无标题-4

|  |
| --- |
|  |



文档版本： ()

|  |
| --- |
| © 2014 绿盟科技 |

|  |
| --- |
| ■ 版权声明 |
| 本文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，版权均属北京神州绿盟信息安全科技股份有限公司（简称）所有，受到有关产权及版权法保护。任何个人、机构未经的书面授权许可，不得以任何方式复制或引用本文的任何片断。 |

目录

[前言 1](#_Toc392259051)

[1 产品概述 3](#_Toc392259052)

[1.1 产品特点 3](#_Toc392259053)

[1.2 主要功能 5](#_Toc392259054)

[1.3 管理方式 5](#_Toc392259055)

[1.3.1 Web管理 5](#_Toc392259056)

[1.3.2 Console管理 10](#_Toc392259057)

[2 首页 14](#_Toc392259058)

[2.1 状态 14](#_Toc392259059)

[2.2 入侵防护事件 16](#_Toc392259060)

[2.3 高级威胁事件 19](#_Toc392259061)

[2.4 信誉事件 20](#_Toc392259062)

[2.5 URL分类事件 21](#_Toc392259063)

[2.6 防病毒事件 21](#_Toc392259064)

[2.7 流量分析 22](#_Toc392259065)

[2.7.1 流量 22](#_Toc392259066)

[2.7.2 查看应用流量监控 24](#_Toc392259067)

[2.7.3 查看IP流量监控 26](#_Toc392259068)

[2.8 在线用户 26](#_Toc392259069)

[3 系统维护 28](#_Toc392259070)

[3.1 系统升级 28](#_Toc392259071)

[3.1.1 查看系统更新状态 28](#_Toc392259072)

[3.1.2 在线升级配置 29](#_Toc392259073)

[3.1.3 离线升级配置 31](#_Toc392259074)

[3.2 备份恢复 32](#_Toc392259075)

[3.2.1 备份文件 32](#_Toc392259076)

[3.2.2 恢复文件 32](#_Toc392259077)

[3.2.3 系统配置还原 33](#_Toc392259078)

[3.3 系统配置 34](#_Toc392259079)

[3.3.1 引擎配置 34](#_Toc392259080)

[3.3.2 配置专业参数 36](#_Toc392259081)

[3.4 安全中心 36](#_Toc392259082)

[3.4.1 连接安全中心 36](#_Toc392259083)

[3.4.2 配置接口升级 39](#_Toc392259084)

[3.5 帐号管理 40](#_Toc392259085)

[3.5.1 账号管理 40](#_Toc392259086)

[3.5.2 参数配置 42](#_Toc392259087)

[3.6 诊断工具 44](#_Toc392259088)

[3.6.1 Ping工具 44](#_Toc392259089)

[3.6.2 Traceroute工具 45](#_Toc392259090)

[3.6.3 网络连接状态 45](#_Toc392259091)

[3.6.4 网卡状态 46](#_Toc392259092)

[3.6.5 路由信息 47](#_Toc392259093)

[3.6.6 回放测试 47](#_Toc392259094)

[3.6.7 专家诊断 48](#_Toc392259095)

[3.6.8 抓包 49](#_Toc392259096)

[3.7 证书管理 50](#_Toc392259097)

[3.7.1 查看证书状态 50](#_Toc392259098)

[3.7.2 导入证书 52](#_Toc392259099)

[3.8 系统控制 53](#_Toc392259100)

[3.9 其他配置 54](#_Toc392259101)

[4 网络配置 56](#_Toc392259102)

[4.1 接口 56](#_Toc392259103)

[4.2 安全区 60](#_Toc392259104)

[4.3 DNS配置 61](#_Toc392259105)

[4.4 IPMAC绑定配置 62](#_Toc392259106)

[4.4.1 新建IP/MAC绑定规则 62](#_Toc392259107)

[4.4.2 导入IP/MAC绑定规则 63](#_Toc392259108)

[4.5 静态路由 65](#_Toc392259109)

[4.6 SNMP 67](#_Toc392259110)

[4.6.1 Agent访问控制 67](#_Toc392259111)

[4.6.2 Trap 69](#_Toc392259112)

[4.6.3 系统配置信息 72](#_Toc392259113)

[4.7 高可用性 73](#_Toc392259114)

[4.7.1 基本概念 73](#_Toc392259115)

[4.7.2 基本配置 74](#_Toc392259116)

[4.7.3 直通配置 75](#_Toc392259117)

[4.7.4 非对称路由支持 78](#_Toc392259118)

[4.8 外置bypass配置 79](#_Toc392259119)

[5 对象 82](#_Toc392259120)

[5.1 规则对象 82](#_Toc392259121)

[5.1.1 系统规则模板 83](#_Toc392259122)

[5.1.2 用户规则模板 85](#_Toc392259123)

[5.1.3 自定义规则 86](#_Toc392259124)

[5.1.4 例外规则 94](#_Toc392259125)

[5.1.5 规则查询 96](#_Toc392259126)

[5.2 网络对象 98](#_Toc392259127)

[5.2.1 网络对象 98](#_Toc392259128)

[5.2.2 节点对象 99](#_Toc392259129)

[5.2.3 MAC地址对象 101](#_Toc392259130)

[5.2.4 IP池对象 103](#_Toc392259131)

[5.2.5 网络组对象 104](#_Toc392259132)

[5.3 服务对象 105](#_Toc392259133)

[5.3.1 系统服务对象 106](#_Toc392259134)

[5.3.2 自定义服务对象 106](#_Toc392259135)

[5.3.3 服务组对象 109](#_Toc392259136)

[5.3.4 服务超时 110](#_Toc392259137)

[5.4 应用对象 111](#_Toc392259138)

[5.4.1 系统应用对象 112](#_Toc392259139)

[5.4.2 自定义应用对象 113](#_Toc392259140)

[5.4.3 配置过滤器 117](#_Toc392259141)

[5.5 时间对象 119](#_Toc392259142)

[5.5.1 自定义时间对象 119](#_Toc392259143)

[5.5.2 时间组对象 120](#_Toc392259144)

[5.6 敏感数据对象 121](#_Toc392259145)

[5.7 流量通道对象 123](#_Toc392259146)

[6 策略配置 126](#_Toc392259147)

[6.1 策略通用操作 127](#_Toc392259148)

[6.2 入侵防护策略 129](#_Toc392259149)

[6.2.1 入侵防护策略 129](#_Toc392259150)

[6.2.2 DoS防护策略 131](#_Toc392259151)

[6.3 高级威胁防御策略 135](#_Toc392259152)

[6.3.1 敏感数据保护策略 135](#_Toc392259153)

[6.3.2 文件识别策略 137](#_Toc392259154)

[6.3.3 服务器异常防护策略 139](#_Toc392259155)

[6.3.4 服务器异常学习 142](#_Toc392259156)

[6.4 信誉 143](#_Toc392259157)

[6.4.1 僵尸网络防护 143](#_Toc392259158)

[6.4.2 Web信誉 144](#_Toc392259159)

[6.5 URL分类过滤策略 145](#_Toc392259160)

[6.5.1 配置URL分类模式 145](#_Toc392259161)

[6.5.2 新建URL过滤策略 146](#_Toc392259162)

[6.5.3 新建自定义URL分类规则 148](#_Toc392259163)

[6.5.4 URL测试 150](#_Toc392259164)

[6.6 防病毒策略 150](#_Toc392259165)

[6.7 用户管理策略 152](#_Toc392259166)

[6.7.1 服务器配置 152](#_Toc392259167)

[6.7.2 用户认证 157](#_Toc392259168)

[6.7.3 用户识别 158](#_Toc392259169)

[6.7.4 认证策略 159](#_Toc392259170)

[6.8 应用管理策略 161](#_Toc392259171)

[6.9 流量管理策略 163](#_Toc392259172)

[6.9.1 流量管理策略 163](#_Toc392259173)

[6.9.2 流量分析策略 166](#_Toc392259174)

[7 日志报表 168](#_Toc392259175)

[7.1 日志分析 168](#_Toc392259176)

[7.1.1 日志配置 168](#_Toc392259177)

[7.1.2 日志查看 169](#_Toc392259178)

[7.2 统计报表 175](#_Toc392259179)

[7.2.1 报表配置 175](#_Toc392259180)

[7.2.2 报表详情 176](#_Toc392259181)

[8 Console管理 177](#_Toc392259182)

[8.1 查看系统信息 177](#_Toc392259183)

[8.2 诊断工具 178](#_Toc392259184)

[8.3 维护工具 179](#_Toc392259185)

[8.4 系统初始化 180](#_Toc392259186)

[8.5 重新启动系统 181](#_Toc392259187)

[8.6 关闭系统 182](#_Toc392259188)

[8.7 退出配置界面 183](#_Toc392259189)

[A 缩略语 184](#_Toc392259190)

[B 管理AD域配置器 185](#_Toc392259191)

[B.1 安装AD域配置器 185](#_Toc392259192)

[B.2 配置AD域配置器 188](#_Toc392259193)

[C 出厂参数 190](#_Toc392259194)

[C.1 引擎接口初始设置 190](#_Toc392259195)

[C.2 引擎初始管理员 190](#_Toc392259196)

[C.2.1 Web操作员初始帐号 190](#_Toc392259197)

[C.2.2 Web审计员初始帐号 190](#_Toc392259198)

[C.2.3 Console口管理员初始帐号 190](#_Toc392259199)

[C.3 Console口通讯参数 190](#_Toc392259200)

[C.4 CLI管理员初始帐号 191](#_Toc392259201)

插图

[图1-1 零配置处理流程 4](#_Toc392259202)

[图1-2 零配置上线默认生成的安全策略 4](#_Toc392259203)

[图1-3 登录时的安全警报界面 7](#_Toc392259204)

[图1-4 Web管理登录界面 7](#_Toc392259205)

[图1-5 Web管理页面布局 8](#_Toc392259206)

[图1-6 配置快速连接 11](#_Toc392259207)

[图1-7 登录界面 11](#_Toc392259208)

[图1-8 语言选择 12](#_Toc392259209)

[图1-9 Console管理主菜单 12](#_Toc392259210)

[图2-1 系统状态 15](#_Toc392259211)

[图2-2 流量监控 15](#_Toc392259212)

[图2-3 版本信息 16](#_Toc392259213)

[图2-4 接口信息 16](#_Toc392259214)

[图2-5 入侵防护事件 17](#_Toc392259215)

[图2-6 入侵防护事件分析 18](#_Toc392259216)

[图2-7 添加例外 19](#_Toc392259217)

[图2-8 确认添加例外 19](#_Toc392259218)

[图2-9 高级威胁事件 20](#_Toc392259219)

[图2-10 信誉事件 20](#_Toc392259220)

[图2-11 URL分类事件 21](#_Toc392259221)

[图2-12 防病毒事件 22](#_Toc392259222)

[图2-13 总流量 23](#_Toc392259223)

[图2-14 应用历史记录 23](#_Toc392259224)

[图2-15 应用会话数 24](#_Toc392259225)

[图2-16 各类应用流量所占总流量比例 24](#_Toc392259226)

[图2-17 流量管理策略对应上、下行速率 25](#_Toc392259227)

[图2-18 上下行速率排名详情 25](#_Toc392259228)

[图2-19 IP流量监控 26](#_Toc392259229)

[图2-20 查看在线用户 27](#_Toc392259230)

[图3-1 查看系统当前版本 29](#_Toc392259231)

[图3-2 在线升级 30](#_Toc392259232)

[图3-3 离线升级 31](#_Toc392259233)

[图3-4 备份文件 32](#_Toc392259234)

[图3-5 恢复文件 33](#_Toc392259235)

[图3-6 手动还原点 33](#_Toc392259236)

[图3-7 自动还原点 34](#_Toc392259237)

[图3-8 引擎配置 35](#_Toc392259238)

[图3-9 与绿盟科技企业安全中心连接 37](#_Toc392259239)

[图3-10 高级选项 38](#_Toc392259240)

[图3-11 帐号管理 40](#_Toc392259241)

[图3-12 新建帐号 41](#_Toc392259242)

[图3-13 帐号管理的参数配置 43](#_Toc392259243)

[图3-14 Ping工具诊断结果 45](#_Toc392259244)

[图3-15 Traceroute工具诊断结果 45](#_Toc392259245)

[图3-16 网络连接状态 46](#_Toc392259246)

[图3-17 Server状态 46](#_Toc392259247)

[图3-18 查看网卡状态 47](#_Toc392259248)

[图3-19 查看路由信息 47](#_Toc392259249)

[图3-20 回放测试 48](#_Toc392259250)

[图3-21 专家诊断 48](#_Toc392259251)

[图3-22 抓包 49](#_Toc392259252)

[图3-23 查看证书状态信息 51](#_Toc392259253)

[图3-24 导入证书 52](#_Toc392259254)

[图3-25 导入授权证书确认对话框 53](#_Toc392259255)

[图3-26 系统控制 54](#_Toc392259256)

[图3-27 SQL注入白名单 55](#_Toc392259257)

[图4-1 网络接口列表 57](#_Toc392259258)

[图4-2 配置接口信息 58](#_Toc392259259)

[图4-3 网络安全区列表 60](#_Toc392259260)

[图4-4 新建安全区 61](#_Toc392259261)

[图4-5 新建DNS客户端 62](#_Toc392259262)

[图4-6 IP和MAC绑定规则列表 62](#_Toc392259263)

[图4-7 新建IP/MAC规则 63](#_Toc392259264)

[图4-8 导入IP/MAC规则 – 文件导入 64](#_Toc392259265)

[图4-9 导入IP/MAC规则 – 手工填写 64](#_Toc392259266)

[图4-10 静态路由 65](#_Toc392259267)

[图4-11 新建静态路由 66](#_Toc392259268)

[图4-12 SNMP Agent访问控制 67](#_Toc392259269)

[图4-13 V1和V2c版本Agent访问控制 68](#_Toc392259270)

[图4-14 V3版本Agent访问控制 68](#_Toc392259271)

[图4-15 SNMP Trap 70](#_Toc392259272)

[图4-16 V1和V2版本Trap 70](#_Toc392259273)

[图4-17 V3版本Trap 71](#_Toc392259274)

[图4-18 SNMP系统配置信息 72](#_Toc392259275)

[图4-19 高可用性基本参数 74](#_Toc392259276)

[图4-20 HA直通参数配置 76](#_Toc392259277)

[图4-21 非对称路由支持列表 78](#_Toc392259278)

[图4-22 新建非对称路由支持 79](#_Toc392259279)

[图4-23 NIPS与bypass交换机联动的拓扑图 80](#_Toc392259280)

[图4-24 外置bypass设备 81](#_Toc392259281)

[图5-1 系统规则模板 84](#_Toc392259282)

[图5-2 新建派生规则模板 84](#_Toc392259283)

[图5-3 用户规则模板 85](#_Toc392259284)

[图5-4 新建用户规则模板 86](#_Toc392259285)

[图5-5 基本规则 87](#_Toc392259286)

[图5-6 新建自定义IP规则 87](#_Toc392259287)

[图5-7 新建自定义UDP规则 89](#_Toc392259288)

[图5-8 新建自定义ICMP规则 90](#_Toc392259289)

[图5-9 高级规则 91](#_Toc392259290)

[图5-10 新建高级规则 92](#_Toc392259291)

[图5-11 添加与关系 93](#_Toc392259292)

[图5-12 添加或关系协议字段 93](#_Toc392259293)

[图5-13 例外规则 95](#_Toc392259294)

[图5-14 规则详情 95](#_Toc392259295)

[图5-15 确认取消例外 96](#_Toc392259296)

[图5-16 规则库搜索 97](#_Toc392259297)

[图5-17 查询条件高级选项 97](#_Toc392259298)

[图5-18 网络对象 98](#_Toc392259299)

[图5-19 新建网络对象 99](#_Toc392259300)

[图5-20 节点对象 100](#_Toc392259301)

[图5-21 新建节点对象 100](#_Toc392259302)

[图5-22 选择CSV文件 101](#_Toc392259303)

[图5-23 MAC地址对象 102](#_Toc392259304)

[图5-24 新建MAC地址对象 102](#_Toc392259305)

[图5-25 IP池对象 103](#_Toc392259306)

[图5-26 新建IP池对象 103](#_Toc392259307)

[图5-27 网络组对象 104](#_Toc392259308)

[图5-28 新建网络组对象 105](#_Toc392259309)

[图5-29 系统服务对象 106](#_Toc392259310)

[图5-30 自定义服务 107](#_Toc392259311)

[图5-31 新建自定义服务对象 – TCP/UDP 107](#_Toc392259312)

[图5-32 新建自定义服务对象 – IP 108](#_Toc392259313)

[图5-33 自定义服务组 109](#_Toc392259314)

[图5-34 新建服务组对象 109](#_Toc392259315)

[图5-35 服务超时 110](#_Toc392259316)

[图5-36 新建服务超时 111](#_Toc392259317)

[图5-37 系统应用对象 112](#_Toc392259318)

[图5-38 查询系统应用对象 113](#_Toc392259319)

[图5-39 应用对象 – 自定义应用对象列表 114](#_Toc392259320)

[图5-40 应用对象 – 新建应用对象 114](#_Toc392259321)

[图5-41 过滤器 117](#_Toc392259322)

[图5-42 新建过滤器 118](#_Toc392259323)

[图5-43 自定义时间对象 119](#_Toc392259324)

[图5-44 新建自定义时间对象 119](#_Toc392259325)

[图5-45 时间组对象 120](#_Toc392259326)

[图5-46 新建时间组对象 121](#_Toc392259327)

[图5-47 敏感数据对象 122](#_Toc392259328)

[图5-48 新建敏感数据 122](#_Toc392259329)

[图5-49 流量通道对象 123](#_Toc392259330)

[图5-50 新建流量通道对象 124](#_Toc392259331)

[图6-1 策略配置流程 126](#_Toc392259332)

[图6-2 移动策略 127](#_Toc392259333)

[图6-3 复制策略 128](#_Toc392259334)

[图6-4 入侵防护策略 129](#_Toc392259335)

[图6-5 新建入侵防护策略 130](#_Toc392259336)

[图6-6 Flood防护 132](#_Toc392259337)

[图6-7 PortScan防护 133](#_Toc392259338)

[图6-8 PINGSweep防护 134](#_Toc392259339)

[图6-9 ARPSpoof防护 135](#_Toc392259340)

[图6-10 敏感数据保护策略 136](#_Toc392259341)

[图6-11 新建敏感数据保护策略 136](#_Toc392259342)

[图6-12 文件识别策略 137](#_Toc392259343)

[图6-13 新建文件识别策略 138](#_Toc392259344)

[图6-14 服务器异常防护策略 139](#_Toc392259345)

[图6-15 新建服务器异常防护策略 140](#_Toc392259346)

[图6-16 定义服务器的正常外联行为 141](#_Toc392259347)

[图6-17 服务器异常学习 142](#_Toc392259348)

[图6-18 僵尸网络防护 143](#_Toc392259349)

[图6-19 Web信誉 144](#_Toc392259350)

[图6-20 URL分类 145](#_Toc392259351)

[图6-21 URL分类模式 146](#_Toc392259352)

[图6-22 新建URL过滤策略 147](#_Toc392259353)

[图6-23 新建URL分类 149](#_Toc392259354)

[图6-24 URL测试 150](#_Toc392259355)

[图6-25 URL测试结果 150](#_Toc392259356)

[图6-26 防病毒策略 151](#_Toc392259357)

[图6-27 新建防病毒策略 151](#_Toc392259358)

[图6-28 AD域认证拓扑图 153](#_Toc392259359)

[图6-29 服务器配置 154](#_Toc392259360)

[图6-30 配置AD域认证服务器 154](#_Toc392259361)

[图6-31 配置Radius认证服务器 155](#_Toc392259362)

[图6-32 配置EPS联动服务器 155](#_Toc392259363)

[图6-33 配置LDAP认证服务器 156](#_Toc392259364)

[图6-34 用户认证 157](#_Toc392259365)

[图6-35 用户识别 – 关闭状态 158](#_Toc392259366)

[图6-36 用户识别 – 配置参数 159](#_Toc392259367)

[图6-37 用户管理 – 认证策略 159](#_Toc392259368)

[图6-38 用户管理 – 新建认证策略 160](#_Toc392259369)

[图6-39 应用管理策略 161](#_Toc392259370)

[图6-40 新建应用管理策略 161](#_Toc392259371)

[图6-41 流量管理策略 163](#_Toc392259372)

[图6-42 新建流量通道线路 164](#_Toc392259373)

[图6-43 添加流量管理策略 165](#_Toc392259374)

[图6-44 新建流量分析策略 166](#_Toc392259375)

[图7-1 入侵防护日志 169](#_Toc392259376)

[图7-2 高级威胁日志 170](#_Toc392259377)

[图7-3 信誉日志 170](#_Toc392259378)

[图7-4 应用管理日志 171](#_Toc392259379)

[图7-5 URL分类日志 172](#_Toc392259380)

[图7-6 防病毒日志 172](#_Toc392259381)

[图7-7 认证日志 173](#_Toc392259382)

[图7-8 认证状态日志 173](#_Toc392259383)

[图7-9 运行日志 174](#_Toc392259384)

[图7-10 系统日志 175](#_Toc392259385)

[图8-1 引擎串口管理 – 查看系统信息 178](#_Toc392259386)

[图8-2 引擎串口管理 – 诊断工具 179](#_Toc392259387)

[图8-3 引擎串口管理 – 维护工具 180](#_Toc392259388)

[图8-4 引擎串口管理 – 系统初始化 181](#_Toc392259389)

[图8-5 引擎串口管理 – 重新启动系统 182](#_Toc392259390)

[图8-6 引擎串口管理 – 关闭系统 182](#_Toc392259391)

[图8-7 引擎串口管理 – 退出系统 183](#_Toc392259392)

表格

[表1-1 用户权限信息 6](#_Toc392259393)

[表1-2 页面布局 8](#_Toc392259394)

[表1-3 常用操作 9](#_Toc392259395)

[表1-4 Console口按键说明 13](#_Toc392259396)

[表3-1 升级参数 30](#_Toc392259397)

[表3-2 升级文件类型 31](#_Toc392259398)

[表3-3 引擎主要参数 35](#_Toc392259399)

[表3-4 安全中心基本配置参数 37](#_Toc392259400)

[表3-5 安全中心高级选项参数 39](#_Toc392259401)

[表3-6 接口升级参数 40](#_Toc392259402)

[表3-7 帐号参数 41](#_Toc392259403)

[表3-8 账号登录参数 43](#_Toc392259404)

[表3-9 抓包任务参数 49](#_Toc392259405)

[表3-10 证书状态参数 51](#_Toc392259406)

[表4-1 接口参数 58](#_Toc392259407)

[表4-2 安全区类型 60](#_Toc392259408)

[表4-3 安全区参数 61](#_Toc392259409)

[表4-4 IP/MAC绑定规则参数说明 63](#_Toc392259410)

[表4-5 静态路由参数 66](#_Toc392259411)

[表4-6 V1和V2c版本Agent访问控制参数 69](#_Toc392259412)

[表4-7 V3版本Agent访问控制参数 69](#_Toc392259413)

[表4-8 V1和V2c版本Trap参数 71](#_Toc392259414)

[表4-9 V3版本Trap参数 71](#_Toc392259415)

[表4-10 SNMP系统配置参数 73](#_Toc392259416)

[表4-11 高可用性基本参数 74](#_Toc392259417)

[表4-12 HA直通参数 76](#_Toc392259418)

[表4-13 非对称路由支持参数 79](#_Toc392259419)

[表4-14 外置bypass参数说明 81](#_Toc392259420)

[表5-1 内置规则模板 83](#_Toc392259421)

[表5-2 派生规则模板参数 85](#_Toc392259422)

[表5-3 用户规则模板参数 86](#_Toc392259423)

[表5-4 自定义IP规则参数 88](#_Toc392259424)

[表5-5 自定义UDP规则参数 89](#_Toc392259425)

[表5-6 自定义ICMP规则参数 90](#_Toc392259426)

[表5-7 自定义高级规则基本参数 92](#_Toc392259427)

[表5-8 协议字段的配置总结 94](#_Toc392259428)

[表5-9 高级选项参数 98](#_Toc392259429)

[表5-10 网络对象参数 99](#_Toc392259430)

[表5-11 节点对象参数 100](#_Toc392259431)

[表5-12 MAC地址参数 102](#_Toc392259432)

[表5-13 IP池参数 104](#_Toc392259433)

[表5-14 网络组参数 105](#_Toc392259434)

[表5-15 自定义服务对象参数 108](#_Toc392259435)

[表5-16 服务组对象参数 110](#_Toc392259436)

[表5-17 服务超时时间参数 111](#_Toc392259437)

[表5-18 系统应用查询参数 113](#_Toc392259438)

[表5-19 自定义应用对象参数 114](#_Toc392259439)

[表5-20 标签及其对应危险程度 115](#_Toc392259440)

[表5-21 过滤器参数 118](#_Toc392259441)

[表5-22 自定义时间对象参数 120](#_Toc392259442)

[表5-23 时间组对象参数 121](#_Toc392259443)

[表5-24 敏感数据对象参数 123](#_Toc392259444)

[表5-25 流量通道对象参数 124](#_Toc392259445)

[表6-1 入侵防护策略参数 130](#_Toc392259446)

[表6-2 Flood防护策略参数 132](#_Toc392259447)

[表6-3 敏感数据保护策略参数 136](#_Toc392259448)

[表6-4 文件识别策略参数 138](#_Toc392259449)

[表6-5 服务器异常防护策略参数 140](#_Toc392259450)

[表6-6 服务器外联参数 141](#_Toc392259451)

[表6-7 服务器学习参数 142](#_Toc392259452)

[表6-8 信誉值描述信息 144](#_Toc392259453)

[表6-9 URL过滤策略参数 147](#_Toc392259454)

[表6-10 自定义URL分类参数 149](#_Toc392259455)

[表6-11 防病毒策略参数 151](#_Toc392259456)

[表6-12 服务器参数 156](#_Toc392259457)

[表6-13 用户认证参数 158](#_Toc392259458)

[表6-14 认证策略参数 160](#_Toc392259459)

[表6-15 应用管理策略参数 162](#_Toc392259460)

[表6-16 流量通道线路参数 164](#_Toc392259461)

[表6-17 流量管理规则主要参数 165](#_Toc392259462)

[表7-1 各类事件统计信息 176](#_Toc392259463)

前言

概述

本文将覆盖绿盟网络入侵防护系统（NSFOCUS Network Intrusion Prevention System，以下简称NIPS）的Web管理界面和串口管理界面的所有功能点，并详细介绍其使用方法。

本手册仅作为使用指导，实际产品可能会由于版本升级或其他原因，与手册描述有略微差异。

读者对象

期望了解本产品主要技术特性和使用方法的管理员、系统管理员、网络管理员等。本文假设您对下面的知识有一定的了解：

* Linux和Windows操作系统
* TCP/IP协议
* 网络安全相关知识

内容简介

| 章节 | 概述 |
| --- | --- |
| 1 产品概述 | 介绍NIPS的产品特点、主要功能以及管理方式。 |
| 2 首页 | 介绍NIPS设备的Web首页的基本信息。 |
| 3 系统维护 | 介绍NIPS系统维护的常用操作内容和方法。 |
| 4 网络配置 | 介绍NIPS系统的网络连接相关的配置。 |
| 5 对象 | 介绍NIPS系统对象的详细配置方法。 |
| 6 策略配置 | 介绍NIPS系统策略的详细配置方法。 |
| 7 日志报表 | 介绍NIPS系统各类日志、报表的查看方法和内容。 |
| 8 Console管理 | 介绍NIPS串口界面的登录和管理内容。 |
| A 缩略语 | 介绍本文出现的缩略语。 |
| B 管理AD域配置器 | 介绍如何安装和配置AD域配置器。 |
| C 出厂参数 | 介绍NIPS的出厂默认配置。 |

格式约定

| 符号 | 说明 |
| --- | --- |
| 粗体字 | 菜单、命令和关键字 |
| 斜体字 | 文档名、变量 |
| 说明 | 对描述内容的补充和引用信息 |
| 提示 | 使用设备时的技巧和建议 |
| 注意 | 需要特别注意的事项和重要信息 |
| 警告 | 有可能造成人身伤害的警告信息 |
| 【XXX】 | 按钮名称的表示方式 |
| A > B | 菜单项选择的表示方式 |

获得帮助

如需获取网络安全相关资料，请访问绿盟科技网站：<http://www.nsfocus.com>。

如需获取更详尽的绿盟科技网络安全专业服务信息、商务信息，您可通过如下方式与我们联系：

客户服务热线：400-818-6868（手机和固话均可拨打）

非工作时间服务热线：13321167330

网站：<http://support.nsfocus.com>

邮箱：[support@nsfocus.com](mailto:support@nsfocus.com)

# 产品概述

近年来，企业所面临的安全问题越来越复杂，安全威胁正在飞速增长，尤其是混合威胁的风险，如蠕虫、病毒、间谍软件、DDoS攻击、垃圾邮件、网络资源滥用（P2P下载、IM即时通讯、网游、视频……）等，极大地困扰着用户，给企业的信息网络造成严重的破坏。

NIPS是绿盟科技独立研发并拥有自主知识产权的新一代安全产品，作为一种在线部署的产品，其设计目标旨在准确监测网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断，而不是在监测到恶意流量的同时或之后才发出告警。这类产品弥补了防火墙、入侵检测等产品的不足，提供动态的、深度的、主动的安全防御，为企业提供了一个全新的入侵防护解决方案。

| 功能 | 描述 |
| --- | --- |
| 产品特点 | 介绍NIPS的显著特点。 |
| 主要功能 | 介绍NIPS的主要功能。 |
| 管理方式 | 介绍NIPS支持的管理方式。 |

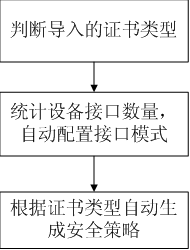
## 产品特点

NIPS相比其他厂商的入侵防御设备最突出的特点是提供开箱即用的零配置上线功能。零配置上线是指NIPS设备预置成熟的默认安全策略模板，并根据导入的证书自动进行接口配置、自动选择适合的安全策略模板，添加一条默认安全策略，并启用防护模式。

一般情况下，IPS设备的配置较为复杂，往往会给从未接触过安全设备的客户带来不小的烦恼。为了屏蔽复杂的配置，降低客户烦恼，增加用户易用性，绿盟科技NIPS内嵌不同的场景模型，实现用户即插即用、零配置上线这一重要功能特点。

绿盟NIPS设备零配置上线功能的基本处理流程如图1-1所示。

零配置处理流程



|  |  |
| --- | --- |
| 说明 | NIPS设备在导入相应证书后自动将相邻两个网络接口配置为一对直通口。 |

一般情况下，零配置上线处理流程完成后，NIPS会生成一条源地址对象、目的地址对象、用户对象、时间对象均为any，规则模板为default，默认启用防护模式的安全策略，如图1-2所示。

零配置上线默认生成的安全策略



零配置上线功能虽然简单实用，但是不能覆盖所有的有特殊配置需要的场景。比如实际网络中需要混合部署，接口岔开部署等。因此，用户可以根据自身需要修改接口配置以及安全策略配置。

在生成零配置功能的时候，设备会对当前配置进行判断，如果发现用户进行了自定义配置或者设备不处于出厂的初始状态，则不会对接口以及安全策略进行自动配置。

## 主要功能

NIPS采用先进的体系架构集成领先的入侵防护技术，并以全面深入的协议分析技术为基础，以协议识别、协议异常检测和关联分析技术为核心的新一代入侵防护引擎，能够协助客户实现以下功能：

* 网络防护

NIPS具有实时的、主动的网络防护功能。此外，NIPS还具有流量管理功能，对于可能出现的异常流量，提供抗拒绝服务攻击功能。

* 应用防护

NIPS提供对应用层的防护功能，针对操作系统、应用软件以及数据库，提供深度的内容检测技术、过滤报文中的恶意流量和攻击行为，保护存在的漏洞，防止操作系统和应用程序损坏或宕机。

* 内容管理

NIPS对企业内部网络资源提供内容管理，可有效检测并阻断间谍软件，包括木马后门、恶意程序和广告软件等，并可对即时通讯、P2P下载、网络游戏、在线视频和网络流媒体等内容进行监控并阻断。

* 防病毒

NIPS可对HTTP、SMTP、POP3、FTP等多种协议类型的近百万种病毒进行查杀，包括木马、蠕虫、宏病毒、脚本病毒等，同时可对多线程并发、深层次压缩文件等进行有效控制和查杀。

## 管理方式

NIPS主要支持以下两种管理方式：

* Web管理

最直观的人机交互管理方式，提供最全面的功能管理界面。NIPS支持IE和Firefox浏览器。

* Console管理

通过控制台以命令行方式对NIPS进行简单配置和管理。

### Web管理

Web管理系统为管理员提供了更直观的人机交互方式，管理员通过Web管理界面实现对NIPS的管理和配置。下面详细介绍Web管理的用户、登录方法、页面布局以及常用操作。

#### Web用户

NIPS在Web管理界面下，有两类用户：

* 操作员

具有对系统的Web界面进行管理、配置的功能，weboper为系统自带的缺省操作员。

* 审计员

具有查看系统日志的功能，webaudit为系统自带的缺省审计员。

NIPS系统中用户的权限各不相同，具体用户的权限如表1-1所示。

用户权限信息

| 用户 | | 权限 |
| --- | --- | --- |
| 操作员 | weboper（缺省） | 具有除管理审计员和查看系统日志外的所有权限。 |
| 新建操作员（读写）  （由weboper创建） | 具有除管理其他用户和查看系统日志外的所有权限。 |
| 新建操作员（读）（由weboper创建） | 只有修改当前用户密码和查看操作员操作界面的权限。 |
| 审计员 | webaudit（缺省） | 只有管理审计员用户和查看系统日志的权限。 |
| 新建审计员  （由webaudit创建） | 只有修改当前用户密码和查看系统日志的权限。 |

#### Web登录

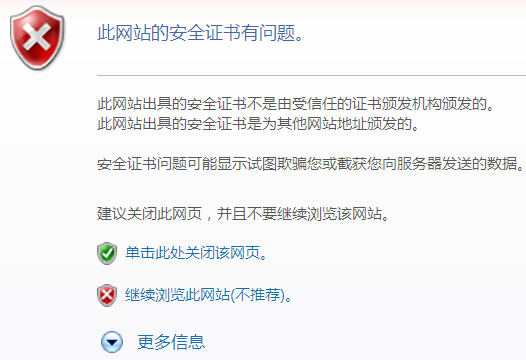
本节以IE浏览器为例，介绍登录NIPS的Web管理系统的详细步骤。

确认客户端主机可以和NIPS正常通讯（如果通过防火墙，请将443端口打开）。

打开IE浏览器，用HTTPS方式连接NIPS的管理IP地址，例如<https://192.168.1.1>。

回车后出现安全警报信息，如图1-3所示。

登录时的安全警报界面



单击“继续浏览此网站（不推荐）”，接受NIPS许可证加密的通道，跳转到NIPS的Web登录页面，如图1-4所示。

Web管理登录界面



输入正确的用户名和密码。

初次登录可使用缺省系统操作员登录，用户名和密码均为weboper。

单击【登录】按钮，进入Web管理页面。

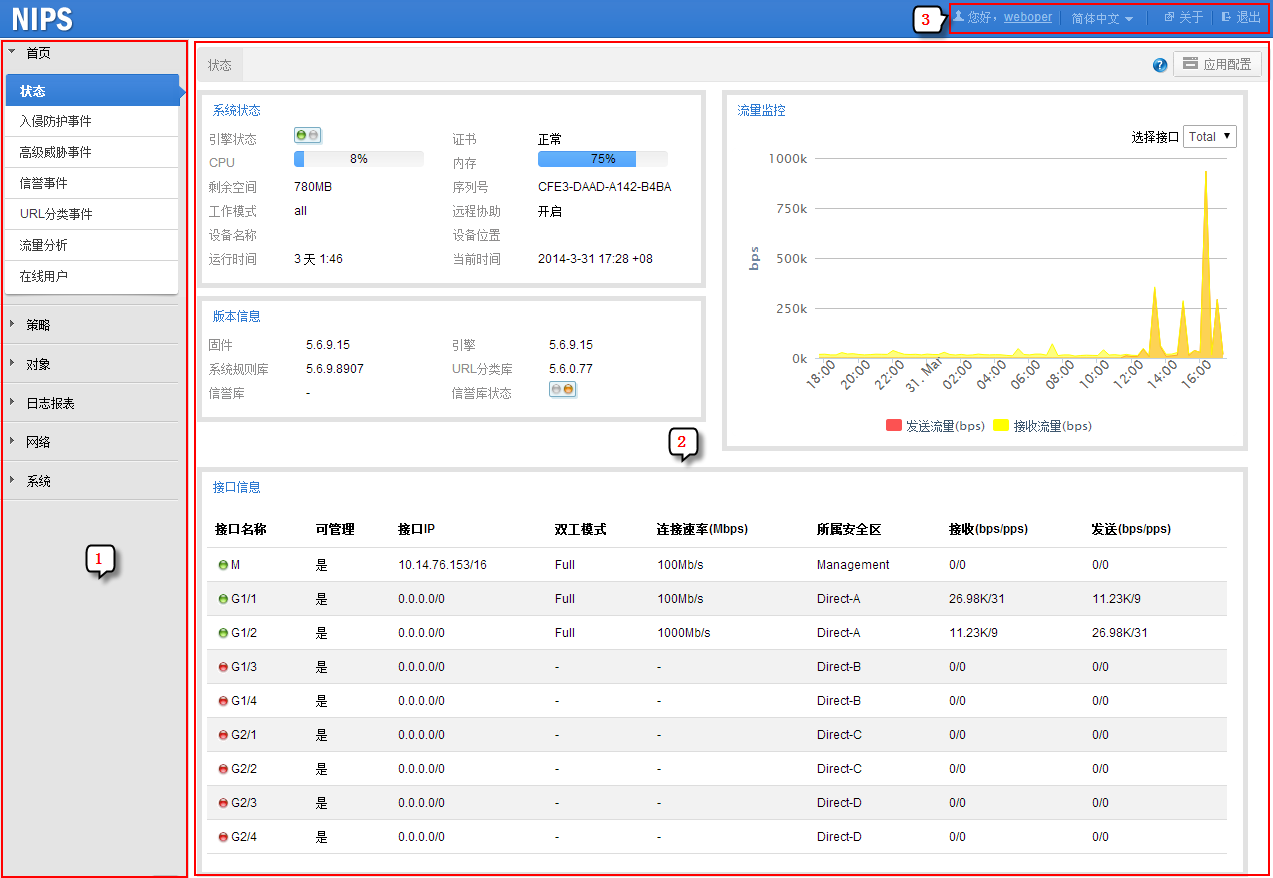
----结束

|  |  |
| --- | --- |
| 说明 | * 登录本系统之前，请检查浏览器是否设置了禁止弹出窗口属性或者禁止javascript；如果是，请撤销此设置。 * 建议使用Firefox最新版本浏览器或IE7.0及以上版本浏览器，屏幕分辨设置为1024\*768或更高。 * 初次使用本系统时可用默认的缺省操作员登录，用户名和密码均是weboper。登录后必须修改用户密码，具体操作方法请参见。 * 管理员登录后，如果不活动的时间超过5分钟，系统将超时并自动退回到登录页面，请重新登录继续使用。 * 登录失败的原因有可能是：①用户名输入错误；②密码输入错误；③未区分大小写；④帐户被禁用或删除。 |

#### Web页面布局

Weboper用户成功登录后，进入系统当前运行的页面，布局如图1-5所示。

Web管理页面布局



Web页面布局说明如表1-2所示。

页面布局

| 编号 | 区域 | 描述 |
| --- | --- | --- |
| 1 | 导航栏 | 系统的功能导航栏。 |
| 2 | 工作区 | 系统各类功能的配置、操作、浏览都在此区域进行。  单击查看NIPS的在线帮助。 |
| 3 | 快捷键操作栏 | 系统设定的几个快捷按键：   * ：修改当前账户密码。 * ：修改Web环境语言。 * ：NIPS的相关信息。 * ：退出Web管理系统。   表格中说明  为确保用户帐号的安全，建议用户单击退出系统。 |

|  |  |
| --- | --- |
| 说明 | 系统页面布局中的菜单和工作区会因用户权限不同，显示的内容有所不同。 |

#### 常用操作

Web管理页面中常见的操作按钮及功能如表1-3所示。

常用操作

| 按钮 | 功能 |
| --- | --- |
| edit | 编辑当前配置信息。 |
| delete | 删除当前配置项。  表格中说明   * 系统预定义的配置项不能删除，如子网对象中的“any”。 * 不能删除被引用的配置项。 |
| apply | 刷新当前页面。 |
|  | 启动某个操作。 |
|  | 停止正在运行的操作。 |
| move | 在列表中上下移动某个策略。 |
| / | 启用/禁用某策略。 |
|  | 复制当前配置项。 |
| 、、 | 将日志、报表以HTML、WORD、EXCEL格式导出到本地主机。 |
|  | 打印日志、报表。 |
|  | 在文本框中输入查找关键字，单击【查找】按钮。 |

|  |  |
| --- | --- |
| 提示 | 将鼠标置于相应操作图标上，将显示操作图标的提示信息。 |

除表1-3中的常用操作按钮外，NIPS还有一个非常重要的应用配置操作。

NIPS中，许多操作配置完成后，需要应用配置才能生效。应用配置有如下两种方式：

* 单击页面右上方的。
* 选择菜单 系统 > 系统控制，单击【应用配置】按钮。

### Console管理

通过Console口连接可以访问NIPS引擎的串口管理界面，在此处提供给管理员一些系统初始配置、状态检测和恢复初始化配置等功能，Web管理界面中无法进行管理的部分，可以在此进行管理操作。下面详细介绍控制台用户以及如何通过控制台登录NIPS的串口管理界面。

#### 控制台用户

conadmin为NIPS系统默认的Console口用户，密码为conadmin。

#### 控制台登录

Console用户登录NIPS之前，需进行以下准备工作：

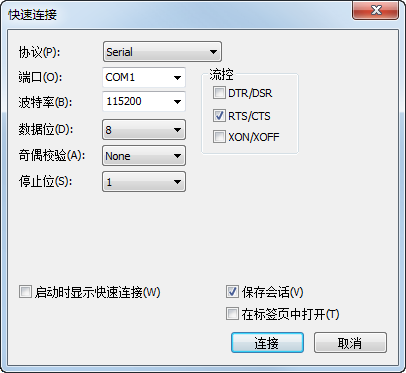
* 工作计算机1台
* 串口线1根（包含在出厂配件中）
* 能够连接串口的终端软件
* 用串口线分别连接NIPS和工作计算机的串口

下面以SecureCRT为例，介绍登录NIPS串口管理界面的详细步骤。

单击SecureCRT.exe，打开SecureCRT工具。

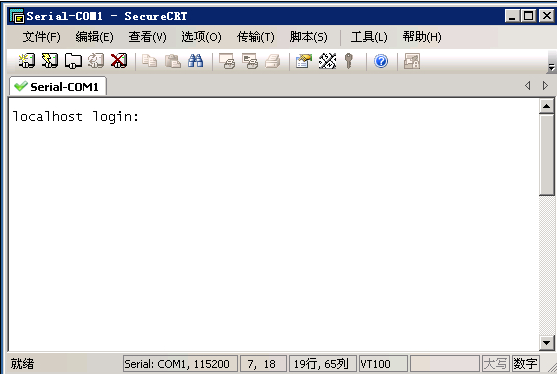
配置快速链接信息，协议配置为Serial，波特率为115200，数据位8，其他参数保持默认，如图1-6所示。

配置快速连接



单击【连接】按钮后按回车键，进入登录界面，如图1-7所示。

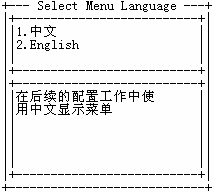
登录界面



输入控制台管理员的用户名和密码（默认控制台管理员用户名和密码均为conadmin）。

用户名和密码正确即可成功登录NIPS，首先进入控制台管理的语言选择界面，如图1-8所示。

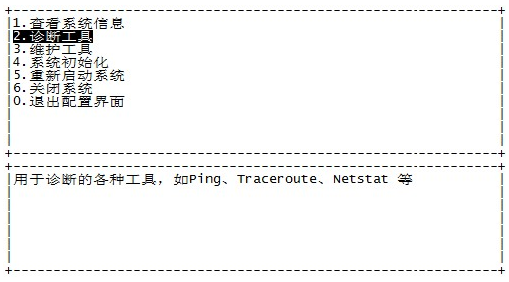
语言选择



|  |  |
| --- | --- |
| 提示 | 连接后将终端类型设为VT100，可以获得最佳显示效果。 |

选择1.中文后按回车键，进入Console管理中文菜单页面，如图1-9所示。

Console管理主菜单



----结束

在串口管理界面中只能用键盘进行操作，键盘操作按键含义如表1-4所示。

Console口按键说明

| 键盘 | 含义 |
| --- | --- |
| ↑ | ①切换到输入框 ②上移 |
| ↓ | ①切换到【确定】 ②下移 |
| ← | ①切换到【确定】 ②左移 |
| → | ①切换到【取消】 ②右移 |
| Esc | 直接取消 |
| Enter | 直接确认 |
| Tab | 在输入框、【确定】、【取消】之间切换 |
| BackSpace | 删除当前光标所在位置的前一字符 |

Console口管理界面中各功能菜单的操作和含义请参见。

# 首页

通过首页可以查看系统的基本状态、各种告警事件、流量分析和在线用户的信息。本章主要内容包括：

| 功能 | 描述 |
| --- | --- |
| 状态 | 介绍如何查看系统状态、流量监控、版本信息和接口信息。 |
| 入侵防护事件 | 介绍如何查看入侵防护事件及基本操作。 |
| 高级威胁事件 | 介绍如何查看高级威胁事件。 |
| 信誉事件 | 介绍如何查看信誉事件。 |
| URL分类事件 | 介绍如何查看URL分类事件。 |
| 防病毒事件 | 介绍如何查看防病毒事件。 |
| 流量分析 | 介绍如何查看流量分析数据。 |
| 在线用户 | 介绍如何查看在线用户信息。 |

|  |  |
| --- | --- |
| 说明 | 系统默认显示最近发生的20条事件信息，支持手动刷新和自动刷新。 |

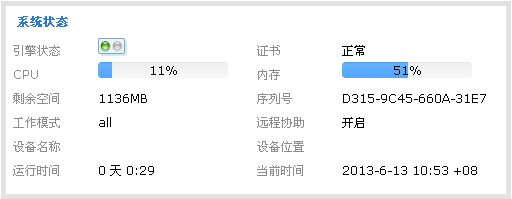
## 状态

登录NIPS后，系统默认进入菜单 首页 > 状态，该页面展示分别展示了系统状态、流量监控、版本信息和接口信息。

* + - * 1. 系统状态

系统状态图中显示NIPS系统的基本信息，如图2-1所示。

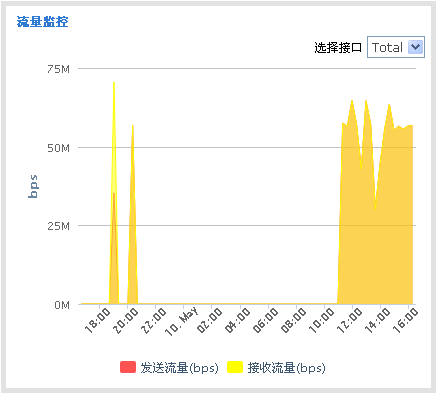
系统状态



* + - * 1. 流量监控

流量监控图中展示最近24小时内NIPS系统监控的发送和接收的总流量数据图，如图2-2所示。

流量监控



系统默认显示所有接口的流量信息，用户可单击右上角的“选择接口”下拉框，选择指定的设备接口，查看该接口在最近24小时内发送和接收的流量数据图。

* + - * 1. 版本信息

版本信息图中展示NIPS系统的固件版本、引擎版本以及加载的各种规则库的版本信息，如图2-3所示。

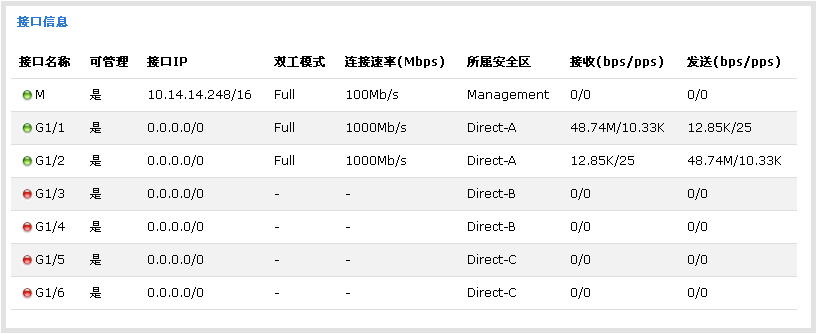
版本信息



* + - * 1. 接口信息

接口信息图中展示接口的基本信息和接收发送流量的速率，如图2-4所示。

接口信息



接口名称包括了当前设备的所有接口，绿色表示接口处于UP状态，红色表示接口处于DOWN状态。不同的设备，接口的数量有所不同。

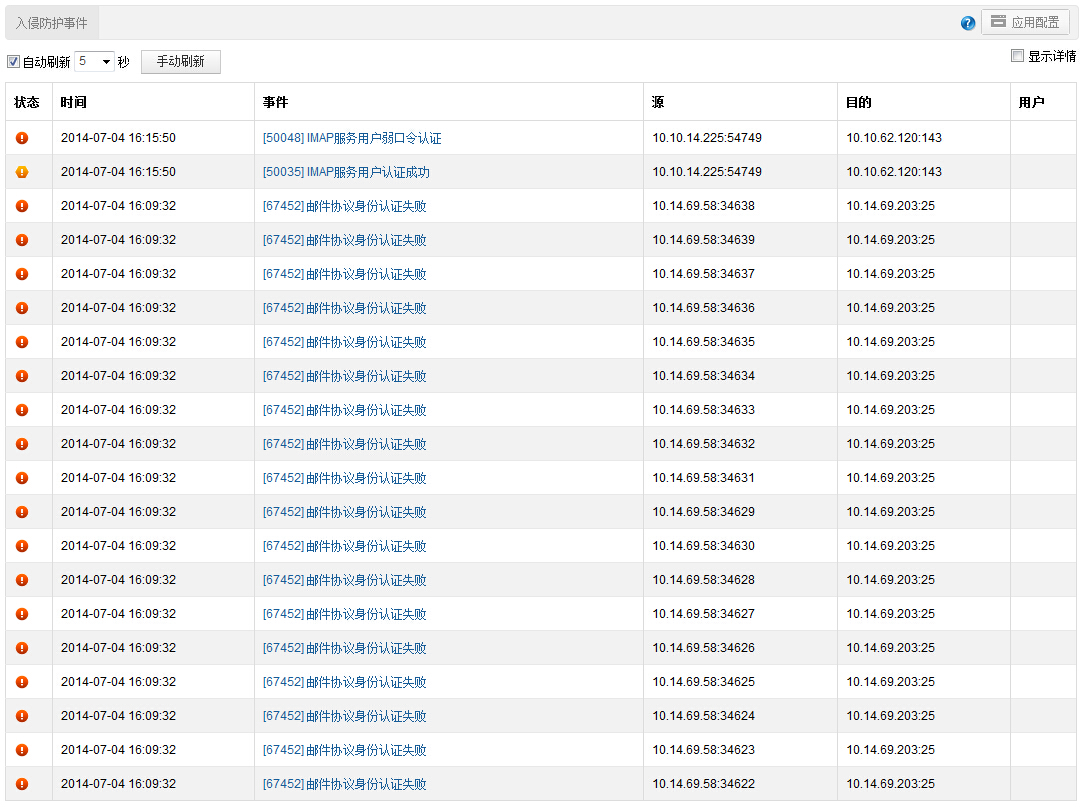
## 入侵防护事件

只有配置了规则模板并在入侵防护策略中引用，入侵防护事件列表中才有数据。有关入侵防护策略的介绍请参见。

NIPS系统中可以实时显示最近发生的20条入侵防护事件的状态、时间、事件内容、源/目的IP及用户，并可以显示事件的详细信息。

选择菜单 首页 > 入侵防护事件，进入入侵防护事件显示页面，如图2-5所示。

入侵防护事件



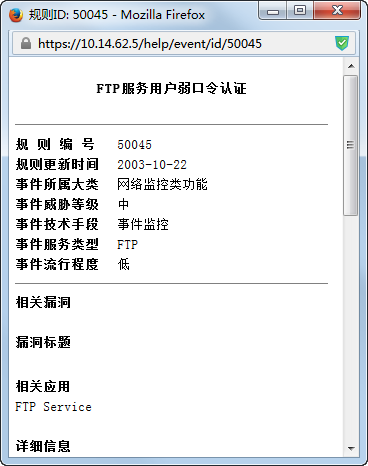
基本操作

* 选中“自动刷新”复选框，然后设置刷新时间后，每隔指定时间，系统将自动刷新入侵防护事件。
* 单击【手动刷新】按钮，可手动刷新当前页面中的入侵防护事件。
* 勾选“显示详情”复选框，可以显示入侵防护事件的详细信息。

查看入侵防护事件详情

单击某个事件名称，可查看该事件的详细分析信息，主要是对事件做出详细分析并提供解决方案，如图2-6所示。

入侵防护事件分析



单击漏洞标题、NSFOCUS ID、BUGTRAQ ID（包括但不限于）等蓝色链接文字，可链接到该漏洞的详细介绍页面。

添加例外

当用户需要对首页中某条规则的实时告警忽略不检测时，可以使用添加例外功能。

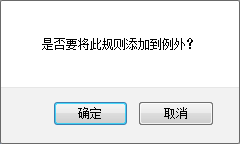
当鼠标指向某一入侵防护事件，入侵事件名称后显示“添加例外”，如图2-7红框所示。

添加例外



单击“添加例外”，弹出确认添加例外对话框，如图2-8所示。

确认添加例外



单击【确定】按钮，确认添加。

添加成功后可在菜单 对象 > 规则 > 例外规则中进行查看和取消例外的操作。

应用配置，使添加生效。

----结束

## 高级威胁事件

NIPS系统中可以实时显示最近发生的20条高级威胁事件的状态、时间、事件内容、源/目的IP及用户，并可以显示事件的详细信息。

选择菜单 首页 > 高级威胁事件，进入高级威胁事件显示页面，如图2-9所示。状态栏中没有任何图标表示放行，若显示图标表示阻断。

高级威胁事件



选中“自动刷新”复选框，然后设置刷新时间后，每隔指定时间，系统将自动刷新高级威胁事件。

单击【手动刷新】按钮，即可手动刷新最近发生的高级威胁事件并显示到当前页面中。

## 信誉事件

NIPS系统中可以实时显示最近发生的20条信誉事件的状态、时间、源/目的IP、事件分类、事件内容和用户信息。

选择菜单 首页 > **信誉**事件，进入信誉事件显示页面，如图2-10所示。状态栏中没有任何图标表示放行，若显示图标表示阻断。

信誉事件



选中“自动刷新”复选框，然后设置刷新时间后，每隔指定时间，系统将自动刷新信誉事件。

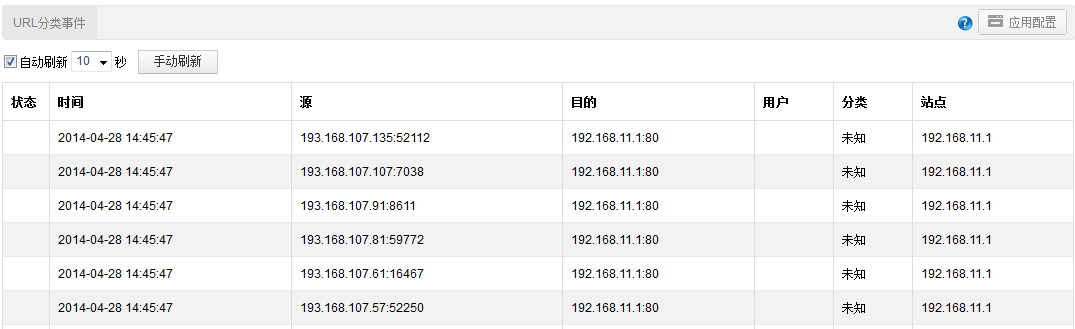
单击【手动刷新】按钮，即可手动刷新最近发生的信誉事件并显示到当前页面中。

## URL分类事件

NIPS系统中可以实时显示最近发生的20条URL分类事件的状态、时间、源/目的IP、用户、URL分类和站点信息。

选择菜单 首页 > **URL分类**事件，进入URL分类事件显示页面，如图2-11所示。状态栏中没有任何图标表示放行，若显示图标表示阻断。

URL分类事件



选中“自动刷新”复选框，然后设置刷新时间后，每隔指定时间，系统将自动刷新URL分类事件。

单击【手动刷新】按钮，即可手动刷新最近发生的URL分类事件并显示到当前页面中。

## 防病毒事件

防病毒事件列表中实时显示最近发生的20条防病毒事件的状态、时间、事件内容、源/目的IP和用户信息。

|  |  |
| --- | --- |
| 说明 | 只有配置了防病毒模板并在安全策略中引用，防病毒事件列表中才有数据。有关防病毒策略的介绍请参见。 |

选择菜单 首页 > 防病毒事件，进入防病毒事件告警列表页面，如图2-12所示。

防病毒事件



选中“自动刷新”复选框，设置刷新时间后，每隔指定时间，系统将自动刷新防病毒事件。

单击【手动刷新】按钮，即可手动刷新当前页面中的防病毒事件。

选中“显示详情”复选框，可以显示防病毒事件的详细信息。

## 流量分析

流量分析模块主要内容包括：流量、应用流量监控和IP流量监控。用户在各页签下都能进行以下通用操作：

* 自动刷新流量分析数据

选中“自动刷新”复选框，然后设置刷新时间后，每隔指定时间，系统将自动刷新流量分析数据。

* 手动刷新流量分析数据

单击【手动刷新】按钮，即可手动刷新当前页面中流量分析数据。

下面分别介绍各类流量统计的详情。

### 流量

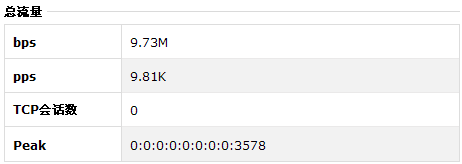
选择菜单 首页 > 流量分析 > 流量，进入查看流量页面，流量信息包括：流经NIPS设备的总流量信息、应用历史记录和应用会话数。

对于应用历史记录和应用会话数，用户还可以选择显示粒度和应用。

* 选择显示粒度：选择小时、天和周分别表示查看最近1小时、最近1天和最近1周的应用历史记录或应用会话数。
* 选择应用：根据应用的分类选择查看指定分类或者全部应用的应用历史记录或应用会话数。
  + - * 1. 总流量

总流量是流经NIPS设备所有接口的流量总和，如图2-13所示。

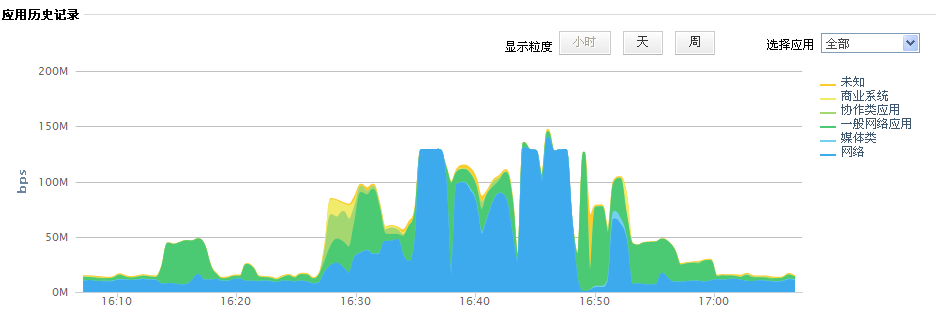
总流量



* + - * 1. 应用历史记录

应用历史记录指应用程序流量统计历史记录，如图2-14所示。

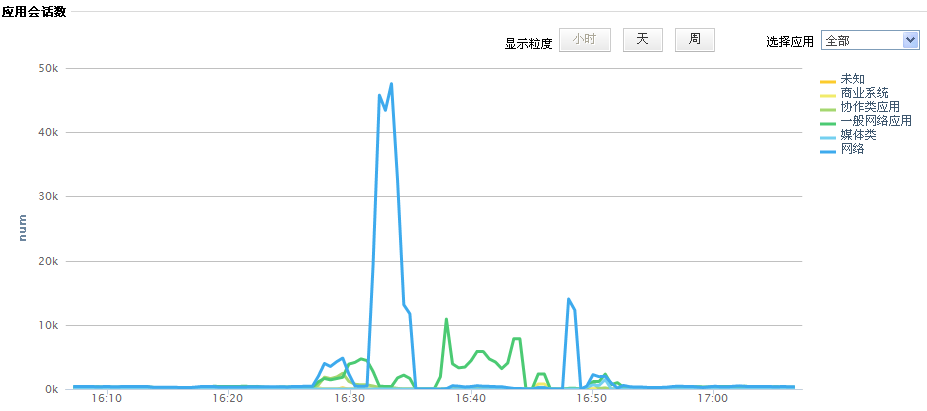
应用历史记录



* + - * 1. 应用会话数

应用会话数指应用会话数历史记录，如图2-15所示。

应用会话数



### 查看应用流量监控

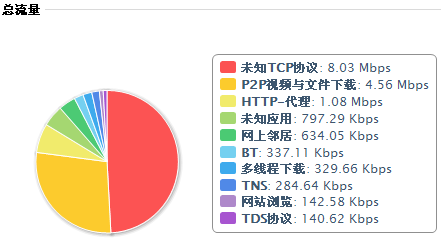
选择菜单 首页 > 流量分析 > 应用流量监控，进入查看应用流量页面，应用流量信息包括：应用协议总流量分布、策略流量上行速率TOP10和策略流量下行速率TOP10。

|  |  |
| --- | --- |
| 说明 | 只有在菜单 系统 > 系统配置 > 专业参数 中启用open\_global\_stream\_analyse参数，才能查看应用流量监控内容。 |

* + - * 1. 总流量

总流量是指各类型应用协议流量所占所有类型应用协议流量总和的比例，如图2-16所示。

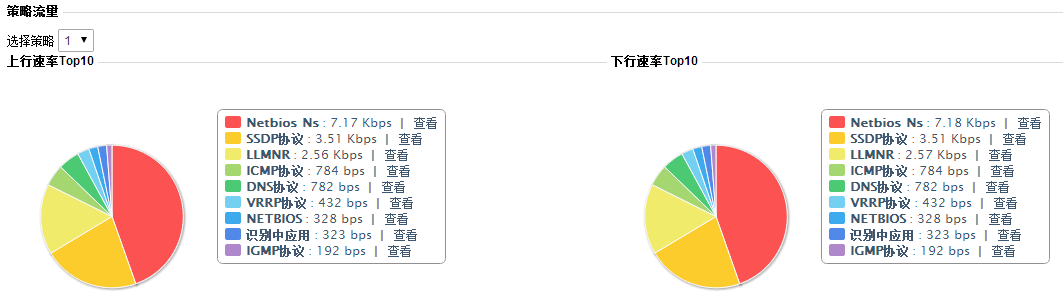
各类应用流量所占总流量比例



* + - * 1. 策略流量

策略流量可以查看某一条流量管理策略对应的各应用协议的上行、下行速率排名，如图2-17所示。

流量管理策略对应上、下行速率



在图2-17所示页面中，单击某类应用右侧的“查看”链接，可以查看该流量管理策略上行、下行速率排名详情，如图2-18所示。

上下行速率排名详情

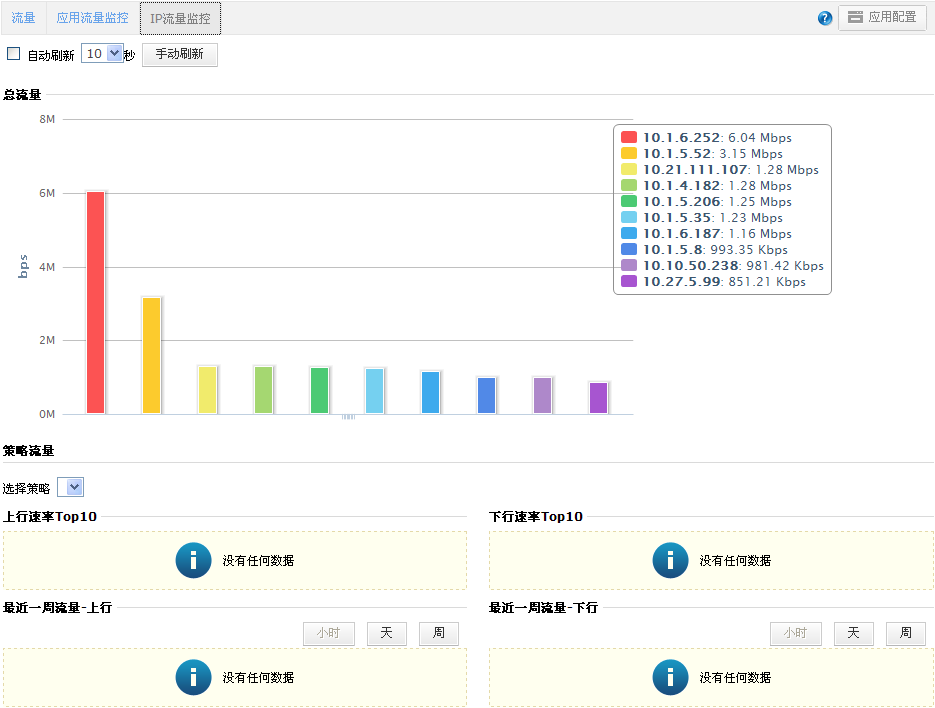


### 查看IP流量监控

选择菜单 首页 > 流量分析 > IP流量监控，进入查看IP总流量、各流量管理策略的上/下行IP速率Top10和最近一周流量-上/下行的页面，如图2-19所示。

|  |  |
| --- | --- |
| 说明 | 只有在菜单 系统 > 系统配置 > 专业参数 中启用open\_global\_stream\_analyse参数，才能查看IP流量监控内容。 |

IP流量监控



## 在线用户

NIPS系统中可以实时显示当前在线的用户，包括登录IP和登录用户名称。在线用户包括通过AD域服务器上报给NIPS的用户和通过Web重定向的方式认证上网的用户。

选择菜单 首页 > 在线用户，进入在线用户显示页面，如图2-20所示。

查看在线用户



选中“自动刷新”复选框，然后设置刷新时间后，每隔指定时间，系统将自动刷新在线用户信息。

单击【手动刷新】按钮，即可手动刷新当前页面中的在线用户信息。

# 系统维护

本章介绍了系统维护的常用操作内容和方法，具体内容如下：

| 功能 | 描述 |
| --- | --- |
| 系统升级 | 介绍在线和离线状态下进行系统升级的方法。 |
| 备份恢复 | 介绍如何备份及恢复参数文件、规则文件、配置文件等。 |
| 系统配置 | 介绍系统引擎及专业参数的配置方法。 |
| 安全中心 | 介绍与安全中心连接的方法。 |
| 帐号管理 | 介绍系统管理员帐号的管理方法。 |
| 诊断工具 | 介绍系统内置的各种诊断工具及其使用方法。 |
| 证书管理 | 介绍系统许可证的导入和查看方法。 |
| 系统控制 | 介绍系统重启引擎、重启系统等操作。 |
| 其他配置 | 介绍配置SQL注入白名单的方法。 |

## 系统升级

系统升级除可升级引擎外，还可以升级系统规则库（包含入侵防护特征库、应用特征库和高级威胁防御库）、病毒特征库以及URL分类库。下面介绍查看系统当前更新状态、在线升级以及离线升级的方法。

### 查看系统更新状态

选择菜单 系统 > 系统升级 > 更新，可查看系统引擎、系统规则库、病毒特征库和URL分类库的当前版本，如图3-1所示。

查看系统当前版本



* 升级设备的操作如下：

在线升级状态下，当系统检测到更新时，自动弹出提示框提示用户进行更新。

单击【点击更新】，进入图3-1所示页面。

单击操作列的图标update，开始升级设备。

系统只记录最新的一个版本号，单击版本号对应操作列的update升级设备。

* 保存升级包的操作如下：

单击图标save，保存当前升级包至本地。

### 在线升级配置

若NIPS设备可访问互联网，用户可以通过在线升级方式升级NIPS设备。系统提供两种在线升级的方式：定时升级和立即升级，本节将对其进行详细介绍。

|  |  |
| --- | --- |
| 说明 | * 无论自动升级还是立即升级，前提条件是NIPS可访问互联网。管理员需要在DNS客户端中配置适当的DNS服务器地址，以便能连接到绿盟科技的官方网站进行升级，具体配置请参见。 * 同时注意接口配置中不要包含DNS服务器地址，否则会有地址冲突导致升级不成功。 |

#### 定时升级

当启用定时升级后，系统自动检测新的升级包，当检测到新升级包后会在管理员设定的升级时间自动升级系统引擎和所有规则库文件，无需管理员手动干预。

配置定时升级的操作如下：

选择菜单 系统 > 系统升级 > 在线升级，进入在线升级配置页面，如图3-2所示。

在线升级



配置升级地址与升级参数，参数信息如表3-1所示。

升级参数

| 配置项 | 描述 |
| --- | --- |
| 升级地址 | 系统升级包的网络地址，一般情况下指绿盟科技的官方网站。升级地址的格式为不以http://开头的url地址，默认升级地址为：update.nsfocus.com。 |
| 自动升级（推荐） | 系统自动检测更新并在设定的时间安装升级包。 |
| 升级时间 | 系统自动安装升级包的时间。   * 当自动升级开启后，可选每天、周一、周二、周三、周四、周五、周六、和周日的任一整点时间升级。 * 建议操作员选择夜间网络使用率低的时候升级系统。 |
| 升级包含引擎 | 升级时是否包含引擎升级。   * 是：开启引擎的升级。 * 否：不升级引擎。   表格中说明  引擎在升级过程中会自动重启，可能引起短暂的业务中断。 |

单击【应用】按钮，保存配置。

应用配置，使配置生效。

----结束

#### 立即升级

当需要即时升级设备时，可采用立即升级的方式。

立即升级的操作如下：

选择菜单 系统 **>** 系统升级 **>** 在线升级，进入在线升级配置页面，如图3-2所示。

配置升级地址与升级参数。参数信息如表3-1所示。

单击【立即升级】按钮，立即升级设备。

----结束

### 离线升级配置

如果NIPS不能访问绿盟科技的官方网站，用户可以通过导入升级文件对设备进行升级。

离线升级的操作如下：

选择菜单 系统 > 系统升级 > 离线升级，进入离线升级页面，如图3-3所示。

离线升级



选择升级文件类型。升级文件类型如表3-2所示。

升级文件类型

| 配置项 | 描述 |
| --- | --- |
| 系统升级文件（\*.bin） | 导入后，系统根据升级包内容自行判断是否需要自动重启引擎。 |
| 系统规则库（\*.rule） | 系统规则库中包含入侵防护特征库、应用特征库、高级威胁防御库、帮助文件以及描述文件。  导入后引擎会自动加载生效。 |
| 病毒特征库升级文件（\*.av） | 导入后，系统根据升级包内容自行判断是否需要自动重启引擎。 |
| URL分类库（\*.urlibx） | 导入后，引擎会自动加载生效。 |

单击【浏览】按钮，导入升级文件。

单击【上传】按钮，立即升级设备。

----结束

## 备份恢复

介绍如何备份、恢复参数文件、规则文件、配置文件、文档等以及如何使用系统还原功能。

### 备份文件

目前，NIPS中能够备份的文件包括：全部配置文件、引擎参数文件、接口参数文件、自定义规则、本地认证文件、流媒体服务器列表文件、对象配置文件、规则配置文件、入侵防护策略配置文件、Snmp Agent MIB文件、Snmp Trap相关文档、Syslog相关文档、系统运行状态文件以及证书文件。

下面以备份引擎参数文件为例，介绍如何备份各类文件。

选择菜单 系统 > 备份恢复 > 备份，进入系统备份的页面，如图3-4所示。

备份文件



在下拉列表框中选择引擎参数文件。

单击【下载备份】按钮，下载引擎参数文件至本地。

----结束

### 恢复文件

目前，NIPS中能够恢复的备份文件包括：引擎参数文件、接口参数文件、自定义规则、本地认证文件、流媒体服务器列表文件、配置文件。

只有提前备份过的文件才能执行恢复操作。支持在不同的NIPS设备上恢复同一备份文件。

恢复文件的操作如下：

选择菜单 系统 > 备份恢复 > 恢复，进入系统恢复的页面，如图3-5所示。

恢复文件



单击【浏览…】按钮，在弹出的对话框中选择需要恢复的文件。

单击【上传】按钮，完成恢复文件的操作。

----结束

### 系统配置还原

系统配置还原是指按照NIPS设备上创建的还原点，对NIPS系统配置进行还原。NIPS设备支持通过手动和自动两种方式创建还原点。

* 手动创建还原点

在任何时候将NIPS设备当前的系统配置文件进行备份。

* 自动创建还原点

配置自动备份周期和时间，NIPS按照设定时间对全部配置文件进行备份。

为了节约NIPS设备磁盘空间，只保存最近一次创建的手动还原点和自动还原点。

#### 手动还原点

系统配置发生重要变动时，建议即时手动创建还原点。

选择菜单 系统 > 备份恢复 > 系统配置还原，进入系统配置还原页面，手动还原点区域如图3-6所示。

手动还原点



单击【手动创建】按钮，手动创建还原点。

备份需要一定时间，请耐心等待。手动创建还原点成功后，页面将出现或刷新还原点信息。

单击【还原】按钮，将NIPS设备的系统配置恢复到还原点创建时的配置情况。

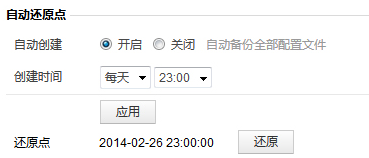
----结束

#### 自动还原点

按照创建周期自动创建还原点需要开启并设置自动创建功能。

选择菜单 系统 > 备份恢复 > 系统配置还原，进入系统配置还原页面，自动还原点区域如图3-7所示。

自动还原点



选择“开启”，开启自动创建还原点功能。

设置还原点创建时间。

自动创建周期可以按天或按周。

单击【应用】按钮，保存自动创建还原点参数。

NIPS设备将按照设置的创建时间自动进行还原点创建，页面将出现或刷新还原点信息。

单击【还原】按钮，将NIPS设备的系统配置恢复到还原点创建时的配置情况。

----结束

## 系统配置

本节主要介绍NIPS设备相关的系统配置，主要包括引擎和专业参数的配置。

### 引擎配置

配置引擎的操作如下：

选择菜单 系统 > 系统配置 > 引擎，进入引擎配置的页面，如图3-8所示。

引擎配置



配置引擎参数。引擎的主要参数含义如表3-3所示。

引擎主要参数

| 配置项 | 描述 |
| --- | --- |
| 远程协助 | 选择开启，可以通过50022端口进行远程管理（仅限绿盟科技的技术人员在网络调试时使用）。 |
| Ping(Icmp) | 是否开启NIPS设备对Icmp请求应答的功能。   * 开启：允许当前NIPS设备对Icmp请求作出应答，方便管理员调试设备故障； * 关闭：当前NIPS设备对Icmp请求不作出应答。 |
| Syslog服务器1 IP地址：端口 | Syslog服务器1的IP地址及其端口。 |
| Syslog服务器2 IP地址：端口 | Syslog服务器2的IP地址及其端口。 |
| 时间设置 | NIPS设备与时间同步服务器进行时间同步的方式。可选项为自动同步和手工设置。时间设置方式设定后，需要重启引擎才能生效。 |
| 时间同步服务器 | 开启自动同步后，需要设置时间同步服务器的IP地址（保证引擎管理口和该时间同步服务器能够正常通讯）。 |
| 同步间隔（秒） | 开启自动同步后，需要设置NIPS设备与时间同步服务器进行自动时间同步的间隔时间，单位：秒。 |
| 时间 | 开启手工设置后，需要设置当前日期和时间。 |
| 时区 | NIPS设备所在的时区。 |
| 设备名称 | 修改NIPS在Web页面的设备名称。 |
| 设备位置 | 对NIPS的位置说明。 |
| 强制硬件bypass | 选择开启，表示设备将被强制进入bypass状态。 |

单击【应用】按钮，保存配置即可。

----结束

### 配置专业参数

选择菜单 系统 > 系统配置 > 专业参数，进入专业参数配置页面。

专业参数为适应特殊网络环境的参数配置，正常情况下无需使用。专业参数的改动有可能造成系统或网络异常，建议用户在绿盟科技的技术人员指导下配置。

## 安全中心

NIPS支持与安全中心连接，安全中心是面向绿盟科技系列产品的集中管理平台，具有多产品的系统集中监控、策略统一配置和报表综合管理等多种功能管理监控，可以极大的提高用户的安全管理工作效率。

### 连接安全中心

选择菜单 系统 > 安全中心，进入NIPS引擎与绿盟科技企业安全中心连接的配置页面，如图3-9所示。

与绿盟科技企业安全中心连接



配置安全中心基本配置参数，参数说明如表3-4所示。

安全中心基本配置参数

| 配置项 | 描述 |
| --- | --- |
| 本地IP地址 | 配置引擎用于和绿盟科技云安全中心以及绿盟科技企业安全中心通讯的IP地址，通常为某个有管理功能的接口IP或管理口IP。 |
| 绿盟科技云安全中心地址 | 配置绿盟科技云安全中心的地址。绿盟科技云安全中心地址为：espp.api.nsfocus.com。 |
| 绿盟科技企业安全中心地址X | 配置与引擎连接的企业安全中心的IP地址，最多支持与4个企业安全中心连接。勾选“启动”后，重启引擎与企业安全中心连接。  表格中说明  若已经启动了引擎与企业安全中心的连接却显示“已断开”，可以将鼠标移动至“已断开”图标上查看断开原因，从而解决断开问题重新建立与企业安全中心的连接。 |

（可选）配置绿盟科技云安全中心以及绿盟科技企业安全中心的高级参数。

单击，显示高级参数配置页面，如图3-10红框所示。

高级选项



配置高级参数。高级选项参数说明如表3-5所示。

安全中心高级选项参数

| 配置项 | 描述 |
| --- | --- |
| 绿盟科技云安全中心 | 配置与引擎连接的绿盟云安全中心的认证方式、认证端口以及是否上传日志。  表格中说明   * 当选择SSL或TCP方式认证时，默认端口已经配置好，如需变更，请查看云安全中心对端口的相关配置，务必使云安全中心与设备的相应端口保持一致。 * 勾选“上传日志”即允许NIPS设备向云安全中心上传日志，由于云安全中心服务器硬盘空间有限，默认不开启上传日志功能。 |
| 绿盟科技企业安全中心X | 配置与引擎连接的绿盟科技企业安全中心X的认证密码、认证方式、认证端口或密码、FTP端口以及FTP密码。  表格中说明   * 认证密码必填，可以是企业安全中心设置的认证密码或者默认认证密码中的任意一个。 * 当选择SSL或TCP方式认证时，默认端口已经配置好，如需变更，请查看企业安全中心对端口的相关配置，务必使企业安全中心与设备的相应端口保持一致。 * 各企业安全中心的FTP端口、FTP密码默认已经配置，设置端口和密码为空则关闭FTP上传相关日志；若因修改造成端口及密码与安全中心配置不一致，将导致设备的应用管理日志、流量分析日志等不能上传至企业安全中心。 * 各企业安全中心的FTP端口、FTP密码必须同时设置，不允许出现设置端口但密码为空，或者设置密码但端口为空的情况。 |
| 替换证书 | NPAI接口的认证证书。 |

高级选项参数配置完成后，单击【确定】按钮保存配置。

|  |  |
| --- | --- |
| 说明 | * 若企业安全中心认证密码输入错误，将导致引擎不能与企业安全中心建立连接，此时需重新输入正确的认证密码或单击【恢复默认配置】按钮来恢复默认认证密码。 * 配置基本参数和高级参数后需要选择菜单 系统 > 系统控制，单击【重启引擎】按钮，使配置生效。 |

----结束

### 配置接口升级

NIPS支持手动升级与安全中心连接的NPAI接口，通过手动上传NPAI接口升级包实现。

升级NPAI接口的具体操作如下：

选择菜单 系统 > 安全中心 > 安全中心，进入安全中心配置页面，如图3-9所示。

配置“其他配置”参数。参数的详细信息如表3-6所示。

接口升级参数

| 配置项 | 描述 |
| --- | --- |
| 接口版本 | NPAI接口的版本信息。 |
| 接口升级时间 | NPAI接口的升级时间信息。 |
| 自动升级 | 是否启用NPAI接口升级功能。 |
| 接口升级 | 1. 单击【浏览】按钮，选择NPAI接口升级文件。 2. 单击【升级】按钮，进行升级。 |
| 调试信息 | NIPS通过NPAI接口与设备联动的状态信息。  单击【一键获取】按钮，可将调试信息保存到本地。 |

----结束

## 帐号管理

在帐号管理界面下，可以管理登录设备的帐号，并对登录过程中的参数进行配置。

### 账号管理

系统自带两个默认的帐户：缺省操作员weboper和缺省审计员webaudit，他们各自可以新建操作员和审计员，具体权限如表1-1所示。

* 以系统缺省的操作员weboper帐号登录设备时，帐号列表中只显示操作员帐号信息。在此可以进行操作员帐号的添加、修改和删除等操作。
* 以系统缺省的审计员webaudit帐号登录时，帐号列表中只显示审计员帐号信息。在此可以进行审计员帐号的添加、修改和删除等操作。

#### 添加用户帐号

只有缺省操作员和缺省审计员才有新建帐号的权限。以缺省操作员weboper登录设备为例，介绍如何新建帐号。

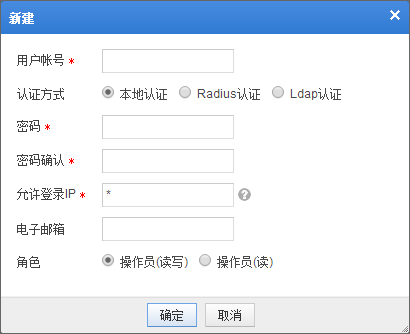
选择菜单 系统 > 帐号管理 > 帐号管理，即可进入帐号管理页面，如图3-11所示。

帐号管理



单击【新建】按钮，进入新建帐号页面，如图3-12所示。

新建帐号



配置帐号参数，参数说明如表3-7所示。

帐号参数

| 配置项 | 描述 |
| --- | --- |
| 用户帐号 | 登录ID，长度必须大于6小于等于20个字符，用户名必须以字母开头，后跟字母、数字、连接符或下划线。创建成功后的用户名称，不能修改。 |
| 认证方式 | 登录设备的认证方式，包括：本地认证、Radius认证和Ldap认证。   * 本地认证：保持默认设置。 * Radius认证：需要配置Radius认证服务器、端口、认证方式和认证共享密钥，具体请参见。 * Ldap认证：要配置Ldap认证服务器，具体请参见。 |
| 密码 | 登录密码，不能和用户帐号相同，长度和密码复杂度应满足中的设置。 |
| 密码确认 | 再输入一次登录密码。 |
| 允许登录IP | 允许管理员登录系统的IP地址。可以输入单个IP地址、网段以及多个独立IP地址。  缺省值：\*（允许管理员通过任意IP地址登录系统）。 |
| 电子邮箱 | 管理员有效的电子邮件地址。 |
| 角色 | 各帐号角色拥有的权限不同，请选择该帐号隶属于哪个角色。 |

单击【确定】按钮保存配置。

|  |  |
| --- | --- |
| 说明 | 默认情况下，所有新建帐号均处于启用状态。只有处于启用状态的帐号才能生效。 |

----结束

#### 修改用户帐号

以缺省系统帐号weboper和webaudit登录设备，单击中操作列的图标，即可修改对应的帐号信息。

* 缺省系统帐号可以修改其他帐号信息，但不能修改帐号的名称。
* 新建的操作员和审计员可以修改自己的帐号信息，但不能修改帐号的名称。
* 如果忘记修改后的缺省系统帐号密码，可以通过引擎串口管理界面重置密码，具体请参见。
* 用户可以通过Web界面的快捷方式修改当前用户信息，具体请参见。

#### 删除用户帐号

只有缺省操作员weboper和缺省审计员webaudit拥有删除帐号的权限，只能删除各自创建的帐号，不允许删除系统缺省帐号。

### 参数配置

“参数配置”页面中主要用于配置帐号登录相关参数和第三方认证服务器的登录参数。配置步骤如下：

选择菜单 系统 > 帐号管理 > 参数配置，进入用户帐号参数配置页面，如图3-13所示。

帐号管理的参数配置



配置账号登录参数，参数说明如表3-8所示。

账号登录参数

| 配置项 | 描述 |
| --- | --- |
| 登录验证失败次数 | 用户连续错误登录的次数。  默认为3次；最多只能设置3次。 |
| 登录验证失败锁定时间（分钟） | 用户在规定的登录尝试次数内没有成功登录设备后，需要等待一段时间才能重新登录设备。默认为3分钟。 |
| 登录多次失败后的处理方式 | 选择是否封锁超过登录尝试次数的用户帐号。  选中“锁定用户”复选框后，即使用户改变IP地址重新登录，也能被系统封锁。  表格中说明   * 系统默认开启了封IP的功能，直到超过设定的“登录验证失败锁定时间”后才能解锁，然后才能重新登录设备。 * 系统封锁用户帐号的同时还将产生审计日志，审计员登录系统后可查看。 |
| 最小密码长度 | 可以设定登录NIPS本地设备用户使用的密码最小长度，默认为10位。 |
| 密码复杂度 | 选择密码包含的字符种类数，密码应该包括数字、大写字母、小写字母、符号中的至少两种（可设置）的组合。  缺省值：2；可选值：2～4。 |
| 操作空闲退出时间（秒） | 当用户空闲操作的时间超过设定值，在该用户需要执行其它操作之前，需要重新进行身份鉴别，默认为5分钟，设置为0表示关闭该功能。  表格中说明  建议设置为10分钟以内。 |
| Ldap认证服务器 | Ldap认证服务器的IP地址。 |
| Radius认证服务器 | Radius认证服务器的IP地址。 |
| Radius认证端口 | Radius认证服务器监听认证请求的服务端口。  Radius协议的认证端口默认为1812。 |
| Radius认证方式 | Radius认证服务器的认证方式。  可选值：pap、spap、chap、mschapv1、mschapv2、eap\_md5。 |
| Radius认证共享密钥 | Radius认证服务器的认证共享密钥。  表格中说明  NIPS中配置的认证共享密钥必须与Radius服务器中的配置一致，否则NIPS和服务器之间无法通信。 |

单击【应用】按钮保存配置。

----结束

## 诊断工具

选择菜单 系统 **>** 诊断工具，即可进入诊断工具页面，查看当前网络的连接状态和网卡状态等信息，例如：发生异常情况时，可通过Ping或Traceroute等工具进行相应的诊断和查看。

### Ping工具

Ping工具用于检测主机存活或与当前网络的连接情况，NIPS的Ping工具同时支持IPv4和IPv6，如图3-14所示。

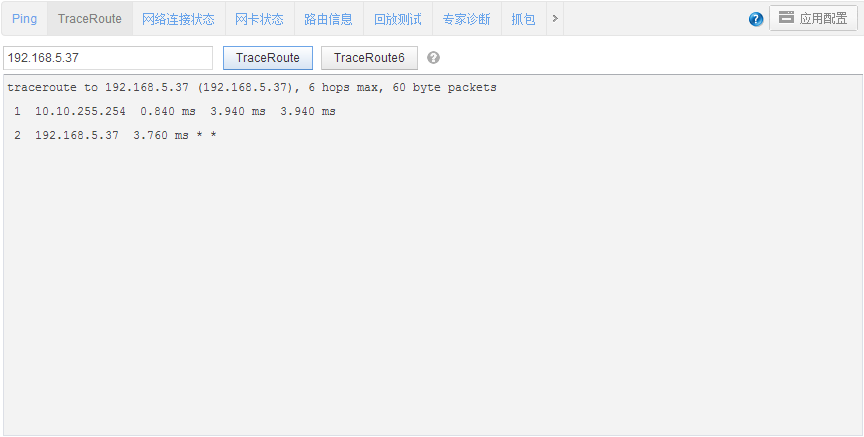
Ping工具诊断结果



### Traceroute工具

Traceroute即路由追踪，用于检测网络路由线路，NIPS的Traceroute工具同时支持IPv4和IPv6，如图3-15所示。

Traceroute工具诊断结果



### 网络连接状态

可以查看系统的网络连接状态和Server状态信息，并支持清空系统中的会话信息。

* 查看系统的网络连接状态，包括使用的协议及端口等，如图3-16所示。

网络连接状态



* 查看Server状态信息，如图3-17所示

Server状态



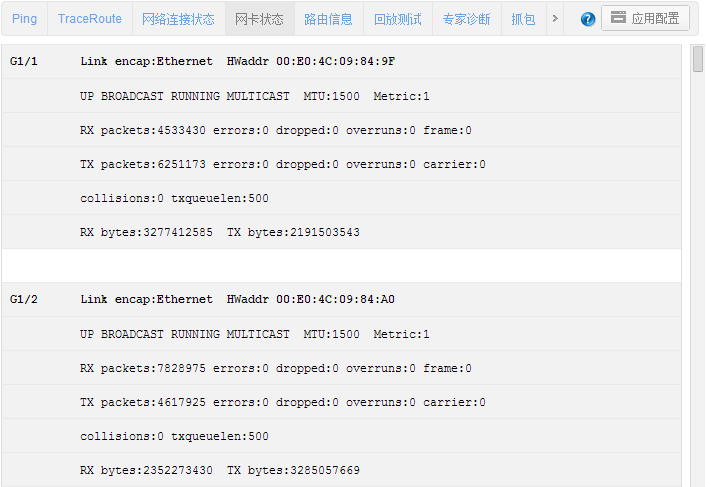
* 单击【清空会话表】按钮，清空所有会话信息并重启引擎。

该操作会导致网络暂时中断，请谨慎操作。

### 网卡状态

通过查看网卡状态信息，帮助用户排查网卡故障，如图3-18所示。

查看网卡状态



### 路由信息

查看当前设备上的实时路由信息，如图3-19所示。

查看路由信息



### 回放测试

NIPS支持通过监听接口读取抓包文件，帮助用户分析网络数据。

回放测试的操作如下：

选择菜单 系统 **>** 诊断工具 **>** 回放测试，进入回放测试页面，如图3-20所示。

回放测试



单击【浏览…】按钮，选择CAP/PCAP文件。

在【回放接口】下拉列表框中，选择回放测试中数据流入的监听接口。

单击【确定】按钮，查看回放数据。

----结束

### 专家诊断

当客户的设备出现故障并需要公司技术人员进行远程协助时，公司技术人员可以通过SSH方式远程登录设备后台进行问题的判断和处理。

设备的后台程序中内置了SSH服务器的地址和端口，SSH服务器部署在公网中。启用专家诊断功能后，绿盟科技技术支持人员可以通过SSH客户端与SSH服务器建立连接，登录映射设备的后台进行故障处理。

* 如果设备能访问公网，可以启动设备上的专家诊断功能。
* 如果设备能够访问SSH服务器，则设备会将自身的SSH口映射到SSH服务器；
* 如果设备不能访问SSH服务器，但是某台与设备路由可达的主机可以访问SSH服务器，则在该主机中运行PortGo.exe并进行相关设置后，即可将设备的SSH口映射到SSH服务器。
* 如果设备不能访问公网，暂时不能提供专家诊断功能。

|  |  |
| --- | --- |
| 说明 | * PortGo.exe由前端工程人员提供并使用，暂时不随机提供给用户。 * 目前，一个技术支持端主机可以同时连接多台映射设备，但是多个技术支持端PC不能同时连接到一台映射设备中。 |

开启专家诊断功能的具体操作如下所示：

选择菜单 系统 > 诊断工具 > 专家诊断，如图3-21所示。

专家诊断



单击【启动】按钮，启动专家诊断功能。

----结束

### 抓包

用户可以从设备接口直接抓包，用于分析、调试网络部署中遇到的问题。抓包任务的操作如下：

选择菜单 系统 > 诊断工具 > 抓包，进入抓包页面，如图3-22所示。

抓包



配置抓包任务参数，参数说明如表3-9所示。

抓包任务参数

| 配置项 | 描述 |
| --- | --- |
| 接口 | 选择一个接口号，表示本次任务是对该接口进行抓包；默认选择any，表示本次任务是对除管理口外的所有接口进行抓包。 |
| 协议 | 可以选择any、IP、TCP、UDP、ICMP、IPv6或ICMPv6，默认选择any，表示本次任务是对所有协议进行抓包。 |
| 对比抓包 | 是否开启抓包对比模式，默认关闭。   * 开启：分别将抓取的收包和发包保存为两个抓包文件，压缩在一个压缩文件中。 * 关闭：抓取收包和发包后，保存为一个抓包文件并压缩。 |
| 源IP/子网掩码 | 本次抓包任务的源IP及其子网掩码，不填写表示不对源IP进行限制。 |
| 源端口 | 本次抓包任务的源端口，0表示任意端口。 |
| 目的IP/子网掩码 | 本次抓包任务的目的IP及其子网掩码，不填写表示不对目标IP进行限制。 |
| 目的端口 | 本次抓包任务的目的端口，0表示任意端口。 |
| 抓包时间（秒） | 本次抓包任务的时间，0表示不限时间。 |
| 包数 | 需要抓包的数量，0表示不限数量。 |
| ruleid | 通过设置规则编号进行抓包。0表示不起作用。 |
| appid | 通过设置应用编号进行抓包。0表示不起作用。 |

单击【应用】按钮，保存配置。

单击【开始】按钮，开始抓包任务。

结束抓包任务。

* 根据抓包时间(秒)，结束抓包任务。
* 抓包过程中，单击【停止】按钮，结束抓包任务。

单击【下载】按钮，将抓包文件下载至本地，并进行分析。

----结束

## 证书管理

NIPS的证书分为以下两类：

* 试用证书

试用证书过期后，将无法继续使用本系统。

* 销售证书

销售证书过期后，可以继续使用本系统，但无法进行系统升级。

### 查看证书状态

通过查看证书状态，用户可以了解NIPS产品支持的功能模块及其限用日期等信息。

选择菜单 系统 > 证书管理 > 证书管理，进入系统证书管理页面，如图3-23所示。

查看证书状态信息



查看证书状态信息。主要参数含义如表3-10所示。

证书状态参数

| 配置项 | 描述 |
| --- | --- |
| 证书状态 | 显示“正常”，表示证书已正确导入，系统状态正确，可以正常使用本系统；显示“过期”，表示证书已超过有效使用期。 |
| 证书类型 | NIPS设备中导入的证书的类型。   * 试用证书过期后，将无法继续使用NIPS。 * 正式证书过期后，可以继续使用NIPS，但无法进行系统升级。 |
| 产品型号 | 证书对应的产品型号。 |
| 序列号 | 证书的序列号。 |
| 功能模块 | 用户已购买的证书中支持的功能模块信息。 |
| 颁发对象 | 有权使用NIPS的用户。 |
| 本期服务起始日期/本期服务终止日期 | 显示证书的有效时间，有效时间从“本期服务起始日期”的0点到“本期服务终止日期”的24点。  表格中说明   * 正式证书的日期指的是产品升级授权服务日期，试用证书为产品的使用日期。 * 正式证书到期后，产品可以正常使用，但不能升级；试用证书到期后，NIPS系统自动跳转到证书导入界面，且不能进行其他任何功能操作。正式证书和试用证书在证书日期内都可以升级，定制产品根据项目要求确定。 * 正式证书终止日期前一个月提醒用户更新证书，并在过期后给出提醒信息；试用证书不予提醒。 |

----结束

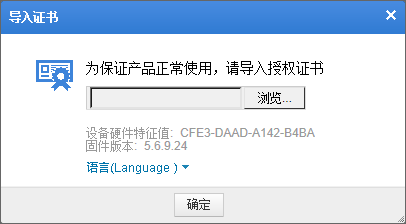
### 导入证书

初次登录系统时，必须导入证书，否则无法使用NIPS设备。导入证书的操作步骤如下：

选择菜单 系统 **>** 证书管理 **>** 证书管理，进入系统证书管理页面，如图3-23所示。

单击【导入证书】按钮，弹出导入证书页面，如图3-24所示。

导入证书



单击【浏览…】按钮，选取证书文件（\*.lic），弹出证书信息确认对话框，如图3-25所示。

导入授权证书确认对话框



确认导入证书。

* 证书状态正确，单击【确定】按钮，完成导入，证书立即生效；
* 证书状态不正确，单击【取消】按钮，重新执行以上步骤。

----结束

## 系统控制

选择菜单 系统 > 系统控制，进入系统控制的操作页面，如图3-26所示。

系统控制



通过单击相应的按钮可以进行以下系统控制的操作：

* 单击【应用配置】

除了接口以外，所有策略和引擎配置将被重新加载生效。这里的策略包括入侵防护策略、高级威胁防御策略、Web信誉策略、URL分类过滤策略、防病毒策略、用户管理策略、流量管理策略、应用管理策略。

* 单击【重启引擎】

重新启动引擎，所有策略和引擎配置将被重新加载生效，包括接口的配置。

* 单击【重启系统】

重新启动NIPS硬件系统。

* 单击【开始调试】

进入网络调试的模式（仅限绿盟科技的技术人员在网络调试时使用）。

* 单击【结束调试】

退出网络调试的模式（仅限绿盟科技的技术人员在网络调试时使用）。

|  |  |
| --- | --- |
| 注意 | 执行重启系统后，所有报表的数据将被清空，重新开始统计。 |

## 其他配置

本节主要介绍NIPS设备实现核心的入侵防护功能相关的SQL注入白名单配置。

当入侵防护规则的事件对象中包含[29001]Web服务远程SQL注入攻击规则时，若是希望该规则对某些服务器不起防护作用，即可设置SQL注入白名单，将这些服务器的URL添加进来。

选择菜单 系统 > 其他配置 > SQL注入白名单，进入SQL注入白名单配置界面，如图3-27所示。

SQL注入白名单



输入不需要进行入侵防护的服务器的URL。

|  |  |
| --- | --- |
| 说明 | * 填写主机名及其域名，用“/”隔开，例如www.google.cn/zh-CN。 * 每行填写一个主机。 |

单击【更新】按钮，保存配置。

单击【重置】按钮，可以恢复到上一次保存的配置。

应用配置，使配置生效。

----结束

# 网络配置

网络配置模块为管理员提供设备的接口、安全区、路由等网络连通信息的配置功能，具体包括以下内容：

| 功能 | 描述 |
| --- | --- |
| 接口 | 介绍NIPS接口的配置方法。 |
|  | 介绍NIPS安全区的配置方法。 |
| DNS配置 | 介绍NIPS域名系统的配置方法。 |
| IPMAC绑定配置 | 介绍IPMAC绑定及配置方法。 |
| 静态路由 | 介绍NIPS静态路由的配置方法。 |
| SNMP | 介绍NIPS作为Agent、Trap消息发送以及SNMP基本功能的配置方法。 |
| 高可用性 | 介绍NIPS高可用性的配置方法。 |
| 外置bypass配置 | 介绍NIPS外置bypass的配置方法。 |

## 接口

接口是设备与设备之间交换数据并相互作用的部分，其功能就是完成设备之间的数据交换。物理接口是真实存在、有相应硬件支持的接口，如NIPS系统支持的M口、H1口、G口（即千兆口，包括G1/1、G1/2等）和T口（即万兆口，包括T1/1、T1/2等）。

通常，NIPS设备默认生产为多路直通设备，即除管理口M外，其余工作口全部成对设置为属于一个直通类型的安全区，例如：G1/1和G1/2同属于安全区Direct – A，G1/3和G1/4同属于安全区Direct – B等。

用户在实际使用中，可以根据需要修改接口的安全区，以下几种情况不允许修改接口所属安全区：

* 非千兆intel网卡的接口不允许修改所属安全区。
* 不能修改管理口M口和H1口的所属安全区。
* 接口存在路由策略时不允许修改所属安全区。
* 证书存在问题时不允许修改所属安全区，例如：未导入证书之前不允许修改任何接口的所属安全区。
* 接口被策略引用时不允许修改所属安全区。

下面介绍如何配置NIPS的接口信息：

选择菜单 网络 > 接口，进入系统接口的列表页面，默认显示当前所有接口的信息，如图4-1所示。

网络接口列表



单击接口列表操作栏的图标，进入接口配置信息页面，如图4-2所示。

配置接口信息



配置接口参数，详细信息如表4-1所示。

接口参数

| 配置项 | | 描述 |
| --- | --- | --- |
| 所属安全区 | | 接口所在的安全区，有关安全区的详细信息请参见。  表格中说明  M口和H1口不能修改所属安全区。 |
| 可管理 | | 接口是否可用于Web管理。   * 是：可通过该接口对设备进行管理； * 否：只能进行数据传送。 |
| IPv4 | 地址 | 接口的IPv4地址。 |
| 网络掩码 | 接口的网络掩码。 |
| 网关 | 接口的网关地址。 |
| 缺省网关 | 接口的网关是否作为系统的默认网关。   * 是：输入的网关IP作为系统的默认网关； * 否：输入的网关IP不作为系统的默认网关。 |
| IPv6 | 配置方式 | 该接口IPv6地址的配置方式。   * 自动获取：该接口通过EUI-64算法自动获取IPV6地址。 * 手动配置：手动配置接口的IPV6地址。   表格中说明  只有当接口所属安全区为Management时，该接口才能支持IPv6协议。 |
| 地址 | 接口的IPV6地址。  表格中说明  只有在手动配置方式下，才允许配置接口的IPv6地址。 |
| 网关 | 接口的IPV6网关地址。 |
| 缺省网关 | 接口的网关是否作为系统的默认网关。   * 是：输入的网关IP作为系统的默认网关； * 否：输入的网关IP不作为系统的默认网关。 |
| 网卡参数 | 双工速率 | 接口的双工模式，有如下三类：   * Auto：与连接网口自动协商接口的双工模式。 * Half：半双工模式，同一时刻只能单向传输数据，或接收数据或发送数据。 * Full：全双工模式，数据传输是双向同步进行的，即同时发送和接收数据。 |
| 连接速率 | 强制接口的协商速率，可选auto、10MB、100MB和1000MB。  请根据与系统连接的网络设备的特性，选择适当的协商速率（默认为自动协商），以保证网络通讯正常。 |
| MTU | 网络最大传输单元，默认为1500。 |

单击【保存】按钮，完成编辑。

应用配置，使配置生效。

----结束

## 安全区

安全区是指拥有相同工作类型的接口的集合。NIPS支持的安全区类型如表4-2所示。

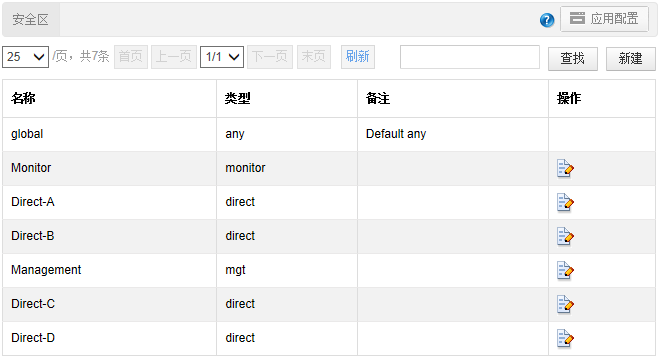
安全区类型

| 类型 | 说明 |
| --- | --- |
| direct | 直通类型安全区，在此类安全区之内的接口处于inline工作模式。 |
| monitor | 监听类型安全区，在此类安全区之内的接口处于监听工作模式。 |
| mgt | 管理类型安全区，在此类安全区之内的接口处于原有工作模式，并可以作为带外管理使用。 |
| interconnect | 互联类型安全区，在此类安全区之内的接口处于互联工作模式。 |
| global | 系统缺省安全区，不可配置，包含所有的安全区。 |

新建安全区的操作如下所示：

选择菜单 网络 > 安全区，进入安全区列表页面，其中，global安全区不能被编辑或删除，如图4-3所示。

网络安全区列表



单击【新建】按钮，弹出新建安全区对话框，如图4-4所示。

新建安全区



配置安全区参数，参数的详细信息如表4-3所示。

安全区参数

| 配置项 | 描述 |
| --- | --- |
| 安全区名称 | 安全区的名称。  安全区名称中不能包含/%\{}`@^<>'&":和空格等非法字符，并且不能与已有安全区名称重复，安全区名称大小写敏感。 |
| 类型 | 安全区的工作类型，目前包括：direct、monitor、mgt和interconnect 4类。 |
| 备注 | 对该安全区的描述信息。 |

单击【确定】按钮，保存安全区内容。

应用配置，使配置生效。

----结束

## DNS配置

DNS服务是互联网上非常重要和基础的服务之一，用来确定主机域名和IP地址之间的对应关系。NIPS作为DNS客户端，可以向指定的DNS服务器请求域名解析服务。

配置DNS客户端的操作如下所示：

选择菜单 网络 > DNS > 客户端，进入配置DNS客户端的页面，如图4-5所示。

新建DNS客户端



配置DNS服务器的IP地址。

单击【应用】按钮，保存配置。

----结束

## IPMAC绑定配置

配置IP地址和MAC地址的绑定，可以防止非法主机冒用合法主机IP地址访问网络的情况，有效避免非法用户进行IP地址欺骗。

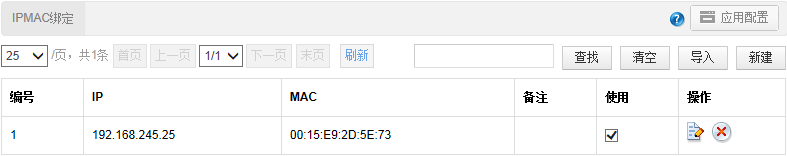
本节主要介绍如何新建、导入IP/MAC绑定规则。

### 新建IP/MAC绑定规则

新建IPMAC绑定规则的操作如下所示：

选择菜单 网络 > IPMAC绑定，进入IPMAC绑定规则的管理页面，如图4-6所示。

IP和MAC绑定规则列表



单击【新建】按钮，弹出新建IP/MAC绑定规则对话框，如图4-7所示。

新建IP/MAC规则



配置绑定规则参数，参数说明如表4-4所示。

IP/MAC绑定规则参数说明

| 配置项 | 描述 |
| --- | --- |
| IP | 待与指定MAC地址绑定的IP地址。  表格中说明  该IP地址既不能与已有IP/MAC规则中的IP地址相同，也不能与NIPS的网关IP相同。 |
| MAC | 待与指定IP地址绑定的MAC地址。  表格中说明  该MAC地址不能与已有IP/MAC规则中的MAC地址相同。 |
| 备注 | IP/MAC规则的描述信息。 |

单击【确定】按钮，保存配置。

----结束

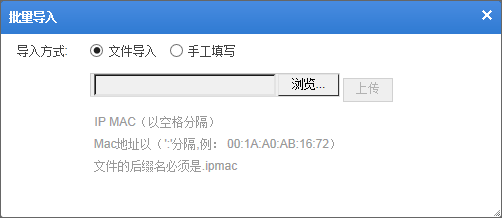
### 导入IP/MAC绑定规则

NIPS提供了IP/MAC规则的批量导入功能，管理员可以通过导入文件的方式批量导入多条IP/MAC规则，也可以通过手工填写的方式一次性添加多条IP/MAC规则，具体操作如下所示：

在图4-6所示页面中，单击【导入】按钮，进入IP/MAC绑定规则的导入页面。

文件导入方式如图4-8所示，手工填写方式如图4-9所示。

导入IP/MAC规则 – 文件导入



导入IP/MAC规则 – 手工填写



添加IP/MAC规则。

|  |  |
| --- | --- |
| 说明 | * 无论是文件导入方式还是手工填写方式，IP/MAC绑定规则的输入格式均为：IP MAC，即：IP地址和MAC地址中间以空格分隔，MAC地址中每两个16进制数之间用冒号分隔。 * 批量添加的IP/MAC规则中的IP地址不能与已有IP/MAC规则中的IP地址重复，也不能与NIPS的网关IP地址重复。 * 批量添加的IP/MAC规则中的MAC地址不能与已有IP/MAC规则中的MAC地址重复。 |

* 文件导入方式下，单击【浏览】按钮，选择待导入的文件（后缀名必须是“.ipmac”），然后单击【上传】按钮即可将该文件中所有的IP/MAC绑定规则批量导入到NIPS中。
* 手工填写方式下，每行输入一条IP/MAC绑定规则，回车换行后可以输入下一条IP/MAC绑定规则。手工填写完成后，单击【确定】按钮保存配置即可将手工填写的IP/MAC绑定规则批量添加到NIPS中。

----结束

## 静态路由

静态路由是管理员手工配置的一类路由，适用于规模较小且不经常变化的网络。由于静态路由不能自动适应网络变化，当网络拓扑结构发生变化时，需要管理员手动修改静态路由信息。

在静态路由中有一类特殊的路由，那就是缺省路由，其的目的IP用0.0.0.0/0表示。当设备在路由表中没有找到与数据包相匹配的路由时，通常将其丢弃，如果配置了缺省路由，则路由设备可以根据缺省路由的配置来转发报文。

目前，NIPS支持IPV4静态路由和IPV6静态路由。IPv6静态路由与IPv4静态路由类似，适合于一些结构比较简单的IPv6网络。它们之间的主要区别是目的地址和下一跳地址有所不同，IPv6静态路由使用的是IPv6地址，而IPv4静态路由使用IPv4地址。

|  |  |
| --- | --- |
| 说明 | * 配置IPv4静态路由时，如果指定的目的地址为0.0.0.0，掩码为0.0.0.0，则表示配置了一条IPv4缺省路由。当IPV4报文的目的地址无法匹配路由表中的任何一项时，设备将选择IPv4缺省路由进行转发。 * 配置IPv6静态路由时，如果指定的目的地址为::/0（前缀长度为0），则表示配置了一条IPv6缺省路由。当IPV6报文的目的地址无法匹配路由表中的任何一项时，设备将选择IPv6缺省路由进行转发。 |

新建静态路由的具体操作如下所示：

选择菜单 网络 > 路由 > 静态路由，进入静态路由页面，如图4-10所示。

静态路由



单击【新建】按钮，弹出新建静态路由对话框，如图4-11所示。

新建静态路由



配置静态路由参数，参数说明如表4-5所示。

静态路由参数

| 配置项 | 描述 |
| --- | --- |
| 静态路由名称 | 静态路由的名称。  不能包含/%\{}`@^<>'&":和空格等非法字符。 |
| 目的IP地址 | 目标主机的IPV4地址及其掩码，或者IPV6地址及其前缀，用于标识IP包的目的地址或目的网络。  表格中说明  当目的IP地址为0.0.0.0/0或者::/0时，配置的为设备的缺省路由，即当查找路由表失败后，根据缺省路由进行包的转发。 |
| 网关地址 | 静态路由的网关地址，通常为下一跳设备的入口IP地址。 |
| 接口 | 静态路由出口的网络接口。 |
| 优先级 | 静态路由的优先级，值越小，优先级越高。当同一目的地存在多条静态路由时，优先级高的路由将成为当前的最优路由。取值范围为1-30。 |

单击【确定】按钮保存配置。

----结束

## SNMP

NIPS设备支持SNMP（Simple Network Management Protocol，简单网络管理协议）管理，NIPS设备可以作为Agent响应SNMP管理主机的查询，向SNMP管理主机返回相应的运行状态信息，同时也可以主动地向SNMP管理主机发送Trap消息。

NIPS设备支持SNMP V3版本，同时兼容V1和V2版本。当使用SNMP V1和V2 对NIPS设备进行网络查询时，只需设置团体名即可，但存在的最大问题是传输的认证和管理数据没有加密、数据的收发缺乏鉴别机制，因此对网络的管理缺乏安全保障。当使用SNMP V3对NIPS设备进行查询时，不仅将传送的信息使用加密算法（支持DES和AES）进行加密，而且还需设置用户的密钥，以便防火墙验证用户身份，因此进一步提高了对防火墙设备进行SNMP管理的安全性。

NIPS设备支持主流的SNMP管理软件，如MIB BROWSER、solarwind。

### Agent访问控制

NIPS设备必须启动SNMP代理服务并配置相关代理访问控制参数后才能支持SNMP管理主机对NIPS设备进行SNMP管理以及进行SNMP报警。启动SNMP Agent的操作请参见，下面主要介绍如何配置Agent访问控制参数。

选择菜单 网络 > SNMP > Agent访问控制，进入SNMP Agent访问控制管理页面，如图4-12所示。

SNMP Agent访问控制



单击【新建】按钮，弹出新建Agent访问控制对话框，V1和V2、V3版本的Agent访问控制对话框分别如图4-13和图4-14所示。

V1和V2c版本Agent访问控制



V3版本Agent访问控制



配置Agent访问控制参数，V1和V2、V3版本的Agent访问控制参数说明分别如表4-6和表4-7所示。

V1和V2c版本Agent访问控制参数

| 配置项 | 描述 |
| --- | --- |
| 团体名 | NIPS设备开启SnmpAgent代理功能后，SNMP管理主机访问NIPS设备时使用的团体名。 |
| 请求来源 | SNMP管理主机的来源IP地址。 |
| MIB子树 | 管理主机对NIPS设备中管理信息库子树的访问权限，访问权限是通过OID（Object identifier，对象标识）实现的控制。  1表示具有所有节点的访问权限，例：1.3.6.1.4.1.19849.2。 |
| 读写权限 | 管理主机对NIPS设备中管理信息库子树的读写权限，可选项：rw（读写）、r（读）。 |

V3版本Agent访问控制参数

| 配置项 | 描述 |
| --- | --- |
| 用户名 | SNMP V3用户的名称。 |
| 认证协议 | 进行认证时使用的认证协议，可选项：MD5和SHA。 |
| 认证用key | 进行认证时使用的密钥。 |
| 加密协议 | 加密传送信息时使用的加密算法，可选项：DES和AES。 |
| 加密用key | 进行信息加密时使用的密钥。 |
| MIB子树 | 管理主机对NIPS设备中管理信息库子树的访问权限，访问权限是通过OID（Object identifier，对象标识）实现的控制。  1表示具有所有节点的访问权限，例：1.3.6.1.4.1.19849.2。 |
| 读写权限 | 管理主机对NIPS设备中管理信息库子树的读写权限，可选项：rw（读写）、r（读）。 |
| 安全等级 | 用户必须满足什么安全等级才能访问，可选项：不认证、需认证、认证且加密。 |

单击【确定】按钮，完成配置。

----结束

### Trap

Trap是一种自陷信息，是指NIPS作为SNMP Agent设备可以在任何时候向SNMP管理主机报告自身情况，而并不需要等到SNMP管理主机为获得这些情况而轮询他的时候才发送。

NIPS设备必须启动SNMP Trap并配置相关参数后才能向SNMP管理主机主动发出情况信息。

启动SNMP Trap的操作请参见，下面主要介绍如何配置SNMP Trap。

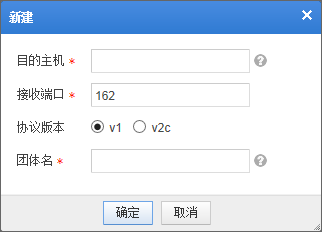
选择菜单 网络 > SNMP > Trap，进入SNMP Trap管理页面，如图4-15所示。

SNMP Trap



单击【新建】按钮，弹出新建Trap对话框，V1和V2、V3版本的Trap对话框分别如图4-16和图4-17所示。

V1和V2版本Trap



V3版本Trap



配置Trap参数，V1和V2、V3版本的Trap参数说明分别如表4-8和表4-9所示。

V1和V2c版本Trap参数

| 配置项 | 描述 |
| --- | --- |
| 目的主机 | 接收NIPS设备发出SNMP Trap报警消息的主机。  支持IPv4或IPv6地址，例：192.168.1.0 或 2001:abcd:123:1::。 |
| 接收端口 | 用于接收SNMP Trap报警消息的端口号。 |
| 协议版本 | 使用的SNMP协议的版本。可选项：V1和V2C。 |
| 团体名 | 接收SNMP Trap报警消息的主机的团体名。 |

V3版本Trap参数

| 配置项 | 描述 |
| --- | --- |
| 目的主机 | 接收NIPS设备发出SNMP Trap报警消息的主机。  支持IPv4或IPv6地址，例：192.168.1.0 或 2001:abcd:123:1::。 |
| 接收端口 | 用于接收SNMP Trap报警消息的端口号。 |
| 用户名 | SNMP V3用户的名称。 |
| 认证协议 | 进行认证时使用的认证协议，可选项：MD5和SHA。 |
| 认证用key | 进行认证时使用的密钥。 |
| 加密协议 | 加密传送信息时使用的加密算法，可选项：DES和AES。 |
| 加密用key | 进行信息加密时使用的密钥。 |
| 安全等级 | 用户必须满足什么安全等级才能访问，可选项：不加密不认证、需认证、认证且加密。 |
| engineID | SNMP引擎的ID号。  ID号为16位的16进制数，例：0x8000000001020304。 |

单击【确定】按钮，完成配置。

----结束

### 系统配置信息

NIPS设备需要进行基本的配置后才能支持SNMP管理，下面介绍如何在NIPS设备上进行设置，从而支持SNMP管理。

选择菜单 网络 > SNMP > 系统配置信息，进入SNMP系统配置信息页面，如图4-18所示。

SNMP系统配置信息



配置参数，参数说明如表4-10所示。

SNMP系统配置参数

| 配置项 | 描述 |
| --- | --- |
| 系统位置 | NIPS设备本身在网络环境中所处的位置。 |
| 联系方式 | NIPS设备直接负责人的联系方式。  可以为电话号码或Email地址，默认显示绿盟科技客服的Email地址。 |
| 系统描述信息 | NIPS设备的介绍信息。 |
| Snmp Trap | 是否开启NIPS设备主动向Snmp主机发送报警消息的功能。开启后中配置生效。 |
| SnmpAgent | 是否开启NIPS设备接受SNMP管理主机管理的功能。开启后中的配置生效。 |

单击【确定】按钮，完成配置。

----结束

## 高可用性

在数据通信过程中，各种软件和硬件错误都可能导致网络连接异常中断，造成数据传输失败。为了避免单点故障引起数据通信中断，有效增强网络可靠性，绿盟网络入侵防护系统提供了高可用性功能。

目前，绿盟网络入侵防护系统的高可用性功能应用于两台设备之间，本节将对其工作原理和功能配置进行详细介绍。

### 基本概念

* 主从模式

主从模式下的两台设备，其中一台作为主机，另一台作为从机。主机处理所有业务，并将产生的会话信息和配置信息发送到从机进行备份；从机不处理业务，只用做备份。当主机故障，从机接替主机处理业务，从而保证新发起的会话能正常建立，当前正在进行的会话也不会中断。

* 抢占模式

抢占模式下，主机宕掉后，链路会切换到从机，主机恢复正常后，将抢占从机流量，此时主机切换到激活状态，而从机切换到非激活状态。

* 非抢占模式

非抢占模式下，主机宕掉后，链路会切换到从机，主机恢复正常后，不会抢占从机流量，从机仍然处于激活状态，主机则处于非激活状态，直到从机宕掉后，主机才会接管流量。

* 非对称路由支持

配置非对称路由支持后，非对称路由支持组中的NIPS设备相互转发数据报文传输信息，以便在传输出去的数据选择其他路由回来时进行数据信息整合，形成完整的数据传输会话，从而在不改变数据传输路径的同时完成数据包的深度检测。

### 基本配置

两台设备之间各通过一个管理口（心跳口）相连，用于设备之间收发心跳信息、同步配置文件和会话信息。

高可用性的基本配置如下：

选择菜单 网络 > 高可用性设置 > 基本配置，进入高可用性基本参数配置页面，如图4-19所示。

高可用性基本参数



配置基本参数，参数说明如表4-11所示。

高可用性基本参数

| 配置项 | 描述 |
| --- | --- |
| 同步配置 | NIPS仅支持手动同步策略、对象的配置。   * 单击【对端 >> 本地】按钮，将对端设备的配置信息同步到本地； * 单击【本地 >> 对端】按钮，将本地的配置信息同步到对端设备。   表格中说明  仅当启用了直通HA后，才能够在两台设备之间同步指定的配置文件。 |
| HA状态 | 心跳口的工作状态。  心跳口有三种状态：未启动、正常、异常。   * 未启动：当HA未启动时，无论心跳接口是否配置、连接是否正常，HA状态均显示为“未启动”。 * 正常：HA运行后，若心跳接口配置正确，且网线连接正确，HA状态显示为“正常”。 * 异常：HA运行后，若心跳网络连接异常（网线没有插好或接口被宕掉），HA状态显示为“异常”。   表格中说明  使用HA功能时，可以根据此状态排查网络问题。 |
| HA配置 | * 心跳接口：本设备的心跳口，该接口必须是管理口或可管理工作口。 * 对端IP地址：对端设备心跳口的IP地址。该接口必须是对端设备的管理口或可管理工作口，并且必须与本设备心跳口在同一网段。 * 会话同步：启动HA后，是否实时同步对端的会话信息。   表格中说明   * 必须配置“心跳接口”和“对端IP地址”，否则HA无法启动。 * 本地和对端设备的“会话同步”配置必须一致。 |

|  |  |
| --- | --- |
| 说明 | 启动HA后，HA的基本配置不可编辑。 |

单击【确定】按钮，保存配置。

----结束

### 直通配置

直通配置即直通HA配置，当设备使用直通安全区时使用该HA方式。NIPS的直通HA仅支持主从模式。

启用直通HA后，主设备处于工作状态，承担报文转发任务，从设备处于备份状态并准备随时接替任务。主、从设备之间周期性的发送心跳信息，通告本地直通口网卡的个数。

在两种情况下可以发生主从切换：

* 主机的任何一个直通口宕掉后，其他直通口将自动宕掉，然后切换到备份状态。此时，从机会在收到的心跳信息中发现主机的直通口网卡个数小于自身的直通口网卡个数，认为对端故障，于是切换到工作状态，进行数据转发。
* 心跳信息丢失：当心跳口宕掉或者心跳模块异常时，本机无法接收到对端设备的心跳信息，就认为对端宕掉，然后本机切换到工作状态（心跳丢失前处于工作状态的设备仍保持工作状态，处于备份状态的设备将切换到工作状态），此时，可能会出现主、从设备均处于工作状态的现象，因此一定要保持心跳口的正常工作。

直通HA的详细配置步骤如下所示：

配置安全区和接口。

在主、备设备中分别选择一对直通口和一个管理口。直通口用于连接两端的交换机、转发数据和故障切换；管理口作为心跳口，用于收发心跳信息、同步配置文件和会话信息。

一般情况下，NIPS设备自动初始化后，相邻接口为一对直通口，且每对直通口默认属于一个安全区，用户只需选择和直通口相应的安全区即可。

若需要配置安全区和接口，请参见和的相关描述，此处不再赘述。

配置HA的公共参数，具体操作请参见。

配置HA直通参数。

选择菜单 网络 > 高可用性设置 > 直通配置，进入配置HA直通参数页面，如图4-20所示。

HA直通参数配置



配置HA直通参数，参数说明如表4-12所示。

HA直通参数

| 配置项 | 描述 |
| --- | --- |
| 工作状态 | 本机的工作状态：运行、停止。   * 运行：成功启动了直通HA后，本机工作状态显示为“运行”。 * 停止：停止直通HA或未启动直通HA时，本机工作状态显示为“停止”。   表格中说明  使用HA功能时，可以根据此状态排查网络问题。 |
| 本机系统状态/对端系统状态 | 本机系统状态包括：激活、非激活、关闭。  对端系统状态包括：激活、非激活、关闭、未知。  表格中说明   * 如果成功启动了直通HA，并且本机处于主模式，同时与备用设备相连的心跳线良好，则本机系统状态显示为“激活”；对端系统状态显示为“非激活”。 * 如果成功启动了直通HA，并且本机处于备用模式，同时与主设备相连的心跳线良好，则本机系统状态显示为“非激活”；对端系统状态显示为“激活”。 * 如果成功启动了直通HA，但是心跳线没有接好或者是心跳口宕了，则本机系统状态显示为“激活”，对端系统状态显示为“未知”。 * 如果设备没有启动直通HA，则本机系统状态和对端系统状态均显示为“关闭”。 |
| 工作模式 | 本机的工作模式：主机、从机。   * 主机：指本机工作在主机模式，并在启动直通HA后承担报文转发任务，直到发生故障切换。 * 从机：指本机工作在从机模式，并在启动直通HA后处于备份状态，不转发数据，直到发生故障切换。   表格中说明  目前，绿盟网络入侵防护系统的直通HA仅支持主从模式，即配置的两台设备，一台是主机，一台是备机。 |
| 抢占模式 | 是否开启“抢占”模式，即主机宕机后，当恢复正常工作时，是否夺回主机的地位，重新转发数据。  表格中说明  主机、从机的“抢占模式”设置必须一致，同时开启或同时关闭。 |
| 心跳时间间隔（毫秒） | 指向对端发送心跳信息的时间间隔。缺省值：1000毫秒；取值范围：大于等于1000毫秒。  表格中说明  主机、从机的“心跳时间间隔”参数值必须一致。 |
| 失去心跳次数 | 当本机未接到对端心跳信息的次数超过这个值时，本机就认为对端设备宕掉了。此时，如果本机正处于主机状态，则还保持主机状态不变，同时将“对端设备状态”显示为“未知”；如果本机正处于从机状态，则切换到主机状态进行报文转发，同时将“本机系统状态”显示为“激活”，而将“对端系统状态”显示为“未知”。  缺省值：3次。  表格中说明  主机、从机的“失去心跳次数”参数值必须一致。 |

|  |  |
| --- | --- |
| 说明 | 启动直通HA后，直通配置和基本配置中的“HA配置”不可编辑。 |

单击【确定】按钮使配置生效。

启用直通HA功能。

单击控制区域的【启动】按钮，弹出重启引擎的确认信息。

单击【确定】按钮后，系统将自动重启引擎启用直通HA。

----结束

### 非对称路由支持

两台直通部署的NIPS设备可配置非对称路由支持功能。下面介绍新建非对称路由支持的详细步骤。

配置非对称路由。

选择菜单 网络 > 高可用性设置 > 非对称路由支持，进入非对称路由支持列表页面，如图4-21所示。

非对称路由支持列表

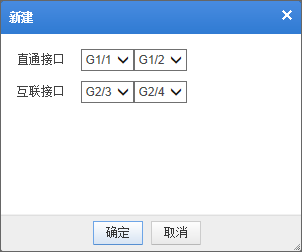


单击【启动】按钮，启动非对称路由支持功能。

|  |  |
| --- | --- |
| 注意 | 当没有可启用的策略时，非对称路由支持功能不生效。 |

单击【新建】按钮，弹出新建非对称路由支持对话框，如图4-22所示。

新建非对称路由支持



配置非对称路由支持参数，参数说明如表4-13所示。

非对称路由支持参数

| 配置项 | 描述 |
| --- | --- |
| 直通接口 | NIPS设备非对称路由支持时使用的直通接口。 |
| 互联接口 | NIPS设备和非对称路由支持组中其他NIPS设备的互联接口。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

## 外置bypass配置

通常，NIPS设备部署于网络的重要位置，为内网安全提供综合防护功能，一旦失效，将导致网络中断等严重问题。

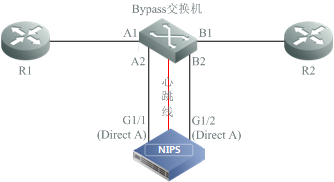
为了避免NIPS设备因网关失效（如断电或死机等）而成为单点故障，可以将其与外置bypass交换机进行联动，以便使光路绕过故障的网关或链路，实现光路直通。

NIPS设备断电或心跳口宕掉后，与之关联的bypass交换机自动切换到bypass方式，并将网络流量绕开NIPS设备，然后将其旁路到下一跳设备中，以保障网络畅通；NIPS设备恢复正常工作后，bypass交换机自动切换到normal方式，网络流量重新流经NIPS设备，然后被其接收、处理并转发。

|  |  |
| --- | --- |
| 注意 | * 只有在设备断电或者心跳口宕掉的情况下，Bypass交换机才会切换到bypass方式，并使光路直通。工作口宕掉时，并不会切换到Bypass方式。 * 设备恢复正常后，Bypass交换机会自动切换为normal方式。 * 设备中的一个direct口宕掉时，另外一个direct口并不会宕掉。 |

以图4-23为例，NIPS正常工作时，Bypass交换机处于normal状态，此时从R1来的流量路线为：R1 → Bypass交换机的A1口 → Bypass交换机的A2口 → NIPS的G1/1口 → NIPS的G1/2口 → Bypass交换机的B2口 → Bypass交换机的B1口 → R2； NIPS断电或心跳口宕掉时，Bypass交换机切换到Bypass状态，光路从Bypass交换机直通，不经过NIPS，此时流量路线为：R1 → Bypass交换机的A1口 → Bypass交换机的B1口 → R2。

NIPS与bypass交换机联动的拓扑图



配置外置bypass的操作如下所示：

选择菜单 网络 > 其他配置，进入外置bypass管理页面，如图4-24所示。

外置bypass设备



配置外置bypass参数，参数说明如表4-14所示。

外置bypass参数说明

| 配置项 | 描述 |
| --- | --- |
| 工作状态 | 是否开启设备的外置bypass功能。  表格中说明  开启外置Bypass开关后，需要确保NIPS自身的带外管理口与外置Bypass交换机之间能够通信。有关外置Bypass交换机的安装及使用方法，请参考《绿盟科技BYPASS交换机用户使用手册》。 |
| 地址 | bypass交换机1~4的IP地址。 |
| 密码 | bypass交换机的登录密码。 |

单击【确定】按钮保存配置。

----结束

# 对象

对象，即将一些分散的同类型事物如IP地址、规则、服务等组合在一起，并给该组定义一个别名，这个别名就是对象的名称。

NIPS系统中，所有策略的配置都是基于对象的，因此在配置策略之前，必须预先定义相关的所有对象。管理员可定义的对象包括规则、网络、服务、应用、时间、敏感数据和流量通道。

对象概念的引入极大简化了NIPS的管理工作。当某个对象发生变化时，管理员只需要修改对象本身的属性即可，而无需再逐一修改引用到该对象的策略，使得NIPS的策略管理更加简化、灵活。有关策略的配置请参见。

本章主要介绍NIPS中的系统对象，具体包括以下内容：

| 功能 | 描述 |
| --- | --- |
| 规则对象 | 介绍规则对象的配置方法。 |
| 网络对象 | 介绍网络对象的配置方法。 |
| 服务对象 | 介绍服务对象的配置方法。 |
| 应用对象 | 介绍应用对象的配置方法。 |
| 时间对象 | 介绍时间对象的配置方法。 |
| 敏感数据 | 介绍敏感数据对象的配置方法。 |
| 流量通道对象 | 介绍流量通道对象的配置方法。 |

## 规则对象

规则对象用于描述各种不同行业的IPS客户的拓扑环境、实际需求以及面向的不同保护对象和应用环境。

NIPS设备的规则对象包括：

* 规则模板

规则模板提供多个典型的用户环境模板，可增强用户配置IPS策略时的易用性，减少普通用户的使用不便。规则模板又分为以下两类：

* 系统规则模板

系统规则模板分为内置模板和派生模板。内置模板即系统初始化自带模板，不允许修改，只允许进行查看和新建策略时引用；派生模板是拷贝默认模板后，根据需求进行一定限度修改（只能修改模板内的规则动作——告警、阻断、隔离，但不允许添加与删除规则）生成的规则模板。

* 用户规则模板

用户规则模板是管理员根据需要在规则集范围内进行规则的添加、删除以及修改规则动作，如告警、阻断等后生成的规则模板。

* 规则

规则是组成规则模板的基本单元，NIPS设备内置了绿盟科技多年积累的入侵防护规则库中的系统规则，在此基础之上，管理员可以根据需要自定义规则。同时，管理员还可以添加例外规则。

NIPS在支持以上规则对象的同时，还提供规则查询功能，下面进行详细介绍。

### 系统规则模板

NIPS系统按照用户使用NIPS设备的典型场景，将入侵防护规则库中的多条规则进行组合，形成7个典型的系统内置规则模板，如表5-1所示。

内置规则模板

| 模板 | 描述 |
| --- | --- |
| Default | 适用于大多数环境。 |
| DMZ区服务器 | 所有攻击类型规则，使用TFTP、RIP、NETBIOS、NFS和WINS的利用漏洞攻击规则除外。 |
| 内网客户端 | 所有攻击规则，使用RIP和路由协议的利用漏洞攻击规则除外。 |
| Web服务器 | 所有侦测和DoS攻击规则、一般后门程序以及使用DNS、HTTP和FTP协议的利用漏洞攻击规则。 |
| Windows服务器 | 受影响的操作系统包括Windows的所有攻击规则。 |
| 通用服务器 | 所有侦测和DoS攻击规则、一般后门程序以及使用DNS、SMTP、POP3、IMAP、DNS、NFS/RPC和NETBIOS/SMB协议的利用漏洞攻击规则。 |
| UNIX类服务器 | 受影响的操作系统包括UNIX、Linux、Solaris的所有攻击规则。 |

NIPS系统预定义的7个典型内置规则模板，是绿盟科技多年入侵防护事件防护经验与技术工程人员现场服务经验的积累和总结，能够满足绝大部分网络部署环境下的网络区域，建议用户在配置入侵防护策略时，尽可能使用内置规则模板。

系统规则模板除内置模板外，还有从内置规则模板派生的规则模板，下面介绍如何从内置规则模板新建派生规则模板。

选择菜单 对象 > 规则 > 系统规则模板，进入系统规则模板页面，如图5-1所示。

系统规则模板



单击内置规则模板对应的图标，弹出新建派生规则模板对话框，如图5-2所示。

新建派生规则模板



配置派生规则模板参数，参数说明如表5-2所示。

派生规则模板参数

| 配置项 | 描述 |
| --- | --- |
| 模板名称 | 派生模板的名称，系统默认派生规则模板的名称为“原系统默认规则模板名称+派生”。 |
| 备注 | 派生规则模板的描述信息。 |
| 事件 | 派生规则模板中包含的入侵防护事件。只能修改各条入侵防护事件的处理动作：告警、阻断、隔离。  表格中说明  当策略启用防护模式时，勾选“隔离”选项将会在指定时间内对触发规则的攻击IP进行隔离。 |

单击【确定】按钮，保存配置。

新建派生模板将显示在页面下方派生模板列表中。

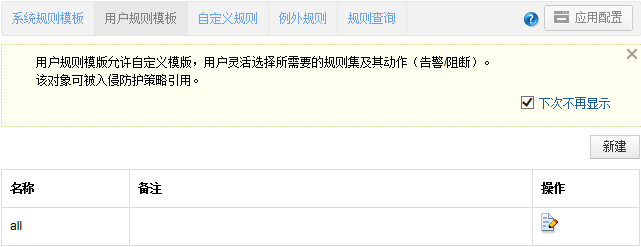
----结束

### 用户规则模板

用户规则模板是系统规则模板的补充，由管理员根据特殊用户网络部署环境制定。下面介绍如何新建用户规则模板。

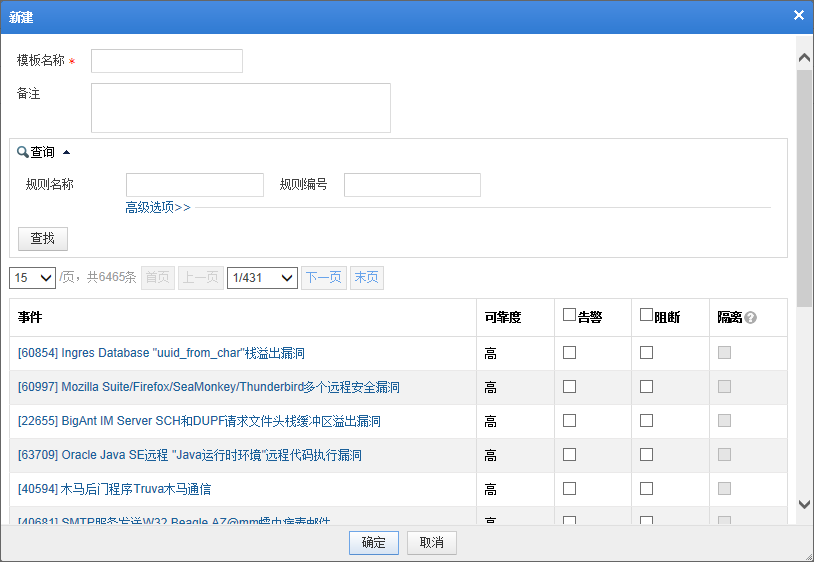
选择菜单 对象 > 规则 > 用户规则模板，进入用户规则模板页面，如图5-3所示。

用户规则模板



单击【新建】按钮，弹出新建用户规则模板对话框，如图5-4所示。

新建用户规则模板



配置用户规则模板参数，参数说明如表5-3所示。

用户规则模板参数

| 配置项 | 描述 |
| --- | --- |
| 模板名称 | 用户模板的名称。 |
| 备注 | 用户规则模板的描述信息。 |
| 事件 | 用户规则模板中包含的入侵防护事件，以及各入侵防护事件的处理动作：告警、阻断、隔离。  表格中说明  在启用防护模式时，勾选“隔离”选项将会在指定时间内对触发规则的攻击IP进行隔离。  可以通过规则查询定位特定事件，查询的详细操作请参见。 |

单击【确定】按钮，保存配置。

----结束

### 自定义规则

自定义规则，即添加各种类型网络协议的自定义规则，是对系统预定义的入侵防护规则库的补充。新建自定义规则编号从80001开始，在规则库中大于80000的规则即为自定义规则。自定义规则分为基本规则和高级规则，下面分别介绍管理员新建基本规则和高级规则的详细步骤。

#### 基本规则

基本规则按照网络协议分为4类，下面分别介绍管理员新建各类基本规则的详细步骤。

选择菜单 对象 > 规则 > 自定义规则 > 基本，进入基本规则页面，如图5-5所示。

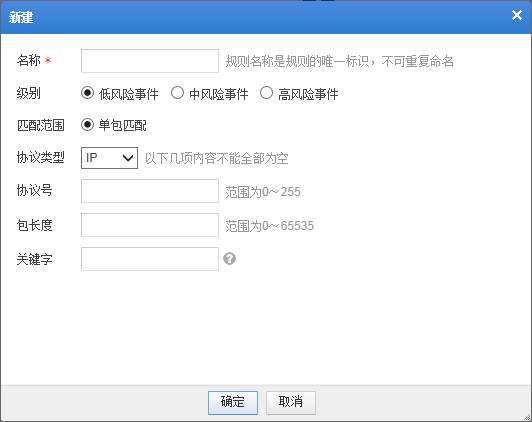
基本规则



* + - * 1. IP规则

单击基本自定义规则列表右上方的【新建】按钮，弹出新建基本自定义规则对话框，协议类型默认为IP，如图5-6所示。

新建自定义IP规则



配置自定义IP规则参数，参数说明如表5-4所示。

自定义IP规则参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 自定义IP规则的名称，用于在NIPS中唯一标识该IP规则。  名称中不能包含如下特殊字符：%、\、`、<、>、’、&、”。 |
| 级别 | IP规则的风险级别，可选级别有高风险事件、中风险事件、低风险事件。 |
| 匹配范围 | 系统默认只能进行单包匹配。  单包匹配是指，由一条或多条特征构成的自定义规则将在网络中的单个数据包内进行匹配和逻辑判断。 |
| 协议类型 | 选择IP。 |
| 协议号 | IP协议的上层协议类型编号，范围为0~255。例：6代表TCP，17代表UDP。 |
| 包长度 | IP数据包长度，范围为0~65535。   * 若类型为6，即TCP协议，其包长度为“20+数据包中data部分的长度”； * 若类型为17，即UDP协议，其包长度为“8+数据包中data部分的长度”。 |
| 关键字 | IP数据包中data部分包含的内容。  表格中说明  关键字可以使用正则表达式和非正则表达式两种方式标识。使用正则表达式时必须以“regex\_”开头，例：“regex\_\d\d”，表示匹配两个整数；使用非正则表达式时，如果以"case\_"开头，表示关键字区分大小写。 |

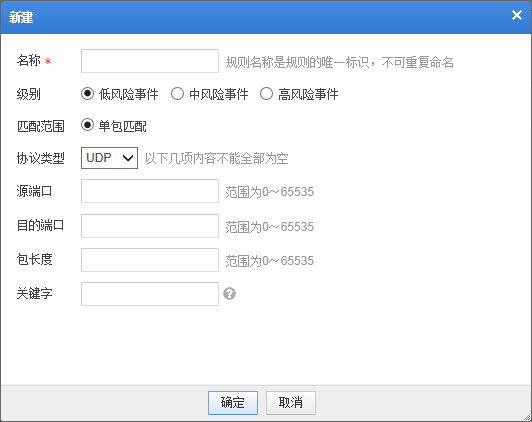
单击【确定】按钮，保存配置。

----结束

* + - * 1. UDP规则

单击自定义规则列表右上方的【新建】按钮，弹出新建自定义规则对话框，协议类型选择UDP，如图5-7所示。

新建自定义UDP规则



配置自定义UDP规则参数，参数说明如表5-5所示。

自定义UDP规则参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 自定义UDP规则的名称，用于在NIPS中唯一标识该UDP规则。  名称中不能包含如下特殊字符：%、\、`、<、>、'、&、"。 |
| 级别 | UDP规则的风险级别，可选级别有高风险事件、中风险事件、低风险事件。 |
| 匹配范围 | 系统默认只能进行单包匹配。  单包匹配是指，由一条或多条特征构成的自定义规则将在网络中的单个数据包内进行匹配和逻辑判断。 |
| 协议类型 | 选择UDP。 |
| 源/目的端口 | UDP数据包的源/目的端口号。 |
| 包长度 | UDP数据包中data部分的长度。 |
| 关键字 | UDP数据包中data部分包含的内容。 |

单击【确定】按钮，保存配置。

----结束

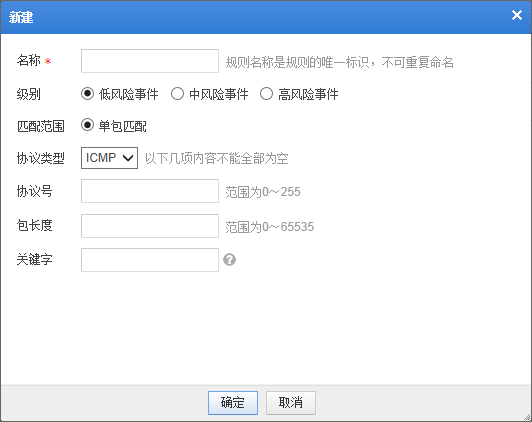
* + - * 1. TCP规则

自定义TCP规则与自定义UDP规则类似，详细步骤请参见，此处不再赘述。

* + - * 1. ICMP规则

单击自定义规则列表右上方的【新建】按钮，弹出新建自定义规则对话框，协议类型选择ICMP，如图5-8所示。

新建自定义ICMP规则



配置自定义ICMP规则参数，参数说明如表5-6所示。

自定义ICMP规则参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 自定义ICMP规则的名称，用于在NIPS中唯一标识该规则。  名称中不能包含如下特殊字符：%、\、`、<、>、'、&、"。 |
| 级别 | ICMP规则的风险级别，可选级别有高风险事件、中风险事件、低风险事件。 |
| 匹配范围 | 系统默认只能进行单包匹配。  单包匹配是指，由一条或多条特征构成的自定义规则将在网络中的单个数据包内进行匹配和逻辑判断。 |
| 协议类型 | 选择ICMP。 |
| 协议号 | ICMP消息类型对应的协议号。  协议号范围为0~255。例：查询的ping应答类型对应8，而差错的网络不可达错误类型对应3。 |
| 包长度 | ICMP数据包中data部分的长度。 |
| 关键字 | ICMP数据包中data部分包含的内容。 |

单击【确定】按钮，保存配置。

----结束

#### 高级规则

高级规则是对HTTP、FTP、SMTP、POP3、MSN、QQ协议中的各个字段进行与关系、或关系的组合后的结果，下面介绍管理员新建高级规则的详细步骤。

选择菜单 对象 > 规则 > 自定义规则 > 高级，进入高级规则页面，如图5-9所示。

高级规则



单击高级规则列表右上方的【新建】按钮，弹出新建高级规则对话框，如图5-10所示。

新建高级规则



配置高级规则基本参数，参数说明如表5-7所示。

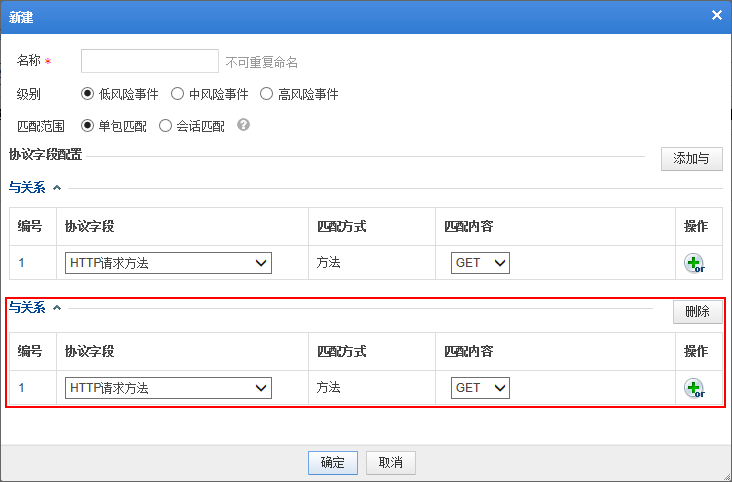
自定义高级规则基本参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 自定义高级规则的名称，用于在NIPS中唯一标识该规则。  名称中不能包含如下特殊字符：%、\、`、<、>、'、&、"。 |
| 级别 | 高级规则的风险级别，可选级别有高风险事件、中风险事件、低风险事件。 |
| 匹配范围 | 规则进行匹配和逻辑判断的范围，可选项：单包匹配、会话匹配。   * 单包匹配：由一条或多条特征构成的自定义规则将在网络中的单个数据包内进行匹配和逻辑判断。数据包（packet）为在封包交换网络中的最小传输数据单元， 单包匹配的范围小于会话匹配。 * 会话匹配：由一条或多条特征构成的自定义规则将在网络中的单个会话内进行匹配和逻辑判断。会话（session）是一个客户与服务器之间的不中断的请求响应序列。 |

配置协议字段。

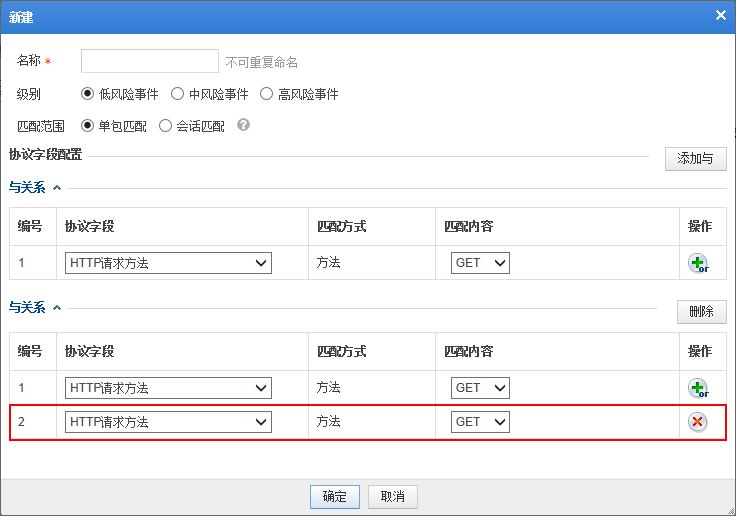
单击【添加与】按钮，添加与关系的协议字段，如图5-11红框所示。

添加与关系



单击操作栏中图标，在相应的与关系中添加或关系的协议字段，如图5-12红框所示。

添加或关系协议字段



配置协议字段及其匹配方式和匹配内容。

在协议字段栏的下拉列表中选择字段后，配置匹配方式和匹配内容。所有协议字段按照匹配方式分为方法、正则和数值三类，匹配内容具体如表5-8所示。

协议字段的配置总结

| 匹配方式 | | 匹配内容 |
| --- | --- | --- |
| 方法 | HTTP请求命令 | HTTP协议的请求类型。   * GET：接收到的数据； * POST：发送出去的数据。 |
| FTP/POP3请求命令 | FTP/POP3协议的请求类型。   * USER * PASS * LIST |
| SMTP请求命令 | SMTP协议的请求类型。   * MAIL * DATA * RCPT |
| 正则 | | 直接填写正则表达式。 |
| 数值 | | =、>、<或者in-range的数值。 |

单击【确定】按钮，保存配置。

----结束

### 例外规则

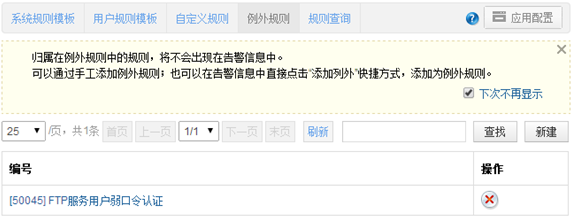
当管理员明确知道某条入侵防护事件产生了入侵防护事件告警，并且肯定该告警事件不会对现有网络环境的安全产生威胁或严重影响时，管理员可以将该入侵防护事件加入例外规则。

当该入侵防护事件加入例外规则后，NIPS设备不会再对该事件进行告警或阻断，并且首页也不再显示该例外规则。例外规则的添加请参见，下面介绍如何查看例外规则和取消例外规则。

* + - * 1. 查看例外规则

选择菜单 对象 > 规则 > 例外规则，进入例外规则页面，如图5-13所示。

例外规则



单击规则编号，查看规则详情，如图5-14所示。

规则详情

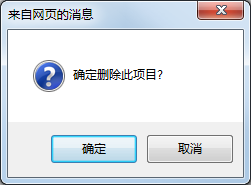


----结束

* + - * 1. 取消例外规则

单击例外规则列表操作栏中的图标，弹出确认取消对话框，如图5-15所示。

确认取消例外



单击【确定】按钮，取消相应的例外规则。

应用配置，保存配置。

----结束

### 规则查询

选择菜单 对象 > 规则 > 规则查询，进入规则查询页面，可以查询NIPS设备入侵防护事件规则库中详细的规则信息，如图5-16所示。

规则库搜索



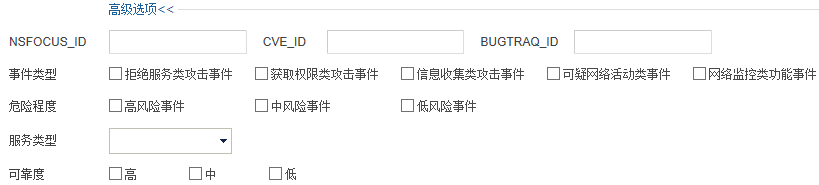
管理员可以按照规则编号或规则名称进行搜索。

* 按规则编号
* 按规则名称

同时，管理员还可以配置查询条件的高级选项，进一步缩小规则搜索范围，使得查询结果更加准确。

单击，显示查询条件的高级选项，如图5-17所示。

查询条件高级选项



高级选项参数说明如表5-9所示。

高级选项参数

| 配置项 | 描述 |
| --- | --- |
| NSFOCUS\_ID | 按照入侵防护事件在绿盟科技入侵防护规则库中的编号进行查询。 |
| CVE\_ID | 按照入侵防护事件在CVE规则库中的编号进行查询。 |
| BUGTRAQ\_ID | 按照入侵防护事件的BUGTRAQ\_ID进行查询。 |
| 攻击手段 | 按照入侵防护事件的攻击手段进行查询。 |
| 危险程度 | 按照入侵防护事件的危险程度进行查询。 |
| 服务类型 | 按照入侵防护事件的服务类型进行查询。 |
| 可靠度 | 按照入侵防护事件的可靠度进行查询。 |

## 网络对象

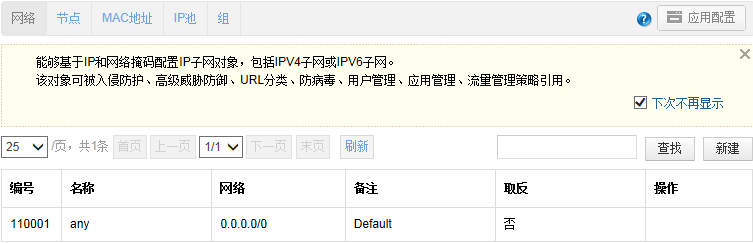
网络对象用于描述各类网络设备或设备组对象，目前支持的网络对象包括：网络、节点、MAC地址、IP池和网络组。

### 网络对象

网络对象是指一个网段，即根据IP和网络掩码来指定的IP子网对象，包括IPV4子网或IPV6子网。下面详细介绍如何新建网络对象。

选择菜单 对象 > 网络 > 网络，进入网络对象页面，如图5-18所示。

网络对象



单击【新建】按钮，弹出新建网络对象对话框，如图5-19所示。

新建网络对象



配置网络对象参数，参数说明如表5-10所示。

网络对象参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 网络对象名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。 |
| IP地址 | 网络对象的地址及其掩码，包括IPV4网络或者IPV6网络。 |
| 取反 | 是否对IP地址进行取反。   * 是：将指定IP以外的IP地址作为该网络对象； * 否：将指定IP作为该网络对象。 |
| 备注 | 网络对象的描述信息。 |

单击【确定】按钮，保存配置。

----结束

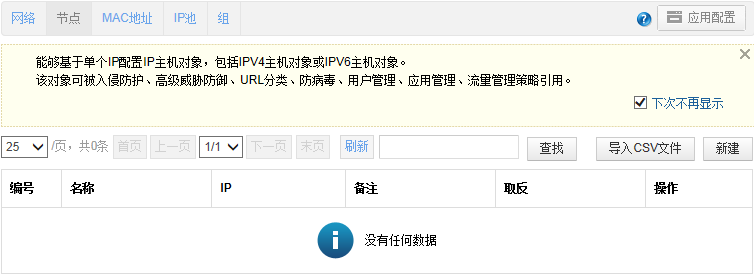
### 节点对象

节点对象是指单个IP，即根据IP来指定的IP主机对象，包括IPV4主机对象或IPV6主机对象。NIPS设备支持通过新建和导入两种方式添加节点对象。

#### 新建节点对象

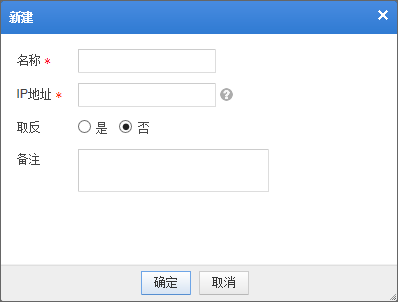
选择菜单 对象 > 网络 > 节点，进入节点对象页面，如图5-20所示。

节点对象



单击【新建】按钮，弹出新建节点对象对话框，如图5-21所示。

新建节点对象



配置节点对象参数，参数说明如表5-11所示。

节点对象参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 节点对象名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。 |
| IP地址 | 节点对象的地址，可以输入IPv4地址或IPv6地址，如：192.168.1.1 或 fe80::250:56ff:fec0:8。 |
| 取反 | 是否对节点对象进行取反。   * 是：将指定IP以外的IP地址作为该节点对象； * 否：将指定IP作为该节点对象。 |
| 备注 | 节点对象的描述信息。 |

单击【确定】按钮，保存配置。

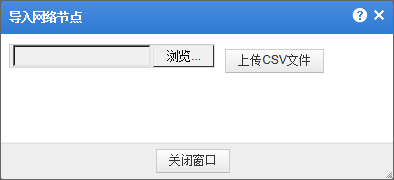
----结束

#### 导入节点对象

导入CSV文件之前，管理员需要从第三方设备获取或自己创建一个存储了大量节点信息的CSV文件。

在如图5-20所示页面中，单击【导入CSV文件】按钮，弹出选择文件对话框，如图5-22所示。

选择CSV文件



单击【浏览…】按钮，选择文件。

单击【上传CSV文件】按钮，执行导入。

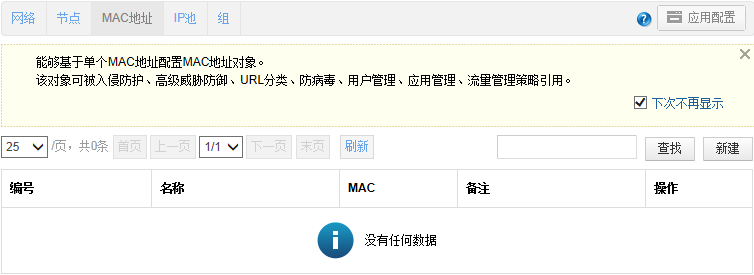
----结束

### MAC地址对象

MAC地址对象是指单个MAC地址，下面详细介绍如何新建MAC地址对象。

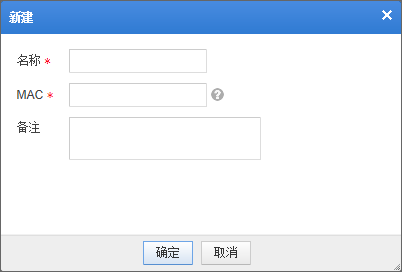
选择菜单 对象 > 网络 > MAC地址，进入MAC地址对象页面，如图5-23所示。

MAC地址对象



单击【新建】按钮，弹出新建MAC地址对象对话框，如图5-24所示。

新建MAC地址对象



配置MAC地址参数，参数说明如表5-12所示。

MAC地址参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | MAC地址对象名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。 |
| MAC | 该对象的MAC地址。MAC地址格式可以为XX-XX-XX-XX-XX-XX 或XX:XX:XX:XX:XX:XX, 其中X为十六进制数。 |
| 备注 | MAC地址对象的描述信息。 |

单击【确定】按钮，保存配置。

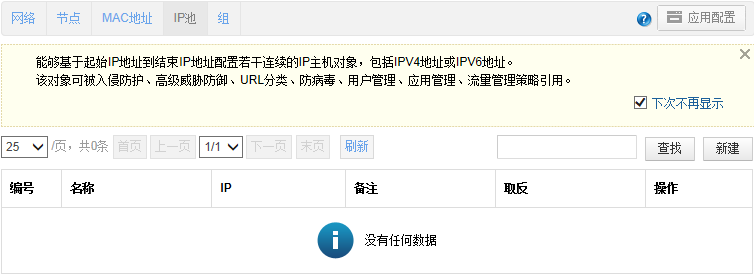
----结束

### IP池对象

IP池对象是指一段连续的IP，即从起始IP地址到结束IP地址之间的若干IP主机对象，包括IPV4地址或IPV6地址。下面详细介绍如何新建IP池对象。

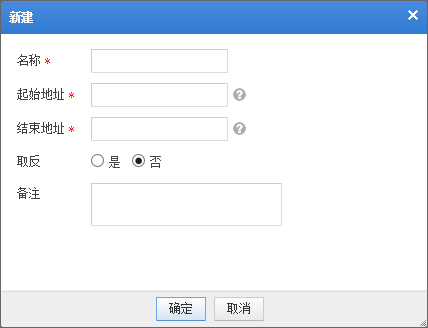
选择菜单 对象 > 网络 > IP池，进入IP池对象页面，如图5-25所示。

IP池对象



单击【新建】按钮，弹出新建IP池对象对话框，如图5-26所示。

新建IP池对象



配置IP池参数，参数说明如表5-13所示。

IP池参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | IP池对象名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。 |
| 起始地址 | IP池对象的起始地址，可以输入IPV4地址或者IPV6地址。  必须与“结束地址”属于同一协议类型的IP地址。 |
| 结束地址 | IP池对象的结束地址，可以输入IPV4地址或者IPV6地址。  必须与“开始地址”属于同一协议类型的IP地址，且必须大于起始地址。 |
| 取反 | 是否对IP池对象进行取反操作。   * 是：将指定IP段以外的IP范围作为该IP池对象； * 否：将指定IP段作为该IP池对象。 |
| 备注 | IP池对象的描述信息。 |

单击【确定】按钮，保存配置。

----结束

### 网络组对象

网络组对象是指若干个网络对象、节点对象、MAC地址对象、IP池对象、已有的网络组对象组成的逻辑集合。下面详细介绍如何新建网络组对象。

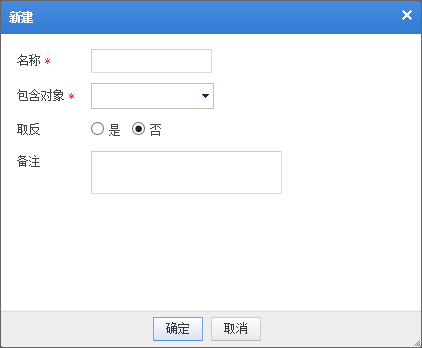
选择菜单 对象 > 网络 > 网络组，进入网络组对象页面，如图5-27所示。

网络组对象



单击【新建】按钮，弹出新建网络组对象对话框，如图5-28所示。

新建网络组对象



配置网络组参数，参数说明如表5-14所示。

网络组参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 网络组对象名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。 |
| 包含对象 | 网络组对象包含的网络对象（可以多选）。 |
| 取反 | 是否对网络组中的对象进行取反操作。   * 是：将没选中的网络对象作为该网络组对象； * 否：将选中的网络对象作为该网络组对象。 |
| 备注 | 网络组对象的描述信息。 |

单击【确定】按钮，保存配置。

----结束

## 服务对象

服务对象用于描述NIPS系统中各类系统服务、自定义服务、服务组和服务超时对象，本节将分别对其进行详细介绍。

### 系统服务对象

系统服务对象，即NIPS系统中预定义的服务对象，支持协议自识别和非固定端口的协议识别，包括常见的ftp、bittorrent等协议。下面介绍如何查看系统服务对象。

选择菜单 对象 > 服务 > 系统，进入系统服务页面，如图5-29所示。

系统服务对象



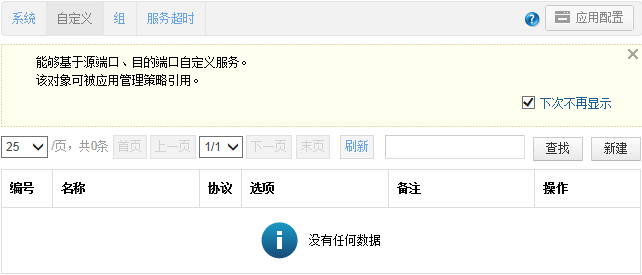
列表中展示NIPS预先定义的所有系统服务对象信息。管理员不能对系统服务对象进行新建、编辑和删除操作，只能对其进行引用和查看操作。

### 自定义服务对象

管理员可以根据管理需要自定义服务对象，即自定义服务端口。本节将详细介绍如何新建自定义服务对象。

选择菜单 对象 > 服务 > 自定义，进入自定义服务页面，如图5-30所示。

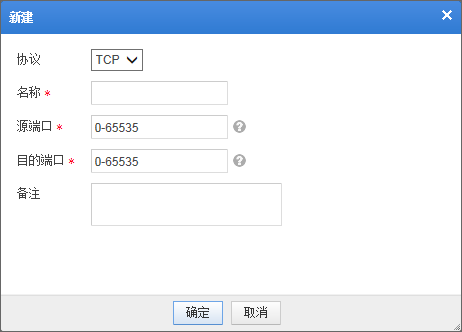
自定义服务



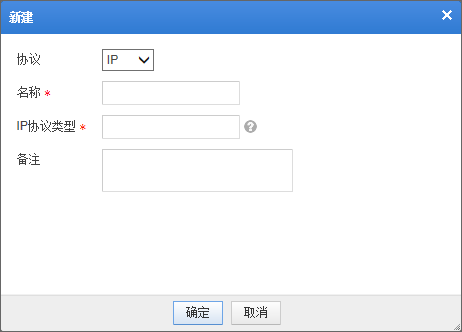
单击【新建】按钮，弹出新建自定义服务对象对话框。

自定义TCP协议和UDP协议的服务对象时，如图5-31所示；自定义IP协议的服务对象时，如图5-32所示。

新建自定义服务对象 – TCP/UDP



新建自定义服务对象 – IP



配置自定义服务对象参数，参数说明如表5-15所示。

自定义服务对象参数

| 配置项 | 描述 |
| --- | --- |
| 协议 | 选择一个协议类型，TCP、UDP或者IP。  不同的类型对应不同的参数设置，例如：选择TCP或UDP协议则需要设置源/目的端口；选择IP协议则需要设置IP协议类型。 |
| 名称 | 自定义服务对象的名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。 |
| 源端口 | 服务对象使用的源端口。  可以指定多个端口或端口范围，填写范围是0-65535（仅当选择TCP或UDP协议时，设置此项）。 |
| 目的端口 | 该服务对象使用的目的端口。  可以指定多个端口或端口范围，填写范围是0-65535（仅当选择TCP或UDP协议时，设置此项）。 |
| IP协议类型 | IP协议号，例如：1表示ICMP协议；2表示IGMP协议。取值范围：0-255。  仅当选择IP协议时，才能设置此项。 |
| 备注 | 自定义服务对象的描述信息。 |

单击【确定】按钮，保存配置。

，使配置生效。

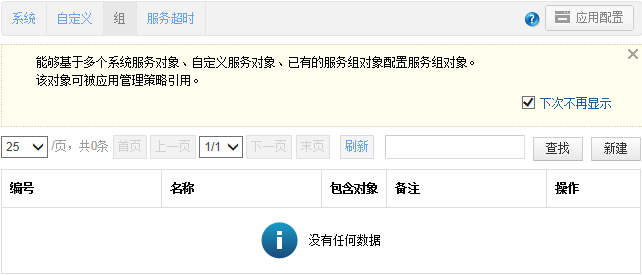
----结束

### 服务组对象

本小节的“服务组”对象是指若干系统服务对象、自定义服务对象、已有的服务组对象组成的逻辑集合。下面详细介绍如何新建服务组对象。

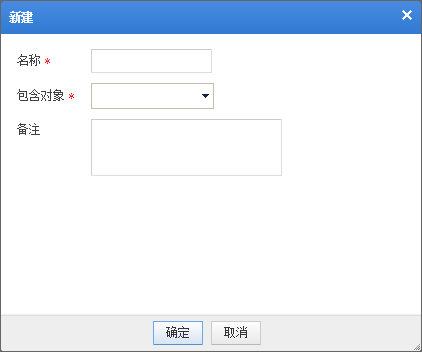
选择菜单 对象 > 服务 > 组，进入自定义服务组页面，如图5-33所示。

自定义服务组



单击【新建】按钮，弹出新建服务组对象对话框，如图5-34所示。

新建服务组对象



配置服务组对象参数，参数说明如表5-16所示。

服务组对象参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 服务组对象名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。 |
| 包含对象 | 该服务组对象包含的服务对象（可以多选）。 |
| 备注 | 服务组对象的描述信息。 |

单击【确定】按钮，保存配置。

，使配置生效。

----结束

### 服务超时

多数协议都可以设定协议通信的时间长度，管理员可以根据具体情况来自定义服务超时时间。下面详细介绍如何新建服务超时时间。

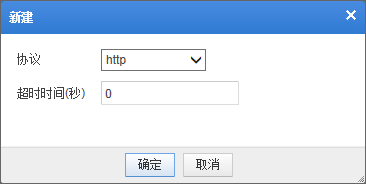
选择菜单 对象 > 服务 > 服务超时，进入服务超时页面，如图5-35所示。

服务超时



单击【新建】按钮，弹出新建服务超时对话框，如图5-36所示。

新建服务超时



配置服务超时时间参数，参数说明如表5-17所示。

服务超时时间参数

| 配置项 | 描述 |
| --- | --- |
| 协议 | 需要设定通信时长的协议类型。  表格中说明  针对每种协议类型的超时时间只能设置一次。 |
| 超时时间（秒） | 协议通信的时间，缺省为0秒，表示永不超时。  表格中说明  超时时间统计的是协议数据流之间的间隔时间；在配置的超时时间段内，服务不会被断开。当协议传输的数据流间隔时间较长时，建议配置更长的超时时间。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

## 应用对象

应用对象用于描述各类应用技术，如“酷我音乐盒”等。系统中预定义的一些缺省的应用对象，管理员也可以自定义应用对象和过滤器，以便在应用管理策略中通过指定应用对象对数据包进行过滤。

本节将详细介绍如何查看系统应用对象、新建自定义应用对象以及配置过滤器。

### 系统应用对象

系统应用对象（即系统预定义的应用对象）是NIPS系统自带的，管理员不能新建、编辑或删除系统应用对象，只能对其进行引用和查看。

选择菜单 对象 > 应用 > 应用，进入系统应用对象页面，如图5-37所示。

单击系统应用对象的名称，可以查看该系统应用对象的详细信息。

系统应用对象



单击，显示系统应用对象的查找参数，如图5-38所示。

查询系统应用对象



配置查询参数，参数说明如表5-18所示。

系统应用查询参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 待查询的应用对象的名称。 |
| 类别 | 选择应用对象所属类别和子类。 |
| 实现技术 | 选择应用对象的实现技术，包括：基于浏览器、客户端-服务器、网络协议、P2P、未知技术。 |
| 风险等级 | 选择应用对象所属风险等级，分为1~5级，风险等级依次递增。 |
| 标签 | 选择应用对象的标签类型，包括：易规避、消耗带宽、容易误操作、传输文件、以其他应用为管道、易被恶意软件利用、包含漏洞、广泛使用等。 |

单击【查询】按钮，符合条件的系统应用对象即可显示在列表中。

----结束

### 自定义应用对象

除了系统应用对象，管理员可以自定义应用对象。本节将详细介绍如何新建自定义应用对象。

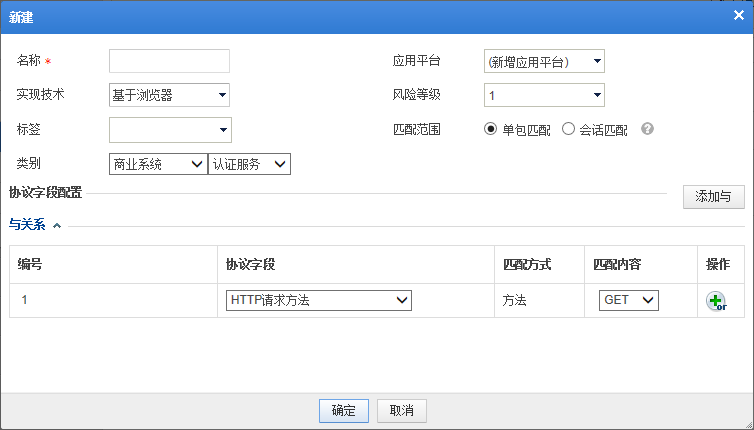
选择菜单 对象 > 应用 > 自定义应用，进入自定义应用对象的管理页面，该页面中列出了当前系统中所有的自定义应用对象，如图5-39所示。

应用对象 – 自定义应用对象列表



单击自定义应用对象列表右上方的【新建】按钮，进入新建应用对象的页面，如图5-40所示。

应用对象 – 新建应用对象



配置自定义应用对象参数，参数说明如表5-19所示。

自定义应用对象参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 应用对象的名称。 |
| 应用平台 | 应用对象所属的应用平台。  若选择“（新增应用平台）”，则该应用对象所属的应用平台与该应用对象的名称相同。 |
| 实现技术 | 自定义应用对象的实现技术，包括：基于浏览器、客户端-服务器、网络协议、P2P、未知技术。 |
| 风险等级 | 应用对象的风险等级，分为1~5级，风险等级依次递增。应用对象的风险等级计算方法请参见 的描述。 |
| 标签 | 应用对象的标签类型，包括：易规避、消耗带宽、容易误操作、传输文件、以其他应用为管道、易被恶意软件利用、包含漏洞、广泛使用等。 |
| 匹配范围 | 自定义应用对象进行匹配和逻辑判断的范围，可选项：单包匹配、会话匹配。   * 单包匹配：自定义应用对象将在网络中的单个数据包内进行匹配和逻辑判断。数据包（packet）为在封包交换网络中的最小传输数据单元，单包匹配的范围小于会话匹配。 * 会话匹配：自定义应用对象将在网络中的单个会话内进行匹配和逻辑判断。会话（session）是一个客户与服务器之间的不中断的请求响应序列。 |
| 类别 | 自定义应用对象所属类别。 |

配置协议字段。

协议字段的配置方法与自定义高级规则对象一致，具体操作请参见。

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

应用对象风险等级计算方法

应用对象的风险等级根据应用的所有标签计算得出，按照标签的威胁度分为高、中、低3个风险级别。

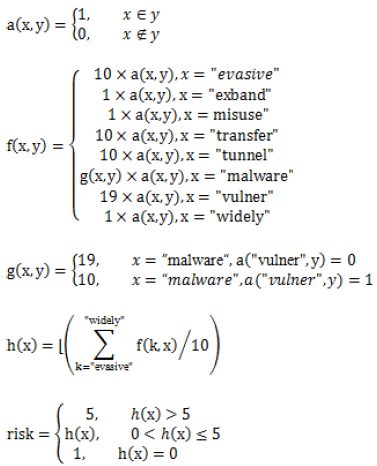
* 高度危险：包含漏洞或者易被恶意软件利用，容易对主机或者整个网络造成严重影响；
* 中度危险：数据传输或者以其他应用为管道，对网络具有潜在影响；
* 低度危险：使用广泛但对主机或者网络安全不构成威胁。

标签及其对应的威胁程度请参见表5-20。

标签及其对应危险程度

| 标号 | 标签（中文） | 标签（英文简称） | 危险程度 |
| --- | --- | --- | --- |
| 1 | 易规避 | evasive | 中 |
| 2 | 消耗带宽 | exband | 低 |
| 3 | 容易误操作 | misuse | 低 |
| 4 | 传输文件 | transfer | 中 |
| 5 | 以其他应用为管道 | tunnel | 中 |
| 6 | 易被恶意软件使用 | malware | 高 |
| 7 | 包含已知漏洞 | vulner | 高 |
| 8 | 广泛使用 | widely | 低 |

根据标签的风险级别，给予一定的权值，通过如下的公式来计算风险等级。



下面给出一个风险等级计算实例：

x ={ “exband”,”malware”,”vulner”,”widely” }

h(x) = L( ( 0 + f(“exband”,x) + 0 + 0 + 0 + f(“malware”,x) + f(“vulner”,x) + f(“widely”,x) ) / 10)

h(x) = L( (1\*a(“exband”,x) + g( “malware”,x) \* a(“malware”,x) + f(“vulner”,x) + f(“widely”,x) ) / 10)

h(x) = L( (1 + 10\*1 + 19 + 1 )/10 )

h(x) = L( 31/10 )

h(x) = 3

因为0 < h(x) <= 5

所以risk = h(x) = 3

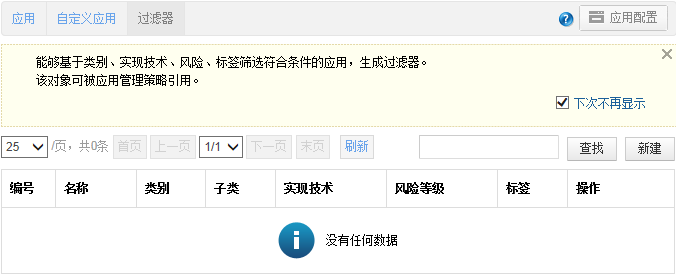
### 配置过滤器

为了能从大量流量数据中筛选出用户关注的数据，NIPS设备提供了过滤器功能，以便针对NIPS设备截取到的数据根据指定的过滤条件进行过滤。

单独配置的过滤器没有任何过滤效果，只有在应用管理策略中引用这些过滤器，才能够达到预期的过滤效果。配置应用管理策略的操作请参见，本节主要介绍如何新建过滤器。

选择菜单 对象 > 应用 > 过滤器，进入过滤器页面，如图5-41所示。

过滤器



单击【新建】按钮，弹出新建过滤器对话框，如图5-42所示。

新建过滤器



配置过滤器参数，参数说明如表5-21所示。

过滤器参数

| 配置项 | 描述 |
| --- | --- |
| 过滤器名称 | 过滤器的名称。 |
| 类别 | 待过滤的应用对象的类别及其子类。 |
| 实现技术 | 待过滤的应用对象的实现技术。 |
| 风险等级 | 待过滤的应用对象的风险等级。 |
| 标签 | 待过滤的应用对象的标签。 |

输入过滤条件，单击【查看筛选结果】按钮，可以查看到符合过滤条件的所有应用对象。

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

## 时间对象

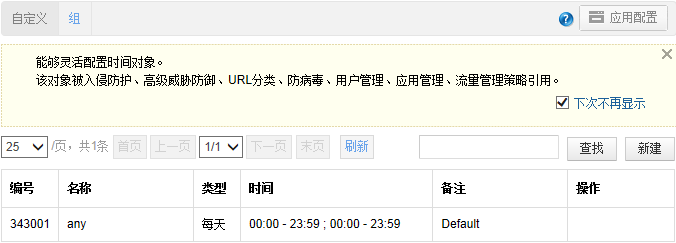
NIPS系统使用时间对象来表示一个时间范围，时间对象包括单个时间对象和时间组对象。本节将详细介绍如何创建自定义单个时间对象和时间组对象。

### 自定义时间对象

每个时间对象均可包含两个时间段，管理员可以根据具体情况来自定义时间对象。下面将详细介绍如何新建自定义时间对象。

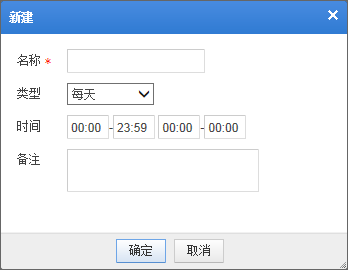
选择菜单 对象 > 时间 > 自定义，进入自定义时间对象页面，如图5-43所示。

自定义时间对象



单击【新建】按钮，弹出新建时间对象对话框，如图5-44所示。

新建自定义时间对象



配置自定义时间对象参数，参数说明如表5-22所示。

自定义时间对象参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 自定义时间对象的名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括\%`@^<>{}’&”:和空格）。 |
| 类型 | 时间类型，包括每天、每个工作日、每周和每月，其中“每个工作日”表示每周一至周五。 |
| 时间 | 时间对象可以包含两个时间段，如果只需定义一个时间段，则将第二个时间段都保持为系统默认的00:00即可。对于每月，还需设置具体日期。 |
| 备注 | 自定义时间对象的描述信息。 |

单击【确定】按钮，保存配置。

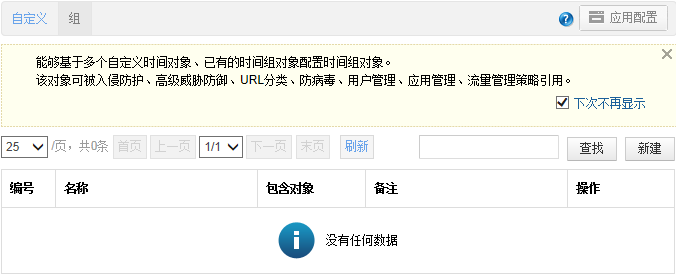
----结束

### 时间组对象

时间组对象是指若干自定义时间对象、已有的时间组对象组成的逻辑集合。下面将详细介绍如何新建时间组对象。

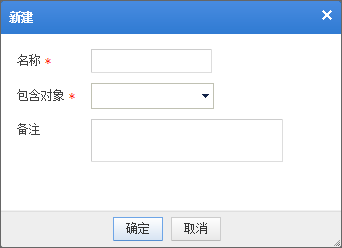
选择菜单 对象 > 时间 > 组，进入时间组对象页面，如图5-45所示。

时间组对象



在所示页面中，单击时间组对象列表右上方的【新建】按钮，进入时间组对象的新建页面，如图5-46所示。

新建时间组对象



配置时间组对象参数，参数说明如表5-23所示。

时间组对象参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 时间组对象名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。 |
| 包含对象 | 时间组对象包含的时间对象或者时间组对象（可以多选）。 |
| 备注 | 时间组对象的描述信息。 |

单击【确定】按钮，保存配置。

----结束

## 敏感数据对象

敏感数据对象描述身份证号码、银行卡号、电话号码3种类型的关键敏感数据，用于保护内部敏感数据，防止敏感文件外泄。下面主要介绍如何新建敏感数据对象。

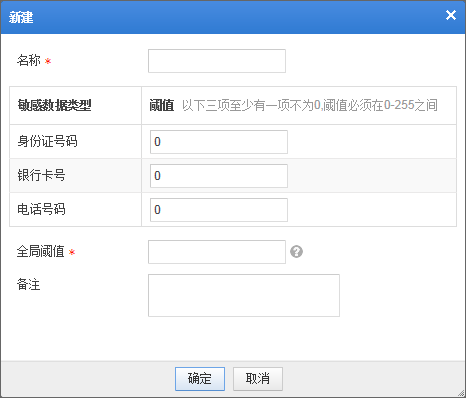
选择菜单 对象 > 敏感数据 > 敏感数据，进入敏感数据页面，如图5-47所示。

敏感数据对象



单击【新建】按钮，弹出新建敏感数据对象对话框，如图5-48所示。

新建敏感数据



配置敏感数据对象参数，参数说明如表5-24所示。

敏感数据对象参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 敏感数据对象的名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括\%`@^<>{}’&”:和空格）。 |
| 身份证号码 | 身份证号码类型的敏感数据阈值，必须小于全局阈值。 |
| 银行卡号 | 银行卡号类型的敏感数据阈值，必须小于全局阈值。 |
| 电话号码 | 电话号码类型的敏感数据阈值，必须小于全局阈值。 |
| 全局阈值 | 敏感数据的全局阈值，必须大于每个敏感数据类型阈值，范围为0~65535。  当网络中出现的敏感数据（身份证号码、银行卡号码、电话号码）总数大于全局阈值时，即会产生一条全局的敏感数据告警。 |
| 备注 | 敏感数据对象的描述信息。 |

单击【确定】按钮，保存配置。

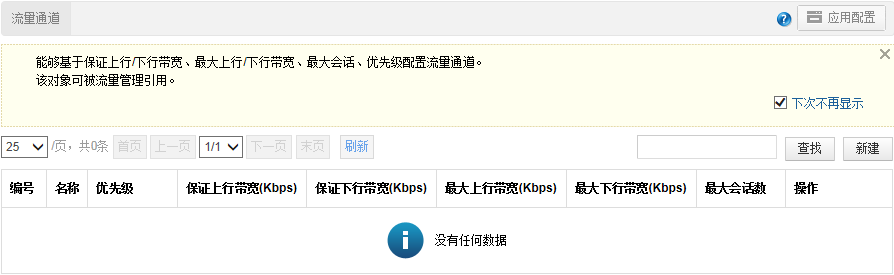
----结束

## 流量通道对象

流量通道对象为设置流量通道策略提供了多个对象，方便管理员设置不同的通道对流量管理。下面主要介绍如何新建流量通道对象。

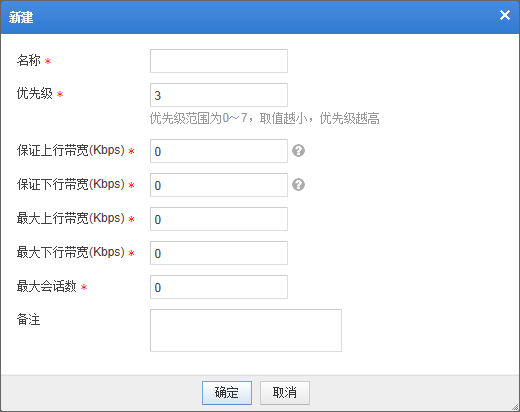
选择菜单 对象 > 流量通道 > 流量通道，进入流量通道对象页面，如图5-49所示。

流量通道对象



单击【新建】按钮，弹出新建流量通道对象对话框，如图5-50所示。

新建流量通道对象



配置流量通道对象参数，参数说明如表5-25所示。

流量通道对象参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 流量通道对象的名称。  不能和已有对象重名，且不能使用非法字符（非法字符包括\%`@^<>{}’&”:和空格）。 |
| 优先级 | 流量规则的优先级别，可选范围0～7之间的整数；值越小级别越高。 |
| 保证上行带宽（Kbps） | 流量流出的最小使用带宽（单位为Kbps），默认为0，表示不限制带宽。  表格中说明  线路上行流量总和必须大于该线路中所有策略的流量通道的保证上行带宽的总和。 |
| 保证下行带宽（Kbps） | 流量流入的最小使用带宽（单位为Kbps），默认为0，表示不限制带宽。  表格中说明  线路下行流量总和必须大于该线路中所有策略的流量通道的保证下行带宽的总和。 |
| 最大上行带宽（Kbps） | 流量流出的最大使用带宽（单位为Kbps），默认为0，表示不限制带宽。 |
| 最大下行带宽（Kbps） | 流量流入的最大使用带宽（单位为Kbps），默认为0，表示不限制带宽。 |
| 最大会话数 | 流量通道允许的最大TCP协议会话数，默认为0，表示不限制会话数。 |
| 备注 | 流量通道对象的描述信息。 |

单击【确定】按钮，保存配置。

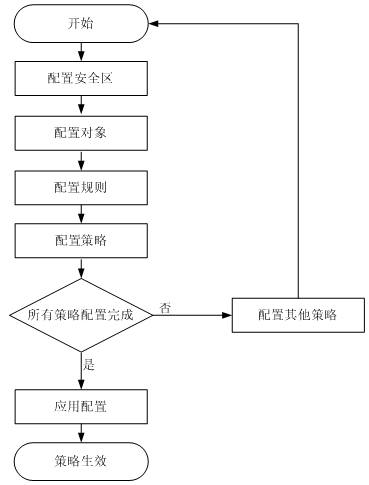
----结束

# 策略配置

策略是NIPS设备对网络进行入侵防护的执行依据，NIPS共有8种类型策略，各种策略相互配合，对流经NIPS设备的数据进行规则匹配，从而实现对网络各种入侵防护事件的防护，保证内网安全。

添加策略的常用流程如图6-1所示。

策略配置流程



|  |  |
| --- | --- |
| 注意 | 对策略进行操作后必须进行“应用配置”操作，新的策略才会生效。 |

本章介绍了策略配置的各类规则、策略的详细配置信息，具体包括以下内容：

| 功能 | 描述 |
| --- | --- |
| 策略通用操作 | 介绍NIPS系统中各种策略的通用操作。 |
| 入侵防护策略 | 介绍入侵防护策略以及DoS防护策略的配置方法。 |
| 高级威胁防御策略 | 介绍高级威胁防御策略的配置方法。 |
| 信誉 | 介绍僵尸网络和信誉策略的配置方法。 |
| URL分类过滤策略 | 介绍URL分类过滤策略的配置方法。 |
| 防病毒策略 | 介绍防病毒策略的配置方法。 |
| 用户管理策略 | 介绍用户管理策略的配置方法。 |
| 应用管理策略 | 介绍应用管理策略的配置方法。 |
| 流量管理策略 | 介绍流量管理策略的配置方法。 |

## 策略通用操作

NIPS中策略的通用操作包括：移动和复制。本节介绍通用操作的详细步骤，新建各种类型策略的详细步骤请参见本章后续内容。

* + - * 1. 移动策略

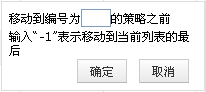
入侵防护策略、敏感数据保护策略、文件识别策略、URL分类过滤策略、防病毒策略、用户认证策略、应用管理策略和流量管理策略支持移动。

当各种类型的策略列表中包含多个策略时，NIPS将按照策略列表中的顺序依次与数据报文进行匹配，因此匹配条件严格的策略应当置于条件宽松的策略之前，以提高NIPS处理数据报文的效率。

移动入侵防护策略的操作如下。

单击策略列表中的图标，弹出策略排序设置对话框，如图6-2所示。

移动策略



配置移动参数。

单击【确定】按钮，完成操作。

----结束

* + - * 1. 复制策略

新建策略时，若要新建的策略与已有策略参数类似，NIPS操作员可以复制已有策略，再根据需要修改原有策略参数，使策略的管理更加便捷。

单击策略列表中的图标，弹出复制策略对话框，如图6-3所示。

复制策略



根据实际情况适当调整策略参数。

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

## 入侵防护策略

入侵防护策略主要包括入侵防护策略和DoS防护，下面分别予以介绍。

### 入侵防护策略

通过设置入侵防护策略，NIPS可以实现主动防御已知和未知攻击以及实时阻断各种黑客攻击（如缓冲区溢出、SQL注入、暴力猜测、拒绝服务、扫描探测、非授权访问、蠕虫病毒、僵尸网络等）的功能。

下面主要介绍如何新建入侵防护策略。

选择菜单 策略 > 入侵防护 > 入侵防护策略，进入入侵防护策略页面，如图6-4所示。

入侵防护策略



单击【新建】按钮，弹出新建入侵防护策略对话框，如图6-5所示。

新建入侵防护策略



配置入侵防护策略参数，参数说明如表6-1所示。

入侵防护策略参数

| 配置项 | 描述 |
| --- | --- |
| 安全区 | 对经过哪个安全区的报文应用该入侵防护策略。  “global”表示来自任何安全区的报文均匹配该策略。 |
| 源地址对象 | 对来自哪些地址的报文应用该入侵防护策略。  “any”表示任意地址。 |
| 目的地址对象 | 对发往哪些地址的报文应用该入侵防护策略。  “any”表示任意地址。 |
| 用户 | 入侵防护策略的用户对象，分为如下四类：   * any：任意用户。 * 信任用户：在线用户。有关在线用户的介绍，请参见。 * 非信任用户：在线用户IP地址范围之外的其他所有IP地址会被识别为非信任用户。 * 自定义用户：从AD域配置器获取到的用户列表中选择的用户，有关AD域配置器的介绍请参见。 |
| 时间对象 | 入侵防护策略生效的时间段。  “any”表示所有时间。 |
| 规则模板 | 入侵防护策略引用的规则模板。  规则模板的介绍请参见。 |
| 防护模式 | 是否启用防护模式，默认启用。  启用防护模式后，NIPS将阻断匹配到该入侵防护策略的报文。 |
| 备注 | 入侵防护策略的描述信息。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

### DoS防护策略

DoS拒绝服务攻击最常见的有计算机网络带宽入侵和连通性入侵。带宽入侵是制造超过网络最大承载力的数据流量冲击网络，占用所有可用网络资源，达到拒绝服务的目的。连通性入侵是指制造大量的连接请求访问计算机，耗尽所有的操作系统资源，达到拒绝服务的目的。

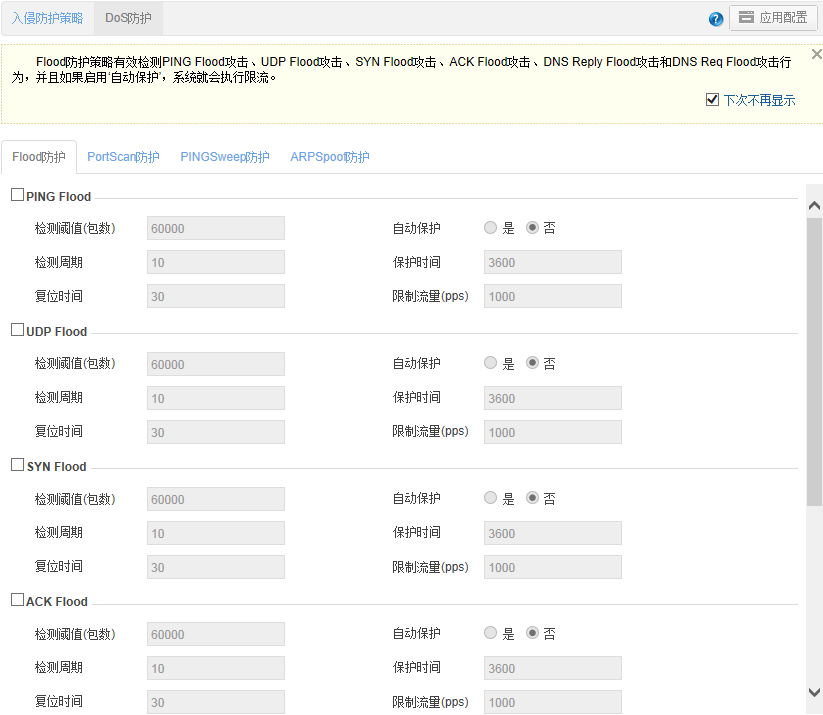
NIPS设备内置的DOS防护模块，可以有效检测并抵御抗拒绝服务攻击行为，管理员通过DoS防护策略可以保护指定的网络对象免于受到以下类型的攻击：Flood攻击、PortScan攻击、PINGSweep攻击和ARPSpoof攻击，下面将对各类DoS防护策略的配置进行详细介绍。

#### Flood防护策略

Flood攻击指攻击者向攻击目标发送大量的虚假请求，驱使被攻击者由于不断应付这些无用信息而筋疲力尽，合法的用户却由此无法享受到相应服务，即发生拒绝服务。目前，主流Flood攻击包括：PING Flood攻击、UDP Flood攻击、SYN Flood攻击、DNS Reply Flood攻击、ACK Flood攻击和DNS Req Flood攻击。NIPS系统的Flood防护策略可以有效防护上述Flood攻击，具体操作如下：

选择菜单 策略 > 入侵防护 > DoS防护 > Flood防护，进入Flood防护策略的配置页面，如图6-6所示。

Flood防护



勾选某类Flood防护左侧复选框启用该类防护后，配置相应防护策略的参数。参数说明如表6-2所示。

Flood防护策略参数

| 配置项 | 描述 |
| --- | --- |
| 检测阈值（包数） | 当系统在检测周期内检测到向某目标主机发送报文的个数达到或超过了此处指定的“检测阈值”时，即认为发生了Flood攻击。 |
| 检测周期 | Flood攻击的检测周期。单位：秒。 |
| 复位时间 | 每隔此处配置的时间，系统就会将检测数据清零，重新开始检测。单位：秒。 |
| 自动保护 | 当系统检测到有Flood攻击发生时，是否启用自动保护功能。  如果启动了自动保护，当有Flood攻击发生时，系统就会执行限流并报警；否则，系统仅执行报警。 |
| 保护时间 | 限流的时间，超过该时间后，系统将重新进行检测。单位：秒。 |
| 限制流量（pps） | 执行限流时，系统限制的发包速率。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

#### PortScan防护策略

Port Scan（端口扫描）攻击通过扫描目标主机的TCP端口或者UDP端口，确定该主机开启的服务，为进一步侵入目标系统做准备。NIPS系统的PortScan防护策略可以有效防护TCP端口扫描和UDP端口扫描，具体操作如下：

选择菜单 策略 > 入侵防护 > DoS防护 > PortScan防护，进入PortScan防护策略的配置页面，如图6-7所示。

PortScan防护



勾选某类PortScan防护左侧复选框启用该类防护后，配置防护策略，参数说明与Flood防护策略类似，请参见表6-2。

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

#### PINGSweep防护策略

通常，攻击者通过PING Sweep（即PING扫描）方式探测网络上存在的活动主机，以便大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入目标系统做准备。NIPS系统的PINGSweep防护策略可以有效防护此类攻击，具体操作如下：

选择菜单 策略 > 入侵防护 > DoS防护 > PINGSweep防护，进入PINGSweep防护策略的配置页面，如图6-8所示。

PINGSweep防护



选中“PING Sweep”左侧复选框启用该防护后即可配置该防护策略，参数说明与Flood防护策略类似，请参见表6-2。

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

#### ARPSpoof防护策略

ARP Spoof攻击是通过伪造IP地址和MAC地址实现ARP欺骗，不仅会造成网络不稳定甚至断网的问题，而且能进一步实施中间人攻击，以此非法获取游戏、网银、文件服务等系统的帐号和口令。NIPS系统的ARPSpoof防护策略可以有效防护此类攻击，具体操作如下：

选择菜单 策略 > 入侵防护 > DoS防护 > ARPSpoof防护，进入ARPSpoof防护策略配置页面，如图6-9所示。

ARPSpoof防护



选中“ARP Spoof”左侧复选框启用该防护后，配置防护策略，参数说明与Flood防护策略类似，请参见表6-2。

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

## 高级威胁防御策略

高级威胁防御策略通过敏感数据保护、文件识别、服务器异常防护对内网安全进行防护。

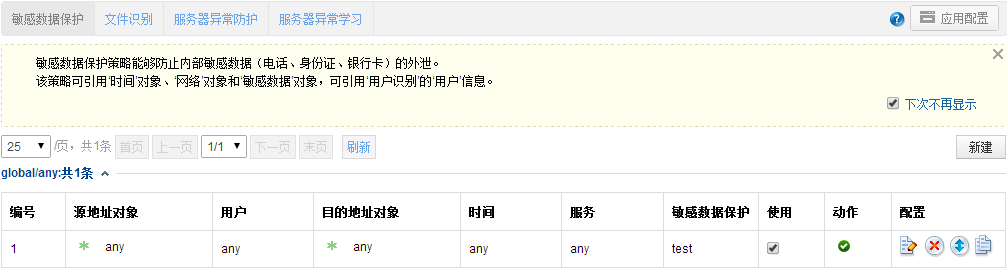
### 敏感数据保护策略

敏感数据保护策略用于对特定条件下的数据流量进行关键数据（电话、身份证、银行卡）识别，防止内部敏感数据外泄，从而保证内网信息安全。

下面主要介绍如何新建敏感数据保护策略。

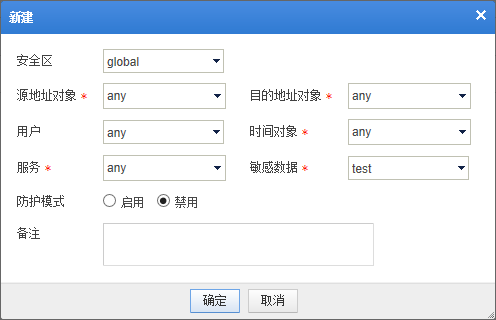
选择菜单 策略 > 高级威胁防御 > 敏感数据保护，进入敏感数据保护策略页面，如图6-10所示。

敏感数据保护策略



单击【新建】按钮，弹出新建敏感数据保护策略对话框，如图6-11所示。

新建敏感数据保护策略



配置敏感数据保护策略参数，参数说明如表6-3所示。

敏感数据保护策略参数

| 配置项 | 描述 |
| --- | --- |
| 安全区 | 对经过哪个安全区的报文应用该敏感数据保护策略。  “global”表示来自任何安全区的报文均匹配该策略。 |
| 源地址对象 | 对来自哪些地址的报文应用该敏感数据保护策略。  “any”表示任意地址。 |
| 目的地址对象 | 对发往哪些地址的报文应用该敏感数据保护策略。  “any”表示任意地址。 |
| 用户 | 敏感数据保护策略的用户对象，分为如下四类：   * any：任意用户。 * 信任用户：在线用户。有关在线用户的介绍，请参见。 * 非信任用户：在线用户IP地址范围之外的其他所有IP地址会被识别为非信任用户。 * 自定义用户：从AD域配置器获取到的用户列表中选择的用户，有关AD域配置器的介绍请参见。 |
| 时间对象 | 敏感数据保护策略生效的时间段。  “any”表示所有时间。 |
| 服务 | 敏感数据保护策略对哪些服务产生的数据报文生效。  可选项有：any、HTTP、FTP、EMAIL。“any”表示所有服务。 |
| 敏感数据 | 敏感数据保护策略进行识别的敏感数据对象。 |
| 防护模式 | 是否启用防护模式，默认禁用。  启用防护模式后，NIPS将阻断匹配到该敏感数据保护策略的报文。 |
| 备注 | 敏感数据保护策略的描述信息。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

### 文件识别策略

文件识别策略用于对特定条件下的数据流量进行文件格式识别，从而保证内网信息安全。

下面主要介绍如何新建文件识别策略。

选择菜单 策略 > 高级威胁防御 > 文件识别，进入文件识别策略页面，如图6-12所示。

文件识别策略



单击【新建】按钮，弹出新建文件识别策略对话框，如图6-13所示。

新建文件识别策略



配置文件识别策略参数，参数说明如表6-4所示。

文件识别策略参数

| 配置项 | 描述 |
| --- | --- |
| 安全区 | 对经过哪个安全区的报文应用该文件识别策略。  “global”表示来自任何安全区的报文均匹配该策略。 |
| 源地址对象 | 对来自哪些地址的报文应用该文件识别策略。  “any”表示任意地址。 |
| 目的地址对象 | 对发往哪些地址的报文应用该文件识别策略。  “any”表示任意地址。 |
| 用户 | 文件识别策略的用户对象，分为如下四类：   * any：任意用户。 * 信任用户：在线用户。有关在线用户的介绍，请参见。 * 非信任用户：在线用户IP地址范围之外的其他所有IP地址会被识别为非信任用户。 * 自定义用户：从AD域配置器获取到的用户列表中选择的用户，有关AD域配置器的介绍请参见。 |
| 时间对象 | 文件识别策略生效的时间段。  “any”表示所有时间。 |
| 服务 | 文件识别策略对哪些服务产生的数据报文生效。  可选项有：any、HTTP、FTP、EMAIL。“any”表示所有服务。 |
| 文件格式 | 文件识别策略进行识别的文件格式。“any”表示所有文件格式。 |
| 防护模式 | 是否启用防护模式，默认禁用。  启用防护模式后，NIPS将阻断匹配到该文件识别策略的报文。 |
| 备注 | 文件识别策略的描述信息。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

### 服务器异常防护策略

服务器异常防护策略用于对特定条件下服务器的外联行为进行识别，管理员通过设定允许服务器外联的地址、允许通过的协议及端口来定义服务器的正常外联行为，手工定义的正常外联行为之外的所有外联行为全部作为非法外联，按照服务器异常防护策略的设定进行处理。NIPS最多支持对1000个服务器外联行为进行防护。

新建服务器异常防护策略有普通新建和快速新建两种方式。

#### 普通新建

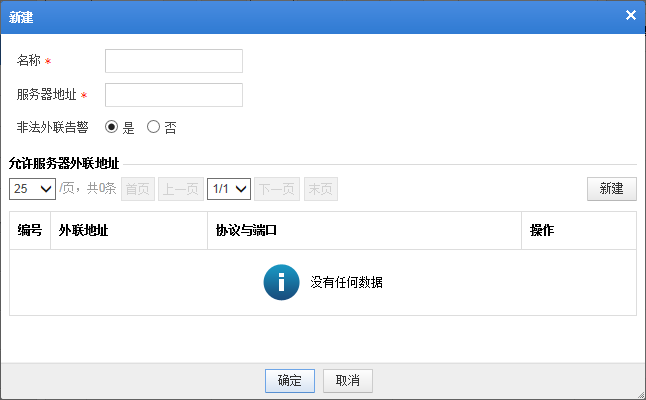
选择菜单 策略 > 高级威胁防御 > 服务器异常防护，进入服务器异常防护策略页面，如图6-14所示。

服务器异常防护策略



单击【新建】按钮，弹出新建文件识别策略对话框，如图6-15所示。

新建服务器异常防护策略

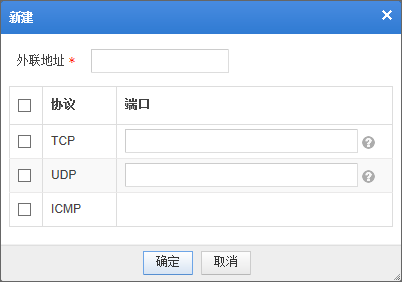


配置服务器异常防护策略参数，参数说明如表6-5所示。

服务器异常防护策略参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 服务器异常防护策略的名称。 |
| 服务器地址 | 策略防护的服务器的IP地址。 |
| 非法外联告警 | 是否开启外服外联告警功能。 |
| 允许服务器外联地址 | 定义服务器的正常外联行为，作为策略判断服务器外联是否非法的依据。  单击【新建】按钮，弹出如图6-16所示的新建正常外联行为对话框，配置参数后单击【确定】按钮保存配置，参数说明如表6-6所示。 |

定义服务器的正常外联行为



服务器外联参数

| 配置项 | 描述 |
| --- | --- |
| 外联地址 | 服务器正常外联的IP地址。 |
| TCP/端口 | 对该外联地址，允许服务器进行连接的TCP端口。 |
| UDP/端口 | 对该外联地址，允许服务器进行连接的UDP端口。 |
| ICMP | 对该外联地址，是否允许服务器访问ICMP服务。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

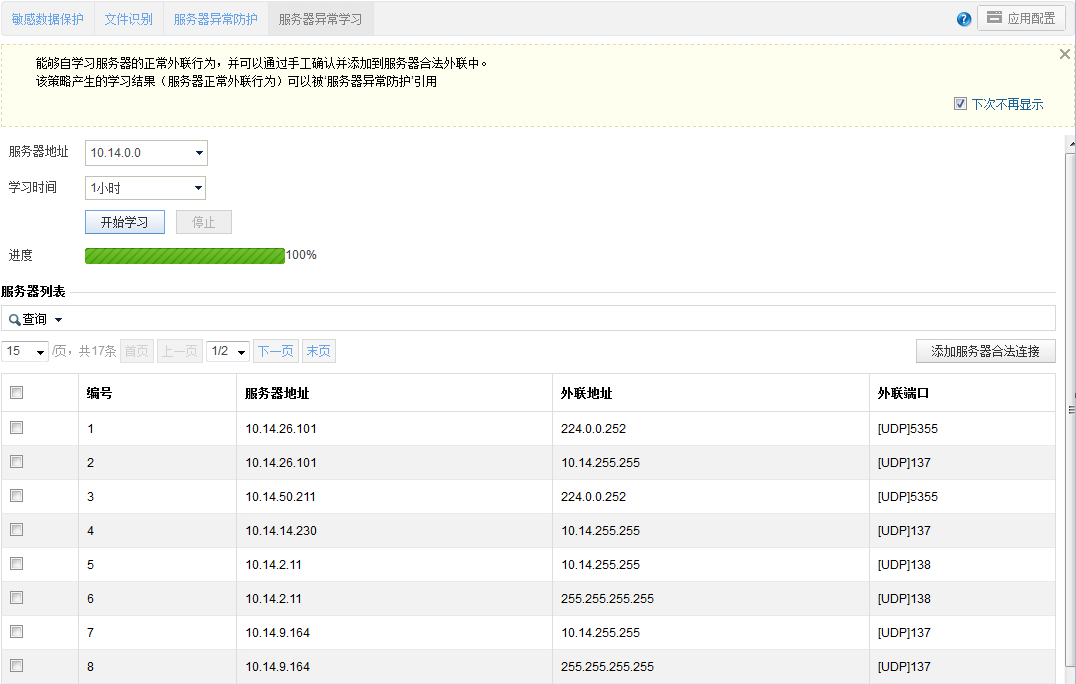
----结束

#### 快速新建

通过NIPS设备自学习到的外联信息，管理员可以快速新建服务器异常防护策略。

选择菜单 策略 > 高级威胁防御 > 服务器异常学习，进入服务器异常学习页面，页面下方的服务器列表中显示学习到的服务器外联信息，如图6-17所示。

服务器异常学习



快速新建服务器异常防护策略。

在列表中勾选一个或多个服务器外联网络行为。

单击【添加服务器合法连接】按钮，将服务器、外联地址、服务器开放的外联端口信息设置为服务器正常外联，即快速新建一条或多条服务器异常防护策略。

快速新建的服务器异常防护策略可以在如图6-14所示的页面中进行查看。

----结束

### 服务器异常学习

NIPS设备支持服务器自学习功能，配置服务器异常学习后，NIPS设备将对特定服务器主动发起的外联数据进行获取，并从获取到的主动外联数据中学习服务器开放的端口及其提供的服务信息。NIPS设备通过服务器自学习功能判定服务器的所有网络行为，用户可通过学习结果，来判断哪些外联行为是正常的。

下面介绍如何配置服务器异常学习。

选择菜单 策略 > 高级威胁防御 > 服务器异常学习，进入服务器异常学习页面，页面上方可配置服务器异常学习参数，如图6-17所示。

配置服务器学习参数，参数说明如表6-7所示。

服务器学习参数

| 配置项 | 描述 |
| --- | --- |
| 服务器地址 | NIPS设备进行自学习的服务器IP地址。  从下拉列表中选择服务器地址，地址选项来源于网络对象，单击蓝色链接文字“新建”可新建网络对象，网络对象的详情请参见。 |
| 学习时间 | NIPS对指定服务器主动外联行为数据学习的时间范围。可选项有：1小时、12小时、1天、1周。 |

单击【开始学习】按钮，服务器自学习开始执行。

学习进度可以通过进度条及百分比查看。

（可选）单击【停止】按钮，停止学习。

----结束

## 信誉

NIPS信誉包括僵尸网络防护和Web信誉。

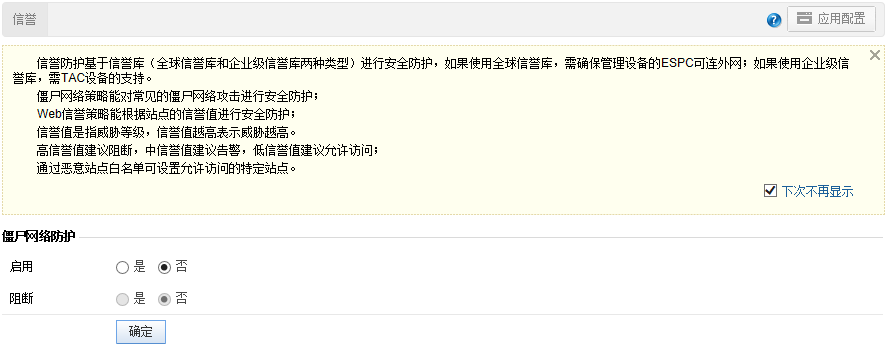
### 僵尸网络防护

僵尸网络主要通过侵入主机植入僵尸程序来构建，其传播方式有远程漏洞攻击、弱口令扫描入侵、邮件附件、恶意文件等，其中网页挂马是主要的传播方式。

NIPS内置先进的僵尸网络检测引擎并结合实时的僵尸网络云规则，对僵尸网络实现“进不来、藏不住、出不去”的防护。“进不来、藏不住、出不去”即僵尸程序无法进入网络传播，如有被感染主机，无法潜伏隐藏并无法对外发起攻击行为和数据泄密行为。

选择菜单 策略 > 信誉 > 信誉，僵尸网络防护区域如图6-18所示。

僵尸网络防护



设置是否启用僵尸网络检测功能。

设置是否阻断僵尸网络连线。

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

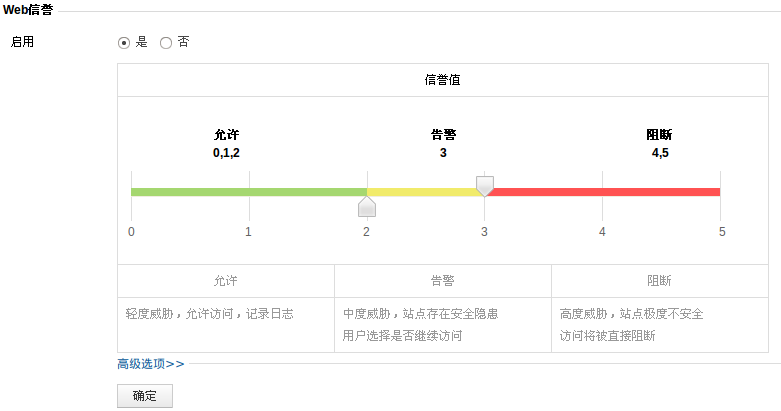
### Web信誉

NIPS设备内置绿盟科技积累多年经验形成的恶意站点库，并支持管理员根据恶意站点库中站点的信誉值灵活设置web信誉策略，从而达到站点过滤的目的。当NIPS设备保护的企业内网中，有访问被植入木马站点的行为发生时，NIPS设备会根据web信誉策略的设置，及时采取告警、阻断或告警并阻断等措施，有效抵御Web安全威胁渗入企业内网，防止潜在的隐私侵犯，保护企业机密信息。

下面介绍如何配置Web信誉。

选择菜单 策略 > 信誉 > 信誉，Web信誉区域如图6-19所示。

Web信誉



启用Web信誉。

配置Web信誉。

鼠标移动上方游标，设置进行告警、阻断的站点信誉值，信誉值的详细描述如表6-8所示。

鼠标移动下方游标，设置允许访问的站点信誉值，信誉值的详细描述如表6-8所示。

单击“高级选项>>”，配置允许访问的站点白名单。

信誉值描述信息

| 信誉值 | 描述 |
| --- | --- |
| 0 | 轻微不良记录，例如少量低威胁行为。 |
| 1 | 少量不良记录，例如多次低威胁行为。 |
| 2 | 一般不良记录，例如少量中威胁行为或大量低威胁行为。 |
| 3 | 中等不良记录，例如多次中威胁行为。 |
| 4 | 严重不良记录，例如少量高威胁行为或大量中威胁行为。 |
| 5 | 极度严重不良记录，例如多次高威胁行为。 |

单击【确定】按钮，完成配置。

----结束

## URL分类过滤策略

URL分类过滤是一种网页过滤功能，NIPS的URL分类过滤策略可以根据源/目的地址、用户、时间、过滤站点等对HTTP的请求报文进行过滤。

NIPS设备可以通过以下3种来源获取URL分类：

* 本地内置：NIPS设备缺省内置了一些系统URL分类规则（每个系统分类规则下均包含了一些过滤站点）；
* 在线服务器获取：从在线服务器上获取更多的URL分类规则；
* 自定义URL分类：管理员根据实际情况手动配置需要过滤的站点URL分类。

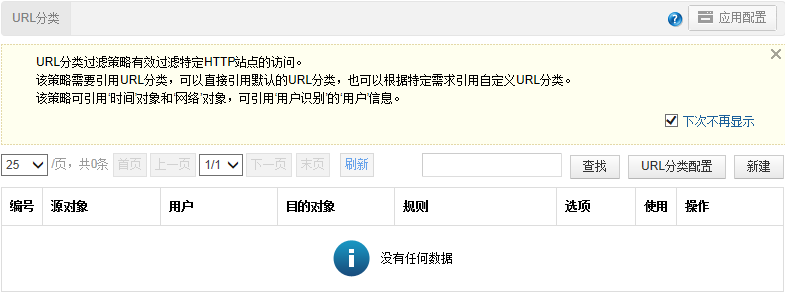
下面主要介绍配置NIPS设备URL分类模式、新建自定义URL分类规则以及URL分类测试。

### 配置URL分类模式

URL分类模式决定了URL过滤策略中可管理的URL分类。

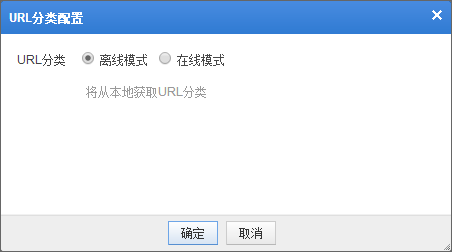
选择菜单 策略 > URL分类 > URL分类，URL分类页面如图6-20所示。

URL分类



单击【URL分类配置】按钮，弹出URL分类模式配置对话框，如图6-21所示。

URL分类模式



选择URL分类模式。

* 离线模式：从NIPS设备本地获取URL分类，主要由内置系统URL分类、自定义URL分类组成。
* 在线模式：从NIPS设备本地以及在线服务器上获取URL分类，主要由内置系统URL分类、自定义URL分类以及服务器上的URL分类组成

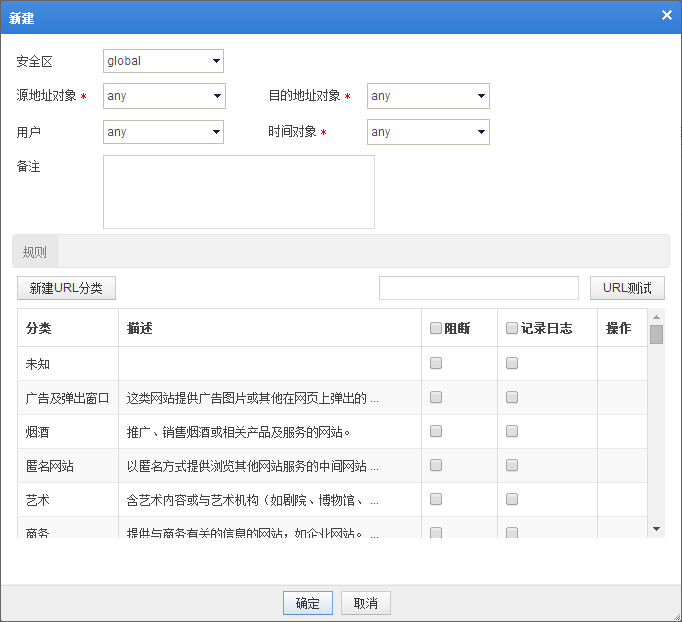
单击【确定】按钮，完成配置。

----结束

### 新建URL过滤策略

在图6-20所示页面中，单击【新建】按钮，弹出新建URL过滤策略对话框，如图6-22所示。

新建URL过滤策略



配置URL过滤策略参数，参数说明如表6-9所示。

URL过滤策略参数

| 配置项 | 描述 |
| --- | --- |
| 安全区 | 对经过哪个安全区的报文应用该URL过滤策略。  如果不指定，表示来自任何安全区的报文均匹配该策略。 |
| 源地址对象 | 对来自哪些地址的报文应用该URL过滤策略。  “any”表示任意地址。 |
| 目的地址对象 | 对发往哪些地址的报文应用该URL过滤策略。  “any”表示任意地址。 |
| 用户 | 应用URL过滤策略的用户对象，分为如下四类：   * any：任意用户。 * 信任用户：在线用户。有关在线用户的介绍，请参见。 * 非信任用户：在线用户IP地址范围之外的其他所有IP地址会被识别为非信任用户。 * 自定义用户：从AD域配置器获取到的用户列表中选择的用户，有关AD域配置器的介绍请参见。 |
| 时间对象 | URL过滤策略生效的时间段。  “any”表示所有时间。 |
| 备注 | URL过滤策略的描述信息。 |
| 规则 | URL过滤策略中包含的URL分类以及对URL分类的处理方法。可选处理方法有：阻断和记录日志。 |

单击【确定】按钮保存配置。

应用配置，使配置生效。

----结束

### 新建自定义URL分类规则

自定义分类规则用于管理员根据实际需要手动添加一些过滤站点，如果系统内置的分类规则可以满足需求，可以忽略该操作。

在图6-22所示页面中，单击【新建URL分类】按钮，弹出新建自定义URL分类对话框，如图6-23所示。

新建URL分类



配置自定义URL分类规则，参数如表6-10所示。

自定义URL分类参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 新建自定义URL分类的名称。 |
| 描述 | 新建自定义URL分类的描述信息。 |
| 域名 | 新建自定义URL分类中包含的站点域名。 |
| 关键字 | 新建自定义URL分类中的站点域名匹配的关键字或正则表达式。  多个关键字或正则表达式用换行分隔。 |

|  |  |
| --- | --- |
| 注意 | 网址对于系统具有唯一性，当一个网址写入自定义分类后，就不再存在于URL过滤库的系统分类中。 |

单击【确定】按钮，保存配置。

----结束

### URL测试

NIPS内置系统默认的URL分类库，通过URL测试功能，管理员可以快捷地在URL分类库中查找到某个URL属于哪个分类。对于属于“其他”的URL，用户可以自定义URL分类对其进行分类，自定义URL分类的操作请参见，下面介绍如何通过URL测试进行URL所属分类查询。

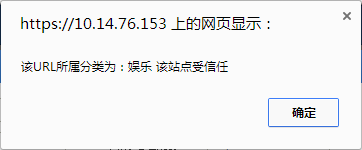
在图6-22所示页面中，在【URL测试】按钮左侧文本框中输入待查询的URL，如图6-24中的“www.youku.com”。

URL测试



单击【URL测试】按钮，系统弹出提示框以显示该URL所属分类，如图6-25所示。

URL测试结果



单击提示框的【确定】按钮，完成测试操作。

----结束

## 防病毒策略

防病毒策略可帮助NIPS设备实现病毒防护的安全防护功能，设置病毒白名单可以实现对某些特殊病毒文件的放行。管理员可以对防病毒策略进行新建、编辑、删除、排序以及复制的操作。下面介绍管理员如何新建防病毒策略。

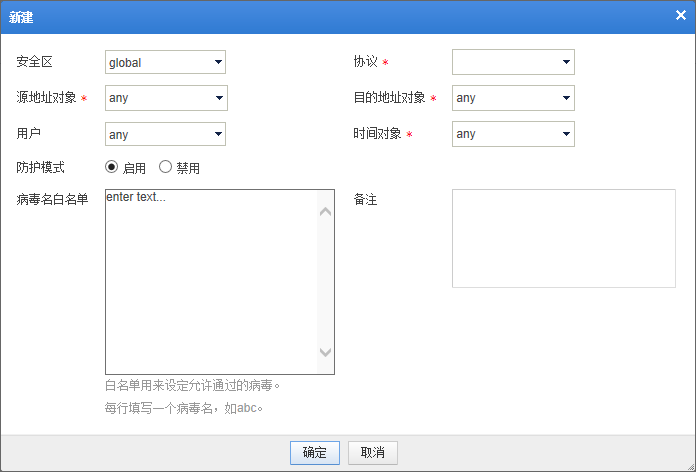
选择菜单 策略 > 防病毒 > 防病毒策略，进入防病毒策略页面，如图6-26所示。

防病毒策略



单击【新建】按钮，弹出新建防病毒策略对话框，如图6-27所示。

新建防病毒策略



配置防病毒策略参数，参数说明如表6-11所示。

防病毒策略参数

| 配置项 | 描述 |
| --- | --- |
| 安全区 | 对经过哪个安全区的报文应用该防病毒策略。  “global”表示来自任何安全区的报文均匹配该策略。 |
| 协议 | 对那个协议报文应用该防病毒策略。可选项有：http、ftp、smtp、pop3、imap。 |
| 源地址对象 | 对来自哪些地址的报文应用该防病毒策略。“any”表示任意地址。 |
| 目的地址对象 | 对发往哪些地址的报文应用该防病毒策略。“any”表示任意地址。 |
| 用户 | 防病毒策略的用户对象，分为如下四类：   * any：任意用户。 * 信任用户：在线用户。有关在线用户的介绍，请参见。 * 非信任用户：在线用户IP地址范围之外的其他所有IP地址会被识别为非信任用户。 * 自定义用户：从AD域配置器获取到的用户列表中选择的用户，有关AD域配置器的介绍请参见。 |
| 时间对象 | 防病毒策略生效的时间段。“any”表示所有时间。 |
| 病毒名白名单 | 白名单中的病毒名不会被防病毒引擎扫描。多个病毒名之间用换行分隔。 |
| 备注 | 防病毒策略的描述信息。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

## 用户管理策略

NIPS支持对用户进行认证，认证方式包括本地认证、第三方服务器认证，其中第三方服务器认证包括：

* AD域认证
* RADIUS认证
* EPS联动认证
* LDAP认证

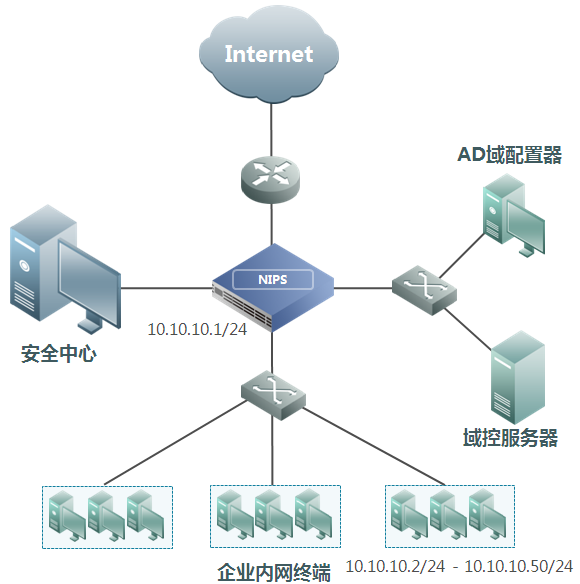
本节将主要介绍如何配置第三方认证服务器、用户认证方式、用户识别规则以及用户认证策略。

### 服务器配置

下面主要介绍如何在NIPS设备中配置认证服务器。

对于AD域认证方式来说，内网用户是由AD域服务器进行管理的，NIPS设备通过AD域配置器定期获取在线用户信息以及每个用户对应的IP地址等信息，其具体网络拓扑如图6-28所示。

AD域认证拓扑图



使用AD域认证方式前，AD域配置器必须已经安装完成，以便管理AD域服务器获取到的用户信息，具体操作请参见，然后还需要在NIPS上配置以下信息：

* 配置AD域服务器，请参见本节下述内容。
* 配置AD域服务器的用户列表更新方式，请参见。

NIPS设备中配置认证服务器的操作如下。

以缺省操作员weboper帐号登录设备后，选择菜单 策略 > 用户管理 > 服务器配置，进入认证服务器配置页面，如图6-29所示。

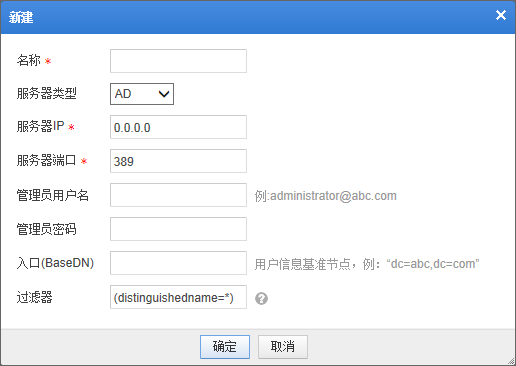
服务器配置



单击【新建】按钮，弹出新建认证服务器对话框。

不同类型认证服务器的参数有所不同，AD域认证服务器的配置页面如图6-30所示；Radius认证服务器的配置页面如图6-31所示；EPS联动服务器的配置页面如图6-32所示；LDAP认证服务器的配置页面如图6-33所示。

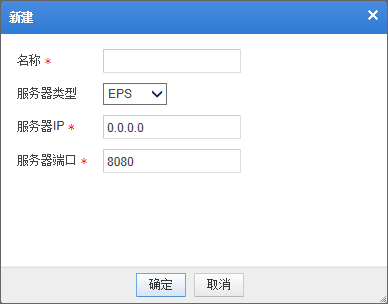
配置AD域认证服务器



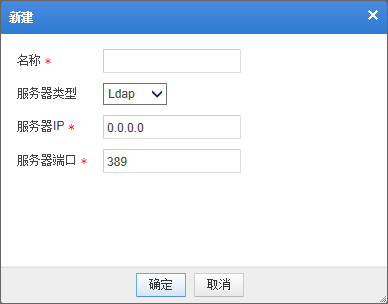
配置Radius认证服务器



配置EPS联动服务器



配置LDAP认证服务器



配置服务器参数，参数说明如表6-12所示。

服务器参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 认证服务器的名称。  不能和已有服务器配置重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。 |
| 服务器类型 | 认证服务器的类型，包括AD、Radius、EPS和Ldap。   * AD：认证服务器的认证类型为AD域认证。 * Radius：认证服务器的认证类型为Radius认证。、 * EPS：配置NIPS与NSFOCUS EPS的联动功能。开启EPS联动功能后，客户端将自动跳转到EPS的认证页面，并在下载Agent后由EPS对客户端进行认证。   表格中说明   * NIPS与NSFOCUS EPS进行联动时，必须使用纯管理口或可管理的工作口。 * 如需了解EPS产品的详细功能，请联系绿盟科技的技术支持人员。 * Ldap：认证服务器类型为Ldap认证。 |
| 服务器IP/端口 | 认证服务器或联动服务器NSFOCUS EPS的IP地址和端口信息。 |
| 管理员用户名/管理员密码 | 登录AD域服务器的用户名/密码。  表格中说明  只有AD域认证方式下才需要配置这两个参数。 |
| 入口 | 用户信息基准节点。  表格中说明  只有AD域认证方式下才需要配置该参数。 |
| 过滤器 | 缺省为“(distinguishedname=\*)”，表示可以获取全部用户列表。其他更高级的用法请参见LDAP Search Filter 的相关语法。  表格中说明  只有AD域认证方式下才需要配置该参数。 |
| 认证方式 | Radius认证服务器的认证方式。可选值：pap、spap、chap、mschapv1、mschapv2、eap\_md5。  表格中说明  只有Radius认证方式下才需要配置该参数。 |
| 认证共享密钥 | Radius认证服务器的认证共享密钥。  表格中说明   * NIPS中配置的认证共享密钥必须与Radius服务器中的配置一致，否则NIPS和服务器之间无法通信。 * 只有Radius认证方式下才需要配置该参数。 |

单击【确定】按钮保存配置。

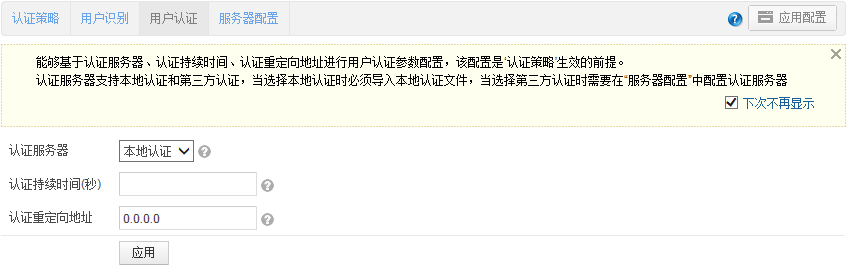
----结束

### 用户认证

用户认证配置完成后，将自动重启引擎。NIPS设备中选择认证服务器及相关认证参数的配置如下。

选择菜单 策略 > 用户管理 > 用户认证，进入用户认证配置页面，如图6-34所示。

用户认证



配置用户认证参数，参数说明如表6-13所示。

用户认证参数

| 配置项 | 描述 |
| --- | --- |
| 认证服务器 | 选择认证服务器，包括本地认证和配置的第三方认证服务器。  开启本地认证之前，必须导入本地认证文件，具体导入方法请参见。 |
| 认证持续时间（秒） | 认证的持续时间。  对于与EPS联动，认证持续时间必须大于EPS中配置的认证时间间隔。 |
| 认证重定向地址 | 客户端进行认证时，NIPS将客户端的认证页面重定向到“认证重定向地址”表示的页面。  表格中说明  该地址必须是NIPS设备管理口的IP地址或者可管理的工作口的IP地址，并且在客户端访问网络时，该地址必须可达。 |

单击【应用】按钮，保存配置。

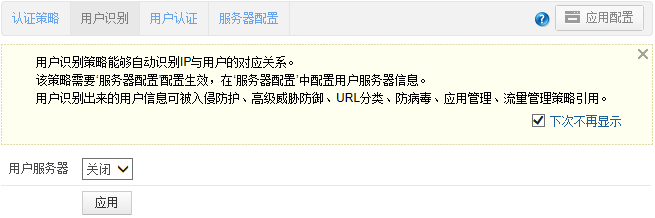
----结束

### 用户识别

目前，NIPS支持基于AD域服务器的用户识别功能。根据管理员的配置，可以由系统自动更新用户列表，或者由管理员手动更新用户列表。该功能的配置步骤如下所示：

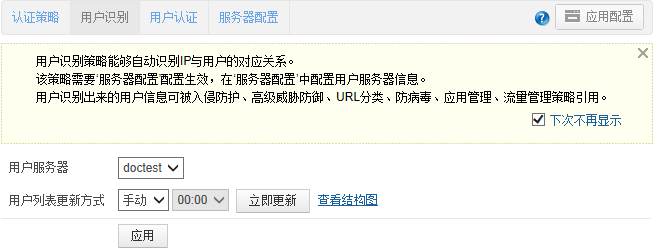
选择菜单 策略 > 用户管理 > 用户识别，进入用户识别配置页面，默认情况下，用户服务器处于关闭状态，如图6-35所示。

用户识别 – 关闭状态



选择AD域认证服务器。选择AD域类型的第三方认证服务器后，界面如图6-36所示。

用户识别 – 配置参数



配置用户列表更新方式（手动更新或者定期自动更新）。

* 如果选择“手动”，表示由管理员手动更新用户列表；
* 如果选择“每天”、“周一”、“周二”、“周三”、“周四”、“周五”、“周六”、“周日”，还需要配置具体的更新时间，表示由系统定期自动更新用户信息。

单击【应用】按钮，保存配置。

应用配置，使配置生效。

（可选）单击【立即更新】按钮，可以立即手动将AD域控制器中保存的用户列表更新到NIPS设备中。

（可选）单击“查看结构图”链接，可以查看当前用户列表的树形结构图。

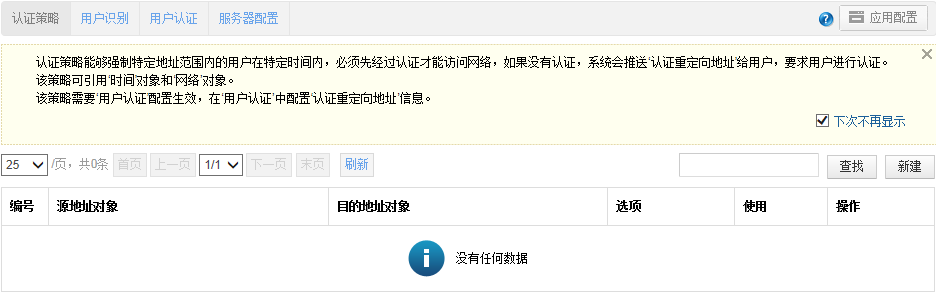
----结束

### 认证策略

当用户传输的数据包匹配到认证策略时，系统将对该用户进行认证。配置用户认证的操作请参见，本节主要介绍如何新建认证策略。

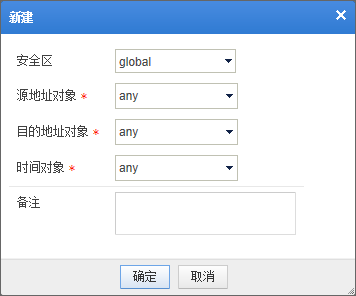
选择菜单 策略 > 用户管理 > 认证策略，进入认证策略管理页面，如图6-37所示。

用户管理 – 认证策略



单击【新建】按钮，弹出新建认证策略对话框，如图6-38所示。

用户管理 – 新建认证策略



配置认证策略参数，参数说明如表6-14所示。

认证策略参数

| 配置项 | 描述 |
| --- | --- |
| 安全区 | 对经过哪个安全区的报文应用该认证策略。  如果不指定，表示来自任何安全区的报文均匹配该策略。 |
| 源地址对象 | 指对来自哪些地址的报文应用该认证策略。  “any”表示任意地址。 |
| 目的地址对象 | 指对发往哪些地址的报文应用该认证策略。  “any”表示任意地址。 |
| 时间对象 | 该认证策略生效的时间段。  “any”表示所有时间。 |
| 备注 | 认证策略的描述信息。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

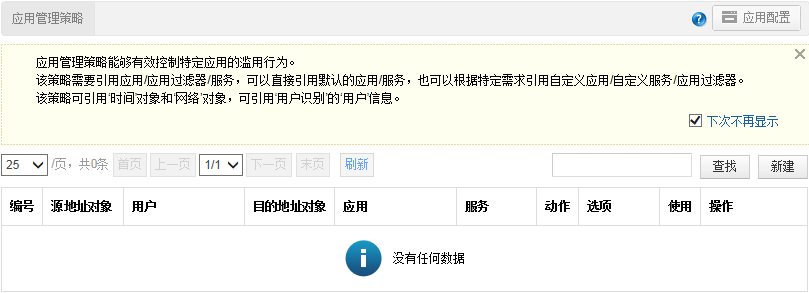
## 应用管理策略

通过执行应用管理策略，NIPS可以基于应用或服务对流经设备的数据包进行控制，包括允许、阻断和进行日志告警。

本节主要介绍如何新建应用管理策略。

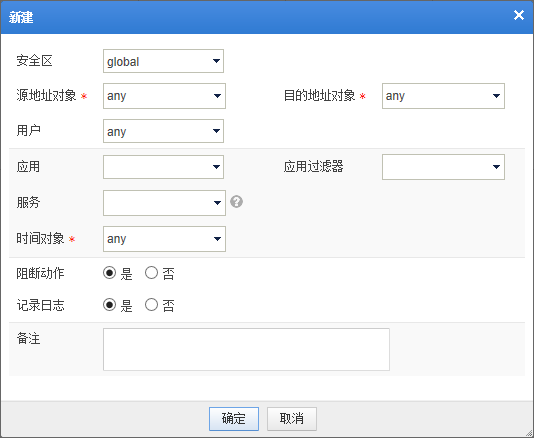
选择菜单 策略 > 应用管理 > 应用管理策略，进入应用管理策略页面，如图6-39所示。

应用管理策略



单击【新建】按钮，弹出新建应用管理策略对话框，如图6-40所示。

新建应用管理策略



配置应用管理策略参数，参数说明如表6-15所示。

应用管理策略参数

| 配置项 | 描述 |
| --- | --- |
| 安全区 | 对经过哪个安全区的报文应用该应用管理策略。  如果不指定，表示来自任何安全区的报文均匹配该策略。 |
| 源地址对象 | 指对来自哪些地址的报文应用该应用管理策略。  “any”表示任意地址。 |
| 目的地址对象 | 指对发往哪些地址的报文应用该应用管理策略。  “any”表示任意地址。 |
| 用户 | 应用管理策略的用户对象，分为如下四类：   * any：任意用户。 * 信任用户：在线用户。有关在线用户的介绍，请参见。 * 非信任用户：在线用户IP地址范围之外的其他所有IP地址会被识别为非信任用户。 * 自定义用户：从AD域配置器获取到的用户列表中选择的用户，有关AD域配置器的介绍请参见。 |
| 应用 | 该策略要匹配的应用对象。  配置应用对象的操作请参见和。  表格中说明  至少需要配置应用、应用过滤器或服务中的一种参数。 |
| 应用过滤器 | 通过选择应用过滤器，指定该策略要匹配的符合过滤条件的应用对象。  配置应用过滤器的操作请参见。  表格中说明  至少需要配置应用、应用过滤器或服务中的一种参数。 |
| 服务 | 应用管理策略要匹配的服务对象。  表格中说明  至少需要配置应用、应用过滤器或服务中的一种参数。 |
| 时间对象 | 应用管理策略要匹配的时间对象。  “any”表示所有时间。 |
| 阻断动作 | 是否阻断匹配到该应用管理策略的报文。 |
| 记录日志 | 是否记录日志。  如果选择了记录日志，则当报文匹配到该应用管理策略时，将记录日志。 |
| 备注 | 应用管理策略的描述信息。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

## 流量管理策略

流量管理策略用于限制通道流量，控制授权用户流量许可和优先级，实现网络资源的合理利用，使得网络中不同类型的流量的比例和分布更为合理。同时结合最小带宽、最大带宽和会话限制，有效保证关键带宽的畅通。

NIPS系统的流量管理策略包括流量管理策略和流量分析策略。

流量管理策略和流量分析策略的配置思路如下所示：

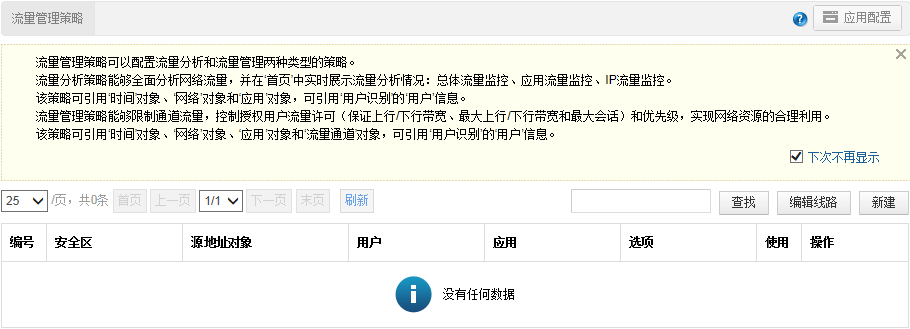
* + - * 1. 配置流量通道对象（请参见）。
        2. 配置流量通道线路。
        3. 新建流量管理策略/流量分析策略。
        4. 应用配置。

### 流量管理策略

下面介绍如何新建流量管理策略。

选择菜单 策略 > 流量管理 > 流量管理策略，进入流量管理策略页面，如图6-41所示。

流量管理策略



（可选）新建流量通道线路。

管理员也可选择不添加线路，使用系统默认线路。

单击【编辑线路】按钮，弹出新建流量通道线路对话框，如图6-42所示。

新建流量通道线路



单击图标，新增一条新的流量线路。

配置流量通道线路参数，参数说明如表6-16所示。

流量通道线路参数

| 配置项 | 描述 |
| --- | --- |
| 名称 | 流量通道线路名称。 |
| 上行流量总和（Kbps） | 线路上行流量总和必须大于该线路中所有策略的流量通道的保证上行带宽的总和。 |
| 下行流量总和（Kbps） | 线路下行流量总和必须大于该线路中所有策略的流量通道的保证下行带宽的总和。 |
| 备注 | 流量通道线路的描述信息。 |

|  |  |
| --- | --- |
| 注意 | 同时需要修改 系统 > 系统配置 > 专业参数 中的相关参数，配置才会生效。 |

单击【确定】按钮，保存配置返回流量管理策略列表。

新建流量管理策略。

单击【新建】按钮，弹出添加流量管理策略的页面，如图6-43所示。

添加流量管理策略



配置流量管理策略参数，参数说明如表6-17所示。

流量管理规则主要参数

| 配置项 | 描述 |
| --- | --- |
| 线路 | 限定流量通道的线路，只对流量管理策略生效。 |
| 策略设置 | 策略类型，这里选择流量管理。   * 流量分析：对源地址对象的相关服务的流量进行分析。 * 流量管理：执行流量管理策略，限制通道流量。 |
| 流量通道 | 流量通道对象，只对流量管理策略生效。 |
| 安全区/源地址对象 | 上行流量的安全区和地址对象。  表格中说明   * 当源安全区设置为global或direct时，不能选择any做为其源地址对象。 * 每个IP只对流量管理策略生效。勾选后，将只对源地址对象的每个IP地址做流量控制；不勾选，将只对源地址对象整体做流量控制。 |
| 用户 | 流量管理策略的用户对象。 |
| 应用 | 流量管理策略要匹配的应用对象。 |
| 时间对象 | 流量管理策略的生效时间。 |
| 备注 | 流量管理策略的描述信息。 |

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

### 流量分析策略

流量分析策略用于对网络流量进行数据分析。管理员可以对流量分析策略进行查找、新建、编辑、删除以及排序的操作。下面介绍管理员如何新建流量分析策略。

执行至。

新建流量分析策略。

单击【新建】按钮，弹出新建流量分析策略对话框，如图6-44所示。

新建流量分析策略



配置流量分析策略参数，参数说明如表6-16所示。

单击【确定】按钮，保存配置。

应用配置，使配置生效。

----结束

# 日志报表

本章主要包括以下内容：

| 功能 | 描述 |
| --- | --- |
| 日志分析 | 介绍日志配置和查看各类日志的方法。 |
| 统计报表 | 介绍报表配置和查看各类报表的方法。 |

## 日志分析

日志分析主要操作包括日志配置和日志查看。

管理员可以设置条件，对NIPS的各类日志进行查询，从中发现攻击者的蛛丝马迹和防护网络的实时情况，及时调整防护策略，做到更有效的网络或服务器的安全防护。

NIPS设备最多能够存储最近时间内的10000条日志，界面最多能够显示最近时间内的1000条日志，设备重启后日志将被清空。

### 日志配置

系统日志支持以下配置：

* 日志查询

设置日志的查询条件时，可以根据时间范围、动作、协议、端口、地址等关键字（不同日志的查询条件各有不同，请以实际界面为准）进行查询。

* 导出日志

查询日志以后，还可以将查询结果导出，以便于进一步的统计分析。在日志列表页面，分别单击图标html、word、即可将当前日志按照HTML、WORD、EXCEL格式保存到本地。

* 清空数据

单击日志列表右上方的【清空数据】按钮，可将当前日志内的所有数据删除，删除无法恢复。一般情况下，建议将报表内容下载后再清空数据。

* 打印日志

在日志列表页面，单击图标print即可将当前日志打印出来。打印之前，请确认打印机已正常连接。

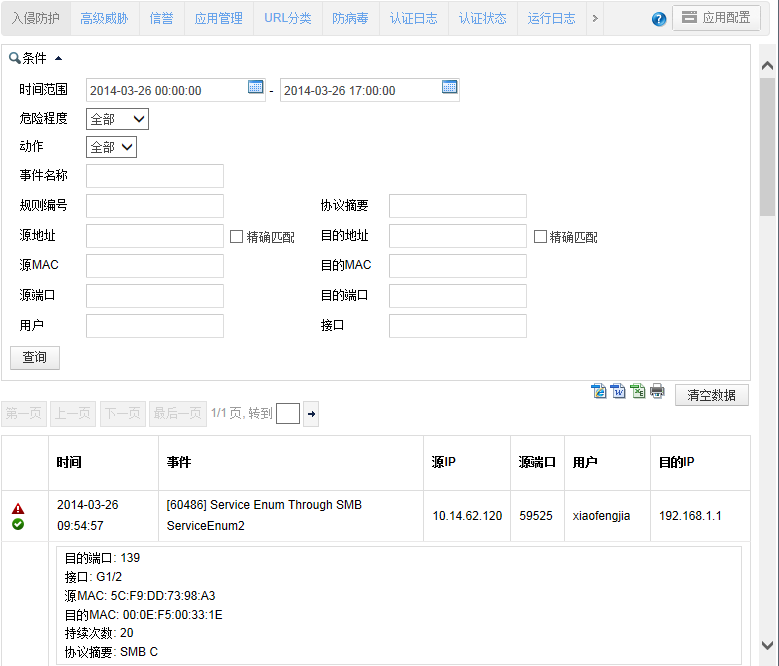
### 日志查看

通过查看各类日志，可以方便管理员对各类事件进行分析。下面介绍NIPS系统中各类日志的查看方法。

#### 查看入侵防护日志

选择菜单 日志报表 > 日志分析 > 入侵防护，入侵防护日志的查询条件及结果显示页面如图7-1所示。

入侵防护日志



#### 查看高级威胁日志

选择菜单 日志报表 > 日志分析 > 高级威胁，高级威胁日志的查询条件及结果显示页面如图7-2所示。

高级威胁日志



#### 查看信誉日志

选择菜单 日志报表 > 日志分析 > 信誉，信誉日志的查询条件及结果显示页面如图7-3所示。

信誉日志



#### 查看应用管理日志

选择菜单 日志报表 > 日志分析 > 应用管理，应用管理日志查询后的页面如图7-4所示。

应用管理日志



#### 查看URL分类日志

选择菜单 日志报表 > 日志分析 > URL分类日志，URL分类日志查询后的页面如图7-5所示。

URL分类日志



#### 查看防病毒日志

通过查看防病毒日志，可以帮助管理员检查网络中传输的病毒信息，包括病毒源地址、目的地址和协议摘要等。

选择菜单 日志报表 > 日志分析 > 防病毒，防病毒日志查询后的页面如图7-6所示。

防病毒日志

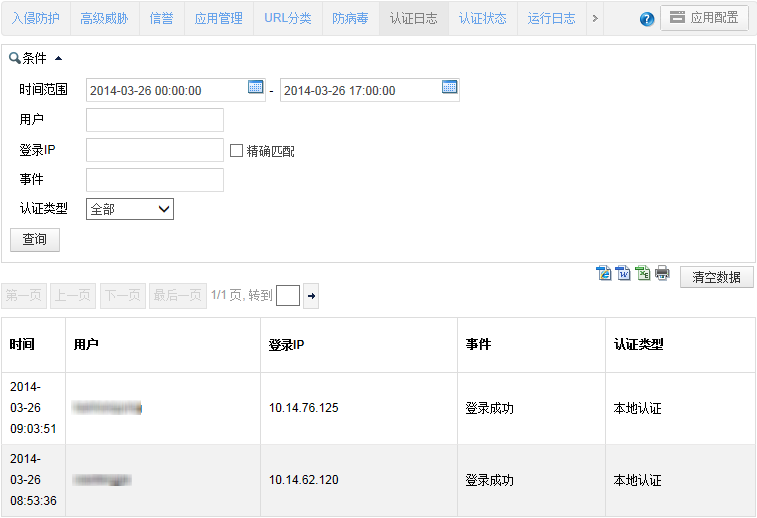


#### 查看认证日志

通过查看认证日志，可以帮助管理员管理网络通信时使用的认证方式。

选择菜单 日志报表 > 日志分析 > 认证日志，认证日志查询后的页面如图7-7所示。

认证日志



#### 查看认证状态日志

选择菜单 日志报表 > 日志分析 > 认证状态，认证状态日志查询后的页面如图7-8所示。

认证状态日志

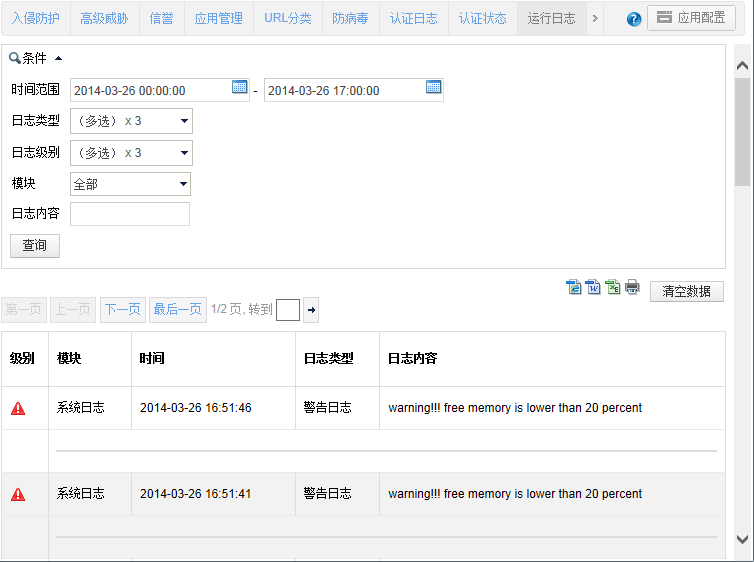


#### 查看运行日志

通过查看运行日志，管理员可以对三种日志级别（正常、警告和严重）、三种日志类型（警告、运行和调试）的接口状态日志、高可用性日志、系统日志以及bypass日志进行过滤查看。

选择菜单 日志报表 > 日志分析 > 运行日志，运行日志查询后的页面如图7-9所示。

运行日志

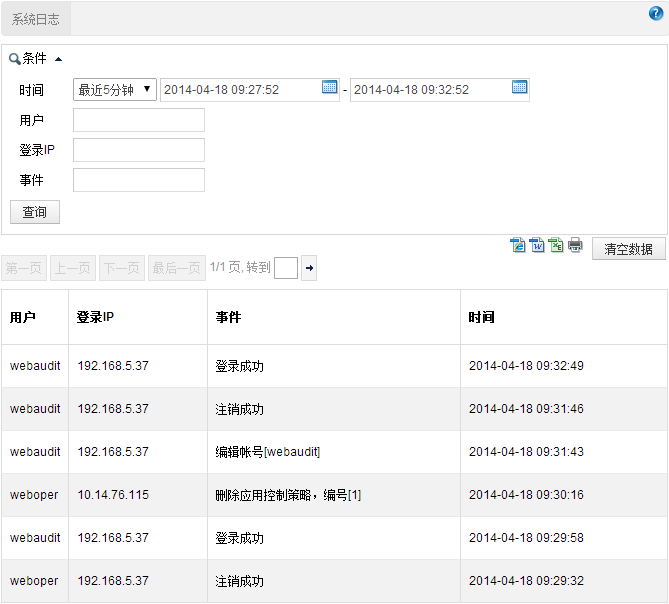


#### 查看系统日志

只有审计员（缺省审计员的用户名和密码均为webaudit）才有查看系统日志的权限。系统日志包括所有登录日志、操作日志和系统启动日志。

选择菜单 日志报表 > 日志分析 > 系统日志，系统日志查询后的页面如图7-10所示。

系统日志



## 统计报表

下面通过介绍报表配置方法和报表详情来介绍NIPS的统计报表。

### 报表配置

系统报表支持以下配置：

* 报表查询

设置报表的查询条件时，可以根据报表类型（日报表、周报表、月报表和年报表）和接口名称关键字进行查询。

* 导出报表

查询报表以后，还可以将查询结果导出，以便于进一步的统计分析。在报表页面，分别单击图标html、word、即可将当前报表按照HTML、WORD、EXCEL格式保存到本地。

* 打印报表

在报表页面，单击图标即可将当前报表打印出来。打印之前，请确认打印机已正常连接。

### 报表详情

在各类报表中，根据指定的查询条件，可以查看符合条件的各类事件的统计图表，统计信息如表7-1所示。

各类事件统计信息

| 类型 | 统计内容 |
| --- | --- |
| 入侵防护统计报表 | 包括全部事件的源/目的地址Top10、阻断事件的源/目的地址Top10、全部事件Top10和阻断事件Top10。 |
| 高级威胁统计报表 | 包括全部事件的总览、非法外联事件的源/目的地址Top10、敏感数据的事件分布、敏感数据的源/目的地址Top10、敏感数据的源/目的地址阻断事件Top10、文件识别的文件类型事件分布、文件识别的源/目的地址Top10、文件识别的源/目的地址阻断事件Top10。 |
| 应用管理统计报表 | 包括全部事件和阻断事件的源/目的地址Top10、用户Top10、应用Top10。 |
| 信誉统计报表 | 包括以下3方面信息：   * 信誉概况：事件类型和事件动作各自发生次数和所占比例。 * web信誉：全部事件和阻断事件的源地址Top10、域名Top10、用户访问Top10。 * 僵尸网络：全部事件和阻断事件的源地址Top10、僵尸网络服务器Top10、用户访问Top10。 |
| URL分类统计报表 | 包括全部事件和阻断事件的源/目的地址Top10、分类访问Top10、站点访问Top10。 |
| 防病毒统计报表 | 包括全部事件的源/目的地址Top10、阻断事件的源/目的地址Top10、病毒名称的Top10。 |

# Console管理

通过连接Console口，串口管理员conadmin可以访问NIPS引擎的串口管理界面，进行系统初始配置、状态检测和恢复初始化配置等功能。当Web管理界面中出现故障无法登录时，或在Web界面无法进行管理的部分，可以通过串口对NIPS进行管理操作。

本章主要内容如下：

| 功能 | 描述 |
| --- | --- |
| 查看系统信息 | 介绍如何查看系统软件、硬件及其他基本信息。 |
| 诊断工具 | 介绍控制台界面中可用的网络调试工具。 |
| 维护工具 | 介绍控制台界面可操作的系统维护功能。 |
| 系统初始化 | 介绍如何还原系统出厂配置。 |
| 重新启动系统 | 介绍如何重启系统硬件。 |
| 关闭系统 | 介绍如何关闭系统硬件。 |
| 退出配置界面 | 介绍如何退出控制台管理界面及注意事项。 |

## 查看系统信息

如图8-1所示，管理员可以进行以下操作：

* 显示接口设置

查看系统当前所有网络接口的信息，包括接口名称、接口IP、接口管理IP和所属安全区（引擎各网络接口的设置仅能在Web管理界面中修改，具体操作方法请参见）。

* 显示证书信息

查阅NIPS的引擎证书，包括证书状态、证书类型、颁发日期、截止日期等。

* 设置接口IP地址

设置管理接口M或H1的IP地址，以供管理员登录设备后对设备进行管理。

* 启动重要进程

启动重要进程，保证设备正常运行。

* 设置系统时钟

设置系统时钟，以供通讯和日志记录时使用。

* 设置系统时区

设置系统时区，方便引擎位于其他时区时的使用（默认为东8时区，取值范围为-12到12）。

* 硬件特征值

硬件特征值是每台网络引擎的唯一标识，在为其制作证书时需要获取该值。

* 产品状态值

该值是提供给绿盟科技工程人员使用的内部口令，每天会变化一次。

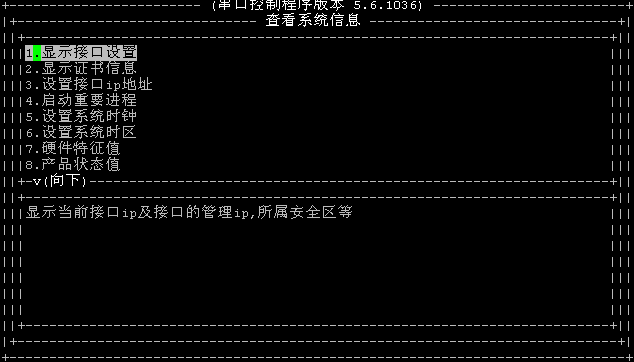
* 产品版本信息

显示当前引擎版本和引擎固件版本的详细信息。

* 返回上级菜单

返回到上一级配置菜单中。

引擎串口管理 – 查看系统信息



|  |  |
| --- | --- |
| 说明 | NIPS出厂时未配置证书，可以通过引擎的Web管理界面进行证书导入。有关导入引擎证书的操作方法，请参见。 |

## 诊断工具

如图8-2所示，此处包括UNIX标准下的一些系统诊断工具，管理员可利用它们检查网络状况和排除系统安装中的困难。管理员可以进行以下操作：

* Ping

查看引擎与目标IP地址的网络连接状态。

* 追踪路线

查看引擎和指定IP地址间的路由状况。

* 网络状态

查看引擎当前的网络连接情况。

* 显示路由信息

查看引擎当前的路由表信息。

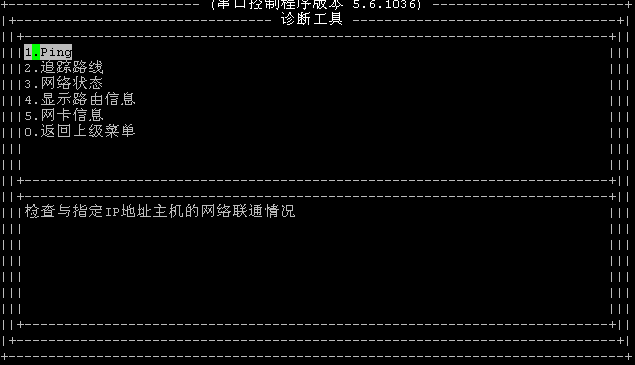
* 网卡信息

查看引擎的网卡信息。

* 返回上级菜单

返回到上一级配置菜单中。

引擎串口管理 – 诊断工具



|  |  |
| --- | --- |
| 说明 | 管理员也可以在NIPS引擎的Web管理中使用诊断工具，相关操作方法请参见。 |

## 维护工具

如图8-3所示，管理员可以进行以下操作：

* 设置管理员密码

设置引擎管理界面登录帐号conadmin的密码（请妥善保管此密码，如果忘记，将不能通过串口配置系统，必须联系绿盟科技的技术支持人员重置密码）。

* 设置CLI管理员密码

设置CLI管理界面登录帐号shell的密码（请妥善保管此密码，如果忘记，将不能通过CLI管理界面配置动态路由，必须联系绿盟科技的技术支持人员重置密码）。

* 重置Web用户

重置Web管理模式下的系统管理员信息，其中，系统的两个缺省管理员（weboper和webaudit）的密码等信息被重置；自定义的管理员信息全部被删除。

* 清空临时文件

清除引擎在运行中产生的临时文件（一般情况下，不建议清空临时文件。执行此项操作后，若出现无法正常使用Web管理或其他问题，请重启NIPS引擎系统，以保证正常使用）。

* 关闭/开启远程协助

远程协助默认关闭，按回车键可修改为开启状态（如需关闭，请再次按回车键）。

* 禁止/开启Ping（Icmp）

Ping（Icmp）默认开启，按回车键可修改为禁止状态（如需开启，请再次按回车键）。

* 关闭强制硬件bypass

仅用于关闭强制硬件bypass（重启系统后该设置生效），完成此操作之后必须存储当前设置。在此不提供开启强制硬件Bypass功能。

* 返回上级菜单

返回到上一级配置菜单中。

引擎串口管理 – 维护工具



## 系统初始化

如图8-4所示，初始化NIPS的配置，系统会将程序文件或全部数据恢复到初始状态，包括密码和配置。管理员可以进行以下操作：

* 初始化配置

将所有配置初始化为出厂状态（其中，系统时钟和对象配置文件不会改变），但硬件证书会被删除，初始化配置之前，请确认证书的副本是否已经保存，并在配置完成后重启浏览器。

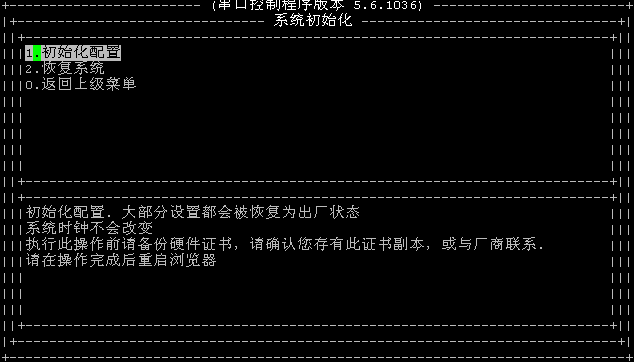
* 恢复系统

所有程序和设置都会被恢复为出厂状态。

* 返回上级菜单

返回到上一级配置菜单中。

引擎串口管理 – 系统初始化



|  |  |
| --- | --- |
| 说明 | 执行初始化配置后，需要重启系统才能生效。 |

## 重新启动系统

如图8-5所示，选择【是】即可重新启动NIPS系统；选择【否】，则返回到当前菜单。

引擎串口管理 – 重新启动系统



## 关闭系统

如图8-6所示，选择【是】即可关闭NIPS系统，设备只关机，不断电；选择【否】，则返回到当前菜单。

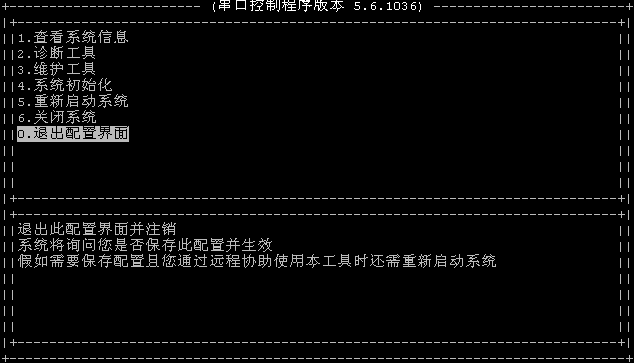
引擎串口管理 – 关闭系统



## 退出配置界面

NIPS引擎各项配置完毕，将光标移到0.退出配置界面，按回车键将退出NIPS引擎串口配置界面，如图8-7所示。

引擎串口管理 – 退出系统



退出控制台管理界面时，配置界面自动注销并保存所有配置并使其生效。退出后如需再次配置，请重新登录。

1. 缩略语

| 缩写 | 英文全称 | 中文全称 |
| --- | --- | --- |
| ARP | Address Resolution Protocol | 地址解析协议 |
| CSRF | Cross-site request forgery | 跨站请求伪造 |
| CGI | Common Gateway Interface | 公共网关接口 |
| CSS/XSS | Cross Site Scripting | 跨站脚本攻击 |
| DDoS | Distributed Denial of Service | 分布式拒绝服务攻击 |
| DNS | Domain Name System | 域名解析系统 |
| HA | High Availability | 高可用性 |
| HTTP | Hyper Text Transfer Protocol | 超文本传输协议 |
| IDC | Internet Data Center | 国际数据中心 |
| NAT | Network Address Translation | 网络地址转换 |
| IP | Internet Protocol | 网络互连的协议 |
| MAC | Media Access Control | 介质访问控制 |
| NIPS | Network Intrusion Prevention System | 网络入侵防护系统 |
| ESPC | Enterprise Security Planning Customer | 绿盟科技企业安全中心 |
| SSL | Secure Sockets Layer | 安全套接层 |
| SQL | Structured Query Language | 结构化查询语言 |
| URL | Uniform Resource Locator | 统一资源定位符 |

1. 管理AD域配置器

当NIPS上配置了AD域服务器，并在AD域服务器或NSFOCUS ESPC所在的主机上安装AD域配置器（即用户管理配置工具），并进行适当配置后，NIPS可以通过AD域配置器获取AD域中已登录用户信息。

* 1. 安装AD域配置器

在开始安装之前，需准备如下内容：

* 准备一台域成员PC或域控服务器。
* 创建用户。在AD域服务器上创建一个用户，并为该用户分配日志访问权限。
* 获取安装软件。请联系绿盟科技的技术支持人员获取该软件。

AD域配置器的安装步骤如下：

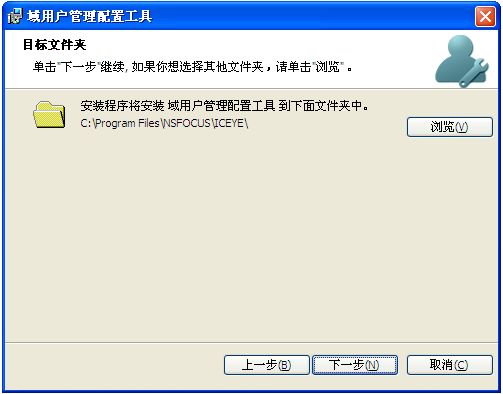
双击setup.exe文件，启动安装向导，如图 B-1所示。

启动安装文件



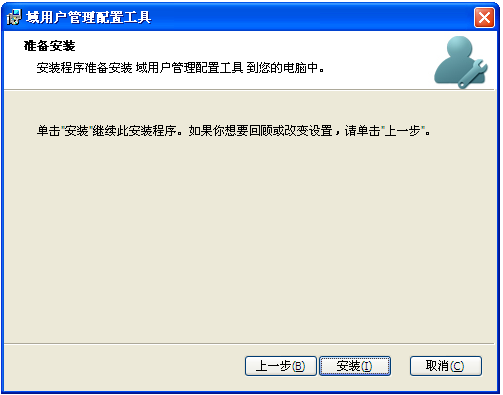
单击【下一步】，选择安装路径，如图 B-2所示为默认的安装路径。

选择安装路径



单击【下一步】，准备安装软件，如图 B-3所示。单击【安装】，开始安装。

开始安装



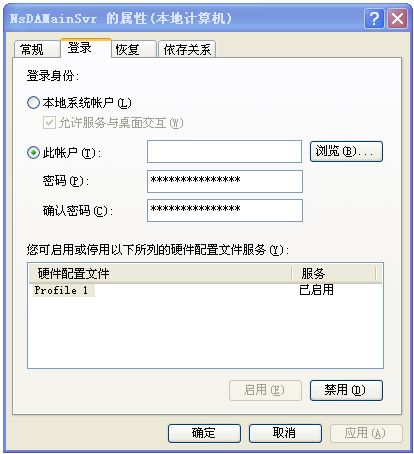
安装完毕，单击【完成】，完成安装，如图 B-4所示。

安装完毕



安装AD域配置器后，还必须配置NsDomainSvr服务。选择菜单 控制面板 > 性能和维护 > 管理工具 > 服务，配置NsDomainSvr服务的启动帐户为安装AD域配置器之前创建的用户，如图 B-5所示。

配置NsDomainSvr服务



* 1. 配置AD域配置器

AD域配置器有如下两种工作类型：

* 扫描器

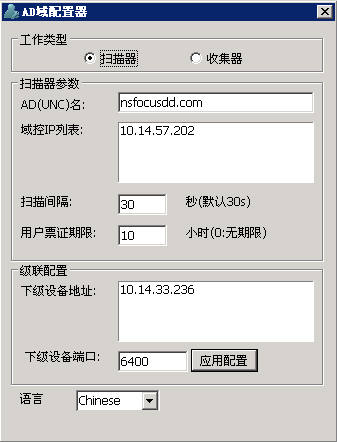
定时从AD域服务器的安全日志中扫描一定时间范围内的已登录用户列表，并通过指定方式发送给NIPS设备。如果有多个扫描器复用时，也可发送日志给指定的收集器。

* 收集器

定时将收到的扫描器扫描的用户列表整合过滤，统一发送给NIPS设备。

成功安装并配置AD域配置器工具后，双击桌面的快捷方式，登录操作界面，如图 B-6所示。

AD域配置器的配置



配置AD域配置器参数，参数说明如表B-1所示。

AD域配置器参数

| 配置项 | 描述 |
| --- | --- |
| AD（UNC）名 | AD服务器的域名。 |
| 域控IP列表 | 扫描的IP地址列表，仅对扫描器配置有效。如果有多个IP地址，请用回车间隔，每行一个。 |
| 扫描间隔 | 扫描或收集用户登录信息的时间间隔。 |
| 用户票证期限 | 用户的认证有效时间，默认为10小时。 |
| 下级设备地址 | NIPS设备的IP地址。如果有多个NIPS设备IP地址，请用回车间隔，每行一个。 |
| 下级设备端口 | NIPS设备的通信端口，默认为6400。 |

1. 出厂参数
   1. 引擎接口初始设置

| IP | M:192.168.1.1  H1:192.168.2.1（H1口是否存在视硬件平台而定）  G1/1:0.0.0.0  G1/2:0.0.0.0  ……（除管理口外，其余工作口初始IP均为0.0.0.0） |
| --- | --- |
| 网络掩码 | 255.255.255.0 |

* 1. 引擎初始管理员
     1. Web操作员初始帐号

| 用户名 | weboper |
| --- | --- |
| 密码 |

* + 1. Web审计员初始帐号

| 用户名 | webaudit |
| --- | --- |
| 密码 |

* + 1. Console口管理员初始帐号

| 用户名 | conadmin |
| --- | --- |
| 密码 |

* 1. Console口通讯参数

| 波特率 | 115200 |
| --- | --- |
| 传输位数 | 8 |

* 1. CLI管理员初始帐号

| 用户名 | shell |
| --- | --- |
| 密码 |