
天清异常流量清洗系统 ADM-Guard

Web 管理用户手册



北京启明星辰信息安全技术有限公司

Beijing Venustech Cybervision Co., Ltd

二零一二年五月

版 权 声 明

北京启明星辰信息安全技术有限公司版权所有，并保留对本文档及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其他相关权利均属于北京启明星辰信息安全技术有限公司。未经北京启明星辰信息安全技术有限公司书面同意，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京启明星辰信息安全技术有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京启明星辰信息安全技术有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

信箱：北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦 邮编：100193

电话：010-82779088

传真：010-82779000

您可以访问启明星辰网站：www.venustech.com.cn 获得最新技术和产品信息。

目 录

第 1 章 前言.....	9
1.1 导言.....	9
1.2 本书适用对象.....	9
1.3 本书适合的产品.....	9
1.4 手册章节组织.....	9
1.5 相关参考手册.....	10
第 2 章 如何开始.....	11
2.1 概述.....	11
2.1.1 产品特点.....	11
2.1.2 主要功能.....	11
2.1.3 硬件描述.....	13
2.1.4 软件描述.....	15
2.1.5 附带软件描述.....	16
2.2 拆箱检查.....	16
2.3 安装.....	16
2.3.1 检查安装场所.....	16
2.3.2 安装.....	17
2.3.3 网络连接.....	17
2.4 配置管理方法.....	17
2.4.1 网络接口 WEB 配置.....	17
2.4.2 网络接口 CLI 配置.....	17
2.4.3 本地串口 CLI 配置.....	18
2.5 登录管理界面.....	18
2.5.1 登录方法.....	18
2.5.2 证书认证.....	19
2.5.3 登录过程.....	19
2.5.4 一般配置过程.....	20
2.5.5 退出登录.....	20
第 3 章 系统管理.....	22
3.1 系统信息.....	22
3.1.1 版本信息.....	22
3.1.2 License 信息.....	22
3.1.3 设备名称.....	23
3.1.4 日期时间.....	23
3.2 系统服务.....	25
3.2.1 本地服务.....	25
3.2.2 SSH 服务.....	26
3.2.3 Telnet 服务.....	28
3.2.4 SNMP 配置.....	29
3.2.5 WebUI 超时.....	31
3.3 配置管理.....	31

3.3.1 配置文件管理.....	31
3.3.2 存储设备管理.....	32
3.3.3 当前配置查看.....	33
3.4 维护升级.....	33
3.4.1 系统升级.....	33
3.4.2 License 升级.....	35
3.4.3 特征库升级.....	35
3.5 证书管理.....	36
3.5.1 导入证书.....	36
3.5.2 本地证书.....	37
3.5.3 CA 中心.....	42
3.6 集中管理.....	45
3.7 批处理工具.....	45
第 4 章 网络管理.....	46
4.1 网络接口.....	46
4.1.1 接口 IP 地址.....	46
4.1.2 接口配置.....	51
4.2 ARP.....	56
4.2.1 静态 ARP.....	56
4.2.2 ARP 查看.....	58
4.2.3 免费 ARP.....	58
4.3 路由.....	59
4.3.1 静态路由.....	59
4.3.2 OSPF.....	62
4.3.3 智能路由.....	65
4.3.4 路由表信息.....	71
4.3.5 ISIS.....	71
4.4 DNS 设置.....	73
4.5 DHCP.....	74
4.5.1 服务器配置.....	74
4.5.2 地址池配置.....	75
4.5.3 DHCP 中继.....	78
第 5 章 IPv6.....	80
5.1 网络管理.....	80
5.1.1 地址配置.....	80
5.1.2 邻居配置.....	81
5.1.3 服务段前缀.....	81
5.1.4 自动配置.....	82
5.1.5 静态路由.....	82
5.2 资源定义.....	83
5.2.1 地址.....	83
5.2.2 服务.....	85
5.2.3 时间.....	90

5.2.4 包分类.....	93
5.3 防火墙.....	97
5.3.1 包过滤.....	97
5.3.2 默认过滤策略.....	97
5.4 流量牵引.....	98
5.4.1 BGP 牵引.....	98
5.4.2 OSPF.....	109
5.5 流量分析.....	110
5.5.1 自学习配置.....	110
5.5.2 自学习管理.....	112
5.6 流量清洗.....	113
5.6.1 攻击处理方式.....	113
5.6.2 日志采样.....	114
5.6.3 DNS 防护.....	114
5.6.4 高级型攻击.....	120
5.6.5 自定义特征.....	124
5.7 流量统计.....	126
5.7.1 事件统计.....	126
5.7.2 攻击类型 TOP5.....	126
5.7.3 攻击来源 TOP5.....	127
5.7.4 攻击目的 TOP5.....	127
5.7.5 攻击流量统计.....	128
5.7.6 保护域流量统计.....	128
第 6 章 虚拟网关.....	130
6.1 网关管理.....	130
6.1.1 虚拟网关划分.....	130
6.1.2 接口归属查看.....	132
6.2 全局资源.....	132
6.2.1 地址.....	132
6.2.2 服务.....	137
6.2.3 时间.....	142
6.2.4 应用协议.....	145
6.2.5 包分类.....	146
6.3 全局策略.....	150
6.3.1 包过滤.....	150
6.3.2 DNAT 策略.....	151
6.3.3 SNAT 策略.....	152
6.3.4 长连接.....	154
第 7 章 资源定义.....	156
7.1 地址.....	156
7.1.1 地址列表.....	156
7.1.2 地址池.....	157
7.1.3 地址组.....	158

7.1.4 服务器地址.....	160
7.2 服务.....	161
7.2.1 服务对象定义.....	161
7.2.2 ICMP 服务.....	162
7.2.3 基本服务.....	162
7.2.4 服务组.....	164
7.2.5 ALG 定义.....	165
7.3 时间.....	166
7.3.1 时间列表.....	167
7.3.2 时间组.....	168
7.4 应用协议.....	169
7.4.1 应用协议.....	169
7.4.2 应用协议组.....	170
7.5 包分类.....	170
第 8 章 流量牵引.....	174
8.1 BGP 牵引.....	174
8.1.1 BGP 本地配置.....	174
8.1.2 BGP 邻居配置.....	175
8.1.3 访问控制链表.....	177
8.1.4 路由映射.....	179
8.1.5 路由牵引配置.....	181
8.2 OSPF.....	183
8.2.1 配置路由重分发.....	183
8.2.2 启动、停止 OSPF 功能.....	184
8.2.3 修改路由器 ID.....	184
8.2.4 设置区域.....	184
8.2.5 设置网络.....	184
8.2.6 设置网络接口认证.....	185
第 9 章 流量分析.....	186
9.1 自学习配置.....	186
9.1.1 学习配置.....	186
9.1.2 学习过程.....	188
9.2 自学习管理.....	188
9.2.1 学习结果.....	188
9.2.2 学习曲线.....	189
9.2.3 应用查看.....	190
第 10 章 流量清洗.....	191
10.1 攻击处理方式.....	191
10.2 日志采样.....	191
10.3 攻击证据提取.....	191
10.3.1 攻击证据提取.....	191
10.3.2 捉包分析取证.....	192
10.4 DNS 防护.....	193

10.4.1 域名列表.....	193
10.4.2 域名访问限制.....	195
10.4.3 DNS 攻击保护.....	197
10.4.4 域名长度参数.....	199
10.5 基本型攻击.....	199
10.6 高级型攻击.....	200
10.7 自定义特征.....	206
10.7.1 TCP.....	206
10.7.2 UDP.....	207
10.7.3 ICMP.....	207
10.7.4 自定义特征开启配置.....	208
第 11 章 流量回注.....	209
11.1 接口转发.....	209
11.2 启动 GRE.....	211
11.3 隧道配置.....	211
第 12 章 流量统计.....	213
12.1 事件统计.....	213
12.1.1 开启统计.....	213
12.1.2 事件统计.....	213
12.2 攻击类型 TOP5.....	213
12.3 攻击来源 TOP5.....	214
12.4 攻击目的 TOP5.....	214
12.5 攻击流量统计.....	215
12.5.1 即时流量统计.....	215
12.5.2 异常流量统计.....	215
12.6 保护域流量统计.....	215
12.6.1 牵引流量统计.....	215
12.6.2 清洗流量统计.....	216
第 13 章 防火墙.....	217
13.1 包过滤.....	217
13.1.1 默认过滤策略.....	218
13.2 DNAT 策略.....	218
13.3 SNAT 策略.....	220
13.4 二层协议.....	221
13.5 地址绑定.....	222
13.6 服务器探测.....	229
第 14 章 会话管理.....	232
14.1 会话配置.....	232
14.2 长连接.....	232
14.3 会话日志.....	233
14.4 会话状态.....	233
14.5 同步选项配置.....	234
第 15 章 带宽管理.....	235

15.1 基于管道的带宽管理.....	235
15.1.1 配置中心.....	235
15.1.2 管道管理.....	235
15.1.3 IP 型策略管理.....	236
15.1.4 动作管理.....	237
15.2 基于接口的带宽管理.....	238
15.2.1 物理限速.....	238
15.2.2 QoS 标签.....	240
15.2.3 IPQoS.....	241
15.2.4 流量监管.....	243
15.2.5 流量整形.....	246
15.2.6 拥塞管理.....	249
15.3 流量优化.....	268
15.3.1 带宽借用.....	268
15.3.2 流量建模.....	271
第 16 章 高可用性.....	273
16.1 节点配置.....	274
16.2 工作模式.....	275
16.3 查看状态.....	277
第 17 章 应用安全.....	278
17.1 DNS 应用防火墙.....	278
17.1.1 基本配置.....	278
17.1.2 自定义域名监测.....	279
17.1.3 静态域名表.....	279
17.1.4 域名黑名单.....	280
17.1.5 QPS 信息.....	282
17.1.6 重定向统计.....	282
17.2 缓存感染监测.....	283
17.2.1 缓存感染监测配置.....	283
17.2.2 缓存感染实时监测统计.....	283
17.2.3 缓存感染历史监测统计.....	284
第 18 章 应用识别.....	285
18.1 特征策略.....	285
18.2 策略应用.....	288
18.3 统计图表.....	290
18.4 日志采样.....	290
第 19 章 用户认证.....	291
19.1 本地用户.....	291
19.2 AAA 认证.....	292
19.2.1 认证服务器.....	293
19.2.2 登录用户.....	294
19.2.3 在线 Portal 用户.....	294
19.2.4 Portal 用户组.....	294

19.2.5 Portal 服务器	296
第 20 章 日志信息	298
20.1 日志配置	298
20.1.1 日志服务器	298
20.1.2 终端信息控制	298
20.1.3 信息终端	299
20.1.4 U 盘日志输出	301
20.2 日志查看	301
20.2.1 日志查看	301
20.2.2 管理日志	302
20.2.3 会话日志	302
20.2.4 抗攻击日志	302
20.2.5 流量牵引日志	303
20.2.6 云安全日志	303
20.3 邮件报警	303
20.3.1 邮件报警	304
20.3.2 邮件测试	306
第 21 章 流量可视	308
21.1 统计配置	308
21.2 网络概览	309
21.3 接口统计	309
21.4 应用统计	310
21.5 会话统计	312
21.6 IP 统计	313
21.7 自定义统计	313
第 22 章 系统监控	316
22.1 CPU 监控	316
22.2 内存监控	316
22.3 接口流量统计	317
第 23 章 在线支持	318
23.1 技术支持	318
23.2 关于	318

第1章 前言

1.1 导言

《天清异常流清洗系统 ADM-Guard Web 管理用户手册》是启明星辰天清异常流量管理与抗拒绝服务系统（天清 ADM）管理员手册中的一本。该手册介绍了如何使用 Web 界面对天清异常流量清洗系统 ADM-Guard（以下简称 Guard）进行配置和管理。

1.2 本书适用对象

本手册适用于负责支持、维护 Guard 的安全管理员，是对 Guard 进行配置管理时的必备手册。

使用本手册的读者，应掌握 TCP/IP 协议，IP 地址及子网掩码等基本知识。

1.3 本书适合的产品

本书适合天清异常流量清洗系统 Guard 系列产品。

1.4 手册章节组织

本手册按照以下章节编排：

- 第1章. 前言，描述本书适用的读者，手册章节组织及相关参考手册等。
- 第2章. 如何开始，介绍安装，配置管理Guard的一般方法。
- 第3章. 系统管理，描述与Guard管理相关的配置，包括：系统信息、系统服务、配置管理、维护升级、证书管理、集中处理及批处理工具。
- 第4章. 网络管理，描述与网络环境相关的配置，包括：网络接口、ARP、路由、DNS 设置、DHCP及路由牵引。
- 第5章. IPV6，介绍IPV6环境可用的配置，包括：网络管理、资源定义、防火墙、流量牵引、流量分析、流量清洗、流量统计及保护域流量统计。
- 第6章. 虚拟网关，介绍配置虚拟网关的一般方法，包括：网关管理、全局资源及全局策略。
- 第7章. 资源定义，描述各种资源的定义方法，这些资源定义可以供Guard等功能使用，包括：资源定义通用地址、服务、时间、应用协议及包分类。
- 第8章. 流量牵引，描述牵引流量的方法，包括：BGP牵引及OSPF。
- 第9章. 流量分析，描述流量自学习的配置及应用，包括：自学习配置及自学习管理。

- 第10章. 流量清洗, 描述流量清洗的配置, 包括: 攻击处理方式、日志采样、攻击证据提取、DNS防护、基本型攻击、高级型攻击及自定义特征。
- 第11章. 流量回注, 描述流量回注的配置, 包括: 接口转发、启动GRE及隧道配置。
- 第12章. 流量统计, 描述流量统计的类型, 包括: 事件统计、攻击类型TOP5、攻击来源TOP5、攻击目的TOP5、攻击流量统计及保护域流量统计。
- 第13章. 防火墙, 描述防火墙相关功能的配置方法, 包括: 包过滤、DNAT策略、SNAT策略、二层协议、地址绑定及服务器探测。
- 第14章. 会话管理, 包括: 会话配置、长连接、会话日志、会话状态及同步选项配置。
- 第15章. 带宽管理, 包括: 基于管道的带宽管理、基于接口的带宽管理及流量优化。
- 第16章. 高可用性, 描述高可靠性配置, 包括: 节点配置、工作模式、查看状态。
- 第17章. 应用安全, 包括: DNS应用防火墙及缓存感染监测。
- 第18章. 应用识别, 描述对应用协议识别的相关配置, 包括: 特征策略、策略应用、统计图表及日志采样。
- 第19章. 用户认证, 描述用户管理相关配置, 包括: 本地用户, AAA认证。
- 第20章. 日志配置, 描述信息中心相关配置, 包括: 日志配置、日志查看及邮件报警。
- 第21章. 流量可视, 包括: 统计配置、网络概览、接口统计、应用统计、会话统计、IP统计及自定义统计。
- 第22章. 系统监控, 描述如何监控系统的运行状态, 包括: CPU监控、内存监控、接口流量监控。
- 第23章. 在线支持, 包括: 在线注册、技术支持、关于。

1.5 相关参考手册

《天清异常流量清洗系统 ADM-Guard 命令行操作手册》: 介绍了如何通过命令行管理天清异常流量清洗系统 Guard。

第2章 如何开始

本章包括天清异常流量清洗系统 Guard 硬件安装和随机附带的软件安装介绍,以及开机登录配置管理界面的方法。这些有助于管理员完成 Guard 软硬件的快速安装和启用。

如果您想尽快配置使用 Guard,可跳过概述部分,直接阅读 2.5 章。

2.1 概述

随着宽带网络的飞速发展、网络安全问题的突出和人们安全意识的提高,异常流量管理系统作为一种有效的流量清洗设备已经不可或缺。

天清异常流量清洗系统 Guard 在硬件板级设计、安全体系结构、配置管理操作系统、配套的管理软件等方面有重大创新。可广泛应用于电信、金融、电力、交通、政府等行业的网络环境。

2.1.1 产品特点

天清异常流量清洗系统 Guard 的特点是“三高一热”。

- 高性能
- 高安全
- 高可用
- 热插拔

Guard 采用 64 位多核多线程处理器,支持最多达 64 颗虚拟 CPU (vCPU)。采用 VSP 通用安全平台以及独有的“矩阵式并行算法”和“多核 CPU 动态调度算法”使得产品的最高处理能力最高可达 20Gbps,VPN 处理速度可达 4Gbps,是国内同类抗 DDoS 攻击产品中处理能力最强的产品。

2.1.2 主要功能

天清异常流量清洗系统 Guard 系统为了满足用户的复杂应用和多种需求,采用模块化设计,包括基本功能模块、可选功能模块(如流量优化功能)。主要具有以下功能:

- **状态检测和动态过滤**

采取主动过滤技术,在链路层截取并分析数据包以提高处理性能,对流经数据包进行基于 IP 地址、端口、用户、时间等的动态过滤,还可以结合定义好的策略,动态生成规则,这样既保证了安全,又满足应用服务动态端口变化的要求。可支持多个动态应用,包括 FTP、TNS 等。

- **双向 NAT 地址转换**

在路由模式下提供了双向地址转换(NAT)功能,能够有效地屏蔽整个子网的内部结构,

使得黑客无从发现子网存在的缺陷，还可使企业能够通过共享 IP 地址的方法解决 IP 地址资源不足的问题。支持静态 NAT、动态 NAT 及 IP 映射（支持负载均衡功能）、端口映射。

- **防 IP 地址欺骗**

对指定接口所连接的网络中主机的 IP 和 MAC 地址进行绑定，防止 IP 盗用，并对非法 IP 的访问提供详细的记录，以便 Guard 管理员查看。

- **时间管理**

支持过滤规则的时间域设定，Guard 管理员在定义好一条规则后，能够指定这条规则的启动、生效、关闭的时间域。

- **带宽管理**

提供 QoS 机制，能够用优先级和流量控制方式分配网络带宽，从而有效地保证需要特殊带宽的网络服务。

- **邮件过滤**

对收件和发件的邮件主题、正文、收发件人、附件名、附件内容等进行过滤，对邮件内容除提供关键字匹配外，还提供基于文本格式的中文内容智能过滤。

- **深度过滤**

实时应用层内容过滤，在 Guard 内核协议栈中实现。支持 HTTP、FTP、SMTP 协议，具体包括 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。

- **交互式实时入侵检测（IDS）与实时阻断**

能够识别并防范对网络和主机的扫描攻击、异常网络协议攻击、IP 欺骗攻击、源 IP 攻击、IP 碎片攻击、DoS/DDoS 攻击等；可根据入侵检测结果自动地调整 Guard 的安全策略，及时阻断入侵的网络连接，并可通过邮件的方式向管理员报警；支持用户自定义监测规则，支持规则库的手动升级。

- **支持 SSN（安全服务区）基于网络服务的负载均衡**

实现了高效的负载均衡算法，通过 DNAT 功能，Guard 可以为用户 SSN（安全服务区）内的服务器有效地均衡网络服务的流量，同时提供服务器探测功能。

- **日志审计**

提供 Guard 日志管理和日志服务器，具有实时监控、审计、报警和自动备份功能，同时日志服务器管理员与 Guard 管理员实行分权管理；并可为管理员提供丰富完整的日志信息和强大完善的安全审计，允许管理员设定审计查询规则，以可理解的格式输出查询结果，生成可理解格式的日志文件，具有日志存储溢出报警和补救功能。

- **远程安全管理**

采用基于密码技术的 PKI-CA 证书的认证方式对管理员进行身份认证，只有认证通过的管理员才能访问配置管理界面并操作相关文件。采用 SSL 加密信道对配置信息进行加密处理，保证数据的安全性和完整性（防篡改）。

- **集中安全管理**

通过天清异常流量管理中心 Manager 可以对网络中的 Guard 完成集中统一的配置、管理和系统监视，并具有设备自动发现功能；支持对安全设备运行状态的实时监控；支持实时安

全事件报警和安全事件的日志管理审计。

- **远程维护**

当开启此功能时,允许授权管理员利用 SSH 的方式对 Guard 设备进行在线维护。由于“远程支持”功能采用安全的协议 SSH 进行 Guard 的管理,可保证网络上传送的管理信息被加密,而不被内部或外部用户嗅探或攻击。

- **HA 支持**

支持双机热备和负载均衡两种方式。通过把 Guard 加入集群,在保证某一 Guard 节点一旦发生问题时,其负载可以迅速切换到集群中其它 Guard 上,从而满足无间断网络要求。

- **配置文件类思科格式, 导入导出、备份恢复**

配置采用类似思科的方式,即视图+命令集,简洁明了;可以把配置从设备导出做备份;需要时可以把以前的配置导入恢复到以前的状态,也可以导入到另一台相同型号的设备,从而为 Guard 的管理员工作带来很大的便利

- **模块升级与灾难恢复**

支持 Guard 软件的版本升级,并提供了完善的灾难恢复机制。当 Guard 由于各种原因而出现证书不可用或过期、IP 地址遗失等现象时,管理员只要初始化主机,并将事前保存的系统配置文件导入 Guard,Guard 就能恢复正常的工作状态。

- **支持非 IP 协议**

支持 IPX 和 NetBIOS 等非 IP 协议,还支持自定义协议,控制是否可以通过,具有优秀的网络适应能力。

- **支持 VLAN (802.1Q)协议**

Guard 可以接受、发送带有 VLAN 标记的网络数据。因此,可把 Guard 置于交换机 TRUNK 口,同时支持多个 VLAN 区间通信,包括透明和路由转发。

- **VPN 安全隧道模块**

Guard 集成的 VPN 功能使您可以在 Internet 上构建基于 IPsec/Gre/L2TP 技术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。

2.1.3 硬件描述

2.1.3.1 产品外观

Guard 正面:



图 2-1 天清异常流量清洗系统 Guard

- 机箱
 - Guard 根据型号的不同，有 4U、2U 的机箱，其中 4U 的机箱是针对电信级设计的机箱，每个 4U 机箱有 2 个设备板槽位、1 个机箱风扇，可支持两个直流或交流电源模块
- 设备板，可支持热插拔，每个设备板有三个卡位，从左到右顺序是 Card2/Card0/Card1
 - ✧ Card0 位：支持 FIC 卡（带有面板灯、USB、R232 串口、4 个 GE 电口）
 - ✧ Card1 位：支持 PIC 卡
 - ✧ Card2 位：支持 PIC 卡
- FIC 卡面板灯介绍
 - Guard 异常流量管理系统在 FIC 卡上支持下列面板灯：
 - ✧ PWR：电源指示灯，当电源出现故障时，灯闪烁，电源正常，灯亮；
 - ✧ FAN：风扇指示灯，当风扇有故障时，灯闪烁，正常时，灯亮；
 - ✧ TMP：温度指示灯，当温度在-55~70 摄氏度之间时，亮灯。在 70~85 摄氏度之间时，灯闪烁，表示处于警戒状态。如果环境温度高于 85 摄氏度，则系统会自动断电，风扇继续运转 7~8 分钟后又自动上电。
 - ✧ ACT：故障告警灯，当电源、风扇、单板、插卡、温度等任何一项出现问题的时候，灯闪烁，一切正常时，灯亮；
 - ✧ HA1 与 HA2：用于启用 HA 功能时使用
- FIC 卡 RST 键，用于重启设备板
- FIC 卡 Console 和 Aux
 - FIC 卡面板右侧有两个串口接口，从下到上是 Console 和 Aux，用于连接计算机的串口
- PIC 卡，用于网络通信的网卡开，可供选择的接口
 - ✧ 10 口 10/100/1000M GE 接口
 - ✧ 10 口 10/100/1000M SFP 接口，可插单模或多模 GE 光模块
 - ✧ 1 口 10GE XFP 接口，可插单模或多模 10GE 光模块

2. 1. 3. 2 电气性能

- 电源模块

输入： 线路电压范围： 100 - 240VAC
 额定电压范围： 100 - 240VAC
 电流： 1.8A
 频率： 50/60HZ
 输出： 稳定状态： 20W
 峰值： 96W
 最高热耗散： 72 BTU/ 小时

● 环境参数

温度 : 32o 到 104oF (0o 到 40oC)
 相对湿度 : 5 到 95 %，非冷凝
 高度 : 0 到 984 0 ft (3 000 m)
 冲击 : 1.14 m/sec (45 in./sec) 1/2 正弦输入
 震动 : 0.41 Grms2 (3 到 500 Hz) 随机输入
 噪音 : 最高 60 dBa

2. 1. 3. 3 执行标准

- GB/T 18019-1999 包过滤防火墙安全技术要求
- GB/T 18020-1999 应用级防火墙安全技术要求

2.1.4 软件描述

界面框架如图 2-2 所示



图 2-2Guard 系统界面框架图页

页面分为三个区域：工具栏区，菜单区和显示区。

表 2-1 工具栏中的按钮说明

项目	功能说明
首页	直达首页
导出日志	导出日志
导出配置	导出设备配置
保存	保存当前配置
帮助	在线帮助
退出	退出 WEB 管理页面

菜单采用类似 Windows 操作系统资源管理器的树型结构。

菜单的分类和排列含有逻辑关系，了解这些逻辑关系将有助于管理员记忆并快速定义操作页面。

2.1.5 附带软件描述

附带软件有：

- 日志审计服务器（系统软件）

2.2 开箱检查

在打开包装之后，请您先检查随机附带的电源线、交叉线、光盘、串口线和等设备是否齐全，所有部件请对照装箱单进行检查，如有缺损请及时和销售人员联系。

注意：

取出设备后，不要将外包装丢弃，在需要搬运时，请务必使用原包装，它是为您的异常流量管理系统专门设计的包装，具备良好的防震功能。每当您需要维修服务时也最好用原包装将异常流量管理系统设备返回到北京启明星辰信息技术股份有限公司的维修服务部门。

2.3 安装

2.3.1 检查安装场所

Guard 必须在室内使用，无论您将 Guard 安装在机柜内还是直接放在工作台上，都需要保证以下条件：

1. 确认 Guard 的入风口及通风口处留有空间，以利于 Guard 机箱的散热。
2. 确认机柜和工作台自身有良好的通风散热系统。
3. 确认机柜和工作台足够牢固，能够支撑 Guard 及其安装附件的重量。
4. 确认机柜和工作台的良好接地。

2.3.2 安装

Guard 可以放置在桌面上，也可以放在标准的 19 英寸机架上。安放在桌面上不需要特别的安装，安放在机架上时需要螺丝刀。将 Guard 固定在机架上的固定托架，相关螺钉等随机配备在产品机箱中。

2.3.3 网络连接

1. 请安装 Guard 在机架上或放在一个水平面上。
2. 确认 Guard 电源是关闭的。
3. 连接电源线。
4. 将 Guard 连接在用户当前的网络中。
5. 检查当前 Guard 面板上的指示灯

2.4 配置管理方法

Guard 的配置界面有两种方式：基于 WEB 的图形方式和基于 CLI 的命令行方式，可以利用网络连接（SSH）或串口连接进行命令行配置。

2.4.1 网络接口 WEB 配置

支持远程安全管理和集中安全管理两种方式，优越性更表现在其集中安全管理的特性上。

远程安全管理——支持 SSL 协议，采用基于密码技术的 PKI-CA 证书认证和基于双因子硬件一次性口令认证技术的管理员身份认证，使得只有认证通过的管理员才能通过远程访问配置 WEB 管理界面、操作相关文件，所有 Guard 配置文件及与安全有关的数据都经加密处理存放。

集中式安全管理——管理员通过集中管理中心可以对全局网络中的 Guard 进行统一的配置与管理，支持 SNMP、SSL 协议，利用 SNMP 的 trap 机制实现安全事件报警。具体包括：

1. 拓扑管理：具有设备自动发现功能，使管理员拥有对 Guard 设备信息的全局掌握和控制。
2. 系统监测：监视 Guard 的设备运行状态和统计数据系统状态，并在事件发生时通过图形界面向管理员发出通知。
3. 配置管理：可以对网络中的 Guard 进行统一的安全配置、管理和系统监视。

2.4.2 网络接口 CLI 配置

提供命令行方式的基本配置管理和灾难恢复功能，通过 SSH 方式进行 Guard 的安全管

理和维护，并由管理员根据实际需要决定本功能的是否启用。

2.4.3 本地串口 CLI 配置

基于串口连接，提供命令行方式的基本配置管理和灾难恢复功能，提供了管理的安全、方便与灵活性。

2.5 登录管理界面

2.5.1 登录方法

Guard 共有四种管理方式：1) 加密 WEB 界面管理 2) 非加密 WEB 界面管理 3) 串口命令行管理 4) 远程 SSH 登录管理，其中管理方式 1) 和 3) 是默认开启的，2) 和 4) 默认是关闭的。

在 WEB 界面管理中，管理主机默认只能连接 Guard 的 g0/0/0，如果需要连接其它网口，必须进行相应的设置。默认的管理主机 IP 地址是 10.1.5.200，加密 WEB 界面管理使用 SSL 协议来加密管理数据通信，因此使用 IE 来管理 Guard 时，在地址栏输入 <https://a.b.c.d:8888/>，来以加密的方式登录 Guard。其中 Guard 的地址“a.b.c.d”初始值为“10.1.5.254”，登录 Guard 的初始用户名和口令都是“administrator”，“administrator”中所有的字母都是小写的。非加密 WEB 界面管理方式同加密 WEB 界面管理方式类似，只是在地址栏输入 <http://a.b.c.d/> 来登陆就可以了。

在串口命令行管理中，管理客户端的配置是 38400-8-N-1，管理主机默认连接 Guard 的 CONSOLE。

注意：

1. 用 WEB 界面管理时，建议管理主机设成小字体，分辨率为 1024*768；其他字体和分辨率可能使界面显示不全或顺序混乱。
2. 非加密的 WEB 界面管理方式可能带来安全隐患，推荐用户使用更安全的加密 WEB 界面管理方式。

SSH 登录管理必须首先在菜单“系统管理>>系统服务”中添加 ssh-server 服务，才可以 通过 SSH 协议远程登录 Guard。以 SecureCRT 5.0 版本客户端为例，客户端设置选择协议为 ssh2，端口为 8283，用户为 administrator，默认密码 administrator。此时客户端的 IP 必须是管理主机 IP 之一。

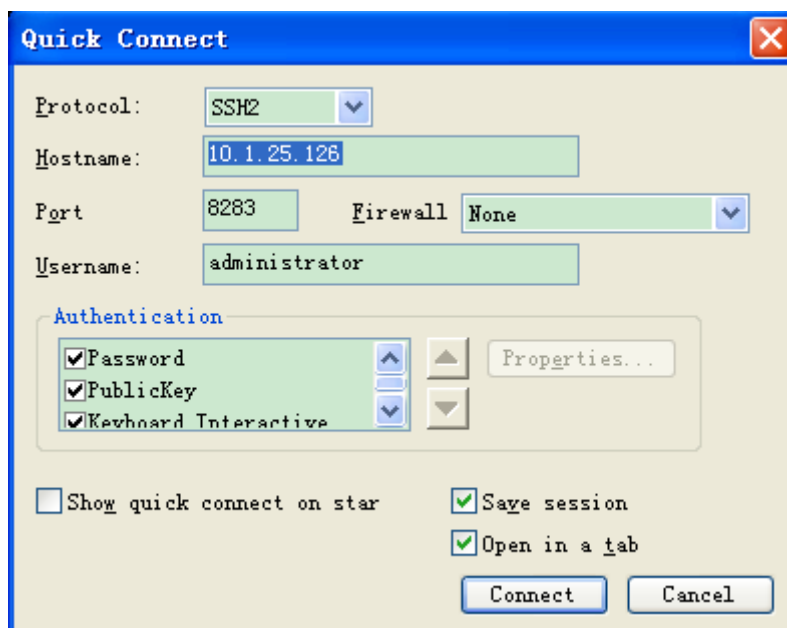


图 2-3 使用 SecureCRT 3.4.3 登录 Guard

2.5.2 证书认证

管理员通过 WEB 方式管理 Guard 还有一种证书认证方式

使用管理证书认证方式，必须在先登录 Guard，开启本地证书认证服务，上载 Guard 证书后，并且在 IE 导入管理员证书后，可通过登录 <https://10.1.5.254:8889/> 登录 Guard 了。开启证书认证后可以关闭本地服务中 https-server 的服务策略，只用具有更高安全特性的证书认证。

2.5.3 登录过程

登录

1. 接通电源，开启 Guard，选用一台带以太网卡和光驱的 PC 机作为 Guard 的管理主机，操作系统应为 Window98/2000/XP，管理主机 IE 浏览器建议为 5.0 以上版本；
2. 使用随机提供的交叉线，连接管理主机和 Guard 的网络接口 g0/0/0；
3. 将管理主机的 IP 地址改为 10.1.5.200（Guard 出厂时默认指定的管理主机 IP）；
4. 使用上一节介绍的认证方法进行认证。
5. 打开 IE 浏览器，浏览 <https://10.1.5.254:8888>，出现如下 Guard 登录界面：



图 2-4 Guard 登录界面

6. 在 Guard 登录界面中输入管理员口令 administrator，进入 Guard 的配置首页。默认的用户帐号和口令都是 administrator。

当您进入天清异常流量清洗系统 Guard 的配置界面后，有关具体参数的说明和配置方法，请参考后续章节。

2.5.4 一般配置过程

以 WEB 界面管理方式为例，配置 Guard 一般遵循以下步骤：

1. 登录管理界面，参考 2.5.1 登录方法和 2.5.3 登录过程
2. 选择“资源定义”菜单项中的子项，定义地址，服务等。
3. 选择“网络管理->网络接口->接口 IP 地址”，增加接口上的 IP 地址。选择“系统服务->本地服务”，添加访问本地服务的安全策略，例如允许 ping 接口。如果网络环境复杂，还需要配置“网络配置->网络接口->”下的 VLAN 设备，桥接设备。
4. 选择“资源定义>>包分类”，添加含有源地址、目的地址等条件的包分类资源策略，在“防火墙>>包过滤”根据需要添加以包分类资源策略为条件的各类安全策略。
5. 系统保存，单击工具栏“保存”字样，保存系统配置。如果没有保存就重新启动，系统将恢复到上一次保存的配置。

在日常的维护中，经常观察设备“系统监控”菜单下的内容和日志服务器中的日志信息，以便了解设备的工作状态。更详细的内容，请参阅设备手册的相关部分。

2.5.5 退出登录

退出 Guard 配置管理界面，虽然可以采用直接关闭浏览器界面的方式，但请尽量采用点

击界面上“退出”，因为这样可以通知 Guard 关闭这个会话，从而最大限度的保证安全性。直接退出还会少记一条管理员退出日志。如果直接关闭浏览器，Guard 没有收到结束会话的指令，则会误以为该管理员仍在线管理中。

第3章 系统管理

本章主要介绍 Guard 的系统管理，由以下部分组成：版本信息、设备名称、日期时间、SNMP 配置、SSH 服务、WEBUI 超时、DNS 设置、邮件报警、证书管理。

3.1 系统信息

3.1.1 版本信息

版本信息用于显示 Guard 主要软件版本信息和相关产品信息。

版本信息	
产品序列号	111b11d131131111
产品型号	Guard-8000
产品平台版本	3.0
BootLoader版本	5.0
产品软件版本	3.6.3.1 Build 25685
产品硬件版本	H2-XLR732F800M-M4G666-P1-AC2
产品硬件逻辑	1.7
版权	Copyright (C) 1996-2011 Beijing Venustech Cybervision Co., Ltd

图 3-1 版本信息

页面内容说明

产品序列号 : 产品唯一标识

产品型号 : 产品型号名称

产品平台版本 : 产品平台系统软件版本号

BootLoader 版本 : BootLoader (用于启动加载产品软件的软件) 的版本

产品软件版本 : Guard 系统的软件版本

版权 : 软件所有权信息

3.1.2 License 信息

License 信息显示硬件的基本信息，如下图所示：

license信息		
定义类型		
网络接口数		14
最大并发连接		2000000
最大IPSEC隧道数		1000
最大L2TP隧道数		1000
最大GRE隧道数		1000
最大安全策略数		10000
最大IPMAC绑定数		10000
加密类型		软硬件加密
最大HA组内设备数		2
最大session支持数 (打开synflood)		2000000
限制类型		
QoS限制内容		y:2028-10-30
DFI限制内容		y:-
全局抗攻击限制内容		y:2028-10-30
流量型抗攻击限制内容		y:2028-10-30
抗常见DOS攻击限制内容		y:2028-10-30
抗常见攻击工具限制内容		y:2028-10-30
IPS限制内容		n:-
IPS升级限制内容		n:-
应用协议识别限制内容		y:2028-10-30
应用协议识别特征更新限制内容		y:2011-10-30
绿色上网特征更新限制内容		y:2011-10-30

图 3-2 license 信息

3.1.3 设备名称

设备名称页面显示了 Guard 的当前名称，用户可以根据需要更改 Guard 的名称。

3.1.4 日期时间

日期时间页面可以对时区、日期时间进行设置，查看系统当前运行时间


时区时间			
时区	夏时制	系统时间	操作
GMT+8:00	✘	2011/07/18 15:18:56	

图 3-3 日期时间

时区

由于 Guard 可能部署世界不同的时区地区，为了与当地时区一致需要调整系统时区，默认设置为北京所在的时区 55，即 GMT+8: 00。

夏时制

即在当地时区标准时间基础上向前调快 1 小时，默认不选择。

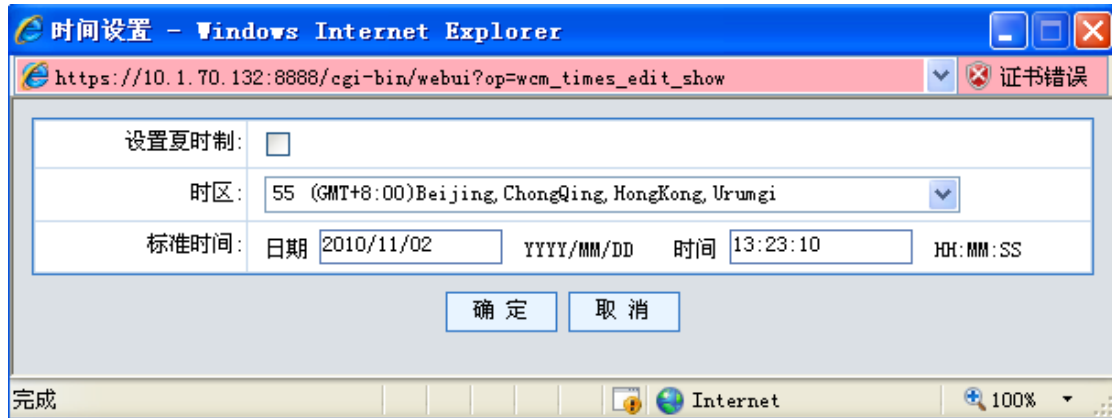


图 3-4 修改系统时区、时钟、设定夏时制

请选择“系统配置->日期时间->时区设置”，点击操作栏“编辑”图标

1. 设置夏时制，在“设置夏时制”后面的选择打勾
2. 点击时区后面的下拉框可以选择需要设置的时区
3. 修改标准时间后面的日期、时间
4. 点击确定完成设置

时间同步

Guard 有两种方法进行时间同步，

- 管理主机进行时间同步
- 采用 NTP 协议与 NTP 时间服务器进行时间同步。

与管理主机时间同步的方法如下：

选择“系统配置->日期时间->时间同步”，点击时间同步按钮，即可完成 Guard 与管理主机的时间同步。

时间同步	
安全网关当前时间:	2011/07/18 15:20:21
管理主机当前时间:	2011/07/18 15:12:08
	<input type="button" value="时间同步"/>

图 3-5 时间同步

采用 NTP 协议与时钟服务器同步的方法见命令行手册。

注意事项：

Guard 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。

运行时间

显示 Guard 从开机时间起一共运行了多少时间。

运行总时间	
系统运行总时间:	00:00:06M:7S (367S)

图 3-6 运行总时间

例如：系统运行总时间：0D:18M:51S(65931S) 表示系统运行了 0 天 18 分 51 秒

3.2 系统服务

3.2.1 本地服务

为了设备自身的安全，默认本机的所有服务全部是关闭的。

提供了一个本地服务的功能，以方便需要的时候可选择的开启某些本机服务。

目前支持的有：

dhcp-server

dhcp-relay

ssh-server

ftp-server

snmp-agent

ping

traceroute

https-server

https-auth-server

ntp

telnet

本地服务显示页面：

序号	规则名	服务	源地址	流入网口	操作
1	snmp	snmp-agent			<input checked="" type="checkbox"/> <input type="checkbox"/>
2	web	https-server			<input checked="" type="checkbox"/> <input type="checkbox"/>
3	ping	ping			<input checked="" type="checkbox"/> <input type="checkbox"/>
4	ssh	ssh-server			<input checked="" type="checkbox"/> <input type="checkbox"/>
5	telnet	telnet-server			<input checked="" type="checkbox"/> <input type="checkbox"/>
6	bgp	bgp-server			<input checked="" type="checkbox"/> <input type="checkbox"/>

第1页/1页 跳转到 页 每页 行

图 3-7 本地服务显示

本地服务添加页面：

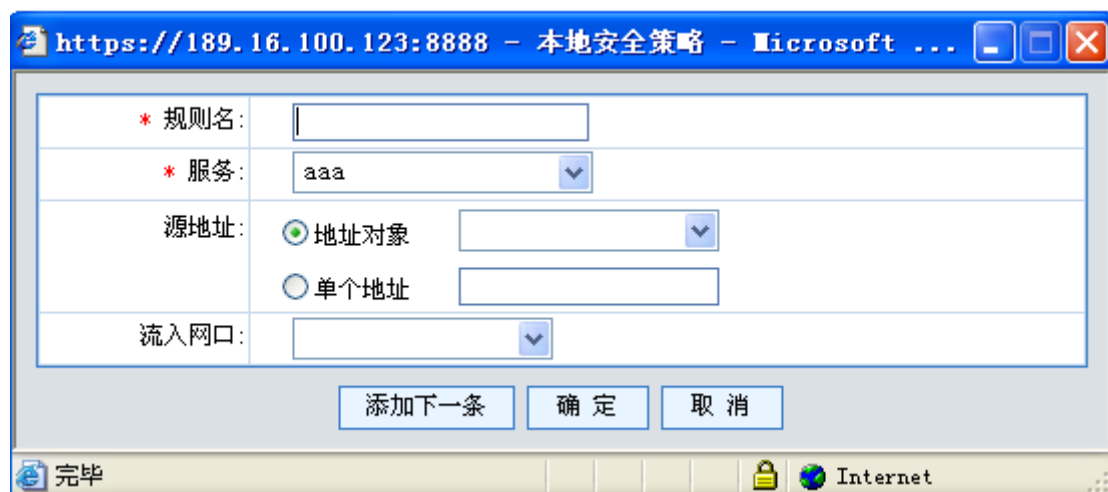


图 3-8 添加本地服务

本地服务修改页面：

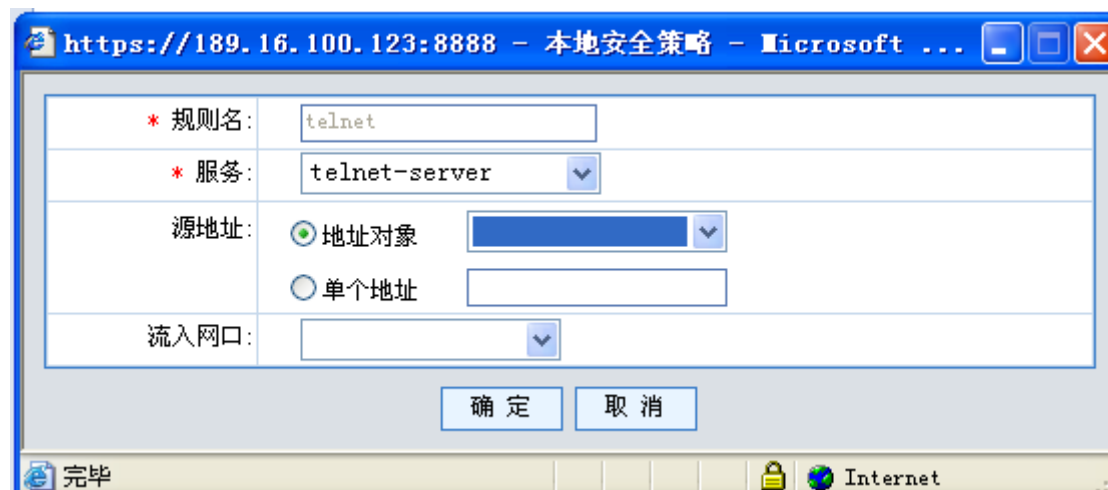


图 3-9 修改本地服务

3.2.2 SSH 服务

Guard 提供 SSH 服务器，用户可通过本地的 ssh 终端软件远程登录到 Guard 上进行系统配置。

ssh server配置

验证方式：	password验证	
密钥更新时间(秒)：	3600	(范围为:3600-86400,缺省为3600秒)
认证超时时间(秒)：	60	(范围为:1-120,缺省为60秒)
验证重试次数：	3	(范围为:1-3,缺省为3次)
兼容ssh1.x版本：	<input checked="" type="checkbox"/>	

ssh user配置

用户名	密钥名	密钥数据	操作
<input type="button" value="添加"/>			

图 3-2 SSH 配置

SSH Server 配置

可以手动修改网关上 SSH 服务器的参数，说明如下表，点击“确定”完成设置。

表 3-1 SSH 服务器的说明列表

域名	说明
验证方法	支持 Password/RSA 验证方法
密钥更新时间	SSH 服务器密钥更新时间
认证超时时间	SSH 协议认证超时时间
验证重试次数	SSH 验证重试次数，超过次数将不再进行验证尝试
兼容 SSH1.x 版本	兼容 SSH 1.x 版本

若验证方法采用 Password 方式，SSH 登录 Guard 的步骤

1. 在“用户管理->本地用户”中添加用户，并配置了 sshServer 服务，详细设置请见相关章节。
2. 在“防火墙->本地服务”中添加允许访问 ssh-server 服务的安全策略，详细设置请见相关章节。
3. 用 ssh 客户端软件（如 SecureCRT），用 SSH2 或 SSH1 协议登录 Guard。

若验证方法采用 RSA 方式，需要进行 SSH 用户配置，针对具体用户设置密钥。

SSH 用户配置

ssh user配置

用户名	密钥名	密钥数据	操作
<input type="button" value="添加"/>			



图 3-3 SSH 用户配置

表 3-2 SSH 用户配置数据域说明

域名	说明
用户名	SSH 用户名称
密钥名	密钥文件名称
密钥数据	密钥中的数据

功能说明：

表 3-3 SSH 用户配置功能说明

域名	说明
	编辑
	删除

添加 ssh 用户

选择系统管理->系统服务->SSH 服务，在 ssh user 配置上，点击“添加”按钮



图 3-4 添加 SSH 用户配置

数据域说明：

表 3-4 添加 SSH 用户配置元素表

域名	说明
用户名	SSH 用户名称
密钥名	密钥文件名称
密钥数据	密钥中的数据

3.2.3 Telnet 服务

telnet 服务如下如所示，在地址列表输入相应的 IP 地址，端口处输入相应的端口号，确定即可。

Telnet配置	
Telnet地址：	<input type="text"/> (请输入本地网络接口的IP地址)
Telnet端口：	<input type="text" value="8286"/> (输入配置端口号只能是：23或8286)
<input type="button" value="确定"/>	

图 3-5 Telnet 配置

3.2.4 SNMP 配置

支持 Guard 的集中管理，Guard 可以与天清异常流量管理中心 ADM-Manager（以下简称 Manager）无缝联动。

管理员首先配置集中管理主机的 IP、SNMP 的团体字串信息，启明星辰集中安全管理系统通过 SNMP 协议从 Guard 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。

SNMP 代理策略可以添加，修改和删除。可以创建最多 4 个 SNMP 代理策略。同时只能启动一个 SNMP 代理，要启动另一个代理策略，必须将已经启动的代理关闭。

SNMP 代理列表页面如下：

SNMP名称	管理主机IP地址	只读权限社区名	读写权限社区名	trap权限社区名	是否启用	是否启用v3	操作
defaultadmin	10.1.5.200 60.0.38.38	readcomm	writecomm	trapcomm	✔	✘	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="button" value="添加"/>							

图 3-6 SNMP 代理列表显示

SNMP 代理添加页面如下：



图 3-7 SNMP 代理添加

表 3-5 集中管理配置元素表

域名	说明
Snmp 名称	策略名称，最大长度为 20 的字符串。
管理主机 IP	管理主机 IP 地址是 SNMP 策略的关键属性，如果需要使一个 SNMP 策略生效，就必须至少配置该属性，管理主机 IP 最多可以配置 5 个不同的地址
只读权限社区名	默认情况下为 public，最大长度为 20 的字符串
读写权限社区名	默认情况下为 private，最大长度为 20 的字符串
启用 V3	启动 SNMP V3 功能
安全级别	设置安全级别，默认为 noauth
认证模式	选择认证模式，默认为 MD5

认证密码	设置认证密码，长度 8 – 16 位
加密模式	选择加密模式，默认为 DES
加密密码	设置加密密码，长度 8 – 16 位
trap 权限社区名	默认情况下为 public，最大长度为 20 的字符串
启用 snmp	同时只能启动一个 SNMP 代理

输入以上各域内容，点“确定”完成集中管理主机配置。

3.2.5 WebUI 超时

为了提高通过 WebUI（Web 用户接口）管理 Guard 的安全性，通过设置管理员登录超时时间，可以允许 WebUI 在管理登录后不做任何操作后的规定时间内自动关闭 web 窗口，防止因为管理员因离开管理主机未关闭管理窗口，而造成设备管理的不安全性。

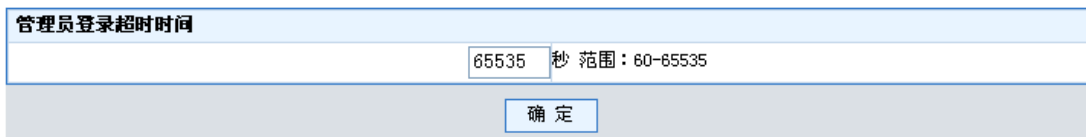


图 3-8 管理员登录超时时间

3.3 配置管理

3.3.1 配置文件管理

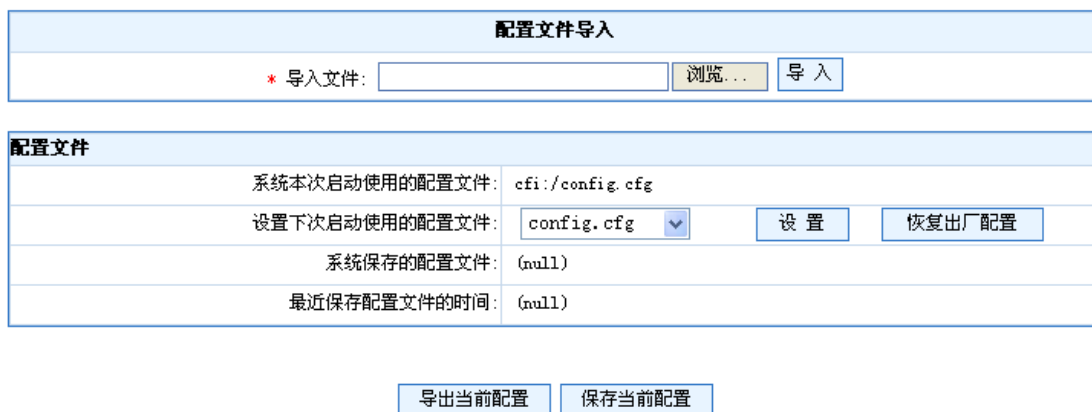


图 3-9 配置文件管理

配置文件管理界面包括以下功能

- 查看系统本次启动使用的配置文件
- 设置系统下次启动使用的配置文件

- 查看系统最近保存的配置文件及保存时间
- 导出当前配置成一个文本文件
- 保存配置到当前使用的配置文件中

3.3.2 存储设备管理

Guard 目前支持的存储设备是 FLASH，可以存储一部分文件，即使设备重启或者断电也能保留。

web方式导入文件

* 导入文件:

ftp方式导入文件

* ftp服务器: * 服务器文件路径:

* 用户名: * 密码:

* 本地文件名: 安全保护:

序号	名称	大小	修改时间	操作		
1	default1.cfg	601 Byte	2011/07/18 14:20:40	<input type="button" value="导出"/>	<input type="button" value="编辑"/>	<input type="button" value="删除"/>
2	default.cfg	601 Byte	2011/07/18 14:20:40	<input type="button" value="导出"/>	<input type="button" value="编辑"/>	<input type="button" value="删除"/>
3	next_cloud_license.txt	35 Byte	2011/07/18 14:20:36	<input type="button" value="导出"/>	<input type="button" value="编辑"/>	<input type="button" value="删除"/>
4	leadsec_cloud_license.txt	35 Byte	2011/07/18 14:20:36	<input type="button" value="导出"/>	<input type="button" value="编辑"/>	<input type="button" value="删除"/>
5	config.cfg	3.9 K	2011/07/13 17:59:14	<input type="button" value="导出"/>	<input type="button" value="编辑"/>	<input type="button" value="删除"/>
6	appcfg.cfg	16 Byte	2010/12/24 14:50:49	<input type="button" value="导出"/>	<input type="button" value="编辑"/>	<input type="button" value="删除"/>
7	temp.cfg	2.7 K	2010/09/25 15:17:29	<input type="button" value="导出"/>	<input type="button" value="编辑"/>	<input type="button" value="删除"/>
8	ipsec.cfg	1.1 K	2010/08/19 11:32:52	<input type="button" value="导出"/>	<input type="button" value="编辑"/>	<input type="button" value="删除"/>

第1页/1页 跳转到 页 每页 行

图 3-10 存储设备管理

存储设备管理包括以下功能

- Web 方式导入文件
- ftp 方式导入文件
- 查看及删除已导入文件

Web 方式导入文件

单击浏览按钮，可以选择主机上要导入的文件；点击导入可以 web 方式导入到设备的 FLASH 中。

FTP 方式导入文件

在“ftp 服务器”一栏中填入 ftp 服务器的地址，在“文件路径”一栏中填入要导入文件在服务器上的完整路径和文件名，如/incoming/test.cfg，然后填入 ftp 服务器的用户名、密码，

在“本地文件名”一栏中填入存储在设备中的文件名，如 local.cfg。

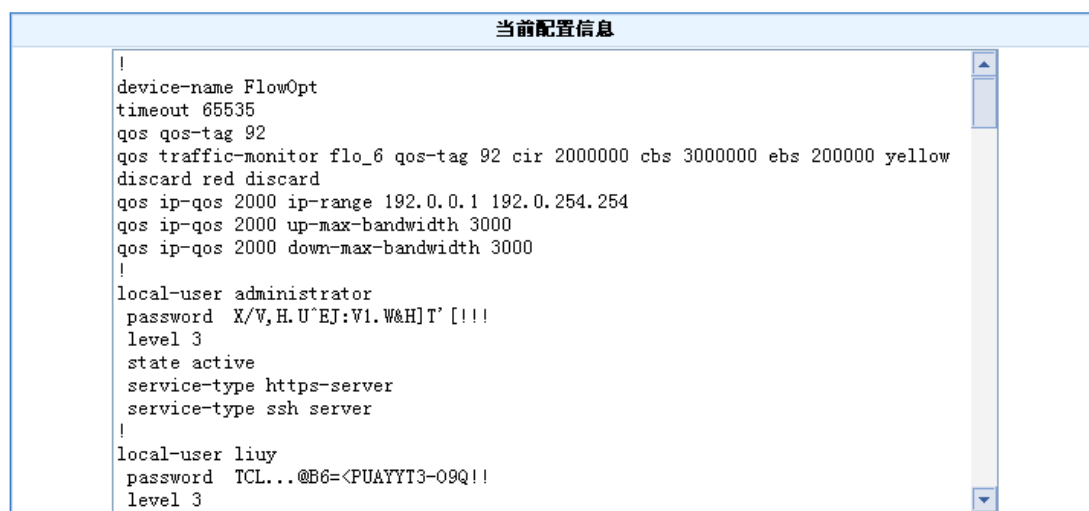
如果导入文件要覆盖设备上已导入文件，且希望文件通过 ftp 方式下载完成前不覆盖原来的文件，可以勾选“安全保护”选项。

- 查看及删除已导入文件

已经导入设备的文件可以在页面的下方查看和删除。

3.3.3 当前配置查看

通过查看当前配置查看列表，看一看当前设备的配置。



```
当前配置信息
!
device-name FlowOpt
timeout 65535
qos qos-tag 92
qos traffic-monitor flo_6 qos-tag 92 cir 2000000 cbs 3000000 ebs 200000 yellow
discard red discard
qos ip-qos 2000 ip-range 192.0.0.1 192.0.254.254
qos ip-qos 2000 up-max-bandwidth 3000
qos ip-qos 2000 down-max-bandwidth 3000
!
local-user administrator
password X/V,H.U`EJ:Vl.W&H]T' [!!!
level 3
state active
service-type https-server
service-type ssh server
!
local-user liuy
password TCL...@B6=<PUAYT3-09Q!!
level 3
```

图 3-11 当前配置查看

3.4 维护升级

3.4.1 系统升级

系统升级功能可以快速响应安全需求，保证网关功能与安全的快速升级。

系统当前软件版本: 1.1.5.0

* 导入文件:

* 备注:

ftp升级

* ftp服务器: 端口:

* 文件名: * 用户名:

* 密码: * 备注:

安全保护:

升级历史记录

序号	升级以后版本号	升级方式	升级时间	更新描述
1	PV1.1.5.0, BUILD25050	ftp升级	2011/7/28 13:20:0	a
2	PV3.1.2.100, BUILD24902	ftp升级	2011/7/27 15:6:56	admin

图 3-12 导入升级文件

系统升级界面包括以下功能

- WEB 升级
- FTP 升级
- 查看升级历史
- 重启 Guard

WEB 升级

1. 点击“浏览”按钮，选择管理主机上的升级包
2. 点击“导入”按钮
3. 填写升级备注
4. 点击“重启 Guard”按钮，重启 Guard 完成升级

FTP 升级

1. 填写 ftp 服务器的 IP 地址，如/incoming/test.cfg，然后填入 ftp 服务器的用户名、密码，在“本地文件名”一栏中填入存储在设备中的文件名，如 local.cfg。点击“导入”按钮
2. 填写 ftp 服务器的端口地址
3. 填写要升级包在服务器上的完整路径和文件名
4. 填入 ftp 服务器的用户名、密码
5. 填写升级备注

点击“重启 Guard”按钮，重启 Guard 完成升级

重启 Guard

点击“重启 Guard”按钮，Guard 将重新启动。

注意：

重启 Guard 前，记住要保存当前配置。

3.4.2 License 升级

License 升级可以采用 web 方式和 ftp 方式升级。

web 方式

点击“浏览”，找到升级的 license 文件，添加备注，点击“确定”。

ftp 方式

需要填写：ftp 服务器地址、文件名（含文件路径）、用户名、密码和备注，然后点击“确定”。

web方式license升级

* 导入license文件:

* 备注:

ftp方式license升级

* ftp服务器: * 文件名:

* 用户名: * 密码:

* 备注:

升级历史记录					
序号	升级时间	升级方式	升级用户	升级结果	更新描述
1	2011/4/27 17:30:51	web升级	administrator	成功	aq
2	2011/4/27 17:28:38	web升级	administrator	失败	a
3	2011/4/27 17:27:52	web升级	administrator	失败	de
4	2011/4/27 17:26:38	web升级	administrator	失败	dd

第1页/1页 跳转到 页 每页 行

图 3-13 导入升级文件

3.4.3 特征库升级

导入新的应用特征库，可以做到设备在线实时升级，更新应用软件的特征。

自动升级

启动:	<input type="checkbox"/> 入侵防护 <input checked="" type="checkbox"/> 绿色上网 <input checked="" type="checkbox"/> 应用识别 <input checked="" type="checkbox"/> 挂马网站 特征库版本信息
升级服务器配置:	<input checked="" type="radio"/> 默认 <input type="radio"/> 自定义
定时升级:	<input type="radio"/> 每天 <input type="radio"/> 每周 日 <input checked="" type="radio"/> 每隔 7 天 (范围为:1-360)
具体时间:	<input style="width: 80px;" type="text" value="00:00:00"/> (有效时间格式 hh:mm:ss)

手动升级

* 导入特征库文件:

序号	成功升级的时间	升级模块	升级后版本号	升级后特征总数	原版本号	原特征总数
<input type="button" value="导出升级历史"/>		<input type="button" value="清空历史记录"/>				

第1页/1页 跳转到 页 每页 行

图 3-14 应用特征库升级

点击“浏览”选择本地的特征库文件，然后选择“导入”，再点击“升级”即可完成特征库的升级。

3.5 证书管理

3.5.1 导入证书

证书管理/导入证书进入如下界面：

证书域	类型	证书名称	密钥名称	根证书名称	操作
<input type="button" value="添加"/>					

第1页/1页 跳转到 页 每页 行

图 3-15 本地证书导入

点击上图的“添加”按钮进入如下界面:分别选择客户端或者服务器端进行导入。

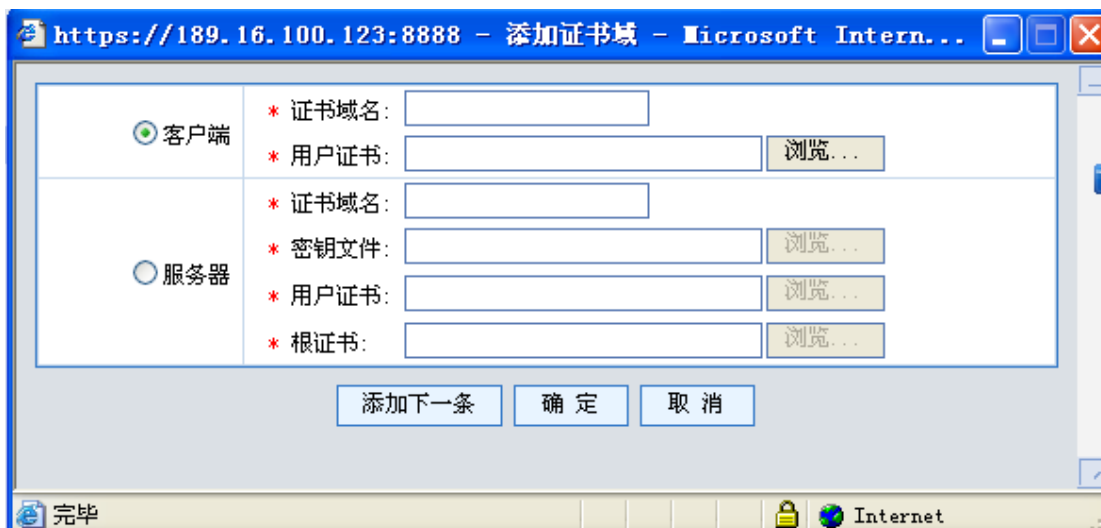


图 3-16 本地证书导入配置界面

3.5.2 本地证书

此界面完成以下功能

- 管理证书域
- 生成用户的密钥
- 生成用户证书请求
- 证书请求文件的导出
- 证书文件和 CA 根证书文件的导入
- 对证书文件和 CA 根证书文件进行格式转换，以支持 IE 浏览器导入证书的格式
- 转换后的证书文件和 CA 根证书文件的导出

添加证书域

首先单击“添加”，新建证书域，



图 3-17 添加证书域

单击“确定”之后，生成新的证书域。



图 3-18 生成新的证书域

表 3-6 本地证书操作列表

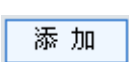
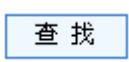






功能	说明
	添加证书域
	查找已存在的证书域
	修改相关属性的内容， 对于生成密钥，则是生成用户密钥文件； 对于证书请求，则是生成用户证书请求文件； 对于格式转换，则是进行对用户证书文件和 CA 根证书文件进行格式转换，以支持 IE 浏览器的格式
	从本地导入文件
	导出文件到本地
	删除此证书域

表 3-7 本地证书说明列表

属性名称	说明
证书域	显示证书域的名称
生成密钥	如果密钥文件已生成，则显示密钥文件名； 如果还未生成，则显示 
证书请求	如果证书请求文件已生成，则显示证书请求文件名； 如果还未生成，则显示 
请求者	显示证书请求文件的申请人
(证书请求) 导出	导出证书请求文件到本地

导入证书	如果证书文件和 CA 根证书文件已导入，则显示文件名； 如果还未导入，则显示 
格式转换	如果证书文件和 CA 根证书文件格式已转换，则显示文件名； 如果还未转换，则显示 
(格式转换)导出	导出格式转换后的证书文件和 CA 根证书文件到本地
操作	对此证书域进行删除操作

生成用户密钥


单击生成密钥的 ,




图 3-19 生成密钥

表 3-8 密钥说明列表

属性名称	说明
证书域名	显示证书域的名称
密码	密码为使用该密钥的口令， 此处密码可不填； 如果此处填写了密码，在后面的生成证书请求和格式转换时，也要输入相应的密码
确认密码	输入第二遍密码，以确认

点击“确定”后生成密钥。

生成用户证书请求

单击证书请求的 ,

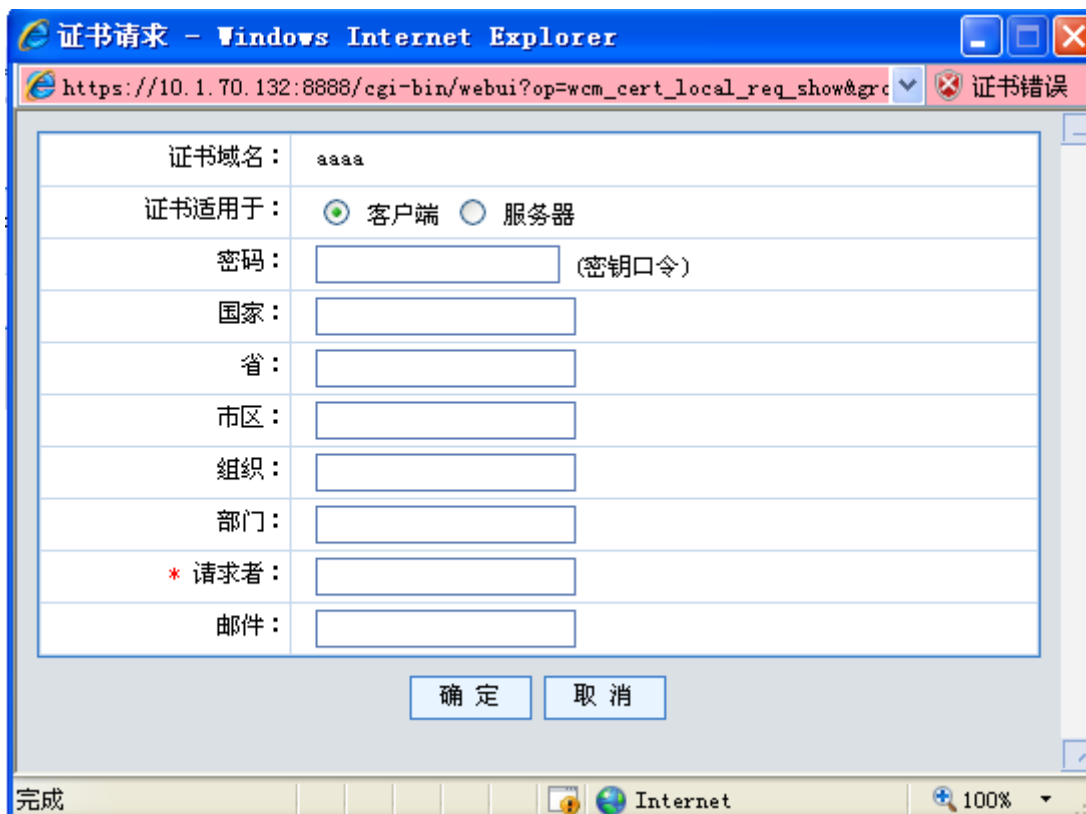



图 3-20 添加证书请求

表 3-9 证书请求配置元素表

属性名称	说明
证书域名	显示证书域的名称
证书适用于	客户端：如果证书用于客户端认证，则选择适用于客户端； 服务器：如果证书用于 web 服务器，则选择适用于服务器
密码	密码为该证书域的密钥的口令， 如果生成密钥时填写了密码，则此处必须填写。
国家	请求者所在的国家代码，长度为 2 个英文字符，默认为 CN
省	请求者所在的省，默认为 Beijing
市区	请求者所在的市区，默认为 Beijing
组织	请求者所在的单位组织或公司名称
部门	请求者所在的单位组织的部门
请求者	请求者的名称，默认为 user
邮件	请求者的 e-mail 地址

点击“确定”后生成证书请求文件。

导出证书请求文件

单击证书请求的导出 ，导出证书请求文件到本地。

导入证书文件


单击 ，点击“浏览”，选择本地文件，点击“确定”后导入用户证书文件和 CA 根证书文件。



图 3-21 证书导入

格式转换


单击格式转换的 ，



图 3-22 格式转换


表 3-10 格式转换配置元素表

属性名称	说明
------	----

证书域名	显示证书域的名称
密码	密码为该证书域的密钥的口令， 如果生成密钥时填写了密码，则此处必须填写。
设置 IE 用户证书密码	设置转换格式后的证书口令，把转换格式后的证书文件导入到 IE 浏览器时，会要求输入此密码。
确认密码	输入第二遍 IE 用户证书密码，以确认

点击“确定”后生成转换格式后的证书文件和 CA 根证书文件。

导出转换格式后的证书文件

单击格式转换的导出 ，分别导出转换格式后的证书文件和 CA 根证书文件到本地。

3.5.3 CA 中心

CA (Certification Authority) 是对数字证书的申请者发放、管理、取消数字证书的机构或受委托发放数字证书的第三方组织或公司。CA 的作用是检查证书持有者身份的合法性，并签发证书 (用加密方法在证书上签字)，以防证书被伪造或篡改。数字证书是用来建立数字签名和公-私(public-private)密钥对的。CA 在这个过程中所起的作用就是保证获得这一独特证书的人就是被授权者本人。

添加证书域

首先单击“添加”，新建证书域，



图 3-23 添加证书域

单击“确定”之后，生成新的证书域。

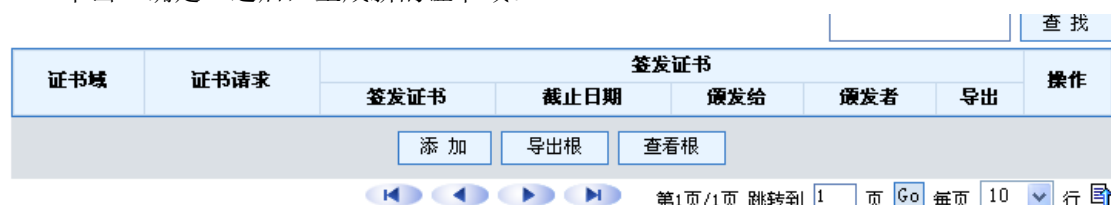




图 3-24 证书域显示


表 3-11 CA 中心操作列表

功能	说明
	添加证书域
	导出 CA 根证书到本地
	查看 CA 根证书
	查找已存在的证书域
	修改相关属性的内容， 对于证书请求，则是导入证书请求文件； 对于签发证书，则是进行签发。
	导出证书文件到本地
	删除此证书域

表 3-12 CA 中心说明列表

属性名称	说明
证书域	显示证书域的名称
证书请求	如果证书请求文件已导入，则显示导入的证书请求文件名； 如果还未导入，则显示 
签发证书	如果已经对证书请求文件进行签发，则显示证书文件名； 如果还未签发，则显示 
截止日期	显示证书文件的有效期
颁发给	显示证书文件的所有者
颁发者	显示 CA 中心的名称
导出	导出证书文件到本地
操作	对此证书域进行删除操作

导入证书请求

单击证书请求的 ，将本地证书导入到证书域。

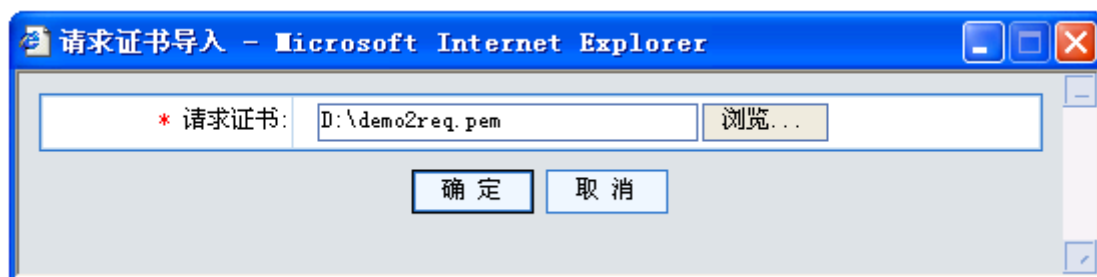


图 3-25 导入证书请求

签发证书

单击签发证书的 , 进行签发。



图 3-26 编辑签发证书

表 3-13 签发证书配置元素表

属性名称	说明
证书域名	显示证书域的名称
CA 中心密码	本设备 CA 中心的密钥口令
有效期限	从当日算起, 所签发的证书的有效天数, 范围为 1-10000, 单位为天; 如果不填写, 则默认为 7300 天(20 年)

导出证书文件

单击 , 导出证书文件到本地。

查看证书

签发完证书之后, 点击证书请求文件名和证书文件名, 例如单击 `demolreq.pem` 和 `demolcert.pem`, 可以查看证书请求文件和证书文件的相关信息。

导出 CA 根证书

单击“导出根”，导出 CA 根证书到本地。

3.6 集中管理

天清异常流量清洗设备 Guard 可以通过异常流量管理中心 Manager 实现集中管理，设备可以在单机运行和集中管理模式下进行切换，单击切换按钮切换到集中管理页面。

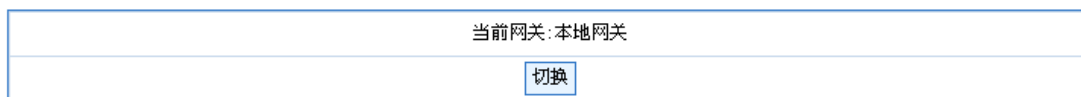


图 3-27 集中管理

3.7 批处理工具

批处理工具页面可以实现对命令的批处理，可以实现对命令的集中管理的功能。下图是批处理工具的页面：

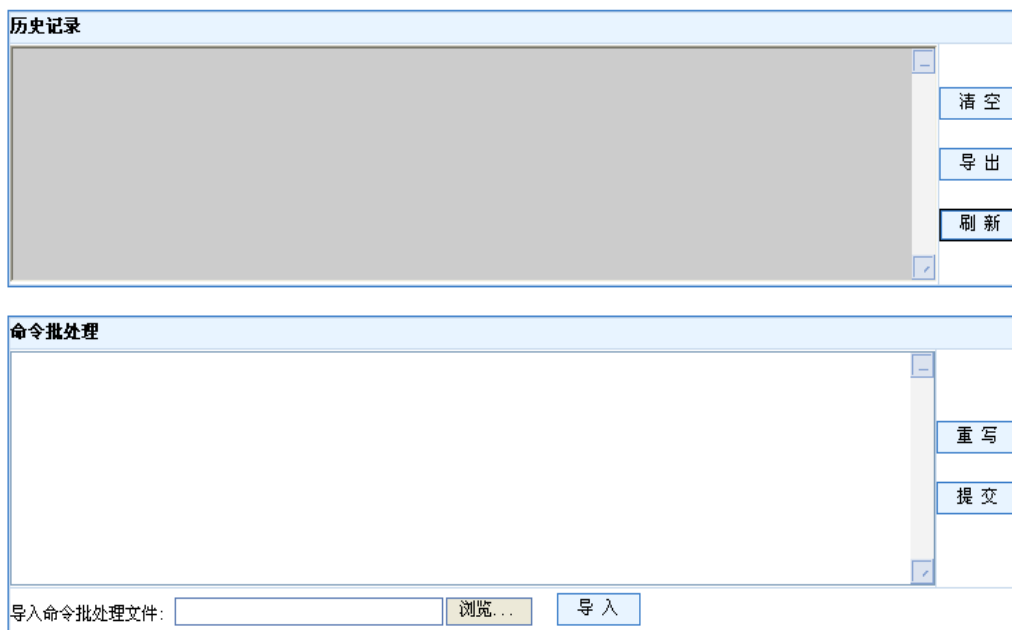


图 3-28 批处理工具

第4章 网络管理

本章主要介绍 Guard 的网络配置，由以下部分组成：网络接口，路由，ARP，用户接入和 DHCP。

4.1 网络接口

Guard 可配置的网络设备有：物理设备，VLAN 设备，桥接设备。下面对各类设备的特点做一简要说明。

物理设备：Guard 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。

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 口相联的 Guard 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：是将多个物理设备置于透明模式，并且进行分组的设备。启用此设备的 Guard 相当于一个二层交换机，但它同时可以过滤三层的内容。Guard 可以创建多个桥接设备，桥接设备绑定的物理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。

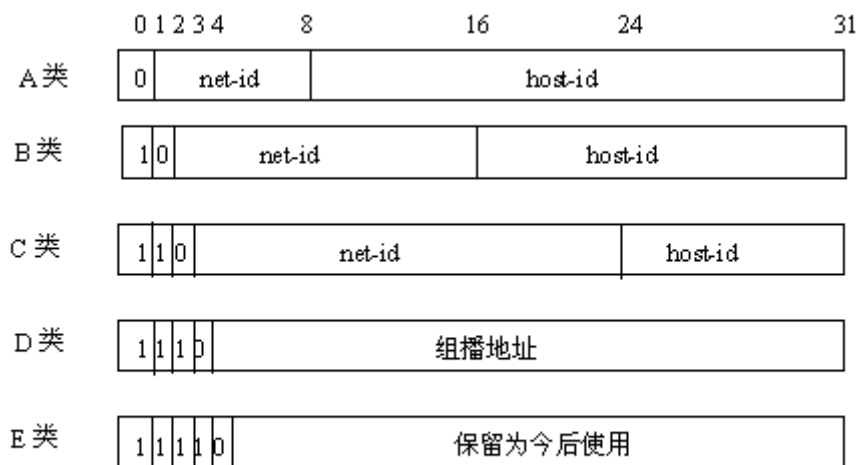
4.1.1 接口 IP 地址

用于设置接口 IP 地址功能。

所谓 IP 地址，是指分配给连接在 Internet 上的主机的一个唯一的 32 比特标识符。IP 地址一般由两部分组成：第一部分为网络号码，第二部分为主机号码。IP 地址的结构使我们可以方便地进行寻址。IP 地址由美国国防数据网的网络信息中心（NIC）进行分配。

为了方便 IP 地址的管理以及组网，Internet 的 IP 地址分成五类。如下图所示，IP 地址由下列两个字段组成：

- 网络号码字段 (net-id)；网络号码字段的前几位称为类别字段（又称为类别比特），用来区分 IP 地址的类型。
- 主机号码字段 (host-id)。



net-id—网络号码，host-id—主机号码

图 4-1 五类 IP 地址

D类地址是一种组播地址，主要是留给 Internet 体系结构委员会 IAB(Internet Architecture Board) 使用。E 类地址保留在今后使用。目前大量使用中的 IP 地址属于 A、B、C 三类中的一种。

在使用 IP 地址时要知道一些 IP 地址是保留作为特殊用途的，一般不使用。下表列出用户可配置的 IP 地址范围。

表 4-1 IP 地址分类及范围

网络类型	地址范围	用户可用的 IP 网络范围	说明
A	0.0.0.0 ~ 127.255.255.255	1.0.0.0 ~ 126.0.0.0	所有形如 127.X.Y.Z 的地址都保留作回路测试，发送到这个地址的分组不会输出到线路上，它们被内部处理并当作输入分组。
B	128.0.0.0 ~ 191.255.255.255	128.0.0.0 ~ 191.254.0.0	-
C	192.0.0.0 ~ 223.255.255.255	192.0.0.0 ~ 223.255.254.0	-
D	224.0.0.0 ~ 239.255.255.255	无	D 类地址是一种组播地址。
E	240.0.0.0 ~ 255.255.255.255	无	255.255.255.255 用于广播地址，其它地址保留今后使用。

IP 地址有一些重要的特点：

1. IP 地址是一种非等级的地址结构，和电话号码的结构不一样，也就是说，IP 地址不能反映任何有关主机位置的地理信息。
2. 当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的 IP 地址，其网络号码 net-id 是不同的，这种主机成为多地址主机 (multihomed host)。
3. 按照 Internet 的观点，用转发器或网桥连接起来的若干个局域网仍为一个网络，因此这些局域网都具有同样的网络号码 net-id。
4. 在 IP 地址中，所有分配到网络号码 (net-id) 的网络，不管是小的局域网还是很大的广域网，都是平等的。

从 1985 年起，为了使 IP 地址的使用更加灵活，只分配 IP 地址的网络号码 net-id，而后面的主机号码 host-id 则是受本单位控制。即某个单位申请到 IP 地址时，实际上只是拿到了一个网络号码 net-id，具体的各个主机号码 host-id 则由该单位自行分配，只要做到在该单位管辖的范围内无重复的主机号码即可。当一个单位的主机很多而且分布在很大的地理范围时，为了便于管理，可将单位内部的主机号码再进一步划分为多个子网。需要注意的是，子网的划分由本单位内部决定，在本单位以外是看不见划分的操作的。从外部看，这个单位只有一个网络号码。只有当外面的报文进入到本单位范围后，本单位的网络设备才根据子网号码再进行选路，找到目的主机。

如下图所示，为一个 B 类 IP 地址划分子网情况，其中子网掩码由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码和子网号码字段，而“0”对应于主机号码字段。

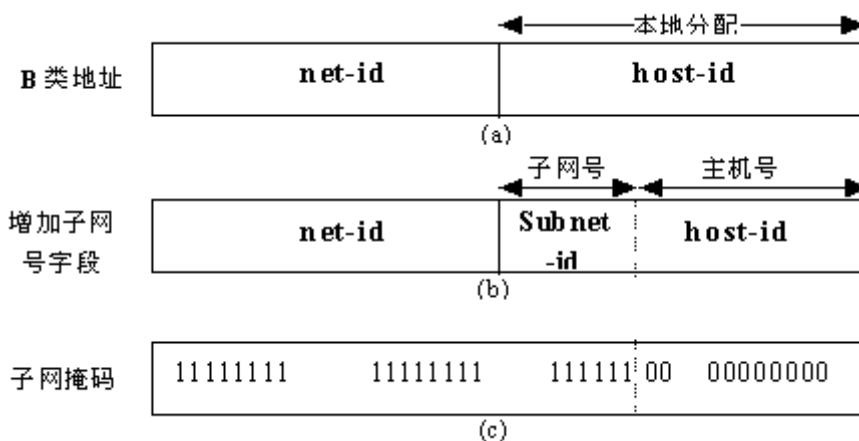


图 4-2 IP 地址子网划分

多划分出一个子网号码字段是要付出代价的。举例来说，本来一个 B 类 IP 地址可以容纳 65534 个主机号码。但划分出 6bit 长的子网字段后，最多可有 64 个子网，每个子网有 10bit 的主机号码，即每个子网最多可有 1022 (2¹⁰-2，去掉全 1 和全 0 的主机号码) 个主机号码。因此主机号码的总数是 64 * 1022 = 65408 个，比不划分子网时要少 126 个。

若一个单位不进行子网的划分，则其子网掩码即为默认值，此时子网掩码中“1”的长度就是网络号码的长度。因此，对于 A, B 和 C 类的 IP 地址，其对应子网掩码的默认值分别为 255.0.0.0; 255.255.0.0 和 255.255.255.0。

一台 Guard 可以用来连接多个网络，具有多个网络的 IP 地址。上面讲的 IP 地址还不能直接用来进行通信。这是因为：

IP 地址只是主机在网络层中的地址，若要将网络层中传送的数据报交给目的主机，必须知道该主机的物理地址。因此必须将 IP 地址解析为物理地址。

用户平时不愿意使用难于记忆的 IP 地址，而是愿意使用易于记忆的主机名，因此也需要将主机名解析为 IP 地址。

下图表示了主机名、IP 地址和物理地址之间的关系。

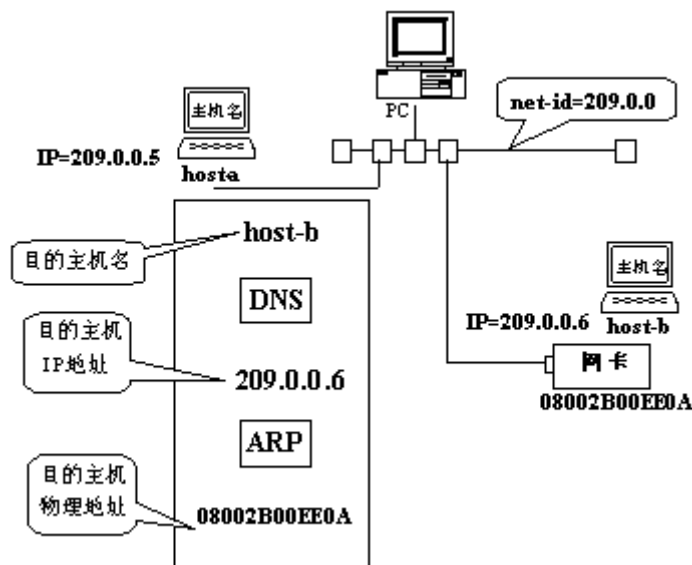


图 4-3 主机名、IP 地址和物理地址之间的关系

序号	接口名称	IP地址/掩码	地址类型	HA静态地址	VRRP组ID	操作
<input type="checkbox"/> 1	Ge0/0/0	189.16.100.123/255.255.255.0	静态	×		
<input type="checkbox"/> 2	Ge0/0/1	100.100.100.1/255.255.255.0	静态	×		
<input type="checkbox"/> 3	Ge0/0/3	3.3.3.1/255.255.255.128	静态	×		

全选 第1页/1页 跳转到 页 Go 每页 行

图 4-4 接口 IP 地址列表

此界面可以完成以下功能：

- 添加接口 IP 地址
- 编辑接口 IP 地址
- 删除接口 IP 地址

添加接口 IP 地址：

- 点“添加”按钮，进入“接口 IP 维护”
- 添加接口 IP 地址参数
- 点“确定”按钮完成添加

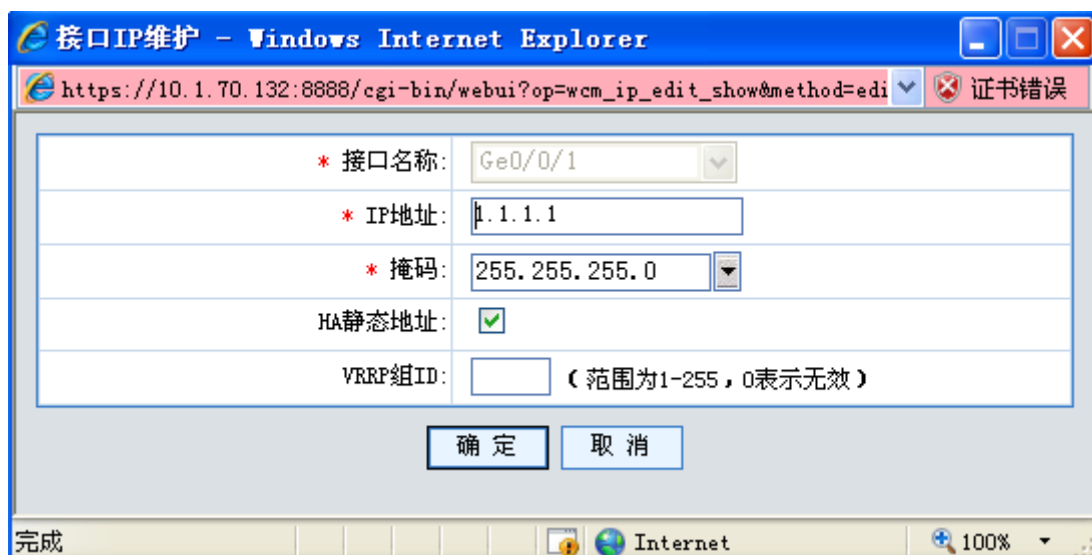


图 4-5 添加接口 IP 地址

编辑接口 IP 地址：

- 点“操作”一栏中的“编辑”图标，打开“接口 IP 维护”界面
- 执行修改操作
- 点击“确定”按钮完成修改

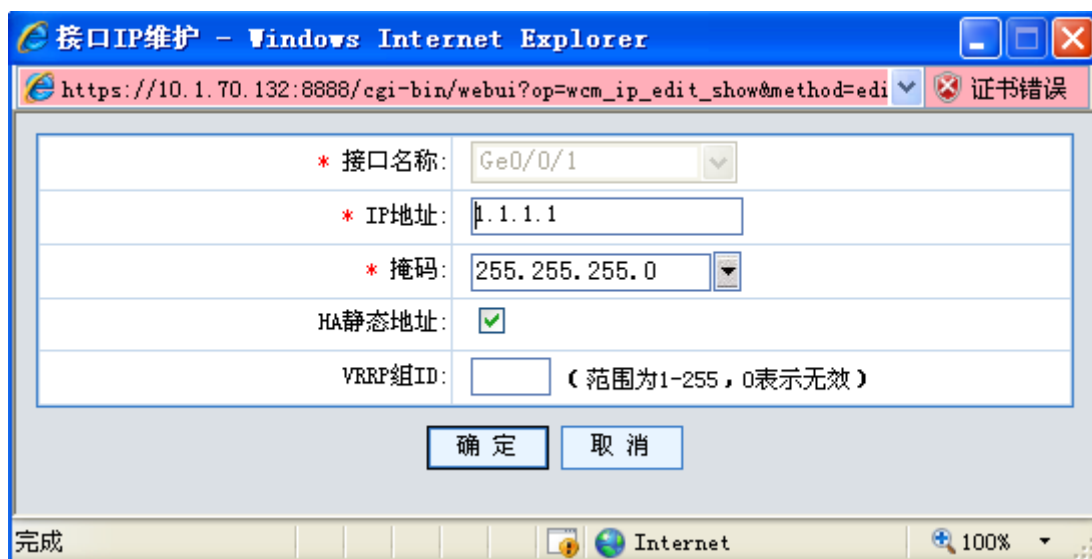


图 4-6 编辑接口 IP 地址

表 4-2 接口 IP 可配置的属性

属性名称	描述
接口名称	接口名称，选择配置 IP 地址的接口名称
IP 地址	接口的 IP 地址
掩码	接口的地址掩码

HA 静态地址	接口 IP 地址是否为 HA 静态地址
VRRP 组 ID	接口 IP 地址所属的 VRRP 组 ID

Guard 的每个接口可以配置多个 IP 地址。

IP 地址的配置支持如下情况：

- 兄弟接口之间不可以是同一网段
- 同一个接口的 IP 地址可以是同一网段。

HA 静态地址选项是标识配置的 IP 地址是静态地址，启动 ha 功能后做为不可迁移地址使用，一般用作 HA 口地址和管理地址，不能迁移到不同主机上。

在 HA 工作在负载分担模式时，可以在接口上配置虚拟路由协议 VRRP 用的备份组地址，需要指定该地址对应的虚拟路由组 ID。vrrp-ID 表示 vrrp 组 ID 号，范围为 1-255 的整数。

缺省情况下，无 IP 地址。

注意：

接口 IP 地址，目前仅支持 A、B、C 类 IP 地址，对于 0 网段以及 127 网段地址也不支持。

当接口设置为动态获取 IP 地址时，不允许配置静态 IP 地址。

当接口加入到桥组中去时，该接口不允许配置静态 IP 地址。

删除接口 IP 地址：

- 点“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

4.1.2 接口配置

4.1.2.1 以太网接口

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 4-3 物理设备上可配置的属性

属性名称	描述
接口名称	接口名称，不能修改。
MAC 地址	接口的 MAC 地址，可以修改。如果忘记了接口最初的 MAC 地址，可以将 MAC 地址置为空值，Guard 会恢复接口的 MAC 地址。
工作模式/速率	接口的工作模式/速率可以选择自适应方式，也可以分别选择固定的设置。 <ul style="list-style-type: none"> ● 接口的工作模式，有全双工、半双工两种 ● 接口的速率，有 10/100/1000M 三种，接口的工作模式/速率的缺省值为自协商。
MTU	接口的 MTU（最大传输单位）。可设置的范围是 68 到 1500。 缺省值为 1500。
地址类型	IP 地址的获取方式，目前支持的有以下两种

	<p>1: 静态</p> <p>2: 通过 DHCP 获取，即 Guard 相应物理设备作为 DHCP 客户端获得 IP 地址。</p> <p>缺省值为静态。</p>
非混杂模式	接口是否为混杂模式
接口启用	是否启用此接口
trunk 模式	<p>是否启用 trunk 模式</p> <p>启用 trunk 模式有以下三种：</p> <p>1: 处理入方向</p> <p>2: 处理出方向</p> <p>3: 处理出和入方向</p>

[以太网接口](#) | [VLAN接口](#) | [桥接口](#) | [链路聚合接口](#)

接口名称	MAC地址	MTU	工作模式/速率	地址类型	启用	备注	操作
Ge0/0/0	0010.FE30.5003	1500	系统自动协商	静态	<input checked="" type="checkbox"/>	Ge Interface	
Ge0/0/1	0010.FE30.5002	1500	系统自动协商	静态	<input checked="" type="checkbox"/>	Ge Interface	
Ge0/0/2	0010.FE30.5001	1500	系统自动协商	静态	<input checked="" type="checkbox"/>	Ge Interface	
Ge0/0/3	0010.FE30.5000	1500	系统自动协商	静态	<input checked="" type="checkbox"/>	Ge Interface	

图 4-7 物理设备列表

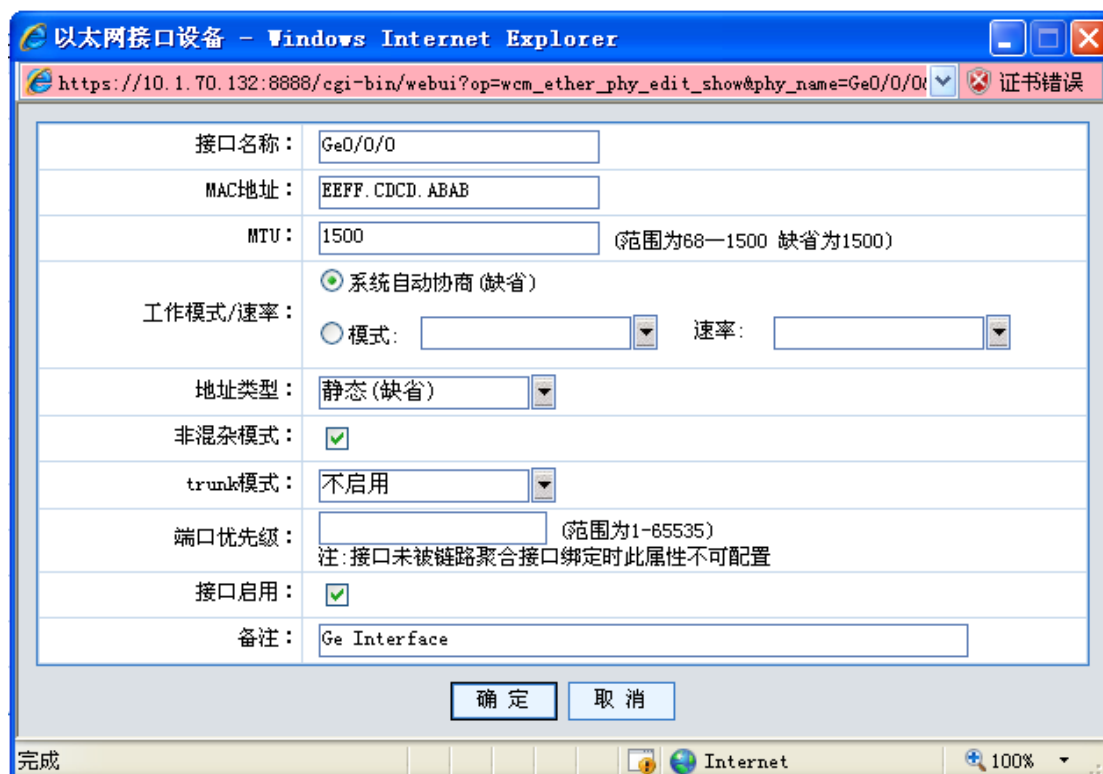


图 4-8 物理设备可配置的属性

4. 1. 2. 2 VLAN 接口

VLAN 设备是一种在物理接口或链路聚合接口基础上创建的设备。VLAN 设备可以与其他同 VLAN 的设备通讯，并通过 Guard 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。

表 4-4 VLAN 设备上可配置的属性

属性名称	描述
填写 VLAN ID	VLAN ID 是一个 1 到 4094 的无符号整数
绑定的物理接口	VLAN 的绑定接口必须是启用的。
VLAN 接口名称	VLAN 接口的名称 由绑定的物理接口+“.”+VLANID 组成。不可更改。
是否启用	是否启用此设备



图 4-9 VLAN 设备列表

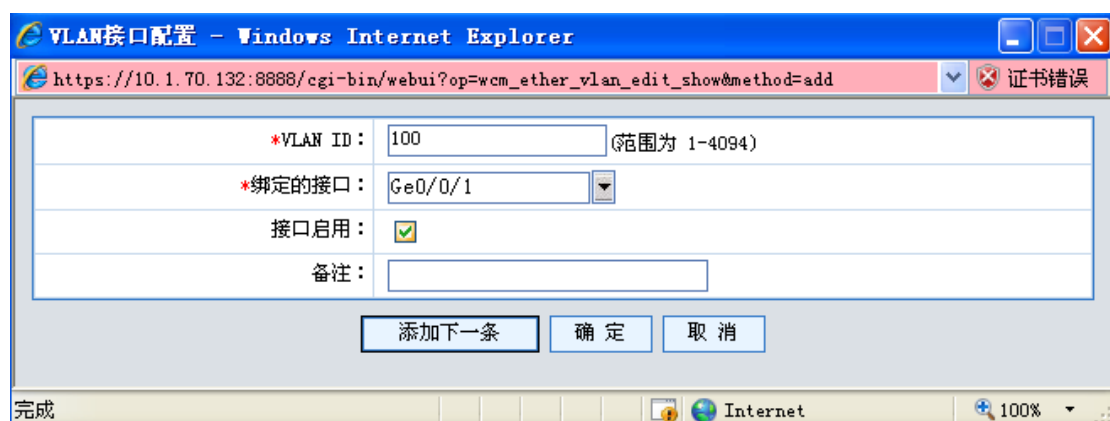


图 4-10 VLAN 设备可配置的属性

4. 1. 2. 3 桥接口

桥接口上可以绑定多个处于启动状态的物理接口或，也可以配置多个 ip 地址。VLAN 设备不允许绑定在桥接口上。桥接口的 ID 是唯一的，对具有同样 ID 的桥接口进行操作被视为修改。

表 4-5 桥接口可配置的属性

属性名称	描述
填写桥接口 ID	桥接口 ID 是一个 0 到 1023 的无符号整数
绑定的物理接口	桥接口的绑定接口必须是启用的。
是否启用 STP 协议	STP（生成树协议）是一个二层管理协议。在一个扩展的局域网中参与 STP 的所有交换机之间通过交换桥协议数据单元 bpd（bridge protocol data unit）来实现
是否启用	是否启用此设备

以太网接口 | VLAN接口 | **桥接口** | 链路聚合接口

序号	桥接口名称	绑定接口名称	启用STP协议	启用接口	备注	操作
<input type="button" value="添加"/>						

⏪ ⏩ 第1页/1页 跳转到 页 每页 行

图 4-11 桥接口列表

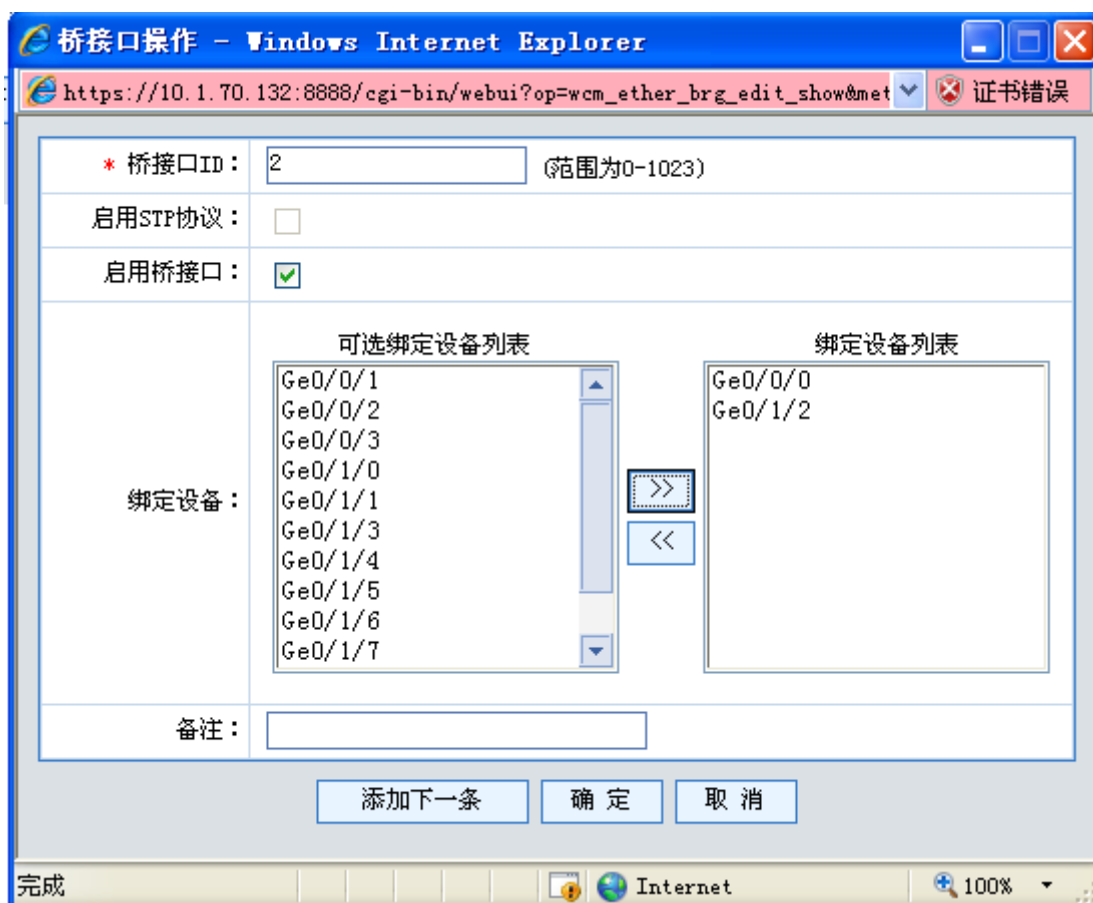


图 4-12 桥接口可配置的属性

4. 1. 2. 4 链路聚合接口

链路聚合接口是将多个以太网端口汇聚在一起形成一个逻辑上的汇聚组,对于上层应用而言,可将同一汇聚组内的多条物理链路视为一条逻辑链路。链路聚合端口可以实现汇聚组中各个成员端口之间进行流量分担,同时,同一汇聚组的各个成员端口之间又互为备份,提高了连接可靠性。

链路聚合接口上可以绑定不超过 10 个以太网接口,也可以配置多个 ip 地址。VLAN 设备不允许绑定在链路聚合接口上。链路聚合接口的 ID 是唯一的,对具有同样 ID 的链路聚合接口进行操作被视为修改。

已绑定接口聚合成功的必要条件:

- 1) 接口必须是全双工模式;
- 2) 同一汇聚组内的接口必须速率一致;

表 4-6 链路聚合接口可配置的属性

属性名称	描述
链路聚合接口 ID	链路聚合接口 ID 是一个 0 到 1023 的无符号整数
MAC 地址	可以指定链路聚合接口的 MAC 地址,默认为空
配置模式	默认是动态 LACP 方式,该方式遵循 IEEE802.3AD 协议标准
MTU	可以指定链路聚合接口的 MTU,默认为 1500
系统优先级	动态 LACP 方式协商过程中使用的参数,默认为 65535
报文发送策略	流量分担时使用的端口选择策略,默认为 src-ip,还支持 src-mac、src-dest-mac、src-ip、dest-ip、src-dest-ip、src-port、dest-port、src-dest-port 共 9 中方式。
启用接口	链路聚合接口必须在启用的状态下,才能绑定以太网接口
绑定设备	仅支持以太网接口。若以太网接口处于未启用状态,则绑定后自动启用。

以太网接口 | VLAN接口 | 桥接口 | **链路聚合接口**

序号	接口名称	绑定接口名称	配置模式	报文发送策略	启用接口	备注	操作
<input type="button" value="添加"/>							

⏪ ⏴ ⏵ ⏩
第 1 页 / 1 页 跳转到 页 每页 行

图 4-13 链路聚合接口列表

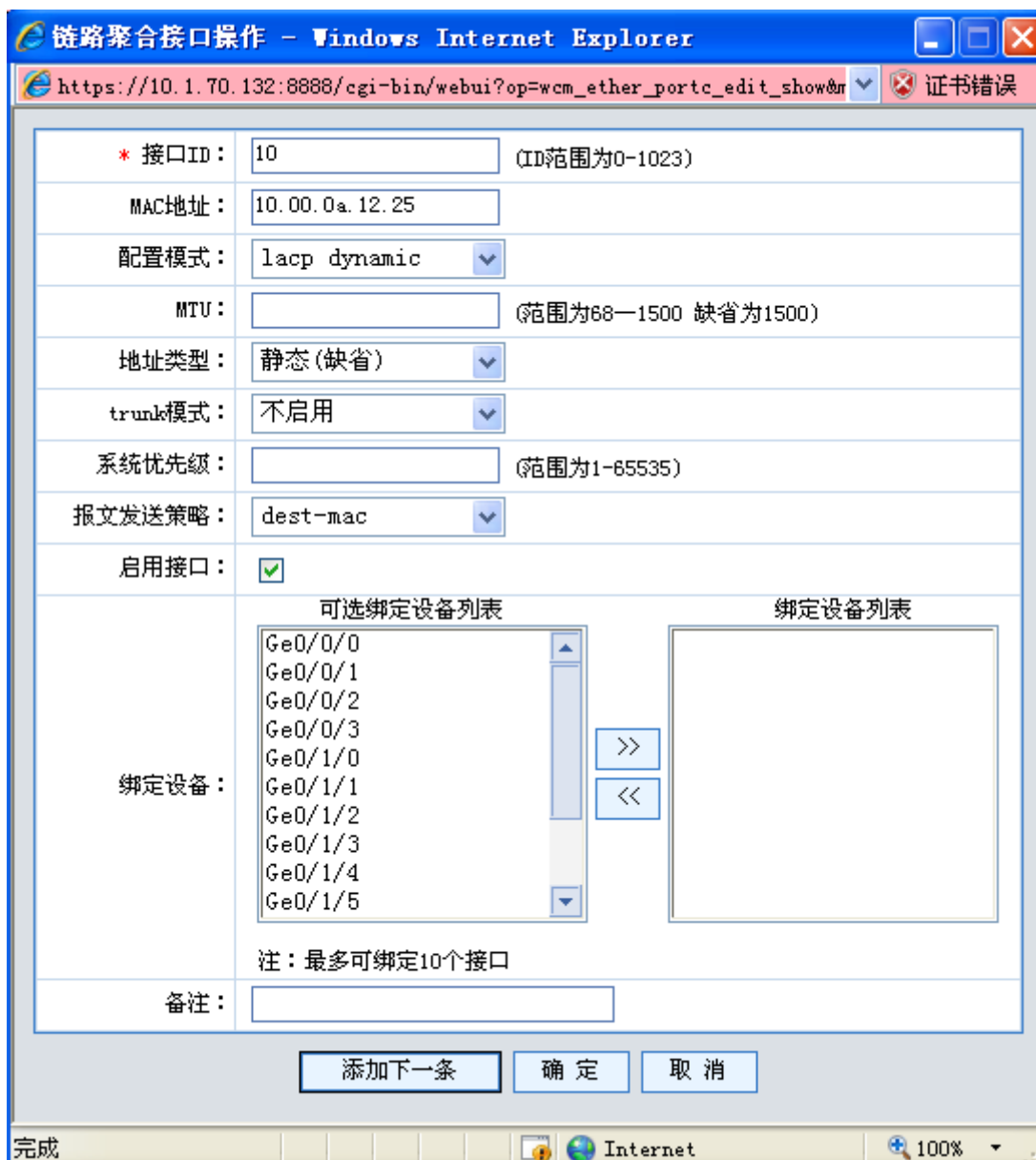


图 4-14 链路聚合接口可配置属性

4.2 ARP

4.2.1 静态 ARP

Guard 提供静态 ARP 功能，可以为指定的 IP 地址设置对应的 MAC 地址。

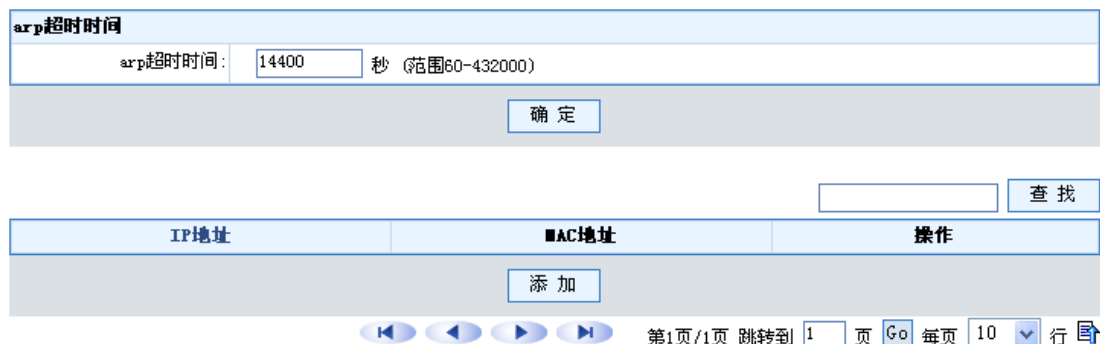


图 4-15 静态 ARP 的显示

此界面可以完成以下功能:

- 添加静态 ARP
- 编辑静态 ARP
- 删除静态 ARP
- 查找静态 ARP

添加静态 ARP:

- 点“添加”按钮, 进入“静态 ARP 维护”
- 设置 IP 地址和 MAC 地址
- 点“确定”按钮完成添加
- 点“添加下一条”可以继续添加



图 4-16 静态 ARP 的添加

编辑静态 ARP:

- 点“操作”一栏中的“编辑”图标, 打开“静态 ARP 维护”界面
- 执行修改操作
- 点击“确定”按钮完成修改

删除静态 ARP:

- 点“操作”一栏中的“删除”图标, 弹出删除对话框

- 点“确定”按钮完成删除

查找静态 ARP:

- 在界面右上角输入框中输入要查找的 IP 地址或者 MAC 地址
- 点“查找”就会显示符合条件的静态 ARP 信息

4.2.2 ARP 查看

Guard 提供 ARP 功能, 可以为指定的 IP 地址设置对应的 MAC 地址。通过下表可以查看其 MAC、ARP 类型、端口号。

IP地址	MAC地址	ARP类型	端口号	操作
189.16.100.152	0010.2030.4103	dynamic	Ge0/0/0	
189.16.100.161	001b.2d30.5003	dynamic	Ge0/0/0	
189.16.100.162	0030.2030.0200	dynamic	Ge0/0/0	
189.16.100.175	001b.2d30.5003	dynamic	Ge0/0/0	
189.16.100.181	00e0.adad.caca	dynamic	Ge0/0/0	
189.16.100.19	0010.2030.5003	dynamic	Ge0/0/0	
189.16.100.191	0010.2033.5003	dynamic	Ge0/0/0	
189.16.100.194	0010.adfe.5003	dynamic	Ge0/0/0	
189.16.100.195	b410.2d3f.5c0f	dynamic	Ge0/0/0	
189.16.100.55	0011.5b13.4f59	dynamic	Ge0/0/0	

第1页/2页 跳转到 页 每页 行

图 4-17 静态 ARP 查看

4.2.3 免费 ARP

Guard 支持发送免费 ARP 功能, 包括一次性发送和定时发送。前者仅触发一次发送免费 ARP 的动作; 后者每隔一段时间都会自动向外发送免费 ARP。

免费ARP全局配置

系统发送免费ARP的时间间隔: 秒 (范围为:1-86400)

单次发送免费ARP

指定系统发送免费ARP的接口:

免费ARP配置

序号	接口名称	发送免费ARP时间间隔	操作
<input type="button" value="添加"/>			

图 4-18 免费 ARP 参数配置界面

- 免费 ARP 全局配置

配置免费 ARP 的发送间隔时间，以秒为单位，对所有以太网接口均有效。

- 单次发送免费 ARP

指定某个接口发送一次免费 ARP，支持所有以太网接口、链路聚合接口和桥接口。

- 免费 ARP 配置

指定某个接口以一定的时间间隔发送免费 ARP，支持所有以太网接口、链路聚合接口和桥接口。



图 4-19 免费 ARP 的添加

表 4-7 免费 ARP 的数据域说明

域名	说明
接口名称	支持以太网接口、链路聚合接口和桥接口
发送免费 ARP 的时间间隔	发送免费 ARP 的时间间隔，以秒为单位

4.3 路由

Guard 提供路由功能，下面分别介绍静态路由和策略路由。

4.3.1 静态路由

Guard 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。

Guard 的默认路由也是在这里手工添加的，也可以删除，修改默认路由。默认路由只能有一个生效。

使用拨号设备时，一般运营商会自动指定一个默认路由，如果事先自己定义了默认路由，有可能会造成拨号设备的默认路由无效，从而造成网络不通，因此如果使用拨号设备，最好不要在这里配置默认路由。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。

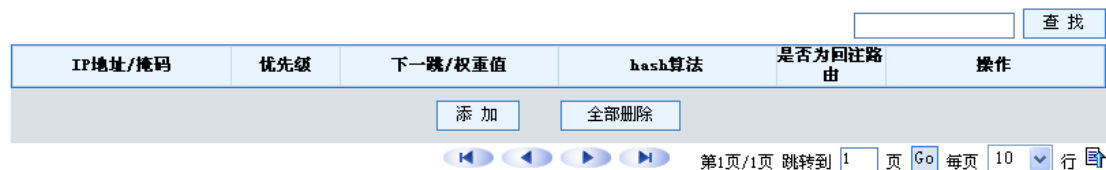


图 4-20 静态路由的显示

此界面可以完成以下功能：

- 添加静态路由
- 编辑静态路由
- 删除静态路由

添加静态路由：

- 点“添加”按钮，进入“静态路由维护”
- 添加静态路由参数
- 点“确定”按钮完成添加

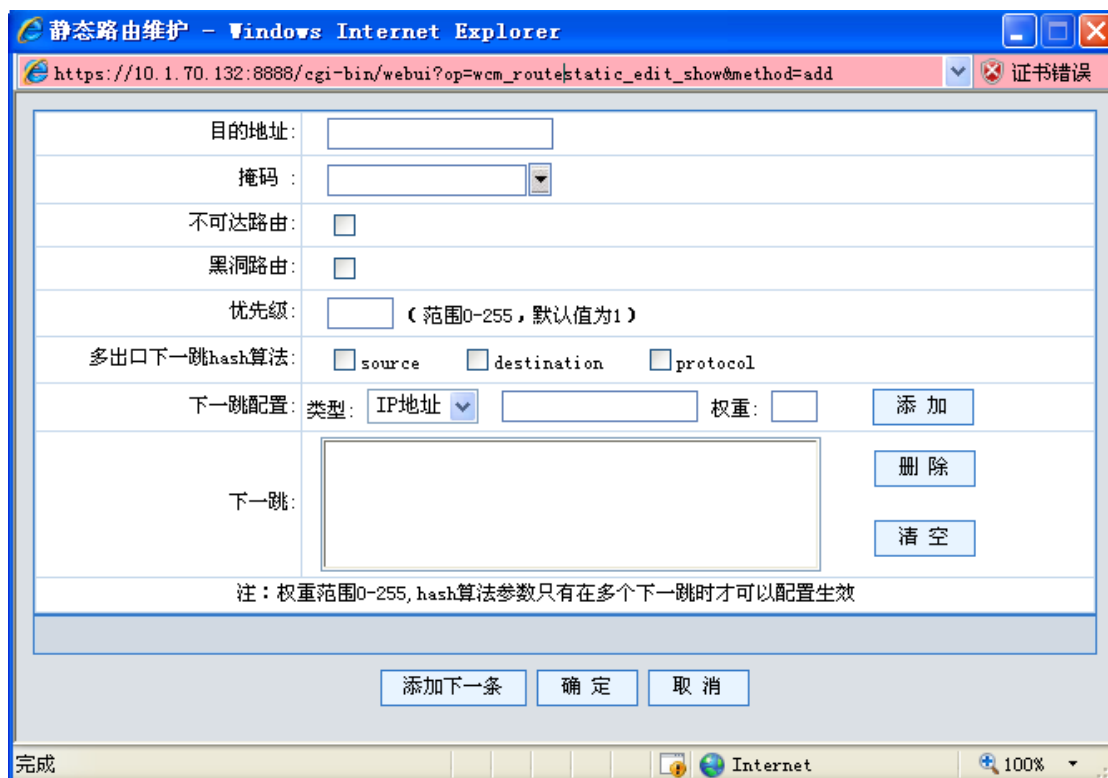


图 4-21 静态路由的添加

编辑静态路由：

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

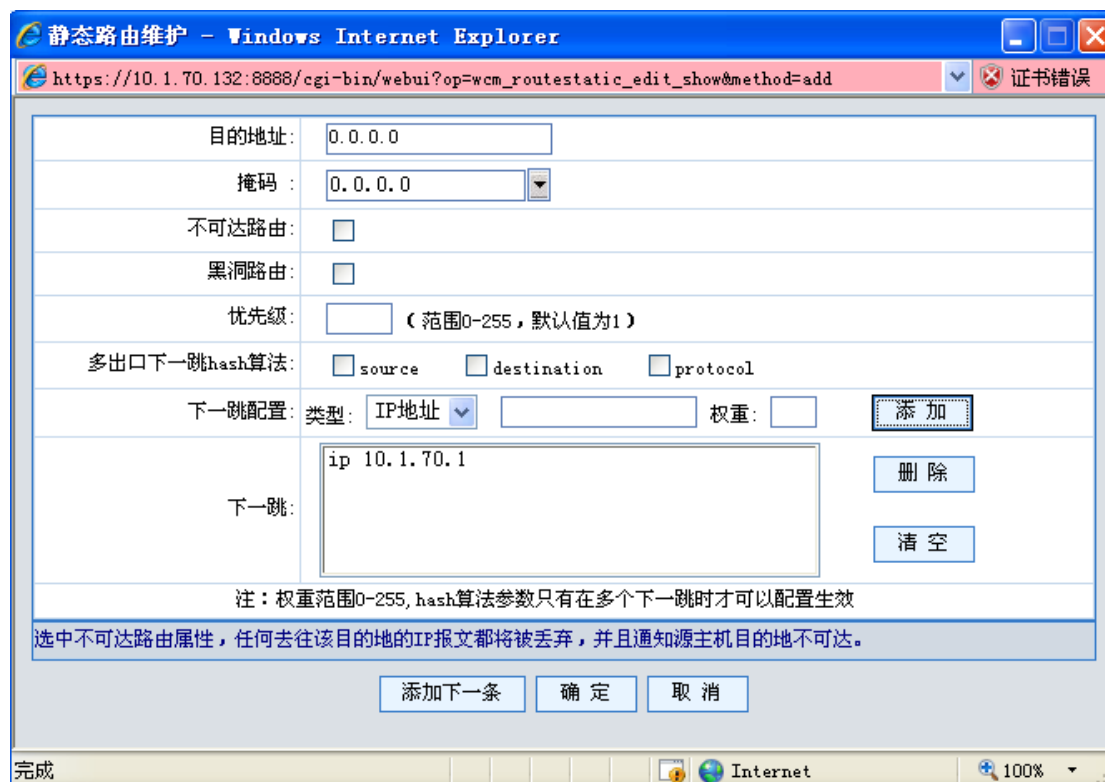


图 4-22 静态路由的维护

表 4-8 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	设置目的 IP 地址	
掩码	设置目的子网掩码	
不可达路由	该静态路由为不可达	
黑洞路由	该静态路由为黑洞	
优先级	静态路由的优先级属性 取值范围 0-255 取值越大优先级越低	
多出口	多出口负载均衡属性 选择该属性会设置多条路由	
多出口下一跳 hash 算法	选择 hash 算法	
下一跳配置	下一跳 IP 地址	
指定发送接口	下一跳为接口	从网络配置>>网络设备中选取接口
权重值	下一跳信息的权重 取值范围 1-255，值越大选择该下一跳的机会越大	

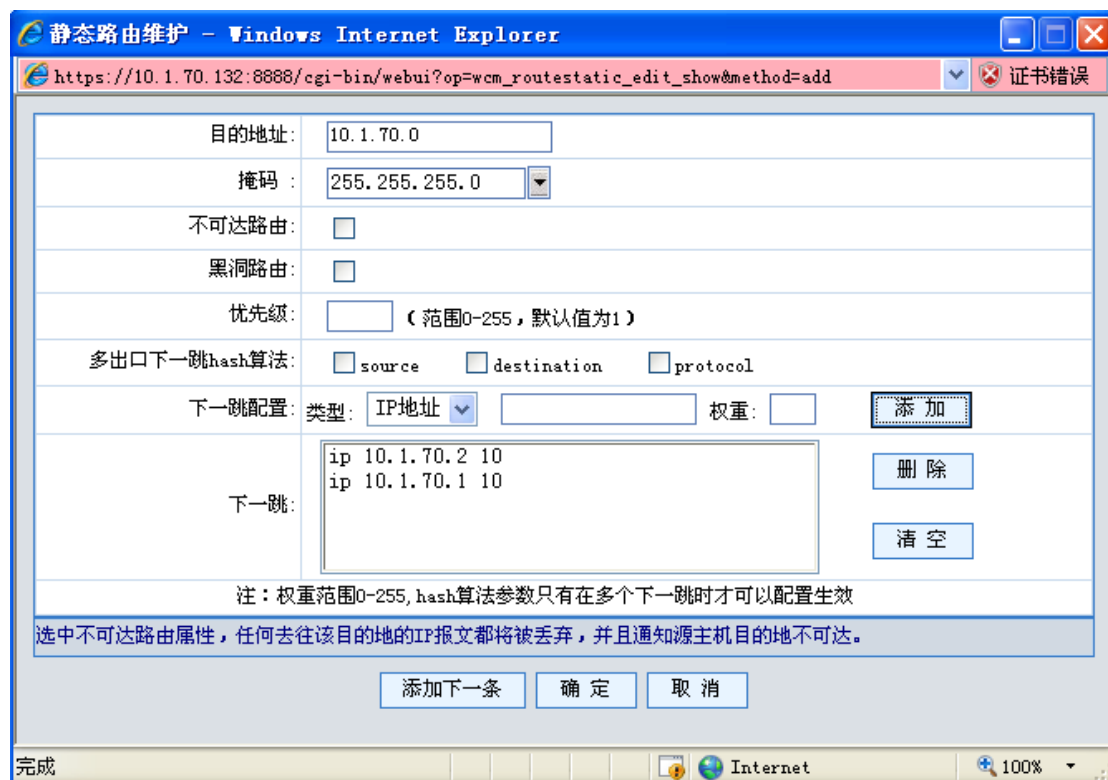


图 4-23 静态路由多出口维护

删除静态路由：

- 点“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

删除所有静态路由：

- 点“全部删除”按钮，即可完成删除所有静态路由工作

4.3.2 OSPF

Guard 提供 OSPF 功能，能够与其它支持 OSPF 功能的网络设备进行动态路由协商。

在 OSPF 页面上，可以配置路由重分发，启动、停止 OSPF 功能，设置路由器 ID，添加、删除区域，设置区域认证方式，添加、删除网络，添加、删除网络接口认证口令。

OSPF		
<input type="button" value="启用"/> <input type="button" value="停止"/>		
Router ID		
路由器ID: <input type="text" value="0.0.0.0"/>		
<input type="button" value="确定"/> <input type="button" value="清除"/>		
区域		
区域	认证	操作
<input type="button" value="添加区域"/>		
网络		
网络	区域	操作
<input type="button" value="添加网络"/>		

图 4-24 OSPF 配置页面

4. 3. 2. 1 路由重分发

打开 OSPF 界面时，将显示已经重分发的路由（bgp、直连、静态、rip）。如需修改，将对应的选项框选中或取消，然后点击确定即可生效。

4. 3. 2. 2 OSPF

OSPF 功能未启动时，会显示“启动”按钮，点击后会启动 OSPF 功能。

OSPF 功能启动后，会显示“停止”按钮，点击后会停止 OSPF 功能。

修改路由器 ID 后，需要点击“启动/停止”按钮以使其生效。

4. 3. 2. 3 区域



图 4-25 OSPF 添加区域对话框

添加区域时，需要指定区域名（可使用十进制形式或 IP 地址形式）和认证方式，认证方式可选择不认证、明文口令认证、消息摘要认证。最多可以添加 255 个区域。

添加区域后，可以修改其认证方式。

可以删除区域，添加了网络的区域不能被删除。

4. 3. 2. 4 网络



图 4-26 OSPF 添加网络对话框

添加网络时，需要指定 IP 地址和掩码，以及所属区域。最多可以添加 255 个网络。可以删除网络。

4. 3. 2. 5 接口



图 4-27 OSPF 添加网络接口明文口令对话框



图 4-28 OSPF 添加网络接口消息摘要密钥对话框

添加明文口令时，需要指定密码。添加消息摘要密钥时，需要指定 ID 和密钥。每个网口接口最多可以添加 1 个明文口令和 255 个消息摘要密钥。所有网络接口的明文口令和消息摘要密钥的总数最多为 255 个。

可以删除明文口令和消息摘要密钥。

4.3.3 智能路由

Guard 提供智能路由功能，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。智能路由优先于静态路由生效。

智能路由的优先级高于静态路由，即数据包到达时，首先根据报文特征匹配智能路由规则，如果找到匹配的规则，则根据规则进行智能路由，如果找不到，则进行静态路由。

4.3.3.1 路由表

路由表页面是专门为选路策略服务的，它与静态路由页面的各表项基本相同，不同之处在于增加了“路由表 ID”项，该项将在选路策略中被引用。

4.3.3.2 选路策略

管理员可以添加、编辑、删除、应用和禁用智能路由规则。智能路由规则的参数包括智能路由策略名称、匹配的 PCP 名称、应用的路由表 ID。

[路由表](#) | [选路策略](#) | [ISP地址](#) | [路由监测](#)

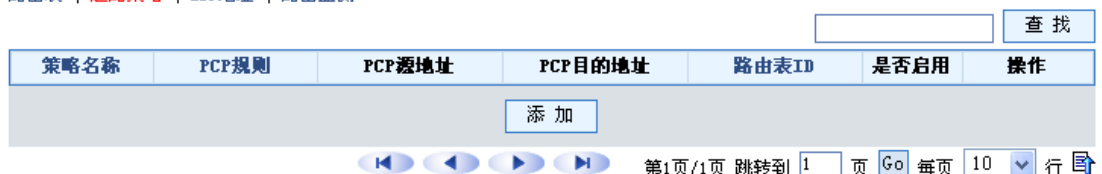


图 4-29 智能路由的显示

此界面可以完成以下功能：

- 添加选路策略

- 编辑选路策略
- 删除选路策略
- 启用/禁用选路策略

添加选路策略：

- 点“添加”按钮，进入“智能路由维护”
- 添加选路策略参数，请务必保证下一跳地址和选择的网络接口在同一网段内。
- 点“确定”按钮完成添加

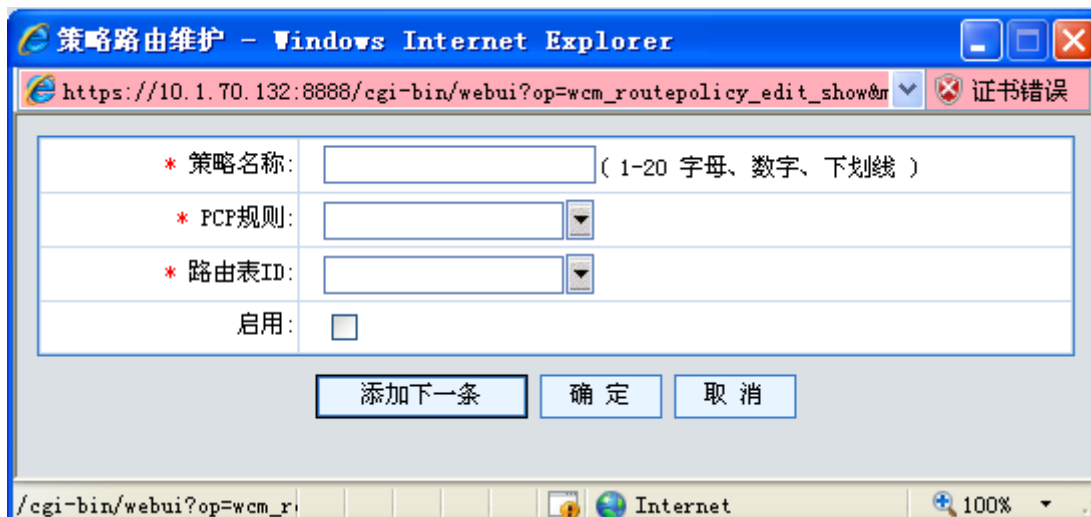


图 4-30 选路策略的添加

编辑选路策略：

- 点“操作”一栏中的“编辑”图标，打开“选路策略维护”界面
- 执行修改操作
- 点击“确定”按钮完成修改



图 4-31 选路策略的维护

删除策略路由：

- 点“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

启用/禁用选路策略：





- 点“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 4-9 添加和编辑时参数说明

域名	说明	和其他界面的关系
策略名称	选路策略名称	
PCP 规则	选路策略引用的 PCP 规则名称	从包分类中选取 PCP 规则
路由表 ID	选路策略使用的路由表 ID	从网络配置>>路由>>智能路由>>路由表中选取

4. 3. 3. 3 ISP 地址

ISP 地址保存了 ISP 服务商提供的地址列表，在选路时可根据访问的目的 IP 智能判断最佳路由出口。

ISP 地址文件分为两种类型，一种是系统预定义文件，在出厂时已预置于系统中；一种是用户自定义文件，用户可根据需要自己生成地址文件。二者的区别在于，前者包含了出厂版本信息，内容大而全，不允许用户删除；后者灵活方便，小而精，可以删除。

ISP 地址文件在格式、大小、数量等方面均有所限制。数量上，两种类型文件的总数不得超过 20；容量上，单个文件的大小不得超过 1MB；格式上，文本中包含的是纯粹的地址信息，并按照下面三种形式组织：

```
xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx --- ip 地址/子网掩码
xxx.xxx.xxx.xxx/xx --- ip 地址/掩码长度
xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx --- ip 地址段
```

当超出文件数目限制时，将不允许导入；当文件容量大于限额时，导入后将被系统自动删除；当格式不符合上述规范时，也会被系统删除。

另外，ISP 地址文件名必须满足以下条件：

1. 文件名以“ISP_”开头，注意大小写；
 2. 文件名总长度不得超过 20；
 3. 文件名中只许包含字母、数字、下划线、点，其他字符一律非法
- 不满足上述条件的文件，将不允许导入。

本界面可以完成以下功能：

- 导入文件
- 更新文件
- 删除文件

导入文件：

- 点“浏览”按钮，选择需要导入的文件
需要注意的是，不仅该文件要符合上述规范，还不得与现有文件重名

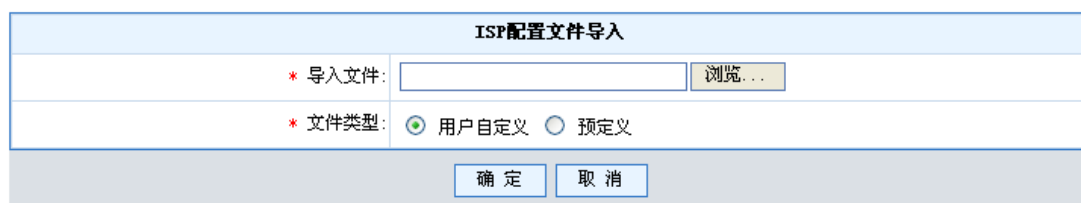
- 选择文件类型

默认是用户自定义

- 点“确定”按钮完成导入

若文件较大，需要等候一段时间；若文件不合法，将会提示错误信息，并删除该文件

[路由表](#) | [选路策略](#) | [ISP地址](#) | [路由监测](#)



ISP配置文件导入




* 导入文件: 浏览...

* 文件类型: 用户自定义 预定义

确定 取消

图 4-32 ISP 配置文件导入

文件列表管理：

- 列表中给出了已有 ISP 配置文件的各项属性，包括文件名、文件类型、文件大小、导入时间(对于系统预定义文件，这里显示的是版本相关信息)
-  图标表示更新文件，更新的文件名必须与现有文件一致； 图标表示导出文件，方便用户查看修改； 图标表示删除文件，当该文件被其他规则使用时，将不允许删除


序号	文件名	文件类型	文件大小	导入时间	操作
1	ISP_CNC.txt	预定义	3.2 K	v1.102009/12/10	 
2	ISP_CTT.txt	预定义	272 Byte	v1.102009/12/10	 
3	ISP_Cernet.txt	预定义	1.4 K	v1.102009/12/10	 
4	ISP_ChinaMobile.txt	预定义	304 Byte	v1.102009/12/10	 
5	ISP_ChinaTelecom.txt	预定义	3.2 K	v1.102009/12/10	 

图 4-33 ISP 配置文件管理列表

更新文件：

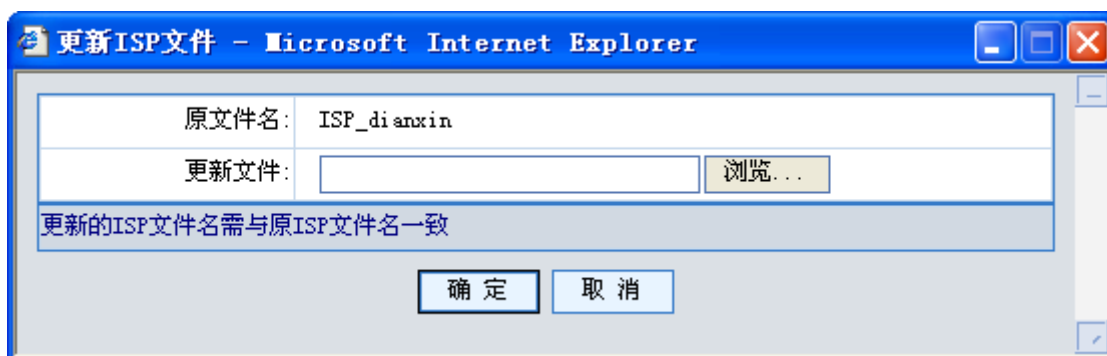


图 4-34 ISP 配置文件更新

4. 3. 3. 4 路由监测

路由监控是智能路由的重要功能，通过设置监控路由对象，可以及时发现路由变化，智能调整路由。

[路由表](#) | [选路策略](#) | [ISP地址](#) | [路由监测](#)

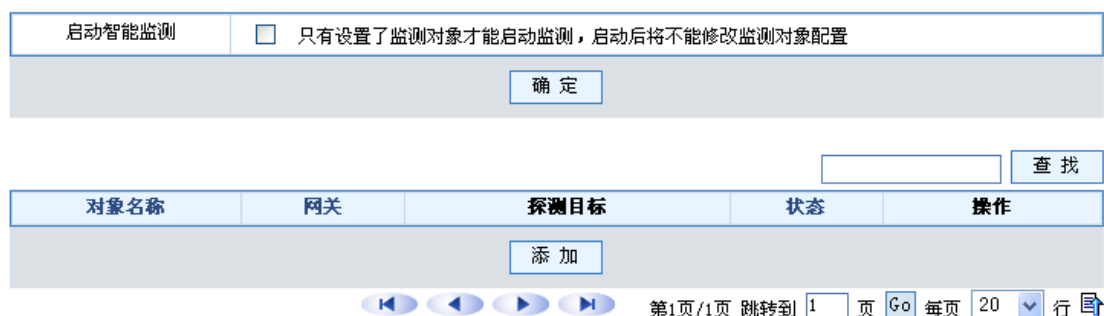


图 4-35 路由监控

该页面可启用智能探测功能，也可添加、删除、修改、查看路由监测对象。

添加路由监控对象

- 点“添加”按钮，进入“路由监测配置”页面
- 设置监测对象名称
- 设置监控网关的地址
- 设置探测主机配置（通过探测主机的健康状态，可判断线路健康状态，可不设置）
- 设置监测时间间隔（可不设置，默认 30 秒）
- 设置监测容错次数（可不设置，默认为 0 次，建议 3）
- 点“确定”按钮完成添加
- 点“添加下一条”可以继续添加

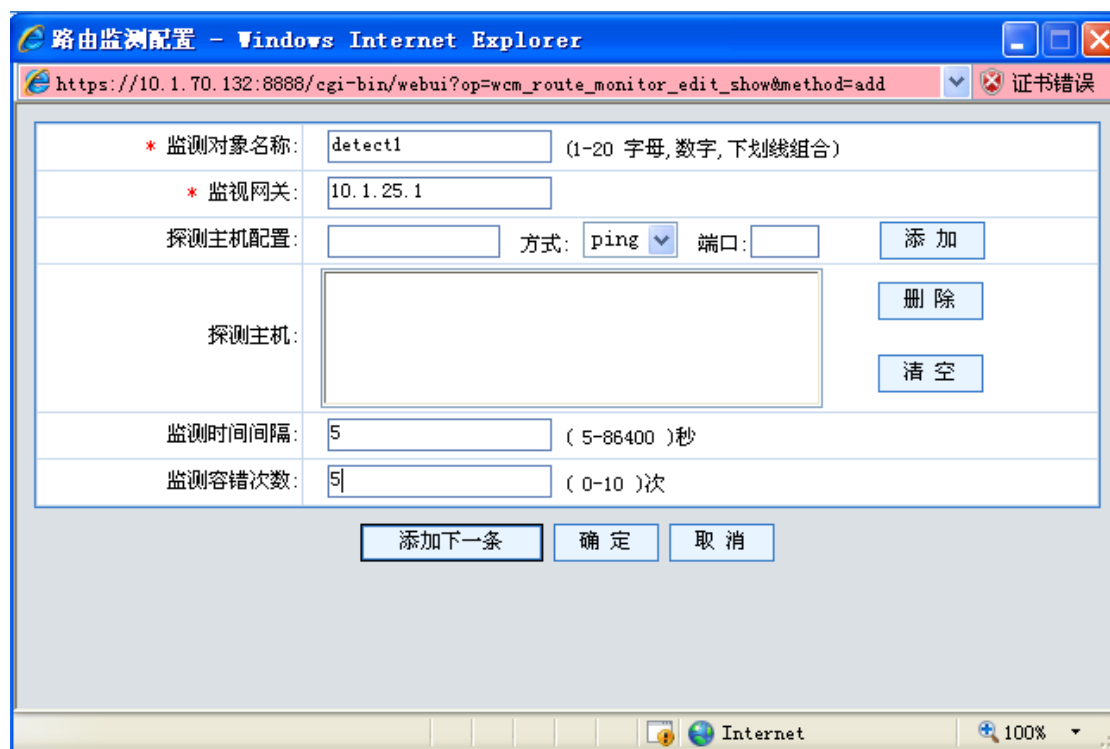


图 4-36 添加/编辑路由监测配置

数据域说明

表 4-10 路由监测配置数据域

域名	说明	和其他界面的关系
监测对象名称	监控对象的命名	
监控网关	监控网关的 IP 地址	
探测主机配置	监控网关时默认采用 Ping 方式,但也可探测远程主机的方式监控此线路的健康程度	
探测主机	支持监测多个主机	
监测时间间隔	监测时间的间隔	
监测容错次数	若监测失败,允许失败的最大次数,超出就认为此网关失效	

编辑路由监控对象

- 点“操作”一栏中的“编辑”图标,打开“路由监控对象”界面
- 执行修改操作
- 点击“确定”按钮完成修改

删除路由监控对象

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

智能路由

4.3.4 路由表信息

路由表信息页面可以查看当前系统中所有路由的具体信息，以及此时路由的状态。

序号	IP地址/掩码	优先级	不可达路由	黑洞路由	下一跳/权重值/状态	hash算法	路由状态
1	3.3.3.0/255.255.255.128	0	✘	✘	Ge0/0/3 / 1 /		UK
2	100.100.100.0/255.255.255.0	0	✘	✘	Ge0/0/1 / 1 /		UK
3	189.16.100.0/255.255.255.0	0	✘	✘	Ge0/0/0 / 1 /		UK
4	156.0.0.0/255.255.0.0	1	✘	✘	3.3.3.2 / 1 /		UGS
5	56.0.0.0/255.255.0.0	1	✘	✘	3.3.3.2 / 1 /		UGS

第1页/1页 跳转到 页 每页 行

图 4-37 路由表信息

表 4-11 路由表中状态字段说明

字段名	说明
G	Gateway
R	Reject
B	Blackhole
K	Kernel add
O	OSPF
S	Static route
P	BGP
I	RIP
E	Dead
F	Disabled

4.3.5 ISIS

Guard 提供 ISIS 功能，能够与其它支持 ISIS 功能的网络设备进行动态路由协商。在 ISIS 页面上，可以进行添加 ISIS 的配置。

名称	类型	Net配置	应用接口	操作
is1	level-1	49.0001.aaaa.bbbb.cccc.00	Ge0/0/3	

添加

第1页/1页 跳转到 页 Go 每页 10 行

图 4-38 添加 ISIS 页面

此界面可以完成以下功能：

- 添加 ISIS 配置
- 编辑 ISIS 配置
- 删除 ISIS 配置

点击添加按钮后进入 ISIS 配置页面，在配置页面中可以对名称、类型、Net、应用接口进行配置，在编辑时可以进行修改。

* 名称:	<input type="text" value="is1"/> (1-20 字母, 数字, 下划线组合)				
类型:	<input type="text" value="level-1"/>				
Net配置:	<input type="text"/> (用英文句号分隔 **.*.*.*.*.*.*.*.*.*.*注:第3、4、5段的配置 必须一样,且最多配置3个)				
Net列表:	<input type="text" value="49.0001.aaaa.bbbb.cccc.00"/> <input type="button" value="添加"/> <input type="button" value="删除"/> <input type="button" value="清空"/>				
应用接口:	<table border="0"> <tr> <td>可选应用接口列表</td> <td>应用接口列表(最多配置4个)</td> </tr> <tr> <td><input type="text" value="Ge0/0/0"/> <input type="text" value="Ge0/0/1"/> <input type="text" value="Ge0/0/3"/> <input type="text" value="Ge0/1/0"/> <input type="text" value="Ge0/1/1"/></td> <td><input type="text" value="Ge0/0/2"/></td> </tr> </table>	可选应用接口列表	应用接口列表(最多配置4个)	<input type="text" value="Ge0/0/0"/> <input type="text" value="Ge0/0/1"/> <input type="text" value="Ge0/0/3"/> <input type="text" value="Ge0/1/0"/> <input type="text" value="Ge0/1/1"/>	<input type="text" value="Ge0/0/2"/>
可选应用接口列表	应用接口列表(最多配置4个)				
<input type="text" value="Ge0/0/0"/> <input type="text" value="Ge0/0/1"/> <input type="text" value="Ge0/0/3"/> <input type="text" value="Ge0/1/0"/> <input type="text" value="Ge0/1/1"/>	<input type="text" value="Ge0/0/2"/>				
<input type="button" value="添加下一条"/> <input type="button" value="确定"/> <input type="button" value="取消"/>					

图 4-39 ISIS 路由配置

数据域说明

表 4-12 ISIS 路由配置数据域

域名	说明	和其他界面的关系
名称	ISIS 域名称	
类型	ISIS 分层类型	
Net 配置	ISIS 网络实体标记配置	

Net 列表	已添加的网络实体标记	
应用接口	选择 ISIS 应用到的网络接口	

点击“确定”按钮完成配置

4.4 DNS 设置

如果管理员设置了报警邮件等采用域名的服务，则需要配置 DNS 设置，用于 Guard 自身向外发送数据包时域名解析。

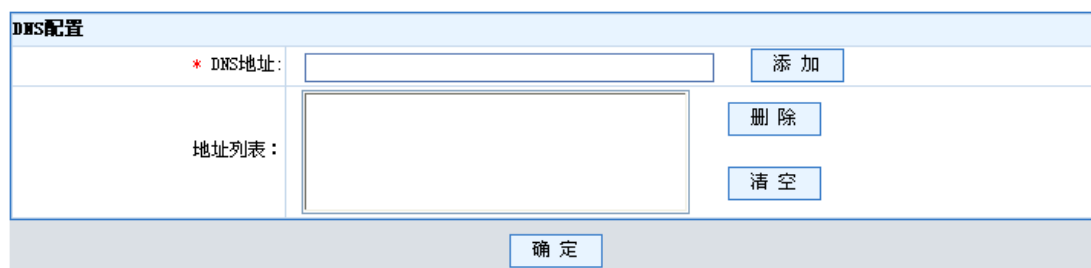


图 4-40 DNS 配置

此界面可以完成以下功能：

- 添加 DNS 地址
- 删除 DNS 地址
- 清空 DNS 地址

添加 DNS 地址

在 DNS 地址的文本框内输入一个 IP 地址，点“添加”按钮，采用此步骤可输入多个 DNS 地址，然后点击“确定”按钮完成 DNS 设置。

删除 DNS 地址

在地址列表里选中地址，点击右侧的“删除”按钮，采用此步骤删除所有需要删除的地址后，点击“确定”按钮完成 DNS 设置。

清空 DNS 地址

点击“清空”按钮，可清空地址列表内所有地址，再点击“确定”按钮完成 DNS 设置。

4.5 DHCP

4.5.1 服务器配置

启动DHCP

DHCP服务器

指定服务接口：	物理接口列表 Ge0/0/0 Ge0/0/1 Ge0/0/2 Ge0/0/3	>> <<	服务接口列表
ping包响应时间：	<input style="width: 100px;" type="text" value="1"/> 秒 (默认值为1秒, 范围为1-10)		

确定

图 4-41 DHCP 服务器配置

数据域说明：

表 4-13 DHCP 服务器配置数据域说明

域名	说明
物理接口列表	系统中所有物理接口列表
侦听接口列表	DHCP 服务器侦听的接口列表
Ping 包响应时间	DHCP 分配客户端地址前发送 Ping 检查后等待响应的时间间隔，范围为 1-10 秒，默认值为 1 秒

功能说明：

表 4-14 DHCP 服务器功能说明

域名	说明
>>	添加侦听接口
<<	删除侦听接口
确定	确认配置生效
启动DHCP	启动 DHCP 服务器

停止DHCP	停止 DHCP 服务器
--------	-------------

4.5.2 地址池配置

地址池名称	IP地址/掩码	地址范围	出口网关	DNS地址	操作
<input type="button" value="添加"/>					



 第1页/1页 跳转到 页 每页 行 

图 4-42 DHCP 地址池配置



数据域说明：

表 4-15 DHCP 地址池配置数据域说明

域名	说明
地址池名称	地址池名称，唯一标识一个地址池
IP 地址/掩码	地址池中可供分配的地址所在网络范围
地址范围	地址池中可供分配的地址范围
出口网关	从地址池获取地址的客户端默认的出口网关地址
DNS 地址	从地址池获取地址的客户端默认的 DNS 地址

功能说明：

表 4-16 DHCP 地址池功能说明

域名	说明
	编辑
	删除

添加新的地址池

- 点击“添加”按钮，弹出 DHCP 地址池配置的设置窗口。
- 输入完成后，点击“确定”按钮，或“添加下一条”按钮，添加下一个 DHCP 地址池。

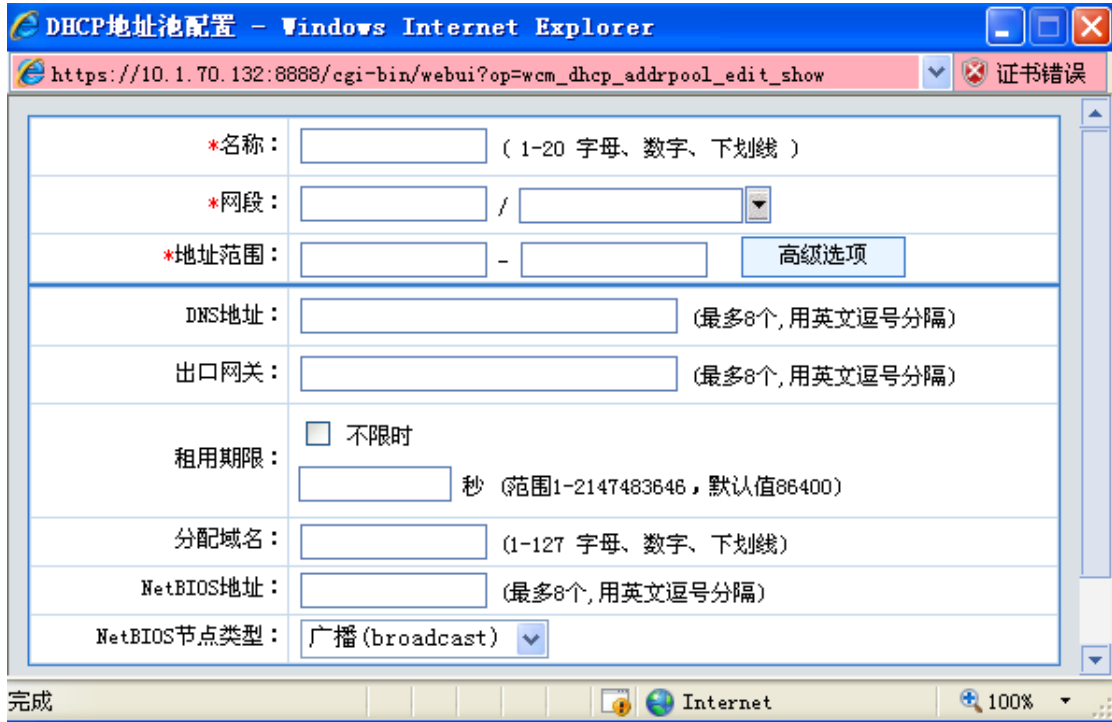


图 4-43 添加 DHCP 地址池

数据域说明

表 4-17 添加 DHCP 地址池配置数据域说明

域名	说明
名称	DHCP 地址池名称，唯一标识一个 DHCP 地址池
网段	DHCP 地址池可供分配地址所在的网络范围
地址范围	DHCP 地址池可供分配的地址范围
DNS 地址	从地址池获取地址的客户端默认的 DNS 地址
出口网关	从地址池获取地址的客户端默认的出口网关地址
租用期限	从地址池获取地址的租用期限，范围是 0-4294967295 秒，默认值为 86400 秒
分配域名	从地址池获取地址的客户端默认域名后缀，1-128 个字符（字母，数字，下划线）
NetBIOS 地址	NetBIOS 服务器地址
NetBIOS 节点类型	NetBIOS 节点配置的节点类型，可选类型有广播（broadcast）、端（peer-to-peer）、混合（mixed）、混合（hybrid）

高级选项配置

不参与自动分配IP：	<input type="text"/>	添加
	<input type="text"/>	删除
		清空
静态地址绑定：	ip <input type="text"/>	添加
	mac <input type="text"/>	
	<input type="text"/>	删除
		清空

图 4-44 DHCP 地址池高级配置

数据域说明

表 4-18 添加 DHCP 地址池高级配置数据域说明

域名	说明
不参与自动分配 IP	DHCP 地址池地址范围中不参与分配的地址
静态地址绑定	DHCP 地址池针对固定 MAC 地址分配的 IP 地址

功能说明：

表 4-19 DHCP 地址池高级配置功能说明

域名	说明
添加	添加（在对应的文本框中输入 IP/MAC 后，点击添加，当输入的内容添加到它下面的文本列表中方才生效）
删除	删除
清空	清空

编辑 DHCP 地址池

- 点击“编辑”按钮，弹出 DHCP 地址池配置的设置窗口。
- 编辑完成后，点击“确定”按钮，或“添加下一条”按钮，添加下一个 DHCP 地址池。

配置如添加 DHCP 地址池。

4.5.3 DHCP 中继

启动负载分担

物理接口	是否启用 DHCP 中继服务	操作
Ge0/0/0	✘	✎ 🔄
Ge0/0/1	✘	✎ 🔄
Ge0/0/2	✘	✎ 🔄
Ge0/0/3	✘	✎ 🔄

图 4-45 DHCP 中继

数据域说明：

表 4-20 DHCP 中继数据域说明

域名	说明
物理接口	系统中物理接口列表
是否启用 DHCP 中继服务	是否启用 DHCP 中继服务

功能说明：

表 4-21 DHCP 中继功能说明

域名	说明
✎	编辑
🗑️	删除
✔️	启用 DHCP 中继服务
✘	停止 DHCP 中继服务
启动负载分担	启用负载分担

编辑 DHCP 中继

- 点击“编辑”按钮，弹出 DHCP 中继配置的设置窗口。
- 编辑完成后，点击“确定”按钮。

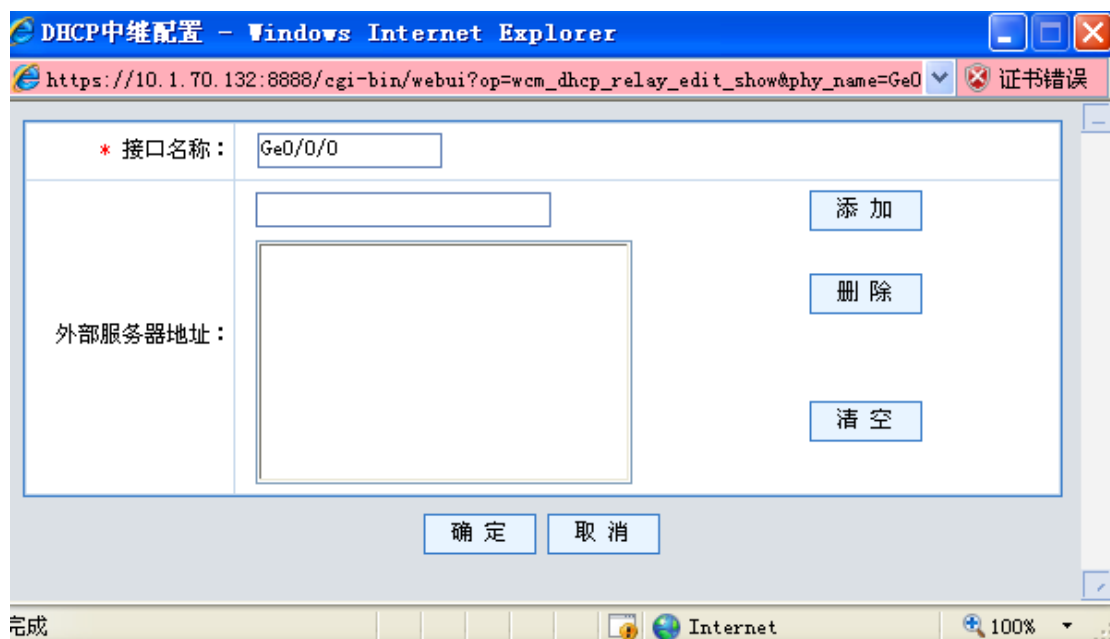


图 4-46 DHCP 中继配置

数据域说明:

表 4-22 DHCP 中继配置数据域说明

域名	说明
接口名称	系统中物理接口名称
外部服务器地址	外部 DHCP 服务器地址

功能说明:

表 4-23 DHCP 中继功能说明

域名	说明
添加	添加（在对应的文本框中输入 IP 地址后，点击添加，当输入的内容添加到它下面的文本列表中方才生效）
删除	删除
清空	清空

第5章 IPv6

本章主要介绍 IPv6 的配置，包括网络配置，资源对象配置，防火墙配置，抗攻击配置和入侵防护配置。

5.1 网络管理

IPv6 的网络管理包含地址配置，邻居配置，服务段前缀，自动配置和静态路由。

5.1.1 地址配置

接口地址页面用于配置和显示配置在接口上的 IPv6 地址。

IPv6 的地址显示页面如图：

序号	接口名称	地址/掩码	地址类型	操作
<input type="checkbox"/> 1	Ge0/0/0	Fe80::210:20Ee:Fe3a:5b03/64	自动配置	
<input type="checkbox"/> 2	Ge0/0/0	2000:2000:2000:2000:2000:2000:2000/16	静态	删除
<input type="checkbox"/> 3	Ge0/0/1	Fe80::210:20Ee:Fe3a:5b02/64	自动配置	
<input type="checkbox"/> 4	Ge0/0/2	Fe80::210:20Ee:Fe3a:5b01/64	自动配置	
<input type="checkbox"/> 5	Ge0/0/3	Fe80::210:20Ee:Fe3a:5b00/64	自动配置	

添加

全选 第1页/1页 跳转到 1 页 Go 每页 10 行 导出

图 5-1 地址的显示

地址有两种类型，其中静态地址是手工添加的，另外一种自动配置的。手工添加的地址可以删除。

IPv6 的地址添加页面如图：



接口地址维护 - Windows Internet Explorer

https://189.16.100.122:8888/cgi-bin/webui?op=wcm_ipv6_edit_show 证书错误

* 接口名称: Ge0/0/1

* 地址: 2000:2000:2000:2000:2000:2000:1000

* 掩码: 32

添加下一条 确定 取消

完成 Internet 100%

图 5-2 地址添加页面

地址添加页面需要选择添加地址的接口，填写 IPv6 格式的 IP 地址，掩码是一个 0-128 的数字。

5.1.2 邻居配置

邻居配置为接口的 IPv6 地址设置对应的 MAC 地址。

邻居配置的显示页面如图：

超时时间				
超时时间: <input type="text" value="30"/> 秒 (范围为: 0-65535)				
确定				
邻居设置				
接口名称	ip地址	mac地址	类型	操作
Ge0/0/1	2000:2000:2000:2000:2000:2000:1000	0010.203a.5b02	静态	
添加				

图 5-3 邻居配置的显示

在显示页面上可以配置超时时间，是一个 0-65535 的数字。

在显示页面上可以添加和删除配置好的邻居。

邻居配置的添加页面如图：

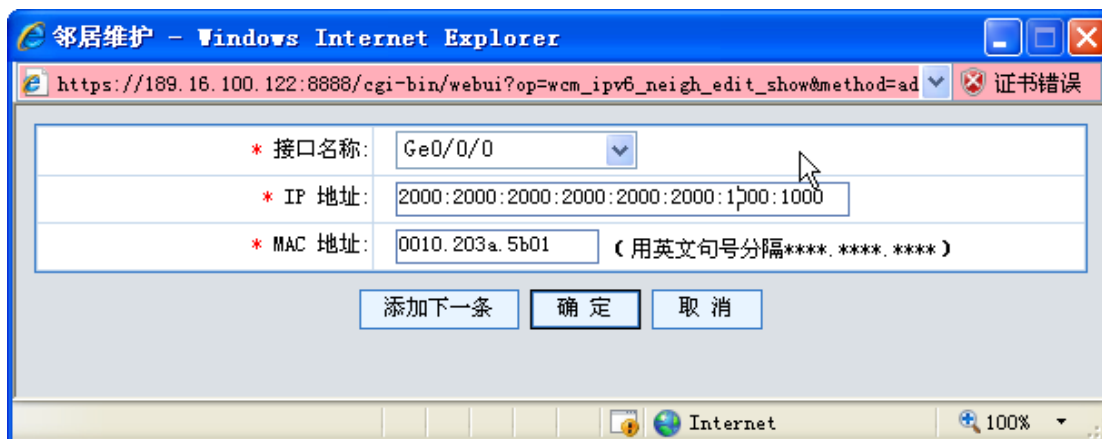


图 5-4 邻居配置的添加页面

在添加页面上，可以选择设备的接口，为其设置 IPv6 地址和对应的 MAC 地址。

5.1.3 服务段前缀

这个页面可以为接口配置 IPv6 地址的服务端前缀。

显示列表页面如图：

序号	接口名称	IP地址/掩码	操作
1	Ge0/0/0	2000:2000::/24	 

添加

图 5-5 服务端前缀的显示页面

在显示页面上，可以添加服务端前缀，也可以对配置好的前缀进行编辑和删除。

服务端前缀的添加页面：



在添加页面上，需要选择一个设备接口，为其设置一个 IPv6 格式的 ip 地址和掩码。

5.1.4 自动配置

自动配置的显示页面如图：






物理接口	自动配置
Ge0/0/0	
Ge0/0/1	
Ge0/0/2	
Ge0/0/3	

图 5-6 自动配置的显示

页面上列出了设备的物理接口的自动配置状态，点击图标 ，可以修改接口的自动配置状态。

5.1.5 静态路由

静态路由页面用来显示和添加 IPv6 格式的设备路由。

路由显示页面：

IP地址/掩码	下一跳接口	metric	类型	操作
fe80::/64	Ge0/0/0	256	自动	
fe80::/64	Ge0/0/1	256	自动	
fe80::/64	Ge0/0/2	256	自动	
fe80::/64	Ge0/0/3	256	自动	
2000::/16	Ge0/0/3	1024	静态	
2000::/16	Ge0/0/0	256	自动	
fe00::/8	Ge0/0/0	256	自动	
fe00::/8	Ge0/0/1	256	自动	
fe00::/8	Ge0/0/2	256	自动	
fe00::/8	Ge0/0/3	256	自动	

添加

第1页/1页 跳转到 1 页 每页 10 行

图 5-7 静态路由显示

IPv6 静态路由有两种类型，静态和自动的，静态的是用户手工配置的，自动的是系统自动获得的。静态和手工配置的路由都可以删除。

路由添加页面如图：

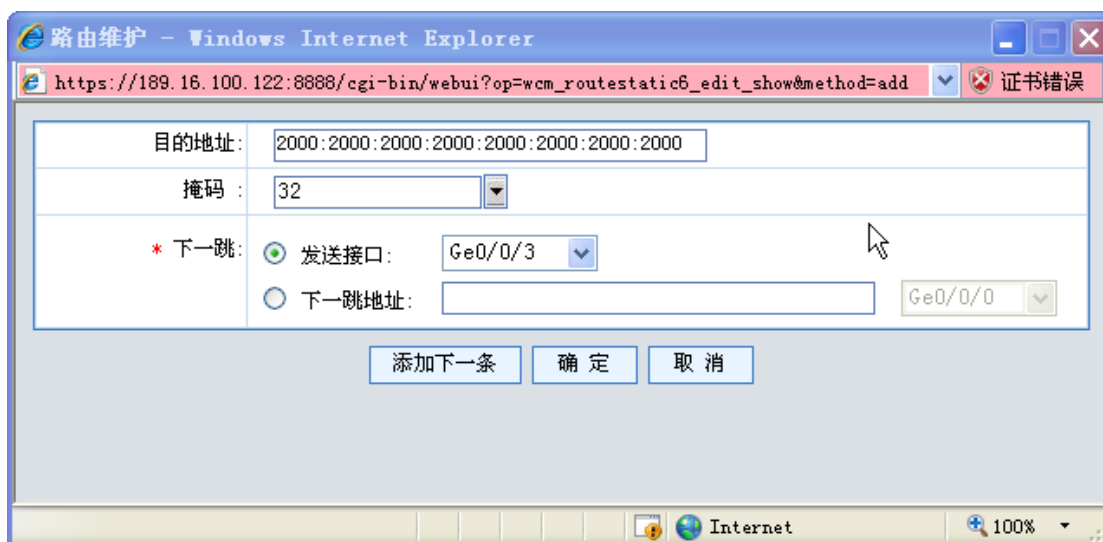


图 5-8 路由添加页面

添加页面需要添加 IPv6 格式的目的地址和掩码，下一跳有两种方式，接口方式和地址接口方式，地址接口方式的地址也是 IPv6 格式的。

5.2 资源定义

5.2.1 地址

5.2.1.1 地址列表

地址列表页面用于添加，显示，查询和删除地址对象功能，可以选择多个地址对象，进行批量删除。

序号	名称	地址	备注	操作
<input type="checkbox"/> 1	a1	2000:2000:2000:2000:2000:2000/2		
<input type="checkbox"/> 2	a2	2000:2000:2000:2000:2000:2000:1000/32		

全选

第1页/1页 跳转到: 1 页 Go 每页 10 行

图 5-9 地址列表

地址对象的添加页面如图:



图 5-10 地址添加页面

添加页面数据域说明:

表 5-1 IP 地址添加主要参数说明

域名	说明
名称	地址对象的名称
地址	可以是 IP 和掩码的方式，也可以是地址段的方式
备注	少于 255 个字符

5. 2. 1. 2 地址组

地址组页面用于对地址组对象进行添加，编辑，查询和删除功能，还可以选择多个地址组对象，进行批量删除。

序号	名称	策略域	成员列表	备注	操作
<input type="checkbox"/> 1	aq1		a1 a2		

全选

第1页/1页 跳转到: 1 页 Go 每页 10 行

图 5-11 地址组对象列表页面

地址组对象添加页面如图所示:



图 5-12 地址组添加页面

地址组页面中左侧的地址列表是已经添加好的地址对象的列表，右侧的地址组成员是需要添加到当前地址组的地址对象名称。

5.2.2 服务

5.2.2.1 服务对象定义

服务对象定义了一些常用的服务，不可以修改，删除，只可以被引用。

序号	名称	策略域	协议	端口	服务简介
1	dns	本地域	17	53	
2	gre	本地域	47	0	
3	http	本地域	6	80	www service
4	https	本地域	6	443	
5	icmp_any	本地域	1	0	icmp service
6	igmp	本地域	2	0	
7	igrp	本地域	88	0	
8	oicq	本地域	17	8000	
9	ospf	本地域	89	0	
10	pop3	本地域	6	110	

图 5-13 预定义服务列表

服务列表显示当前的 ICMP 服务。

序号	服务名	策略域	协议	备注	操作
					添加

第1页/1页 跳转到 1 页 Go 每页 10 行

图 5-14 ICMP 服务列表

添加窗口为：



图 5-15 ICMP 服务添加

表 5-2 ICMP 服务添加元素表

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

5. 2. 2. 2 基本服务

列表中显示了当前已定义的所有基本服务。

序号	服务名	策略域	协议	备注	操作
					添加

全选 第1页/1页 跳转到 1 页 Go 每页 10 行

图 5-16 基本服务列表

点击“添加”，将弹出以下界面：



图 5-17 基本服务添加

表 5-3 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 1 到 65535 源端口通常设为 1-65535，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 1 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 1-65535，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 1-65535。
--	-------------------------------------------------------------------------------------------------

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. 2. 2. 3 服务组



图 5-18 服务组列表

服务组用于“防火墙”下的：包分类、DNAT 策略、安全策略。

服务组的成员可以是“资源定义->服务”中已经定义过的服务对象、ICMP 服务和基本服务。

在“资源定义->服务->服务组”，点击“添加”，将弹出以下界面：







图 5-19 服务组添加

表 5-4 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”中定义的所有服务，包括“服务对象定义”“ICMP 服务”“基本服务”。 本列表的成员被移动到服务组成员列表中之后，将不再显示于本列表中。
服务组成员	列出本组的所有成员。

表 5-5 服务组添加、删除成员列表

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. 2. 2. 4 ALG 定义

由于某些应用协议需要创建动态连接，而创建连接所用的 ip 地址和端口是动态的，为了监视该类协议，这里引入了 ALG (application layer gateway) 即应用层网关。目前支持 ftp, tftp, h.323, h.323gk, mms, rtsp, pptp, rtsp, xdmcp, sip 共 10 种协议。

序号	服务名	端口	是否启用	操作
1	ftp	21	✓	 
2	h323	1720	✓	 
3	h323gk	1719	✓	 
4	mms	1755	✓	 
5	pptp	1723	✓	 
6	rtsp	554	✓	 
7	sip	5060	✓	 
8	tftp	69	✓	 
9	tns	1521	✓	 
10	xdmcp	177	✓	 

图 5-20 ALG 定义列表

对 ALG 定义列表可选的操作有启用/关闭、编辑和恢复默认设置三项。
选中点击“编辑”，将执行编辑操作，并弹出以下界面：



图 5-21 ALG 配置

表 5-6 ALG 添加元素表

值域	说明
端口	协议使用的端口 可输入范围是 1-65535，最多允许设置 8 个，且端口值不可重复
是否可重定向	是否开启 ftp 协议的端口重定向功能 在方框内选中即为开启，反之则关闭

注意：

设置多个端口时，必须用英文逗号分隔，且端口值不可重复。

选中点击“恢复”，将执行恢复默认设置操作，当前配置将被默认配置覆盖。默认情况下，ftp 协议的端口值为 21，可重定向功能开启。

5.2.3 时间

5.2.3.1 时间列表

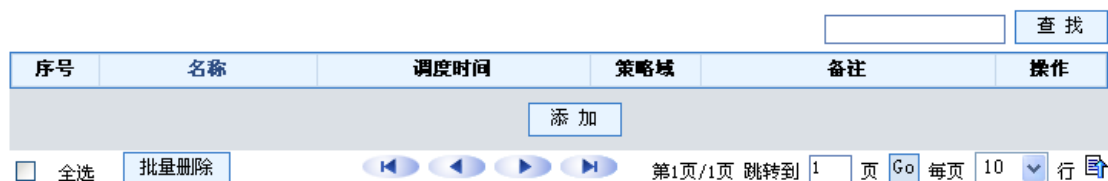


图 5-22 时间列表

可以按照一次性调度和周循环调度两种方式，来定义时间。点击“添加”，如下图所示：

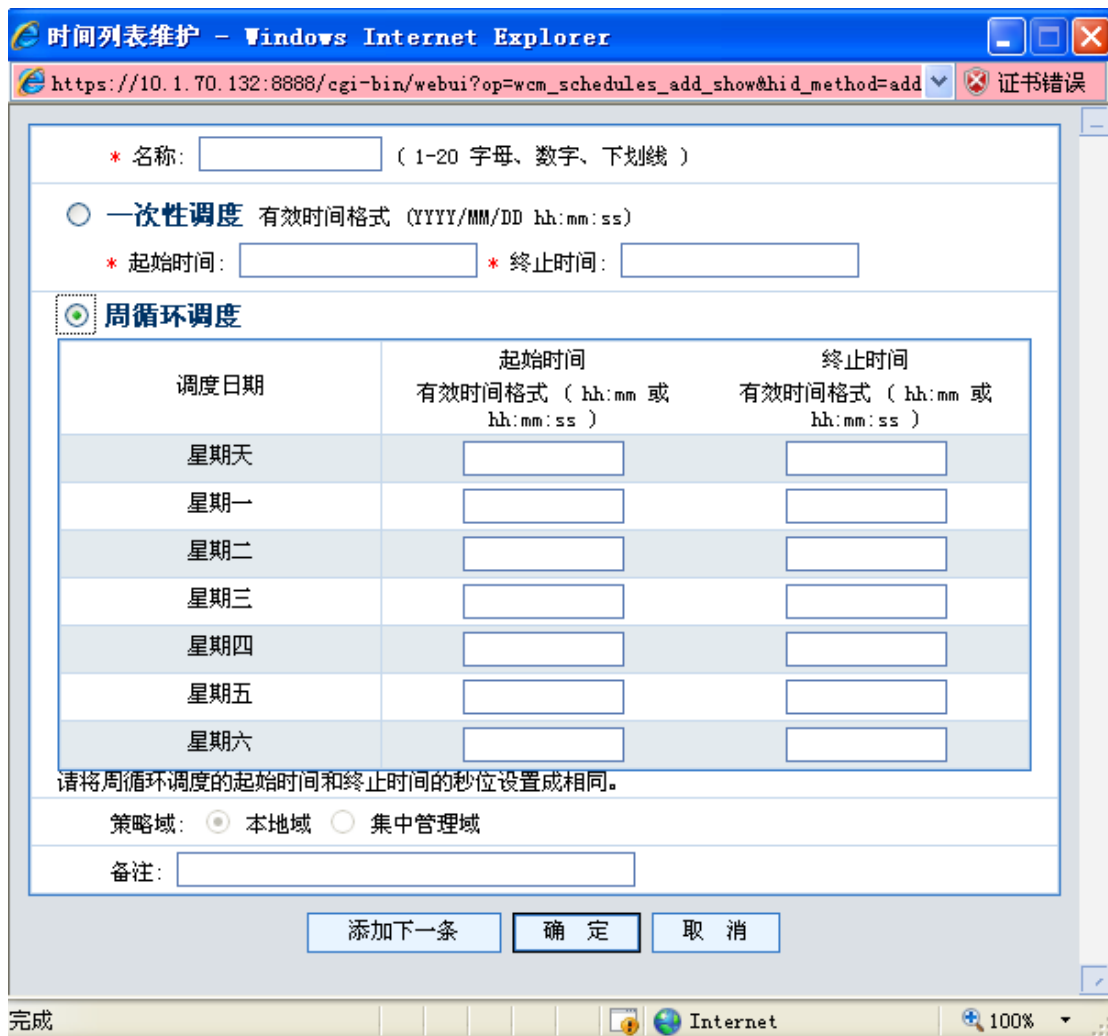


图 5-23 时间资源维护

表 5-7 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“Guard”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。则可以定义一个时间段 worktime 表示工作时间，再在“Guard>>包分类”中定义一个包分类，源地址和目的地址均设为“any”，服务对象选择“HTTP”，时间调度引用 worktime，在安全策略中添加一条规则，引用这个包分类并设置 Guard 策略为阻止即可。

5. 2. 3. 2 时间组



图 5-24 时间组列表







图 5-25 时间组维护

表 5-8 时间组维护添加元素表

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	该时间组的所有成员。

表 5-9 时间组维护添加、删除成员

操作	说明
	添加成员，点击  把选中的时间移动到成员列表 时间列表成员添加至时间组之后，该成员不再显示于时间列表中。
	删除成员，点击  把选中的成员移动到时间列表中

5.2.4 包分类

包分类显示页面：

可以根据序号排名显示，显示包括几个缩略参数，源地址、目的地址、服务和协议等。
可以分屏显示，支持翻页功能等。

界面如下图所示：

按条件查询

序号	分类名	源地址	目的地址	服 务	协 议	内网地址	外网地址	生效时间状态	操作
<input type="checkbox"/>	1 ipqos	192.0.0.0/255.0.0.0						未配置	  
<input type="checkbox"/>	2 df	1.2.3.3/	5.6.6.6/	gre				未配置	  
<input type="checkbox"/>	3 snat	100.100.100.0/255.255.255.0						未配置	  

全选     第1页/1页 跳转到 页 每页 行 

图 5-26 包分类显示

包分类添加页面：

根据包分类支持的几个元素定义分类规则。

具体参数如下图所示：



图 5-27 包分类显示

包分类添加页面还有一个高级选项，可以定义一些不常用的参数配置。
点开后面界面如下图所示：

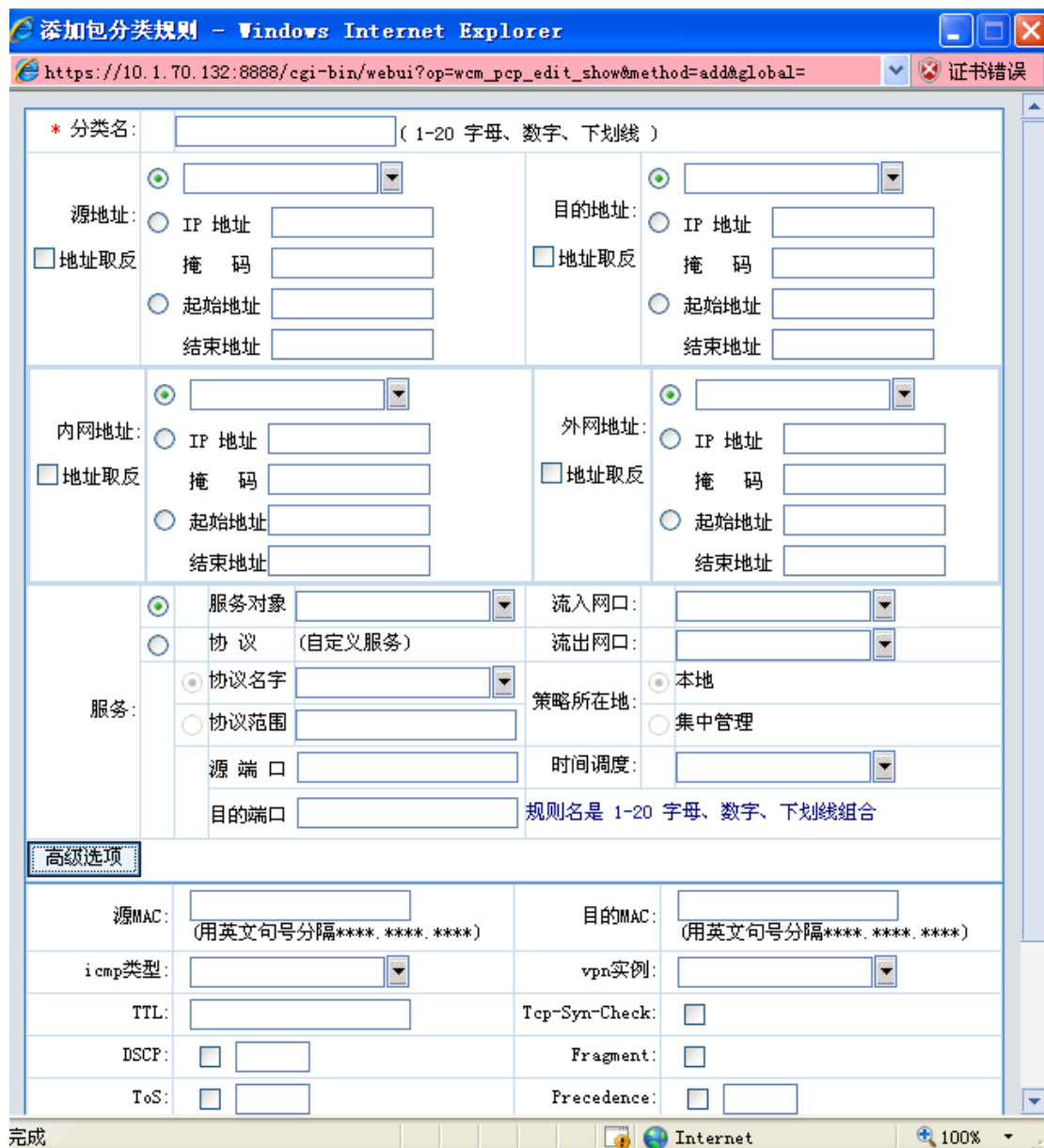


图 5-28 带有高级选项的包分类添加

包分类页面还有修改、排序、删除功能。

包分类修改页面：



图 5-29 包分类修改

删除页面：

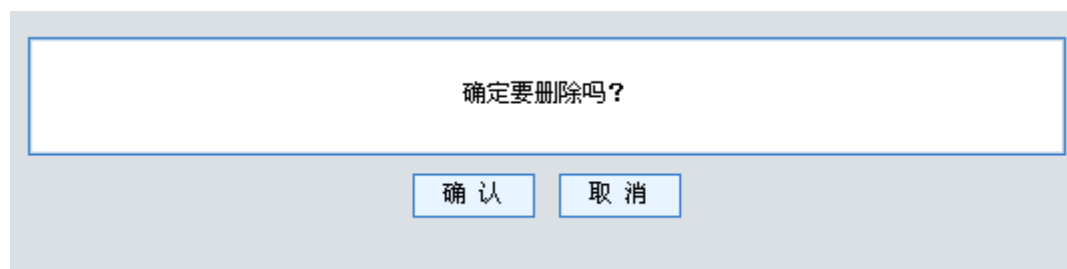


图 5-30 包分类删除

5.3 防火墙

5.3.1 包过滤

包过滤显示页面：

可以根据序号排名显示，显示包括几个缩略参数，源地址、目的地址、服务和动作等。

可以分屏显示，支持翻页功能等。

界面如下图所示：



图 5-31 包过滤

包过滤添加页面：

根据包过滤支持的几个元素定义分类规则。

具体参数如下图所示：

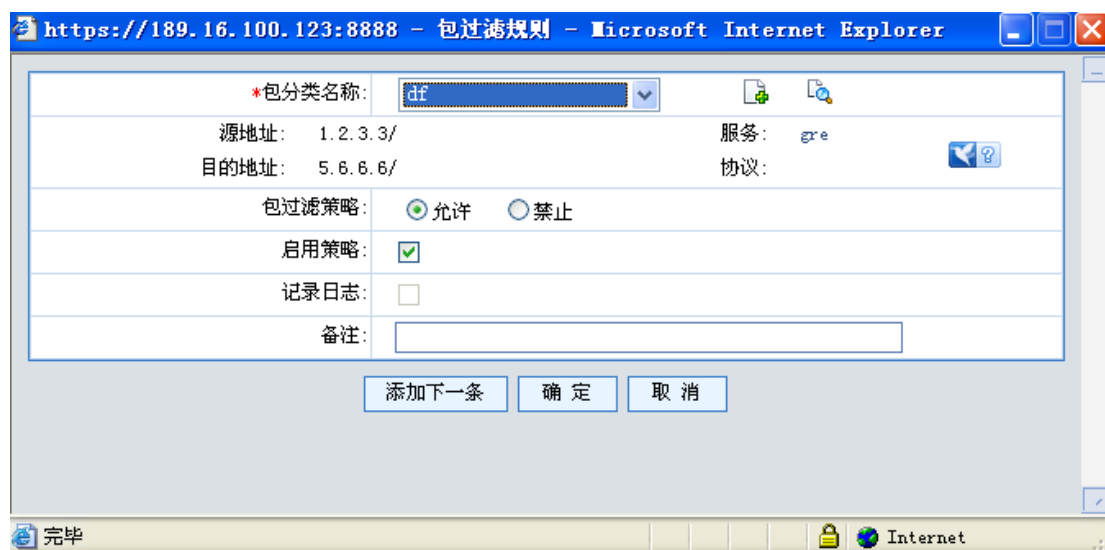


图 5-32 包过滤添加页面

5.3.2 默认过滤策略

设置没有被包过滤规则匹配时的默认策略。

界面如下图所示：

安全业务参数	
包过滤缺省策略:	<input checked="" type="radio"/> 接受 <input type="radio"/> 拒绝
<input type="button" value="确定"/>	

图 5-33 默认过滤策略配置

5.4 流量牵引

5.4.1 BGP 牵引

5.4.1.1 BGP 本地配置

BGP本地配置	BGP邻居配置	访问控制列表	路由映射	路由牵引配置	接口转发								
<table border="1"> <thead> <tr> <th colspan="2">BGP本地参数</th> </tr> </thead> <tbody> <tr> <td>* 本地AS号:</td> <td> <input type="text" value="2"/> (1-65535) </td> </tr> <tr> <td>本地路由标识:</td> <td> <input type="text"/> 单个IP地址 </td> </tr> <tr> <td colspan="2" style="text-align: center;"> <input type="button" value="确定"/> </td> </tr> </tbody> </table>						BGP本地参数		* 本地AS号:	<input type="text" value="2"/> (1-65535)	本地路由标识:	<input type="text"/> 单个IP地址	<input type="button" value="确定"/>	
BGP本地参数													
* 本地AS号:	<input type="text" value="2"/> (1-65535)												
本地路由标识:	<input type="text"/> 单个IP地址												
<input type="button" value="确定"/>													

图 5-34 BGP 参数配置

数据域说明:

表 5-10 BGP 参数配置数据域说明

域名	说明
本地 AS 号	本地自治系统(Autonomous System) 编号, 范围为 1-65535
本地路由标识	本地的路由 ip 标识

功能说明:

表 5-11 BGP 参数配置功能说明

域名	说明
<input type="button" value="确定"/>	确认配置生效

此界面可以完成以下功能:

- 配置本地 AS 号
- 设置本地路由标识

5. 4. 1. 2 BGP 邻居配置

网络配置>>路由牵引>>BGP邻居配置



图 5-35 BGP 邻居配置页面

数据域说明:

表 5-12 BGP 邻居配置数据域

域名	说明
邻居 IP 地址	邻居 IP 地址
邻居 AS 号	邻居 AS 号
下一跳次数	下一跳的跳跃次数
通信接口	通信接口的 ip 地址
映射名称	可以选择在路由映射页面配置的映射名称

此界面可以完成以下功能:

- 添加 BGP 邻居
- 编辑 BGP 邻居
- 删除 BGP 邻居

添加 BGP 邻居

- 点“添加”按钮，进入“BGP 邻居维护”
- 添加 BGP 邻居参数
- 点“确定”按钮完成添加



* 邻居IP地址:	<input type="text"/>
* 邻居AS号:	<input type="text"/> (1-65535)
下一跳次数:	<input type="text"/> (1-255)
BGP会话协商接口地址:	<input type="text"/>
禁止路由同步地址:	<input type="text"/>
路由映射:	<input type="text"/> ▼
下发方向:	out ▼
传递社团属性:	<input checked="" type="checkbox"/>

添加下一条 确定 取消

图 5-36 BGP 邻居配置添加页面

编辑 BGP 邻居



* 邻居IP地址:	<input type="text" value="7.7.7.1"/>
* 邻居AS号:	<input type="text" value="1"/> (1-65535)
下一跳次数:	<input type="text" value="200"/> (1-255)
BGP会话协商接口地址:	<input type="text" value="6.6.6.1"/>
禁止路由同步地址:	<input type="text"/>
路由映射:	qq ▼
下发方向:	out ▼
传递社团属性:	<input checked="" type="checkbox"/>

添加下一条 确定 取消

图 5-37 BGP 邻居配置编辑页面

删除 BGP 邻居:

- 点“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

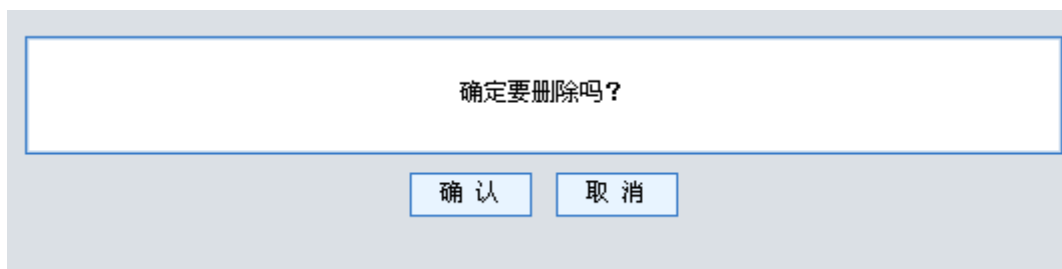


图 5-38 BGP 邻居删除页面

5.4.1.3 访问控制链表

网络配置>>路由牵引>>访问控制链表

链表名称	IP地址/掩码位数	类型	操作
aa	2.2.2.2/24	permit	
	2.4.2.2/32	permit	

第1页/1页 跳转到 页 每页 10 行

图 5-39 访问控制链表显示页面

数据域说明

表 5-13 访问控制链表数据域说明

域名	说明
链表名称	访问控制链表名称
IP 地址/掩码位数 类型	访问控制链表的参数。

此界面可以完成以下功能:

- 添加访问控制链表
- 编辑访问控制链表
- 删除访问控制链表

添加访问控制链表

- 点“添加”按钮，进入“访问链表维护”
- 添加访问链表参数
- 点“确定”按钮完成添加



图 5-40 访问控制链表添加页面

编辑访问链表



图 5-41 访问控制链表添加页面

删除访问链表:

- 点“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

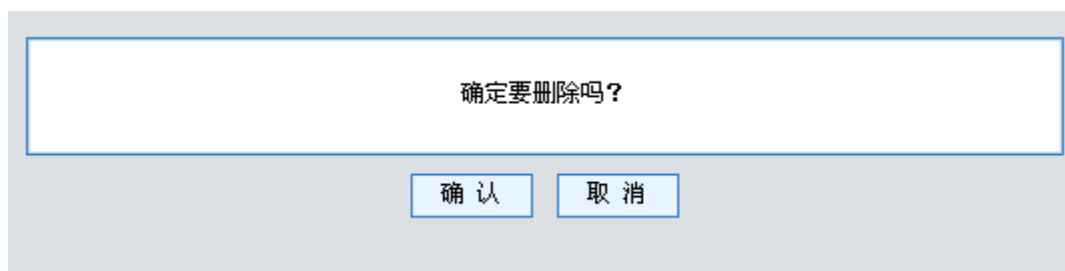


图 5-42 访问控制链表删除页面

5. 4. 1. 4 路由映射

网络配置>>路由牵引>>路由映射



图 5-43 路由映射显示页面

数据域说明：

表 5-14 路由映射数据域说明

域名	说明
映射名称	路由映射的名称
访问控制名称 目的地址 类型 编号 社团属性	路由映射的具体参数，访问控制名称就是在访问控制链表页面所创建的链表名称。

此界面可以完成以下功能：

- 添加路由映射
- 编辑路由映射
- 删除路由映射

添加路由映射

- 点“添加”按钮，进入“路由映射维护”
- 添加路由映射参数
- 点“确定”按钮完成添加



图 5-44 路由映射添加页面

编辑路由映射



图 5-45 路由映射编辑页面

删除路由映射：

- 点“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

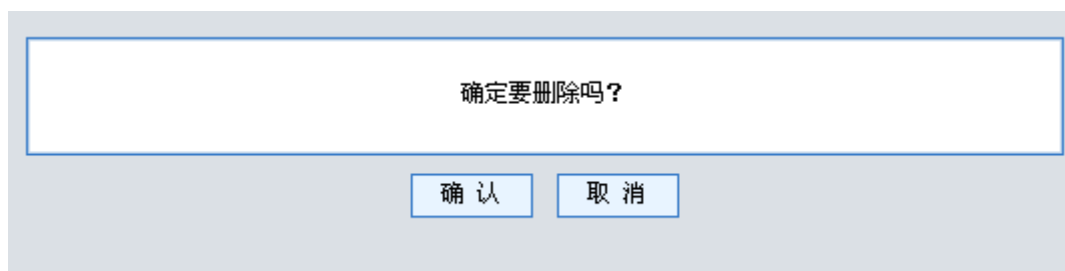


图 5-46 路由映射删除页面

5. 4. 1. 5 路由牵引配置



图 5-47 路由牵引配置页面

数据域说明：

表 5-15 BGP 参数配置数据域说明

域名	说明
IP 地址	需要牵引的 IP 地址
掩码	需要牵引的掩码
静态路由	牵引完数据默认回注的静态路由

此界面可以完成以下功能：

- 添加路由牵引
- 编辑路由牵引
- 删除路由牵引

添加路由牵引

- 点“添加”按钮，进入“路由牵引配置”
- 添加路由牵引参数
- 点“确定”按钮完成添加

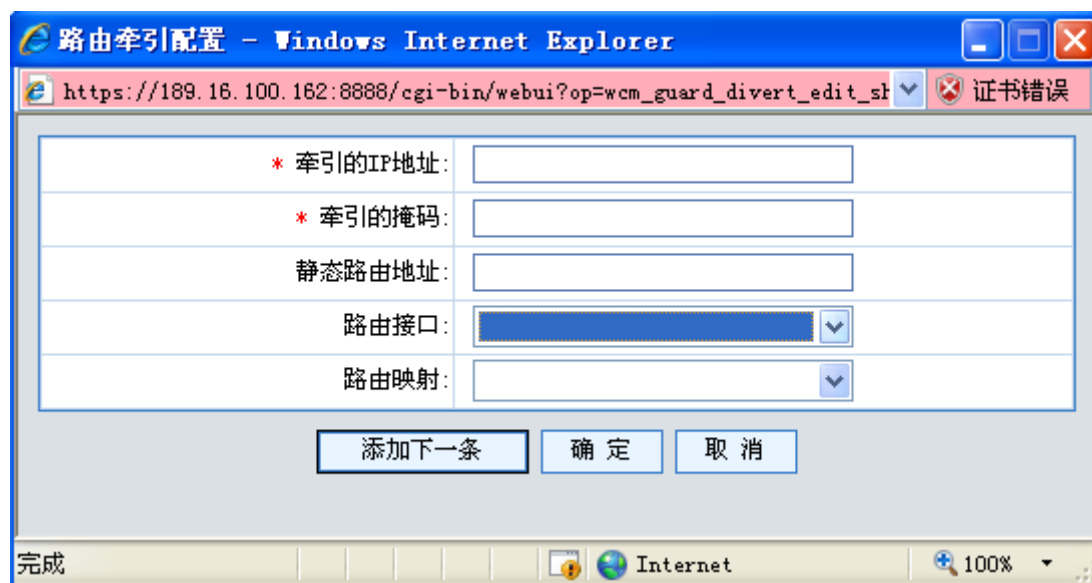


图 5-48 路由牵引配置添加页面

编辑路由牵引

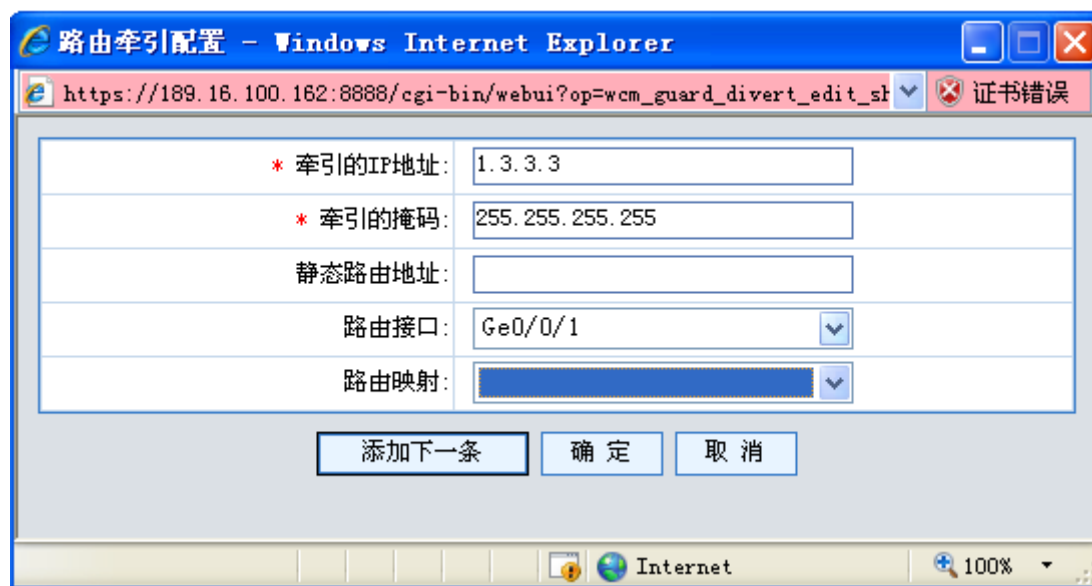


图 5-49 路由牵引配置编辑页面

删除路由牵引:

- 点“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

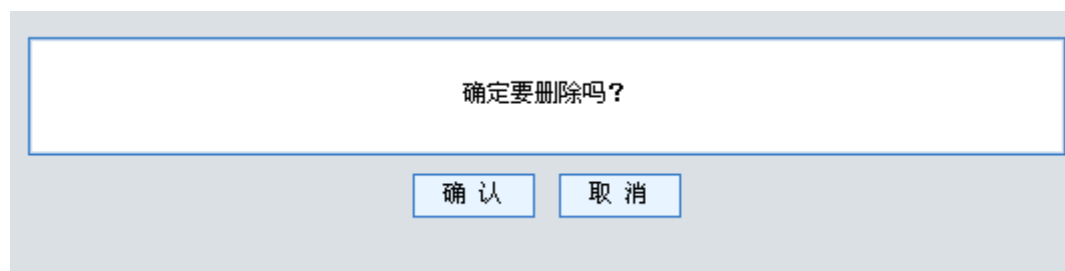


图 5-50 路由牵引配置删除页面

5. 4. 1. 6 接口转发

接口转发功能开关	<input type="checkbox"/>		
<input type="button" value="确定"/>			
入接口名称	出接口名称	网关IP地址	操作
<input type="button" value="添加"/>			

图 5-51 接口转发配置

数据域说明

表 5-16 接口转发数据域说明

域名	说明
接口转发功能开关	可以开启或关闭接口转发功能
入接口名称	入接口的名称
出接口名称	出接口的名称
网关 IP 地址	设置的网关 IP

此界面可以完成以下功能：

- 添加接口转发
- 编辑接口转发
- 删除接口转发
- 添加接口转发
- 点“添加”按钮，进入“接口转发参数配置”
- 添加接口转发参数
- 点“确定”按钮完成添加



图 5-52 接口转发添加页面

编辑接口转发功能



图 5-53 接口转发编辑页面

删除接口转发:

- 点“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

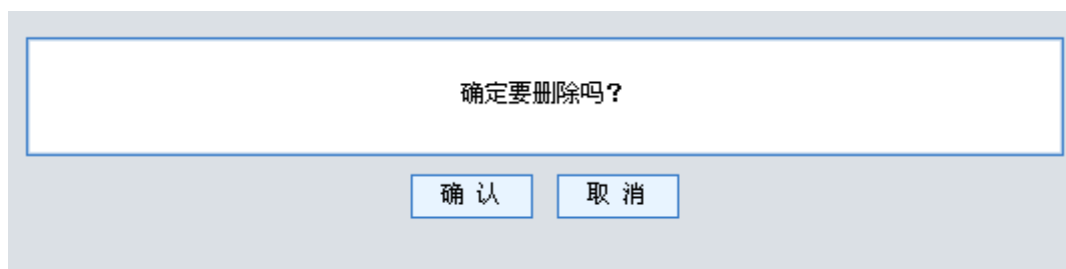


图 5-54 接口转发删除页面

5.4.2 OSPF

Guard 提供 OSPF 功能，能够与其它支持 OSPF 功能的网络设备进行动态路由协商。

在 OSPF 页面上，可以配置路由重分发，启动、停止 OSPF 功能，设置路由器 ID，添加、删除区域，设置区域认证方式，添加、删除网络，添加、删除网络接口认证口令。



图 5-55 OSPF 配置页面

5.4.2.1 配置路由重分发

打开 OSPF 界面时，将显示已经重分发的路由（bgp、直连、静态、rip）。如需修改，将对应的选项框选中或取消，然后点击确定即可生效。

5.4.2.2 修改路由器 ID

修改路由器 ID 后，需要点击“启动/停止”按钮以使其生效。

5.4.2.3 设置区域

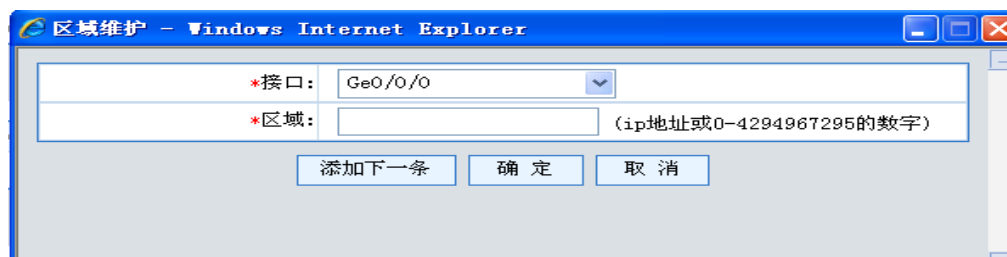


图 5-56 OSPF 添加区域对话框

添加区域时，需要指定区域名（可使用十进制形式或 IP 地址形式）和认证方式，认证方式可选择不认证、明文口令认证、消息摘要认证。最多可以添加 255 个区域。

添加区域后，可以修改其认证方式。

可以删除区域，添加了网络的区域不能被删除。

5.5 流量分析

流量自学习功能是对网络中的正常流量进行统计、分析和计算。一般使用时，可以在上线之初，选择学习模板，打开自学习功能，运行一段时间（最多学习 7 天）后帮助管理员做高级抗攻击的配置。

因此，自学习功能包括了：

- 选择学习模板；
- 输出学习结果；
- 记录学习过程数据；
- 应用/撤销学习结果到高级型抗攻击；

5.5.1 自学习配置

5.5.1.1 学习配置

用于查看自学习当前配置情况



包分类规则	自学习时间	学习模板			状态	操作
		ICMP	TCP	UDP		
aa	0天 1 小时					

图 5-57 自学习配置

图标说明：

表 5-17 流量自学习图标说明

域名	说明
	停止当前正在学习的自学习策略
	重新开始自学习策略
	编辑自学习策略
	删除自学习策略

数据域说明：

表 5-18 流量自学习数据域说明

域名	说明
包分类规则	包分类规则名称，符合命名规则

流量自学习时间	在添加页面设置的自学习时间
学习模板	在添加页面设置的自学习模板

添加流量自学习配置

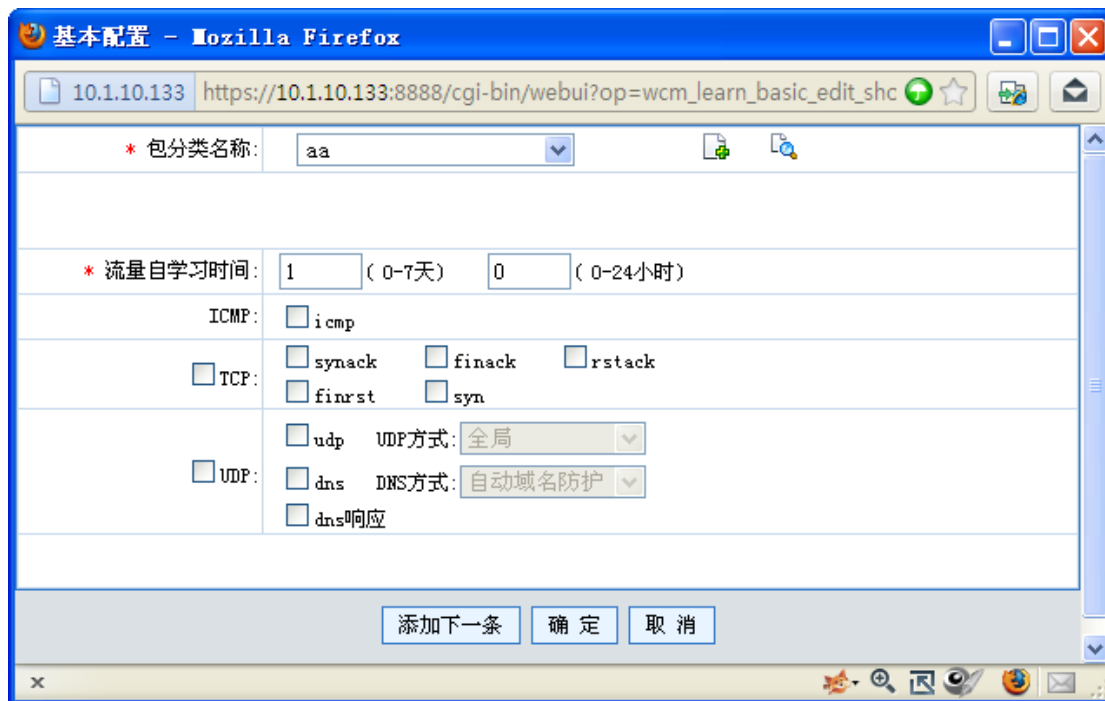


图 5-58 添加流量自学习配置

表 5-19 流量自学习添加项说明

域名	说明
包分类规则名称	选择一个已有的包分类规则, 选择后可以在下面看到相关配置。
流量自学习时间	设置学习时间
学习模板	选择需要学习的模板

5. 5. 1. 2 学习过程

包分类名称	ICMP	TCP	UDP	操作
aa	icmp	synack	udp源	生成快照
		finack	udp全局	
		rstack	dns响应	
		finrst	dns全局	
		syn	自动域名防护	

图 5-59 学习过程

5.5.2 自学习管理

自学习管理主要用于查看学习结果、中间快照和历史学习结果；查看学习过程中个模板的流量曲线图；查看当前应用情况和历史应用情况。支持的学习结果的应用和撤销。

5.5.2.1 学习结果

学习结束后生成学习结果。

包分类名称	ICMP		TCP		UDP		操作	查看历史学习结果与快照	与历史学习结果比较
	icmp	0	synack	0	udp源	0			
aa			finack	0	udp全局	--	应用	查看	比较
			rstack	0	dns响应	0			
			finrst	0	dns全局	0			
			syn	0	自动域名防护	--			

显示“--”表示未配置学习模板；显示“0”表示数据不足，无法学习；阈值显示为红色时，表示学习结果超过对应抗攻击上限值。

第1页/1页 跳转到 1 页 Go 每页 10 行

图 5-60 学习结果

点击应用时出现下面对话框：

确定应用此结果（其中0值应用为默认值，显示红色的应用为最大上限值）？

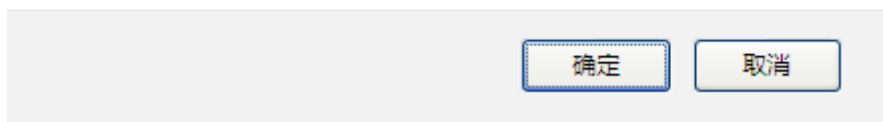


图 5-61 应用学习结果

点击查看，可查看历史学习记录和学习过程中的快照信息：

历史学习记录									
结果名称	ICMP		TCP		UDP		操作		
20111101160907	icmp	0	synack	0	udp源	--	应用		
			finack	0	udp全局	0			
			rstack	0	dns响应	0			
			finrst	0	dns全局	--			
			syn	0	自动域名防护	0			

显示“--”表示未配置学习模板；显示“0”表示数据不足，无法学习；阈值显示为红色时，表示学习结果超过对应抗攻击上限值。

中间快照									
结果名称	ICMP		TCP		UDP		操作		
显示“--”表示未配置学习模板；显示“0”表示数据不足，无法学习；阈值显示为红色时，表示学习结果超过对应抗攻击上限值。									
第1页/1页 跳转到 1 页 Go 每页 10 行									

图 5-62 历史学习结果和中间快照

点击比较时，如果有历史学习结果，可显示历史学习结果与当前学习结果的比较

5.5.2.2 学习曲线

可查看学习过程中的曲线图。

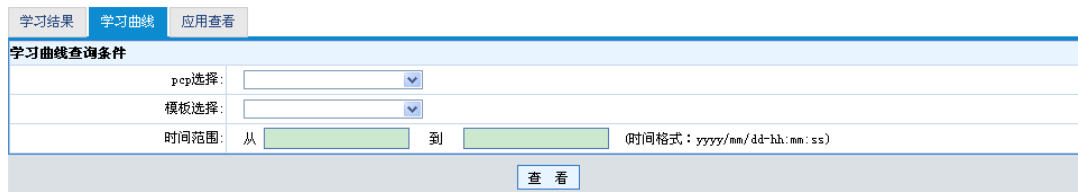


图 5-63 学习曲线

5.5.2.3 应用查看

可查看当前应用和历史应用情况

[查看当前应用](#) | [查看历史应用](#)

包分类名称	ICMP		TCP		UDP		操作
	icmp	0	synack	0	udp源	0	
sa			finack	0	udp全局	--	撤销
			rstack	0	dns响应	0	
			finrst	0	dns全局	0	
			syn	0	自动域名防护	--	

显示“--”表示未配置学习模板；显示“0”表示数据不足，无法学习；阈值显示为红色时，表示学习结果超过对应抗攻击上限值。

第1页/1页 跳转到 1 页 Go 每页 10 行

图 5-64 应用查看

5.6 流量清洗

5.6.1 攻击处理方式

攻击处理方式页面可以对攻击事件处理设置，对攻击事件有两种处理方式。

1. 检测到攻击系统只产生报警
2. 检测到攻击系统产生报警并丢弃报文

攻击处理方式页面设置如下：

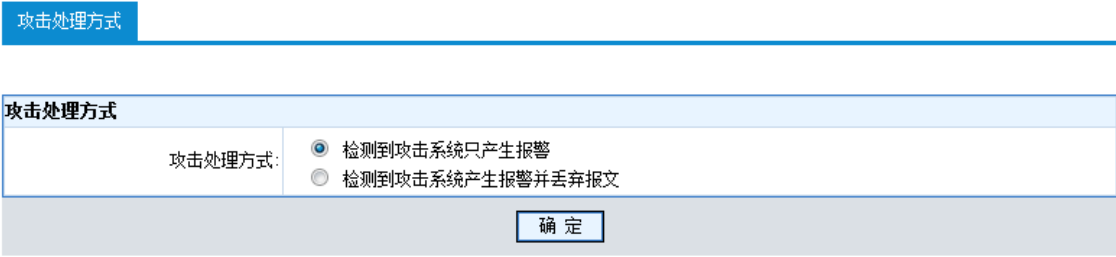


图 5-65 攻击处理方式配置

5.6.2 日志采样

日志采样页面可以对攻击日志采样率进行设置，范围为 1-65535，默认为 50。

日志采样页面设置如下：

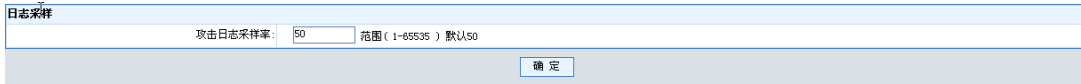


图 5-66 抗攻击日志采样配置

5.6.3 DNS 防护

5.6.3.1 域名黑名单

管理员可以通过域名黑名单对网络的域名访问进行控制，把某个域名加入黑名单来阻止对这个域名的访问。

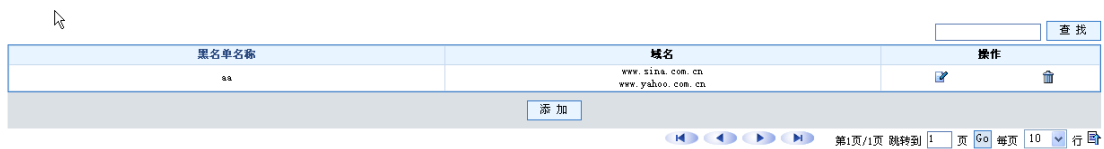


图 5-67 域名黑名单配置

数据域说明

表 5-20 域名黑名单数据域说明

域名	说明
黑名单名称	域名黑名单名称。
域名	加入黑名单的域名。

此界面可以完成以下功能：

- 添加域名黑名单

- 编辑域名黑名单
- 删除域名黑名单
- 添加域名黑名单
- 点“添加”按钮，进入“域名黑名单维护”
- 添加黑名单参数
- 点“确定”按钮完成添加



图 5-68 域名黑名单添加

编辑页面:



图 5-69 域名黑名单编辑

删除页面:

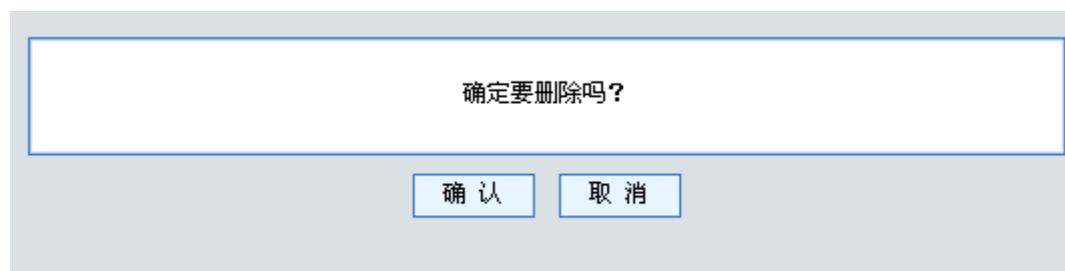
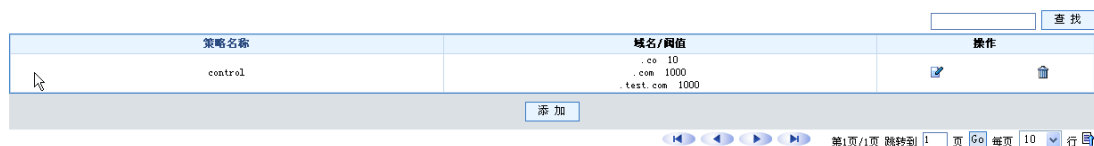


图 5-70 域名黑名单删除

5.6.3.2 域名访问限制

管理员可以通过域名访问限制对网络的域名访问进行控制,为某个域名设置相应的阈值超过这个阈值后的域名不允许访问。





策略名称	域名/阈值	操作
control	.co 10 .com 1000 .test.com 1000	 

图 5-71 域名访问控制配置

数据域说明

表 5-21 域名访问限制数据域说明

域名	说明
策略名称	域名访问限制策略名称。
域名/阈值	添加域名及其相应阈值

此界面可以完成以下功能:

- 添加域名访问限制
- 编辑域名访问限制
- 删除域名访问限制
- 添加域名访问限制
- 点“添加”按钮,进入“域名访问限制维护”
- 添加参数
- 点“确定”按钮完成添加



图 5-72 域名访问控制添加

编辑页面：



图 5-73 域名访问控制编辑

删除页面：

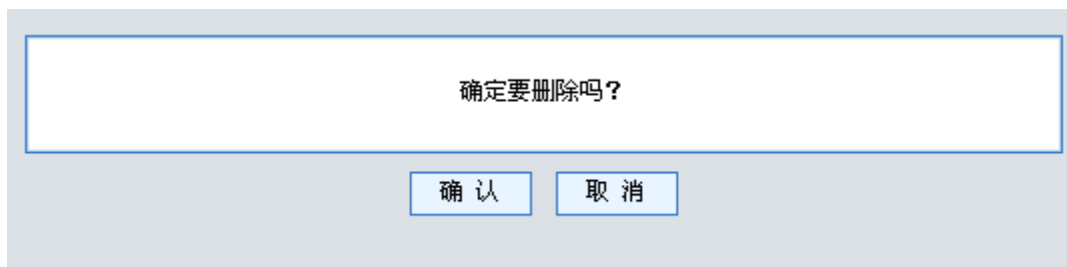


图 5-74 域名访问控制删除

5.6.3.3 DNS 攻击保护

管理员可以通过可以通过包分类的方式，对数据包进行分析，实现 DNS 检测和 DNS 防护的目的。



图 5-75 DNS 攻击保护配置

数据域说明

表 5-22 DNS 攻击保护数据域说明

域名	说明
分类名	包分类名称。
源地址	包分类中的源地址。
目的地址	包分类中的目的地址。
服务	包分类中的服务类型。
dns 检测	DNS 域名检查和 TTL 检测
response flood	DNS 响应报文抗攻击
dns 防护	DNS 请求报文抗攻击

此界面可以完成以下功能：

- 添加 DNS 攻击保护
- 编辑 DNS 攻击保护
- 删除 DNS 攻击保护
- DNS 防护查询
- 添加 DNS 攻击保护
- 点“添加”按钮，进入“DNS 防护”
- 添加参数
- 点“确定”按钮完成添加

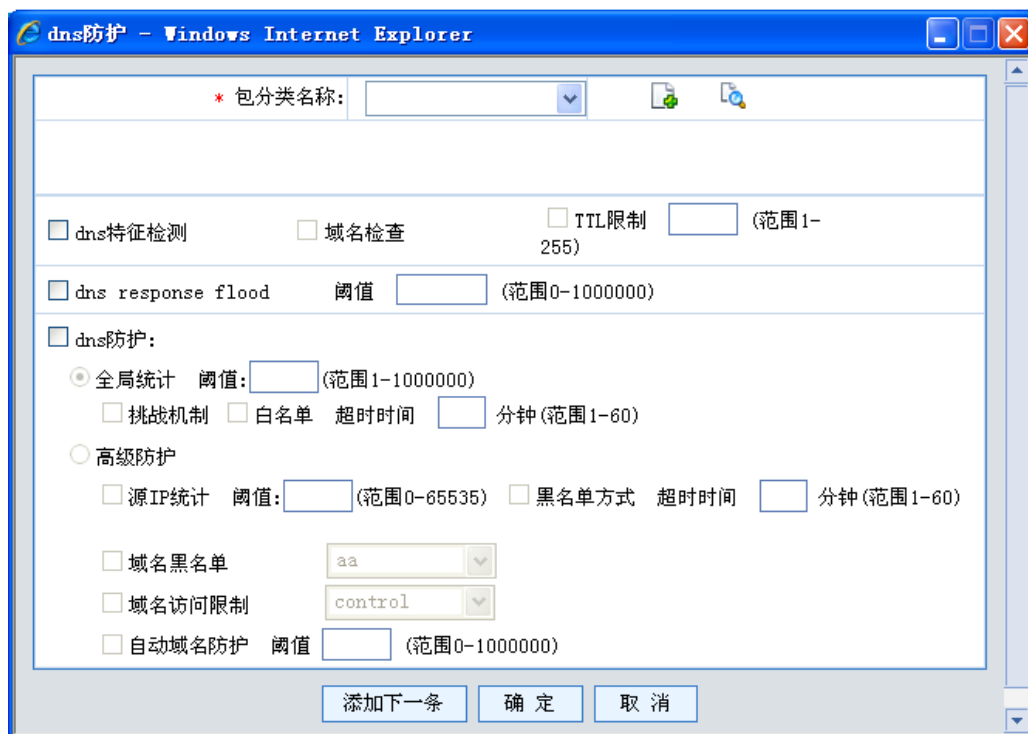


图 5-76 DNS 防护添加

编辑页面:

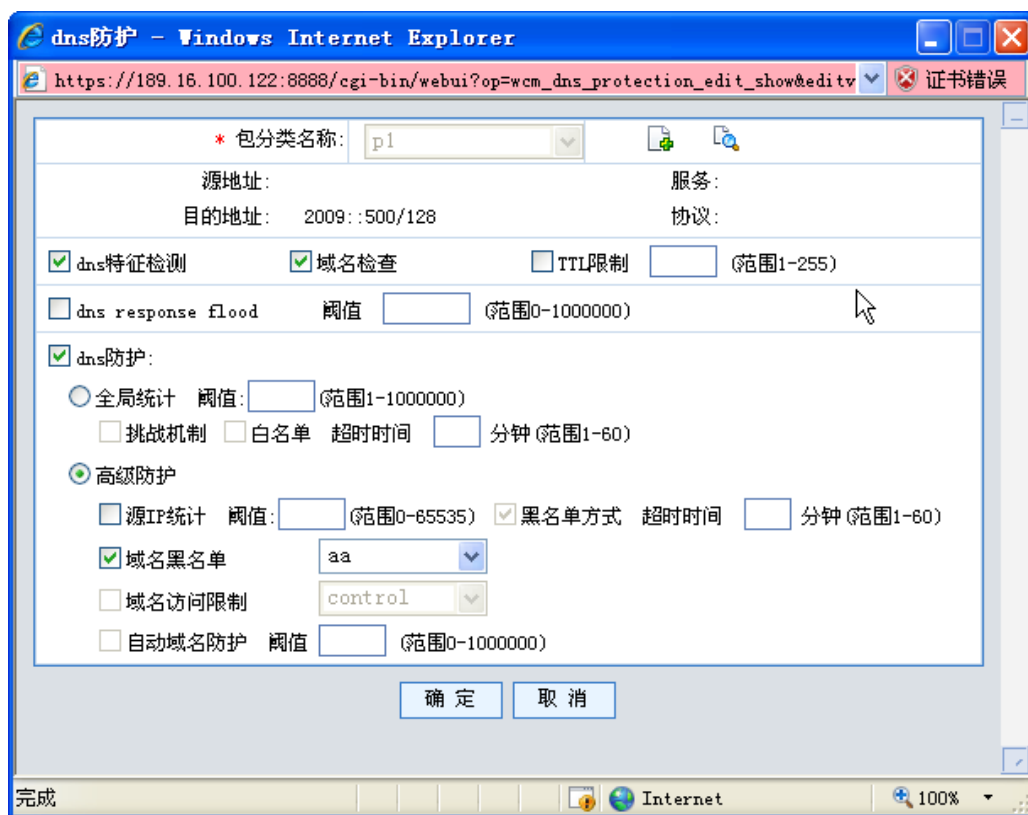


图 5-77 DNS 防护编辑

删除页面：

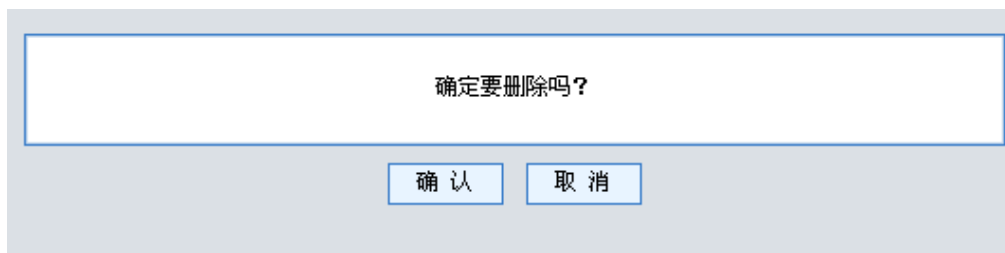


图 5-78 DNS 防护删除

DNS 防护查询

- 点“按条件查询”按钮，进入“dns 防护查询”
- 添加参数
- 点“确定”按钮完成查询



图 5-79 DNS 防护查询

5.6.3.4 域名长度参数

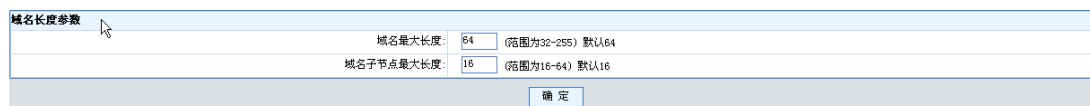


图 5-80 域名长度参数设置

数据域说明

表 5-23 域名长度数据域说明

域名	说明
域名最大长度	域名总长度的最大长度
域名子节点最大长度	域名中的子域名的最大长度

5.6.4 高级型攻击

管理员可以通过保护策略来对网路中的 DDOS、DOS 以及工具型攻击进行管理，并且可以选择是否与 Detector 联动。一条保护策略包括了三个部分：策略名、PCP 名和保护策略功能选择。

高级型攻击功能包括：



- 抗攻击配置



图 5-81 高级型攻击配置


图标说明：

表 5-24 保护策略图标说明

域名	说明
	删除本条记录
	编辑本条记录

数据域说明：

表 5-25 保护策略数据域说明

域名	说明
保护策略名称	保护策略名称，唯一标识，符合命名规则
包分类策略	包分类策略名称，符合命名规则
抗攻击配置	点击  ，可以进行抗攻击参数配置

添加保护策略：

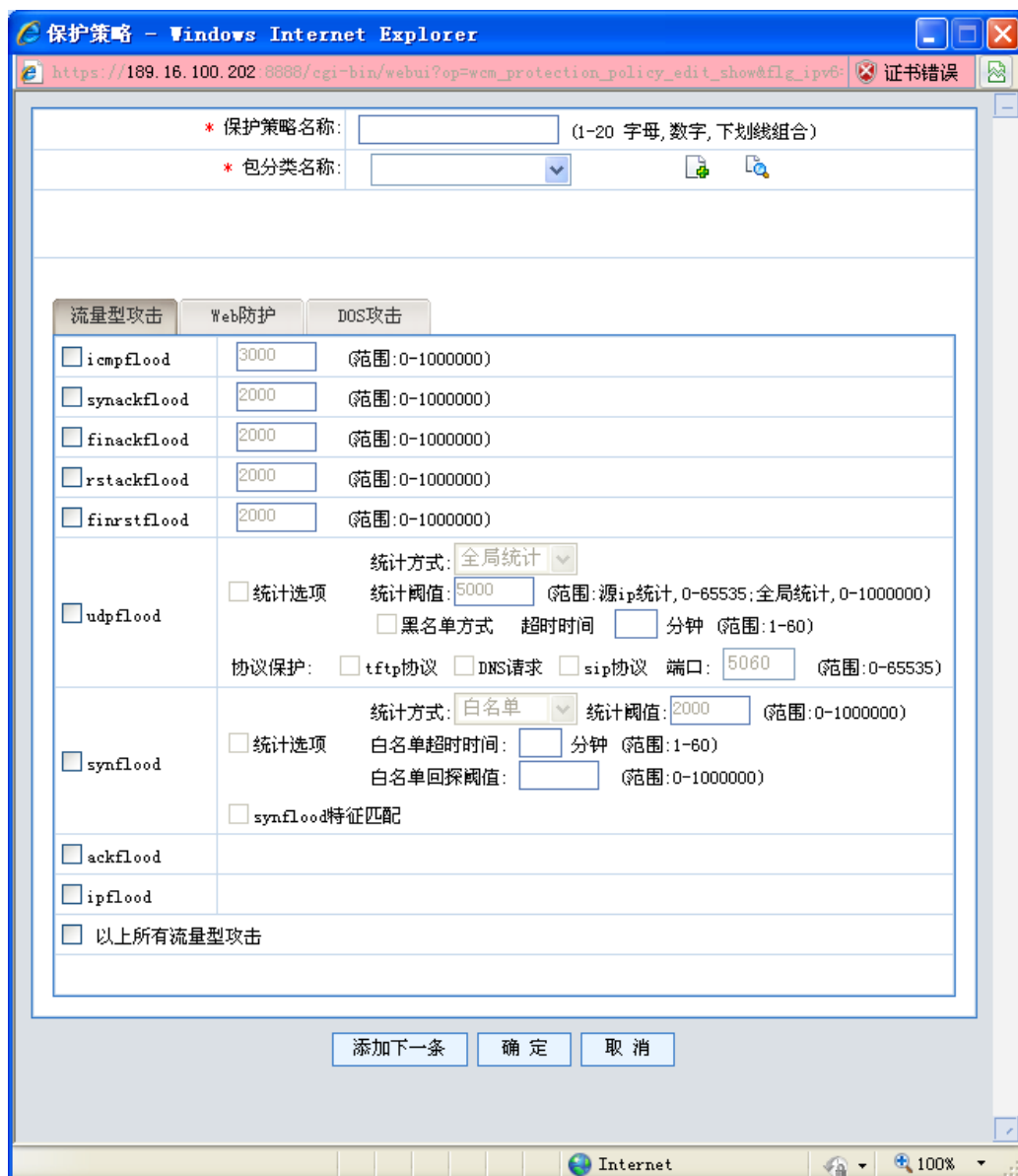


图 5-82 添加保护策略

表 5-26 保护策略添加项说明

域名	说明
保护策略名称	新建保护策略的名称
包分类名称	选择一个已有的包分类规则, 选择后可以在下面看到相关配置。

表 5-27 多种攻击的名词解释

域名	说明
流量型攻	ICMPflood 攻击
	当 ICMP ping 产生的大量回应请求超出了系统的最大

击		限度，以至于系统耗费所有资源来进行响应直至再也无法处理有效的网络信息流时，就发生了 ICMP 泛滥。
	synackflood 攻击	tcp 报文中 syn 和 ack 标志位同时被置的洪水攻击
	finackflood 攻击	tcp 报文中 fin 和 ack 标志位同时被置的洪水攻击
	rstackflood 攻击	tcp 报文中 rst 和 ack 标志位同时被置的洪水攻击
	finrstflood 攻击	tcp 报文中 fin 和 rst 标志位同时被置的洪水攻击
	udpflood 攻击	与 ICMP 泛滥相似。攻击者向同一 IP 地址发送大量的 UDP 包使得该 IP 地址无法响应其它 UDP 请求，就发生了 UDP 泛滥。
	synflood 攻击	TCP 连接是通过三次握手完成的。当网络中充满了会发出无法完成的连接请求的 SYN 封包，以至于网络无法再处理合法的连接请求，从而导致拒绝服务 (DoS) 时，就发生了 SYN 泛滥攻击。攻击者通过不完全的握手过程消耗服务器的半开连接数目达到拒绝服务攻击的目的。攻击者向服务器发送含 SYN 包，其中源 IP 地址已被改为伪造的不可达的 IP 地址。服务器向伪造的 IP 地址发出回应，并等待连接已建立的确认信息。但由于该 IP 地址是伪造的，服务器无法等到确认信息，只有保持半开连接状态直至超时。由于服务器允许的半开连接数目有限，如果攻击者发送大量这样的连接请求，服务器的半开连接资源很快就会消耗完毕，无法再接受来自正常用户的 TCP 连接请求。
Ack flood 攻击	在 TCP 连接建立之后，所有的数据传输 TCP 报文都是带有 ACK 标志位的，主机在接收到一个带有 ACK 标志位的数据包的时候，需要检查该数据包所表示的连接四元组是否存在，如果存在则检查该数据包所表示的状态是否合法，然后再向应用层传递该数据包。如果在检查中发现该数据包不合法，例如该数据包所指向的目的端口在本机并未开放，则主机操作系统协议栈会回应 RST 包告诉对方此端口不存在。	
	ipflood 攻击	ip 协议域不是 tcp、udp、ICMP 常用等协议的报文攻击
Web 防护	httpflood 攻击	利用代理服务器发起大量的 HTTP Get 请求，主要是请求动态画面，数据库服务器负载极高，无法正常相应。
	cc 攻击	攻击主机通过大量代理服务器向目标主机发送 HTTP GET 请求，并随即关闭到代理服务器的连接，从而仅用很少的资源在目标主机上建立大量连接和页面请求，达到拒绝服务式的攻击。

	url-protect	控制和保护 http url
DOS 攻击	Tracert 攻击	防止攻击者找到网路路由路径

5.6.5 自定义特征

自定义特征是用户可以定义网络数据报文的特征，达到抗攻击的目的。

5.6.5.1 开启自定义



图 5-83 自定义特征开启

数据域说明

表 5-28 自定义特征开启 数据域说明

域名	说明
开启开关	自定义的总开关（必选）
IP 地址	保护的目IP 地址（必选）

5.6.5.2 TCP 自定义特征配置

这个页面配置 TCP 协议的特征。

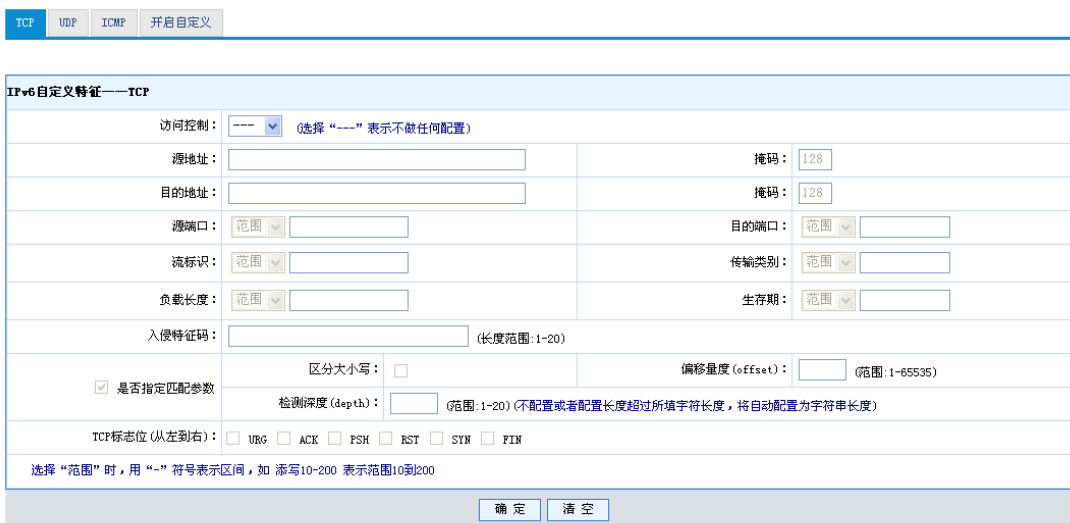


图 5-84 自定义特征配置

数据域说明

表 5-29 自定义特征数据域说明

域名	说明
访问控制	符合特征报文执行的动作，丢弃或者通过
入侵特征码	应用层数据特征串
是否指定匹配参数	如没有勾选，程序则会搜索整个应用层数据

5. 6. 5. 3 UDP

这个页面用于配置 UDP 协议的自定义特征。

图 5-85 UDP

5. 6. 5. 4 ICMP

这个页面用于配置 ICMP 协议的自定义特征。

图 5-86 ICMP

5.7 流量统计

5.7.1 事件统计

事件统计

事件统计

时间范围: 从 到 (时间格式: yyyy/mm/dd hh:mm:ss)

攻击类型

synflood攻击
 udp洪水攻击
 icmp攻击
 dns攻击
 ackflood攻击
 connflood攻击

攻击类型列表

全部
>>
<<

源地址: 从 到

目的地址: 从 到

源端口: 从 到

目的端口: 从 到

协议: TCP UDP ICMP ARP

注: 五源组查询条件如果起始和终止条件一样, 会进行唯一性查询, 而不是范围查询。

生成报表

图 5-87 事件统计配置

5.7.2 攻击类型 TOP5

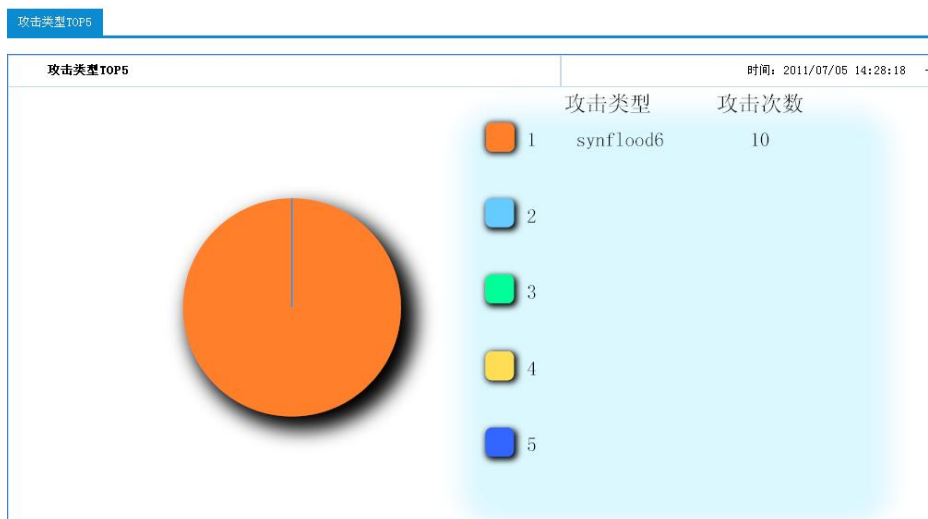


图 5-88 攻击类型 TOP5 显示

5.7.3 攻击来源 TOP5

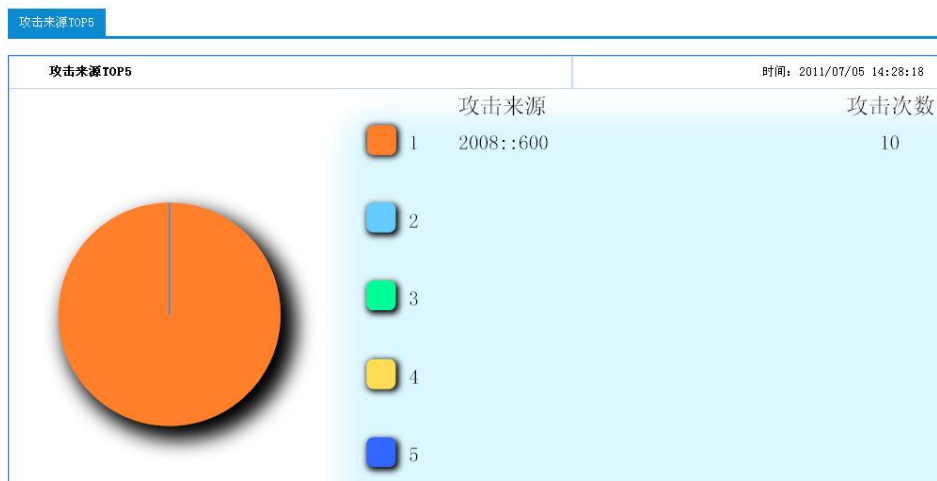


图 5-89 攻击来源 TOP5 显示

5.7.4 攻击目的 TOP5

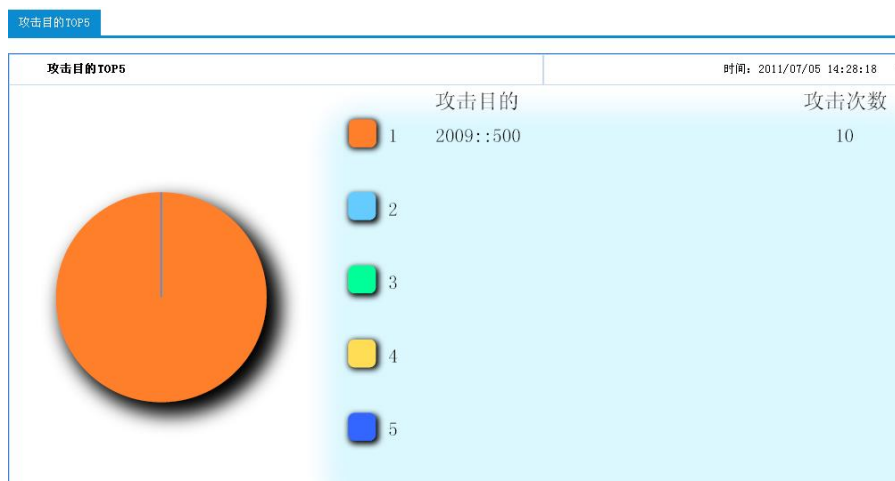


图 5-90 攻击目的 TOP5 显示

5.7.5 攻击流量统计

5.7.5.1 即时流量统计

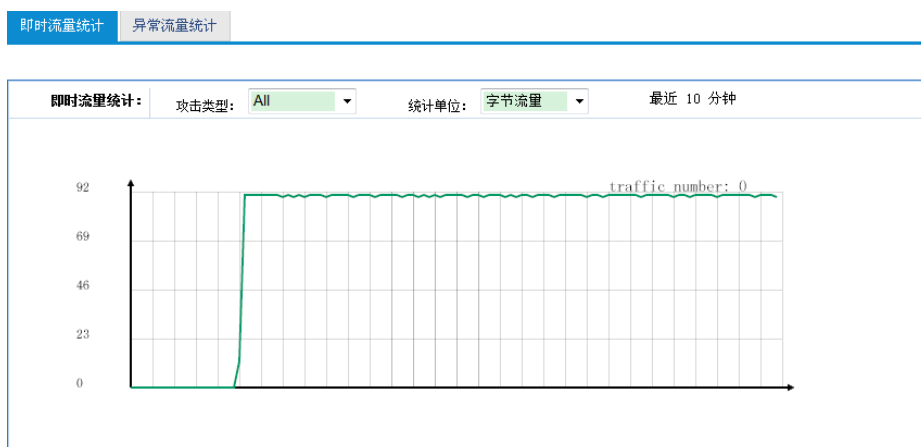


图 5-91 即时流量显示

5.7.5.2 异常流量统计

即时流量统计		异常流量统计	
设置日期		今天	
攻击事件统计	察看统计图	这里可以察看当日synflood、udpFlood、cc等报文的总体统计图	
攻击事件排行	察看统计图	这里可以察看当日排名在前五名的报文排行及详细数据	
攻击流量统计	察看统计图	这里可以察看当日synflood、udpFlood、cc等报文的总体统计图	
攻击流量排行	察看统计图	这里可以察看当日排名在前五名的报文排行及详细数据	

图 5-92 异常流量统计显示

5.7.6 保护域流量统计

5.7.6.1 牵引流量统计

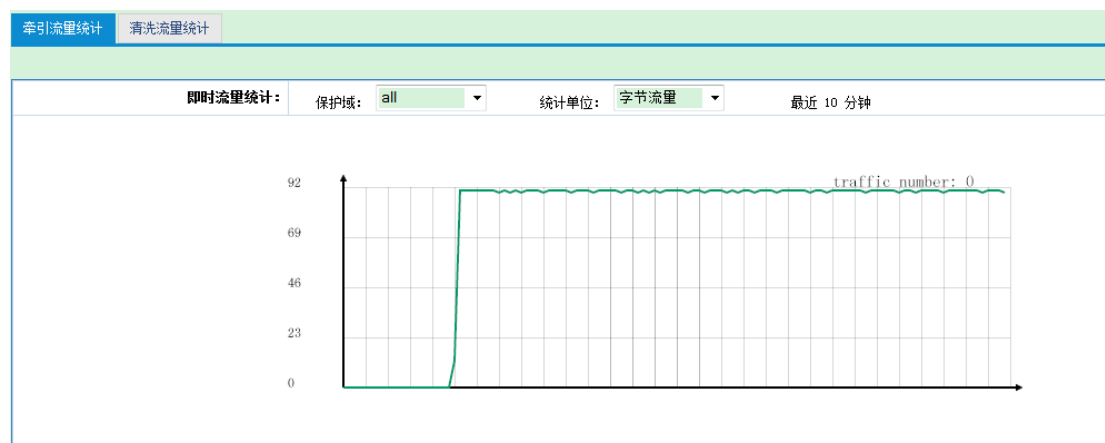


图 5-93 牵引流量统计显示

5. 7. 6. 2 清洗流量统计

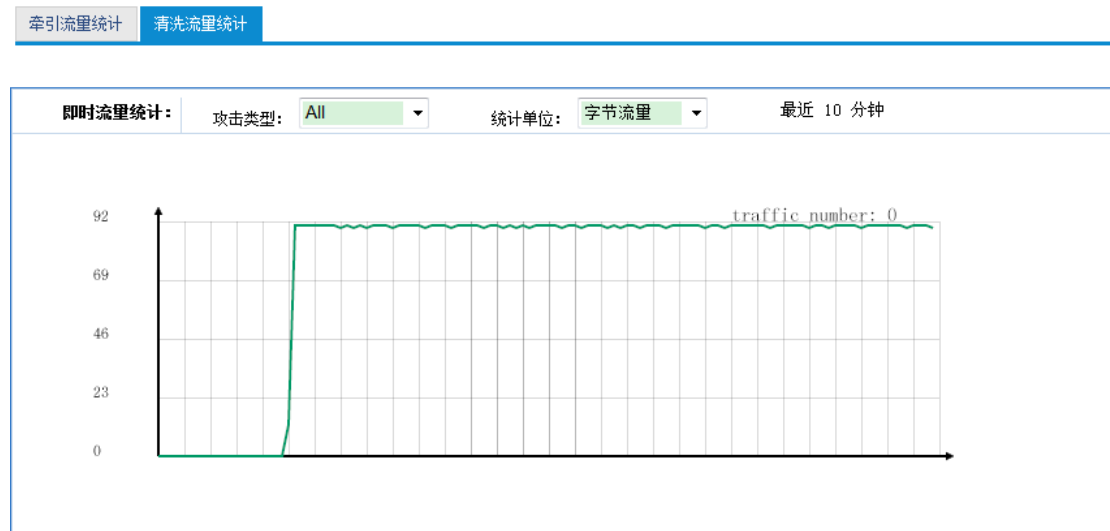


图 5-94 清洗流量统计显示

第6章 虚拟网关

Guard 在启用防火墙功能时，支持虚拟网关（虚拟防火墙）。本章主要介绍虚拟网关的配置方法。

6.1 网关管理

6.1.1 虚拟网关划分

系统已经创建的虚拟网关会在列表页面显示，如下图







名称	共享接口	私有接口	session限制	操作
vf1		Ge0/1/3, Ge0/1/4	100000	  
vf2		Ge0/1/5, Ge0/1/6	100000	  

图 6-1 虚拟列表

列出了已经创建的虚拟网关的名称和享有接口以及 session 的数量限制。

需要新建一个虚拟网关（防火墙）的时候，请点击上图中的“添加”按钮，弹出虚拟防火墙添加窗口如下：



图 6-2 虚拟防火墙添加

添加时请按照界面给出的范围限制和提示。

在列表页面的表格中，操作一栏中列出了对已经存在的防火墙的可进行的动作，包括修

改，删除和切换：

点击修改，弹出的窗口和添加类似，只是不能修改虚拟防火墙的名称



图 6-3 修改虚拟防火墙

点击删除，弹出删除确认窗口：

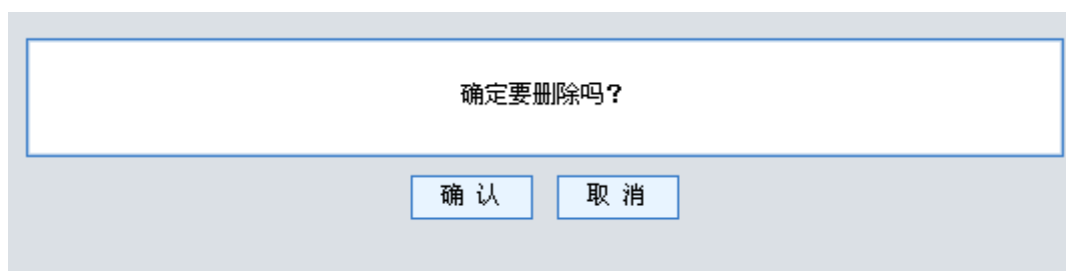


图 6-4 删除虚拟防火墙

需要确认删除动作，以免误删。

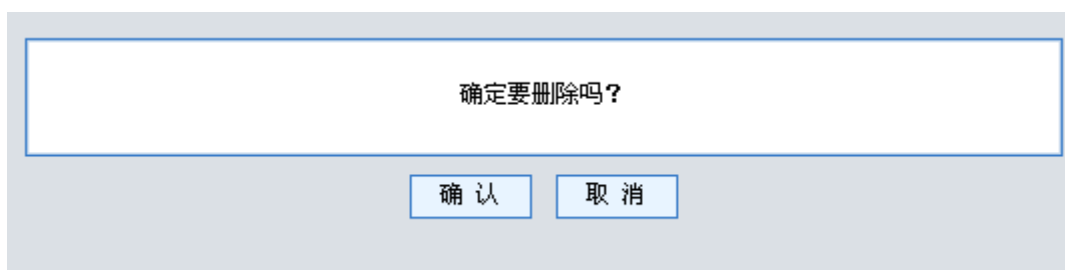


图 6-5 删除虚拟防火墙

点击切换，系统会切换到相应的虚拟防火墙上，比如点击虚拟防火墙 vf1，系统则切换到 vf1 的 web 配置页面上去，可以对虚拟防火墙 vf1 进行配置。

6.1.2 接口归属查看

接口归属查看页面可以查看接口归属于哪个虚拟网关，以及对其进行相应备注。

接口名称	接口状态	归属虚拟网关	备注
Ge0/0/0		vf0	Ge Interface
Ge0/0/1		vf0	Ge Interface
Ge0/0/2		vf0	Ge Interface
Ge0/0/3		vf0	Ge Interface

图 6-6 接口归属查看

6.2 全局资源

6.2.1 地址

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。

6.2.1.1 地址列表



图 6-7 地址列表

地址列表中的地址对象可在以下配置中使用：

- 资源定义：地址->地址组。
- Guard：包分类、DNAT 策略、安全策略、本地服务、连接数控制->静态学习规则、连接数控制->动态学习规则。

可以按两种方式来定义地址：

- IP 地址/掩码
- 地址范围 IP1 — IP2。

注意：

为了避免误操作，这里不支持全网段配置，即 IP 地址不可定义为 0.0.0.0。

如下图所示：

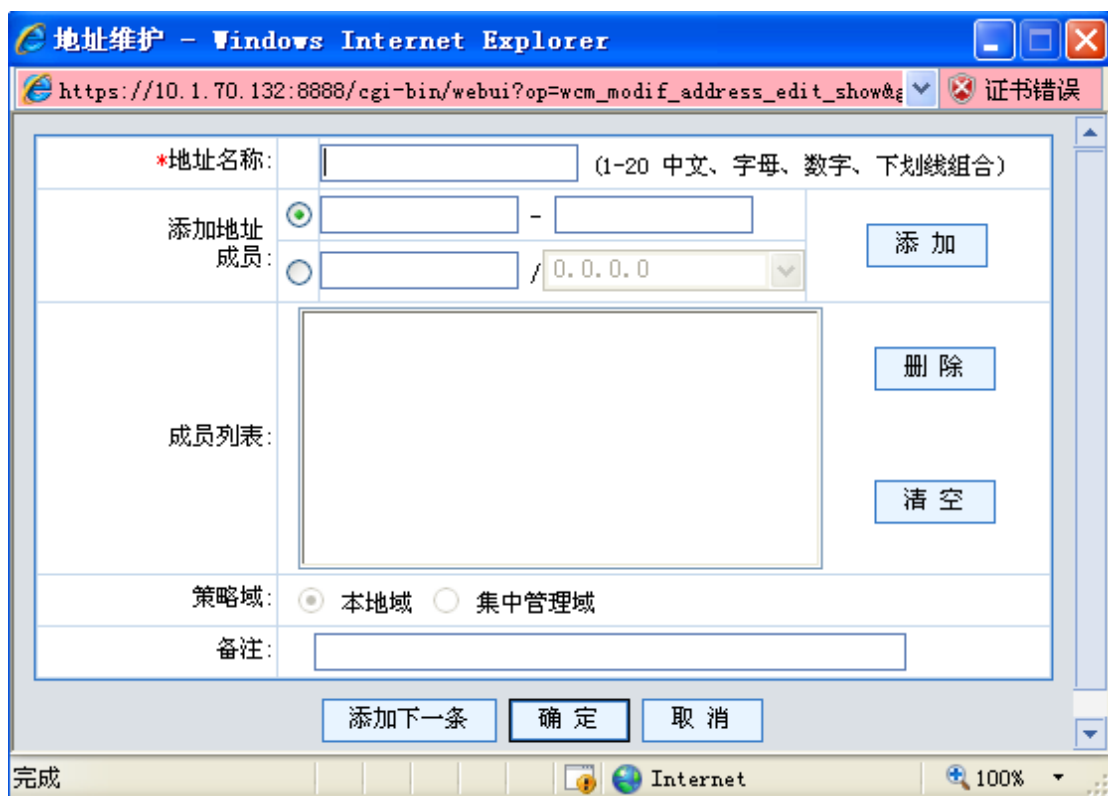


图 6-8 地址维护

表 6-1 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 如果希望指定一台主机，请选择掩码为 255.255.255.255
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

注意：

可以定义 A 类、B 类和 C 类地址。

6. 2. 1. 2 地址池

地址池页面用于对地址池对象进行增加，修改，查询和删除的操作，还可以选择多个地址池对象，进行批量删除。

地址池列表页面如图：

序号	地址池名称	地址池成员	备注	操作
添加				

全选

 第1页/1页 跳转到 页 每页 行

图 6-9 地址池列表

地址池添加页面如图：

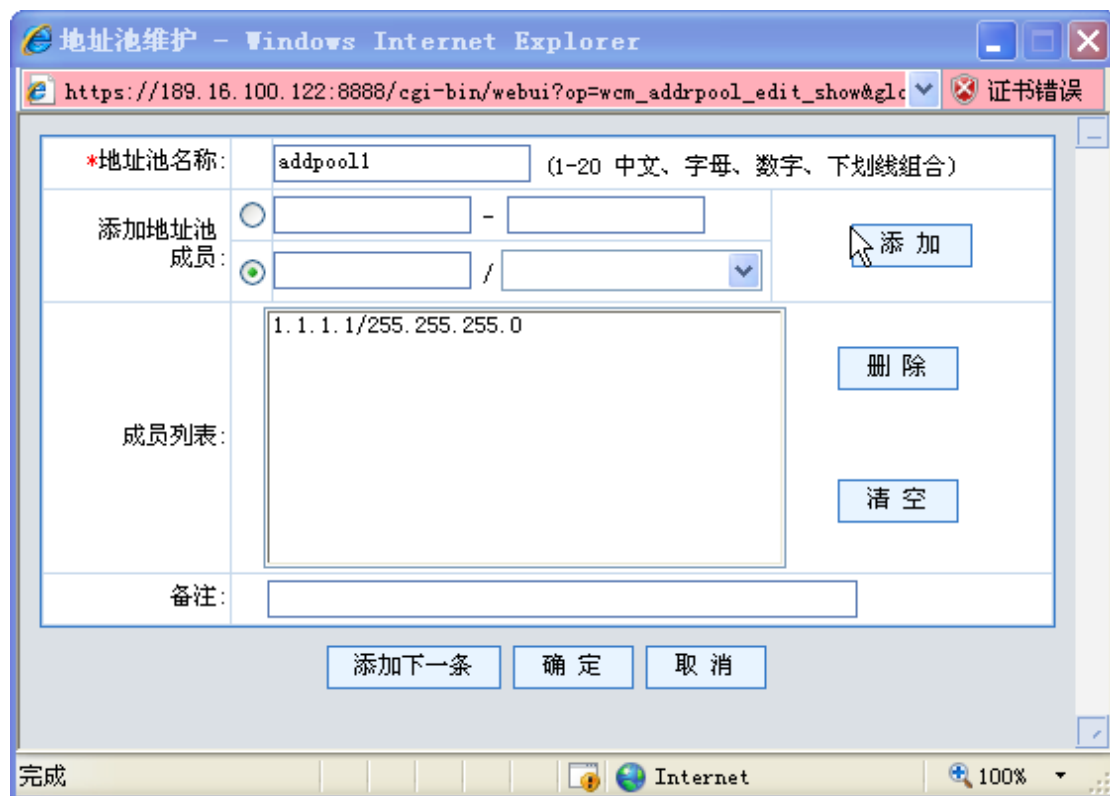


图 6-10 地址池添加页面

一个地址池对象可以添加多个地址池成员，地址池成员可以为 ip 段的方式，也可以是 ip 和掩码的方式。

6. 2. 1. 3 地址组

序号	名称	策略域	成员列表	备注	操作
添加					

全选

 第1页/1页 跳转到 页 每页 行

图 6-11 地址组列表

地址组可在“防火墙”的下列配置中使用：

- 包分类

- DNAT 策略
- 安全策略
- 本地服务

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“添加”，将弹出以下界面：







图 6-12 地址组添加

表 6-2 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”中和“资源定义->地址->服务器地址”中定义的地址。 属于地址列表的成员被移动到地址组成员列表之后，将不再显示于原列表中。
地址组成员	该地址组的所有成员。

表 6-3 添加、删除成员

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
-----------------------------------------------------------------------------------	---------	-----------------------------------------------------------------------------------	----------------

注意：

Ctrl+鼠标左键，可选择列表中的多项一起操作。

6. 2. 1. 4 服务器地址

“服务器地址”用于指定一组内部服务器地址。

序号	名称	服务器IP地址/权重	策略域	备注	操作
<input type="button" value="添加"/>					

全选

第1页/1页 跳转到 页 每页 行

图 6-13 服务器地址列表

在“资源定义->地址->服务器地址”，点击“添加”，将弹出以下界面：



图 6-14 服务器地址添加

表 6-4 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。
负载均衡权值	可输入的范围是 0—2147483647。系统将根据权值的大小和该服务器当前的流量负载来决定是否需要将任务切换至其他服务器，避免单个服务器无法承担过大的流量。 权值越大，意味着相应的服务器可承担的负载越大；权值越小，则服务器可承担的负载越小。权值为 0，则表示系统不会针对该服务器执行负载均衡策略。

6.2.2 服务

服务用于指定“协议 + 源端口 + 目的端口”，主要包括以下五种服务：

- 常用服务：包括 dns, gre, http, https, ICMP-any, igmp, igmp, ispf, oicq, pop3, smtp, snmp, syslog, tcp-any, telnet, udp-any 等
- ICMP 服务：可指定 type 和 code
- 基本服务：可以设置“协议 + 源端口 + 目的端口”
- 服务组：把以上服务组合起来，形成一个服务组
- ALG：目前支持 FTP 协议

以下两处用到服务资源：

- “防火墙”下的：包分类、DNAT 策略、安全策略、本地安全策略
- “资源定义”下的：用户->用户列表

6. 2. 2. 1 服务对象定义

服务对象定义了一些常用的服务，不可以修改，删除，只可以被引用。

序号	名称	策略域	协议	端口	服务简介
1	dns	本地域	17	53	
2	gre	本地域	47	0	
3	http	本地域	6	80	www service
4	https	本地域	6	443	
5	icmp_any	本地域	1	0	icmp service
6	igmp	本地域	2	0	
7	igmp	本地域	88	0	
8	oisq	本地域	17	8000	
9	ospf	本地域	89	0	
10	pop3	本地域	6	110	

◀ ◂ ▶ ▸ 第1页/2页 跳转到 页 每页 行

图 6-15 预定义服务列表

6. 2. 2. 2 ICMP 服务

服务列表显示当前的 ICMP 服务。



图 6-9 ICMP 服务列表

添加窗口为：



图 6-16 ICMP 服务添加

表 6-5 ICMP 服务添加元素表

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

6. 2. 2. 3 基本服务

列表中显示了当前已定义的所有基本服务。



图 6-17 基本服务列表

点击“添加”，将弹出以下界面：



图 6-18 基本服务添加

表 6-6 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 1 到 65535 源端口通常设为 1-65535，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 1 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 1-65535，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 1-65535。
--	-------------------------------------------------------

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。

6. 2. 2. 4 服务组



图 6-19 服务组列表

服务组用于“防火墙”下的：包分类、DNAT 策略、安全策略。

服务组的成员可以是“资源定义->服务”中已经定义过的服务对象、ICMP 服务和基本服务。

在“资源定义->服务->服务组”，点击“添加”，将弹出以下界面：



图 6-20 服务组添加

表 6-7 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”中定义的所有服务，包括“服务对象定

	义”“ICMP 服务”“基本服务”。 本列表的成员被移动到服务组成员列表中之后，将不再显示于本列表中。
服务组成员	列出本组的所有成员。

表 6-8 服务组添加、删除成员列表

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

6. 2. 2. 5 ALG 定义

由于某些应用协议需要创建动态连接，而创建连接所用的 ip 地址和端口是动态的，为了监视该类协议，这里引入了 ALG (application layer gateway) 即应用层网关。目前支持 ftp, tftp, h.323, h.323gk, mms, rtsp, pptp, rtsp, xdmcp, sip 共 10 种协议。

序号	服务名	端口	是否启用	操作
1	ftp	21	✓	 
2	h323	1720	✓	 
3	h323gk	1719	✓	 
4	mms	1755	✓	 
5	pptp	1723	✓	 
6	rtsp	554	✓	 
7	sip	5060	✓	 
8	tftp	69	✓	 
9	tns	1521	✓	 
10	xdmcp	177	✓	 

图 6-21 ALG 定义列表

对 ALG 定义列表可选的操作有启用/关闭、编辑和恢复默认设置三项。
选中点击“编辑”，将执行编辑操作，并弹出以下界面：



图 6-22 ALG 配置

表 6-9 ALG 添加元素表

值域	说明
端口	协议使用的端口 可输入范围是 1-65535，最多允许设置 8 个，且端口值不可重复
是否可重定向	是否开启 ftp 协议的端口重定向功能 在方框内选中即为开启，反之则关闭

注意：

设置多个端口时，必须用英文逗号分隔，且端口值不可重复。

选中点击“撤销”，将执行恢复默认设置操作，当前配置将被默认配置覆盖。默认情况下，ftp 协议的端口值为 21，可重定向功能开启。

6.2.3 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。还可以把多个时间段组合成时间组。

定义的时间和时间组可在“防火墙”的以下几处配置中应用：包分类、DNAT 策略、安全策略。

6. 2. 3. 1 时间列表

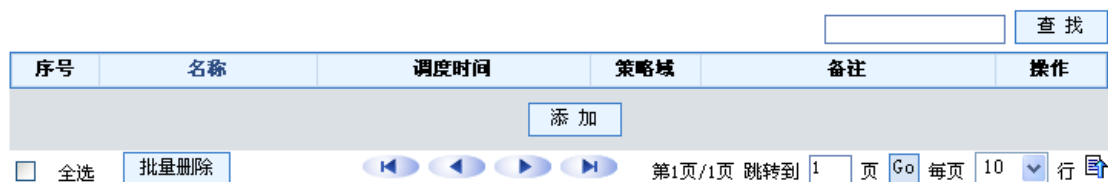


图 6-23 时间列表

可以按照一次性调度和周循环调度两种方式，来定义时间。点击“添加”，如下图所示：

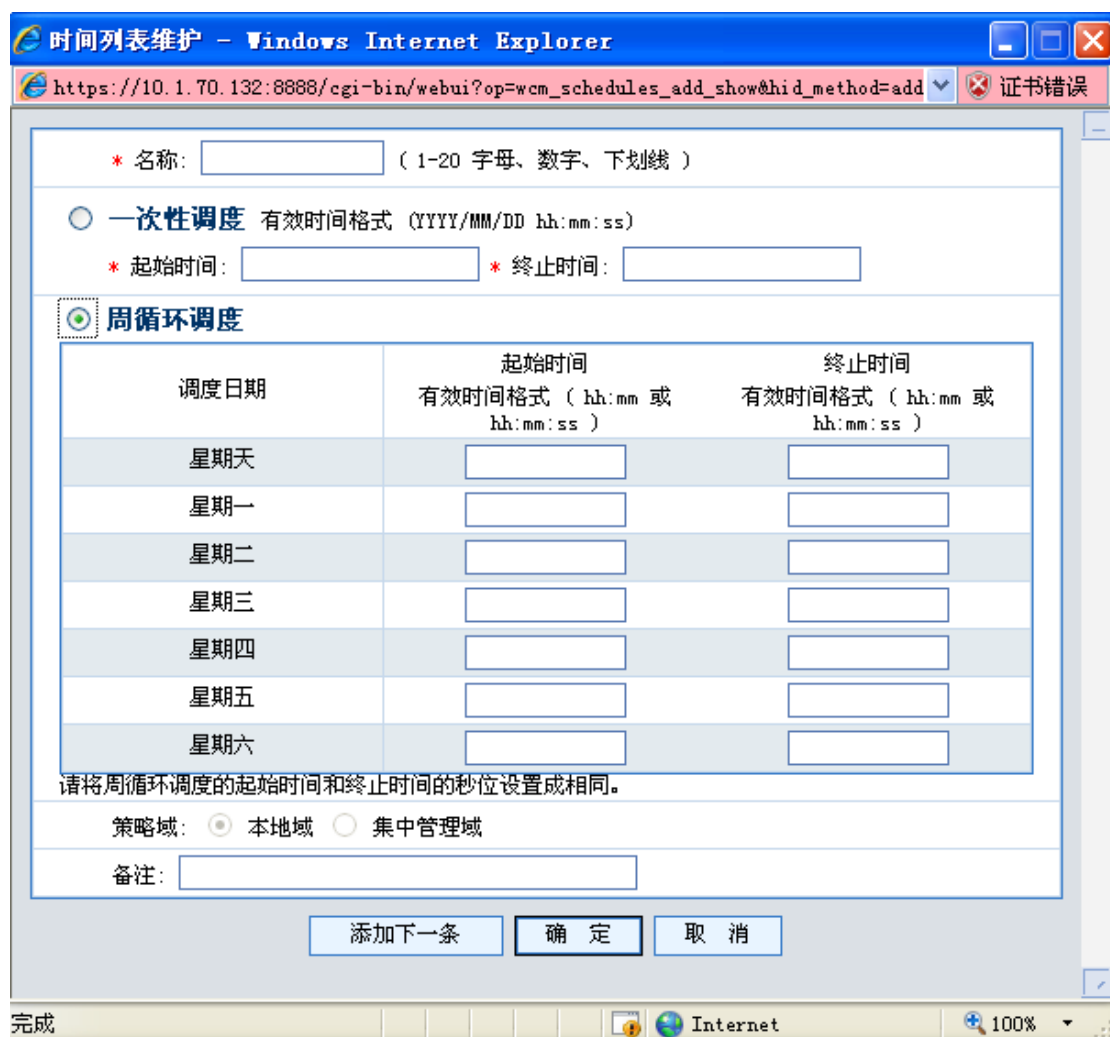


图 6-24 时间资源维护

表 6-10 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“Guard”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。则可以定义一个时间段 worktime 表示工作时间，再在“Guard->包分类”中定义一个包分类，源地址和目的地址均设为“any”，服务对象选择“HTTP”，时间调度引用 worktime，在安全策略中添加一条规则，引用这个包分类并设置 Guard 策略为阻止即可。

6. 2. 3. 2 时间组



图 6-25 时间组列表







图 6-26 时间组维护

表 6-11 时间组维护添加元素表

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	该时间组的所有成员。

表 6-12 时间组维护添加、删除成员

操作	说明
	添加成员，点击  把选中的时间移动到成员列表 时间列表成员添加至时间组之后，该成员不再显示于时间列表中。
	删除成员，点击  把选中的成员移动到时间列表中

6.2.4 应用协议

6.2.4.1 应用协议

点击 资源定义/应用协议选项在如下图的应用协议表中可以查看特征库中对应的应用协议名称和对应的协议 ID 号。

序号	名称	协议ID
1	ftp	1
2	h323	2
3	h323gk	3
4	mms	4
5	pptp	5
6	rtsp	6
7	sip	7
8	tftp	8
9	tns	9
10	xdmcp	10


 第1页/14页 跳转到 页 每页 行 

图 6-27 应用协议表

6.2.4.2 应用协议组

点击资源定义/应用协议/应用协议组，进入应用协议组表其中 audiovideo、p2p、im、stock、normal_server、game 等 5 大类协议，其中每个大类协议中又包括几十种小类协议，见下图：

序号	名称	成员列表	类型	备注	操作
1	audiovideo	pplive qqlive ppstream ppmate feidian uusee xunleikankan sopcast funshion youku.com tudou.com ku6.com 56.com 6.cn SinaVideo kwmusic kugoomusic qianqianmusic qqmusic cctvbox qqmusicradio moshoushijie fankongjingying tiantang hianfang	预定义	audiovideo	

图 6-28 应用协议组表

6.2.5 包分类

包分类显示页面：

可以根据序号排名显示，显示包括几个缩略参数，源地址、目的地址、服务和协议等。可以分屏显示，支持翻页功能等。

界面如下图所示：

按条件查询

序号	分类名	源地址	目的地址	服务	协议	内网地址	外网地址	生效时间状态	操作
<input type="checkbox"/>	1 ipqos	192.0.0.0/255.0.0.0						未配置	
<input type="checkbox"/>	2 df	1.2.3.3/	5.6.6.6/	gre				未配置	
<input type="checkbox"/>	3 snat	100.100.100.0/255.255.255.0						未配置	

全选

 第1页/1页 跳转到 页 每页 行

图 6-29 包分类显示

包分类添加页面：

根据包分类支持的几个元素定义分类规则。

具体参数如下图所示：



图 6-30 包分类显示

包分类添加页面还有一个高级选项，可以定义一些不常用的参数配置。
点开后面界面如下图所示：

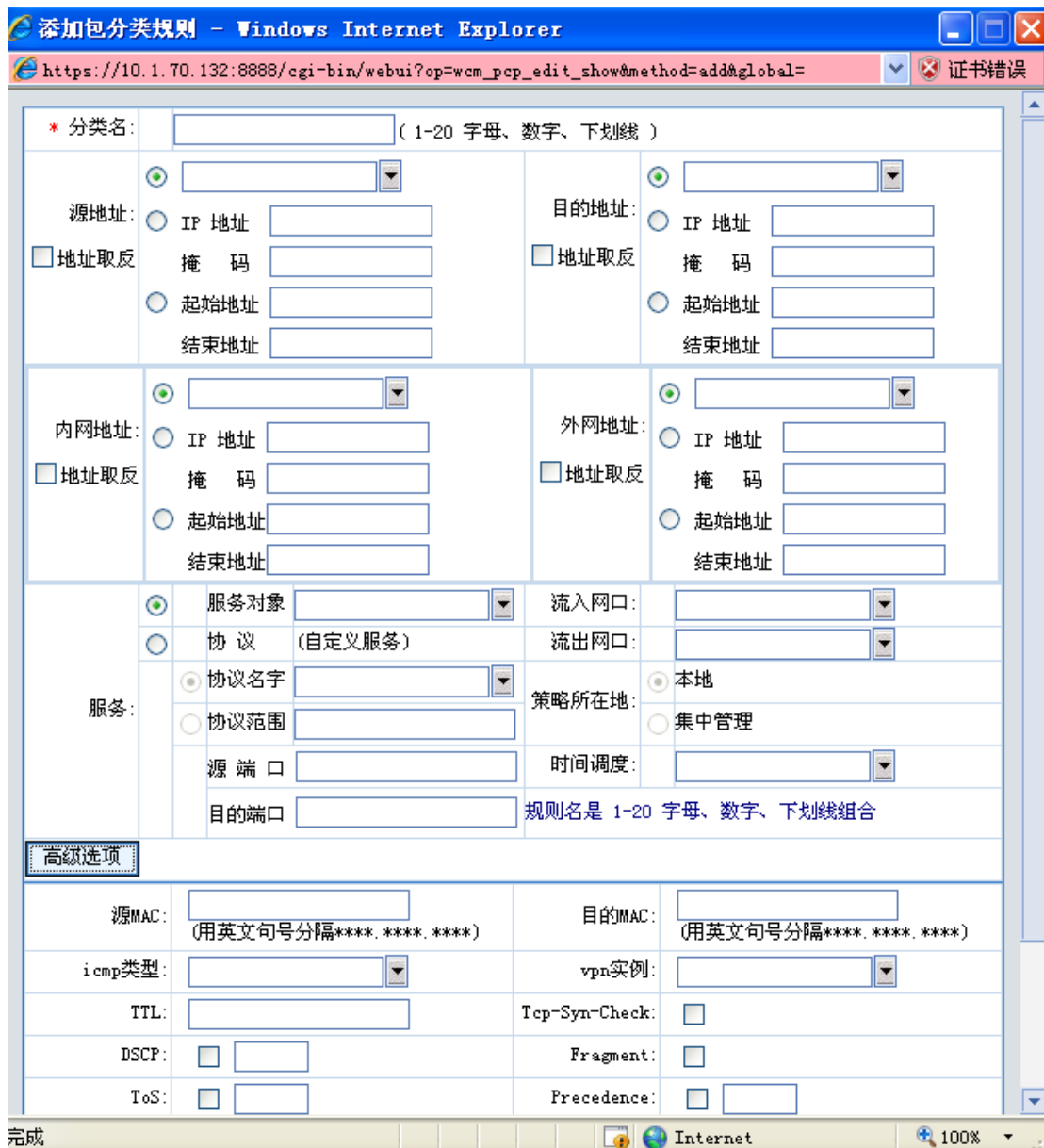


图 6-31 带有高级选项的包分类添加

包分类页面还有修改、排序、删除功能，

如下图所示：



图 6-32 包分类的修改、排序、删除功能示意图

包分类修改页面：



图 6-33 包分类修改

删除页面：

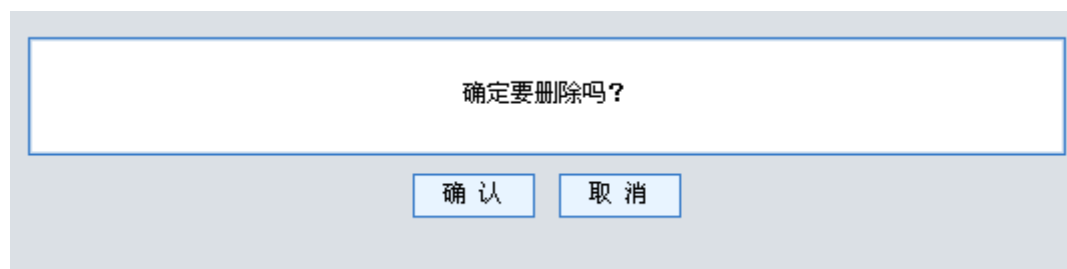


图 6-34 包分类删除

6.3 全局策略

6.3.1 包过滤

包过滤显示页面：

可以根据序号排名显示，显示包括几个缩略参数，源地址、目的地址、服务和动作等。

可以分屏显示，支持翻页功能等。

界面如下图所示：



图 6-35 包过滤

包过滤添加页面：

根据包过滤支持的几个元素定义分类规则。

具体参数如下图所示：

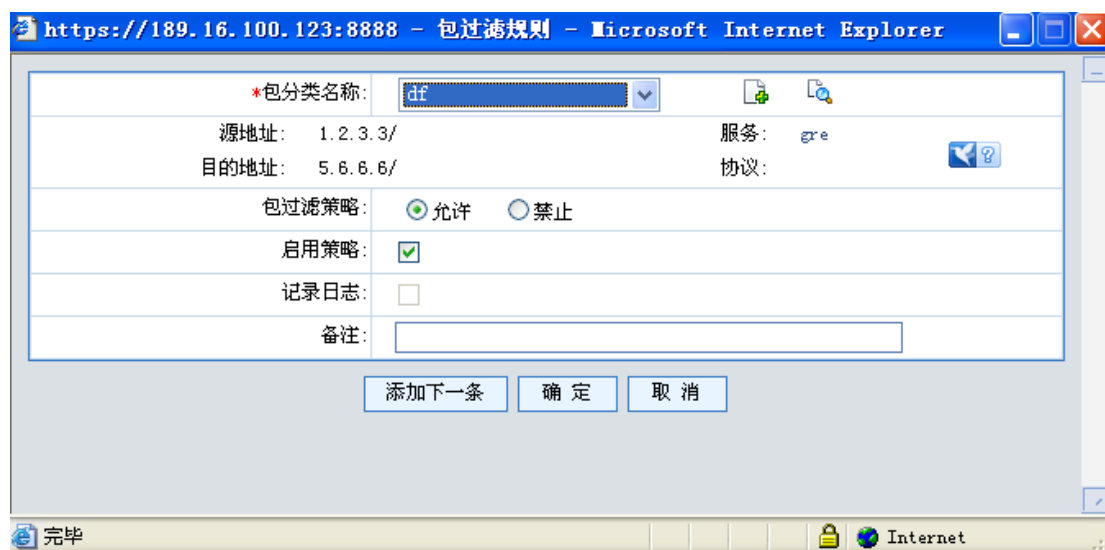


图 6-36 包过滤添加页面

6.3.1.1 默认过滤策略

安全选项提供 Guard 可设置的一些全局安全策略，包括包过滤策略、arp 超时时间、严格状态检查、状态优先以及黑名单检查开关。这些参数对整个 Guard 生效。

界面如下图所示：

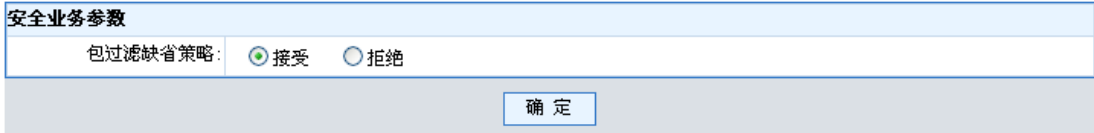


图 6-37 默认过滤策略配置

6.3.2 DNAT 策略

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。

目的地址转换规则显示页面：

可以根据配置的序号排名显示，包括 PCP 的基本参数信息，以及转换后的参数信息等。

可支持分屏显示，翻页等功能。



图 6-38 目的地址转换规则显示

目的地址转换添加规则：

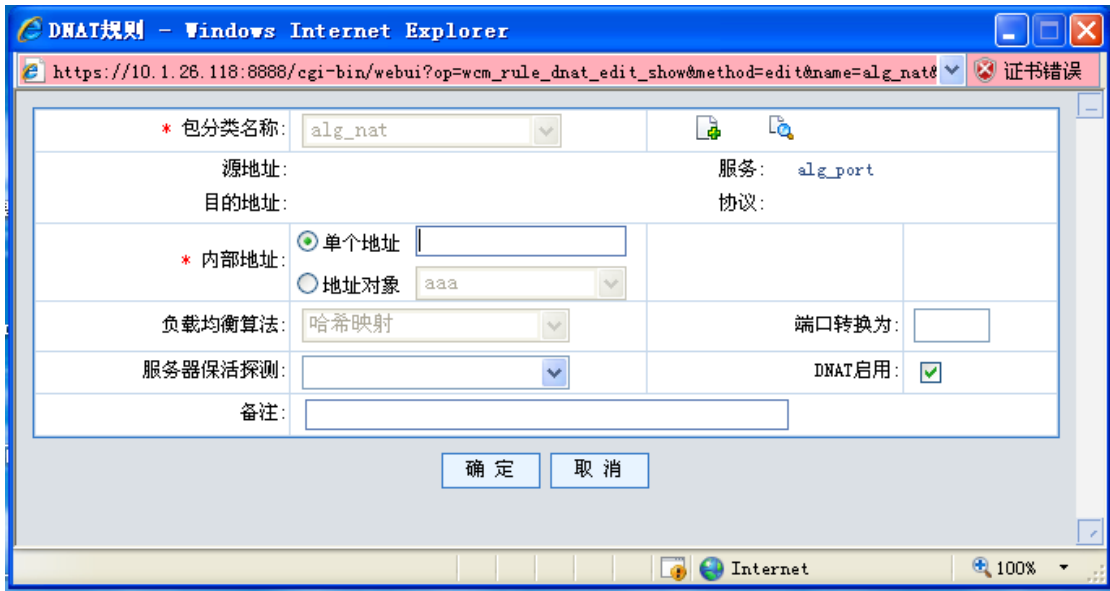


图 6-39 目的地址转换添加规则

目的地址转换修改规则：

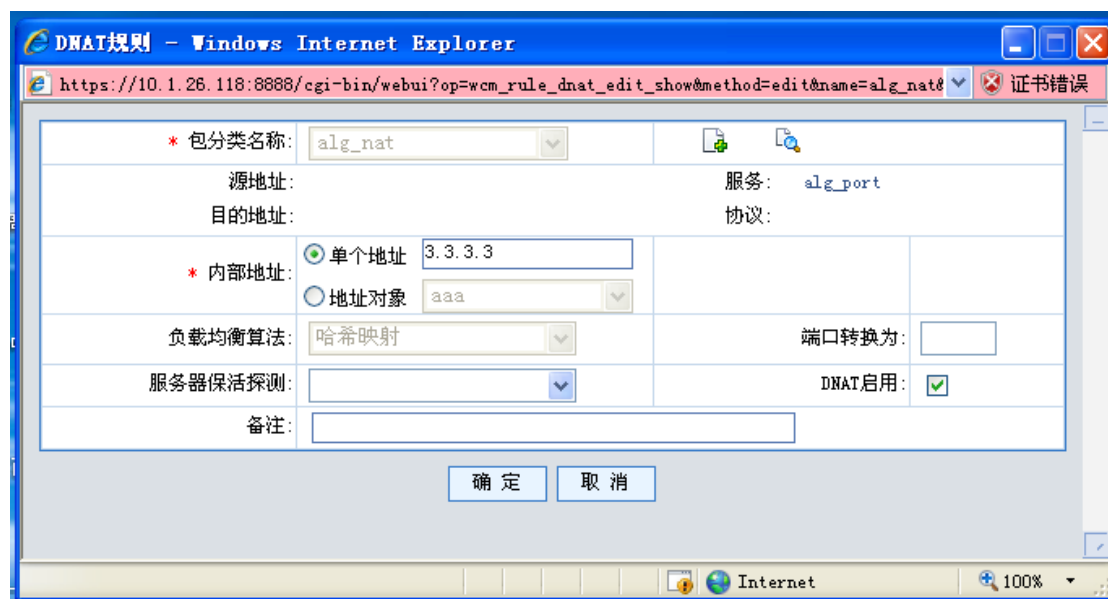


图 6-40 目的地址转换修改规则

目的地址转换删除规则：

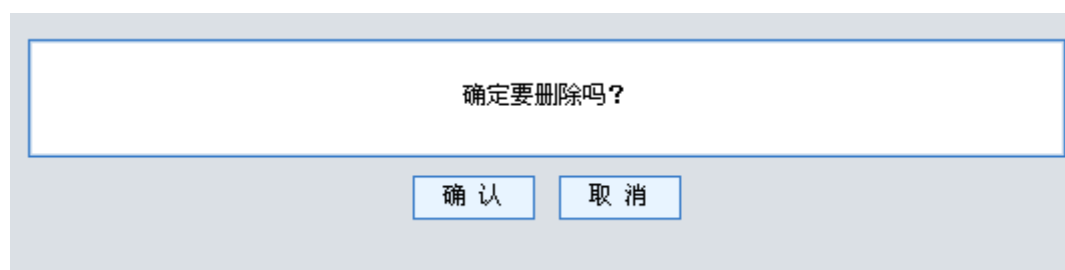


图 6-41 目的地址转换删除规则

6.3.3 SNAT 策略

SNAT，即原地址转换。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。

用户可通过规则设定需要转换的源地址（支持网络地址范围）、源端口。可以通过系统“资源定义->地址”定义的地址对象，支持多对多，多对一，一对多的地址转换关系。

SNAT 配置页面如下：

按条件查询

序号	分类名	源地址	目的地址	服务	转换地址	算法	端口	是否启用	备注	操作
<input type="checkbox"/>	1	df	1.2.3.3/	5.6.6.6/	gre	2.3.3.5	随机端口	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	2	snat	100.100.100.0/255.255.255.0		Ge0/0/0			<input checked="" type="checkbox"/>		

全选

 第1页/1页 跳转到 页 每页 行

图 6-42 安全策略显示

添加 SNAT 规则界面：

图 6-43 添加 SNAT 策略

修改 SNAT 策略界面：

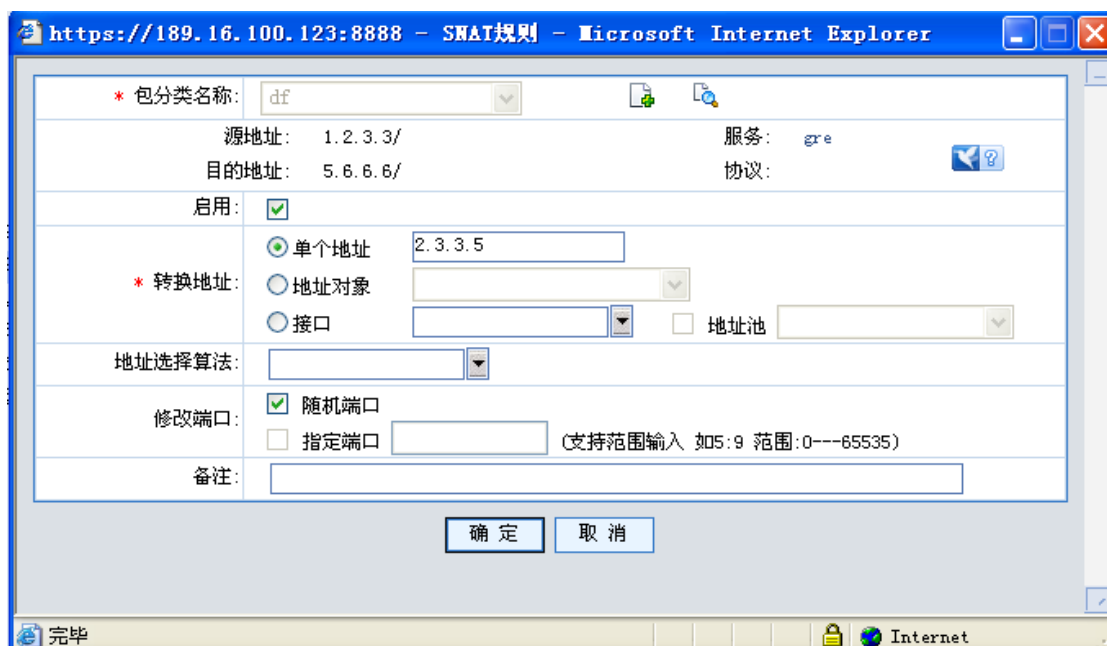


图 6-44 修改 SNAT 策略

删除 SNAT 界面:

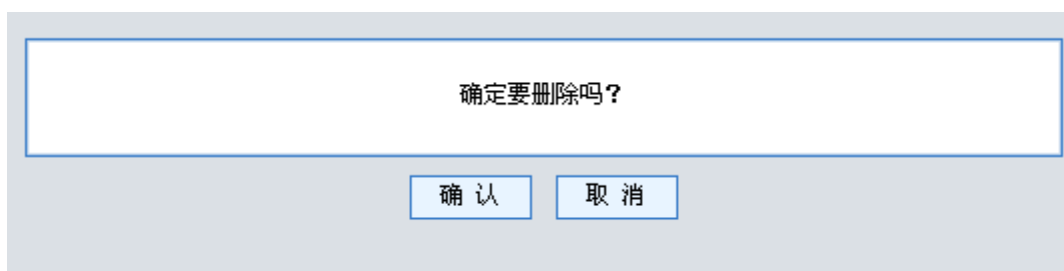


图 6-45 删除 SNAT

6.3.4 长连接

长连接页面如下图所示:



图 6-46 长连接

添加页面:

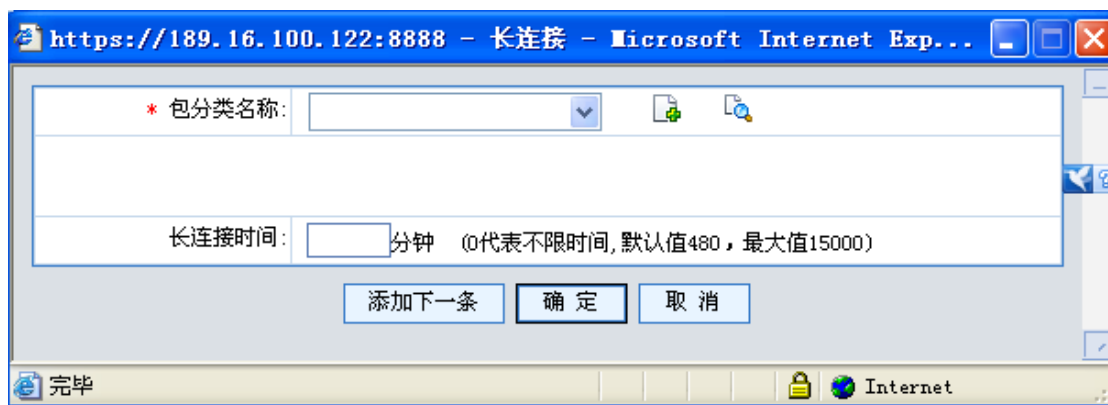


图 6-47 长连接添加页面

删除长连接界面:

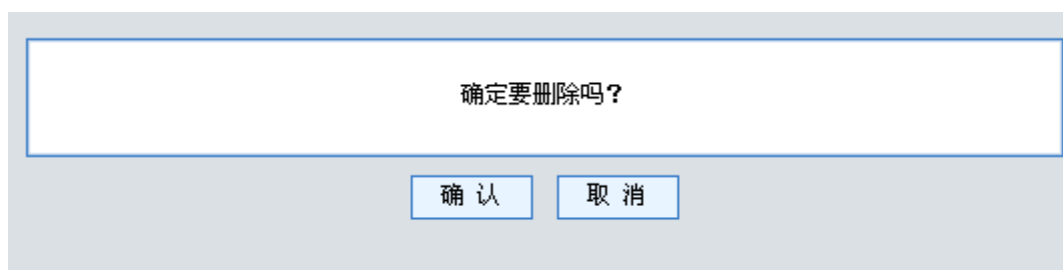


图 6-48 删除长连接

第7章 资源定义

为了简化 Guard 的配置和维护工作，引入了资源定义。Guard 系统可以定义以下资源：

- 地址：地址列表、地址组、服务器地址
- 服务：服务对象、ICMP 服务、基本服务、服务组、ALG 定义
- 时间：时间列表、时间组

7.1 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。

7.1.1 地址列表



图 7-1 地址列表

地址列表中的地址对象可在以下配置中使用：

- 资源定义：地址->地址组。
- Guard：包分类、DNAT 策略、安全策略、本地服务、连接数控制>>静态学习规则、连接数控制->动态学习规则。

可以按两种方式定义地址：

- IP 地址/掩码
- 地址范围 IP1 - IP2。

注意：

为了避免误操作，这里不支持全网段配置，即 IP 地址不可定义为 0.0.0.0。

如下图所示：

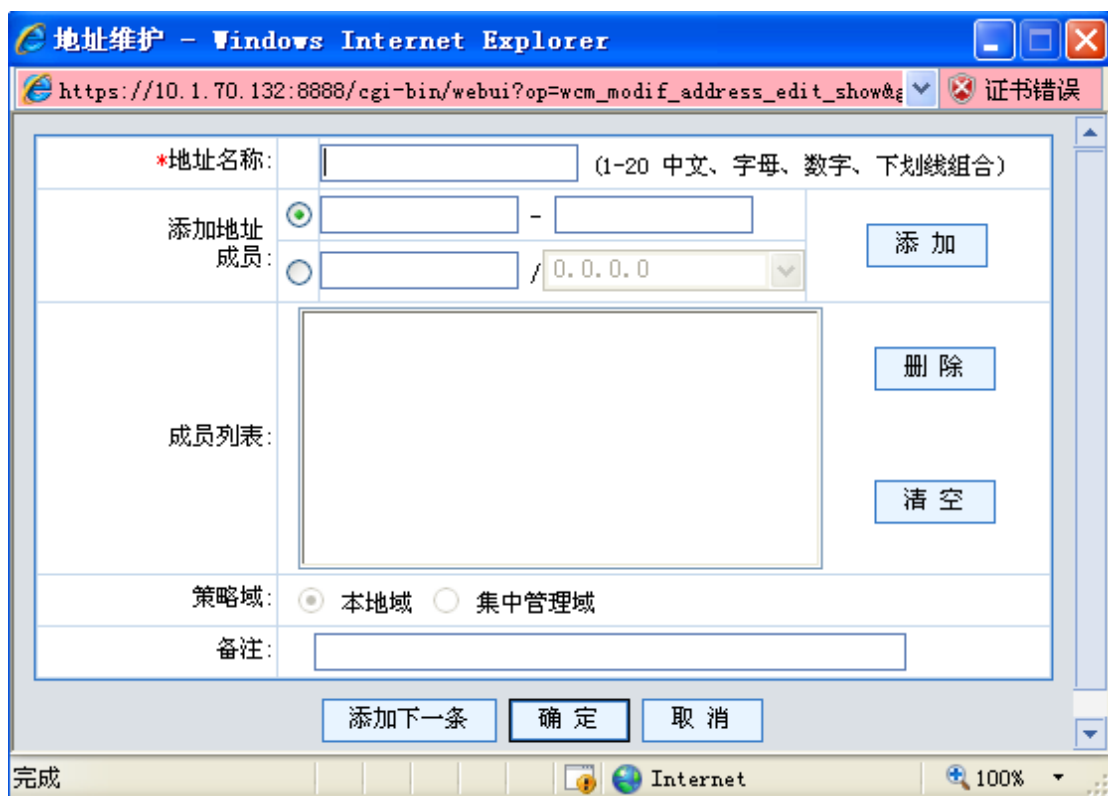


图 7-2 地址维护

表 7-1 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 如果希望指定一台主机，请选择掩码为 255.255.255.255
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

注意：

可以定义 A 类、B 类和 C 类地址。

7.1.2 地址池

地址池页面用于对地址池对象进行增加，修改，查询和删除的操作，还可以选择多个地址池对象，进行批量删除。

地址池列表页面如图：



图 7-3 地址池列表

地址池添加页面如图：

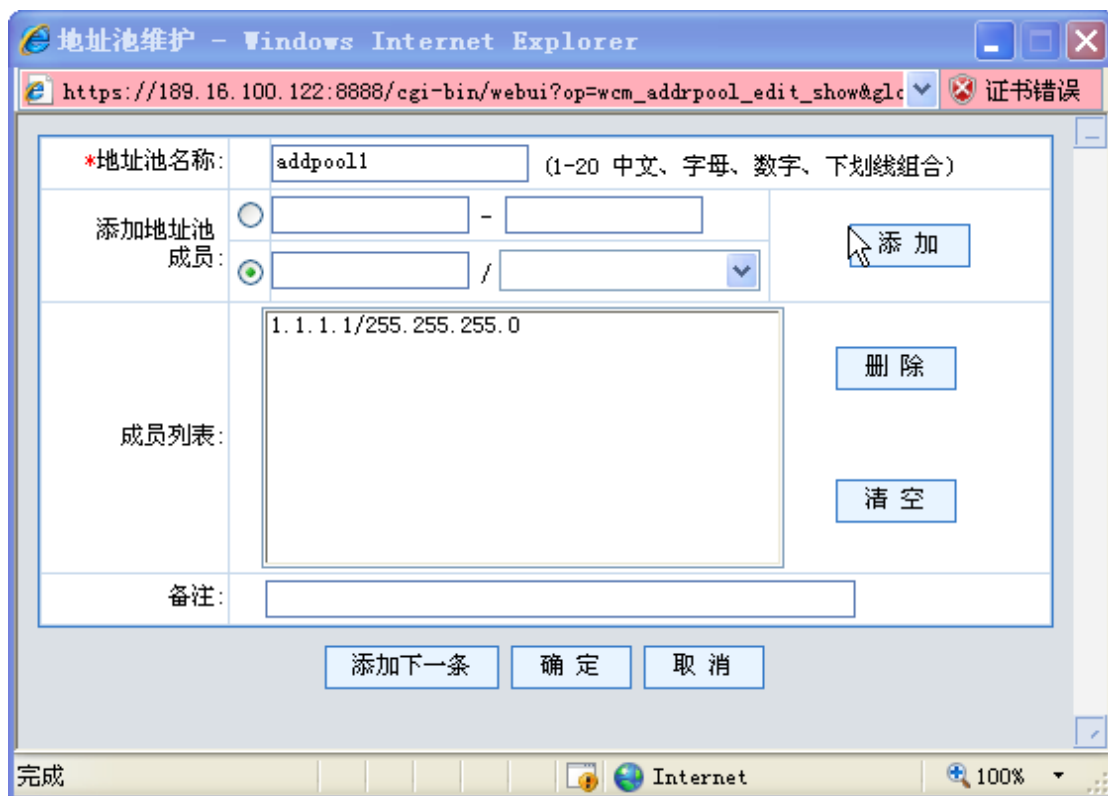


图 7-4 地址池添加页面

一个地址池对象可以添加多个地址池成员，地址池成员可以为 ip 段的方式，也可以是 ip 和掩码的方式。

7.1.3 地址组



图 7-5 地址组列表

地址组可在“防火墙”的下列配置中使用：

- 包分类

- DNAT 策略
- 安全策略
- 本地服务

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“添加”，将弹出以下界面：






图 7-6 地址组添加

表 7-2 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”中和“资源定义->地址->服务器地址”中定义的地址。 属于地址列表的成员被移动到地址组成员列表之后，将不再显示于原列表中。
地址组成员	该地址组的所有成员。

表 7-3 添加、删除成员

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
-----------------------------------------------------------------------------------	---------	-----------------------------------------------------------------------------------	----------------

注意：

Ctrl+鼠标左键，可选择列表中的多项一起操作。

7.1.4 服务器地址

“服务器地址”用于指定一组内部服务器地址。

序号	名称	服务器IP地址/权重	策略域	备注	操作
<input type="button" value="添加"/>					

全选

第1页/1页 跳转到 页 每页 行

图 7-7 服务器地址列表

在“资源定义->地址->服务器地址”，点击“添加”，将弹出以下界面：



图 7-8 服务器地址添加

表 7-4 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。
负载均衡权值	可输入的范围是 0—2147483647。系统将根据权值的大小和该服务器当前的流量负载来决定是否需要将任务切换至其他服务器，避免单个服务器无法承担过大的流量。 权值越大，意味着相应的服务器可承担的负载越大；权值越小，则服务器可承担的负载越小。权值为 0，则表示系统不会针对该服务器执行负载均衡策略。

7.2 服务

服务用于指定“协议 + 源端口 + 目的端口”，主要包括以下五种服务：

- 常用服务：包括 dns, gre, http, https, ICMP-any, igmp, igmp, ispf, oicq, pop3, smtp, snmp, syslog, tcp-any, telnet, udp-any 等
- ICMP 服务：可指定 type 和 code
- 基本服务：可以设置“协议 + 源端口 + 目的端口”
- 服务组：把以上服务组合起来，形成一个服务组
- ALG：目前支持 FTP 协议

以下两处用到服务资源：

- “防火墙”下的：包分类、DNAT 策略、安全策略、本地安全策略
- “资源定义”下的：用户->用户列表

7.2.1 服务对象定义

服务对象定义了一些常用的服务，不可以修改，删除，只可以被引用。

序号	名称	策略域	协议	端口	服务简介
1	dns	本地域	17	53	
2	gre	本地域	47	0	
3	http	本地域	6	80	www service
4	https	本地域	6	443	
5	icmp_any	本地域	1	0	icmp service
6	igmp	本地域	2	0	
7	igmp	本地域	88	0	
8	oicq	本地域	17	8000	
9	ospf	本地域	89	0	
10	pop3	本地域	6	110	

第1页/2页 跳转到 1 页 Go 每页 10 行

图 7-9 预定义服务列表

7.2.2 ICMP 服务

服务列表显示当前的 ICMP 服务。



图 7-10 ICMP 服务列表

添加窗口为：

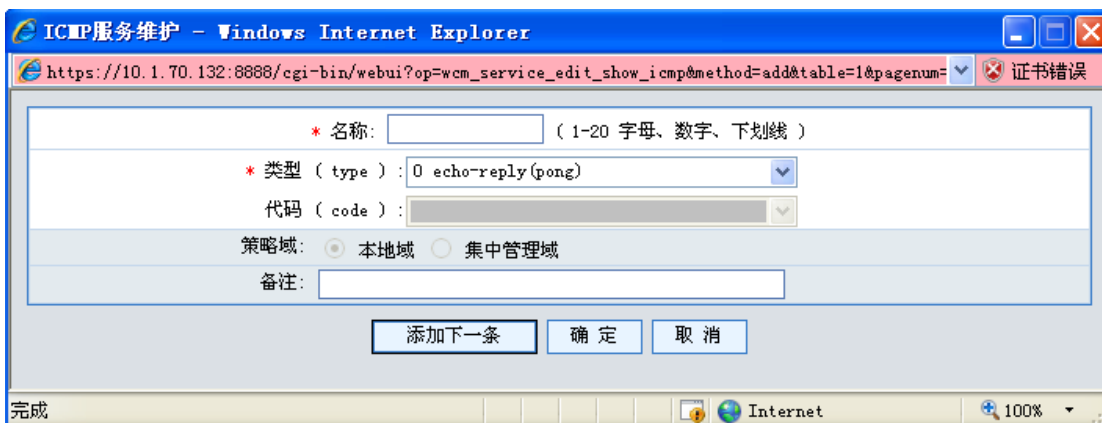


图 7-11 ICMP 服务添加

表 7-5 ICMP 服务添加元素表

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

7.2.3 基本服务

列表中显示了当前已定义的所有基本服务。



图 7-12 基本服务列表

点击“添加”，将弹出以下界面：



图 7-13 基本服务添加

表 7-6 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 1 到 65535 源端口通常设为 1-65535，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 1 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 1-65535，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 1-65535。
--	-------------------------------------------------------

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。

7.2.4 服务组

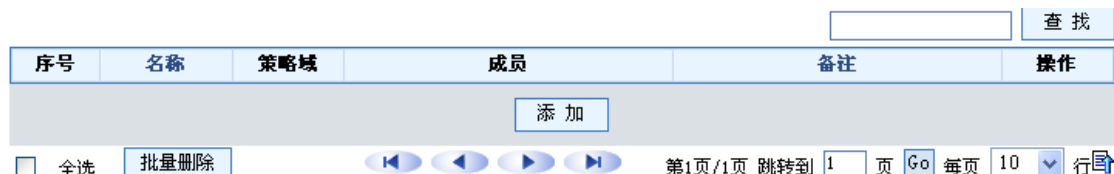


图 7-14 服务组列表

服务组用于“防火墙”下的：包分类、DNAT 策略、安全策略。

服务组的成员可以是“资源定义->服务”中已经定义过的服务对象、ICMP 服务和基本服务。

在“资源定义->服务->服务组”，点击“添加”，将弹出以下界面：



图 7-15 服务组添加

表 7-7 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”中定义的所有服务，包括“服务对象定义”“ICMP 服务”“基本服务”。 本列表的成员被移动到服务组成员列表中之后，将不再显示于本列表中。
服务组成员	列出本组的所有成员。

表 7-8 服务组添加、删除成员列表

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

7.2.5 ALG 定义

由于某些应用协议需要创建动态连接，而创建连接所用的 ip 地址和端口是动态的，为了监视该类协议，这里引入了 ALG (application layer gateway) 即应用层网关。目前支持 ftp, tftp, h.323, h.323gk, mms, rtsp, pptp, rtsp, xdmcp, sip 共 10 种协议。

序号	服务名	端口	是否启用	操作
1	ftp	21	✓	 
2	h323	1720	✓	 
3	h323gk	1719	✓	 
4	mms	1755	✓	 
5	pptp	1723	✓	 
6	rtsp	554	✓	 
7	sip	5060	✓	 
8	tftp	69	✓	 
9	tns	1521	✓	 
10	xdmcp	177	✓	 

图 7-16 ALG 定义列表

对 ALG 定义列表可选的操作有启用/关闭、编辑和恢复默认设置三项。

选中点击“编辑”，将执行编辑操作，并弹出以下界面：



图 7-17 ALG 配置

表 7-9 ALG 添加元素表

值域	说明
端口	协议使用的端口 可输入范围是 1-65535，最多允许设置 8 个，且端口值不可重复
是否可重定向	是否开启 ftp 协议的端口重定向功能 在方框内选中即为开启，反之则关闭

注意：

设置多个端口时，必须用英文逗号分隔，且端口值不可重复。

选中点击“撤销”，将执行恢复默认设置操作，当前配置将被默认配置覆盖。默认情况下，ftp 协议的端口值为 21，可重定向功能开启。

7.3 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。还可以把多个时间段组合成时间组。

定义的时间和时间组可在“防火墙”的以下几处配置中应用：包分类、DNAT 策略、安全策略。

7.3.1 时间列表

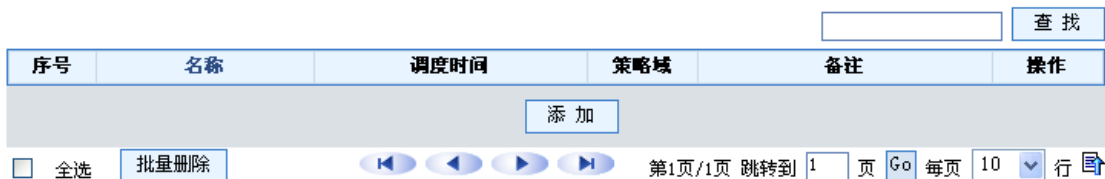


图 7-18 时间列表

可以按照一次性调度和周循环调度两种方式，来定义时间。点击“添加”，如下图所示：

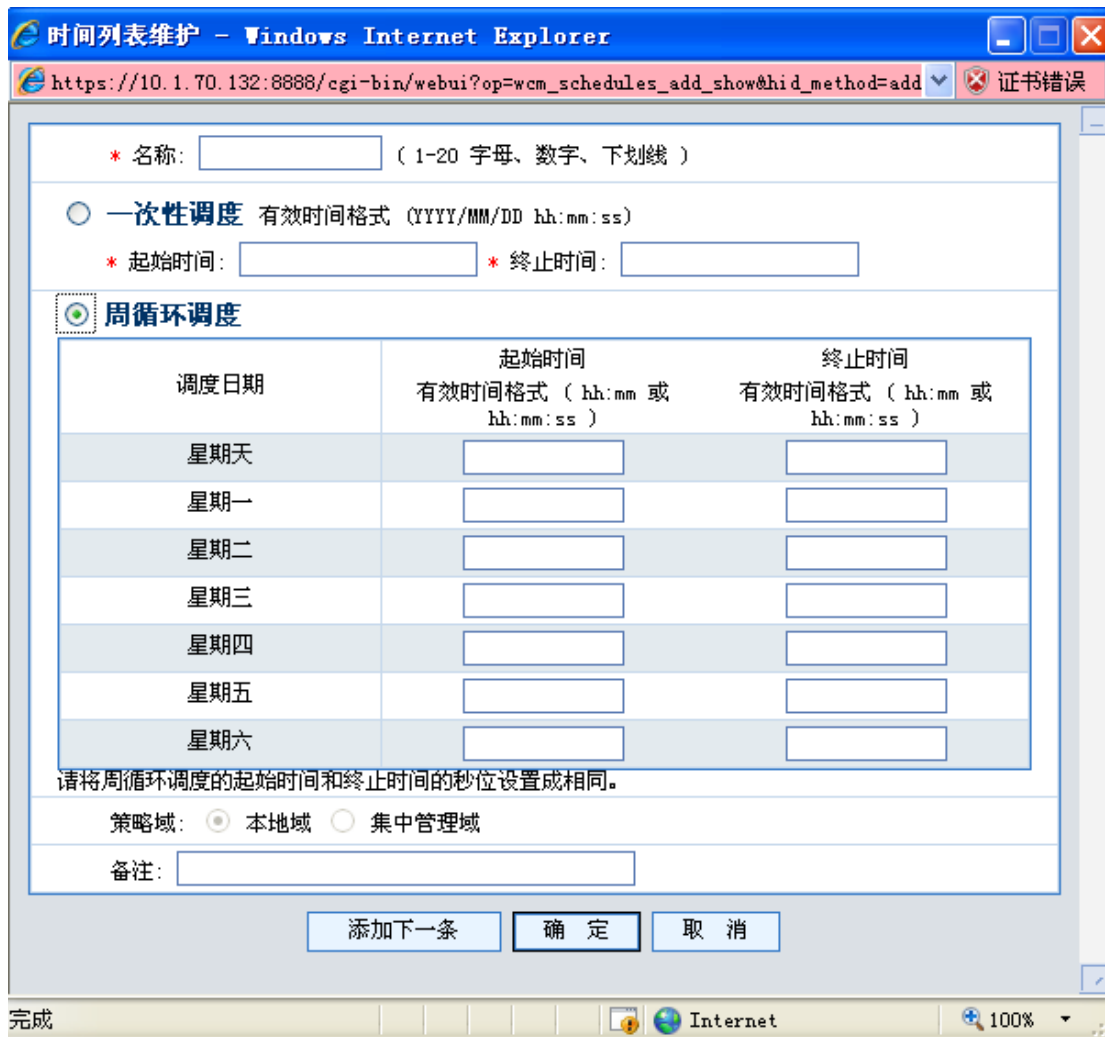


图 7-19 时间资源维护

表 7-10 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“Guard”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。则可以定义一个时间段 worktime 表示工作时间，再在“Guard>>包分类”中定义一个包分类，源地址和目的地址均设为“any”，服务对象选择“HTTP”，时间调度引用 worktime，在安全策略中添加一条规则，引用这个包分类并设置 Guard 策略为阻止即可。

7.3.2 时间组



图 7-20 时间组列表







图 7-21 时间组维护

表 7-11 时间组维护添加元素表

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	该时间组的所有成员。

表 7-12 时间组维护添加、删除成员

操作	说明
	添加成员，点击  把选中的时间移动到成员列表 时间列表成员添加至时间组之后，该成员不再显示于时间列表中。
	删除成员，点击  把选中的成员移动到时间列表中

7.4 应用协议

7.4.1 应用协议

点击 资源定义/应用协议选项在如下图的应用协议表中可以查看特征库中对应的应用协议名称和对应的协议 ID 号。

序号	名称	协议ID
1	ftp	1
2	h323	2
3	h323gk	3
4	mms	4
5	pptp	5
6	rtsp	6
7	sip	7
8	tftp	8
9	tns	9
10	xdmcp	10


第1页/14页 跳转到 页 每页 行 

图 7-22 应用协议表

7.4.2 应用协议组

点击资源定义/应用协议/应用协议组，进入应用协议组表其中 audiovideo、p2p、im、stock、normal_server、game 等 5 大类协议，其中每个大类协议中又包括几十种小类协议，见下图：

序号	名称	成员列表	类型	备注	操作
1	audiovideo	pplive qqlive ppstream ppmate feidian uusee xunleikankan sopcast funshion youku.com tudou.com ku6.com 56.com 6.cn SinaVideo kwmusic kugoomusic qianqianmusic qqmusic cctvbox qqmusicradio moshoushijie fankongjingying tiantang hianfens	预定义	audiovideo	

图 7-23 应用协议组表

7.5 包分类

包分类显示页面：

可以根据序号排名显示，显示包括几个缩略参数，源地址、目的地址、服务和协议等。

可以分屏显示，支持翻页功能等。

界面如下图所示：

按条件查询

序号	分类名	源地址	目的地址	服务	协议	内网地址	外网地址	生效时间状态	操作
<input type="checkbox"/>	1	ipqos	192.0.0.0/255.0.0.0					未配置	
<input type="checkbox"/>	2	df	1.2.3.3/	5.6.6.6/	gre			未配置	
<input type="checkbox"/>	3	snat	100.100.100.0/255.255.255.0					未配置	

添加

全选 第1页/1页 跳转到 页 每页 行

图 7-24 包分类显示

包分类添加页面：

根据包分类支持的几个元素定义分类规则。

具体参数如下图所示：



添加包分类规则 - Windows Internet Explorer

https://10.1.70.132:8888/cgi-bin/webui?op=wcm_pcp_edit_show&method=add&global=

* 分类名: (1-20 字母、数字、下划线)

源地址: IP 地址 地址取反 掩 码 起始地址 结束地址

目的地址: IP 地址 地址取反 掩 码 起始地址 结束地址

内网地址: IP 地址 地址取反 掩 码 起始地址 结束地址

外网地址: IP 地址 地址取反 掩 码 起始地址 结束地址

服务: 服务对象 协议 (自定义服务) 协议名字 协议范围 源 端口 目的端口

流入网口: 流出网口:

策略所在地: 本地 集中管理

时间调度:

只有协议为tcp或udp时,设置端口才有效,端口可以用冒号(:)分隔表示端口段

图 7-25 包分类显示

包分类添加页面还有一个高级选项，可以定义一些不常用的参数配置。

点开后面界面如下图所示：

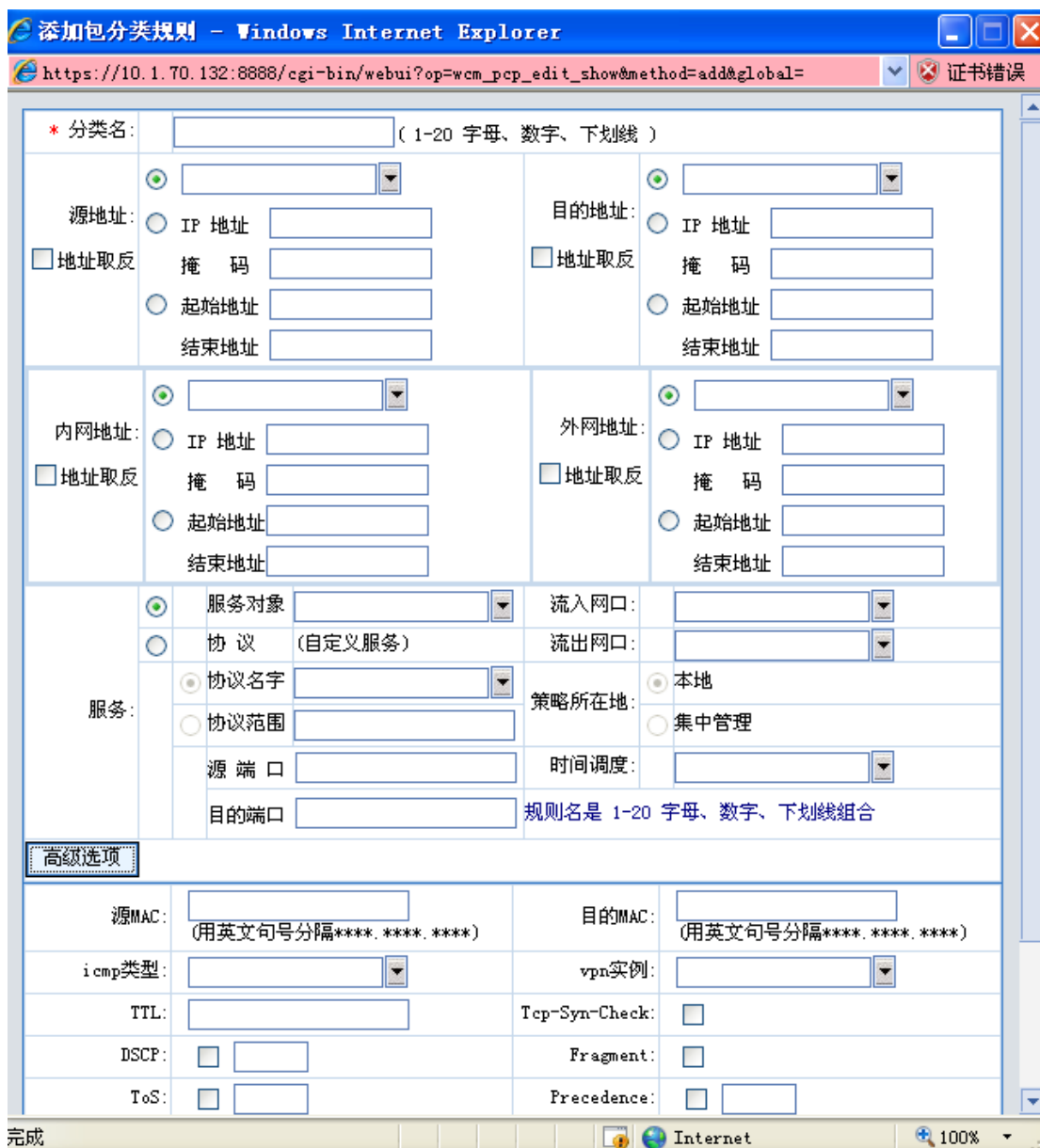


图 7-26 带有高级选项的包分类添加

包分类页面还有修改、排序、删除功能，
如下图所示：



图 7-27 包分类的修改、排序、删除功能示意图

包分类修改页面：



图 7-28 包分类修改

删除页面：

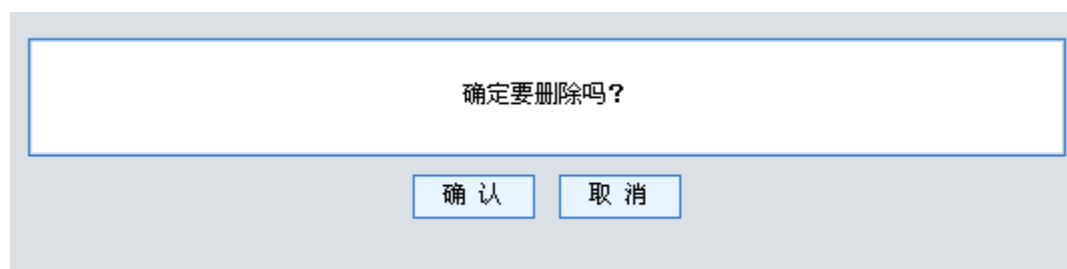


图 7-29 包分类删除

第8章 流量牵引

本章是异常流量清洗系统 Guard 配置的重点。制定符合安全需求的流量牵引和清洗策略是保证 Guard 真正起到防护作用的基础。配置错误的流量牵引规则不仅会使 Guard 系统形同虚设，甚至有可能妨碍对网络正常功能的使用。

8.1 BGP 牵引

8.1.1 BGP 本地配置



图 8-1 BGP 参数配置

数据域说明：

表 8-1 BGP 参数配置数据域说明

域名	说明
本地 AS 号	本地自治系统(Autonomous System) 编号，范围为 1-65535
本地路由标识	本地的路由 ip 标识

功能说明：

表 8-2 BGP 参数配置功能说明

域名	说明
确定	确认配置生效

此界面可以完成以下功能：

- 配置本地 AS 号
- 设置本地路由标识

8.1.2 BGP 邻居配置

网络配置 >> 路由牵引 >> BGP 邻居配置

邻居IP地址	邻居AS号	下一跳次数	通信接口	映射名称	操作
7.7.7.1	1	200	6.6.6.1	qq	
2.2.2.2	7675	0			
2.3.32.2	7675	0			

第1页/1页 跳转到 页 每页 10 行

图 8-2 BGP 邻居配置页面

数据域说明：

表 8-3 BGP 邻居配置数据域

域名	说明
邻居 IP 地址	邻居 IP 地址
邻居 AS 号	邻居 AS 号
下一跳次数	下一跳的跳跃次数
通信接口	通信接口的 ip 地址
映射名称	可以选择在路由映射页面配置的映射名称

此界面可以完成以下功能：

- 添加 BGP 邻居
- 编辑 BGP 邻居
- 删除 BGP 邻居

添加 BGP 邻居

- 点“添加”按钮，进入“BGP 邻居维护”
- 添加 BGP 邻居参数
- 点“确定”按钮完成添加



* 邻居IP地址:	<input type="text"/>
* 邻居AS号:	<input type="text"/> (1-65535)
下一跳次数:	<input type="text"/> (1-255)
BGP会话协商接口地址:	<input type="text"/>
禁止路由同步地址:	<input type="text"/>
路由映射:	<input type="text"/>
下发方向:	<input type="text" value="out"/>
传递社团属性:	<input checked="" type="checkbox"/>

添加下一条 确定 取消

图 8-3 BGP 邻居配置添加页面

编辑 BGP 邻居



* 邻居IP地址:	<input type="text" value="7.7.7.1"/>
* 邻居AS号:	<input type="text" value="1"/> (1-65535)
下一跳次数:	<input type="text" value="200"/> (1-255)
BGP会话协商接口地址:	<input type="text" value="6.6.6.1"/>
禁止路由同步地址:	<input type="text"/>
路由映射:	<input type="text" value="qq"/>
下发方向:	<input type="text" value="out"/>
传递社团属性:	<input checked="" type="checkbox"/>

添加下一条 确定 取消

图 8-4 BGP 邻居配置编辑页面

删除 BGP 邻居:

- 点“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

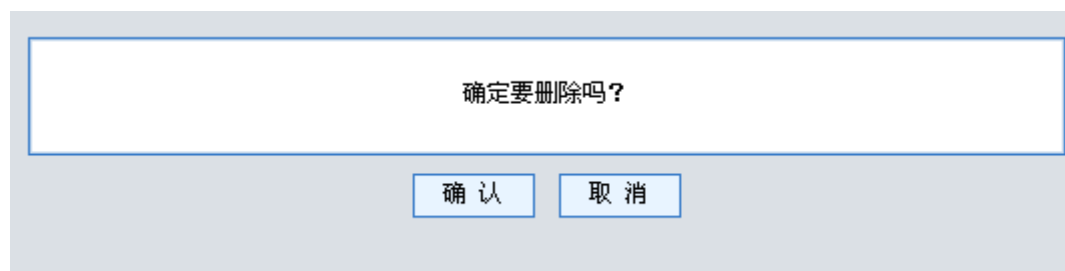


图 8-5 BGP 邻居删除页面

8.1.3 访问控制链表

网络配置>>路由牵引>>访问控制链表

链表名称	IP地址/掩码位数	类型	操作
aa	2.2.2.2/24	permit	<input type="checkbox"/> <input type="checkbox"/>
	2.4.2.2/32	permit	

跳转到 页 每页 行

图 8-6 访问控制链表显示页面

数据域说明：

表 8-4 访问控制链表数据域说明

域名	说明
链表名称	访问控制链表名称
IP 地址/掩码位数 类型	访问控制链表的参数。

此界面可以完成以下功能：

- 添加访问控制链表
- 编辑访问控制链表
- 删除访问控制链表

添加访问控制链表

- 点“添加”按钮，进入“访问链表维护”
- 添加访问链表参数
- 点“确定”按钮完成添加



图 8-7 访问控制链表添加页面

编辑访问链表



图 8-8 访问控制链表添加页面

删除访问链表:

- 点“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

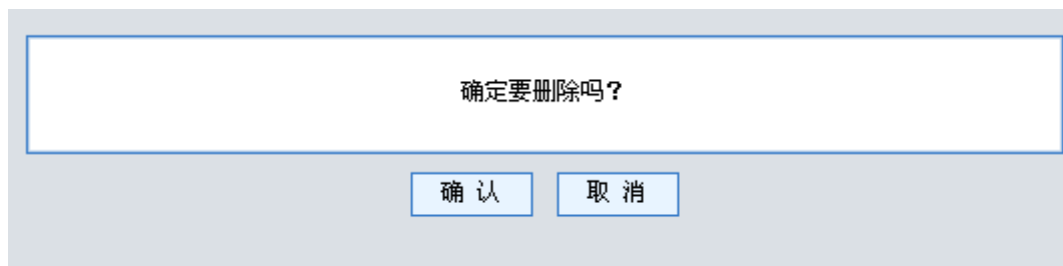


图 8-9 访问控制链表删除页面

8.1.4 路由映射

网络配置>>路由牵引>>路由映射



映射名称	访问控制名称	目的地址	类型	编号	社团属性	操作
qq	aa	3.3.3.3	permit	1	local-AS	✎ 🗑
	aa	4.4.4.4	permit	2	333:444	

添加

第1页/1页 跳转到 1 页 Go 每页 10 行

图 8-10 路由映射显示页面

数据域说明：

表 8-5 路由映射数据域说明

域名	说明
映射名称	路由映射的名称
访问控制名称 目的地址 类型 编号 社团属性	路由映射的具体参数，访问控制名称就是在访问控制链表页面所创建的链表名称。

此界面可以完成以下功能：

- 添加路由映射
- 编辑路由映射
- 删除路由映射

添加路由映射

- 点“添加”按钮，进入“路由映射维护”
- 添加路由映射参数
- 点“确定”按钮完成添加



图 8-11 路由映射添加页面

编辑路由映射



图 8-12 路由映射编辑页面

删除路由映射：

- 点“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

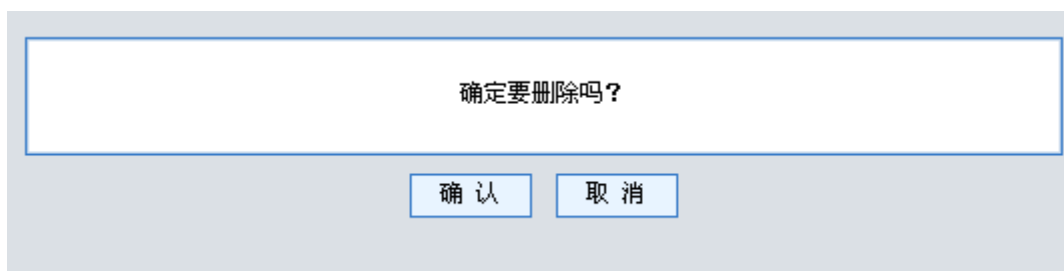


图 8-13 路由映射删除页面

8.1.5 路由牵引配置



图 8-14 路由牵引配置页面

数据域说明:

表 8-6 BGP 参数配置数据域说明

域名	说明
IP 地址	需要牵引的 IP 地址
掩码	需要牵引的掩码
静态路由	牵引完数据默认回注的静态路由

此界面可以完成以下功能:

- 添加路由牵引
- 编辑路由牵引
- 删除路由牵引

添加路由牵引

- 点“添加”按钮，进入“路由牵引配置”
- 添加路由牵引参数
- 点“确定”按钮完成添加

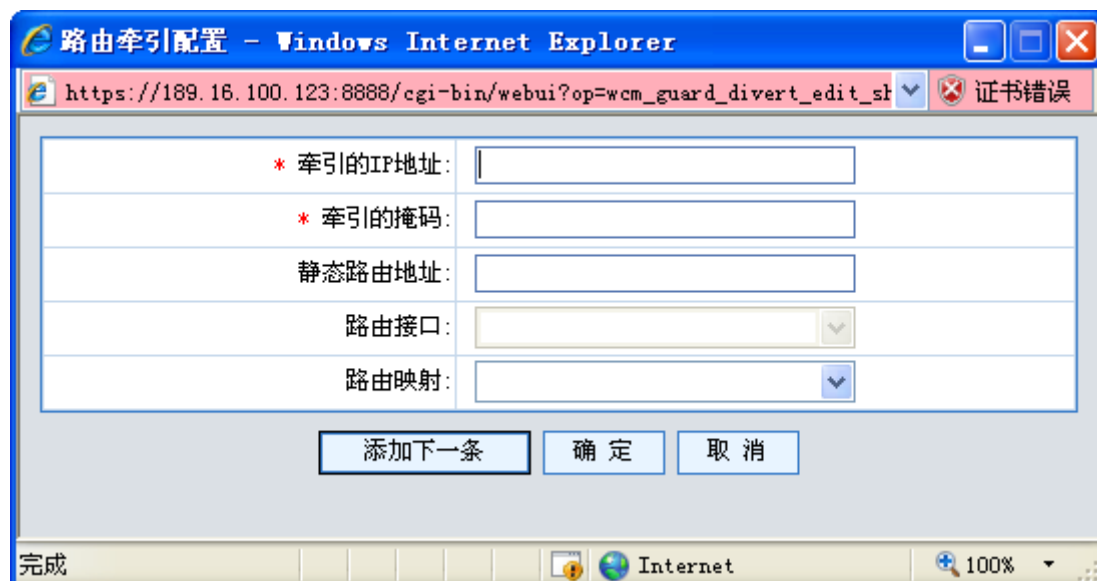


图 8-15 路由牵引配置添加页面

编辑路由牵引

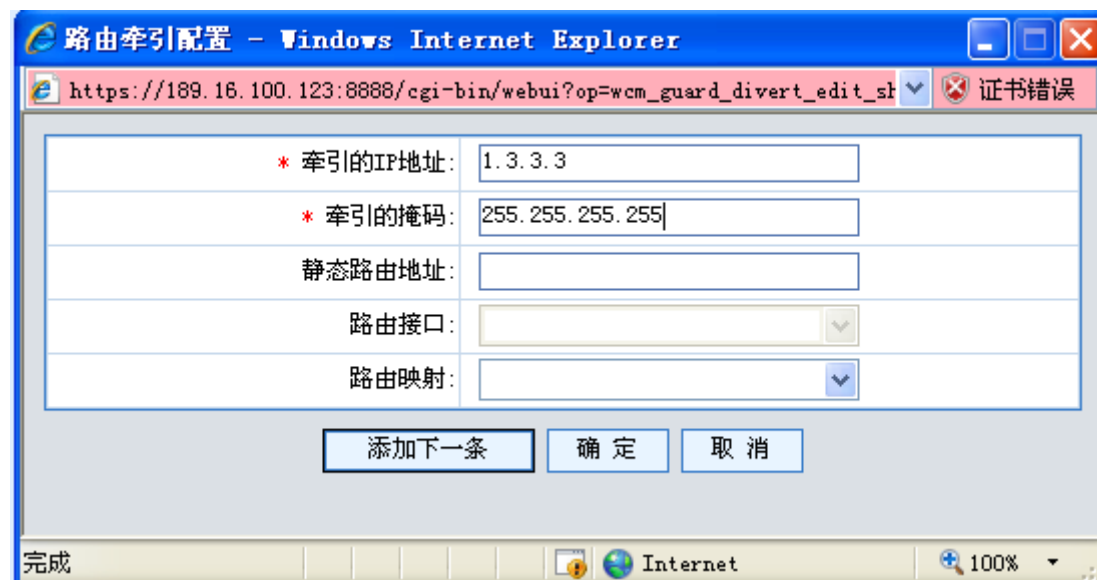


图 8-16 路由牵引配置编辑页面

删除路由牵引:

- 点“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

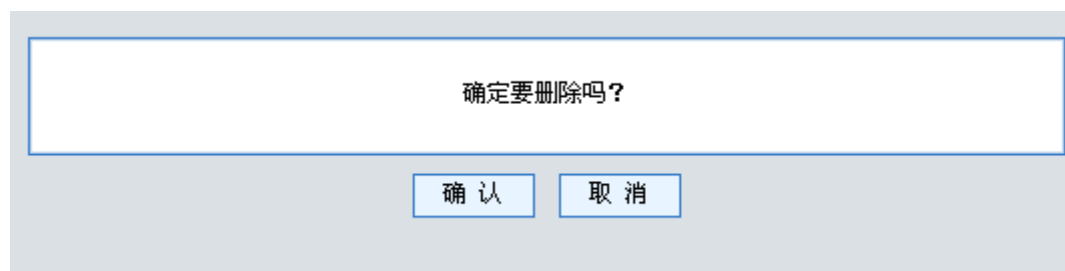


图 8-17 路由牵引配置删除页面

8.2 OSPF

Guard 提供 OSPF 功能，能够与其它支持 OSPF 功能的网络设备进行动态路由协商。

在 OSPF 页面上，可以配置路由重分发，启动、停止 OSPF 功能，设置路由器 ID，添加、删除区域，设置区域认证方式，添加、删除网络，添加、删除网络接口认证口令。

Router ID					
路由器ID: <input type="text" value="0.0.0.0"/>					
		<input type="button" value="确定"/>		<input type="button" value="清除"/>	

区域		
区域	认证	操作
<input type="button" value="添加区域"/>		

网络		
网络	区域	操作
<input type="button" value="添加网络"/>		

接口					
接口	代价	优先级	Hello间隔	失效间隔	操作
<input type="button" value="添加接口"/>					

认证				
接口	认证方式	Message-digest ID	密码	操作
<input type="button" value="添加接口"/>				

图 8-18 OSPF 配置页面

8.2.1 配置路由重分发

打开 OSPF 界面时，将显示已经重分发的路由（bgp、直连、静态、rip）。如需修改，将对应的选项框选中或取消，然后点击确定即可生效。

8.2.2 启动、停止 OSPF 功能

OSPF 功能未启动时，会显示“启动”按钮，点击后会启动 OSPF 功能。

OSPF 功能启动后，会显示“停止”按钮，点击后会停止 OSPF 功能。

8.2.3 修改路由器 ID

修改路由器 ID 后，需要点击“启动/停止”按钮以使其生效。

8.2.4 设置区域



The dialog box for adding an OSPF area. It contains two input fields: '*区域 (IP):' and '*认证:'. The '*认证:' field has a dropdown menu with 'Null' selected. At the bottom, there are three buttons: '添加下一条', '确定', and '取消'.

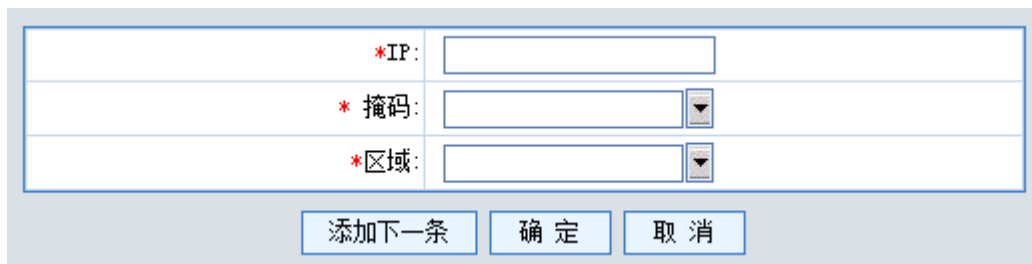
图 8-19 OSPF 添加区域对话框

添加区域时，需要指定区域名（可使用十进制形式或 IP 地址形式）和认证方式，认证方式可选择不认证、明文口令认证、消息摘要认证。最多可以添加 255 个区域。

添加区域后，可以修改其认证方式。

可以删除区域，添加了网络的区域不能被删除。

8.2.5 设置网络



The dialog box for adding an OSPF network. It contains three input fields: '*IP:', '*掩码:', and '*区域:'. The '*掩码:' and '*区域:' fields have dropdown menus. At the bottom, there are three buttons: '添加下一条', '确定', and '取消'.

图 8-20 OSPF 添加网络对话框

添加网络时，需要指定 IP 地址和掩码，以及所属区域。最多可以添加 255 个网络。

可以删除网络。

8.2.6 设置网络接口认证

*接口:	Ge0/0/0	▼
*认证:	Text	▼
*密码:	<input type="text"/>	(1-8 字符)

图 8-21 OSPF 添加网络接口明文口令对话框

*接口:	Ge0/0/0	▼
*认证:	Message-digest	▼
*Message-digest 密钥ID:	<input type="text"/>	(1-255)
*Message-digest 密钥:	<input type="text"/>	(1-16 字符)

图 8-22 OSPF 添加网络接口消息摘要密钥对话框

添加明文口令时，需要指定密码。添加消息摘要密钥时，需要指定 ID 和密钥。每个网口接口最多可以添加 1 个明文口令和 255 个消息摘要密钥。所有网络接口的明文口令和消息摘要密钥的总数最多为 255 个。

可以删除明文口令和消息摘要密钥。

第9章 流量分析

流量自学习功能是对网络中的正常流量进行统计、分析和计算。一般使用时，可以在上线之初，选择学习模板，打开自学习功能，运行一段时间（最多学习 7 天）后帮助管理员做高级抗攻击的配置。

因此，自学习功能包括了：

- 选择学习模板；
- 输出学习结果；
- 记录学习过程数据；
- 应用/撤销学习结果到高级型抗攻击；

9.1 自学习配置

9.1.1 学习配置

用于查看自学习当前配置情况



包分类规则	自学习时间	学习模板					状态	操作
		IP	ICMP	TCP	UDP	应用层		
p1	0天 1 小时	●	●	●	●	●		

添加

第1页/1页 跳转到 1 页 Go 每页 10 行

图 9-1 自学习配置

图标说明：

表 9-1 流量自学习图标说明

域名	说明
	停止当前正在学习的自学习策略
	重新开始自学习策略
	编辑自学习策略
	删除自学习策略

数据域说明：

表 9-2 流量自学习数据域说明

域名	说明
包分类规则	包分类规则名称, 符合命名规则
流量自学习时间	在添加页面设置的自学习时间
学习模板	在添加页面设置的自学习模板

添加流量自学习配置

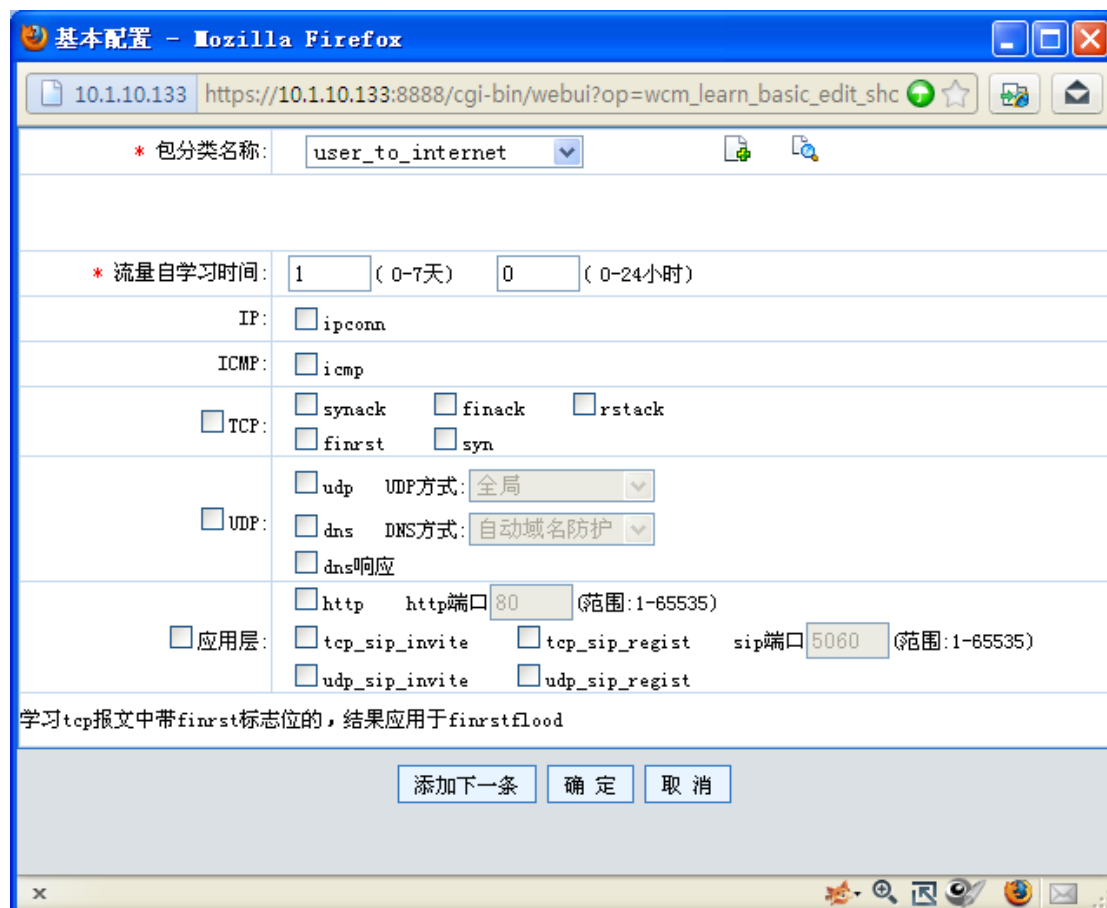


图 9-2 添加流量自学习配置

表 9-3 流量自学习添加项说明

域名	说明
包分类规则名称	选择一个已有的包分类规则, 选择后可以在下面看到相关配置。
流量自学习时间	设置学习时间
学习模板	选择需要学习的模板

9.1.2 学习过程

包分类名称	IP		ICMP		TCP		UDP		应用层		操作
p1	ipconn		icmp		synack		udp源		http		生成快照
					finack		udp全局		tcp_sip_invite		
					rstack		dns响应		tcp_sip_regist		
					finrst		dns全局		udp_sip_invite		
					syn		自动域名防护		udp_sip_regist		

第1页/1页 跳转到 1 页 Go 每页 10 行

图 9-3 学习过程

9.2 自学习管理

自学习管理主要用于查看学习结果、中间快照和历史学习结果；查看学习过程中个模板的流量曲线图；查看当前应用情况和历史应用情况。支持的学习结果的应用和撤销。

9.2.1 学习结果

学习结束后生成学习结果。

包分类名称	IP		ICMP		TCP		UDP		应用层		操作	查看历史学习结果与快照	与历史学习结果比较
p1	ipconn	0	icmp	3000000	synack	5000	udp源	0	http	500	应用	查看	比较
					finack	3000	udp全局	--	tcp_sip_invite	0			
					rstack	0	dns响应	0	tcp_sip_regist	0			
					finrst	0	dns全局	0	udp_sip_invite	200			
					syn	3000	自动域名防护	--	udp_sip_regist	0			

显示 "--" 表示未配置学习模板；显示 "0" 表示数据不足，无法学习；阈值显示为红色时，表示学习结果超过对应攻击上限值。

第1页/1页 跳转到 1 页 Go 每页 10 行

图 9-4 学习结果

点击应用时出现下面对话框：

确定应用此结果（其中0值应用为默认值，显示红色的应用为最大上限值）？

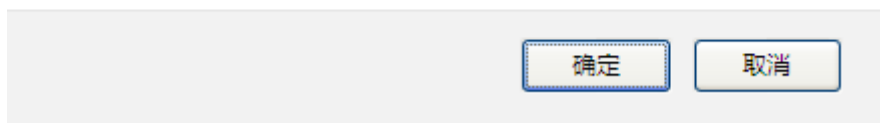


图 9-5 应用学习结果

点击查看，可查看历史学习记录和学习过程中的快照信息：

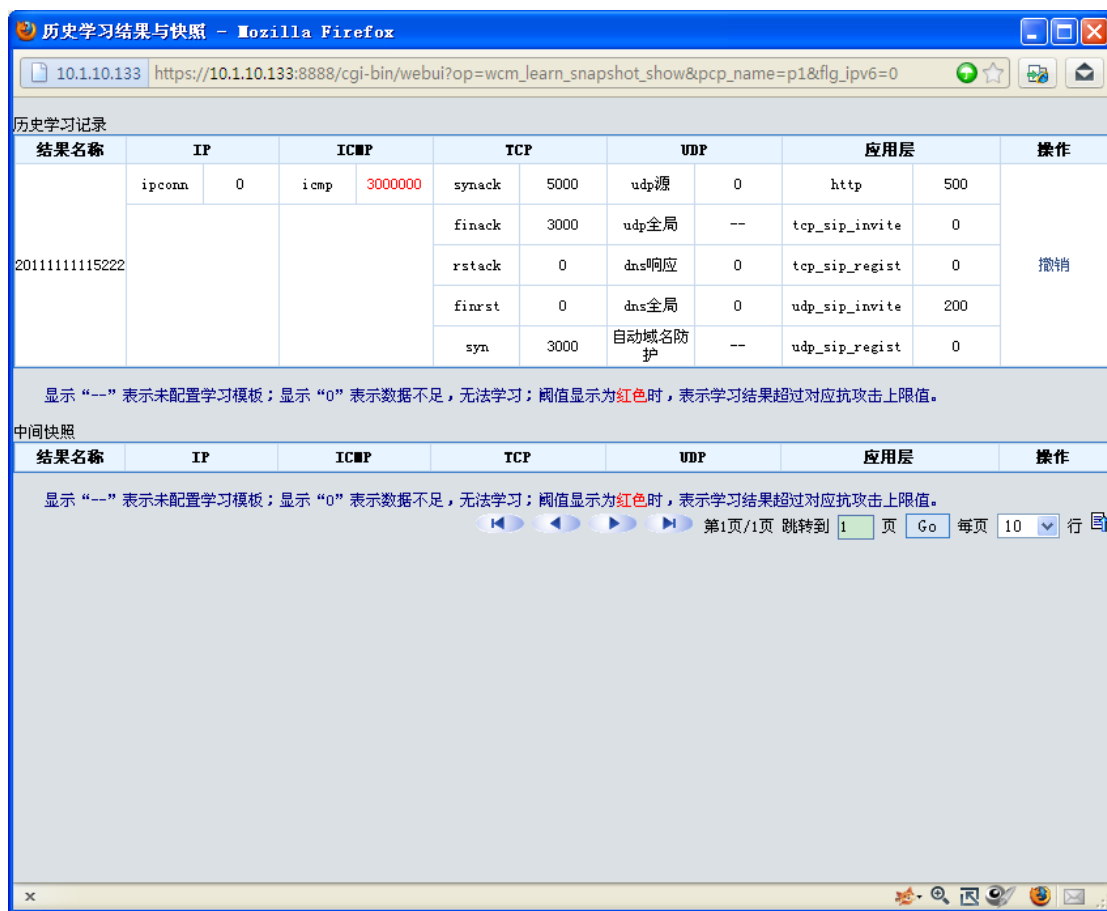


图 9-6 历史学习结果和中间快照

点击比较时，如果有历史学习结果，可显示历史学习结果与当前学习结果的比较

9.2.2 学习曲线

可查看学习过程中的曲线图。

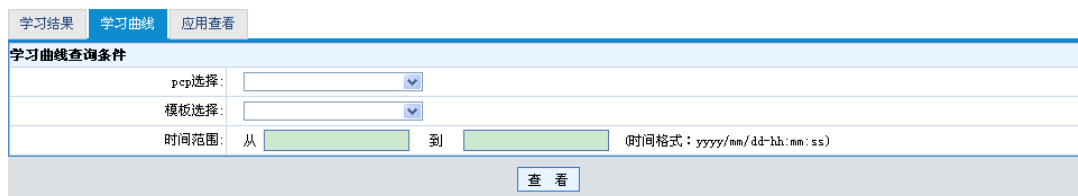


图 9-7 学习曲线

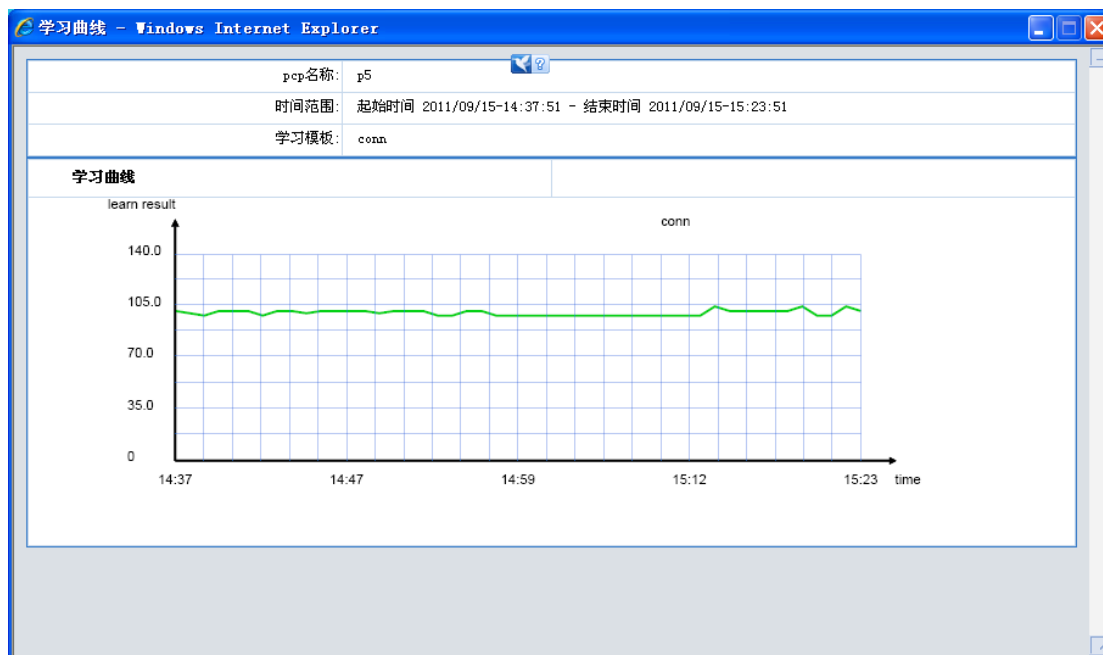


图 9-8 曲线图

9.2.3 应用查看

可查看当前应用和历史应用情况

查看当前应用 | 查看历史应用

包分类名称	IP		ICMP		TCP		UDP		应用层		操作
p1	ipconn	0	icmp	3000000	synack	5000	udp源	0	http	500	撤销
					finack	3000	udp全局	--	tcp_sip_invite	0	
					rstack	0	dns响应	0	tcp_sip_regist	0	
					finrst	0	dns全局	0	udp_sip_invite	200	
					syn	3000	自动域名防护	--	udp_sip_regist	0	

显示“-”表示未配置学习模板；显示“0”表示数据不足，无法学习；阈值显示为红色时，表示学习结果超过对应抗攻击上限值。

第1页/1页 跳转到 页 每页 10 行

图 9-9 应用查看

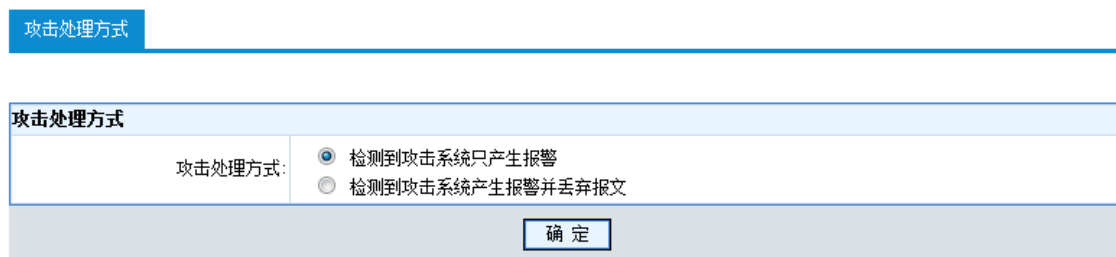
第10章 流量清洗

10.1 攻击处理方式

攻击处理方式页面可以对攻击事件处理设置，对攻击事件有两种处理方式：

1. 检测到攻击系统只产生报警
2. 检测到攻击系统产生报警并丢弃报文

攻击处理方式页面设置如下：



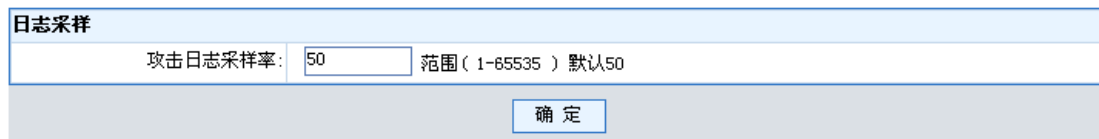
攻击处理方式	
攻击处理方式:	<input checked="" type="radio"/> 检测到攻击系统只产生报警 <input type="radio"/> 检测到攻击系统产生报警并丢弃报文
<input type="button" value="确定"/>	

图 10-1 攻击处理方式配置

10.2 日志采样

日志采样页面可以对攻击日志采样率进行设置，范围为 1-65535，默认为 50。

日志采样页面设置如下：



日志采样	
攻击日志采样率:	<input type="text" value="50"/> 范围(1-65535) 默认50
<input type="button" value="确定"/>	

图 10-2 抗攻击日志采样配置

10.3 攻击证据提取

10.3.1 攻击证据提取

攻击证据提取页面可以开启/关闭该功能，可以设置提取攻击报文的接口，设置攻击报文的采样率，采样率是一个 1-65535 的数字。

攻击证据提取	
<input type="checkbox"/> 是否提取攻击证据	攻击报文接口名: <input type="text"/> 攻击报文采样率: <input type="text"/> (范围1-65535, 默认100)
<input type="button" value="确定"/>	

图 10-3 证据提取配置

10.3.2 捉包分析取证

捉包分析取证页面可以用于添加，查询，修改和删除取证策略，并将抓包发送到指定 FTP 服务器上。

攻击证据提取		捉包分析取证			
* ftp服务器:	<input type="text"/>	* 端口:	<input type="text" value="21"/>		
* 用户名:	<input type="text"/>	* 密码:	<input type="text"/>		
<input type="button" value="确定"/> <input type="button" value="清空"/>					
			<input type="text"/> <input type="button" value="查找"/>		
包分类策略	最大包长	报文数量	抓包时间 (min)	采样率	操作
<input type="button" value="添加"/>					
<input type="button" value="⏪"/> <input type="button" value="⏩"/> 第1页/1页 跳转到 <input type="text" value="1"/> 页 <input type="button" value="Go"/> 每页 <input type="text" value="10"/> 行					

图 10-4 捉包分析取证

捉包分析取证的添加页面：

图 10-5 捉包分析取证的添加页面

添加策略时需要选择已经存在的 pcp，最大包长是 40-1534，报文数量时 1-10000，抓包时间是 1-60，采样率是 1-65535 的数字。

10.4 DNS 防护

10.4.1 域名列表

管理员可以通过域名黑名单对网络的域名访问进行控制，把某个域名加入黑名单来阻止对这个域名的访问。



图 10-6 域名黑名单配置

数据域说明

表 10-1 域名黑名单数据域说明

域名	说明
黑名单名称	域名列表名称。
域名	加入域名列表的域名。

此界面可以完成以下功能：

- 添加域名列表
- 编辑域名列表
- 删除域名列表

添加域名列表

- 点“添加”按钮，进入“域名列表维护”
- 添加域名列表参数
- 点“确定”按钮完成添加



图 10-7 域名黑名单添加

编辑页面:



图 10-8 域名黑名单编辑

删除页面:

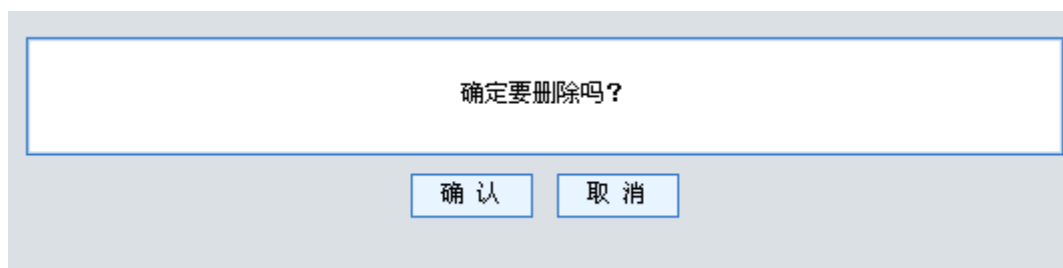


图 10-9 域名黑名单删除

10.4.2 域名访问限制

管理员可以通过域名访问限制对网络的域名访问进行控制,为某个域名设置相应的阈值超过这个阈值后的域名不允许访问。



图 10-10 域名访问控制配置

数据域说明

表 10-2 域名访问限制数据域说明

域名	说明
策略名称	域名访问限制策略名称。
域名/阈值	添加域名及其相应阈值

此界面可以完成以下功能:

- 添加域名访问限制
- 编辑域名访问限制
- 删除域名访问限制
- 添加域名访问限制
- 点“添加”按钮,进入“域名访问限制维护”
- 添加参数
- 点“确定”按钮完成添加



图 10-11 域名访问控制添加

编辑页面:



图 10-12 域名访问控制编辑

删除页面:

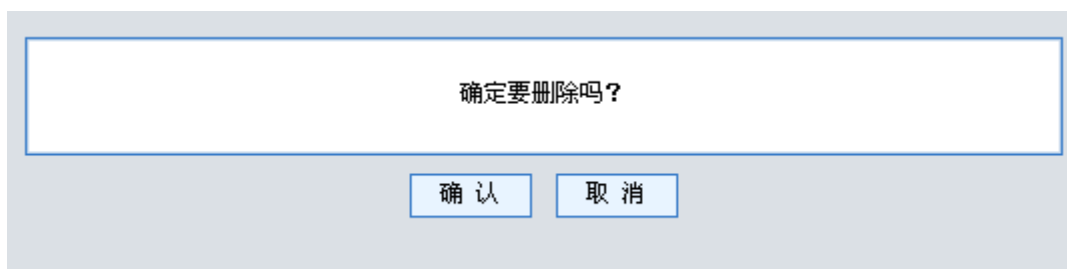


图 10-13 域名访问控制删除

10.4.3 DNS 攻击保护

管理员可以通过包分类的方式，对数据包进行分析，实现 DNS 检测和 DNS 防护的目的。

按条件查询

序号	分类名	源地址	目的地址	服务	dns检测	response flood	dns防护	操作
<input type="checkbox"/> 1	df	1.2.3.3/	5.6.6.6/	gre	✓	✗	✗	
<input type="checkbox"/> 2	ipqos	192.0.0.0/255.0.0.0			✓	✓	✓	

添加

全选 第1页/1页 跳转到 页 每页 行

图 10-14 DNS 攻击保护配置

数据域说明

表 10-3 DNS 防护数据域说明

域名	说明
分类名	包分类名称。
源地址	包分类中的源地址。
目的地址	包分类中的目的地址。
服务	包分类中的服务类型。
dns 检测	DNS 域名检查和 TTL 检测
response flood	DNS 响应报文抗攻击
dns 防护	DNS 请求报文抗攻击

此界面可以完成以下功能：

- 添加 DNS 攻击保护
 - 编辑 DNS 攻击保护
 - 删除 DNS 攻击保护
 - DNS 防护查询
- 添加 DNS 攻击保护
- 点“添加”按钮，进入“DNS 防护”
 - 添加参数
 - 点“确定”按钮完成添加

编辑页面：



图 10-15 DNS 防护编辑

删除页面:

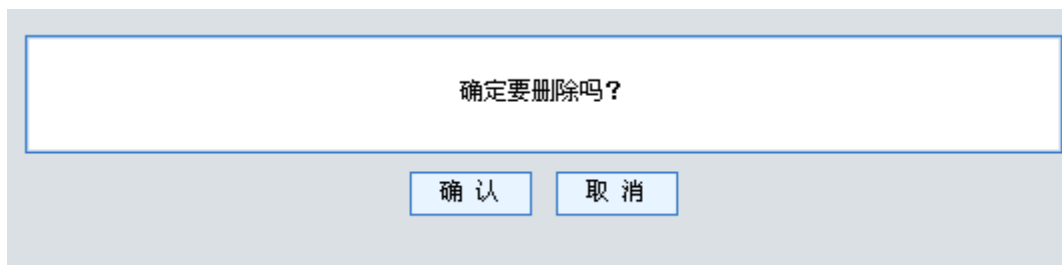


图 10-16 DNS 防护删除

DNS 防护查询

- 点“按条件查询”按钮，进入“dns 防护查询”
- 添加参数
- 点“确定”按钮完成查询

dns防护查询

dns防护查询	
分类名:	<input type="text"/>
源地址:	<input type="text"/> (可输入地址或地址对象)
目的地址:	<input type="text"/> (可输入地址或地址对象)
服务:	<input type="text"/> ▼
<input type="button" value="查找"/> <input type="button" value="返回"/>	

图 10-17 DNS 防护查询

10.4.4 域名长度参数

域名长度参数	
域名最大长度:	<input type="text" value="64"/> (范围为32-255) 默认64
域名子节点最大长度:	<input type="text" value="16"/> (范围为16-64) 默认16
<input type="button" value="确定"/>	

图 10-18 域名长度参数

数据域说明

表 10-4 域名长度数据域说明

域名	说明
域名最大长度	域名总长度的最大长度
域名子节点最大长度	域名中的子域名的最大长度

10.5 基本型攻击

设定基本型的抗攻击选项，包括抗地址欺骗攻击，抗 ARP 欺骗，抗反向查询攻击，抗 Teardrop 攻击，抗分片洪水攻击，抗源路由攻击，抗 ARP 洪水攻击。选中后，Guard 将对所有数据包进行抗攻击检查。

表 10-5 几种攻击的名词解释

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主机发起的，从而使之可以通过路由器或 Guard。

ARP 欺骗	从影响网络连接通畅的方式来看，ARP 欺骗分为二种，一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。
反向查询攻击	可以配置限制对同一个 MAC 地址的查询报文数量，以及所有 ARP 反向查询报文的连接速率。
Teardrop 攻击	Teardrop 类的攻击利用 UDP 包重组时重叠偏移的漏洞对系统主机发动拒绝服务攻击，最终导致主机宕掉；对于 Windows 系统会导致蓝屏死机，并显示 STOP 0x0000000A 错误。
分片洪水攻击	将有大量看上去完全一样的 IP 数据包，具有高偏移地址，去往同一个 IP 地址。
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。
ARP 洪水攻击	攻击者不断地发送大量伪造的 ARP 请求报文到路由器，路由器就会不断地构造 ARP 应答报文，这样一来路由器的资源就被白白消耗掉了，导致正常报文无法处理。
ICMP 洪水攻击	当 ICMP ping 产生的大量回应请求超出了系统的最大限度，以至于系统耗费所有资源来进行响应直至再也无法处理时就会造成 ICMPflood。

基本型抗攻击配置界面如下图：

抗攻击

<input type="checkbox"/> 抗地址欺骗攻击	<input type="checkbox"/> 抗源路由攻击	<input type="checkbox"/> 抗反向查询攻击
<input type="checkbox"/> 抗Teardrop攻击	<input type="checkbox"/> 抗分片洪水攻击	
<input type="checkbox"/> 抗ARP洪水攻击	[] (范围0-1000000)	
<input checked="" type="checkbox"/> 抗icmpflood-localin攻击	[100] (范围0-1000000)	
<input type="checkbox"/> 抗ARP欺骗 <input type="checkbox"/> 广播本机 <input type="checkbox"/> 特征检查 <input type="checkbox"/> 检查ARP应答报文 <input type="checkbox"/> 禁止自动更新ARP缓存		
<input type="checkbox"/> 以上所有抗攻击		

注：在旁路情况下，不建议使用抗地址欺骗攻击功能。

什么是icmpflood-localin攻击

是指针对本地的icmpflood攻击，只对发往本地的icmpflood攻击起防范作用。

图 10-19 基本型抗攻击显示

10.6 高级型攻击

管理员可以通过保护策略来对网路中的 DDOS、DOS 以及工具型攻击进行管理，并且可以选择是否与 Detector 联动。一条保护策略包括了三个部分：策略名、PCP 名和保护策略功能选择。

高级型攻击功能包括：



- 抗攻击配置



图 10-20 高级型攻击配置


图标说明：

表 10-6 保护策略图标说明

域名	说明
	删除本条记录
	编辑本条记录

数据域说明：

表 10-7 保护策略数据域说明

域名	说明
保护策略名称	保护策略隧道名称，唯一标识，符合命名规则
包分类策略	包分类策略名称，符合命名规则
抗攻击配置	点击  ，可以进行抗攻击参数配置

添加保护策略：

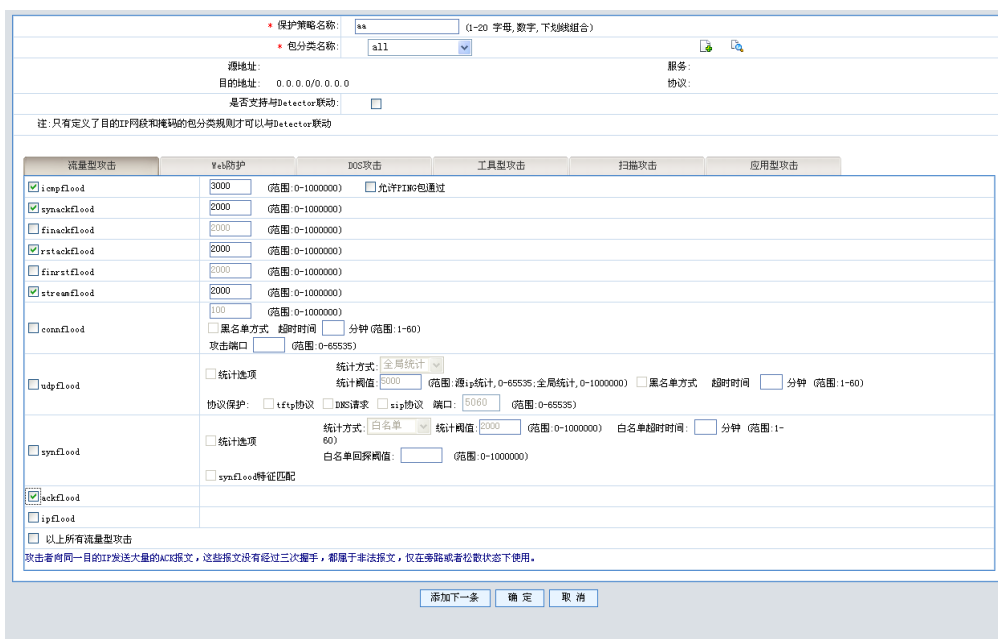


图 10-21 添加保护策略

表 10-8 保护策略添加项说明

域名	说明
保护策略名称	新建保护策略的名称
包分类名称	选择一个已有的包分类规则,选择后可以在下面看到相关配置。

表 10-9 多种攻击的名词解释

域名	说明	
流量型攻击	ICMP flood 攻击	当 ICMP ping 产生的大量回应请求超出了系统的最大限度,以至于系统耗费所有资源来进行响应直至再也无法处理有效的网络信息流时,就发生了 ICMP 泛滥。
	Syn-ack flood 攻击	大量 TCP 标志位 syn 和 ack 被置位的报文攻击
	Fin-ack flood 攻击	tcp 报文中 fin 和 ack 标志位同时被置的洪水攻击
	Rstack flood 攻击	tcp 报文中 rst 和 ack 标志位同时被置的洪水攻击
	Finrst flood 攻击	tcp 报文中 rst 和 fin 标志位同时被置的洪水攻击
	Stream flood 攻击	著名的黑客工具 stream 发出的洪水攻击,它们都有共同的特征。
	Conn flood 攻击	攻击者发送大量连接报文使被攻击对象无法正常工作
	Udp flood 攻击	与 ICMP 泛滥相似。攻击者向同一 IP 地址发送大量的 UDP 包使得该 IP 地址无法响应其它 UDP 请求,就发生了 UDP 泛滥。
	Syn flood 攻击	TCP 连接是通过三次握手完成的。当网络中充满了会发出无法完成的连接请求的 SYN 封包,以至于网络无法再处理合法的连接请求,从而导致拒绝服务(DoS)时,就发生了 SYN 泛滥攻击。攻击者通过不完全的握手过程消耗服务器的半开连接数目达到拒绝服务攻击的目的。攻击者向服务器发送含 SYN 包,其中源 IP 地址已被改为伪造的不可达的 IP 地址。服务器向伪造的 IP 地址发出回应,并等待连接已建立的确认信息。但由于该 IP 地址是伪造的,服务器无法等到确认信息,只有保持半开连接状态直至超时。由于服务器允许的半开连接数目有限,如果攻击者发送大量这样的连接请求,服务器的半开连接资源很快就会消耗完毕,无法再接受来自正常用户的 TCP 连接请求。
ack flood 攻击	在 TCP 连接建立之后,所有的数据传输 TCP 报文都是带	

		有 ACK 标志位的, 主机在接收到一个带有 ACK 标志位的数据包的时候, 需要检查该数据包所表示的连接四元组是否存在, 如果存在则检查该数据包所表示的状态是否合法, 然后再向应用层传递该数据包。如果在检查中发现该数据包不合法, 例如该数据包所指向的目的端口在本机并未开放, 则主机操作系统协议栈会回应 RST 包告诉对方此端口不存在。
	Ip flood 攻击	ip 协议域不是 tcp、udp、ICMP 常用等协议的报文攻击
Web 防护	http flood 攻击	利用代理服务器发起大量的 HTTP Get 请求, 主要是请求动态画面, 数据库服务器负载极高, 无法正常相应。
	cc 攻击	攻击主机通过大量代理服务器向目标主机发送 HTTP GET 请求, 并随即关闭到代理服务器的连接, 从而仅用很少的资源在目标主机上建立大量连接和页面请求, 达到拒绝服务式的攻击。
	url-protect	控制和保护 http url
DOS 攻击	land 攻击	“陆地”攻击将 SYN 攻击和 IP 欺骗结合在了一起, 当攻击者发送含有受害方 IP 地址的欺骗性 SYN 包, 将其作为目的和源 IP 地址时, 就发生了陆地攻击。接收系统通过向自己发送 SYN-ACK 封包来进行响应, 同时创建一个空的连接, 该连接将会一直保持到达到空闲超时值为止。向系统堆积过多的这种空连接会耗尽系统资源, 导致 DoS。攻击者发送特殊的 SYN 包, 其中源 IP 地址、源端口和目的 IP 地址、目的端口指向同一主机, 早期的操作系统收到这样的 SYN 包时可能会当机。
	WinNuke 攻击	WinNuke 是一种常见的应用程序, 其唯一目的就是使互联网上任何运行 Windows 的计算机崩溃。这种专门针对 Windows 3.1/95/NT 的攻击曾经猖獗一时, 受攻击的主机可以在片刻间出现蓝屏现象 (系统崩溃)。WinNuke 通过已建立的连接向主机发送带外(OOB) 数据, 通常发送到 NetBIOS 端口 (TCP139 端口), 攻击者只要先跟目标主机的 139 端口建立连接, 继而发送一个带 URG 标志的带外数据报文, 引起 NetBIOS 碎片重叠, 目标系统即告崩溃。重新启动后, 会显示下列信息, 指示攻击已经发生: An exception OE has occurred at 0028:[address] in VxD MSTCP(01) + 000041AE. This was called from 0028:[address] in VxD NDIS(01) + 00008660. It may be possible to continue normally.

	<p>(00008660。有可能继续正常运行。) Press any key to attempt to continue. (请按任意键尝试继续运行。)</p> <p>Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications. (按 CTRL+ALT+DEL 可尝试继续运行。将丢失所有应用程序中的未保存信息。) Press any key to continue. (按任意键继续。) 原因是系统中某些端口的监听程序不能处理“意外”来临的带外数据,造成严重的非法操作。</p>
SYN&FIN 位攻击	正常数据包中,不会同时设置 TCP Flags 中的 SYN 和 FIN 标志,因为 SYN 标志用于发起 TCP 连接,而 FIN 标志用于结束 TCP 连接。不同的 OS 对同时包含 SYN 和 FIN 标志的数据包有不同处理方法,攻击者可利用这种数据包判断被攻击主机的 OS 类型,为后续攻击做准备。
TCP 无标记攻击	正常数据包中,至少包含 SYN、FIN、ACK、RST 四个标记中的一个,不同的 OS 对不包含这四个标记中任何一个标志的数据包有不同处理方法,攻击者可利用这种数据包判断被攻击主机的 OS 类型,为后续攻击做准备。
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。
无确认 FIN 攻击	正常数据包中,包含 FIN 标志的 TCP 数据包同时包含 ACK 标志。不同的 OS 对包含 FIN 标志但不包含 ACK 标志的数据包有不同处理方法,攻击者可利用这种数据包判断被攻击主机的 OS 类型,为后续攻击做准备。
Smurf 攻击	攻击者伪装成被攻击主机向广播地址发送 ICMP 包(以 PING 包为主),这样被攻击主机就可能收到大量主机的回应,攻击者只需要发送少量攻击包,被攻击主机就会被淹没在 ICMP 回应包中,无法响应正常的网络请求。
ping of death 攻击	TCP/IP 规范要求用于数据包传输的封包必须具有特定的大小。许多 ping 实现允许用户根据需要指定更大的封包大小。当攻击者发送超长的 ICMP 包时会引发一系列负面的系统反应,早期的操作系统可能因为缓冲区溢出而宕机,如拒绝服务(DoS)、系统崩溃、死机以及重新启动。

	Fraggle 攻击	Fraggle 攻击对 Smurf 攻击作了简单的修改，使用的是 UDP 应答消息而非 ICMP。
	IP 选项攻击	ip 头部选项
工具型 攻击	trinoo 攻击	trinoo 是复杂的 DDoS 攻击程序，是基于 UDP flood 的攻击软件。它使用“master”程序对实际实施攻击的任何数量的“代理”程序实现自动控制。当然在攻击之前，侵入者为了安装软件，已经控制了装有 master 程序的计算机和所有装有代理程序的计算机。攻击者连接到安装了 master 程序的计算机，启动 master 程序，然后根据一个 IP 地址的列表，由 master 程序负责启动所有的代理程序。接着，代理程序用 UDP 信息包冲击网络，向被攻击目标主机的随机端口发出全零的 4 字节 UDP 包，在处理这些超出其处理能力垃圾数据包的过程中，被攻击主机的网络性能不断下降，直到不能提供正常服务，乃至崩溃。它对 IP 地址不做假，因此此攻击方法用得不多。
	TFN 攻击	Tribe Flood Network 与 trinoo 一样，使用一个 master 程序与位于多个网络上的攻击代理进行通讯，利用 ICMP 给代理服务器下命令，其来源可以做假。TFN 可以并行发动数不胜数的 DoS 攻击，类型多种多样，而且还可建立带有伪装源 IP 地址的信息包。可以由 TFN 发动的攻击包括：SYN flood、UDP flood、ICMP 回音请求 flood 及 Smurf（利用多台服务器发出海量数据包，实施 DoS 攻击）等攻击。
	TFN2k 攻击	TFN 的升级版 TFN2k 进一步对命令数据包加密，更难查询命令内容，命令来源可以做假，还有一个后门控制代理服务器。
	Stacheldraht 攻击	Stacheldraht 也是基于 TFN 和 trinoo 一样的客户机/服务器模式，其中 Master 程序与潜在的成千个代理程序进行通讯。在发动攻击时，侵入者与 master 程序进行连接。Stacheldraht 增加了新的功能：攻击者与 master 程序之间的通讯是加密的，对命令来源做假，而且可以防范一些路由器用 RFC2267 过滤，若检查出有过滤现象，它将只做假 IP 地址最后 8 位，从而让用户无法了解到底是哪几个网段的哪台机器被攻击；同时使用 rcp(remote copy, 远程复制) 技术对代理程序进行自动更新。Stacheldraht 同 TFN 一样，可以并行发动数不胜

		数的 DoS 攻击，类型多种多样，而且还可建立带有伪装源 IP 地址的信息包。Stacheldraht 所发动的攻击包括 UDP 冲击、TCP SYN 冲击、ICMP 回音应答冲击。
扫描攻击	基于特征的抗端口扫描	根据报文中是否具有明显的扫描特征来判断扫描行为。
	基于频率的抗端口扫描	根据源主机访问目的主机或目的端口的频率来判断扫描行为。
应用型攻击	Sip flood	攻击者发送大量 sip 类型的报文使被攻击对象无法正常工作

10.7 自定义特征

自定义特征是用户可以定义网络数据报文的特征，达到抗攻击的目的。

10.7.1 TCP

这个页面用于配置 TCP 协议的自定义特征。




图 10-22 自定义特征配置

数据域说明

表 10-10 自定义特征数据域说明

域名	说明
访问控制	符合特征报文执行的动作，丢弃或者通过
入侵特征码	应用层数据特征串
是否指定匹配参数	如没有勾选，程序则会搜索整个应用层数据

10.7.2 UDP

这个页面用于配置 UDP 协议的自定义特征。

TCP		UDP		ICMP		开启自定义	
自定义特征——UDP							
访问控制: --- (选择“---”表示不做任何配置)							
源地址: <input type="text"/>				目的地址: <input type="text"/>			
掩码: 255.255.255.255				掩码: 255.255.255.255			
源端口: 范围 <input type="text"/>				目的端口: 范围 <input type="text"/>			
IP包头标识(ID): 范围 <input type="text"/>				生存期TTL: 范围 <input type="text"/>			
IP总长度: 范围 <input type="text"/>				TOS: <input type="checkbox"/> (范围: 0-7)			
入侵特征码: <input type="text"/> (长度范围: 1-20)							
<input checked="" type="checkbox"/> 是否指定匹配参数		区分大小写: <input type="checkbox"/>		偏移量度(offset): <input type="text"/> (范围: 0-65535)			
检测深度(depth): <input type="text"/> (范围: 1-20) (不配置或者配置长度超过所填字符长度, 将自动配置为字符串长度)							
选择“范围”时, 用“-”符号表示区间, 如 添写10-200 表示范围10到200							
确定				清空			

图 10-23 udp

10.7.3 ICMP

这个页面用于配置 ICMP 协议的自定义特征。

TCP		UDP		ICMP		开启自定义	
自定义特征——ICMP							
访问控制: --- (选择“---”表示不做任何配置)							
源地址: <input type="text"/>				目的地址: <input type="text"/>			
掩码: 255.255.255.255				掩码: 255.255.255.255			
IP包头标识(ID): 范围 <input type="text"/>				生存期TTL: 范围 <input type="text"/>			
IP总长度: 范围 <input type="text"/>				TOS: <input type="checkbox"/> (范围: 0-7)			
入侵特征码: <input type="text"/> (长度范围: 1-20)							
<input checked="" type="checkbox"/> 是否指定匹配参数		区分大小写: <input type="checkbox"/>		偏移量度(offset): <input type="text"/> (范围: 0-65535)			
检测深度(depth): <input type="text"/> (范围: 1-20) (不配置或者配置长度超过所填字符长度, 将自动配置为字符串长度)							
ICMP类型: <input type="text"/> (范围: 0-18)				ICMP代码: <input type="text"/> (范围: 0-15)			
选择“范围”时, 用“-”符号表示区间, 如 添写10-200 表示范围10到200							
确定				清空			

图 10-24 ICMP

10.7.4 自定义特征开启配置

TCP UDP ICMP **开启自定义**

开启自定义

开启开关 (若要开启自定义功能, 请勾选此项)

IP地址: 掩码: 255.255.255.255

IP列表:

IP地址列表为攻击保护的目标IP, 请至少配置一个地址值

图 10-25 自定义特征开启

表 10-11 自定义特征开启数据域说明

域名	说明
开启开关	自定义的总开关 (必选)
IP 地址	保护的目IP 地址 (必选)

表 10-12 自定义特征数据域说明

域名	说明
访问控制	符合特征报文执行的动作, 丢弃或者通过
入侵特征码	应用层数据特征串
是否指定匹配参数	如没有勾选, 程序则会搜索整个应用层数据

第11章 流量回注

Guard 对牵引过来的流量进行分析，对其中的异常流量和 DDOS 攻击进行清洗，并将清洗后的干净流量回注到网络中继续转发，本章主要介绍 Guard 的流量回注配置。

11.1 接口转发

网络配置>>路由牵引>>接口转发

接口转发功能开关	<input checked="" type="checkbox"/>		
<input type="button" value="确定"/>			
入接口名称	出接口名称	网关IP地址	操作
Tunnel22	Bridge33	1.2.3.4	
Ge0/0/2	Ge0/0/0	22.22.22.22	
<input type="button" value="添加"/>			

图 11-1 接口转发配置

数据域说明：

表 11-1 接口转发数据域说明

域名	说明
接口转发功能开关	可以开启或关闭接口转发功能
入接口名称	入接口的名称
出接口名称	出接口的名称
网关 IP 地址	设置的网关 IP

此界面可以完成以下功能：

- 添加接口转发
- 编辑接口转发
- 删除接口转发
- 添加接口转发
- 点“添加”按钮，进入“接口转发参数配置”
- 添加接口转发参数
- 点“确定”按钮完成添加



图 11-2 接口转发添加页面

编辑接口转发功能



图 11-3 接口转发编辑页面

删除接口转发:

- 点“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

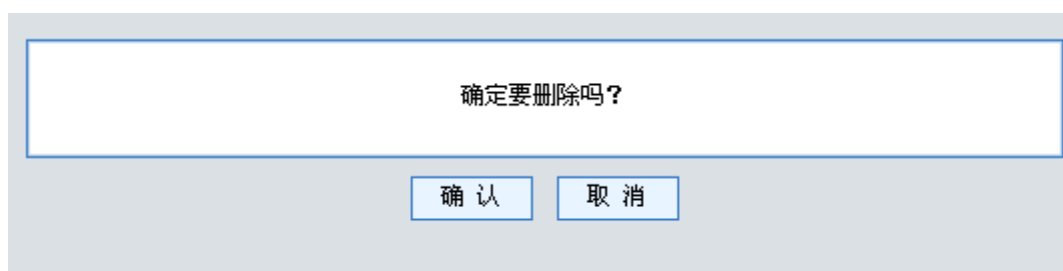


图 11-4 接口转发删除页面

11.2 启动 GRE

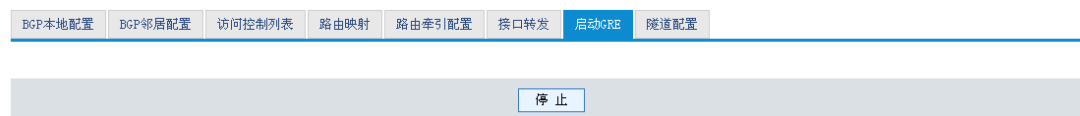


图 11-5 启动 GRE

11.3 隧道配置



图 11-6 隧道配置

数据域说明:

表 11-2 隧道配置数据域说明

域名	说明
隧道名称	隧道名称
虚接口 IP	虚拟接口 IP 地址
源端 IP	源端 IP
目的端 IP	目的端 IP

此界面可以完成以下功能:

- 添加隧道配置
- 编辑隧道配置
- 删除隧道配置
- 添加隧道配置
- 点“添加”按钮，进入“隧道配置参数配置”
- 添加隧道配置参数
- 点“确定”按钮完成添加



图 11-7 隧道配置添加页面

编辑隧道配置功能：



图 11-8 隧道配置编辑页面

删除隧道配置：

- 点“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

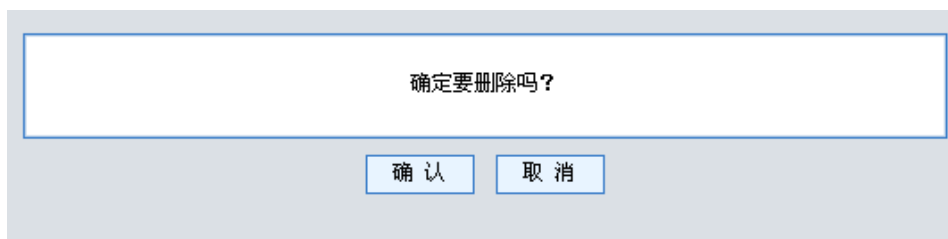


图 11-9 隧道配置删除页面

第12章 流量统计

12.1 事件统计

12.1.1 开启统计

通过这个页面可以开启统计，设置统计采样率。

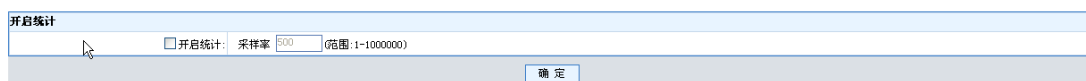


图 12-1 开启统计

12.1.2 事件统计

事件统计可以通过查询条件查询攻击的详细信息。



图 12-2 事件统计配置

12.2 攻击类型 TOP5

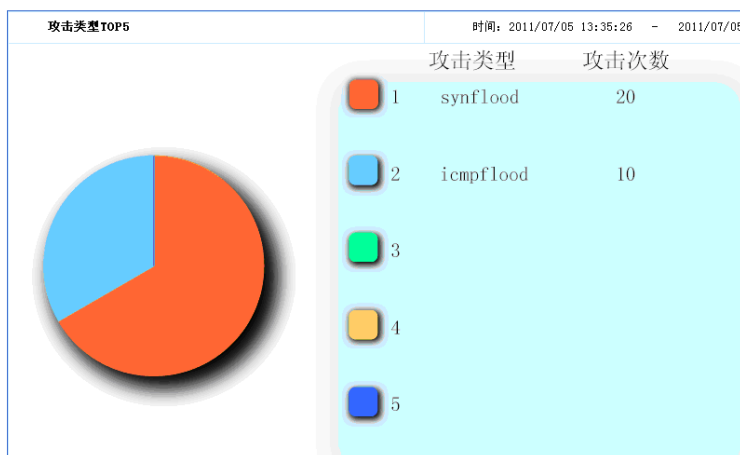


图 12-3 攻击类型 TOP5 显示

12.3 攻击来源 TOP5

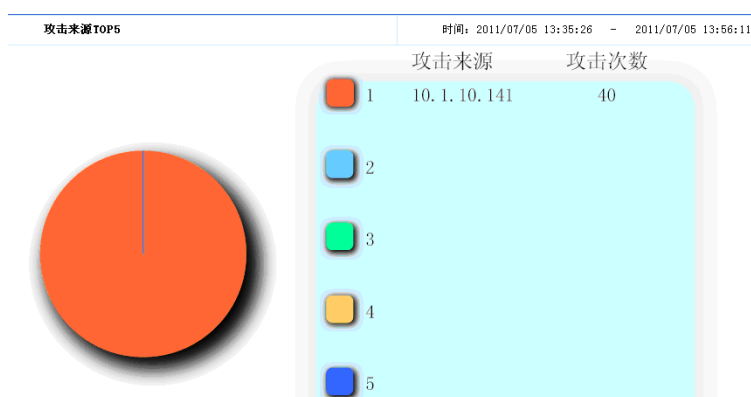


图 12-4 攻击来源 TOP5 显示

12.4 攻击目的 TOP5

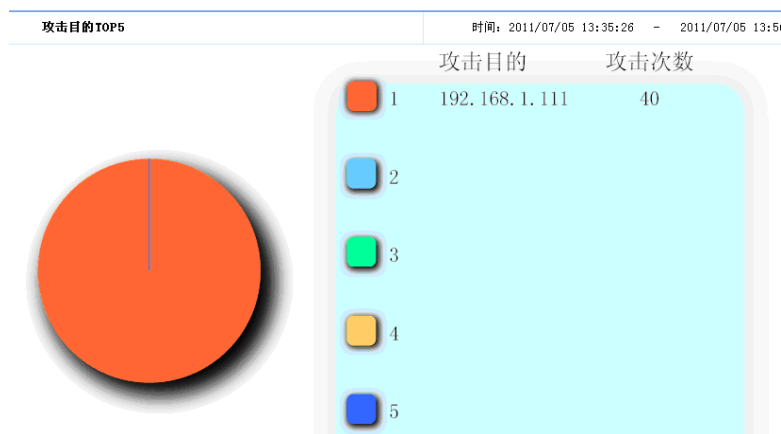


图 12-5 攻击目的 TOP5 显示

12.5 攻击流量统计

12.5.1 即时流量统计

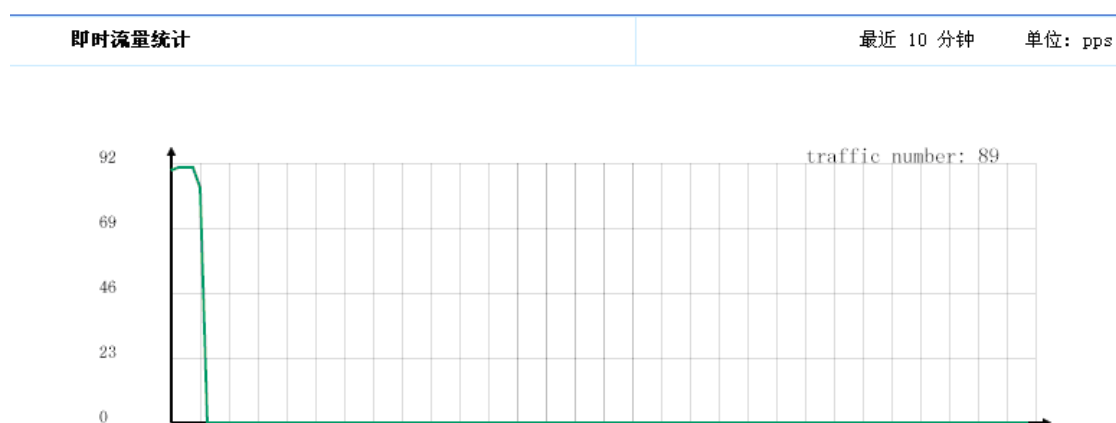


图 12-6 即时流量显示

12.5.2 异常流量统计

设置日期	今天	
流量统计	察看统计图	这里可以察看当日synflood、udp flood、cc等报文的总体统计图
流量排行	察看统计图	这里可以察看当日排名在前五名的报文排行及详细数据

图 12-7 异常流量统计显示

12.6 保护域流量统计

12.6.1 牵引流量统计

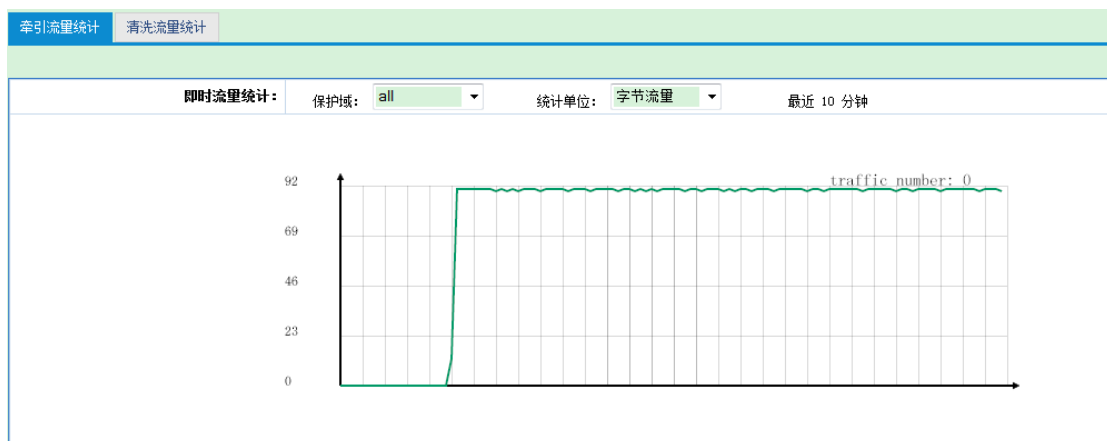


图 12-8 牵引流量统计显示

12.6.2 清洗流量统计

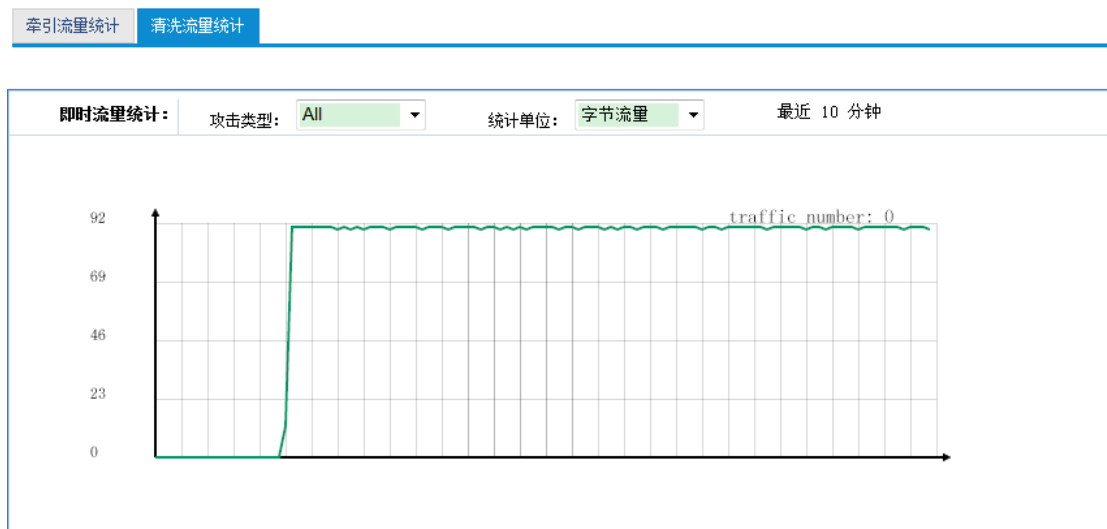


图 12-9 清洗流量统计显示

第13章 防火墙

本章是对 Guard 上防火墙的配置。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。

13.1 包过滤

包过滤显示页面：

可以根据序号排名显示，显示包括几个缩略参数，源地址、目的地址、服务和动作等。

可以分屏显示，支持翻页功能等。

界面如下图所示：



图 13-1 包过滤

包过滤添加页面：

根据包过滤支持的几个元素定义分类规则。

具体参数如下图所示：

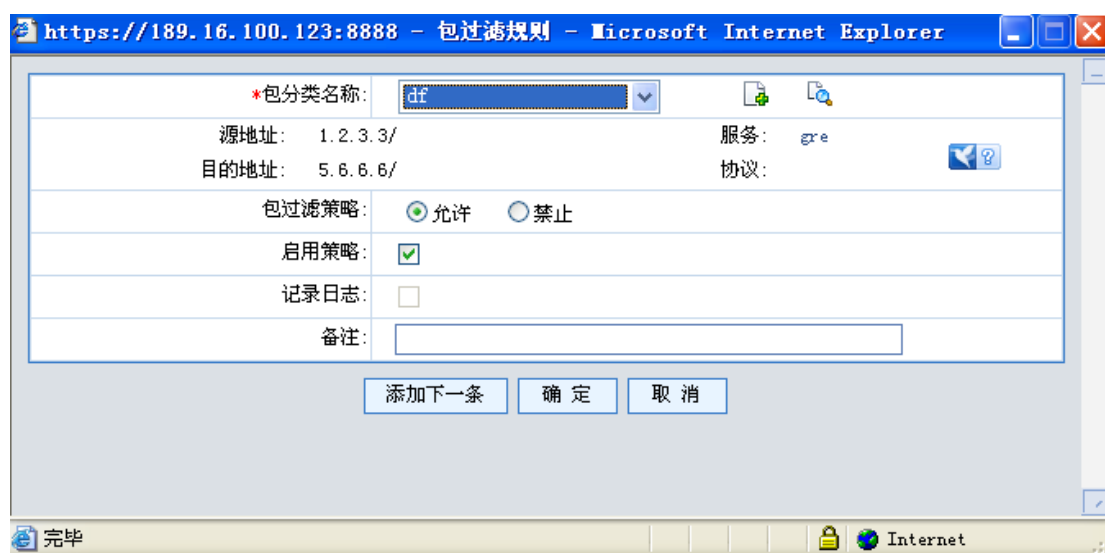


图 13-2 包过滤添加页面

13.1.1 默认过滤策略

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、arp 超时时间、严格状态检查、状态优先以及黑名单检查开关。这些参数对整个防火墙生效。

界面如下图所示：

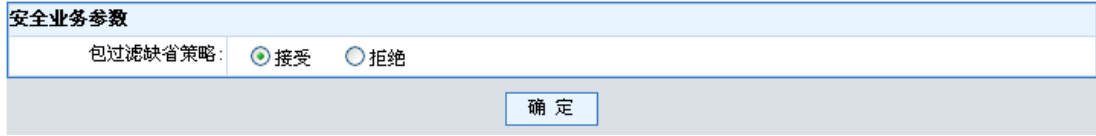


图 13-3 默认过滤策略配置

13.2 DNAT 策略

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。

目的地址转换规则显示页面：

可以根据配置的序号排名显示，包括 PCP 的基本参数信息，以及转换后的参数信息等。

可支持分屏显示，翻页等功能。



图 13-4 目的地址转换规则显示

目的地址转换添加规则：

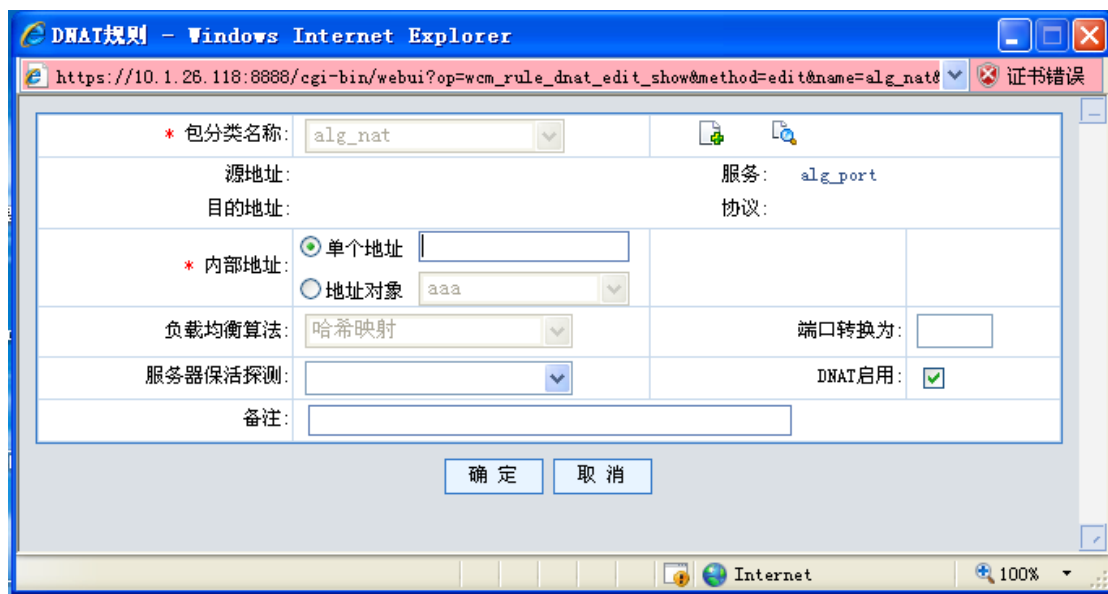


图 13-5 目的地址转换添加规则

目的地址转换修改规则：

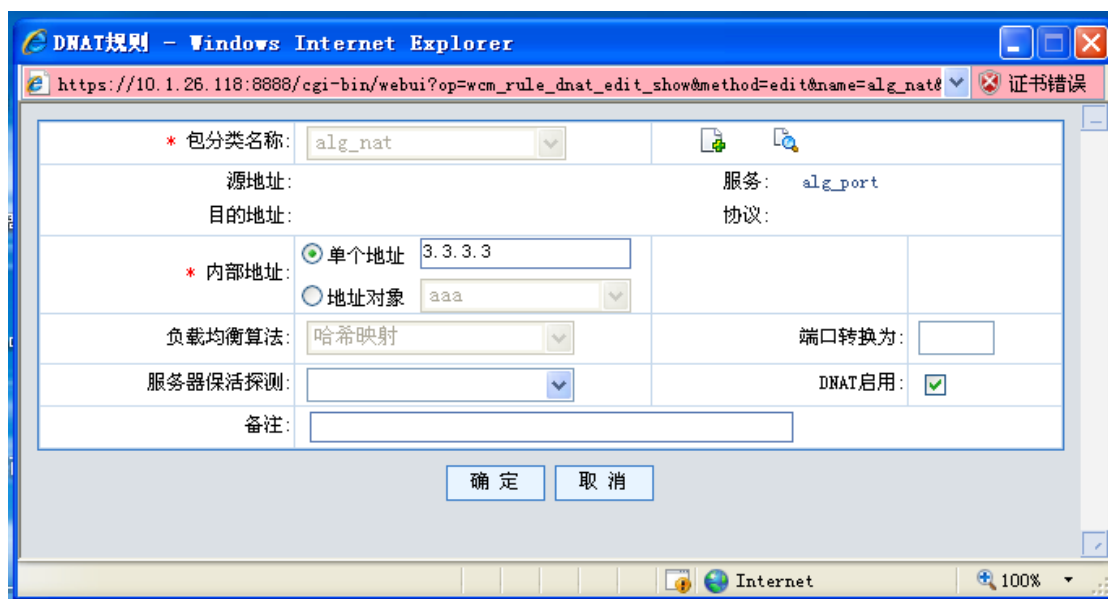


图 13-6 目的地址转换修改规则

目的地址转换删除规则：

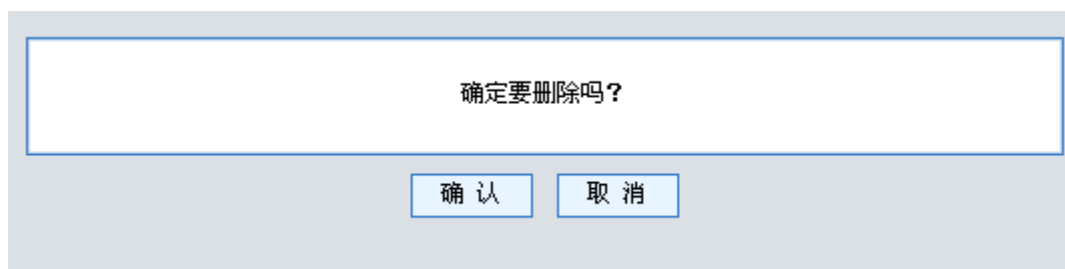


图 13-7 目的地址转换删除规则

13.3 SNAT 策略

SNAT，即原地址转换。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。

用户可通过规则设定需要转换的源地址（支持网络地址范围）、源端口。可以通过系统“资源定义>>地址”定义的对象，支持多对多，多对一，一对多的地址转换关系。

SNAT 配置页面如下：

按条件查询

序号	分类名	源地址	目的地址	服务	转换地址	算法	端口	是否启用	备注	操作
<input type="checkbox"/>	1	df	1.2.3.3/	5.6.6.6/	gre	2.3.3.5	随机端口	●		 
<input type="checkbox"/>	2	snat	100.100.100.0/255.255.255.0		Ge0/0/0			●		 

添加SNAT规则

全选





第1页/1页 跳转到 页 每页 行

图 13-8 安全策略显示

添加 SNAT 规则界面：

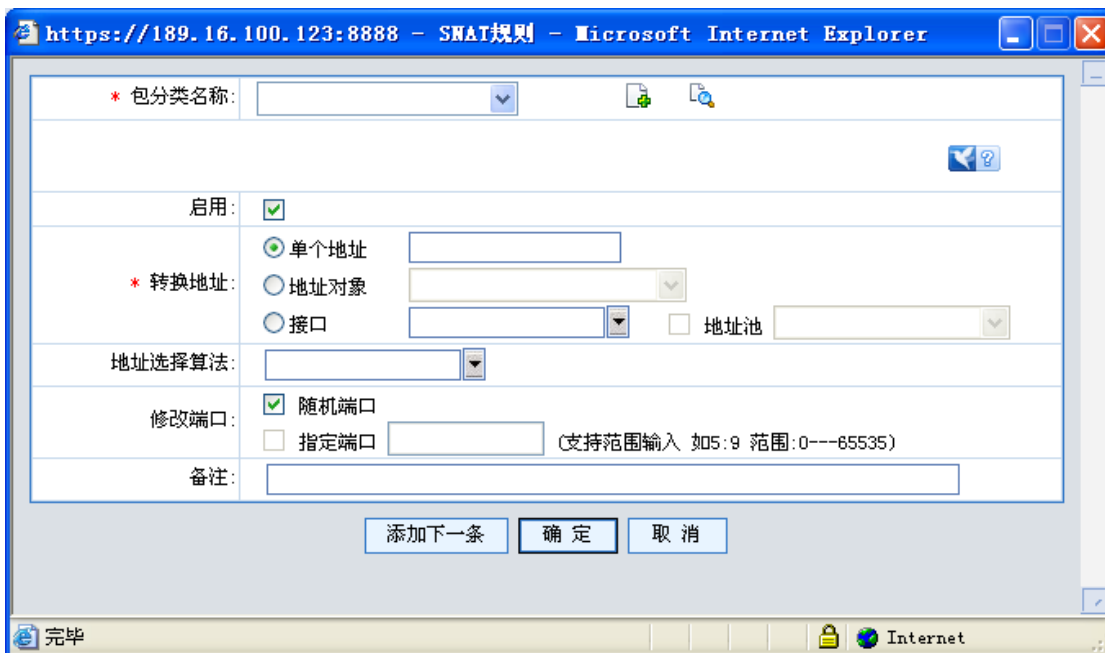


图 13-9 添加 SNAT 策略

修改 SNAT 策略界面：

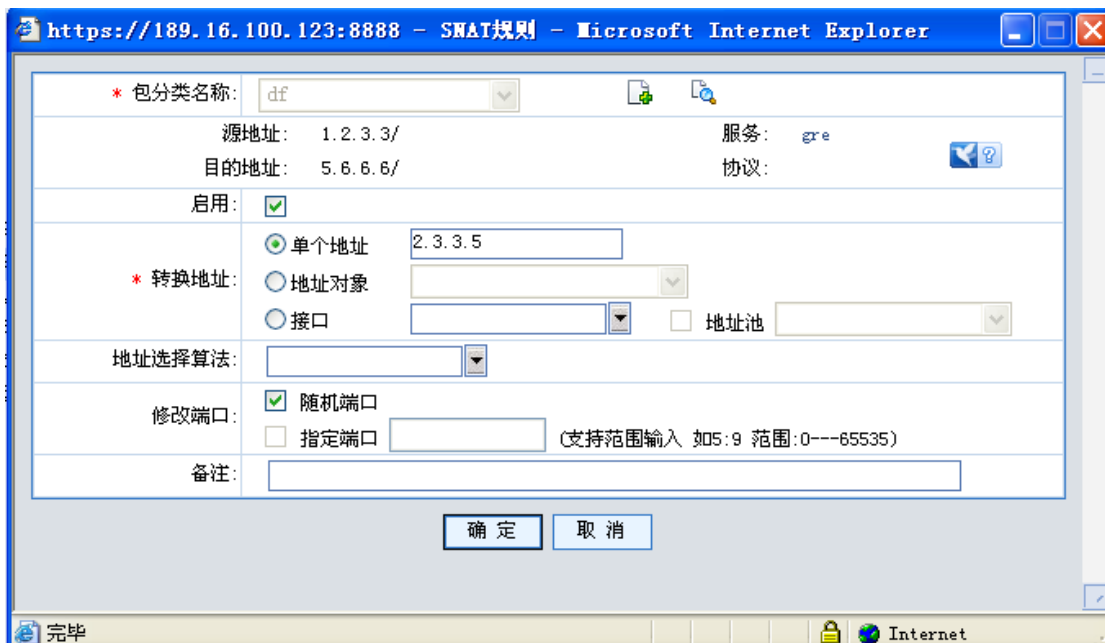


图 13-10 修改 SNAT 策略

删除 SNAT 界面:

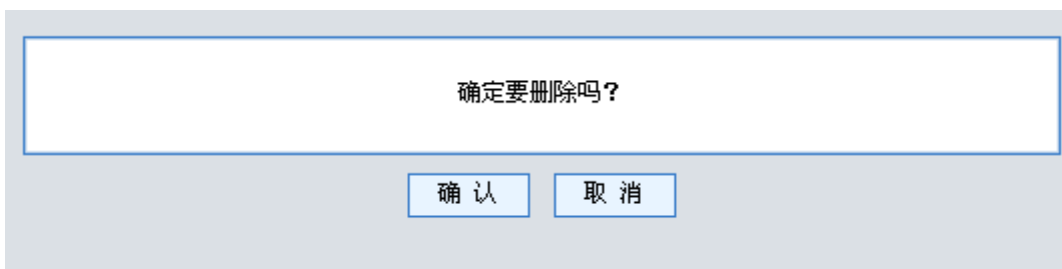


图 13-11 删除 SNAT

13.4 二层协议

点击“防火墙->二层协议”，可看到以下页面：



图 13-12 二层协议界面

有以下功能：

- 是否开启二层透传协议检测。

自定义二层协议：



图 13-13 二层协议配置

表 13-1 二层协议配置说明

域名	说明
协议名称	协议的名称 不超过 20 个字符
协议号	协议的协议号 可输入范围 0-65535，不可与已有协议的协议号相同
允许透传	是否允许透传 允许透传，则该协议的数据包可通过

13.5 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“防火墙>>地址绑定”中的 IP/MAC 检查启用，当 Guard 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，则按物理接口缺省策略执行。



图 13-14 地址绑定配置

“防火墙->地址绑定”可以完成以下功能:

- 启动/关闭 IP/MAC 检查
- IP/MAC 接口绑定检查
- 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

IP/MAC 检查

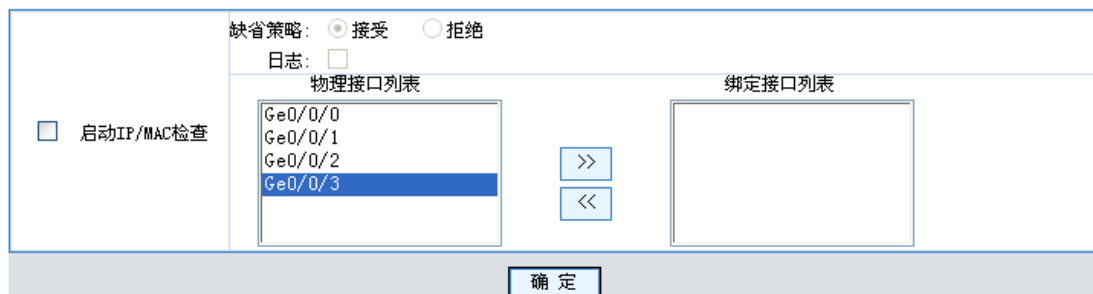


图 13-15 IP/MAC 检查配置

表 13-2 IP/MAC 检查项说明

域名	说明
启动 IP/MAC 检查	启动或者关闭 IP/MAC 检查
缺省策略	对不在已绑定 IP/MAC 列表中的数据包的执行接受或拒绝操作
日志	启动或关闭日志功能 当日志功能启动时，将记录丢弃的数据包信息
物理接口绑定检查	IP/MAC 只对从绑定物理接口进来的报文进行检查

若启用 IP/MAC 检查，则 Guard 接收从绑定物理接口进来的数据包时，将根据数据包中的源 IP 地址与源 MAC 地址，检索已绑定的 IP/MAC 地址列表。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，则按照缺省策略执行。默认缺省策略是接受，此时查找失败的数据包仍允许通过；若缺省策略设为拒绝，则该数据包将被丢弃。

注意：

若管理主机的 IP/MAC 地址未绑定，此时启动 IP/MAC 检查，且缺省策略设为拒绝，则管理主机的数据包会被 Guard 禁止通过，web 页面将无法显示。

探测 IP/MAC 地址对

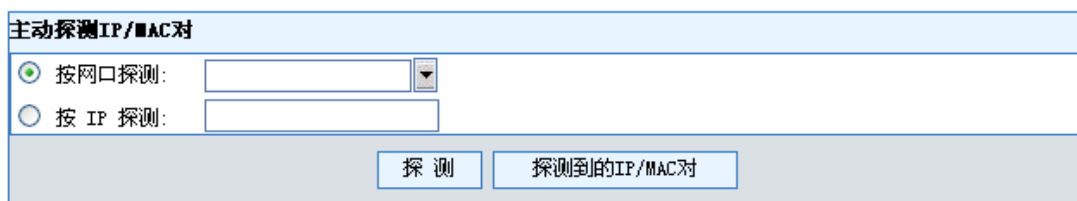


图 13-16 IP/MAC 地址探测

表 13-3 IP/MAC 地址探测项说明表

域名	说明
按网口探测	IP/MAC 地址探测方式。
Ge0/0/n n=0,1,2,3	当前可用的网口列表 管理员根据需求指定要做 IP/MAC 探测的网口
按 IP 探测	IP/MAC 地址探测方式
输入框	输入 IP 地址
探测	点击后，对指定网口或 IP 地址进行 IP/MAC 地址对的探测 探测完成时，本页面会刷新，重新回到探测前的状态。管理员可以点击“探测到的 IP/MAC 对”查看探测结果。
探测到的 IP/MAC 对	点击后，显示当前探测到的 IP/MAC 对列表。

按网口探测 IP/MAC 地址对的操作步骤：

1. 点击“防火墙->地址绑定”菜单，弹出“地址绑定”界面。
2. 选择“按网口探测”，可以指定要做 IP/MAC 探测的网口，每次只能探测一个网口。
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. 当探测完毕时，本页面会刷新，重新回到网口未选中状态。
5. 点击“探测到的 IP/MAC 对”，弹出“探测到的 IP/MAC 对”界面，显示在指定网口当前探测到的 IP、MAC 信息，管理员可以根据探测到的 IP/MAC 地址对完成绑定功能。

按 IP 探测 IP/MAC 地址对的操作步骤：

1. 点击“防火墙->地址绑定”菜单，弹出“地址绑定”界面。
2. 选择“按 IP 探测”，在输入框中输入待探测主机的 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. 当探测完毕时，本页面会刷新，重新回到 IP 地址未输入状态。
5. 点击按钮“探测到的 IP/MAC 对”，弹出“探测到的 IP/MAC 对”界面，显示在指定网口当前探测到的 IP、MAC 信息，管理员可以根据探测到的 IP/MAC 地址对，完成绑定功能。

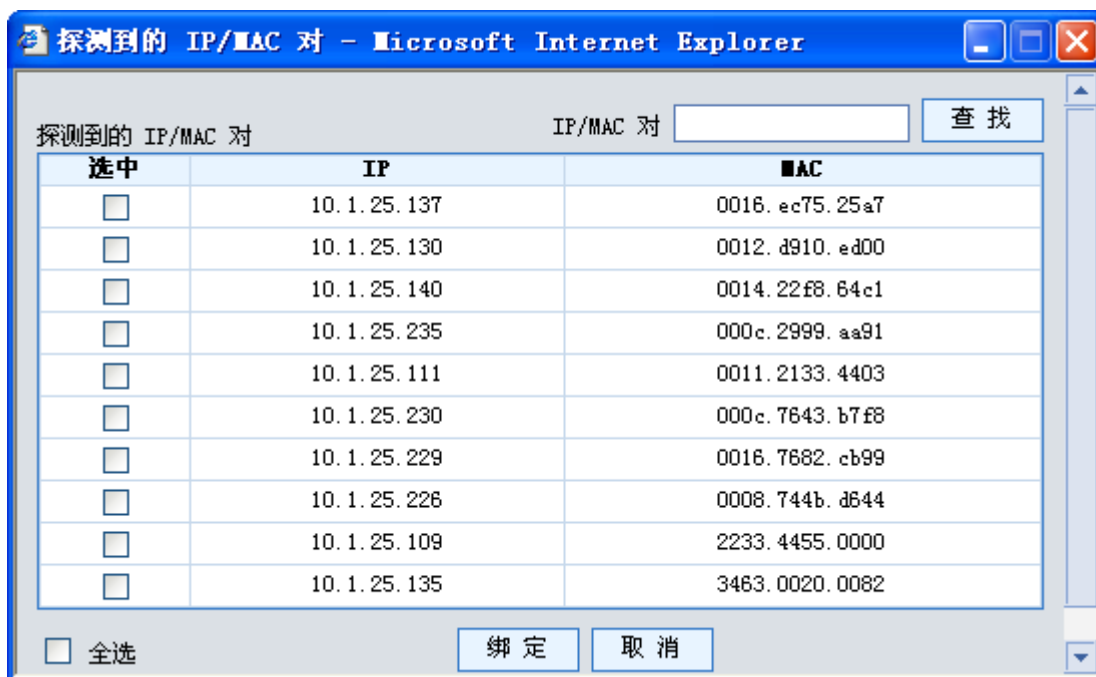


图 13-17 探测到的 IP/MAC 对显示

表 13-4 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，可以根据选择进行绑定或非绑定操作
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
全选	全部选中探测到的 IP/MAC 对，可以根据选择进行绑定或非绑定操作
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，探测结果显示列表将不会再保留该信息
取消	取消本次操作

探测到的 IP/MAC 对界面操作说明：

- 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。
- 针对选中的地址对表项，点击绑定，则地址对完成绑定功能，绑定成功后界面刷新，该 IP/MAC 对信息在探测结果显示列表中消失，显示在已绑定 IP/MAC 对的列表中。
- 在探测结果显示列表中执行绑定操作时，不会进行唯一性检查，默认绑定后启用。
- 探测操作可执行多次，但每次探测完成时都会清空上一次的探测结果。若要实现多个网口的探测绑定功能，需要执行“探测+全选绑定”多次。

绑定 IP/MAC 地址对

已绑定 IP/MAC 对列表：

已绑定IP/MAC对						<input type="text"/>	查找
IP地址	MAC地址	唯一性检查	是否启用	备注	操作		
10.1.25.135	0008.74f1.3b1a	✘	✔				
10.1.25.225	0018.8bac.e89f	✘	✔				
10.1.25.221	0016.9610.30f0	✘	✔				
10.1.25.218	0018.8b02.4cbb	✘	✔				
10.1.25.222	0012.3f0d.6ccb	✘	✔				
10.1.25.219	0010.5cd7.3acf	✘	✔				
10.1.25.217	00e0.9108.9e3a	✘	✔				
10.1.25.214	00e0.9f56.4270	✘	✔				
10.1.25.213	001d.0903.066b	✘	✔				
10.1.25.210	0015.e500.a7ed	✘	✔				

第1页/8页 跳转到 页 每页 行

图 13-18 绑定 IP/MAC 对配置

编辑已绑定的 IP/MAC 地址对：

点击“编辑”将执行编辑操作，可看到以下界面：

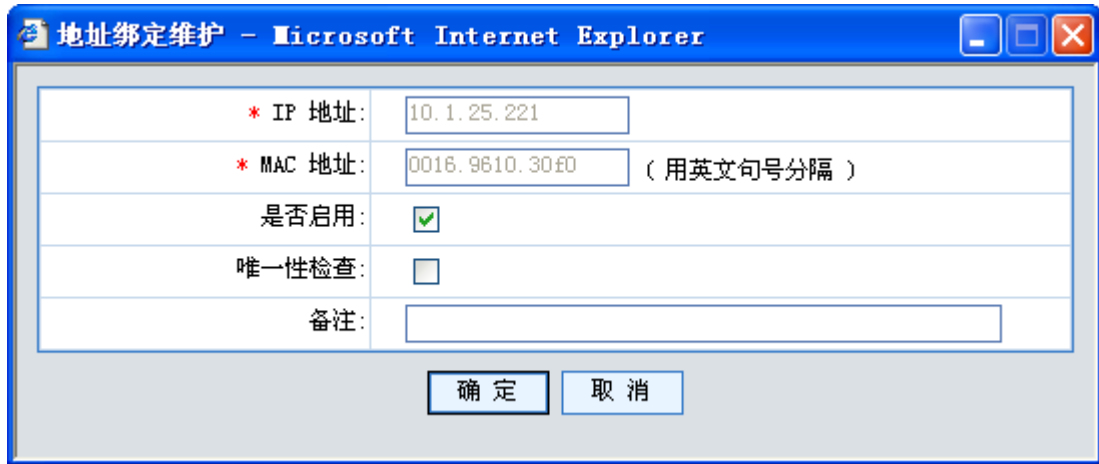


图 13-19 编辑已绑定的 IP/MAC 地址对

表 13-5 编辑地址绑定项说明

域名	说明
IP 地址	已绑定的 IP 地址，无法修改
MAC 地址	已绑定的 MAC 地址，无法修改
是否启用	当前 IP/MAC 对启用或关闭
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。

注意：

已绑定 IP/MAC 对列表中，编辑操作只能修改“是否启用”、“唯一性检查”的状态以及备注。当启用唯一性检查并确定时，系统会检测该 MAC 地址是否被其他 IP 地址占用，若被占用则弹出提示信息，且唯一性检查无法开启。此种情况下，可在已绑定 IP/MAC 列表中搜索该 MAC 地址，获知被哪些 IP 地址所用，删除对该 MAC 地址的多重绑定，唯一性检查才能正常启用。

手动添加 IP/MAC 地址对：

点击“添加”，将执行手动添加操作，弹出以下界面：



图 13-20 添加地址绑定

表 13-6 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 MAC 地址，不能是组播地址
是否启用	当前的绑定是否启用
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。

手工添加 IP/MAC 地址对绑定规则的操作流程：

1. 点击“Guard->地址绑定”菜单，弹出“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。

手工删除 IP/MAC 地址对的操作流程：

1. 点击“Guard->地址绑定”菜单，弹出“地址绑定”界面。
2. 在已绑定 IP/MAC 地址对栏中，选择删除，弹出删除确认界面。

点击确定即可删除当前纪录。

13.6 服务器探测

当配置了服务器地址之后，为了更好的完成服务器负载均衡的 NAT 功能，提供了保活探测功能。这样可以最大程度的保证 NAT 功能正常使用，保证网络访问率。

服务器保活探测提供了 2 个层次的探测方法，

一种为 ICMP 探测，即探测该 IP 地址主机是否存活，

一种为 TCP PORT 探测，即探测该 IP 地址特定端口服务是否开启。

开启服务器探测功能页面：

启动服务器保活探测 秒 范围 (1 - 65535)

图 13-21 启动服务器探测

服务器探测显示页面：

序号	名称	对象/IP	IP地址/协议/端口	探测结果	操作
1	sd2	基于IP	192.168.20.71	●	<input type="button" value="✎"/> <input type="button" value="✖"/>
			0.0.0.0	●	
			0.0.0.0	●	
			0.0.0.0	●	
			0.0.0.0	●	
			0.0.0.0	●	
			0.0.0.0	●	
			0.0.0.0	●	

第1页/1页 跳转到 页 Go 每页 行

图 13-22 服务器保活探测显示

服务器保活探测配置页面：



图 13-23 添加服务器保活探测

服务器保活探测修改页面：



图 13-24 服务器保活探测修改

服务器保活探测删除页面：

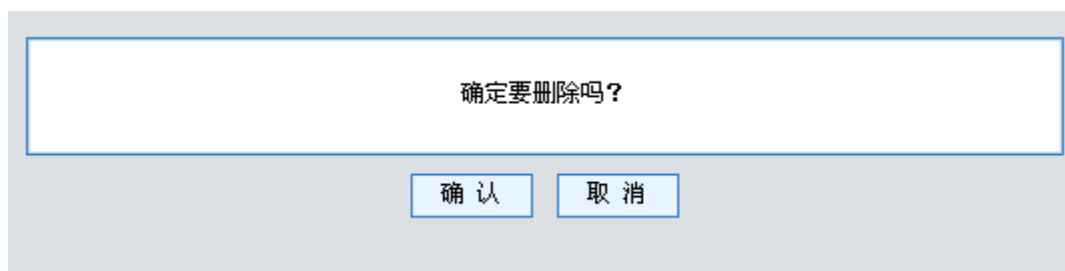


图 13-25 服务器探测删除对话框

第14章 会话管理

14.1 会话配置

点击如图所示框，选择相应的会话检查状态

状态检查:	严格状态检查 ▾
<input type="checkbox"/>	状态优先
<input type="button" value="确定"/>	

图 14-1 会话配置

14.2 长连接

针对每一个链接，内存中保存的连接状态表有一个默认的超时时间为 5 天，但是针对某些特殊业务访问，需要保持更长时间的通讯状态，因此提供了此参数配置界面。下图为长连接的页面显示：

按条件查询

序号	分类名	源地址	目的地址	服务	Lo	操作
<input type="button" value="添加"/>						

全选

⏪ ⏩ ⏴ ⏵

第1页/1页 跳转到 页 每页 行

图 14-2 长连接

长连接的添加页面如下：

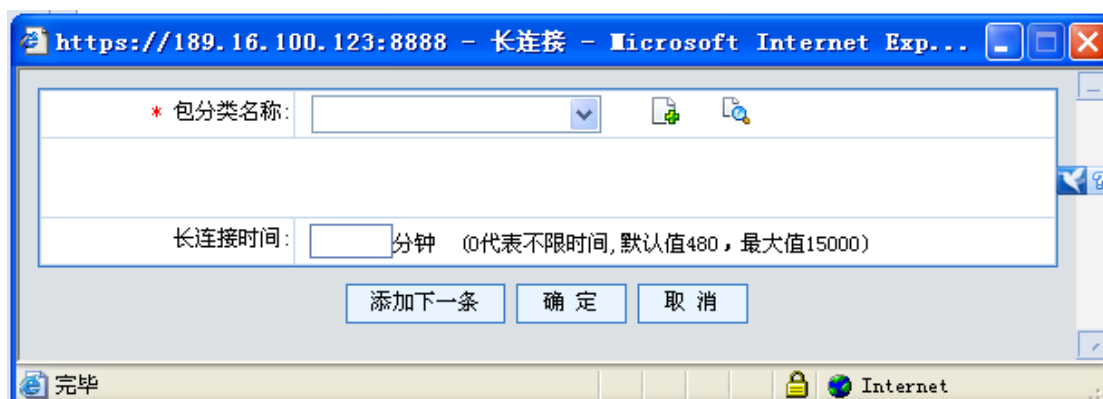


图 14-3 长连接的添加页面

14.3 会话日志



图 14-4 Session 状态图

点击上图添加按钮进入状态日志配置框

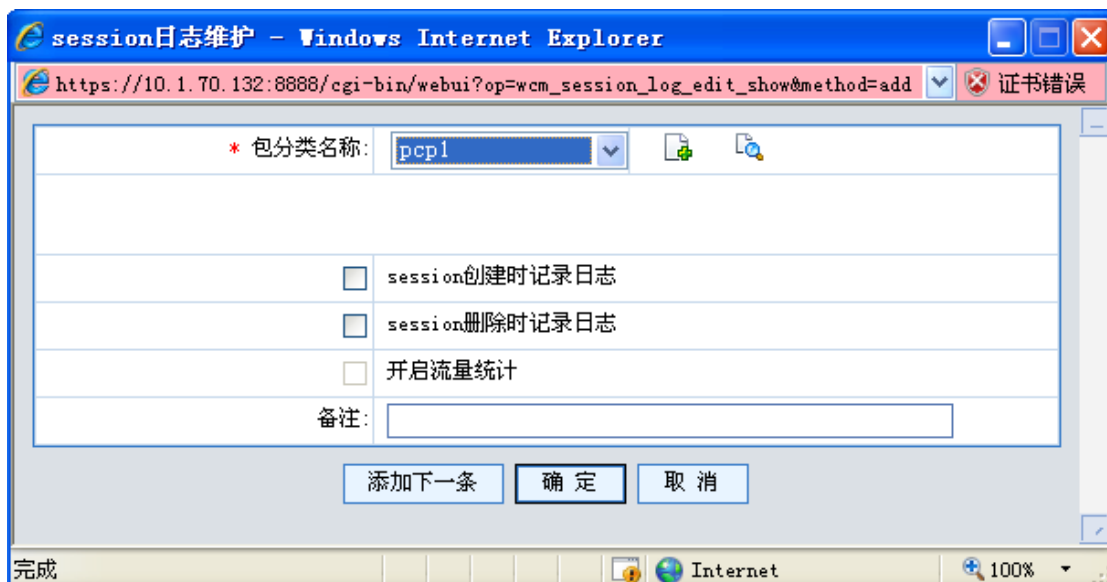


图 14-5 Session 日志维护

14.4 会话状态

会话状态可以显示当时的所有连接，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。

按条件查询 按条件删除 全部删除

序号	协议	源地址	目的地址	源端口	目的端口	超时时间(秒)	状态	回包信息			
								源地址	目的地址	源端口	目的端口
1	tcp	189.16.100.55	189.16.100.123	2884	8888	28799	established	189.16.100.123	189.16.100.55	8888	2884
2	tcp	189.16.100.55	189.16.100.123	2809	8283	23163	established	189.16.100.123	189.16.100.55	8283	2809

第1页/1页 跳转到 页 Go 每页 行

图 14-6 Session 状态图

14.5 同步选项配置



图 14-7 HA 同步选项配置

此界面完成以下功能

- 同步 HA 的时间
- 配置 HA 同步命令行的关键字
- 同步抗攻击黑白名单

表 14-1 同步选项配置参数说明

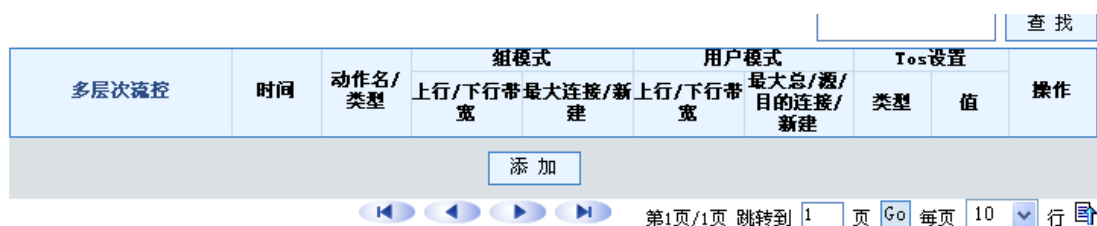
属性名称	描述
同步时间	同步 HA 中各设备的时间，每点击一次同步一次
模块命令	同步关键字的备选项
同步关键字	下发命令时，会被同步的命令关键字，关键字为命令行的首单词（不包含 undo）
抗攻击白名单	同步抗攻击的白名单
抗攻击黑名单	同步抗攻击的黑名单

第15章 带宽管理

15.1 基于管道的带宽管理

15.1.1 配置中心

此页面主要实现带宽管理一些参数控制的限制，下图为配置中心页面：



多层次流控	时间	动作名/ 类型	组模式		用户模式		ToS设置		操作
			上行/下行带最大连接/ 宽	新上行/下行带 建	最大总/源/ 目的连接/ 新建	宽	类型	值	
<input type="button" value="添加"/>									

第1页/1页 跳转到 页 Go 每页 10 行

图 15-1 配置中心

15.1.2 管道管理



管道名称	是否生效	内部接口	外部接口	管道动作	IP型带宽策略	HSQ策略	操作
<input type="button" value="添加"/>							

第1页/1页 跳转到 页 Go 每页 10 行

图 15-2 管道管理

进入系统界面，点击带宽管理—基于管道进入图 19-1 所示的界面，点击“添加”按钮进入管道管理界面。

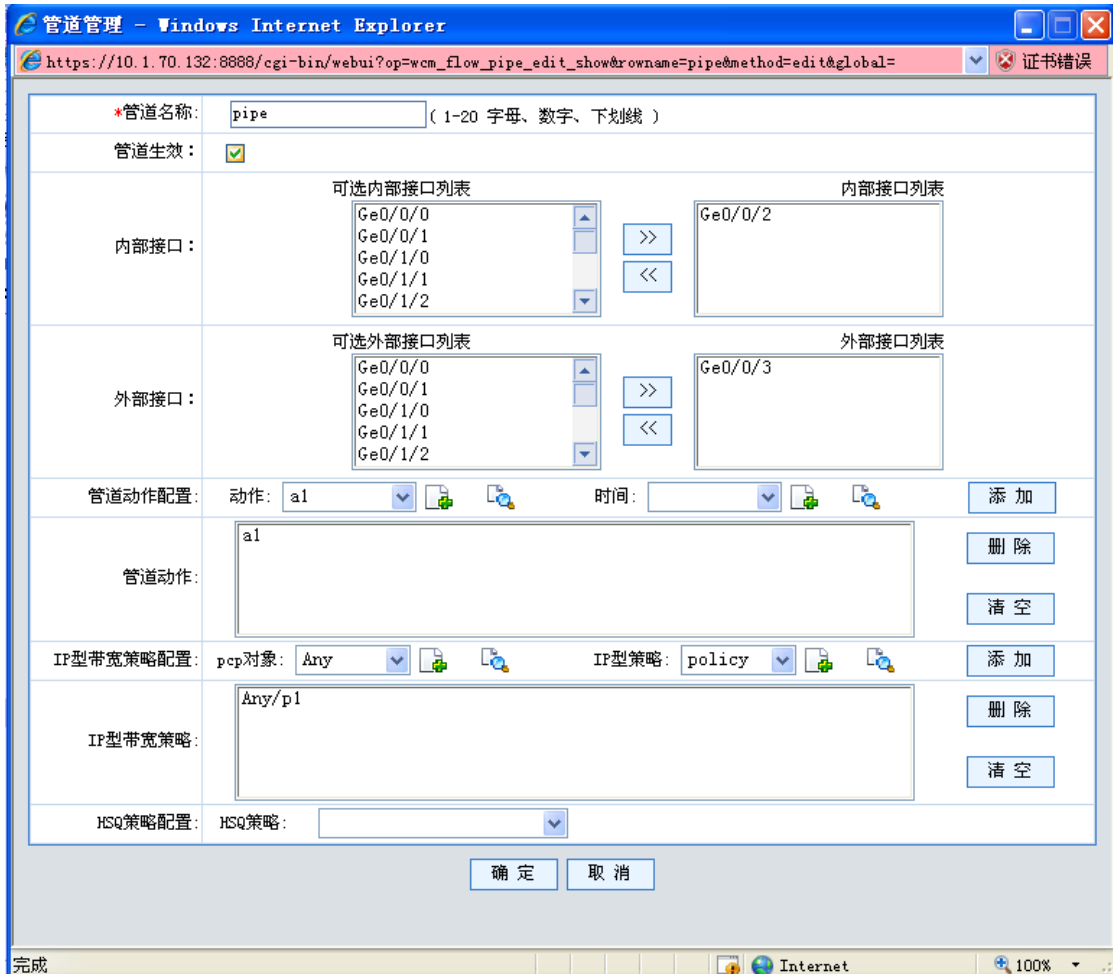




图 15-3 管道管理配置

1. 配置管道名称，管道名称 1~20 长度的字符串，字母开头，字母数字下划线组合，不能是 a、a1、all。
2. 配置内部接口和外部接口，只需选中某个接口点击向右的箭头即可添加到右部空白栏。
3. 同理删除只需选中右栏中的接口点击向左箭头按钮即可。
4. 使管道生效，只需选中即可。
5. 配置动作或 IP 型带宽策略，如果已经配置好动作后策略只需在相应的下拉框中选择即可，否则需要进入相应的界面进行配置。
6. 在图 19-2 所示的管道管理界面中点击时间后面的  进入图 7-4 所示的时间维护界面

15.1.3 IP 型策略管理

在图 19-2 所示的管道管理界面中点击时间后面的  或者图 7-1 点击 IP 型策略管理进入图 19-6 所示的 IP 型策略维护界面

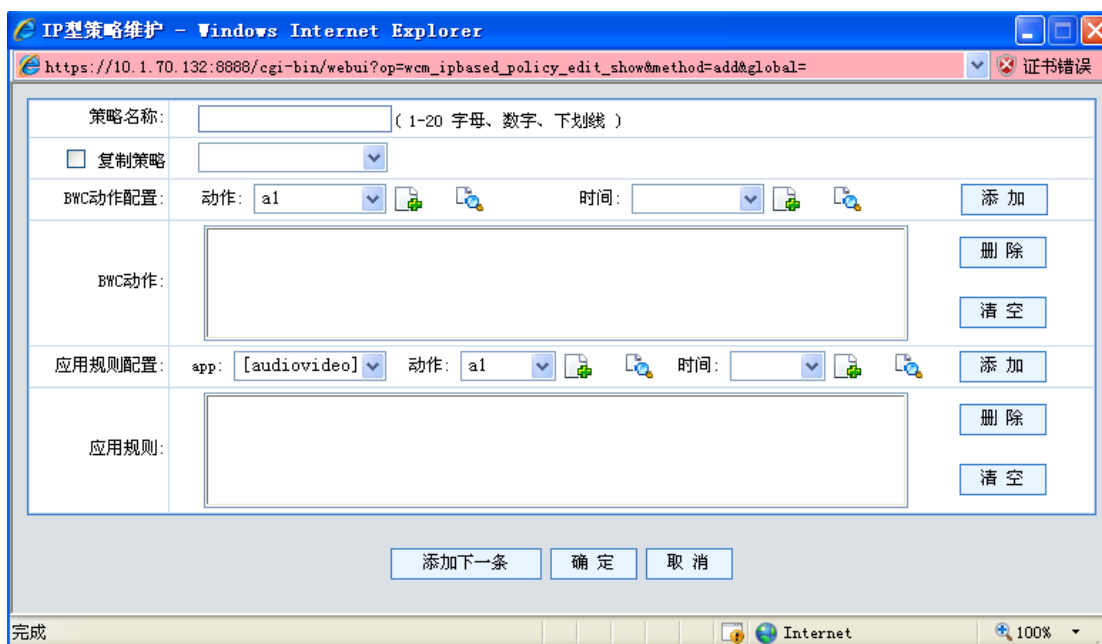


图 15-4 IP 性策略配置


创建策略名称 1~20 长度的字符串，字母开头，字母数字下划线组合，不能是 a、al、all。

在动作的下拉表中寻找自己需要的带宽管理动作，如没有，进入动作维护界面进行相应的动作设置。

时间拉菜单中添加时间对象，如没有进行相应的时间配置。

配置应用规则，应用规则列表中选择需要的应用规则。然后配置相应的动作和时间。

15.1.4 动作管理

在图 19-2 所示的管道管理界面中点击动作后面的  或者图 19-1 点击动作管理进入图 19-3 所示的动作维护界面

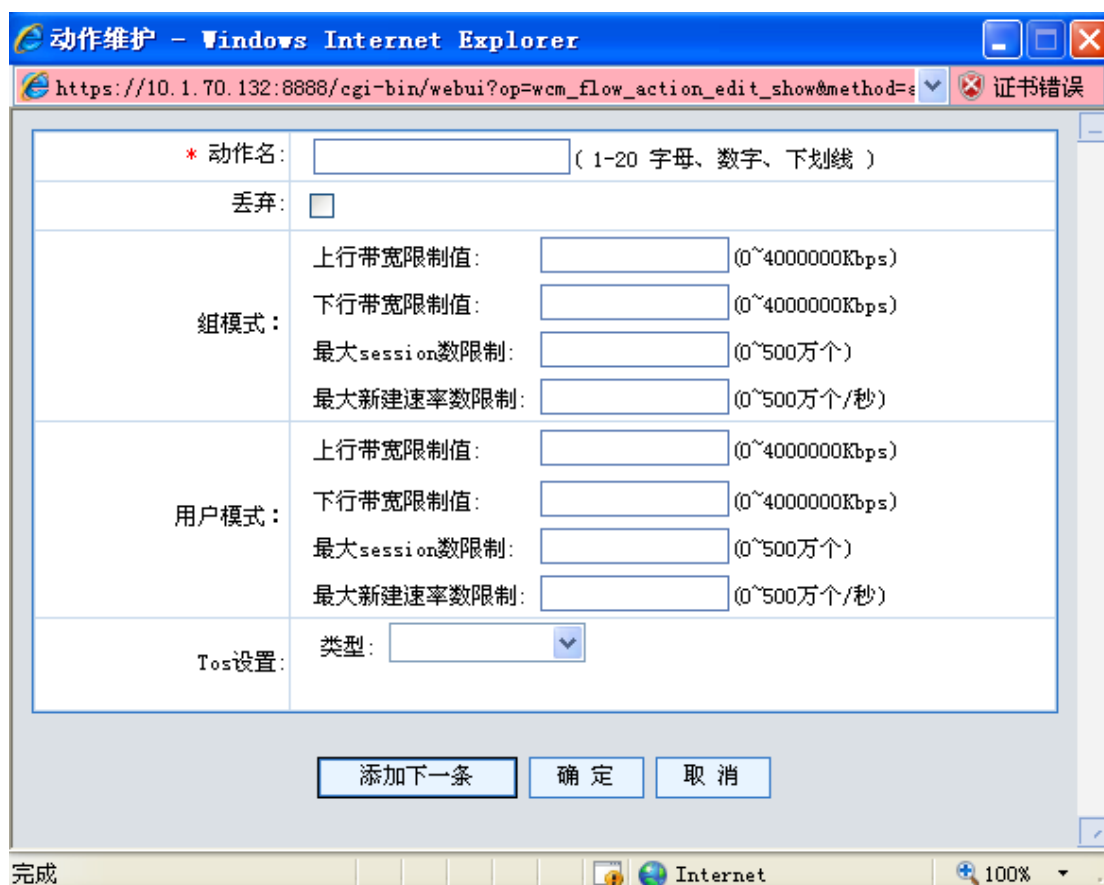


图 15-5 动作列表配置

配置相应的动作名称 1~20 长度的字符串，字母开头，字母数字下划线组合，不能是 a、al、all。

配置相应的带宽模式，可以是组模式也可以用户模式，或者是两者同时配置。

配置相应的优先级，选择必要的类型。

15.2 基于接口的带宽管理

15.2.1 物理限速

物理限速 (Line Rate, LR)，可以在一个物理接口上利用令牌桶限制发送报文的总速率。当用户对所有报文限速时，使用物理限速较为方便。物理限速配置：

接口名称	是否启用物理限速
Ge0/0/0	<input checked="" type="checkbox"/> 详细配置
Ge0/0/1	<input checked="" type="checkbox"/> 详细配置
Ge0/0/2	<input checked="" type="checkbox"/> 详细配置
Ge0/0/3	<input checked="" type="checkbox"/> 详细配置

图 15-6 物理限速

物理限速数据域说明见表。

表 15-1 物理限速数据域说明

域名	说明
接口名称	物理网口的名称
是否启用物理限速	对指定的物理接口进行限速配置

在每一个接口配置行中，点击“详细配置”进入详细配置页面，如图 6-2 所示：



图 15-7 物理限速配置页面

该配置页面对应的数据域说明见表：

表 15-2 物理限速配置数据域说明

域名	说明
承诺信息速率 (CIR)	范围为 0-4000, 000(kbps)，不能超过 CBS×20
承诺突发尺寸 (CBS)	范围介于 CIR/20 和 CIR 之间
超出突发尺寸 (EBS)	范围介于 CIR/20 和 CIR 之间，ebs 必须大于或等于 cbs

当配置完成后，点击“应用”按钮表示配置生效；点击“取消应用”表示取消配置；点击“返回”按钮返回上层页面。

15.2.2 QoS 标签

一个 qos-tag (qos 标签) 既可以认为是一组 QoS 面向目标的集合，也可以认为是针对某类特性的数据流打上的 QoS 标签。可以使用 qos-tag 预定义一个 QoS 规则的目标数据流的特性，也可以将一个 qos-tag 给多个 QoS 规则复用，qos-tag 的存在保证了配置的灵活性和可扩展性。目前 qos-tag 只支持 pcp。

Qos 标签页面：




图 15-8 QoS 标签

QoS 标签数据域描述见表。

表 15-3 QoS 标签数据域

域名	说明
QoS 标签	QoS 标签的标识符
PCP 规则	QoS 标签绑定的 PCP 规则
服务	
操作	对 QoS 标签操作

图标 ：表示编辑 QoS 标签。

图标 ：表示删除 QoS 标签。

按钮“添加”：表示添加新的 QoS 标签。

按钮“查找”：表示查找指定条件的 QoS 标签。

1. 添加 qos-tag

点击“添加”按钮，弹出 qos-tag 添加页面，如图所示：

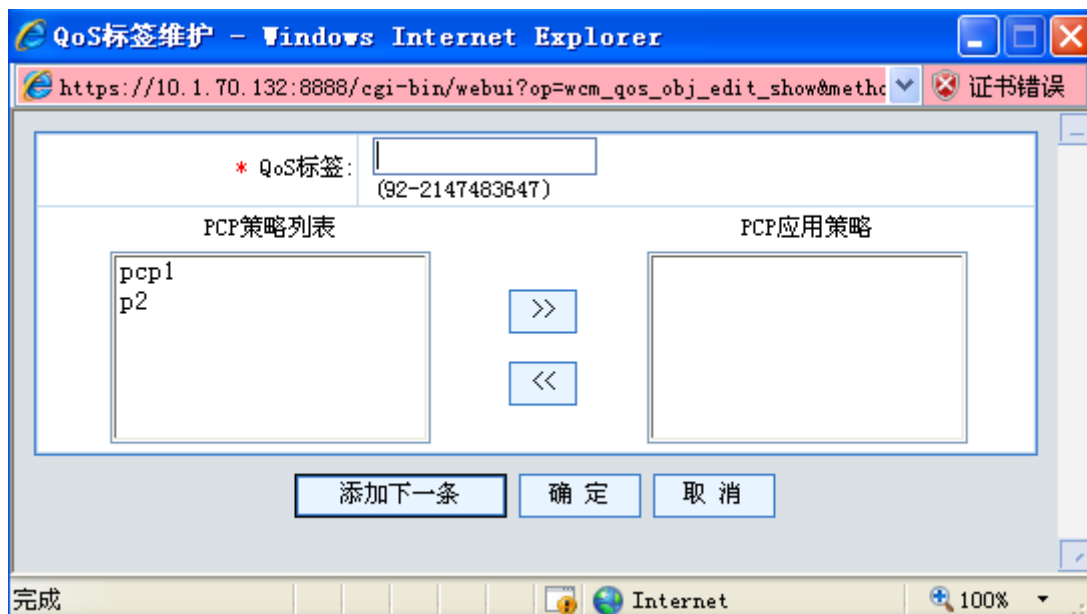


图 15-9 添加 qos-tag

添加 QoS 标签页面对应的数据域说明见表。

表 15-4 添加 QoS 标签数据域

域名	说明
QoS 标签	QoS 标签的标识符，用整数表示，范围为 92~2147483647
PCP 策略列表	系统中已存在的 PCP 列表
PCP 应用策略	将 PCP 规则绑定到该 QoS 标签上

按钮 ”>>”：表示将 PCP 绑定到该 QoS 标签上。

按钮 “<<”：表示将 PCP 从该 QoS 标签摘除下来。

按钮“添加下一条”：表示再添加一条 QoS 标签。

按钮“确定”：表示创建该 QoS 标签。

按钮“取消”：表示取消创建该 QoS 标签。

15.2.3 IPQoS

IPQoS 是一种基于 IP 的带宽管理策略，可以控制单个 IP 的上行和下行的带宽。

IPQoS 控制页面如图 6-8 所示：



图 15-10 IPQoS 页面

IPQoS 的数据域说明见表。

表 15-5 IPQoS 页面

域名	说明
策略序号	IPQoS 的标识符
类型	IPQoS 策略的类型，包括 ip-range 和 qos-tag 两种类型。 ip-range:表示该策略是基于该地址段的所有 IP 进行带宽管理。 qos_tag:表示该策略是基于该 qos_tag 内的所有 IP 进行带宽管理
QoS 标签	基于 qos_tag 类型的 IPQoS 策略绑定的 qos_tag 的序号
IP 地址段	基于 ip-range 类型的 IPQoS 策略绑定的 IP 地址段
上行限制值 (kbps)	上行限制带宽，单位是 kbps
下行限制值 (kbps)	下行限制带宽，单位是 kbps
操作	对该 IPQoS 策略的修改或删除

按钮“查找”：表示查找指定条件的 IPQoS 策略。

按钮“添加”：表示添加新的 IPQoS 策略。

IPQoS 策略添加页面如图所示：



图 15-11 添加 IPQoS 策略

添加 IPQoS 策略页面的数据域见表。

表 15-6 IPQoS 页面

域名	说明
IPQoS 策略序号	IPQoS 的标识符，用整数表示，范围 0~2147483647

限流类型	IPQoS 策略的类型，包括 ip-range 和 qos-tag 两种类型。 ip-range:表示该策略是基于该地址段的所有 IP 进行带宽管理。 qos_tag:表示该策略是基于该 qos_tag 内的所有 IP 进行带宽管理
QoS 标签	基于 qos_tag 类型的 IPQoS 策略绑定的 qos_tag 的序号
IP 地址段	基于 ip-range 类型的 IPQoS 策略绑定的 IP 地址段
上行限制值 (kbps)	上行限制带宽，单位是 kbps
下行限制值 (kbps)	下行限制带宽，单位是 kbps
操作	对该 IPQoS 策略的控制

15.2.4 流量监管

15.2.4.1 策略定义

流量监管策略定义对哪些报文实施流量监管。

本命令的重复执行可以创建最多 128 个流量监管策略。本命令只对 IP 数据包进行处理，对其他的数据包不进行处理。



策略名称	QoS标签	承诺信息速率 (kbps)	承诺突发尺寸 (kbits)	超出突发尺寸 (kbits)	修改TOS	黄色报文	红色报文	操作
fl_5	92	2000000	3000000	200000		丢弃数据包	丢弃数据包	 


图 15-12 流量监管策略显示

策略定义的数据域说明见表。

表 15-7 流量监管页面

域名	说明
策略名称	流量监管的标识符
QoS 标签	和流量监管绑定的 qos_tag
承诺信息速率 (CIR)	范围为 0-4000, 000 (kbps) 不能超过 CBS×20
承诺突发尺寸 (CBS)	范围介于 CIR/20 和 CIR 之间
超出突发尺寸 (EBS)	范围介于 CIR/20 和 CIR 之间，ebs 必须大于或等于 cbs
修改 TOS	修改 TOS 值从而改变报文优先级
黄色报文	是指大于 cir+cbs 小于 cir+ebs 速率的报文。
红色报文	红色报文是指大于 cir+ebs 速率的报文
操作	

“添加”按钮：弹出流量监管策略配置窗口如图所示。

图标 : 表示编辑流量监管策略。

图标 : 表示删除流量监管策略。

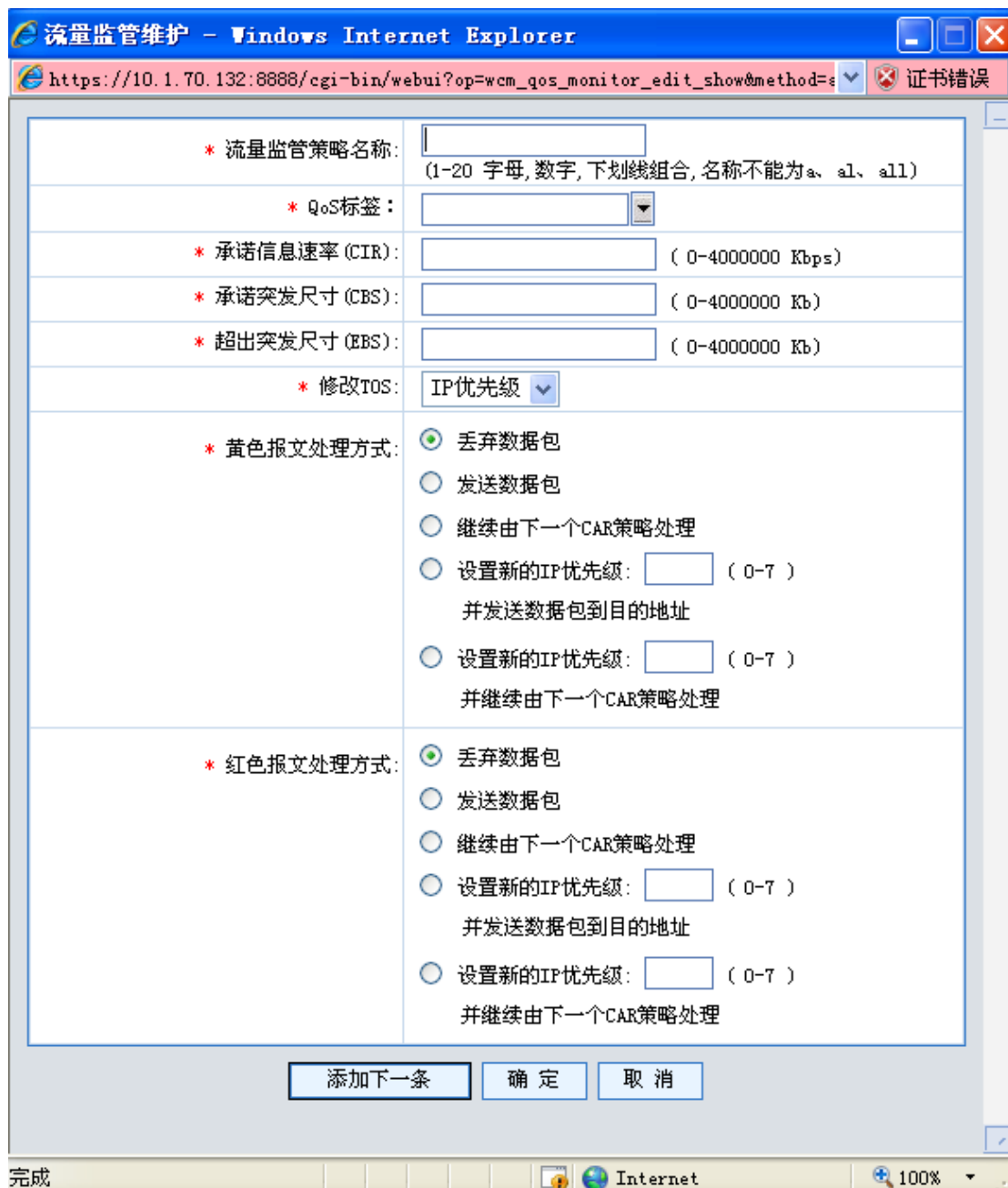


图 15-13 添加流量监管策略

填写相应的配置后点击“确定”按钮完成添加。

表 15-8 流量监管策略配置数据域

域名	说明
流量监管策略名称	流量监管的标识符
QoS 标签	和流量监管绑定的 qos_tag

承诺信息速率 (CIR)	范围为 0-4000, 000 (kbp) 不能超过 CBS×20
承诺突发尺寸 (CBS)	范围介于 CIR/20 和 CIR 之间
超出突发尺寸 (EBS)	范围介于 CIR/20 和 CIR 之间, ebs 必须大于或等于 cbs
修改 TOS	修改 TOS 值从而改变报文优先级
黄色报文处理方式	<p>黄色报文是指大于 cir+cbs 小于 cir+ebs 速率的报文。</p> <ul style="list-style-type: none"> a) 丢弃数据包 b) 发送数据包 c) 继续由下一个 CAR 策略处理: 继续由下一个流量监管策略处理 d) 设置新的 IP 优先级 (范围 0~7), 并发送数据包到目的地址 e) 设置新的 IP 优先级 (范围 0~7), 并继续由下一个 CAR 策略处理
红色报文处理方式	<p>红色报文是指大于 cir+ebs 速率的报文</p> <ul style="list-style-type: none"> a) 丢弃数据包 b) 发送数据包 c) 继续由下一个 CAR 策略处理 d) 设置新的 IP 优先级 (范围 0~7), 并发送数据包到目的地址 5、设置新的 IP 优先级 (范围 0~7), 并继续由下一个 CAR 策略处理
操作	

15. 2. 4. 2 策略应用

在配置了流量监管策略后, 需要在接口上指定一个策略来应用, 在每个接口下最多可以配置 8 条流量监管策略, 在同一接口上应用流量监管策略时, 不能同时应用两条或两条以上针对同一个 qos-tag 的策略, 不能同时应用两条针对所有报文的策略。





接口名称	入口监管策略	出口监管策略	操作
Ge0/0/0	f1o_b		
Ge0/0/1			
Ge0/0/2			
Ge0/0/3			

图 15-14 流量监管策略应用

QoS 流量监管策略应用数据域见表

表 15-9 流量监管策略应用数据域

域名	说明
----	----

接口名称	物理网口的名称
入口监管策略	入口应用的监管策略名称
出口监管策略	出口应用的监管策略名称
操作	编辑操作

在希望应用流量监管策略的接口条目中点击“编辑”按钮，弹出窗口：



图 15-15 编辑应用的流量监管策略

接口流量监管策略应用数据域见表。

表 15-10 流量监管策略应用数据域

域名	说明
接口名称	物理网口的名称
策略名称	选择要应用的策略名称
方向	应用在网口的出或入方向
策略应用	应用列表

15.2.5 流量整形

流量整形（Traffic-Shaping）对网络流量进行识别和控制，使网络不会产生不必要的断网和拥塞。

15.2.5.1 策略定义

流量整形策略定义如图所示：

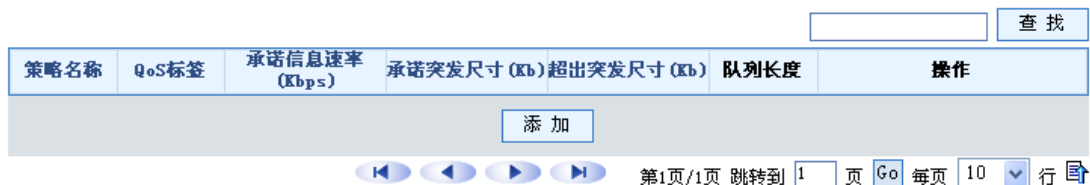


图 15-16 编辑应用的流量监管策略

流量整形策略的数据域见表。

表 15-11 流量整形策略数据域

域名	说明
策略名称	流量整形策略名称
QoS 标签	流量整形要绑定的 QoS 策略
承诺信息速率 (CIR)	范围为 0-4000, 000 (kbps) 不能超过 CBS×20
承诺突发尺寸 (CBS)	范围介于 CIR/20 和 CIR 之间
超出突发尺寸 (EBS)	范围介于 CIR/20 和 CIR 之间, ebs 必须大于或等于 cbs
队列长度	用于整形队列的长度
操作	编辑和删除

“添加”按钮：弹出流量监管策略配置窗口如图所示。

图标：表示编辑流量整形策略。

图标：表示删除流量整形策略。

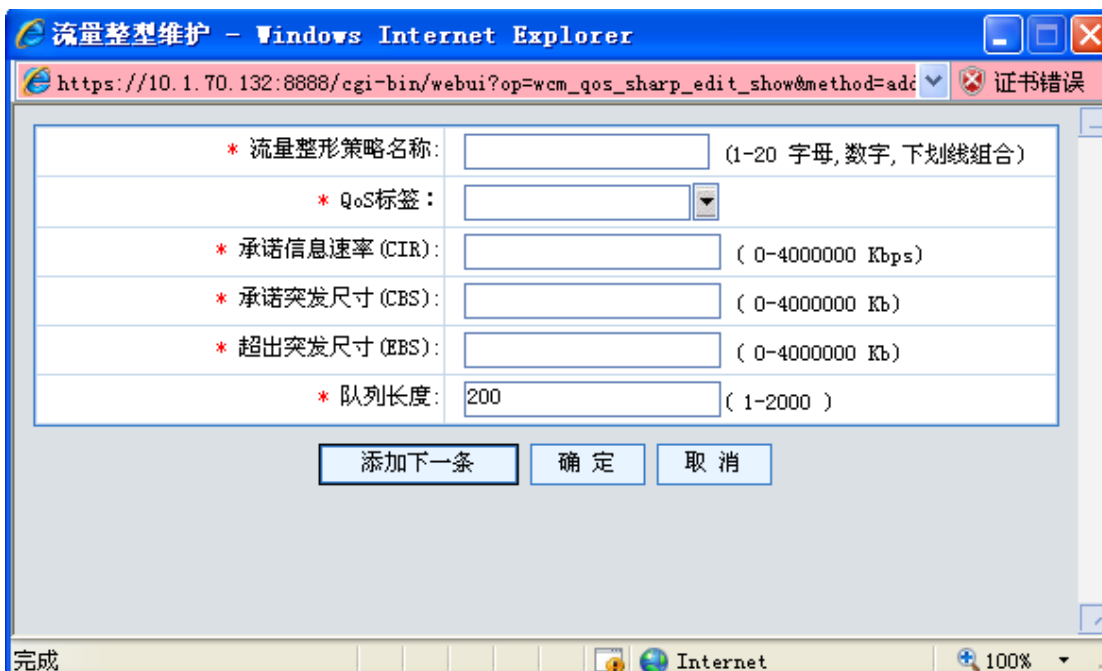


图 15-17 编辑应用的流量监管策略

表 15-12 流量整形添加数据域

域名	说明
----	----

策略名称	流量整形策略名称
QoS 标签	流量整形要绑定的 QoS 策略
承诺信息速率 (CIR)	范围为 0-4000, 000 (kbps) 不能超过 CBS×20
承诺突发尺寸 (CBS)	范围介于 CIR/20 和 CIR 之间
超出突发尺寸 (EBS)	范围介于 CIR/20 和 CIR 之间, ebs 必须大于或等于 cbs
队列长度	用于整形队列的长度
操作	编辑和删除

按钮“添加下一条”：表示再添加一个新的流量整形策略。

按钮“确定”：表示创建该流量整形策略 s

按钮“取消”：表示取消创建该流量整形策略。

15. 2. 5. 2 策略应用

流量整形策略应用界面如图所示：





接口名称	流量整形策略	操作
Ge0/0/0		
Ge0/0/1		
Ge0/0/2		
Ge0/0/3		

图 15-18 流量整形策略应用

流量整形应用策略页面数据域见表

表 15-13 流量整形添加数据域

域名	说明
接口名称	物理网口的名称
流量整形策略	流量整形策略名称
操作	应用


图标：表示应用选择流量整形策略，见图



图 15-19 流量整形策略应用

按钮“>>”：表示应用该策略。

按钮“<<”：表示取消应用该策略。

15.2.6 拥塞管理

对于网络设备，当报文到达的速度大于该接口发送报文的速度时，在该接口处就会产生拥塞。如果没有足够的存储空间来保存这些报文，其中的一部分就会丢失。报文的丢失又可能会导致发送该报文的设备因超时而重传，导致恶性循环。

拥塞管理的中心内容就是当拥塞发生时如何在各个队列之间进行调度，决定报文转发的处理顺序。

拥塞管理配置包括：

- 打开全局的 QOS 拥塞管理开关
- 定义队列调度的参数
- 对于其中的一些队列调度，还要定义 qos-tag
- 在接口上选择一个队列调度方式，对于 PQ 和 CQ 则要选择队列调度策略

15.2.6.1 队列应用

队列应用是接口缺省使用的队列调度机制，可以通过配置命令改变其队列长度。

队列应用拥塞策略配置只有一项：配置 FIFO 队列的长度。

接口名称	先进先出队列 (FIFO)	优先级队列 (PQ)	定制队列 (CQ)	加权公平队列 (WFQ)	分层可共享队列 (HSQ)	CBQ队列 (CBQ)	实时优先级队列 (RTP)
Ge0/0/0	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置
Ge0/0/1	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置
Ge0/0/2	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置
Ge0/0/3	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置	<input checked="" type="checkbox"/> 详细配置

图 15-20 拥塞管理队列应用显示

15. 2. 6. 2 优先级队列

组序号	队列优先级	QoS标签序号	队列长度	缺省队列	操作
<input type="text"/> <input type="button" value="查找"/>					
<input type="button" value="添加"/>					
第1页/1页 跳转到 <input type="text" value="1"/> 页 <input type="button" value="Go"/> 每页 <input type="text" value="10"/> 行					

图 15-21 优先级策略显示

1. 配置具有 qos-tag 标签报文对应的优先级队列

在上图中点击“编辑”编辑按钮，弹出窗口：



图 15-22 优先级队列配置

在四个队列的“QoS 对象”栏中选择“Qos 标签”，



图 15-23 优先级队列配置

点击“确定”按钮。

说明：

组序号：在某个接口上使用时最多只能选择其中的一组使用。

Qos 对象：队列对应的 qos 标签

high: 优先级最高的队列

medium: 优先级次最高的队列

normal: 优先级第三高(次最低)的队列

low: 优先级最低的队列

2. 配置优先级缺省处理队列

如果报文不能匹配 PQ 报文分类策略，则必须为此配置一个缺省处理队列。

可以给一个 PQ 拥塞管理策略定义多条规则，然后把该策略应用在某接口上。当一个报文到达该接口时（注意，这里指报文的出接口），系统沿规则链匹配该报文，如果匹配上某规则，则进入相应的队列，匹配结束；如果报文不与任何规则匹配，则进入缺省队列。

缺省队列的缺省值为 normal。



图 15-24 设置缺省队列

点击“设置默认队列”下的“”按钮，点击“确定”按钮。

3. 配置优先级各个优先级队列的长度



图 15-25 配置优先级队列长度

在队列长度栏的输入框中填写各队列的长度，点击“确定”按钮。



图 15-26 特定端口上的优先级队列

在“优先级队列策略组”中选择一个希望配置的组索引，



图 15-27 特定策略组的优先级队列

点击“应用”按钮。

15.2.6.3 定制队列

根据前面的介绍，定制拥塞管理共有 16 个队列，各个队列之间的调度是按照轮询方式。

定制拥塞管理的配置包括：

- 配置定制拥塞管理策略

- 配置定制缺省处理队列
- 配置定制各个队列长度
- 配置定制允许一个队列最大发送的报文字节数



图 15-28 定制队列策略显示

1. 配置具有 qos-tag 标签报文对应的定制队列


在上图中点击 “” 编辑按钮，弹出窗口：



图 15-29 编辑定制队列策略

在队列的“QoS 对象”栏中选择“Qos 标签”，点击“确定”按钮。

说明：

组序号:CQ 队列配置组索引，范围是从 1 到 16 的整数。最多支持 16 组 CQ 队列配置，在某个接口上使用时最多只能选择其中的一组使用，下面命令行对该字段的解释相同。

队列序号:Cq 内的子队列 id，包含 16 个，用户可以根据自己的环境使用其中的一些或全部。

Qos 对象:队列对应的 qos 标签名称

2. 配置 CQ 缺省处理定制队列



图 15-30 配置 CQ 缺省处理队列

点击上图中“设置默认队列”下的“”按钮，点击“确定”按钮。

说明：

缺省子队列是 16 号子队列。

3. 配置定制队列中缓存的报文的数量限制



图 15-31 配置缓存报文数量限制

在上图中“报文最大数量”栏的输入框中填写各队列的长度，点击“确定”按钮。

说明：

队列中缓存的报文数量的最大限制. 范围为 1-2000，缺省值为 200

4. 配置定制允许一个队列连续发送的报文字节数



图 15-32 配置连续发送的报文字节数

在上图中“连续报文发送数”栏的输入框中填写各队列的长度，点击“确定”按钮。

说明：

1. 连续报文发送数：当 Guard 调度 CQ 的用户队列时，它连续从这个队列中取出报文进行发送，直到发送的字节数大于等于为该队列配置的“连续报文发送数”的值或者队列为空，再转而调度 CQ 的下一个队列。因此，“续报文发送数”的值会影响 CQ 各用户队列之间占用接口带宽的比例关系，并且决定了多长时间 Guard 才会调度 CQ 的下一个队列。”连续报文发送数”的缺省字节数为 15000。
2. 如果“连续报文发送数”的值过小，由于 Guard 每次至少发送一个报文才会转向下一个队列，各个队列实际获得的带宽很可能与预想的效果相差甚远；如果“连续报文发送数”值过大，则可能会造成队列间切换延迟太大。

5. 在接口上选择定制队列

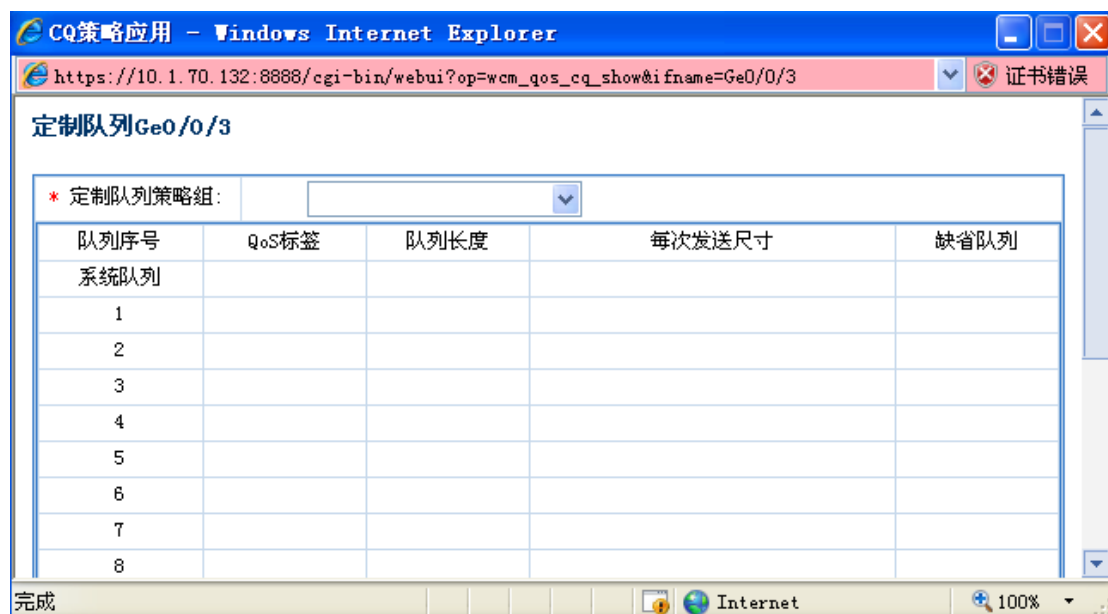


图 15-33 接口上的定制队列

在“定制队列策略组”中选择一个索引，点击“应用”按钮。

说明：

在接口上选择了 CQ 队列后，并不意味着应用该队列策略，还需要打开 QOS 的拥塞管理功能开关才能真正应用。

15. 2. 6. 4 加权公平队列

1. 队列定义

添加加权队列如图所示：



图 15-34 加权公平队列

加权公平队列配置的数据域见表

表 15-14 加权公平队列

域名	说明
队列序号	队列的唯一标识符
解析方式	方式 1-IP 优先级：根据 IP 优先级进行队列调度 方式 2-差分服务编码：根据差分服务编码进行队列调度
队列长度	用于 WFQ 子队列的长度
拥塞避免策略	要应用的拥塞避免的策略

2. 拥塞避免

根据前面的介绍，WFQ 是基于 FQ 拥塞管理机制的。

要想实施加权公平队列拥塞管理，必须对报文进行分类。WFQ 对报文按流进行分类，对于 IP 网络，五元组（源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议号）和 IP 优先级或者 DSCP 相同的报文属于同一个流。在接入层的网络中，通常使用 IP 优先级和五元组配合进行流分类；在汇聚层网络中通常使用 DSCP 值和五元组配合进行流分类。WFQ 默认是使用 IP 优先级和五元组配合进行流分类。

WFQ 加权公平拥塞管理的配置只包括一项：

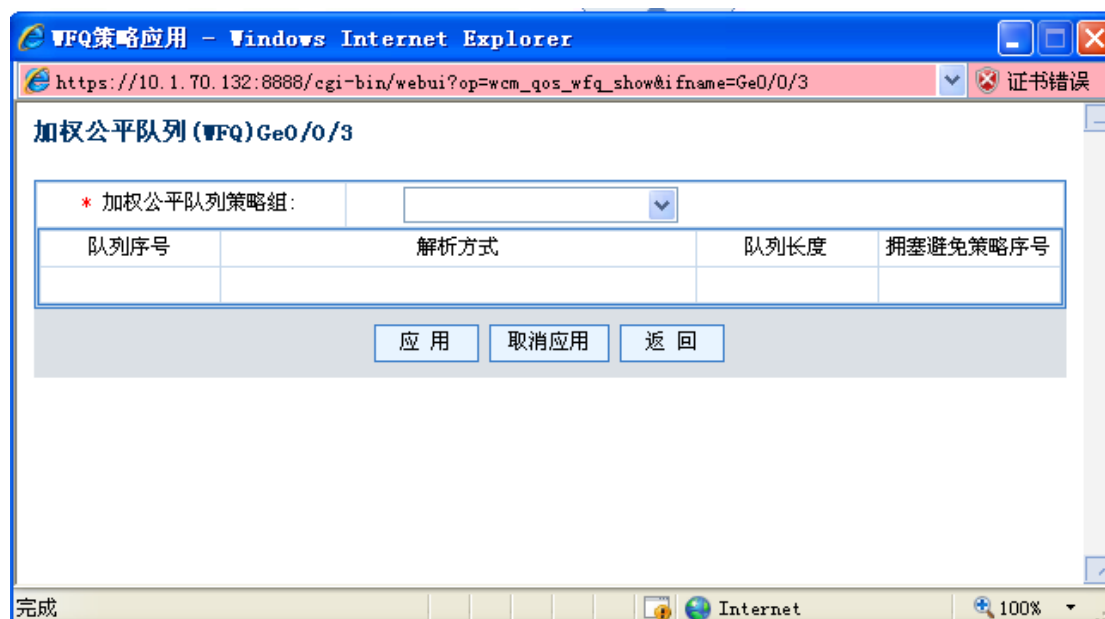


图 15-35 加权公平队列配置

点击“应用”按钮。

说明：

1. 配置队列长度：最大长度为 100，缺省为 10。
2. 子队列总数：队列的总数目，可取的值为：16、32、64、128、256、512、1024、2048、4096，缺省值为 256。

在接口上选择了 WFQ 队列后，并不意味着应用该队列策略，还需要打开 QOS 的拥塞管理功能开关才能真正应用。

15. 2. 6. 5 CBQ 配置队列

1. CBQ 行为

添加 CBQ 行为如图所示：



图 15-36 基于类的队列行为配置

CBQ 行为配置的数据域见表

表 15-15 加权公平队列

域名	说明
行为名称	行为对应的名称
行为类型	类型 1：加速转发行为 类型 2：确保转发行为
带宽配置	类型 1： 带宽速率：行为带宽速率值，范围为（0-4000000kbps） 承诺突发尺寸：突发尺寸，范围为（0-4000000B）可选参数 类型 2： 带宽比例：行为所占总带宽的比例，范围（0-100） 承诺突发尺寸比例：突发尺寸所占总承诺突发尺寸的比例，范围（0-100）

2. CBQ 队列

添加 CBQ 队列如图所示：



图 15-37 基于类的队列配置

CBQ 队列配置的数据域见表

表 15-16 加权公平队列

域名	说明
队列序号	范围：（数字 0-4294967295）
默认队列	类型 1：默认队列采用 FIFO 队列，长度范围（1-2000）默认是长度 200 类型 2：默认队列采用 WFQ 队列，参数为 wfq 队列序号
行为配置	添加/删除默认行为 af1、af2、af3、af4、ef，行为绑定 qos-tag 添加/删除自定义行为，行为绑定 qos-tag

3. 在接口上应用 CBQ

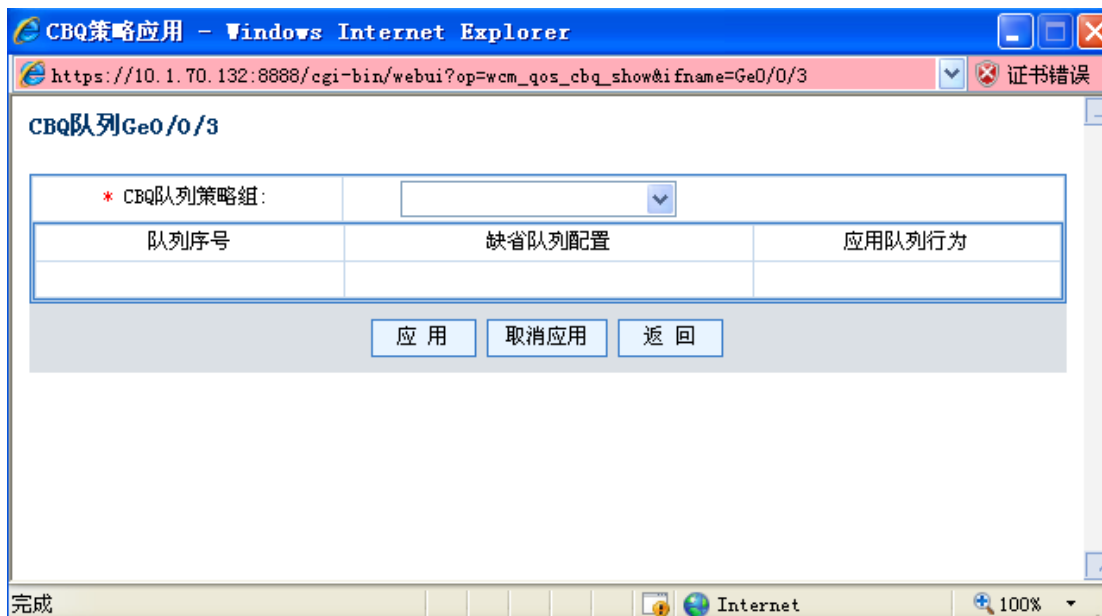


图 15-38 基于类的队列在接口上应用

点击“应用”按钮。

15. 2. 6. 6 分层可共享队列

前面介绍的拥塞管理，基本上都能满足用户的需求，但是，拥塞管理粒度还不够，而且在链路空闲的情况下，灵活的共享带宽方面有所欠缺，为此提出分层令牌桶可共享带宽拥塞管理。

1. 分层可共享(HSQ)管理配置

分层可共享(HSQ)拥塞管理配置包括：

- 对报文进行分类，配置报文分类策略 PCP
- 进入拥塞管理视图
- 规划报文穿过的通道
- 定义拥塞管理策略
- 在接口视图下应用拥塞管理策略

2. 规划报文穿过的通道

报文穿过的通道按照 Tree 层次进行规划，如下图所示：

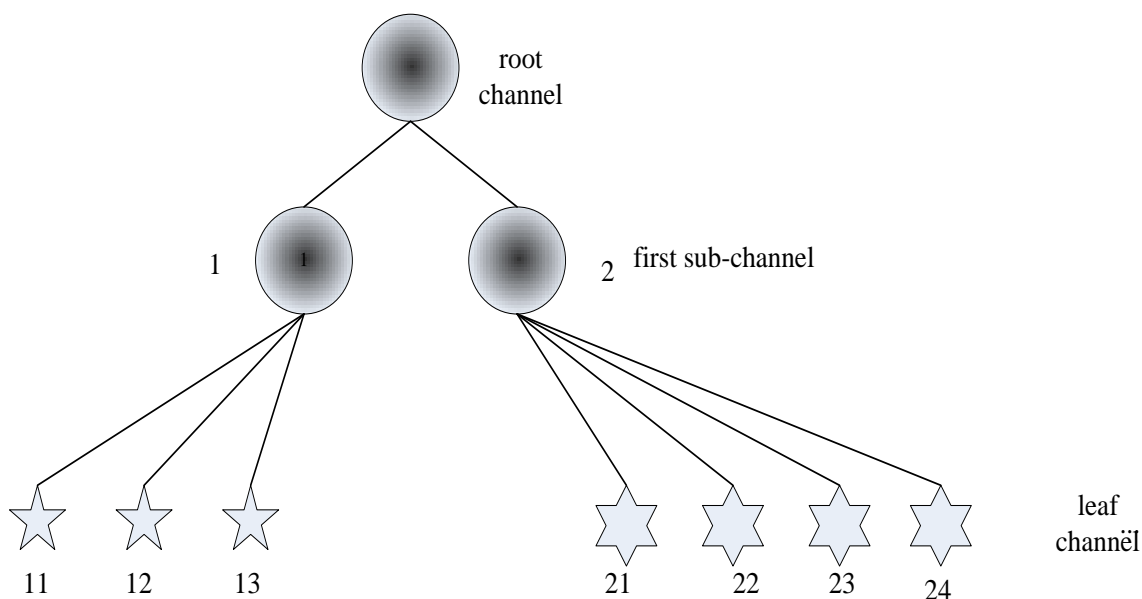


图 15-39 报文穿过的通道规划

通道规划好之后，下面需要对各个通道进行配置。

3. HSQ 定义页面

HSQ 定义显示页面如图所示

根通道配置					一级通道配置	二级通道配置	操作
队列序号	通道序号	保证带宽	最大带宽	突发尺寸	优先级		
<input type="button" value="添加"/>							
第1页/1页 跳转到 <input type="text" value="1"/> 页 Go 每页 10 行							

图 15-40 HSQ 定义列表

4. 添加 HSQ 根通道

要想创建一棵 HSQ 树，首先必须创建其根节点。

HSQ 创建根节点页面如图所示：



图 15-41 HSQ 定义页面

HSQ 配置页面的数据域说明见表。

表 15-17 HSQ 配置页面

域名	说明
队列序号	HSQ 队列的唯一标识符，范围（0~4294967295）
实时队列	优先级最高的队列，每次发送优先发送该类报文
绑定 QoS 标签	实时队列绑定的 QoS 标签列表
根通道配置-序号	根通道的序号
根通道配置-保证带宽	根通道的保证带宽
根通道配置-最大带宽	根通道的最大的带宽
根通道配置-突发尺寸	根通道的报文突发尺寸
根通道配置-优先级	根通道的优先级，数字越小优先级越高
默认队列	没有匹配上 qos_tag 的报文的发送队列，必须是叶子节点

HSQ 在页面上可以配置 2 级通道，也就是说在根通道下最多包含两级子通道，具体子通道配置方法见小节 10.7.5.5

说明：

1. 通道名称：子通道名称
2. 最小带宽：最小带宽最大不能超过其父通道的最小带宽
3. 最大带宽：最大带宽最大不能超过其父通道的最大带宽

注意：删除子通道会删除根通道下的所有子通道和叶子通道。

5. 添加下级通道

添加下级通道如图所示：



图 15-42 HSQ 定义页面

添加一级通道数据域见表。

表 15-18 HSQ 一级通道配置

域名	说明
通道序号	一级通道节点序号，范围（0~4294967295）
保证带宽	一级通道节点保证带宽
最大带宽	一级通道节点最大带宽
突发尺寸	一级通道节点突发尺寸
优先级	一级通道节点优先级（0~8），数字越小优先级越高。
队列长度	根通道的最大的带宽
QoS 标签	根通道的报文突发尺寸

说明：

1. 通道名称:子通道名称
2. 最小带宽: 最小带宽最大不能超过其父通道的最小带宽
3. 最大带宽: 最大带宽最大不能超过其父通道的最大带宽
4. 优先级: 叶子通道的优先级，只有叶子通道能指定优先级。
5. Qos 对象: 和该叶子通道关联的 Qos 对象名称。
6. 缺省通道: 是否将该叶子通道设置为缺省通道。

7. 在接口上应用拥塞管理策略

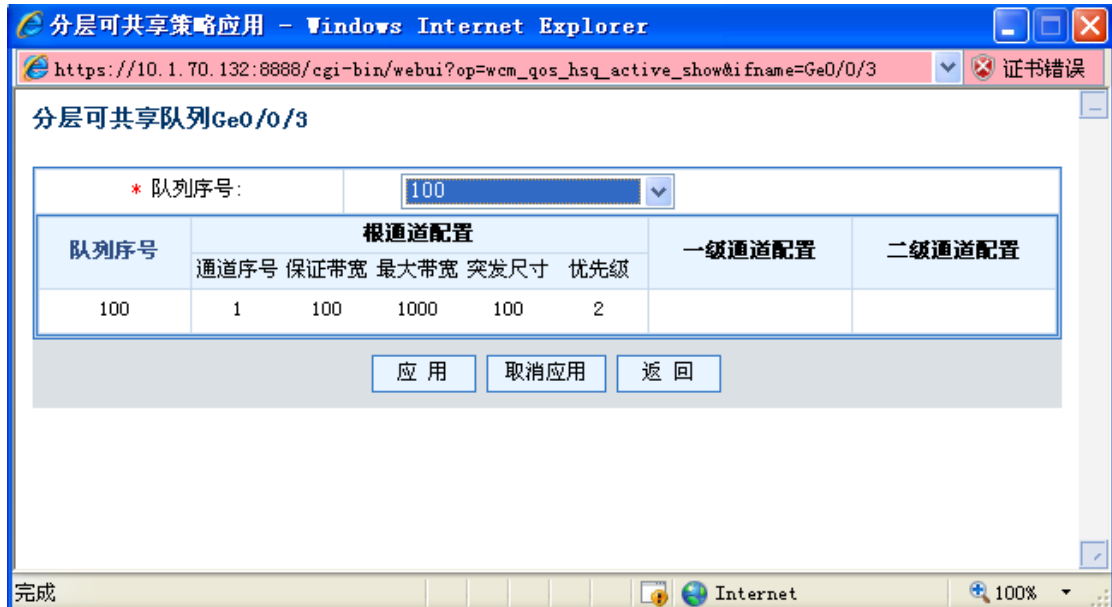


图 15-43 在接口上应用拥塞管理策略

点击“应用”按钮。

注意：

在接口选择 HSQ 队列前，应确保已经配置了缺省叶子通道，否则无法应用，选择了 HSQ 队列后，并不意味着应用该队列策略，还需要打开 QoS 的拥塞管理功能开关才能真正应用。

15. 2. 6. 7 实时优先级队列

8. 实时优先级队列（RTPQ）配置管理

添加 RTP 队列如图所示：

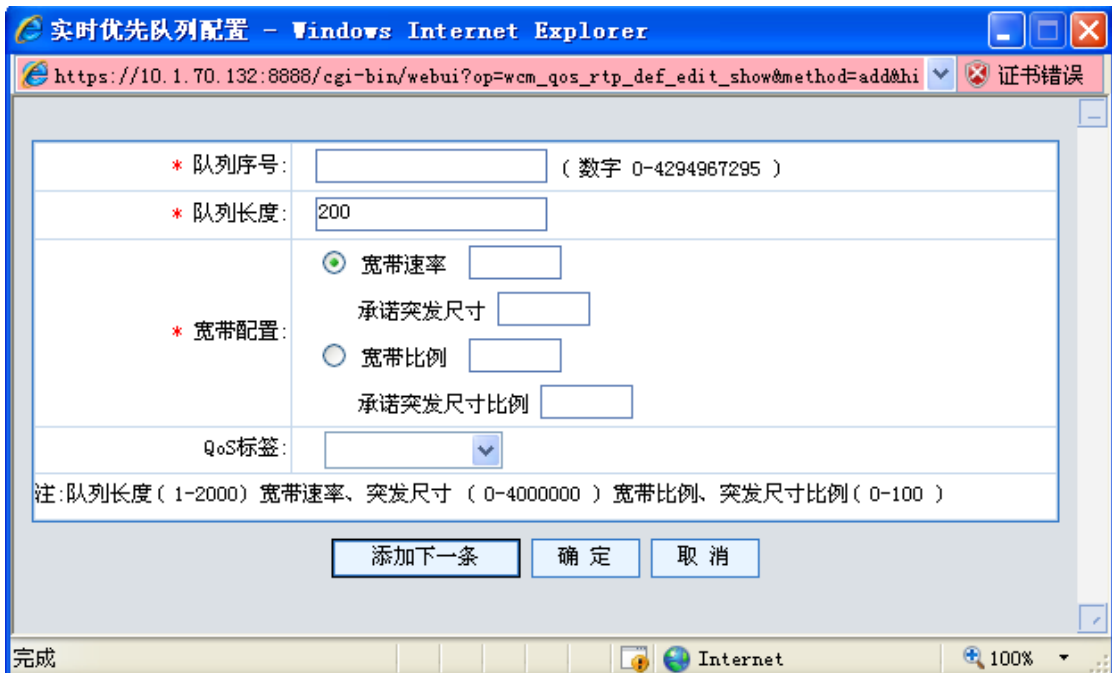


图 15-44 实时优先级队列配置

RTP 队列配置的数据域见表

表 15-19 实时优先级队列

域名	说明
队列序号	队列索引，范围（数字 0-4294967295）
队列长度	配置缓存队列长度，范围（1-2000），默认长度是 200
带宽配置	类型 1： 带宽速率：行为带宽速率值，范围为（0-4000000kbps） 承诺突发尺寸：突发尺寸，范围为（0-4000000B）可选参数 类型 2： 带宽比例：行为所占总带宽的比例，范围（0-100） 承诺突发尺寸比例：突发尺寸所占总承诺突发尺寸的比例，范围（0-100）
QoS 标签	配置对应的报文分类标签

9. 在接口上应用 RTPQ

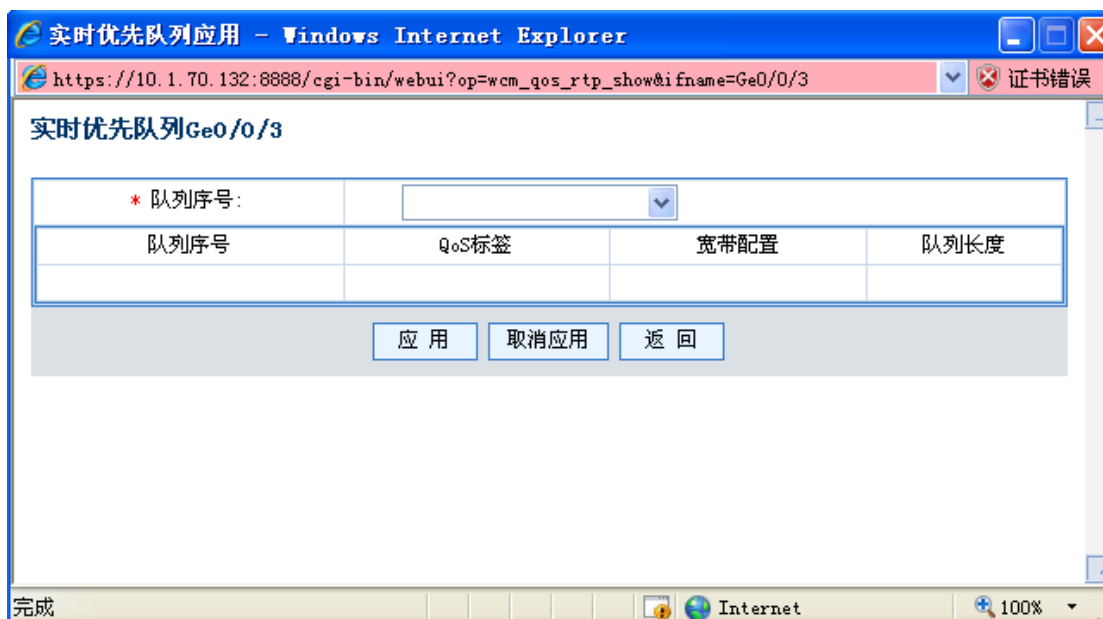


图 15-45 实时优先级队列在接口上应用

点击“应用”按钮。

15. 2. 6. 8 CBQ 配置

CBQ 配置分为 CBQ 行为和 CBQ 队列。

CBQ行为 | CBQ队列

行为名称	行为类型	宽带情况	操作
af1	确保转发行为	2%	 
af2	确保转发行为	2%	 
af3	确保转发行为	2%	 
af4	确保转发行为	2%	 
ef	加速转发行为	2%	 

添加

第1页/1页 跳转到 页 Go 每页 10 行

图 15-46CBQ 配置

15.3 流量优化

15.3.1 带宽借用

带宽借用是在利用分层可共享 (HSQ) 技术的基础上增加上行、下行以及应用协议识别等功能上实现的，可是实现基于管道、PCP、应用协议、上行、下行的分层带宽借用共享功能。

(1) 分层可共享(HSQ)管理配置

分层可共享(HSQ)拥塞管理配置包括：

- 对报文进行分类，配置报文分类策略 PCP 和应用协议
- 规划报文穿过的通道
- 定义 HSQ 管理策略
- 在管道视图下应用 HSQ 管理策略

(2) 规划报文穿过的通道

报文穿过的通道按照 Tree 层次进行规划，如下图所示：

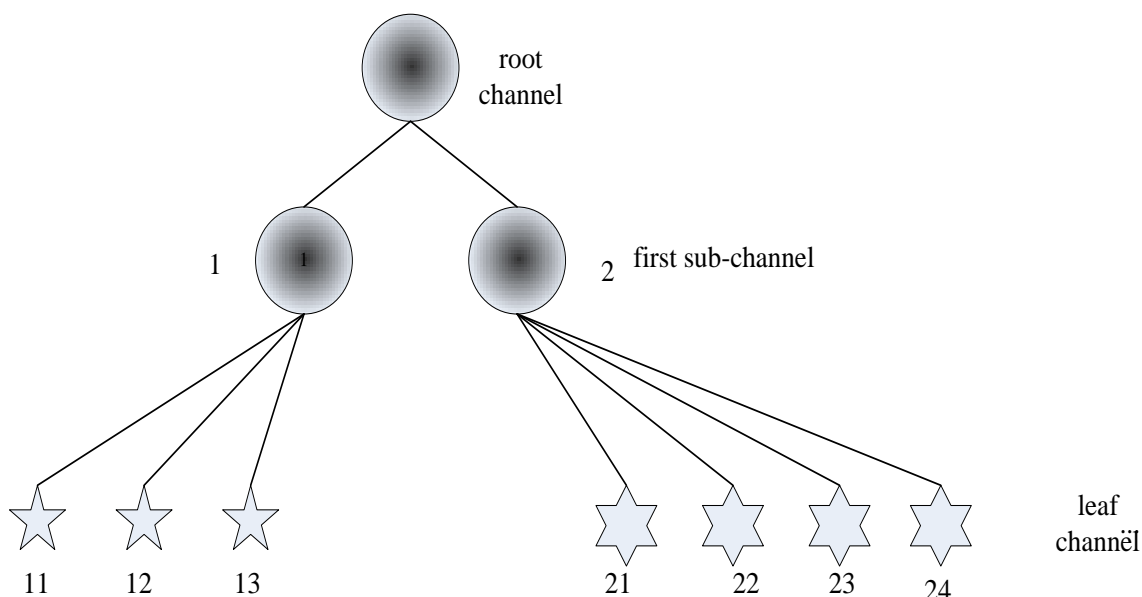


图 15-47 报文穿过的通道规划

通道规划好之后，下面需要对各个通道进行配置。

15. 3. 1. 1 HSQ 策略管理页面

HSQ 策略定义显示页面如图所示



图 15-48 带宽借用 HSQ 添加界面

添加 HSQ 根通道：

要想 HSQ 策略，需要创建一棵 HSQ 树，首先必须创建 HSQ 树的根通道。

HSQ 创建根通道页面如图所示：

点击如下界面的添加按钮进行配置

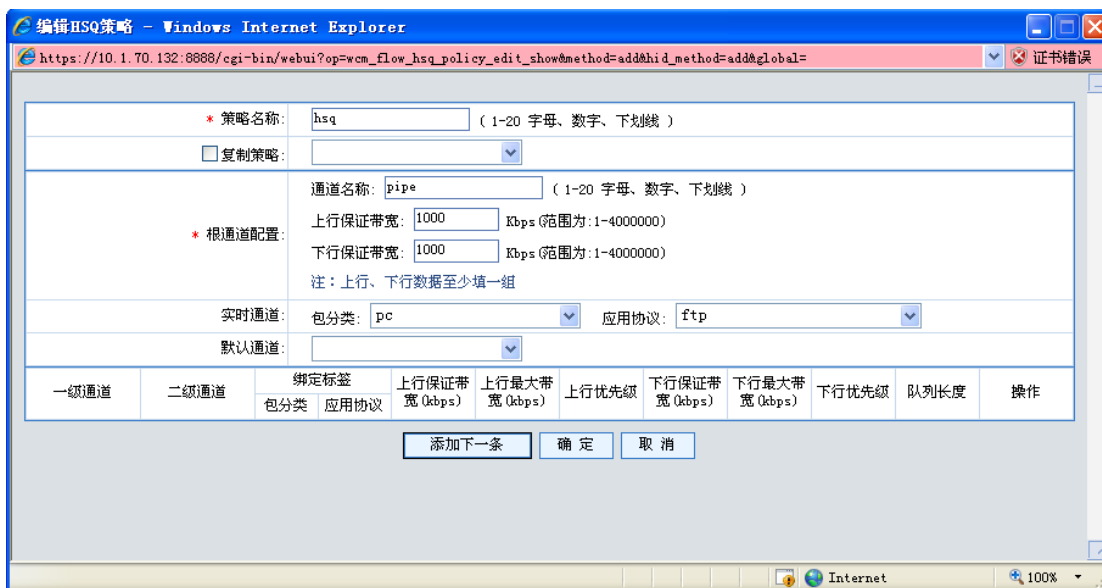


图 15-49 带宽借用主界面

该页面显示了系统中已经存在的 HSQ 队列以及其配置信息。

HSQ 策略根通道配置页面的数据域说明见表。HSQ 策略在页面上可以配置 2 级通道，也就是说在根通道下最多包含两级子通道，具体子通道配置方法见下一小节。

表 15-20 HSQ 策略根通道配置页面

域名	说明
策略名称	HSQ 策略的名称，由 1-20 字母、数字、下划线组成
复制策略	由于 HSQ 不能复用，因此当需复用时，从一个已经存在的 HSQ 策略中复制一个出来，单独使用。
根通道配置-通道名称	根通道的名称，由 1-20 字母、数字、下划线组成
根通道配置-保证带宽	可配置根通道的上行保证带宽和下行保证带宽。
根通道配置-最大带宽	可配置根通道的上行最大带宽和下行最大带宽。
根通道配置-实时通道	为实时报文设置的实时通道，以保证实时报文优先处理。
根通道配置-默认通道	没有匹配上的通道的报文所进入的通道，必须是叶子通道

说明：

1. 最小带宽：最小带宽最大不能超过其父通道的最小带宽，分上下行。
2. 最大带宽：最大带宽最大不能超过其父通道的最大带宽，分上下行。

注意：删除子通道会删除根通道下的所有子通道和叶子通道。

添加下级通道：

添加下级通道如图所示：

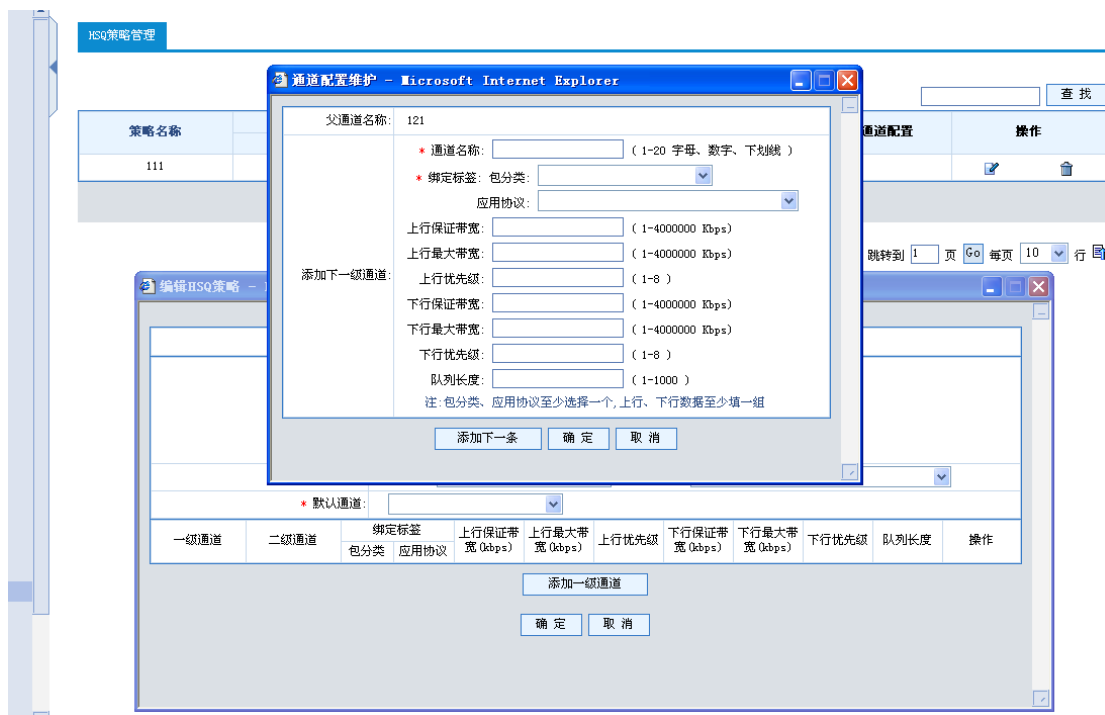


图 15-50 HSQ 添加下一级通道

添加一级通道数据域见表。

表 15-21 HSQ 策略一级通道配置

域名	说明
通道名称	下一级通道名称，由 1-20 字母、数字、下划线组成
保证带宽	可下一级通道的上行保证带宽和下行保证带宽。
最大带宽	可下一级通道上行最大带宽和下行最大带宽。
优先级	可下一级通道上行带宽借用优先级和下行带宽借用优先级，(0~8)，数字越小优先级越高。
队列长度	下一级通道的上下行队列长度（两队列长度一样），
绑定标签	配置报文分类策略 PCP 和应用协议。

说明：

1. 最小带宽：最小带宽最大不能超过其父通道的最小带宽，分上下行。
2. 最大带宽：最大带宽最大不能超过其父通道的最大带宽，分上下行。
3. 优先级：叶子通道的优先级，只有叶子通道能指定优先级。

15.3.2 流量建模

建模页面，单击配置页面，弹出流量可视配置页面页面。

提示: 未配置接口 [点此配置](#)

流量可视配置页面如下:

统计配置	
<input checked="" type="checkbox"/> 开启统计	
统计采样比:	<input type="text" value="10"/> 个 (1-1000)
接口应用:	接口名称: <input type="text" value="Ge0/0/0"/> 类型: <input type="text" value="内部"/> <input type="button" value="添加"/>
应用列表:	<input type="text"/> <input type="button" value="删除"/> <input type="button" value="清空"/>
自定义策略:	<input type="text"/> <input type="button" value=">>"/> <input type="button" value="<<"/> <input type="text"/> <small>注:启用统计策略的总和不能超过5个</small>
流监控:	日志服务器: 流量日志开启: <input type="checkbox"/>
<input type="button" value="确定"/>	

图 15-51 流量可视配置页面

第16章 高可用性

Guard 支持双机热备和负载分担两种工作模式。

双机热备(主备模式):集群中所有节点的任意对应的业务网口的 IP 地址都分别相同(HA 静态地址除外),建议它们的 MAC 地址配置为不同。其中一台 Guard (优先级最高的)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 Guard 节点为从节点,处于热备中,不处理网络数据的转发(但处理本机报文)。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:

1. HA 在双机热备模式下,使用透明模式,桥设备的 STP 不能打开。
2. HA 在双机热备模式下,不支持通过 DHCP 获得网口地址。

负载分担(主主模式)是基于 VRRP (Virtual Router Redundancy Protocol)协议实现的。一组 VRRP 路由器协同工作,共同构成一台虚拟路由器,称为一个备份组。该备份组对外表现为一个具有唯一固定 IP 地址和虚拟 MAC 地址的逻辑路由器。处于同一个 VRRP 备份组中的路由器具有两种互斥的角色:主路由器(Master)和备份路由器(Backup),一个 VRRP 组中有且只有一台处于 Master 角色,可以有一个或者多个处于 Backup 角色。VRRP 协议使用选择策略从 VRRP 组中选出一台作为 Master,负责 ARP 请求的响应和转发 IP 数据包,组中的其它作为 Backup 的角色处于待命状态。当由于某种原因 Master 路由器发生故障时,Backup 路由器能在几秒钟的时延后升级为 Master 路由器。

注意:

负载分担模式下,集群中所有节点的任意对应的业务网口 MAC 地址必须各不相同。

16.1 节点配置

本机节点	节点号	节点IP地址	操作
<input type="button" value="添加"/>			

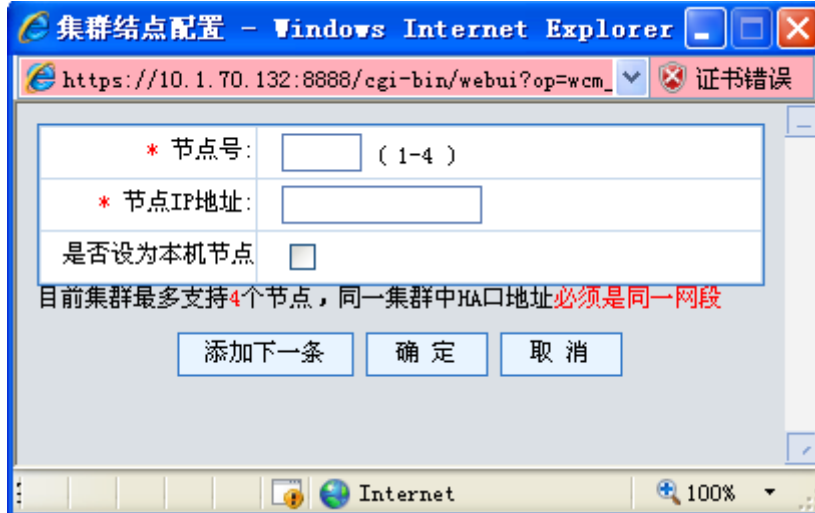


图 16-1 集群节点参数

此界面完成以下功能

- 配置 HA 节点参数
- 配置导入导出操作

表 16-1 集群节点参数说明

属性名称	描述
节点号	为 1-4 的整数, 目前集群最多支持 4 个节点
节点 IP 地址	HA 网口使用的 IP, 集群各个节点的 IP 必须唯一, 且是同一网段
是否设为本机节点	将配置的节点设为本地节点.(即配置本地节点号).

注意:

在配置 HA 基本参数前需要配置本机的 HA 网口 IP 地址, 在网络接口页面配置, 具体见 4.1.9 接口 IP 地址。HA 网口将使用物理网口, 请在设置 HA 网口前, 先确定 HA 网口是否工作在路由模式下。若 HA 网口工作在透明方式下, 请先将它从桥设备中剥离; 若 HA 网口工作在路由模式, 请不要让它再被 VLAN 设备、VPN 设备及其它设备使用, 以保证 HA 网口的专用性, 否则会产生功能问题。

表 16-2 配置导入导出说明

属性名称	描述
------	----

配置导出到所有节点	此操作是将本地配置导出到配置的其他节点上。
配置导出到指定节点	此操作是将本地配置导出到指定节点上。
配置导入到本地节点	将配置从指定节点导入到本地节点。

HA 同步的配置目前是下次启动加载的缺省配置文件。

16.2 工作模式

启动HA

HA基本参数

工作模式:	<input checked="" type="radio"/> 双机热备 <input type="radio"/> 负载均衡 (同一集群中的各节点工作模式必须相同) <input type="radio"/> 主动共享
-------	-----------------------------------------------------------------------------------------------------------------------

确定

主备模式用户配置

* Hello报文间隔配置时间:	600	毫秒 (范围500-1500, 缺省值为600)
* HA节点优先级配置:	100	(范围为1-255, 255最高, 缺省值为100)
HA接口度量值:	0	修改HA接口度量值

确定

图 16-2 HA 工作模式

此界面完成以下功能

- 配置 HA 工作模式
- 配置 HA 主备模式参数
- 启动 HA

表 16-3 配置 HA 基本参数

属性名称	描述
启用 HA	是否启用 HA
工作模式	主备模式或负载分担, 同一集群中的各节点工作模式必须相同

注意:

HA 基本参数需要先配置好 HA 网口

设置主备模式参数:

1. 选中“主备模式”;
2. 点击“显示配置参数”按钮, 在“主备模式用户配置”页面配置。

表 16-4 主备模式参数说明

属性名称	描述
Hello 报文间隔配置时间	心跳通告报文发送间隔，单位为毫秒，范围是 500-1500，默认值为 600 毫秒。
HA 节点优先级配置	HA 节点优先级。范围为 1-255。在主备模式下，HA 节点优先级缺省值为 100。值越大优先级越高，在权值相同时，即网络状况没有变化时，优先级高的为主墙。
HA 接口度量值	在主备模式下，每个需要监控的网口可以配置一定的权值，计算所有连通的网口的权值和作为本机的权值。各接口的 HA 接口度量值默认为 0，点击修改 HA 接口度量值按钮来修改配置。

集群中各个节点的接口 HA 权值和的大小是选举主节点的首要条件，HA 权值和大的为主节点，如果 HA 权值和相同，再比较它们的优先级。如果没有特殊需求，建议集群中各个节点的接口 HA 权值配置成相同。

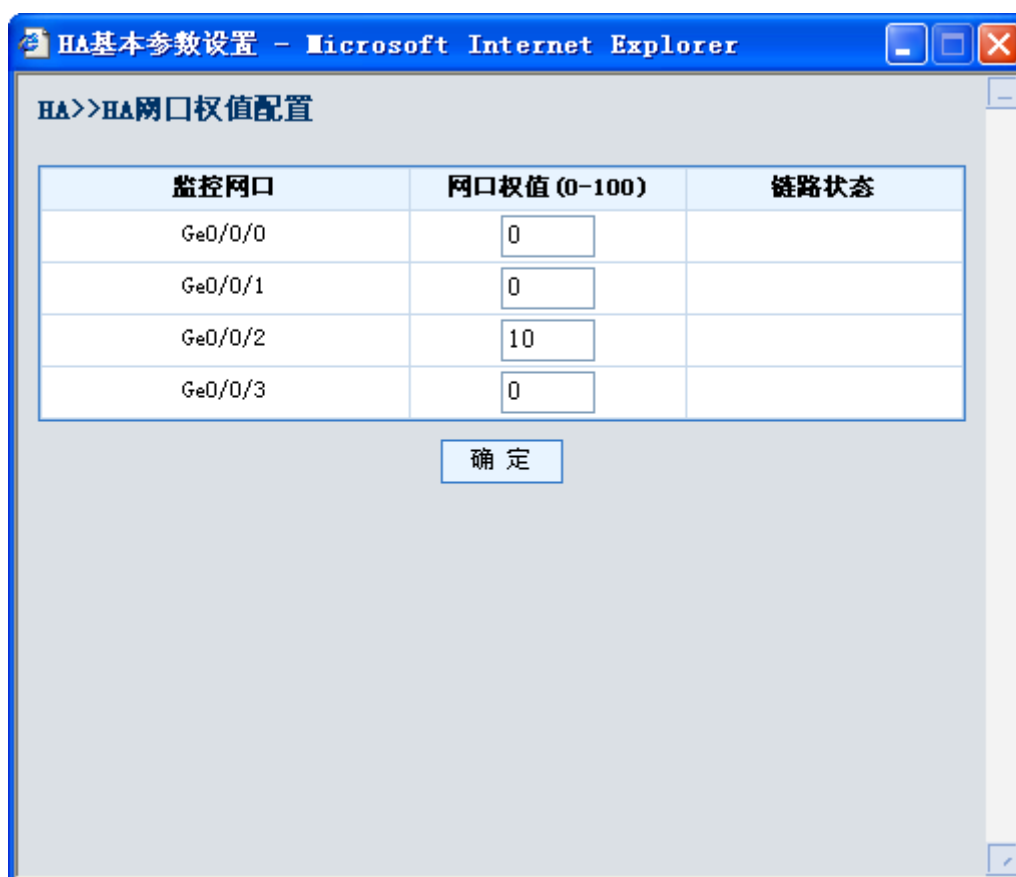


图 16-3 HA 接口度量值

设置 HA 接口度量值：

1. 点击“修改 HA 接口度量值”；
2. 在对应物理接口的“网口权值”项配置权值即可，在“主备模式用户配置”页面“HA 接口度量值中”显示配置的所有接口度量值之和；
3. 在启动 HA 后可以查看链路状态。

16.3 查看状态

当 HA 工作在主备模式时，查看 HA 状态页面显示如下图所示：

当前HA状态		
节点ID号	节点ha状态	监控网口ha权重和

图 16-5 主备模式 HA 状态

第17章 应用安全

17.1 DNS 应用防火墙

DNS 应用防火墙支持静态 DNS 查询设置，域名黑名单，重定向及监测审计功能。

17.1.1 基本配置

在应用安全->DNS 应用防火墙->基本配置配置 DNS 应用防火墙的基本信息。

<input checked="" type="checkbox"/>	DNS静态域名 静态回复控制: <input type="text" value="6000"/> (范围:1-1000000)
<input checked="" type="checkbox"/>	域名黑名单
<input type="checkbox"/>	协议控制安全级别: <input type="text" value="1级"/>
<input type="checkbox"/>	重定向IP地址: <input type="text"/> (协议控制及黑名单阻断, 报文重定向地址) <input type="checkbox"/> 统计
<input checked="" type="checkbox"/>	日志监测
	报表最大显示条数: <input type="text" value="100"/> 条 (范围:1-100)
<input type="checkbox"/>	日志审计
<input type="button" value="确定"/> <input type="button" value="恢复默认值"/>	

图 17-1 DNS 防火墙基本配置

DNS 静态域名是静态域名表的功能开关，勾选后将开启静态回复功能。

域名黑名单是黑名单的功能开关，勾选够将开启黑名单阻断功能。

协议安全级别分为 1,2,3 级和不勾选四个选项：

- 1 级：协议异常只做审计记录，不阻断。
- 2 级：如首部，绝对值信息异常，请求包 qr 字段必须为 0，长度过长或者过短（DNS 部分为空的包）等。审计记录并阻断。
- 3 级：对于相对值处理级别的控制，如递归操作，高级开启后将不允许递归请求包通过(防止恶意请求，递归冲击，导致上一级服务器瘫痪)。审计日志并阻断。

重定向功能勾选后需要设置被重定向的 IP 地址。其功能主要针对被阻断的请求以重定向 IP 进行回复。统计开关勾选后将可在重定向信息表查询每天每小时的重定向次数，便于商家对于重定向增值服务的制定。

日志监测开关开启将对于网络中域名请求情况进行排序记录，从而提供详细的网络使用情况。

日志审计功能开启后，将对于异常处理非法请求及各种攻击的频率进行记录。提供详细的网络安全情况。

17.1.2 自定义域名监测

在应用安全-> DNS 应用防火墙->自定义域名监测配置所要监测的域名信息。可设置用户比较关心的域名进行监测。



序号	域名	操作
1	www.sina.com	
2	www.sohu.com	

图 17-2 自定义域名监测


添加自定义域名：

单击“添加”按钮，进入自定义域名添加界面。



图 17-3 编辑自定义域名

删除自定义域名：

单击每一组的  按钮，删除一个自定义域名。

17.1.3 静态域名表

在应用安全-> DNS 应用防火墙->静态域名表配置静态域名表。可以配置静态回复域名表，同时可以根据请求原端口进行控制。



序号	域名	IP地址	接口名称	操作
1	www.baidu.com	66.249.89.104	any	
2	www.sina.com	10.10.10.1	Ge0/0/0	

图 17-4 静态域名表


添加静态域名表：

单击“添加”按钮，进入静态域名表维护页面。

删除静态域名表：

单击每一组的  按钮，删除一个静态域名或者单击“全部删除”删除全部配置。

修改静态域名表：

单击每一组的  按钮，进入静态域名表维护页面，可以修改静态域名表的内容。

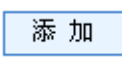
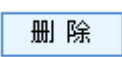
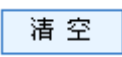
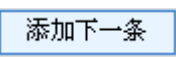
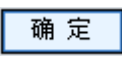
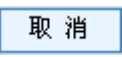
静态域名表维护页面：



图 17-5 静态域名表

静态维护界面可对同一域名添加多条 IP 及接口对应配置。

表 17-1 静态域名表维护操作列表

功能	说明
	可添加多条 IP 及接口对应配置。
	删除静态域名列表中选定配置。
	删除静态域名列表中所有内容。
	只在添加静态域名时出现，添加下一个静态域名表
	在添加或删除或清空静态域名表后，生效改变
	在添加或删除或清空静态域名表后，取消改变

17.1.4 域名黑名单

在应用安全-> DNS 应用防火墙->域名黑名单配置域名黑名单表。可以设置域名黑名单及针对每一条配置设置其需要阻断的时间。


序号	域名	受控时间段一	受控时间段二	操作
1	news.sina.com.cn	0:00-24:00		 
2	www.163.com	9:00-12:00	17:00-20:00	 

图 17-6 域名黑名单


添加域名黑名单:

单击“添加”按钮，进入域名黑名单维护页面。

删除域名黑名单:

单击每一组的  按钮，删除一个域名黑名单或者单击“全部删除”删除全部配置。

修改域名黑名单:

单击每一组的  按钮，进入域名黑名单维护页面，可以修改域名黑名单的内容。

域名黑名单维护页面:



图 17-7 域名黑名单添加

表 17-2 自定义域名黑名单维护操作列表

功能	说明
<input type="button" value="添加下一条"/>	只在添加域名黑名单时出现，添加下一个域名黑名单
<input type="button" value="确定"/>	在配置域名黑名单后，生效改变
<input type="button" value="取消"/>	在配置域名黑名单后，取消改变

17.1.5 QPS 信息

在应用安全-> DNS 应用防火墙->QPS 信息可查看网络中实时 QPS 信息。

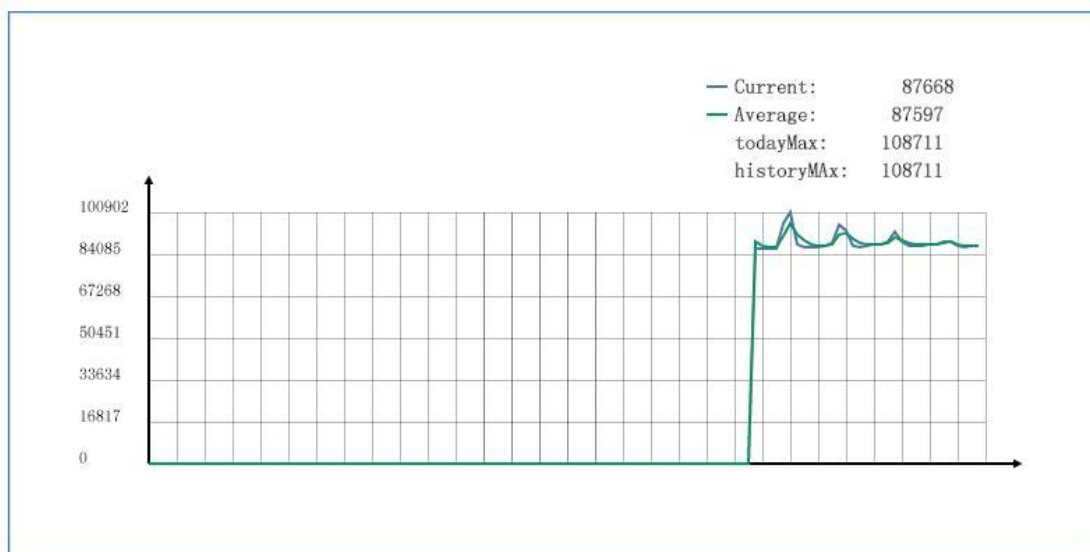


图 17-8 QPS 信息

17.1.6 重定向统计

在应用安全-> DNS 应用防火墙->重定向统计可查看重定向次数。可根据日期查询本月每天的重定向信息。



序号	日期	总数	统计
1	2010/08/26	33807209	查看统计

图 17-9 重定向统计

17.2 缓存感染监测

17.2.1 缓存感染监测配置

用于缓存感染检测功能的配置。

缓存感染监测配置	
验证服务器地址:	<input type="text"/>
受保护DNS服务器地址:	<input type="text"/>
监测抽样率阈值:	<input type="text"/> (1-65535)
递归服务器地址:	<input type="text"/> 回复匹配: <input type="checkbox"/>
DNS缓存投毒阈值:	<input type="text"/> (1-1000000)
日志开关:	<input type="checkbox"/>
缓存感染监测开关:	<input type="checkbox"/>
注：只有填写了“递归服务器地址”才能配置“回复匹配”选项	
<input type="button" value="确定"/>	

图 17-10 缓存感染监测配置界面

可配置的参数说明：

表 17-3 缓存感染监测配置页面

域名	说明
验证服务器地址	Ip 地址
受保护的 DNS 服务器地址	Ip 地址
监测抽样率阈值	1-65535 的一个数字
递归服务器地址	Ip 地址
DNS 缓存投毒阈值	1-1000000 的一个数字

17.2.2 缓存感染实时监测统计

统计当前监测到的攻击情况。

序号	域名	攻击数	时间段
<input type="button" value="刷新"/>			

⏪ ⏩
第1页/1页 跳转到 页 每页 行

图 17-11 缓存感染实时监测统计

17.2.3 缓存感染历史监测统计

统计监测到的攻击历史。



图 17-12 缓存感染历史监测统计

第18章 应用识别




18.1 特征策略

应用识别策略是基于模版生成的，系统中默认存在一个模版策略 template，可以对该模版策略进行查看但不能更改，定义新的策略时可以继承该模版，并在模版基础上做修改。



图 18-1 应用识别特征策略

表 18-1 保护策略图标说明

域名	说明
	删除本条记录
	编辑本条记录
	编辑特征设置

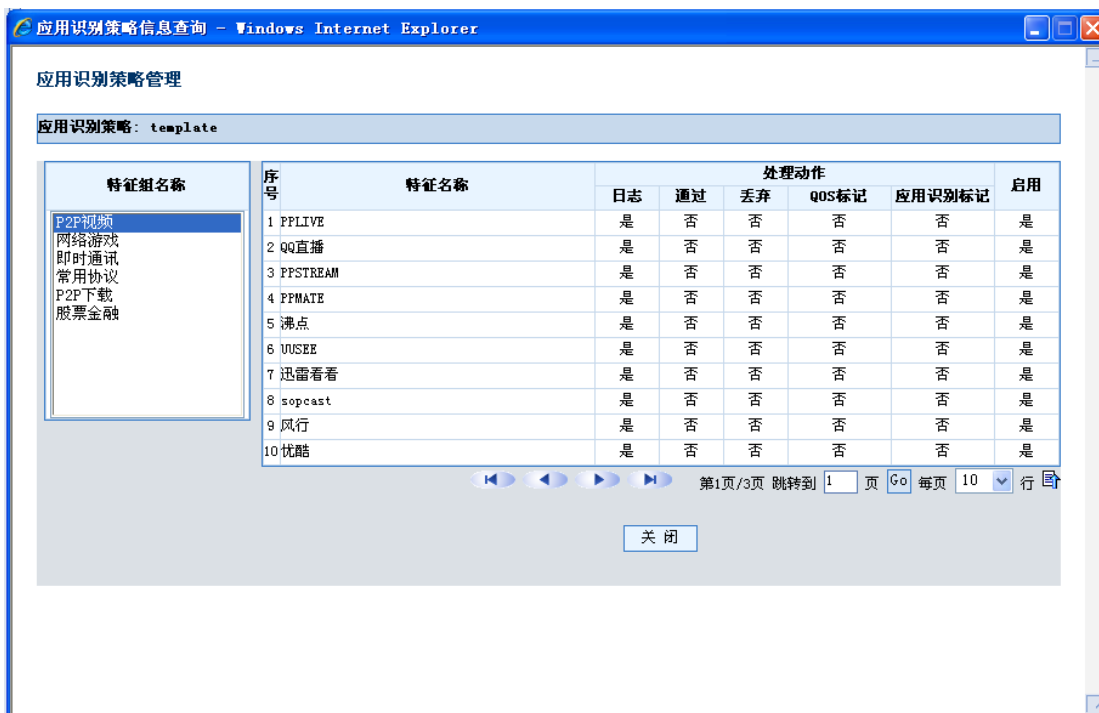


图 18-2 查看应用识别策略模版



图 18-3 添加应用识别策略

在添加了一条应用识别策略后,可以修改备注和 ip 记忆功能的超时时间或者将 ip 记忆功能关闭。

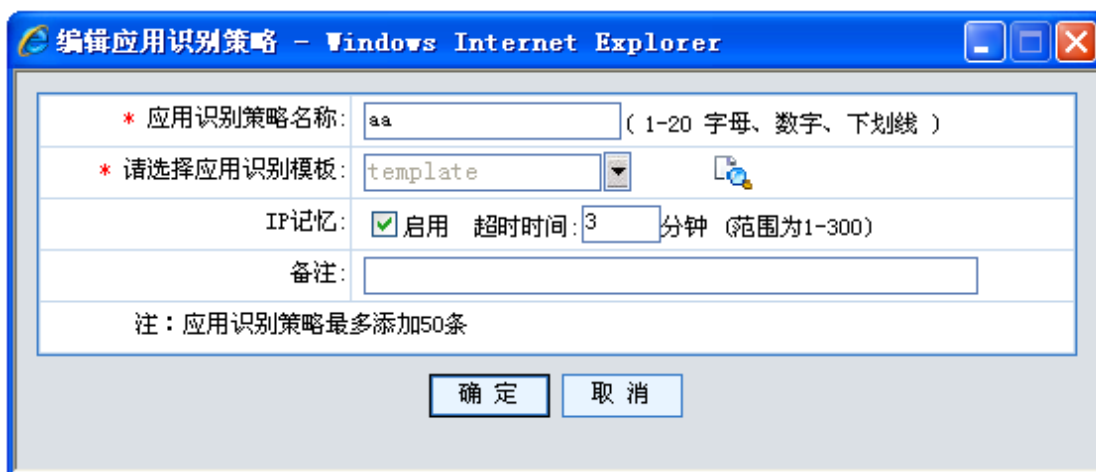


图 18-4 修改应用识别策略备注

可以对策略要识别的应用类型和处理动作做修改。

特征组名称	序号	特征名称	处理动作				应用识别标记	启用	操作
			日志	通过	丢弃	qos标记			
P2P识别		P2P视频	✓	✗	✗	✗	✗	✓	
网络游戏	1	PFLIVE	✓	✗	✗	✗	✗	✓	
即时通讯	2	QQ直播	✓	✗	✗	✗	✗	✓	
常用协议	3	P2PSTRIP	✓	✗	✗	✗	✗	✓	
P2P下载	4	P2PSTATE	✓	✗	✗	✗	✗	✓	
股票金融	5	流点	✓	✗	✗	✗	✗	✓	
	6	USERE	✓	✗	✗	✗	✗	✓	
	7	迅雷看看	✓	✗	✗	✗	✗	✓	
	8	sopcast	✓	✗	✗	✗	✗	✓	
	9	风行	✓	✗	✗	✗	✗	✓	
	10	优酷	✓	✗	✗	✗	✗	✓	

图 18-5 修改应用识别策略的识别应用和处理动作

直接点击 ✓ 和 ✗ 来修改动作和是否启用，也可以选择来编辑特征的处理方式。



图 18-6 编辑特征的处理方式

18.2 策略应用

将应用特征策略与 PCP 绑定，配置应用特征识别规则。

[按条件查询](#)

序号	包分类名称	应用识别策略	QoS标记	操作
<input type="button" value="添加"/>				

全选

 第1页/1页 跳转到 页 每页 行

图 18-7 应用识别规则



图 18-8 添加应用识别规则

添加成功一条规则后可修改该规则中的 QOS 标记值



图 18-9 添加应用识别规则

18.3 统计图表

采用统计图和统计表的形式来显示当前已经识别的应用类型。



图 18-10 应用识别统计图

按条件查询

序号	日期/时间	所属特征组	特征ID	特征名称	动作
1	2010/12/08 11:48:39	常用协议	90	netbios_name_service	通过
2	2010/12/08 11:48:39	常用协议	90	netbios_name_service	通过
3	2010/12/08 11:48:39	常用协议	91	netbios_datagram_service	通过
4	2010/12/08 11:48:37	常用协议	90	netbios_name_service	通过
5	2010/12/08 11:48:37	常用协议	90	netbios_name_service	通过
6	2010/12/08 11:48:37	常用协议	90	netbios_name_service	通过
7	2010/12/08 11:48:37	常用协议	90	netbios_name_service	通过
8	2010/12/08 11:48:36	常用协议	90	netbios_name_service	通过
9	2010/12/08 11:48:36	常用协议	90	netbios_name_service	通过
10	2010/12/08 11:48:36	常用协议	90	netbios_name_service	通过

清空

图 18-11 应用识别统计表

18.4 日志采样

修改应用识别的日志采样率，默认是 1000，即属于某应用的每 1000 个报文记录一次日志。

日志采样率	
日志采样率:	<input type="text" value="1000"/> (范围为:1-65535, 默认值为1000)
<input type="button" value="确定"/>	

图 18-12 应用识别日志采样率设置

第19章 用户认证

从用户所获得的服务来划分，可以将 Guard 的用户划分为：

- Terminal 用户，通过 Console 口登录到 Guard；
- FTP 用户，与 Guard 建立 FTP 连接进行文件传输；
- PPP 用户，与 Guard 建立 PPP 连接（例如拨号、PPPoE 等），从而访问网络；
- SSH 用户，与 Guard 建立 SSH 连接，登录到 Guard。

一个用户可能同时获得几种服务，这样只需一个用户便可以执行多种功能。

系统可以对用户进行分级管理。用户的优先级分为参观（Visit）、监控（Monitor）、系统（System）、管理（Manage）4 个级别，除了通过 Console 口方式之外，登录到 Guard 的用户所能访问的功能由登录所使用的用户界面的级别确定。

19.1 本地用户

序号	用户名	登录web成功次数	登录web失败次数	优先级	用户状态	用户可用服务	操作
1	administrator	2	0	管理	●	sshServer, https-server	 
2	liuy	0	0	管理	●	sshServer, telnetServer	 
3	lql	0	0	管理	●	https-server, telnetServer	 


 第1页/1页 跳转到 页 每页 10 行 

图 19-1 用户列表

点击相应操作栏中的“编辑”按钮，弹出以下界面：

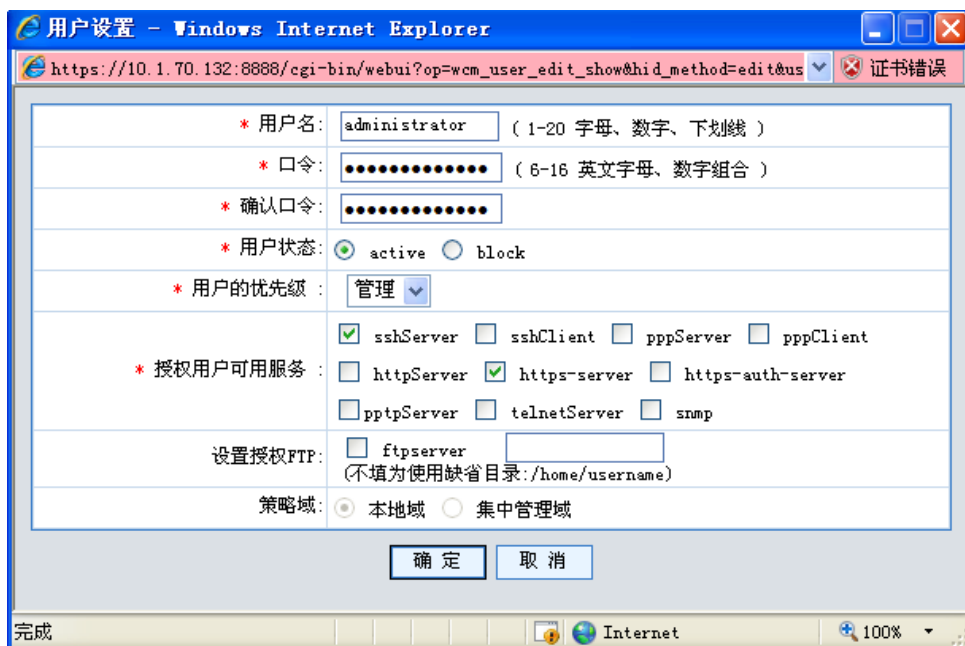


图 19-2 用户维护

编辑用户时，口令域可以不用填，这时候表示不修改该用户的当前密码。
 点操作栏中的“删除”按钮可以删除此用户。
 用户列表下方的“删除所有用户”按钮用来将系统中所有的用户全部删除。
 添加用户界面如下：

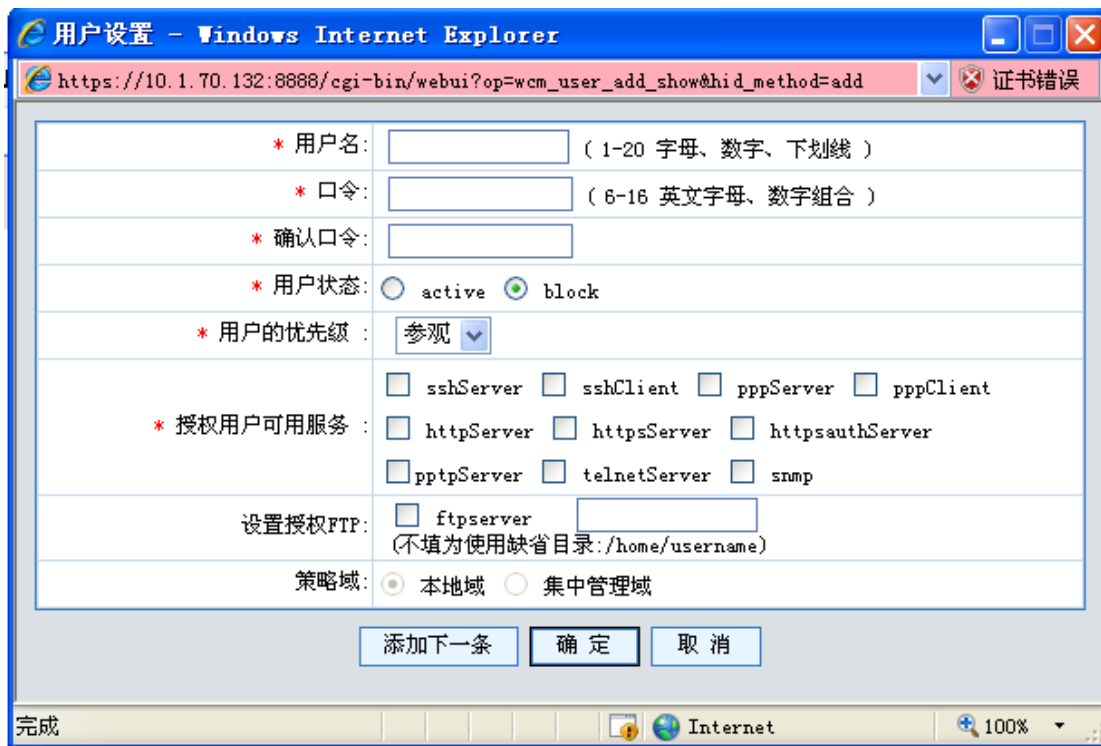


图 19-3 用户添加

表 19-1 用户添加元素列表

值域	说明
用户名	名称必须唯一，必须用字母开头，且不能为 a、al、all 之一
口令	该用户用于认证的口令
用户状态	表示该用户从创建开始是否激活
授权用户可用服务	勾选用户可以使用的服务
设置授权 FTP	用户可以使用 ftp 服务器功能，并可以为用户指定根目录

19.2 AAA 认证

AAA认证是Authentication、Authorization、Accounting（认证、授权、审计）的简称，是网络安全的一种管理机制，提供了认证、授权、审计三类安全功能。

当用户想要通过网络与Guard建立连接，对Guard进行管理，或者通过Guard获得访问其它网络或取得某些网络资源时，AAA认证起到了验证用户身份以及对用户行为进行控制和监督的作用。

作为安全通用开发平台的用户认证系统，系统架构必须适应未来高吞吐率、高性能的趋势。目前流行的系统架构基本上有下面两种：

1. 集中式

认证工作集中在 Guard 上实现，Guard 既要负责网络报文的转发和过滤，又要负责与第三方 AAA 服务器进行用户认证以及用户状态保持。这种方式成本较低，但是 Guard 负担较重，同时在线用户的数目有限，一般用于中低端设备上。

2. 分布式

Guard 上有一个用户认证模块负责收集用户信息，运行在多核硬件平台上。Guard 之外提供一台或多台服务器作为认证服务器，如 cisco ACS 系统，华为 CAMS 系统，负责用户的认证、授权、计费。这种架构成本较高，但是便于支持大用户量，并且，这种方式能够实现整网统一认证，避免出现一个用户经过多个认证点进行多次认证的情况。

Guard 上的用户认证系统采用分布式系统架构。

19.2.1 认证服务器

AAA认证代理服务器配置	
ip地址:	<input type="text"/>
端口:	<input type="text"/> (范围: 1-65535)
<input type="button" value="确定"/>	

登陆认证方式配置	
ssh:	<input type="text" value="local"/> ▼
telnet:	<input type="text" value="local"/> ▼
web:	<input type="text" value="local"/> ▼
ftp:	<input type="text" value="local"/> ▼
<input type="button" value="确定"/>	

图 19-4 认证服务器

需要填入认证代理服务器 IP 地址和端口，为必选项。

登录认证方式配置，可以将 ssh、telnet、web、ftp 配置为本地认证方式，或者采用某种认证协议，目前仅支持 Radius 协议。默认为本地认证方式。

19.2.2 登录用户

序号	用户名	用户源地址	登录方式	认证协议	操作
<input type="text"/> <input type="button" value="查找"/>					
<input type="button" value="◀"/> <input type="button" value="⏪"/> <input type="button" value="⏩"/> <input type="button" value="▶"/>					
第1页/1页 跳转到 <input type="text" value="1"/> 页 <input type="button" value="Go"/> 每页 <input type="text" value="10"/> 行 <input type="button" value="🔍"/>					

图 19-5 登录用户列表

此处查看所有通过 AAA 方式登录到 Guard 上的管理员用户状态。包括用户名，用户源地址，登录方式，认证协议等内容。

19.2.3 在线 Portal 用户

此处查看所有通过认证的在线 portal 用户信息。包括用户 ip 地址，用户名，用户所属的组，用户流量速率。

序号	源IP地址	用户名	用户组	用户流量速率 (K)	操作
<input type="text"/> <input type="button" value="查询"/>					
<input type="button" value="◀"/> <input type="button" value="⏪"/> <input type="button" value="⏩"/> <input type="button" value="▶"/>					
第1 页/1页 跳转到 <input type="text" value="1"/> 页 <input type="button" value="Go"/> 每页 <input type="text" value="10"/> 行 <input type="button" value="🔍"/>					

图 19-6 在线 Portal 用户表

19.2.4 Portal 用户组

此处可以查看系统中的用户组配置。包括用户组名称，是否开启基于组的流量统计，精确度，统计时间间隔，是否开启流量日志，是否启动最低流量限制，最低流量，最低流量时间。

序号	用户组名称	流量统计	精确度	时间间隔	流量日志	最低流量限制	最低流量	最低流量时间	操作
<input type="text"/> <input type="button" value="查找"/>									
<input type="button" value="添加"/> <input type="button" value="全部删除"/>									
<input type="button" value="◀"/> <input type="button" value="⏪"/> <input type="button" value="⏩"/> <input type="button" value="▶"/>									
第1页/1页 跳转到 <input type="text" value="1"/> 页 <input type="button" value="Go"/> 每页 <input type="text" value="10"/> 行 <input type="button" value="🔍"/>									

图 19-7 Portal 用户组

点击“添加”按钮，增加一个 Portal 用户组；

点击每一行的“删除”按钮，可以删除该 Portal 用户组；

点击每一行的“编辑”按钮，可以修改该 Portal 用户组属性；



图 19-8 Portal 用户组属性修改

表 19-2 关键字组数据域说明

域名	说明
用户组名称	用户组名称，20 个字符以内的英文字母、数字、下划线或中文。
流量统计启用	选中时，每隔一段时间计算该用户组内所有用户的流量速率，包括上行下行的流量之和。
流量统计精确度	0-100，该值越高，统计越精确，对性能影响越大。
流量统计时间间隔	流量速率计算的时间间隔，以秒为单位，到达该时间间隔后，更新用户流量速率数据。
流量统计流量日志	流量统计审计开关，时间间隔到达时，向日志服务器发送流量统计日志。
最低流量限制启用	必须流量统计启用被选中的前提下才能选中该功能，可以对该用户组内所有用户的超时进行管理。当用户一段时间内流量小于某值时（如只挂 QQ、MSN 等），Guard 强制用户下线，并通知 Portal 服务器。
最低流量限制最低流量速率	以 KB 为单位，用户的最低流量速率限制。
最低流量限制最低流量时间	时间限制，在该时间段内，用户流量未大于上述最低流量速率限制，则强迫该用户下线。1~120，分钟为单位

19.2.5 Portal 服务器

在 用户管理->AAA 认证->Portal 服务器 页面可以设置 PORTAL 服务器的相关信息，以及 AAA 认证规则的配置。

Portal 服务器配置

Portal 服务器:	ip地址: <input type="text"/>	端口: <input type="text"/> (范围1-65535)
	保活间隔: <input type="text"/> (范围1-3600)秒	保活超时: <input type="text"/> (范围1-30)秒
	重试次数: <input type="text"/> (范围1-10默认为3)次	
重定向服务器地址:	<input type="text"/>	
	跳转: <input checked="" type="checkbox"/>	
端口:	<input type="text"/> (范围1-65535 默认80, 最多8个, 用英文逗号分隔)	
规则:	启用: <input type="checkbox"/>	认证规则优先: <input type="checkbox"/>

规则名	源	目的	认证类型	操作
<input type="button" value="添加"/>				

第1页/1页 跳转到 页 每页 行

图 19-9 PORTAL 服务器设置

表 19-3 关键字组数据域说明

域名	说明
Portal 服务器 IP 地址	Portal 认证服务器与 Guard 通信的 IP。
Portal 服务器 端口	Portal 认证服务器与 Guard 通信的端口。
Portal 服务器 保活间隔	Portal 认证服务器与 Guard 通信的保活报文发送间隔，秒为单位。
Portal 服务器 保活超时	Portal 认证服务器与 Guard 通信的保活报文超时时间，秒为单位。
Portal 服务器 重试次数	Guard 与 Portal 服务器通信发送报文的重试次数。
Portal 服务器 当前状态	当前 Portal 服务器与 Guard 的通信状态。
重定向服务器 地址	Portal 重定向 url 地址，长度 1-255。
端口	Portal 重定向检查的 HTTP 端口号，适用于 HTTP 代理和某些 HTTP 端口非

	80 的情况配置。
流量统计时间间隔	流量速率计算的时间间隔，以秒为单位，到达该时间间隔后，更新用户流量速率数据。
规则启用	如果选中，启用 portal 认证功能。
规则认证规则优先	默认是免认证规则优先。网络上的报文是先匹配免认证规则集，然后匹配 portal 认证规则集。如果选中，认证规则优先。

点击添加或编辑 Portal 规则按钮则可以编辑一条 Portal 认证规则或者免认证规则，包括源，目的和认证类型。

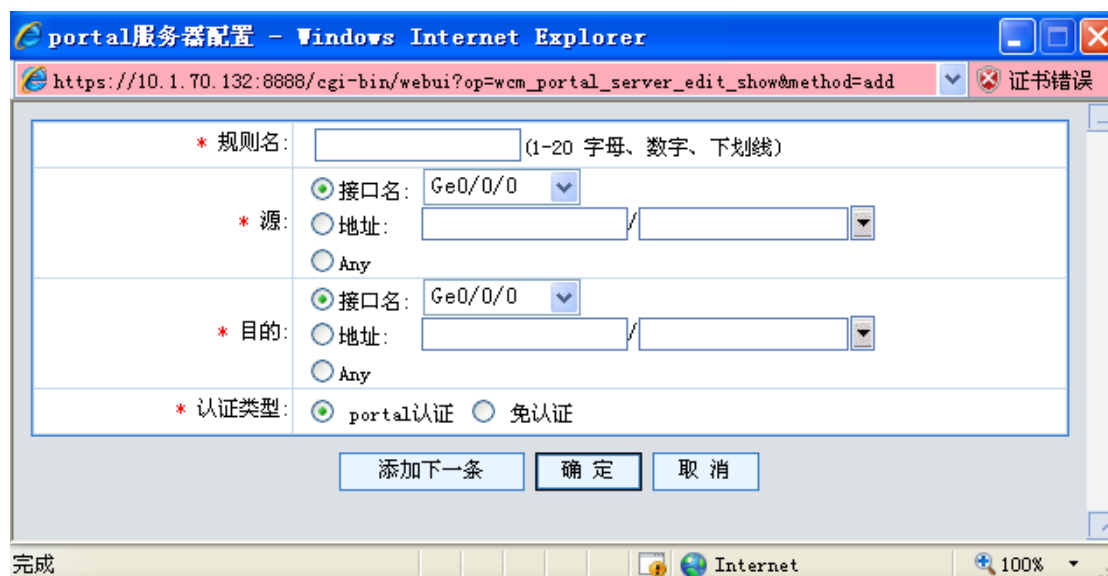


图 19-10 PORTAL 规则设置

第20章 日志信息

日志信息是 Guard 主体软件中不可或缺的一部分，它作为 Guard 的信息枢纽而存在。日志信息接管大多数的信息输出，并能进行细致的分类，从而能够有效地进行信息筛选。它通过与 Debug 程序的结合，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

系统的日志信息具有以下一些特性：

- 共有三类信息：log 类（日志类信息）、trap 类（告警类信息）、debug 类（调试类信息）。
- 信息按重要性划分为八种等级，可按等级进行信息过滤。
- 系统支持六个通道，六个通道有缺省通道名，并且这六个通道缺省的与六个输出方向相关联。
- 支持控制台（console）、ssh 终端和配置终端（monitor）、日志缓冲区（logbuffer）、日志主机（loghost）、告警缓冲区（trapbuffer）、SNMP 6 个方向的信息输出。
- 信息在输出时可以进行中英文选择。
- 每个信息的头部由固定的部分组成，包括时间戳、信息来源的模块、信息级别、信息来源的槽号、信息摘要等。

总之，日志信息的主要工作就是将各种模块的三种类型的信息，按照八种重要程度，根据用户的设置输出到十个信息通道中去，然后，将这十个信息通道再定位到六个输出方向上去。

20.1 日志配置

20.1.1 日志服务器

通过设置日志主机的 IP 地址，将系统产生的信息发送日志服务器中保存下来。

如图：

日志服务器	
日志服务器地址：	<input type="text"/>
<input type="button" value="确定"/>	

图 20-1 设置日志主机地址

20.1.2 终端信息控制

1. 开启/关闭信息中心功能

信息中心缺省情况下处于开启状态。在信息中心开启时，特别是在处理信息较多时，由于信息分类、输出的原因，对系统性能有一定的影响。

2. 终端信息输出控制

信息输出必须要求用户在连接终端设置是否允许 debug/log/trap 信息输出，这些信息是从信息中心发送来的。

1. 打开/关闭终端显示日志信息功能
2. 打开/关闭终端显示告警信息功能
3. 打开/关闭终端显示调试信息功能

缺省情况下，所有调试开关都是关闭的，只有当打开日志开关，才能看到日志信息；打开告警开关，才能看到告警信息；打开调试开关时候，才能看到调试信息

<input checked="" type="checkbox"/>	信息中心
<input checked="" type="checkbox"/>	终端日志
<input checked="" type="checkbox"/>	终端告警
<input checked="" type="checkbox"/>	终端调试
<input type="button" value="确定"/>	

图 20-2 终端信息控制

20.1.3 信息终端

3. 信息终端通道命名

信息通道分别对应信息输出方向，目前支持下面 6 种信息输出通道或者输出方向：

表 20-1 信息通道说明

信息通道	信息输出方向
Console	向 Console 方向输出信息
Vty	向 ssh 终端输出信息
Loghost	向日志主机输出信息，配置 loghost 后，日志不再向其它终端和缓冲区输出
Trapbuffer	向告警缓冲区输出信息
Logbuffer	向日志缓冲区输出信息
Snmpagent	向 SNMP 输出信息
Alert-by-email	通过邮件告警输出日志信息

用户可以针对每种信息通道定义各自的属性。

4. 信息终端通道属性说明

level:设置信息级别，禁止信息级别大于所设置的 priority 的信息输出。priority 是信息级别。

priority:信息优先级域值，取下面几种优先级之一：

- emerg
- alert
- critical

- error
- warning
- notification
- informational
- debugging （单独提出来，有专门对应的命令）

具体含义请参加下面的信息优先级介绍。

注意：

同时有多个 ssh 用户时，各个用户之间共享 vty 通道的属性。当某个用户改变其中某项参数后，在其他 ssh 用户终端上也有反映。

5. 信息优先级说明

信息中心按信息的严重等级或紧急程度将其划分为八个等级；在按等级来进行信息过滤时，采用的规则是：禁止优先级大于所设阈值的信息输出。越紧急的信息报文，其优先级越小，emerg 表示的等级为 0，debugging 为 7，因此，当设置优先级阈值为 debugging 时，所有的信息都会输出。

表 20-2 syslog 定义的优先级

严重等级	描述
Emerg	致命错误
Alert	需立即纠正的错误
Critical	关键错误
Error	需关注但不关键的错误
Warning	警告，可能存在某种差错
Notification	需注意的信息
Informational	一般提示信息
Debugging	调试信息


序号	终端名	日志		调试状态	操作	
		状态	优先级			
1	logbuffer	开启	提示			
2	trapbuffer	开启	警告			
3	loghost	开启	提示			
4	snmpagent	开启	提示			
5	console	开启	警告	开启		
6	vty	开启	警告	开启		
7	alert-by-email	开启	警告			

图 20-3 信息通道显示

20.1.4 U 盘日志输出

U 盘日志输出页面可以对日志文件大小，是否清空日志，u 盘容量大小，是否开启日志输出功能进行设置，下图为 U 盘日志输出页面：

U盘日志输出配置	
U盘日志输出功能:	<input type="checkbox"/>
U盘日志文件大小:	4 M (范围为1-4000)
清空U盘日志:	<input type="button" value="清空"/>
U盘容量大小:	无U盘
<input type="button" value="确定"/>	

图 20-4 U 盘日志输出

20.2 日志查看

20.2.1 日志查看

1. 显示系统中日志缓冲区中的日志信息。
2. 通过设置对话框的内容可以对日志信息进行过滤，过滤的参数有日志时间，日志类型和日志级别。

日期/时间	日志类型	日志级别	详细信息
2011/07/12 08:47:05	配置管理日志	信息	devid=0 date="2011/07/12 08:47:05" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="return" msg= result=Success
2011/07/12 08:47:05	配置管理日志	信息	devid=0 date="2011/07/12 08:47:05" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="return" msg= result=Match
2011/07/12 08:47:05	配置管理日志	信息	devid=0 date="2011/07/12 08:47:05" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="flow_monitor_get_real_appidentify_data" msg= result=Success
2011/07/12 08:47:04	配置管理日志	信息	devid=0 date="2011/07/12 08:47:04" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="flow_monitor_get_real_appidentify_data" msg= result=Match
2011/07/12 08:47:04	配置管理日志	信息	devid=0 date="2011/07/12 08:47:04" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="config" msg= result=Success
2011/07/12 08:47:04	配置管理日志	信息	devid=0 date="2011/07/12 08:47:04" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="config" msg= result=Match
2011/07/12 08:46:59	配置管理日志	信息	devid=0 date="2011/07/12 08:46:59" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="return" msg= result=Success
2011/07/12 08:46:59	配置管理日志	信息	devid=0 date="2011/07/12 08:46:59" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="return" msg= result=Match
2011/07/12 08:46:59	配置管理日志	信息	devid=0 date="2011/07/12 08:46:59" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="flow_monitor_get_real_appidentify_data" msg= result=Success
2011/07/12 08:46:58	配置管理日志	信息	devid=0 date="2011/07/12 08:46:58" dname=KingGuard-9202 logtype=2 pri=6 mod=cli admin=administrator from=189.16.100.34 act="flow_monitor_get_real_appidentify_data" msg= result=Match

图 20-5 日志信息

20.2.2 管理日志

1. 显示管理员的操作日志。
2. 通过设置对话框的内容可以对日志信息进行过滤,过滤的参数有日志时间,关键字。

日期/时间: 关键字:

日期/时间	用户名称	日志级别	IP 地址	模块名称	动作	结果
2011/07/12 08:48:19	administrator	信息	189.16.100.34	cli	return	Success
2011/07/12 08:48:19	administrator	信息	189.16.100.34	cli	return	Match
2011/07/12 08:48:19	administrator	信息	189.16.100.34	cli	flow_monitor_get_real_appidentify_data	Success
2011/07/12 08:48:19	administrator	信息	189.16.100.34	cli	flow_monitor_get_real_appidentify_data	Match
2011/07/12 08:48:19	administrator	信息	189.16.100.34	cli	config	Success
2011/07/12 08:48:19	administrator	信息	189.16.100.34	cli	config	Match
2011/07/12 08:48:13	administrator	信息	189.16.100.34	cli	return	Success
2011/07/12 08:48:13	administrator	信息	189.16.100.34	cli	return	Match
2011/07/12 08:48:13	administrator	信息	189.16.100.34	cli	flow_monitor_get_real_appidentify_data	Success
2011/07/12 08:48:13	administrator	信息	189.16.100.34	cli	flow_monitor_get_real_appidentify_data	Match




 第1页/764页 跳转到 页 每页 行 

图 20-6 管理日志报表

20.2.3 会话日志

1. 显示管理员的操作日志。
2. 通过设置对话框的内容可以对日志信息进行过滤,过滤的参数有日志时间,关键字。

日期/时间: 关键字:

日期/时间	协议	源地址	目的地址	源端口	目的端口	回包信息			动作
						源地址	目的地址	源端口	
<input type="button" value="刷新"/>									



 第1页/1页 跳转到 页 每页 行 

图 20-7 会话日志

20.2.4 抗攻击日志

1. 显示管理员的操作日志。
2. 通过设置对话框的内容可以对日志信息进行过滤,过滤的参数有日志时间,关键字。



图 20-8 抗攻击日志

20.2.5 流量牵引日志

1. 显示管理员的操作日志。
2. 通过设置对话框的内容可以对日志信息进行过滤,过滤的参数有日志时间,关键字。



图 20-9 流量牵引日志

20.2.6 云安全日志

1. 显示管理员的操作日志。
2. 通过设置对话框的内容可以对日志信息进行过滤,过滤的参数有日志时间,关键字。

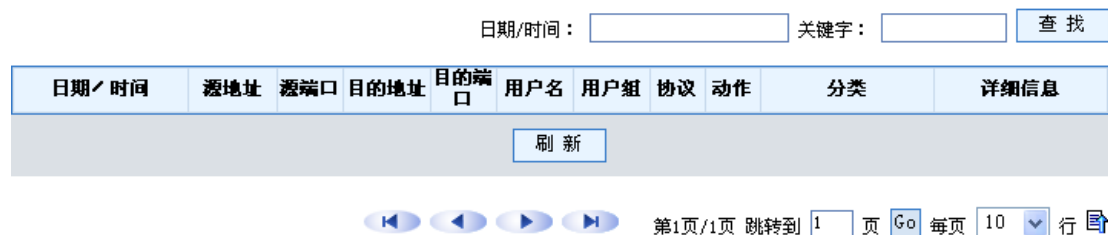


图 20-10 云安全日志

20.3 邮件报警

可以设置 Guard 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 Guard 管理员发报警邮件。

使用邮件报警功能，需要先在**系统配置->DNS 设置**里配置域名解析服务器地址。然后在**日志信息->邮件报警->邮件配置**，设置默认收件人地址和默认发件人地址信息。如果在**日志信息->信息通道**页面将 alert-by-email 设置为开启，则后台会自动使用发件人地址向收件人的地址发送告警邮件。

20.3.1 邮件报警

6. 默认收件人配置

默认收件人地址是后台告警邮件的默认发送地址。

默认收件人配置

收件人地址: 添加

地址列表: 删除

清空

DNS设置

确定

默认发件人配置

邮件服务器	发件人地址	记录日志	操作
添加			

图 20-11 默认收件人配置

表 20-3 默认收件人配置操作列表

功能	说明
添加	把收件人地址添加到地址列表中，最多可添加 5 个收件人地址
删除	删除收件人地址列表中选定的收件人地址
清空	删除收件人地址列表中所有内容
确定	在添加或删除或清空收件人地址后，生效改变

7. 默认发件人配置

由于发件人的 SMTP 服务器需要进行身份验证，每个发件人邮件服务器可设置一个发件人地址。默认使用第一个发件人地址发送告警邮件。

默认发件人配置			
邮件服务器	发件人地址	记录日志	操作
<div style="border: 1px solid black; padding: 2px; display: inline-block;">添加</div>			

图 20-12 默认发件人信息

单击“添加”按钮，进入发件人信息配置页面。

单击每一条记录的“删除”按钮，删除一个发件人邮件服务器。

单击每一条记录的“编辑”按钮，进入发件人配置页面，可以修改发件人的内容。

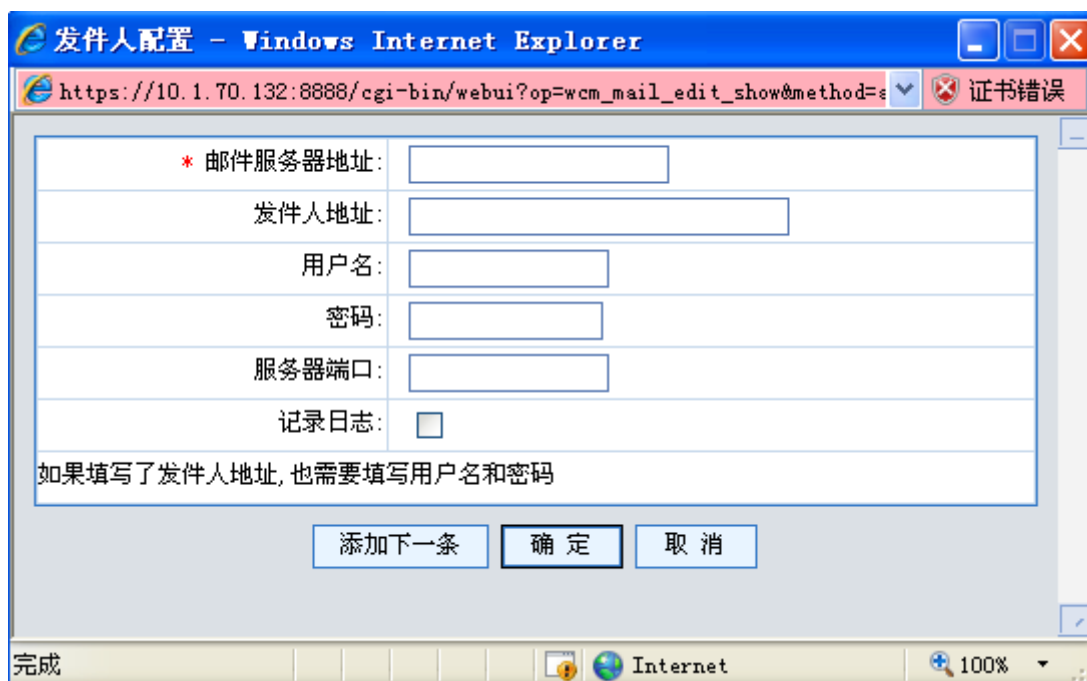


图 20-13 默认发件人配置

表 20-4 默认发件人配置操作列表

功能	说明
<div style="border: 1px solid black; padding: 2px; display: inline-block;">添加下一条</div>	添加下一个发件人邮件服务器
<div style="border: 1px solid black; padding: 2px; display: inline-block;">确定</div>	在添加或修改发件人配置后，生效改变
<div style="border: 1px solid black; padding: 2px; display: inline-block;">取消</div>	在添加或修改发件人配置后，取消改变

表 20-5 发件人配置说明列表

属性名称	说明
邮件服务器地址	发件人的 SMTP 邮件服务器地址，用于发件人的身份认证
发件人地址	发件人的 e-mail 地址
用户名	发件人的用户名(有时和发件人地址相同)
密码	发件人的密码
服务器端口	发件人的 SMTP 邮件服务器端口，一般为 25
记录日志	启用或者关闭日志功能

如果不能正常发邮件，请确认发件人的邮件服务器是否支持 SMTP，并请检查 DNS 配置、邮件服务器地址、用户名和密码是否正确。

20.3.2 邮件测试

可以从 Guard 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，是在日志信息->邮件报警->邮件配置里面设置好的。

也可以在“发件人地址”这一栏中，填写并使用其他的发件人地址，并要求填写用户名和密码。此时，发件人的 SMTP 服务器由发件人的地址域名得到。

发件人收件人配置

发件人地址: 用户名: 密码:

* 收件人地址: 可以填3个收件人地址, 中间用分号(;)分隔

* 邮件主题: (50字符)

邮件内容:
(已使用 个字符 最多可用350字符 1个中文等于2个字符)

上传附件: 选择本地文件 (上传附件不能超过 1.4M)

选择服务器文件

[DNS设置](#)

图 20-14 发件人收件人配置

表 20-6 邮件发送配置操作列表

功能	说明
<input type="button" value="发送邮件"/>	填写完成之后，发送邮件

全部清空	清空填写的内容
清除附件	当上传的附件需要修改时，可以清除已经上传的附件文件

表 20-7 邮件发送配置说明列表

属性名称	说明
发件人地址	如果此处没有填写发件人地址，则使用在 系统配置->邮件报警->邮件配置 里面设置好的发件人信息来发送邮件；如果填写了发件人的 e-mail 地址，则使用此发件人的地址来发送邮件。
用户名	发件人的用户名(有时和发件人地址相同)
密码	发件人的密码
收件人地址	收件人地址必须填写，最多可填写 3 个收件人地址
邮件主题	可以填写长度为 50 的邮件主题，支持中文
邮件内容	可以填写长度为 350 的邮件正文，支持中文和任何符号
上传附件	可以选择本地文件或服务器文件，大小不超过 1.4M，附件文件名暂不支持中文。

如果不能正常发邮件，请确认发件人的邮件服务器是否支持 SMTP，并请检查 DNS 配置、邮件服务器地址、用户名和密码是否正确。

第21章 流量可视

流量可视模块能够显示 Guard 的各种统计信息，包括 session 统计，整机流量，IP 统计，应用统计等，可以帮助 Guard 管理员定位问题，查看网络历史情况。

21.1 统计配置

流量可视的基本参数配置页面，在这里可以配置统计开关，采样比，出入接口，以及流监控的参数。

表 21-1 统计配置参数列表

值域	说明
开启统计	流量可视开关
统计采样比	统计的采样比 范围 1-1000 个
应用列表	配置出接口和入接口
日志服务器	配置的日志服务器地址
流量日志	是否开启流量日志
流监控采样比	流监控的采样比，范围 1-10000
活跃流老化时间	老化时间 范围 1-1800 秒
非活跃流老化时间	老化时间 范围 1-60 秒

统计配置

开启统计

统计采样比: 个 (1-1000)

接口应用: 接口名称: 类型:

应用列表:

Ge0/0/0 inner
 Ge0/0/1 outer
 Ge0/0/2 outer
 Ge0/0/3 inner

自定义策略:

<<"/>

注: 启用统计策略的总和不能超过5个

流监控: 日志服务器:

流量日志开启:

流监控采样比: 个 (1-10000)

活跃流老化时间: 秒 (1 - 1800)

非活跃流老化时间: 秒 (1 - 60)

图 21-1 统计配置页面

21.2 网络概览

显示当前网络情况，显示分为 4 部分：会话总数、整机流量、TOP IP 带宽、TOP 应用

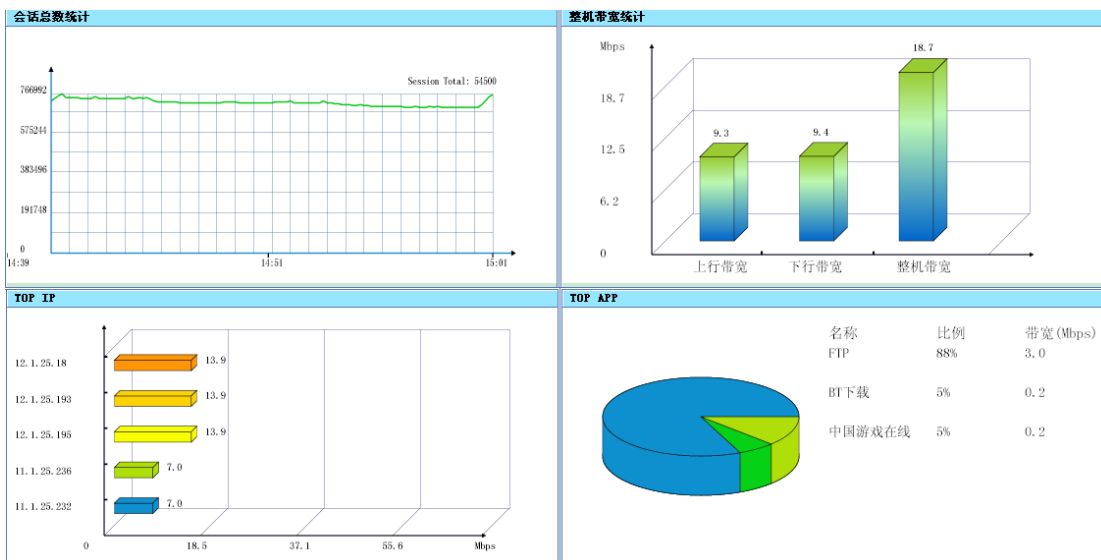


图 21-2 网络概览

21.3 接口统计

接口统计分为图形模式和列表模式。

列表模式 | 图形模式

刷新间隔: 5秒 | 2011-07-18 15:17 - 2011-07-19 15:17 | 刷新

接口	时间	流量 (KB)			带宽 (Kbps)									平均新建会话速率	平均会话总数		
					最小带宽			最大带宽			平均带宽						
		流入	流出	总流量	流入	流出	总带宽	流入	流出	总带宽	流入	流出	总带宽				
Ge0/0/0	15:18 - 15:25																

图 21-3 接口流量统计列表模式

图形模式有 2 张统计图，分别是带宽图和流量图。带宽图表示的是时间段内带宽的变化，流量图是时间段内流量的累加变化。

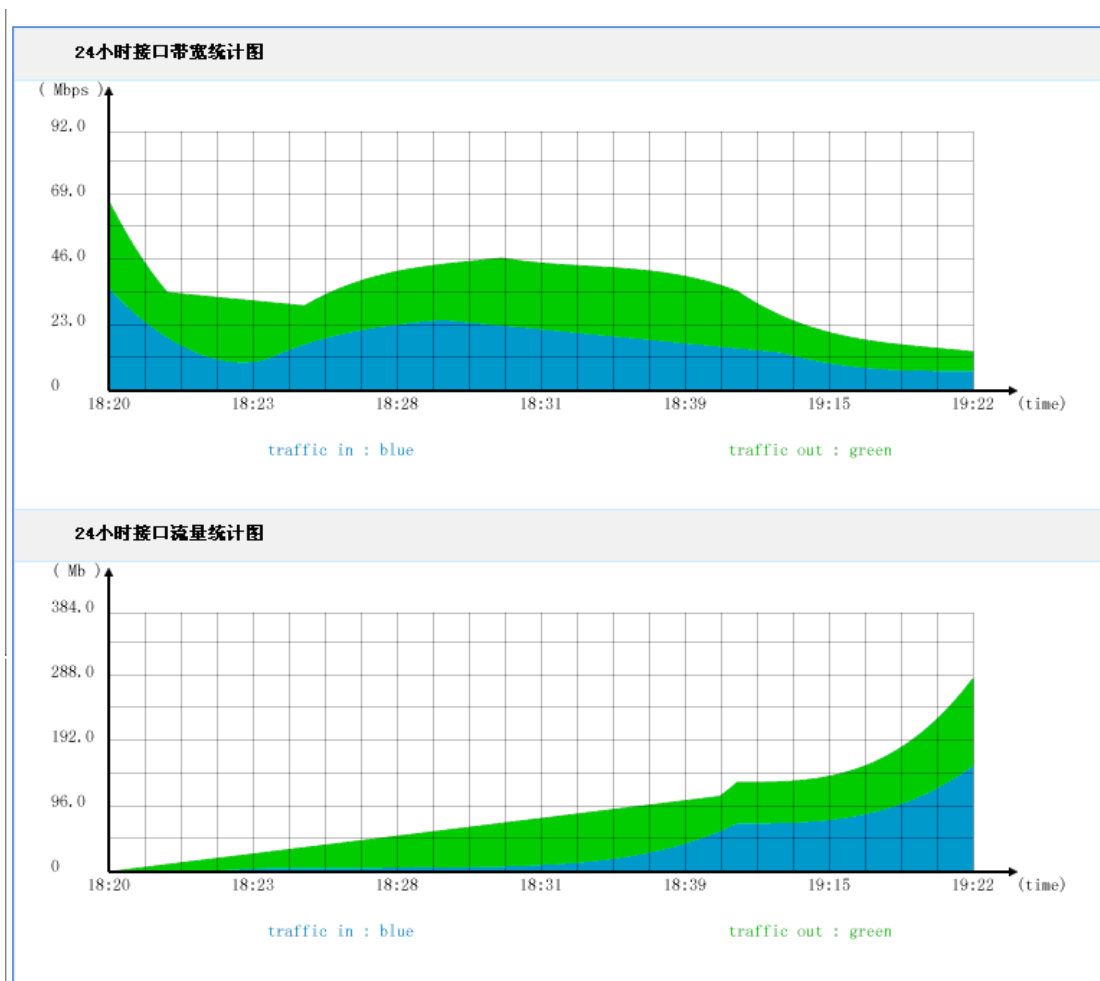


图 21-4 接口流量统计图形模式

21.4 应用统计

应用统计可以查看实时应用统计分布和实时应用 TOP10。

实时应用统计分为图形模式和列表模式。图形模式是以图形模式来展现应用统计信息，列表模式则是详细数字形式来显示应用统计信息。

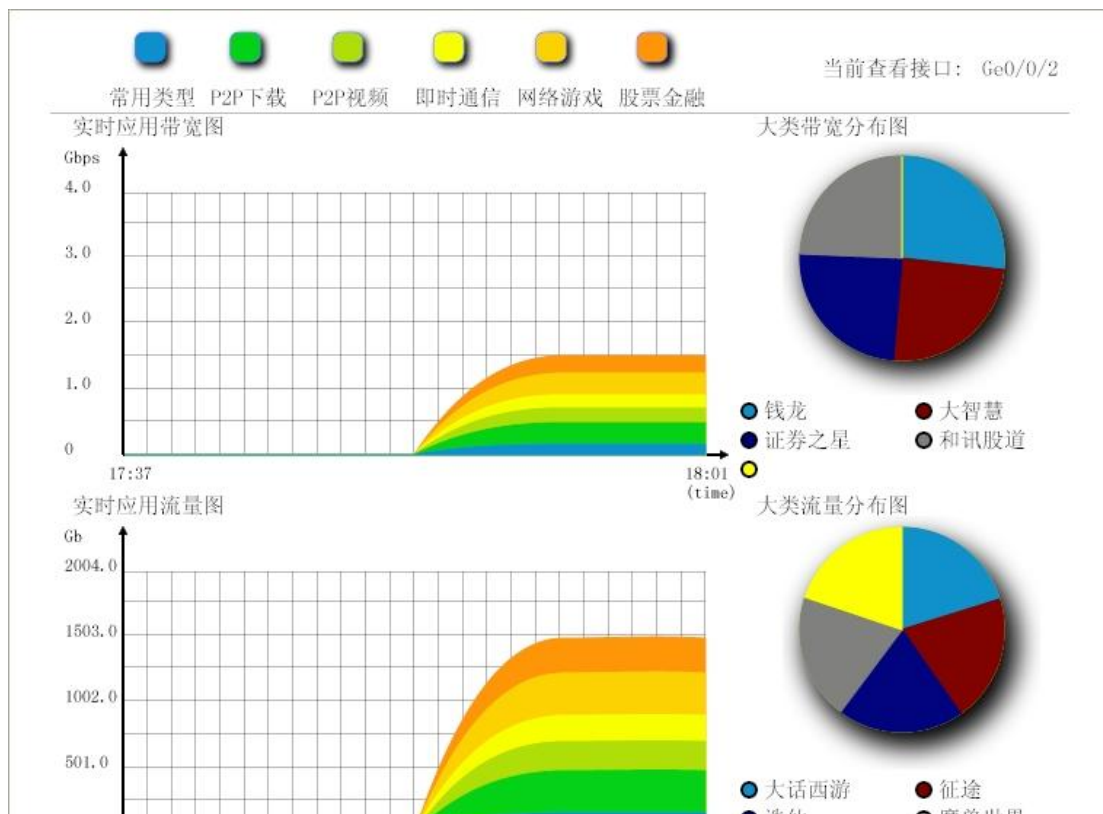


图 21-5 实时应用统计图形模式

列表模式

组名称	小类名称	带宽			流量		
		流入带宽	流出带宽	总带宽	流入流量	流出流量	总流量
常用协议	大类统计	75480	75360	150840	13267	13246	26513
P2P下载	大类统计	164760	163200	327960	28961	28687	57648
	BT下载	32797	32625	65422	5765	5734	11499
	IMESH	32686	32472	65158	5745	5707	11452
	屁屁狗	33237	32888	66125	5842	5781	11623
	脱兔	33045	32643	65688	5808	5738	11546
	pp365	33069	32620	65689	5812	5733	11545
P2P视频	大类统计	107160	115920	223080	18836	20376	39212
	PFLIVE	33129	32650	65779	5823	5739	11562
	沸点	32897	32519	65416	5782	5716	11498
	funshion	41160	50760	91920	7235	8922	16157
即时通讯	大类统计	98640	97680	196320	17339	17170	34509
	腾讯QQ	33068	32643	65711	5812	5738	11550
	百度HI	32789	32561	65350	5763	5723	11486
	kubao	32888	32550	65438	5781	5721	11502
	大类统计	165800	162800	328600	29109	28582	57691
魔兽世界	33238	32353	65591	5842	5887	11729	

图 21-6 实时应用统计列表模式

应用 TOP10



图 21-7 实时应用 TOP10

21.5 会话统计

会话统计可以显示 Guard 新建会话和会话总数的变化趋势。此页面分为 2 张统计图。

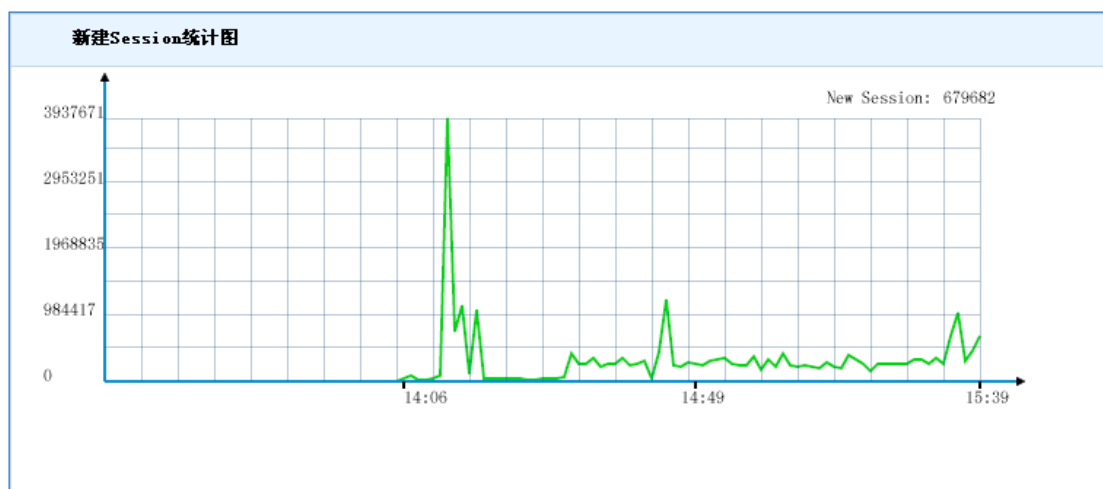


图 21-8 新建会话统计图

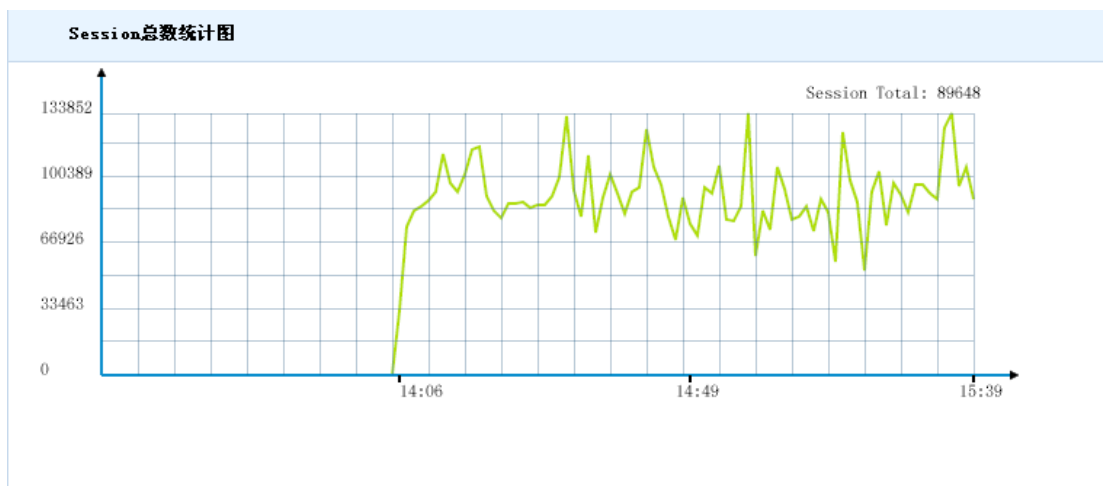


图 21-9 会话总数统计图

21.6 IP 统计

IP 统计可以查看带宽 TOP IP

查看前 个IP

IP名称	IP类型	上行带宽 (Kbps)	下行带宽 (Kbps)
1.1.1.245	内部IP	37	30
1.1.1.246	内部IP	37	30
1.1.1.247	内部IP	37	30
1.1.1.248	内部IP	37	30
1.1.1.249	内部IP	37	30
1.1.1.250	内部IP	37	30
1.1.1.251	内部IP	37	30
1.1.1.252	内部IP	37	30
1.1.1.253	内部IP	37	30
1.1.1.254	内部IP	37	30

第1页/1页 跳转到 页 每页 行

图 21-10 IP 统计显示页面

21.7 自定义统计

自定义统计可以根据参数来进行统计，参数包括：pcp 或接口、ip 范围、应用大类。还可以配置统计结果的显示类别。

首先点击添加按钮，添加一条自定义统计策略。

策略名称	统计方式	状态	统计结果	流量建模	操作
x	PCP方式	统计中	查看	建模	

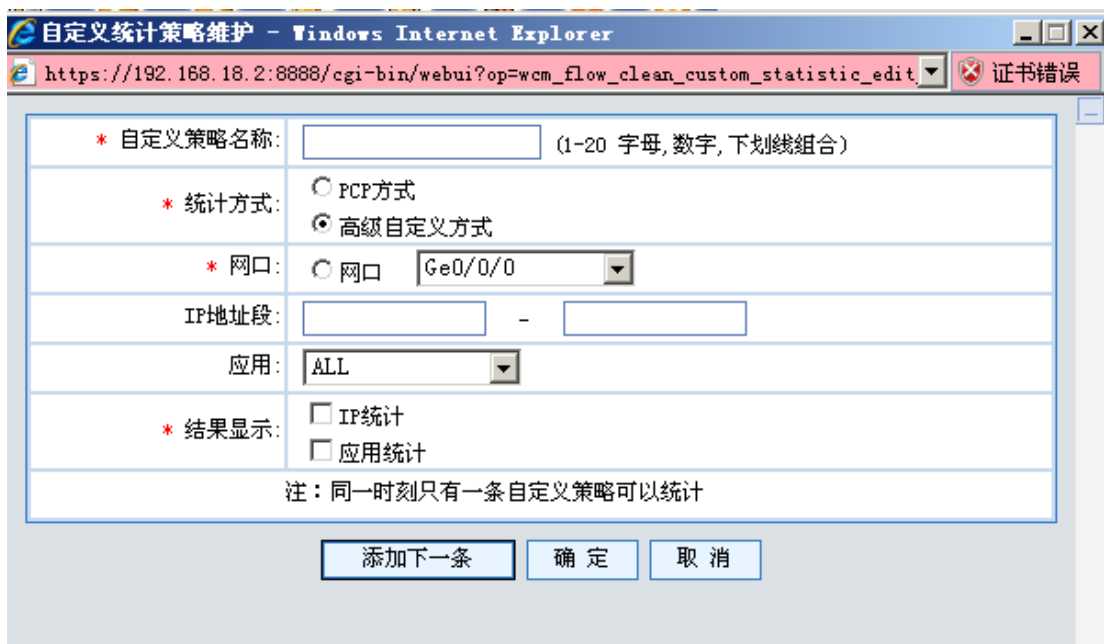
添加

第1页/1页 跳转到 页 Go 每页 行

图 21-11 自定义统计图显示页面

之后可以配置统计选项

这里统计方式有 2 种，一种是根据 pcpl 规则进行统计，另一种是按照自定义方式。



自定义统计策略维护 - Windows Internet Explorer

https://192.168.18.2:8888/cgi-bin/webui?op=wcm_flow_clean_custom_statistic_edit

* 自定义策略名称: (1-20 字母, 数字, 下划线组合)

* 统计方式: PCP方式 高级自定义方式

* 网口: 网口

IP地址段: -

应用:

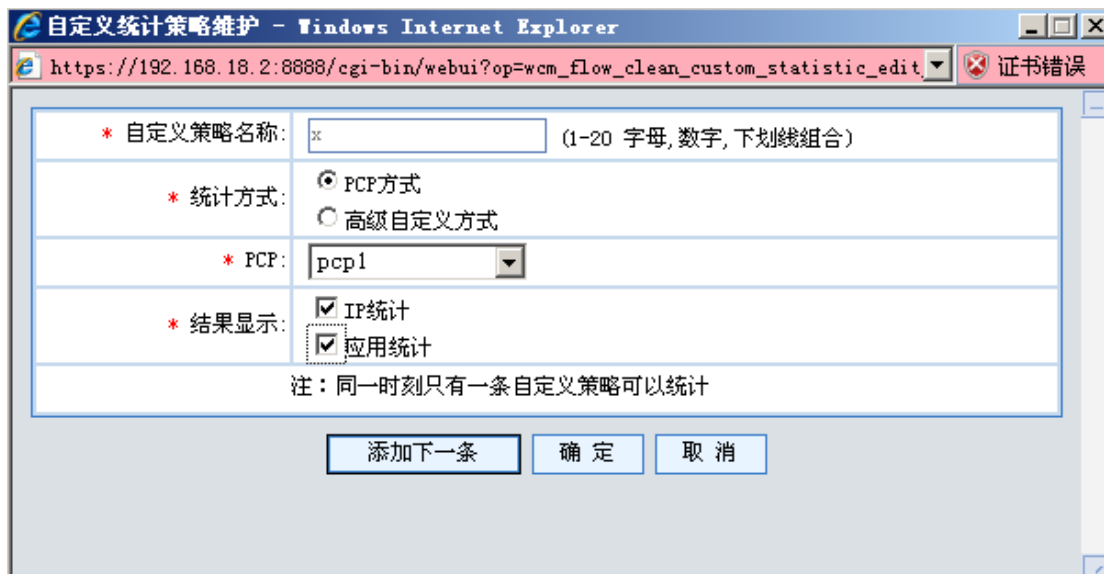
* 结果显示: IP统计 应用统计

注: 同一时刻只有一条自定义策略可以统计

添加下一条 确定 取消

图 21-12 自定义统计图添加页面

配置好之后还可以点击编辑按钮进行修改



自定义统计策略维护 - Windows Internet Explorer

https://192.168.18.2:8888/cgi-bin/webui?op=wcm_flow_clean_custom_statistic_edit

* 自定义策略名称: x (1-20 字母, 数字, 下划线组合)

* 统计方式: PCP方式 高级自定义方式

* PCP:

* 结果显示: IP统计 应用统计

注: 同一时刻只有一条自定义策略可以统计

添加下一条 确定 取消

图 21-13 自定义统计图编辑页面

创建策略之后需要应用策略，页面如下：

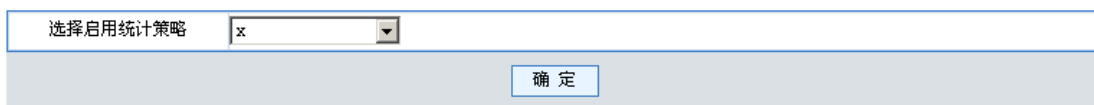


图 21-14 应用自定义统计策略页面

应用之后可以点击 查看 查看统计结果。



策略信息

策略名称:	x
统计方式:	PCF方式
统计参数:	PCF : <u>udp</u>
结果显示:	IP APP

IP地址	带宽 (Kbps)		
	流入带宽	流出带宽	总带宽
1.1.1.102	1	2	3
1.1.1.101	1	2	3
1.1.1.100	1	2	3
1.1.1.97	1	2	3
1.1.1.96	1	2	3
1.1.1.95	1	2	3
1.1.1.94	1	2	3
1.1.1.93	1	2	3
1.1.1.92	1	2	3

应用名称	带宽		
	流入带宽	流出带宽	总带宽
股票金融	0	0	0
即时通讯	0	0	0
P2P下载	0	0	0
网络游戏	0	0	0
P2P视频	0	0	0
常用协议	760	907	1667

图 21-15 自定义统计图查看结果页面

第22章 系统监控

系统监控能够显示 Guard 当时的工作状态,为 Guard 管理员提供了功能强大的监控工具。与启明星辰集中管理软件共同使用,可以搭建全面的安全管理平台。

系统监控里的饼图、曲线、柱状图均采用了新一代图形显示技术 SVG (Scalable Vector Graphics), IE6 正常显示图形需要安装支持 SVG 的控件 Adobe SVG Viewer, 访问相应界面是监控页面会自动检测浏览器是否支持 SVG, 若不支持会提供下载控件网址供下载。

注意: 若页面的曲线数据不发生变化,请修改 IE 设置,方法如下,

点击“工具->Internet 选项->Internet 临时文件->设置”,将“Internet 所存网页的较新版本”选择“每次访问此页时检查”。

22.1 CPU 监控

通过以下页面可以查看 cpu 利用率。



图 22-1 CPU 利用率

22.2 内存监控

通过以下页面可以查看内存利用率

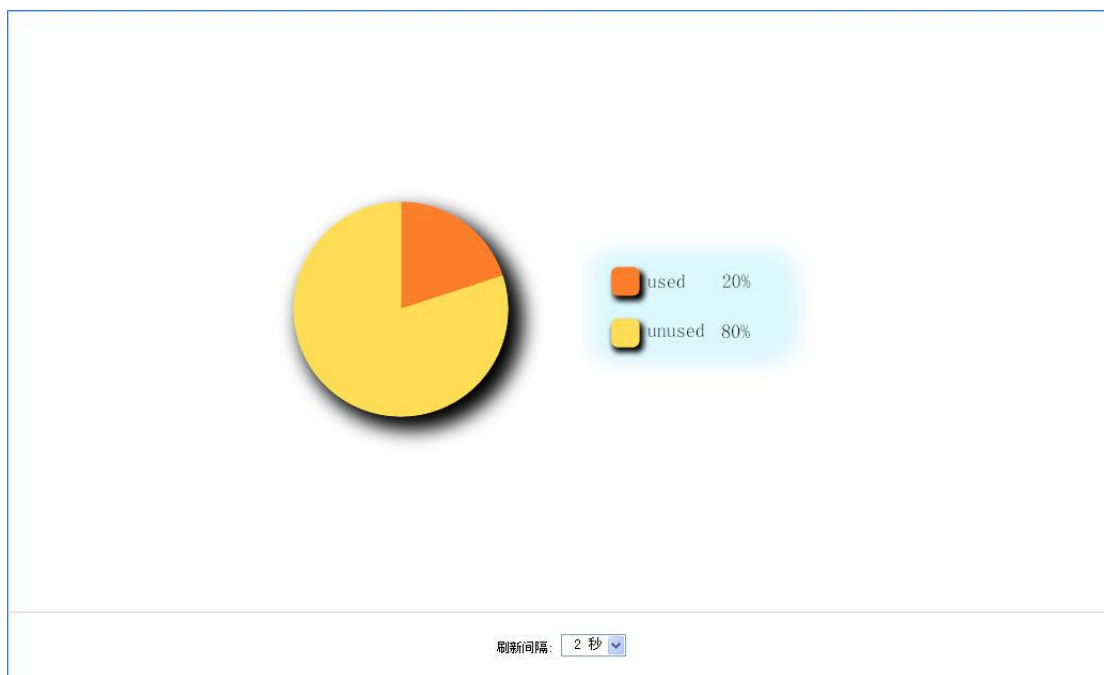


图 22-2 内存利用率

Used 表示已经使用内存占总内存比例

Unused 表示未使用的内存占总内存比例

22.3 接口流量统计

接口流量显示最近 120 秒时间内，指定接口流入/流出的带宽流量

系统监控>>接口流量统计

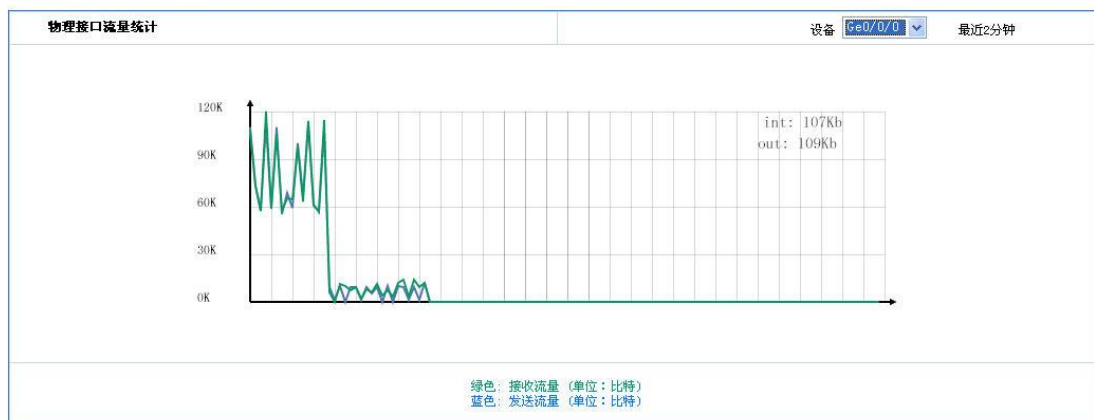


图 22-3 接口流量统计

第23章 在线支持

23.1 技术支持

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

1. 参考随机提供的 Guard 帮助手册
2. 登录到启明星辰的网站 www.venustech.com.cn 寻求帮助
3. 给启明星辰的售后服务人员打电话寻求帮助，热线电话是：400-624-3900 和 800-810-6038



尊敬的用户，如果在使用过程中遇到任何问题，您可以这样做：

1. 参考随机的帮助手册
2. 登录到支持网站<http://www.venustech.com.cn/寻求帮助>
3. 给支持人员打电话寻求帮助，热线电话是：800-810-6038

感谢您使用信息安全产品！

图 23-1 天清异常流量清洗系统 Guard 技术支持

23.2 关于

选择“关于”，出现天清异常流量清洗系统 Guard 的简单说明。



© 1996-2011 北京启明星辰信息安全技术有限公司版权所有

图 23-2 关于天清异常流量清洗系统 Guard