址池，该地址池在系统管理->网络->IP池部分定义
	删除项
	编辑项

表 新建 SNAT 配置项

新建 SNAT 配置过程：

进入防火墙->NAT 策略->SNAT

点击新建按钮，进入新建 SNAT 页面

输入名称

输入源地址

输入源地址掩码

输入目的地址

输入目的掩码

选择出口

选择启用地址池

选择地址池

点击“确定”完成

注意：如果需要同时配置 IPSec 功能，则必须考虑 IPSec 所保护子网和启用 NAT 的子网的重叠关系。这种情况下，NAT 配置中的地址通常不会选择所有的子网（0.0.0.0/0.0.0.0）。

13.6.1 虚拟IP

虚拟 IP 主要用于将内部服务映射到外部端口供外部访问，包括两种方式：主机映射和端口映射。

图 虚拟 IP 列表查看页面

列项	说明
名称	SNAT规则名称
类型	虚拟IP类型(NAT/PAT)
外部接口	外部接口名称
外部地址	外部地址
外部端口	外部端口
内部地址	内部地址
内部端口	内部端口
协议号	协议号
	删除项
	编辑项

图 新建虚拟 IP（主机映射）页面

设置项	说明
名称	SNAT规则名称
外部接口	外部接口名称
类型	虚拟IP类型(NAT/PAT)
外部地址	外部地址
内部地址	内部地址

表 新建虚拟 IP（主机映射）选项

新建虚拟 IP（主机映射）配置过程：

进入防火墙->NAT 策略->虚拟 IP

点击新建按钮，进入新建虚拟 IP 页面

输入名称

选择外部接口

选择静态 NAT 类型

输入外部 IP 地址

输入内部 IP 地址

点击“确定”完成

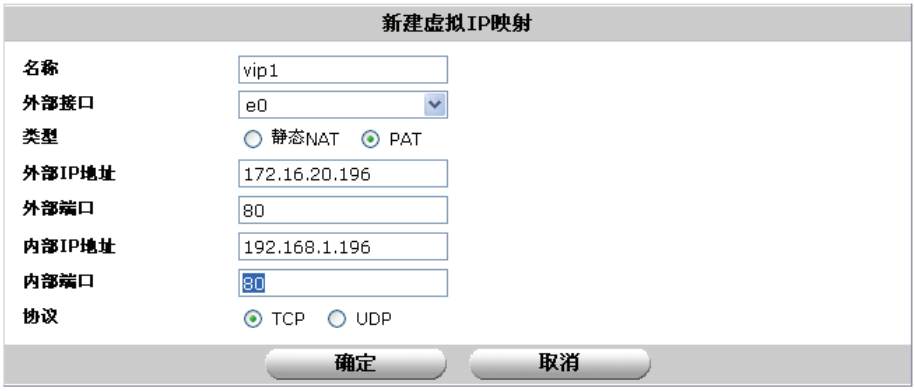


图 新建虚拟 IP（PAT）页面

设置项	说明
名称	SNAT规则名称
外部接口	外部接口名称
类型	虚拟IP类型(NAT/PAT)
外部地址	外部地址
外部端口	外部端口
内部地址	内部地址
内部端口	内部端口
协议	选择协议

表 新建虚拟 IP（PAT）选项

新建虚拟 IP（PAT）配置过程：

进入防火墙->NAT 策略->虚拟 IP

点击新建按钮，进入新建虚拟 IP 页面

输入名称

选择外部接口

选择 PAT 类型

输入外部 IP 地址

输入外部端口

输入内部 IP 地址

输入内部端口

选择协议

点击“确定”完成

13.6.2 NAT策略的生效

在配置 NAT 策略时，对新生成的数据流将立即生效，而对于已经存在的经过防火墙的数据流无法立即生效，所以建议在配置完所有 NAT 策略后，保存配置且重启防火墙。

13.7 MAC绑定

Mac 地址绑定是指将 IP 地址与 MAC 地址进行一对一绑定方式，对于 IP 地址与 MAC 地址不匹配的数据包，我们就可以认为是地址伪装（欺骗），从而可以有效的对用户 IP 进行管理，防止地址欺骗。

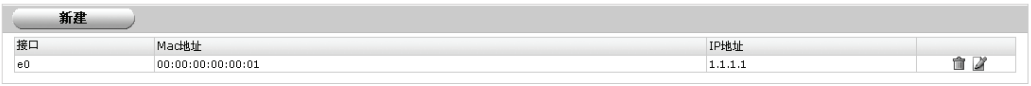


图 IP/MAC 绑定列表查看页面

列项	说明
接口	接口名称
MAC地址	绑定的MAC地址
IP地址	绑定的IP地址
	删除项
	编辑项

表 IP/MAC 绑定列表选项

图 新建 IP/MAC 绑定页面

设置项	说明
接口	接口名称
MAC地址	绑定的MAC地址
IP地址	绑定的IP地址

表 新建 IP/MAC 绑定配置项

新建 IP/MAC 绑定配置过程：

- 进入防火墙->MAC 绑定
- 点击新建按钮，进入新建 IP/MAC 绑定页面
- 选择接口
- 输入 MAC 地址
- 输入 IP 地址
- 点击“确定”完成

第14章　虚拟专网

VPN（虚拟专网）是指在公共网络上建立一条安全通道，保护通讯双方数据的安全传输。天工防火墙支持三种协议方式的 VPN：IPSEC、PPTP、L2TP。

这个章节内容包括 IPSEC、PPTP、L2TP 和证书管理四个部分。

14.1　IPSEC

IPSec VPN 技术在 IP 传输上通过加密隧道，在用公网传送内部专网的内容的同时，保证内部数据的安全性，从而实现企业总部与各分支机构之间的数据、话音、视频业务互通。

14.1.1　阶段 1

阶段 1 过程主要与对端网关或者客户端协商阶段 1 参数（包括模式选择、加密认证算法、认证方式等），生成 ISAKMP SA。

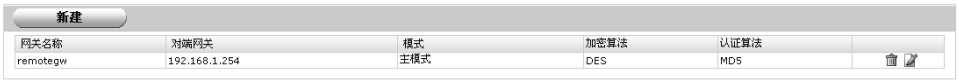


图　阶段 1 查看页面

列项	说明
网关名称	用来标识对端网关的名称
网关IP	对端网关的地址
模式	协商模式（主模式/野蛮模式）
加密算法	阶段1协商的加密算法
认证算法	阶段1协商的认证算法
	删除项
	编辑项

表　阶段 1 列表选项

图　新建 PHASE1 页面

设置项	说明
网关名称	用来标识对端网关的名称
远程网关	 指定远程网关类型(静态地址/动态DNS/移动用户)。
IP地址	对端网关的地址。静态地址方式下为对端网关IP地址；动态DNS方式为对端网关域名；移动用户不用输入。
出口网络接口	指定本地网关接口
模式	协商模式（主模式/野蛮模式）
认证方式	
预共享密钥	密钥内容
证书名称	证书认证方式下，选择用户证书
启用CA认证	证书认证方式下，是否选择CA验证对端网关证书的合法性

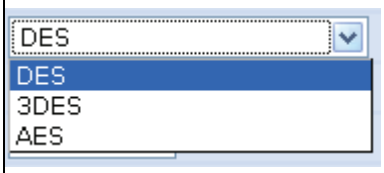
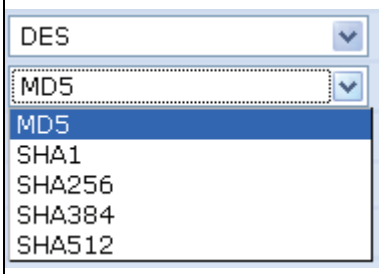
CA证书	CA根证书
DH组	 DH算法组
加密算法	 阶段1协商的加密算法
认证算法	 阶段1协商的认证算法
密钥生存期	阶段1密钥的生存时间
启用NAT穿透	是否启用NAT穿透
保持连接时间	保持存活的有效时间
对端网关检测	是否启用对端网关检测
DPD发送间隔	DPD检测包的发送时间间隔
DPD重试间隔	DPD检测包的重试时间间隔
DPP最大失败次数	DPD检测包的最大失败重试次数

表　阶段 1 设置选项

新建按阶段 1 配置过程：

进入虚拟专网->IPSEC->阶段 1

点击新建按钮，进入新建 VPN 网关页面

输入远程网关名称

选择远程网关类型（静态地址/动态域名/移动用户）

对于静态地址类型网关，输入对端网关 IP 地址

对于动态域名网关，输入对端网关动态域名

对于移动用户，不用输入对端网关

选择出口网络接口

选择 ike 模式（主模式/野蛮模式）

选择认证方式（预共享密钥/证书）

对于预共享密钥方式，输入共享密钥

对于证书方式，选择用户证书，用户证书在虚拟专网->证书->用户证书部分定义。

选择是否启用 CA 认证，启用 CA 认证可以用来验证对端证书的合法性。

如果启用 CA 认证，选择 CA 证书，ca 证书在虚拟专网->证书->CA 证书部分定义。

选择 DH 组

选择加密算法

选择认证算法

选择密钥生存期

选择启用 NAT 穿透

设置保持连接时间

选择启用对端网关检测，输入 dpd 发送检测、dpd 重试间隔和 dpd 最大失败次数

点击“确定”完成

14.1.2 阶段 2

阶段 2 过程主要是协商阶段 2 参数，生成 VPN 隧道。

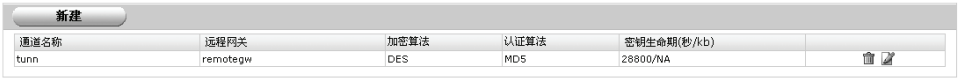


图　阶段 2 列表查看页面

列项	说明
通道名称	用来标识通道名称
远程网关	PHASE1中建立的网关名称
加密算法	阶段2协商的加密算法
认证算法	阶段2协商的认证算法
密钥生命期	IPSEC SA的有效期
	删除项
	编辑项

图　新建阶段 2 页面

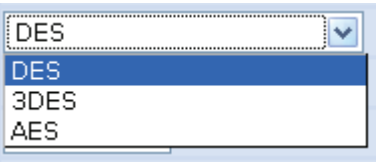
列项	说明
通道名称	用来标识通道名称
远程网关	PHASE1中建立的网关名称
Pfs	启用pfs
DH组	启用pfs下，选择DH交换组
加密算法	 阶段2协商的加密算法
认证算法	 阶段2协商的认证算法
密钥生命期	IPSEC SA的有效期

表　新建阶段 2 设置选项

新建阶段 2 配置过程：

进入虚拟专网->IPSEC->阶段 2

点击新建按钮，进入新建阶段 2 页面

输入通道名称

选择远程网关，在阶段 1 部分定义

选择启用 pfs，选择 dh 组

选择加密算法

选择认证算法

输入密钥生存期

点击“确定”完成

14.1.3　手动模式

手动模式不采用 IKE 密钥交换方式生成加密认证密钥，而是采用手动方式来设定 VPN 隧道的密钥。

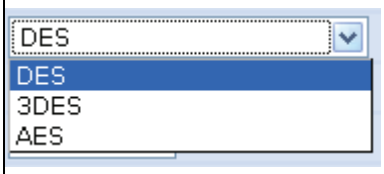
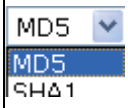
图　手动模式列表查看页面

列项	说明

VPN通道名称	用来标识VPN通道名称
远程网关	指定远程网关地址
加密算法	阶段2协商的加密算法
认证算法	阶段2协商的认证算法
	删除项
	编辑项

表　手动模式列表选项

图　新建手动模式密钥页面

设置项	说明
VPN通道名称	用来标识VPN通道名称
本地SPI	本地SPI
远程SPI	远程SPI
远程网关	指定远程网关地址
出口网络接口	指定本地网关网络接口
加密算法	 指定加密算法
加密密钥	指定加密算法密钥
认证算法	 指定认证算法

认证密钥	指定认证算法密钥

表　新建手动模式配置项

新建手动模式配置过程：

- 进入虚拟专网->IPSEC->手动模式
- 点击新建按钮，进入新建手动模式页面
- 输入 VPN 通道名曾
- 输入本地 spi，用 16 进制表示
- 输入远程 spi，用 16 进制表示
- 选择出口网络接口
- 选择加密算法
- 输入加密密钥
- 选择认证算法
- 输入认证密钥
- 点击“确定”完成

14.1.4　VPN隧道

建立 VPN 安全策略，指定需要 IPSEC 加密的本地网络和对端网络。

图　VPN 隧道列表查看页面

列项	说明
名称	用来标识VPN隧道名称
隧道类型	自动（IKE协商）/手动（手动模式指定密钥）
隧道	阶段2的名称
本地子网地址	本地保护子网网段
本地子网掩码	本地保护子网掩码
远程子网地址	远程保护子网网段
远程子网掩码	远程保护子网掩码
协议	保护数据的通讯协议
启用	隧道的启用状态
	删除项

	编辑项

表　VPN 隧道配置项

图　新建加密隧道页面

设置项	说明
名称	用来标识VPN隧道名称
隧道类型	自动（IKE协商）/手动（手动模式指定密钥）
隧道	如果是自动隧道类型，则从阶段2中选择；如果是手动隧道类型，则从手动模式中选择。
本地子网地址	本地保护子网网段
本地子网掩码	本地保护子网掩码
远程子网地址	远程保护子网网段
远程子网掩码	远程保护子网掩码
协议	保护数据的通讯协议
启用	隧道的启用状态

表　新建加密隧道配置项

新建 VPN 隧道配置过程：

- 进入虚拟专网->IPSEC->VPN 隧道
- 点击新建按钮，进入新建 VPN 隧道页面
- 输入名称
- 选择隧道类型（自动/手动）
- 选择隧道。如果隧道类型为自动方式，则从阶段 2 种选择；如果隧道类型为手动方式，则从手动模式中选择
- 输入本地子网地址
- 输入本地子网掩码

- 输入远程子网地址
- 输入远程子网掩码
- 选择协议
- 选择启用
- 点击“确定”完成

14.1.5 阶段 1 状态

查看当前 IPSEC 阶段 1 的连接状态。

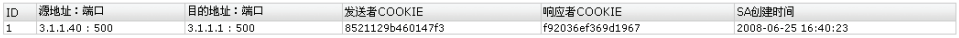


图 IPSEC 阶段 1 状态查看页面

查看项	说明
ID	ID
源地址：端口	SA源地址：端口
目的地址：端口	SA目的地址：端口
发送者COOKIE	发送者COOKIE
响应者COOKIE	响应者COOKIE
SA创建时间	SA创建时间

表 IPSEC 阶段 1 状态查看项

14.1.6 阶段 2 状态

查看当前 IPSEC 阶段 2 的连接状态。

图 IPSEC 阶段 2 状态查看页面

查看项	说明
ID	ID
源网关地址	SA源网关地址
目的网关地址	SA目的网关地址
协议	IPSEC协议名
模式	IPSEC模式
加密算法	加密算法
认证算法	认证算法
SPI（十六进制）	SPI

发送量（Bytes）	发送的数据量
SA创建时间	SA创建时间
剩余时间（秒）	剩余时间（秒）
源地址	受保护的源IP地址
目的地址	受保护的目的IP地址
协议	受保护的协议名

表　IPSEC 阶段 2 状态查看项

14.1.7　IPSec使用中的特殊情况

当配置了防火墙的内外网口都允许 ping 的情况，用户可以从外网口网段 ping 通内网口的接口地址，如果此时再配置了适当的路由和策略，可以 ping 通内网段中的 pc。当此种情况下，配置了保护内网网段的 IPSec，不受保护的外网网段 pc 将无法 ping 通内网网段的 pc，但仍然可以 ping 通防火墙内网口的接口地址。

14.2　PPTP

点对点隧道协议（PPTP）是一种支持多协议虚拟专用网络的网络技术。PPTP 可以用于在 IP 网络上建立 PPP 会话隧道。

14.2.1　PPTP分配地址范围

PPTP 分配地址范围主要用于设置禁用/启用 PPTP 服务，如果启用 PPTP 服务，则设置启用的一些参数，这次参数包括起始 IP、终止 IP、用户组、是否启用加密等。

图 PPTP 设置页面

设置项	说明
启用PPTP/禁用PPTP	启动和禁用PPTP
起始IP	PPTP分配给客户端的起始地址
终止IP	PPTP分配给客户端的终止地址
用户组	PPTP用户认证组，该用户组在设置用户->用户组中定义。

启用加密	是否启用PPTP加密,默认是开启

表　PPTP 配置项

Pptp 配置过程：

- 进入虚拟专网->PPTP
- 选择启用 pptp
- 输入起始 IP
- 输入终止 IP
- 选择用户组，该用户组在设置用户->用户组中定义
- 勾选启用加密
- 点击“应用”完成

14.2.2　PPTP状态

如用户开启 PPTP 服务，则可以查看当前 PPTP 的连接状态。

ID	状态	用户名	客户端PPP地址	接口	客户端地址：端口	接收			发送		
						正确	错误	丢弃	正确	错误	丢弃
0	established	aaaa	172.16.1.1	e0	10.168.40.89 : 44037	103	0	0	9	0	0

图 PPTP 状态查看页面

查看项		说明
ID		PPTP会话ID
状态		PPTP连接的状态，分为： idle 空闲 wait reply 等待应答 established 已连接 stopped 停止
用户名		PPP登录的用户名
客户端PPP地址		客户端PPP接口IP地址
接口		PPTP使用的本地物理接口
客户端地址：端口		客户端连接IP地址：端口
接收	正确	PPP正确的接收包数量
	错误	PPP错误的接收包数量
	丢弃	PPP丢弃的接收包数量
发送	正确	PPP正确的发送包数量
	错误	PPP错误的发送包数量
	丢弃	PPP丢弃的发送包数量

表　PPTP 状态查看项

14.3 L2TP

第二层隧道协议（L2TP）是用来整合多协议拨号服务至现有的因特网服务提供商点。PPP 定义了多协议跨越第二层点对点链接的一个封装机制。L2TP 扩展了 PPP 模型，允许第二层和 PPP 终点处于不同的由包交换网络相互连接的设备来。

天工防火墙支持 L2TP 和 L2TP+IPSEC 模式。

14.3.1 L2TP分配地址范围

L2TP 分配地址范围主要用于设置禁用/启用 L2TP 服务，如果启用 L2TP 服务，则设置启用的一些参数，这次参数包括起始 IP、终止 IP、用户组、是否启用 IPSEC、是否启用加密等。

图 L2TP 设置页面

设置项	说明
启用L2TP/禁用L2TP	启动和禁用L2TP
起始IP	L2TP分配给客户端的起始地址
终止IP	L2TP分配给客户端的终止地址
用户组	L2TP用户认证组，该用户组在设置用户->用户组中定义。
启用IPSEC	L2TP与IPSEC协同工作
IPSEC隧道	IPSEC阶段2的隧道名称
启用加密	启用L2TP加密，默认为开启。

表 L2TP 配置项

L2tp 配置过程：

- 进入虚拟专网->L2TP
- 选择启用 l2tp
- 输入起始 IP

- 输入终止 IP
- 选择用户组，该用户在设置用户->用户组部分定义
- 选择启用 ipsec
- 选择 ipsec 隧道，该隧道在虚拟专网->IPSEC->阶段 2 部分定义
- 勾选启用加密
- 点击“应用”完成

14.3.2 L2TP状态

如用户开启 L2TP 服务，则可以查看当前 L2TP 的连接状态。

隧道ID	会话ID	状态	用户名	主机名	客户端地址：端口	客户端PPP地址	接收			发送		
							正确	错误	丢弃	正确	错误	丢弃
41	20412	established	aaaa	microsof-2fe1b2	10.168.40.121 : 42246	192.168.1.1	61	0	0	10	0	0

图 L2TP 状态查看页面

查看项		说明
隧道ID		隧道ID
会话ID		会话ID
状态		L2TP连接的状态，分为： idle 空闲 wait-connect 等待连接 established 已连接 stopped 停止
用户名		PPP登录的用户名
客户端地址：端口		客户端连接IP地址：端口
客户端PPP地址		客户端PPP接口IP地址
接收	正确	PPP正确的接收包数量
	错误	PPP错误的接收包数量
	丢弃	PPP丢弃的接收包数量
发送	正确	PPP正确的发送包数量
	错误	PPP错误的发送包数量
	丢弃	PPP丢弃的发送包数量

表 L2TP 状态查看项

14.4 证书

证书管理部分提供了用户证书请求生成、用户公钥证书导入和 CA 根证书导入功能。这部分证书用于 IPSEC 选择证书认证方式下 VPN 建立过程中。

14.4.1 本地证书

本地证书用于 IPSEC 阶段 1 时与对端网关进行 IKE 密钥交换，协商 ISAKMP SA。

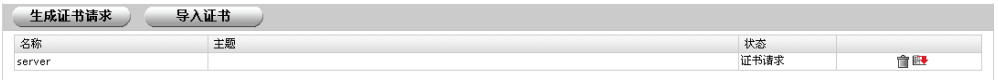


图　本地证书列表查看页面

列项	说明
名称	本地证书名称
主题	本地证书主题内容（注：在证书状态为证书请求时为空）
状态	本地证书状态（证书请求/有效证书对）。 生成证书请求，但没有导入公钥证书时，状态为证书请求；生成证书请求，同时导入合法的公钥证书后，状态为有效证书对。
	查看项，查看证书信息
	删除项
	下载项。当证书状态为证书请求时，下载文件为证书请求文件；当证书状态为有效证书对时，下载文件为公钥证书。

表　本地证书列表选项

图　证书请求生成页面

设置项	说明
证书名称	本地证书名称
国家	国家
省	省名称

城市	城市名称
组织	组织名称
部分	所属部分名称
公共名	公共名称
E-MAIL	邮件地址
密钥大小	密钥长度

表　生成证书请求配置项

新建证书请求过程：

进入虚拟专网->证书->本地证书

点击新建按钮，进入新建证书页面

输入证书名称

选择国家

输入省名称

输入城市名称

输入组织名称

输入公共名

输入 email 地址

选择密钥长度大小

点击“确定”完成

图　导入公钥证书页面

设置项	说明
上传文件	要导入的公钥证书路径

表　本地证书导入设置

证书导入过程：

进入虚拟专网->证书->本地证书

点击状态为证书请求状态项的下载按钮，下载证书请求文件

利用证书请求文件去 CA 中心申请公钥证书

点击导入证书按钮，选择公钥证书

点击“确定”完成上传

14.4.2 CA证书

CA 证书即公共 CA 服务器的根证书，用来验证对端证书的有效性。

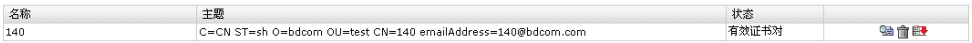


图 CA 证书列表查看页面

列项	说明
名称	CA证书名称
主题	本地证书主题内容（注：在证书状态为证书请求时为空）
	查看项，查看证书信息
	删除项
	下载项。当证书状态为证书请求时，下载文件为证书请求文件；当证书状态为有效证书对时，下载文件为公钥证书。

表 CA 证书列表选项

图 导入 CA 证书页面

设置项	说明
上传文件	要导入的CA根证书路径

表 CA 证书导入设置

CA 证书导入过程：

进入虚拟专网->证书->CA 证书

点击导入证书按钮，选择 CA 证书

点击“确定”完成上传

第15章　入侵防御

IPS（Intrusion Prevension System）与被动的入侵检测系统（IDS）不同，能够检测入侵并采取相应动作。目前我们主要采用入侵特征匹配方式，使用系统自带特征库，最大精度的检测入侵活动。对于入侵活动，我们采取的动作包括：允许通过、丢弃、重置、重置客户端、重置服务端以及记录日志等。

为了启用 IPS，我们需要在防火墙->保护设置中新建保护设置，选择 IPS，然后在防火墙策略中引用该保护设置项。

15.1　特征

精确匹配入侵特征，检测入侵活动。

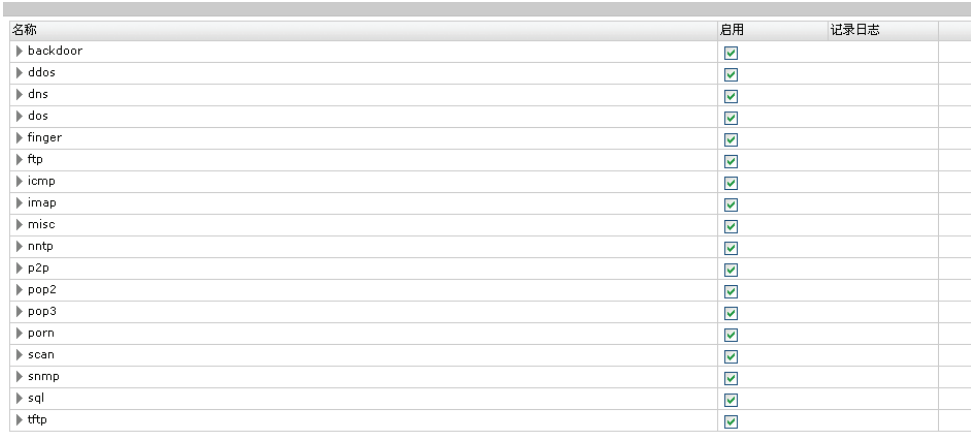


图 入侵特征列表

列项	说明
名称	入侵特征的名称
启用	启用该入侵特征检测。
记录日志	记录入侵活动日志
	编辑项

表　入侵特征列表项

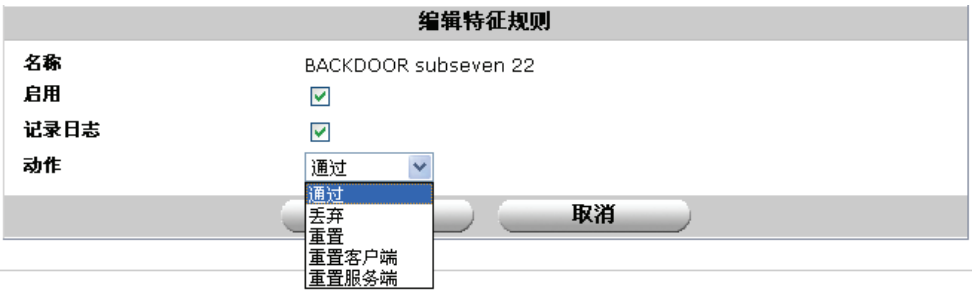


图 编辑入侵特征页面

设置项	说明
名称	入侵特征的名称
启用	启用该入侵特征检测。
记录日志	记录入侵活动日志
动作	采用动作。通过：允许该入侵通过； 丢弃：丢弃入侵数据包；重置：重置入侵连接；重置客户端：重置入侵客户端连接；重置服务端：重置入侵服务端连接。

表 入侵检测特征设置项

设置 IPS 特征处理动作过程：

进入入侵防御->特征

点击要设置的特征的编辑按钮，进入特征编辑页面

选择启用规则

选择记录日志

选择处理动作（通过/丢弃/重置/重置客户端/重置服务端）

点击“确定”完成

第16章 防病毒

我们这里的病毒包括计算机病毒、蠕虫和特洛伊木马。病毒、蠕虫和特洛伊木马是可导致您的计算机和计算机上的信息损坏的恶意程序。它们可能使 Internet 速度变慢，甚至可以使用您的计算机将它们自己传播给您的朋友、家人、同事以及 Web 的其他地方。

我们目前提供基于三种应用的病毒检测和防御：http,smtp,pop3。

16.1 HTTP设置

用于 HTTP 应用的病毒检测设置，可以选择是否启用病毒过滤、采取动作以及记录日志。

图 HTTP 病毒检测部分设置页面

设置项	说明
启用http病毒过滤	是否启用病毒检测
http动作	http病毒检测采取动作
记录日志	是否记录病毒HTTP访问日志

表 HTTP 病毒检测设置表项

防病毒部分设置 HTTP 过程：

- 进入防病毒->HTTP 设置
- 选择启用 http 病毒过滤
- 选择 http 动作（放行/阻塞）
- 选择记录日志
- 点击“确定”完成

16.2 SMTP设置

用于 SMTP 应用的病毒检测设置，可以选择是否启用病毒过滤、采取动作、插入头 FLAG、改写邮件主题以及记录日志。

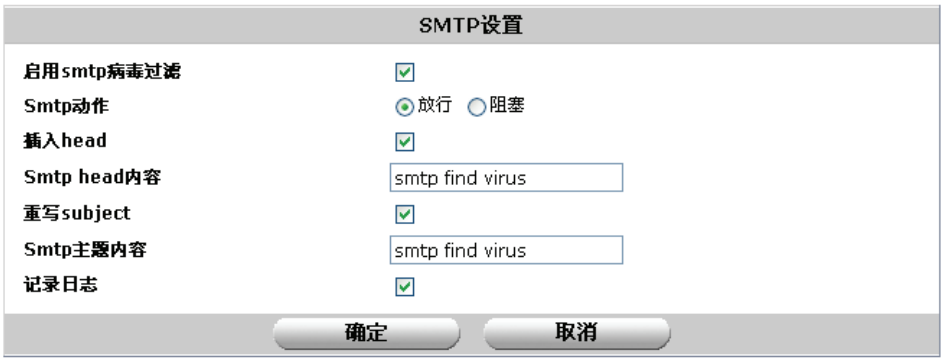


图　SMTP 设置页面

设置项	说明
启用smtp病毒过滤	是否启用病毒检测
Smtp动作	Smtp病毒检测采取动作
插入head	是否在垃圾邮件的头部插入头FLAG
Smtp head内容	插入的头标记内容
重写subject	是否重设垃圾邮件的主题
Smtp主题内容	重置的smtp主题内容
记录日志	是否记录病毒邮件访问日志

表　SMTP 设置选项

防病毒部分 SMTP 设置过程：

- 进入防病毒->SMTP 设置
- 选择启用 smtp 病毒过滤
- 选择 smtp 动作（放行/阻塞）
- 选择插入 head
- 输入 smtp head 内容
- 选择重写 subject
- 输入 smtp 主体内容
- 选择记录日志
- 点击“确定”完成

16.3　POP3设置

用于 POP3 应用的病毒检测设置，可以选择是否启用病毒过滤、采取动作、插入头 FLAG、改写邮件主题以及记录日志。

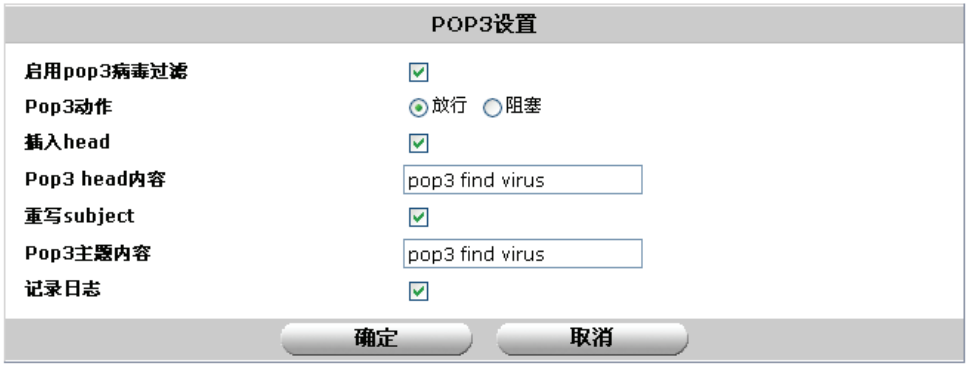


图　POP3 设置页面

设置项	说明
启用pop3病毒过滤	是否启用病毒检测
pop3动作	pop3病毒检测采取动作
插入head	是否在垃圾邮件的头部插入头FLAG
pop3head内容	插入的头标记内容
重写subject	是否重设垃圾邮件的主题
pop3主题内容	重置的pop3主题内容
记录日志	是否记录病毒邮件访问日志

表　POP3 设置选项

防病毒部分 POP3 设置过程：

进入防病毒->POP3 设置

选择启用 pop3 病毒过滤

选择 pop3 动作（放行/阻塞）

选择插入 head

输入 pop3 head 内容

选择重写 subject

输入 pop3 主体内容

选择记录日志

点击“确定”完成

第17章 WEB防护

Web 防护是指能够对不安全、不健康、含有病毒等的网页进行过滤，有效的保证 web 访问的安全性。

为了设置 web 防护，我们需要在防火墙->保护设置中新建保护设置，选择启用 web 防护，然后在防火墙策略中选择启用保护设置并选择它。

Web 防护支持：文件大小过滤、文件扩展名过滤、MIME 类型过滤、站点过滤、URL 过滤、内容过滤和记录日志等，同时还能与防病毒部分结合起来，对网页包含病毒进行检测过滤。

在配置本功能时，请确保内网客户机上配置的 DNS 服务器地址和防火墙配置的 DNS 服务器相同，或者客户机上配置的 DNS 服务器地址为防火墙提供 DNS 转发的地址（即防火墙作 DNS 代理功能）。同时，为了加快处理速度，请选择本地最优的 DNS 服务器地址。

17.1 HTTP设置

http 设置部分用来设置 web 上传的最大文件大小，关键字过滤权值以及日志记录。

图 HTTP 设置页面

设置项	说明
最大上传文件大小	设置网页过滤的最大文件大小
关键字过滤最大权值	设置关键字过滤的阀值，超过该值的就被认为是不安全网页。
记录例外请求	日志记录例外网页
记录拒绝请求	日志记录拒绝网页请求
记录所有访问请求	日志记录所有网页访问
加入头标记	向垃圾邮件头部加入标记

表 HTTP 设置选项

Web 防护部分 http 设置：

- 进入 WEB 防护->HTTP 设置
- 输入最大上传文件大小

- 输入关键字过滤的最大权值
- 选择记录例外请求
- 选择记录拒绝请求
- 选择记录所有访问请求
- 点击“确定”完成

17.2 扩展名

扩展名是指网页中包含的文件的后缀（如”.gif”等），包括例外扩展名和禁止扩展名两种类型。设置例外扩展名可以在病毒扫描部分不检测包含例外扩展名文件的网页，而禁止扩展名则禁止包含该扩展名文件的网页访问。

17.2.1 例外扩展名

图 例外扩展名设置页面

设置项	说明
例外扩展名后缀(如.ade)	选中表示将该类型归入例外扩展名列表中

表 例外扩展名设置选项

17.2.2 禁用扩展名

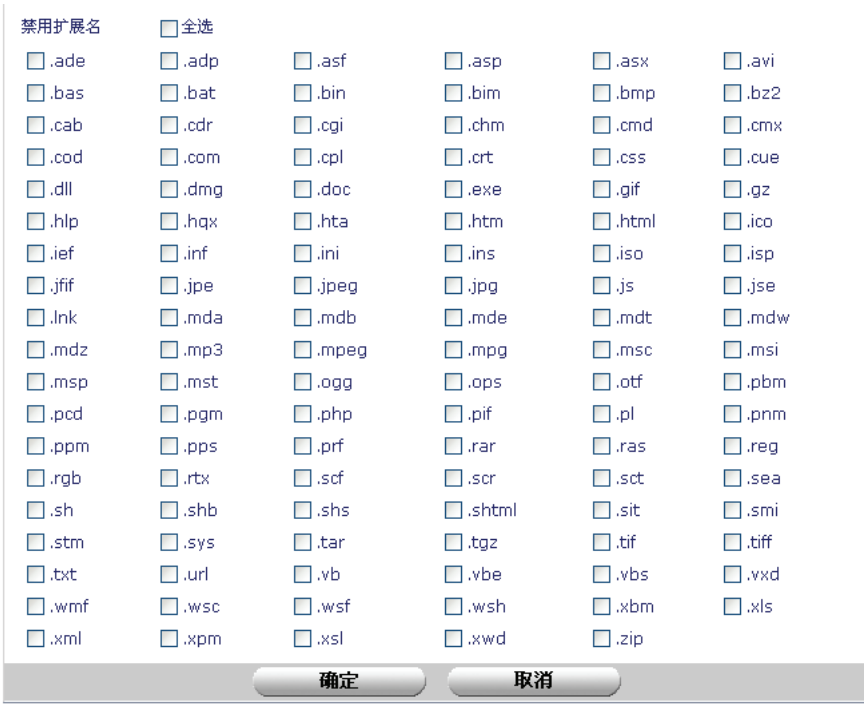


图　禁用扩展名设置页面

设置项	说明
禁用扩展名后缀(如.ade)	选中表示将该类型归入禁用扩展名列表中

表　禁用扩展名设置选项

17.3　MIME类型

多用途互联网邮件扩展(MIME，Multipurpose Internet Mail Extensions)是一个互联网标准，指明了 Web 浏览器或邮件应用程序如何处理从服务器接收的文件。

MIME 类型设置包括例外 MIME 和禁止 MIME 两种类型。设置例外 MIME 可以在病毒扫描部分不检测包含例外 MIME 类型的网页，而禁止 MIME 则禁止包含该 MIME 类型的网页访问。

17.3.1 例外MIME

图 设置例外 MIME 类型页面

设置项	说明
例外MIME类型(如text/plain)	选中表示将该类型归入例外 MIME类型列表中

表 例外 MIME 类型设置选项

17.3.2 禁用MIME

图 设置禁用 MIME 类型页面

设置项	说明
禁用MIME类型(如text/plain)	选中表示将该类型归入禁用 MIME类型列表中

表 禁用 MIME 类型设置选项

17.4 站点过滤

站点过滤是指对整个 web 网站进行过滤，即针对该 web 网站的所有网页。站点过滤又分为例外站点和禁止站点两种。例外站点是指对该站点不进行过滤，而禁止站点则是禁止访问该站点。

例如对 www.sina.com.cn 站点进行过滤，则 www.sina.com.cn 及其 www.sina.com.cn 下所有的 URL 路径均会被过滤（即如 http://www.sina.com.cn，http://www.sina.com.cn/suburls/etc, http://news.sina.com.cn, http://news.sina.com.cn/suburls/etc 这样的网页均会被过滤）

在配置更改之后，如果过滤效果不能马上体现的话可以尝试刷新几次网页。

图 站点过滤查看页面

列项	说明
站点路径	过滤站点路径
站点类型	指明是例外站点还是禁止站点
启用	是否启用该规则
	删除项
	编辑项

表 站点过滤列表选项

图 新建站点过滤页面

设置项	说明
站点路径	过滤站点路径
站点类型	指明是例外站点还是禁止站点
启用	是否启用该规则

表 新建站点过滤选项

新建站点过滤配置过程：

进入 WEB 防护->站点过滤

点击新建按钮，进入新建站点过滤页面

输入站点路径

选择站点类型（例外站点/禁止站点）

选择启用

点击“确定”完成

17.5 URL过滤

URL 过滤是指对该 URL 路径下的网页进行过滤，即针对 web 网站的部分网页。

如对 www.sina.com.cn 进行 url 过滤，则所有 www.sina.com.cn 所有 URL 路径下的页面被过滤（如：http://www.sina.com.cn/suburls/etc，http://news.sina.com.cn/suburls/etc 这样的页面会被过滤。但是 http://news.sina.com.cn 不会被过滤）

在配置更改之后，如果过滤效果不能马上体现的话可以尝试刷新几次网页。

图　URL 过滤查看页面

列项	说明
URL路径	过滤URL路径
URL类型	指明是例外URL还是禁止URL
启用	是否启用该规则
	删除项
	编辑项

表　URL 过滤列表选项

图　新建 URL 过滤页面

列项	说明
URL路径	过滤URL路径
URL类型	指明是例外URL还是禁止URL
启用	是否启用该规则

表　新建 URL 过滤选项

新建 URL 过滤配置过程：

- 进入 WEB 防护->URL 过滤
- 点击新建按钮，进入新建 URL 过滤页面
- 输入 URL 路径
- 选择 URL 类型（例外 URL/禁止 URL）
- 选择启用
- 点击“确定”完成

17.6 关键字过滤

关键字过滤是指对网页正文内容进行过滤，能够有效的过滤不安全，不健康的网页。我们采取加权方式进行过滤，即根据过滤关键字及其权值计算网页的总的权值，如果超过我们设置的最大权值的话，我们则认为该网页为不安全网页

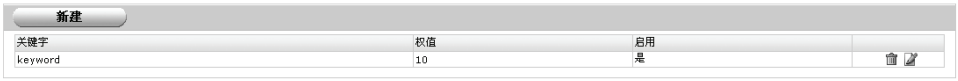


图 关键字列表查看页面

列项	说明
关键字	关键字内容
权值	该关键字对应权值
启用	是否启用该规则
	删除项
	编辑项

表 关键字列表选项

图 新建关键字页面

设置项	说明
关键字	关键字内容

权值	该关键字对应权值
启用	是否启用该规则

表　新建关键字选项

新建关键字配置过程：

进入 WEB 防护->关键字过滤

点击新建按钮，进入新建关键字页面

输入关键字内容

输入权值

选择启用

点击“确定”完成

第18章　垃圾邮件过滤

垃圾邮件是指包含下述属性的电子邮件：

◆ 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；

◆ 收件人无法拒收的电子邮件；

隐藏发件人身份、地址、标题等信息的电子邮件；

含有虚假的信息源、发件人、路由等信息的电子邮件。

目前支持对于 smtp,pop3 协议的垃圾邮件检测能力，过滤功能包括：DCC 过滤、贝叶斯自学习过滤、黑名单/白名单过滤、RBL 过滤以及关键字过滤。系统处理动作分为放行和阻塞两种方式，并且支持向垃圾邮件头部加入 FLAG，向邮件主题加入 TAG，记录日志等操作。同时还能与防病毒部分结合起来，对邮件内容进行病毒检测。

为了设置垃圾邮件防护，我们需要在防火墙->保护设置中新建保护设置，选择启用 smtp 防护或者 pop3 防护，然后在防火墙策略中选择启用保护设置并选择它。

18.1　SMTP设置

Smtp 设置部分用来设置 smtp 协议邮件防护部分选项，包括最大邮件大小的设置、最小剩余空间的设置、最大并发连接数的设置、是否启用垃圾邮件过滤、垃圾邮件处理动作等。

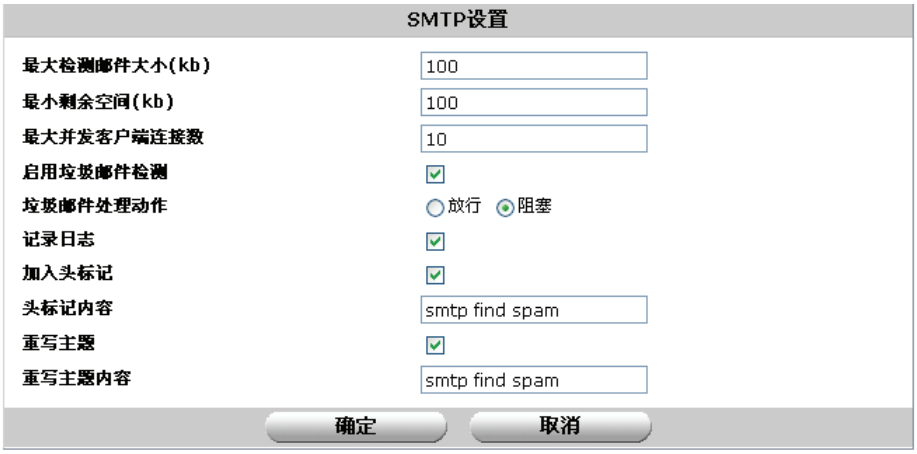


图 smtp 设置部分

设置项	说明
最大邮件大小	设置过滤的最大邮件大小，超过该大小邮件不进行检测。
最小剩余空间	设置最小系统剩余空间，低于该空间时会拒绝邮件扫描。
最大并发客户端连接数	设定最大并行邮件处理数。
启用垃圾邮件检测	开启垃圾邮件检测
记录日志	记录垃圾邮件日志

加入头标记	向垃圾邮件头部加入标记
头标记内容	需要加入的头标记内容
重写主题	修改垃圾邮件的主题部分
重写主题内容	向垃圾邮件主题部分写入的内容

表 smtp 设置表项

SMTP 设置过程：

进入垃圾邮件过滤->SMTP 设置

输入最大邮件大小

输入最小剩余空间

输入最大并发客户端连接数

选择启用垃圾邮件检测

选择记录日志

选择加入头标记

输入头标记内容

选择重写主题

输入重写主题内容

点击“确定”完成

18.2 POP3设置

Pop3 设置部分用来设置 pop3 协议邮件防护部分选项，包括最大邮件大小的设置、最小剩余空间的设置、最大并发连接数的设置、是否启用垃圾邮件过滤、垃圾邮件处理动作等。

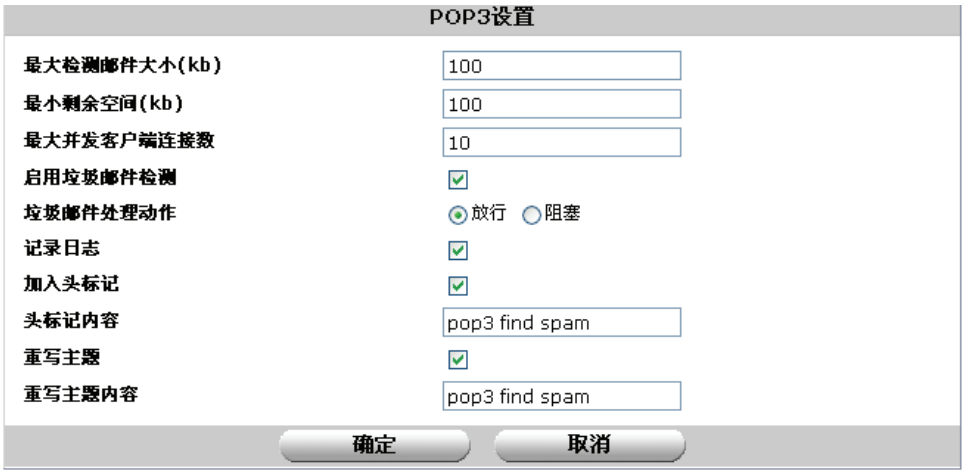


图 pop3 设置部分

设置项	说明

最大邮件大小	设置过滤的最大邮件大小，超过该大小邮件不进行检测。
最小剩余空间	设置最小系统剩余空间，低于该空间时会拒绝邮件扫描。
最大并发客户端连接数	设定最大并行邮件处理数。
启用垃圾邮件检测	开启垃圾邮件检测
记录日志	记录垃圾邮件日志
加入头标记	向垃圾邮件头部加入标记
头标记内容	需要加入的头标记内容
重写主题	修改垃圾邮件的主题部分
重写主题内容	向垃圾邮件主题部分写入的内容

表 pop3 设置表项

POP3 设置过程：

进入垃圾邮件过滤->POP3 设置

输入最大邮件大小

输入最小剩余空间

输入最大并发客户端连接数

选择启用垃圾邮件检测

选择记录日志

选择加入头标记

输入头标记内容

选择重写主题

输入重写主题内容

点击“确定”完成

18.3 垃圾邮件过滤设置

用来设置垃圾邮件过滤引擎系统内置特征过滤部分属性，包括：阀值设置、dcc 设置、贝叶斯设置等。

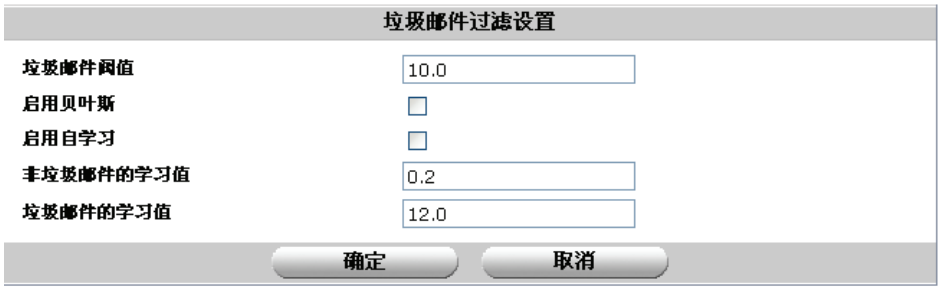


图 垃圾邮件过滤设置页面

设置项	说明
垃圾邮件阀值	设置垃圾邮件过滤阀值(超过该值的邮件被认为是垃圾邮件)，该阀值不宜设置过大。
启用DCC	设置DCC过滤
启用贝叶斯	启用贝叶斯过滤
启用自学习	启用贝叶斯自学习功能
非垃圾邮件的学习值	当邮件权值低于该值时，进行贝叶斯非垃圾邮件特征的学习
垃圾邮件学习值	当邮件权值高于该值时，进行贝叶斯垃圾邮件特征的学习。

表 垃圾邮件过滤设置项

垃圾邮件过滤设置过程：

- 进入垃圾邮件过滤->垃圾邮件过滤设置
- 设置垃圾邮件阀值
- 选择启用 DCC
- 选择启用贝叶斯
- 选择启用自学习
- 设置非垃圾邮件学习值
- 设置垃圾邮件学习值
- 点击“确定”完成

18.4 黑名单

黑名单部分用来设置禁止邮件地址，包括发件人和收件人两种类型。如果发件人地址在发件人黑名单列表中或者收件人地址在收件人黑名单列表中，我们则将该邮件归入垃圾邮件。

图 垃圾邮件黑名单列表查看页面

列项	说明
邮件地址	黑名单地址
类型	黑名单类型（发件人/收件人）
启用	规则启用状态

	删除项
	编辑项

表 垃圾邮件黑名单列表项

图 新建垃圾邮件黑名单页面

设置项	说明
邮件地址	黑名单地址
类型	选择收件人/发件人
启用	规则启用状态

表 新建垃圾邮件黑名单配置项

新建垃圾邮件黑名单过程：

- 进入垃圾邮件过滤->黑名单
- 输入邮件地址
- 选择类型（发件人/收件人）
- 选择启用
- 点击“确定”完成

18.5 白名单

白名单部分用来设置允许邮件地址，包括发件人和收件人两种类型。如果发件人地址在发件人白名单列表中或者收件人地址在收件人白名单列表中，我们则将该邮件归入非垃圾邮件。

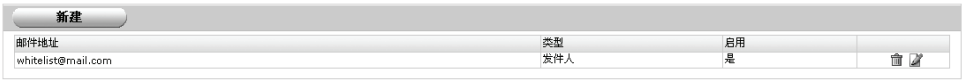


图 垃圾邮件白名单列表查看页面

列项	说明
邮件地址	白名单地址
类型	白名单类型（发件人/收件人）
启用	规则启用状态
	删除项

	编辑项

表 垃圾邮件白名单列表项

图 新建垃圾邮件白名单页面

设置项	说明
邮件地址	白名单地址
类型	选择收件人/发件人
启用	规则启用状态

表 新建垃圾邮件白名单配置项

新建垃圾邮件白名单过程：

进入垃圾邮件过滤->白名单

输入邮件地址

选择类型（发件人/收件人）

选择启用

点击“确定”完成

18.6 RBL列表

RBL（Real-time Blackhole List），是国际反垃圾邮件组织提供的检查垃圾邮件发送者地址的服务。我们到 RBL 服务器查看邮件地址，根据返回结果以及 RBL 类型来判断是否为垃圾邮件。

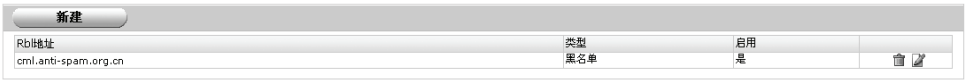


图 垃圾邮件 RBL 查看页面

列项	说明
Rbl地址	RBL地址
类型	CBL类型（黑名单/白名单）。默认黑名单权值为20.00；白名单权值为-20.00
启用	规则启用状态
	删除项

	编辑项

表 垃圾邮件 RBL 列表项

图 新建垃圾邮件 RBL 页面

设置项	说明
RBL地址	RBL地址
类型	选择黑名单/白名单
启用	规则启用状态

表 新建垃圾邮件 RBL 配置项

新建垃圾邮件 RBL 过程：

- 进入垃圾邮件过滤->RBL 列表
- 输入 RBL 地址
- 选择类型（黑名单/白名单）
- 选择启用
- 点击“确定”完成

18.7 关键字

关键字过滤是对邮件正文以及主题进行关键字查找，根据关键字的权值来计算邮件的总权值，最后将总的权值与垃圾邮件阀值比较，判断是否为垃圾邮件。

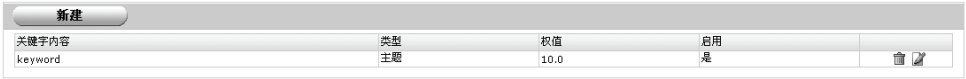


图 垃圾邮件关键字查看页面

列项	说明
关键字内容	关键字字符串
类型	关键字类型（主题/内容）
权值	关键字的权值大小
启用	规则启用状态

	删除项
	编辑项

表 垃圾邮件关键字列表选项

图 新建关键字页面

设置项	说明
关键字内容	关键字字符串
类型	选择主题/内容
权值	关键字权值
启用	规则启用状态

表 新建关键字配置项

新建垃圾邮件关键字配置过程：

进入垃圾邮件过滤->关键字

输入关键字内容

选择类型（主题/内容）

输入权值

选择启用

点击“确定”完成

第19章 日志与报告

概述：

日志是系统重要的审计和统计手段，它能够向用户提供必要的信息，方便我们连接系统的运行状态。天工防火墙日志单元提供了记录和审计事件，用户配置和网络流量的功能。我们可以设置需要记录日志的模块和记录日志的级别来有选择的记录日志。同时我们也可以设置邮件告警部分来定时发送日志到管理员或其他用户邮箱中。

我们将日志分为 3 大类：配置(config)、事件(event)和流量(traffic)。

- 配置日志：主要用于记录用户的配置动作，方便了解用户操作。
- 事件日志：主要用于记录系统各个模块的工作状态和运行信息。
- 流量日志：主要用于记录系统的网络流量，方便管理员了解当前系统的网络状况，如是否出现异常流量等，从而可以采取有效的动作。

我们将每类日志又分为 7 个级别，按照严重级别分别用 0 到 6 来表示，依次为：

级别名称	级别号	级别描述
emerg	0	最高优先级，表明出现系统无法运行的状况
alert	1	必须要立即采取反应动作
crit	2	表示有重要的状况发生
err	3	表示有错误的状况发生
warning	4	表示有警告状况发生
notice	5	一般状况，但也比较重要
info	6	一般信息

下面进行详细的描述，具体包括：

- 日志配置
- 日志访问

19.1 日志配置

我们使用日志配置部分来设置日志记录的位置，级别以及需要记录的模块等。包括：

日志设置

邮件告警

日志过滤

19.1.1 日志设置

我们可以设置日志记录保存的位置，以及需要记录的日志的级别。目前我们支持的日志保存位置有两种：

本地内存：将日志内容记录到本地系统的内存，这种方式下由于本地内存的限制，记录日志的大小有限，一般不长时间记录流量日志等会占用大量空间的日志内容。

远程 syslog 服务器：我们通过标准的 syslog 接口发送日志到远程 syslog 服务器中，这种方式下日志存储仅受 syslog 服务器存放空间的限制，因此可以用来记录大量日志。

日志记录级别如最初描述中所示，可以记录 0 到 6 的各个级别的日志。

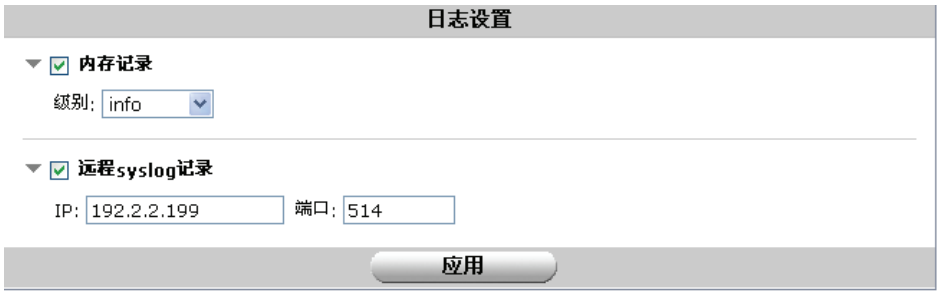


图 日志设置部分

列项	说明
内存记录	将日志记录到本地内存中
级别	记录日志的级别，日志级别采用覆盖方式，即如果选择了info级别，则已经覆盖了前面六种日志级别。关于级别，我们已在前面进行了描述
远程syslog记录	将日志发送到远程syslog服务器中
IP	指定远程日志接收服务器的IP地址
端口	指定远程日志接收服务器的服务开启端口，默认为（514）。

表 日志配置项列表

日志设置过程：

- 进入日志与报告->日志配置->日志设置
- 选择内存记录
- 选择日志级别
- 选择启用远程 syslog 记录
- 输入远程 syslog 服务器 IP
- 输入远程 syslog 服务器端口
- 点击“确定”完成

19.1.2 邮件告警

我们将系统日志通过邮件方式发送给系统管理员或其他用户。

日志与报告->日志配置->邮件告警

图 邮件告警设置部分

列项	说明
SMTP服务器	Smtp服务器地址
邮件来自	邮件的发件人
发送邮件至	邮件的收件人，最多三个
认证	对于有些需要认证的smtp服务器，我们需要开启该项
SMTP用户	Smtp认证的帐号
密码	Smtp认证帐号的密码
告警间隔	告警日志发送的时间间隔

表 邮件告警部分设置选项

邮件告警设置过程：

- 进入日志与报告->日志配置->邮件告警
- 输入 SMTP 服务器地址
- 输入发件人地址
- 输入收件人地址
- 选择认证，启用 smtp 认证
- 输入 smtp 用户、密码
- 设置告警间隔
- 点击“确定”完成

19.1.3 日志过滤

我们可以定制日志记录类型，即有选择记录日志。

日志过滤

名称	内存记录	syslog记录	邮件报警
事件日志	☑	☑	☑
admin	☑	☐	☐
network	☑	☐	☐
system	☑	☐	☐
dhcp	☑	☐	☐
pppoe	☑	☐	☐
ha	☑	☐	☐
time	☑	☐	☐
snmp	☑	☐	☐
maintenance	☑	☐	☐
pptp	☑	☐	☐
l2tp	☑	☐	☐
ipsec	☑	☐	☐
ips	☑	☐	☐
httpguard	☑	☐	☐
smtpguad	☑	☐	☐
pop3guard	☑	☐	☐
userauth	☑	☐	☐
配置日志	☑	☑	☑
network	☑	☐	☐
route	☑	☐	☐
policy	☑	☐	☐
nat	☑	☐	☐
ipsec	☑	☐	☐
流量日志	☑	☑	☑
tfallow	☑	☑	☑
tfdeny	☑	☑	☑

图 事件日志过滤部分

列项	说明
名称	日志类型的名称
内存记录	设置是否记录日志到内存中
Syslog记录	设置是否发送日志到远程syslog服务器中
e-mail告警	设置是否作为邮件告警日志发送

表 日志过滤配置选项

事件日志类型	说明
Admin	系统管理日志(如用户登录等)
Network	记录系统网络信息
System	记录系统信息（如系统运行状况等）
Dhcp	记录dhcp日志
Pppoe	记录pppoe拨号信息

Ha	记录HA
Time	记录时间设置部分(如同步时间服务器)
Snmp	记录snmp事件
Maintenance	记录维护事件
Pptp	记录pptp拨号信息
L2tp	记录l2tp拨号信息
Ipsec	记录ipsec协商信息
Ips	记录IPS
Httpguard	记录http防护信息
Smtpguard	记录smtp邮件防护信息
Pop3guard	记录pop3邮件防护信息
userauth	记录用户认证信息

表 事件日志类型描述

配置日志类型	说明
Route	记录路由配置信息
Policy	记录策略配置信息
Nat	记录nat配置信息
Ipsec	记录ipsec配置信息

表 配置日志类型描述

流量日志类型	说明
Tfallow	记录允许网络流量
Tfdeny	记录禁止网络流量

表 流量日志类型描述

19.2 日志访问

日志访问部分提供了查看和检索内存日志的功能，包括三部分：配置日志、事件日志、流量日志。

19.2.1 配置日志

图 配置日志查看页面

列项	说明
日期	日志产生时的日期
时间	日志产生时的时间
模块	日志产生模块
级别	日志级别
消息	日志内容
模块	可以单击下拉菜单选择一个模块进行查看。 
日志级别	可以单击下拉菜单选择一个日志级别进行查看。 
⏮	首页
◀	上一页
▶	下一页
⏭	最后一页
第3/3页	当前页/总共页数

表 配置日志查看项列表

19.2.2 事件日志

#	日期	时间	模块	级别	消息
1	2008-06-25	16:52:43	ipsec	info	2.2.2.4[500] used for NAT-T
2	2008-06-25	16:52:43	ipsec	info	192.2.2.1[500] used as isakmp port (fd=17)
3	2008-06-25	16:52:43	ipsec	info	192.2.2.1[500] used for NAT-T
4	2008-06-25	16:52:43	ipsec	info	3.1.1.40[500] used as isakmp port (fd=20)
5	2008-06-25	16:52:43	ipsec	info	3.1.1.40[500] used for NAT-T
6	2008-06-25	16:52:43	ipsec	info	127.0.0.1[500] used as isakmp port (fd=21)
7	2008-06-25	16:52:43	ipsec	info	127.0.0.1[500] used for NAT-T
8	2008-06-25	16:52:43	ipsec	info	3.0.6.1[500] used as isakmp port (fd=22)
9	2008-06-25	16:52:43	ipsec	info	3.0.6.1[500] used for NAT-T
10	2008-06-25	17:36:36	admin	info	user admin login success from web(10.168.20.164)

图 事件日志查看页面

列项	说明

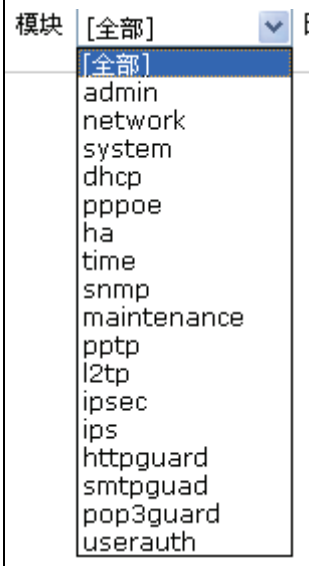
日期	日志产生时的日期
时间	日志产生时的时间
模块	日志产生模块
级别	日志级别
消息	日志内容
模块	可以单击下拉菜单选择一个模块进行查看。 
日志级别	可以单击下拉菜单选择一个日志级别进行查看。 
⏮	首页
◀	上一页
▶	下一页
⏭	最后一页
第10/10页	当前页/总共页数

表 事件日志查看项列表

19.2.3 流量日志

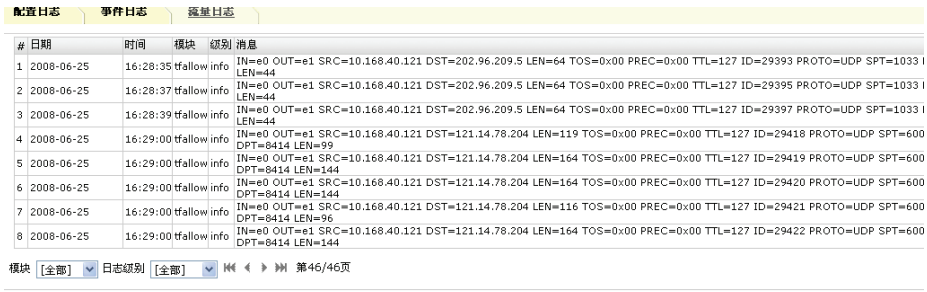


图 流量日志查看页面

列项	说明
日期	日志产生时的日期
时间	日志产生时的时间
模块	日志产生模块
级别	日志级别
消息	日志内容
模块	可以单击下拉菜单选择一个模块进行查看。 
日志级别	可以单击下拉菜单选择一个日志级别进行查看。 
	首页
	上一页
	下一页
	最后一页
第46/46页	当前页/总共页数

表 流量日志查看项列表

第20章　退出系统

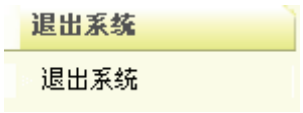


图 退出系统选项

点击退出系统->退出系统，退出当前 web 配置页面，即 web 注销过程。

第21章　案例配置

关于这部分，可以加入几个典型案例的配置。

第22章 注意事项

同时启用 NAT 和 IPSEC 时，NAT 翻译不要配置成对全网段的翻译。

当 IPSEC 一端为移动用户时，不支持预共享密钥方式认证，只支持证书方式。

配置 WEB 防护功能时，请确保内网客户机上配置的 DNS 服务器地址和防火墙配置的 DNS 服务器相同，或者客户机上配置的 DNS 服务器地址为防火墙提供 DNS 转发的地址（即防火墙作 DNS 代理功能）。同时，为了加快处理速度，请选择本地最优的 DNS 服务器地址。

修改防火墙管理口的 IP 地址时，注意同时管理地址、访问权限的对应修改，否则有可能造成再次登陆防火墙时登陆失败。

请注意不要随意关闭防火墙管理口，有可能造成无法登陆防火墙。

需要修改或者删除防火墙的设置时，有些配置由于是关联起来的，修改删除时要按照顺序修改，否则有可能修改或者删除失败。一般被别的配置引用的配置不能修改，要先修改引用的配置，再修改被引用的配置。