页眉

|  |
| --- |
| 网络入侵防护系统  快速使用指南 |



文档版本：V5.6.9-20140531

|  |
| --- |
| © 2014 绿盟科技 |

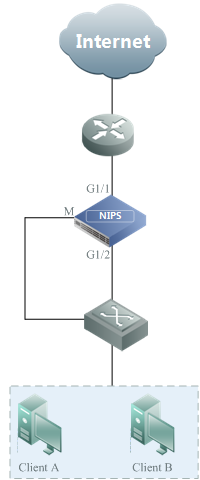
|  |
| --- |
| ■ 版权声明 |
| 本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属所有，受到有关产权及版权法保护。任何个人、机构未经的书面授权许可，不得以任何方式复制或引用本文的任何片断。 |

|  |
| --- |
| 目录 |
| [一. 使用向导 1](#_Toc386549268)  [1.1 典型部署 1](#_Toc386549269)  [1.2 配置流程 2](#_Toc386549270)  [二. 操作简介 4](#_Toc386549271)  [2.1 系统准备阶段 4](#_Toc386549272)  [2.1.1 导入证书 4](#_Toc386549273)  [2.1.2 登录Web管理界面 5](#_Toc386549274)  [2.1.3 配置管理口IP 6](#_Toc386549275)  [2.2 策略管理阶段 8](#_Toc386549276)  [2.2.1 配置入侵防护策略 8](#_Toc386549277)  [2.2.2 配置高级防御策略 11](#_Toc386549278)  [2.2.3 配置信誉 22](#_Toc386549279)  [2.2.4 配置URL分类过滤策略 25](#_Toc386549280)  [2.2.5 配置防病毒策略 28](#_Toc386549281)  [2.2.6 配置应用管理策略 31](#_Toc386549282)  [2.2.7 配置流量管理策略 33](#_Toc386549283)  [2.3 其他配置 37](#_Toc386549284)  [2.3.1 添加例外规则 37](#_Toc386549285)  [2.3.2 规则查询 37](#_Toc386549286)  [2.3.3 系统管理 38](#_Toc386549287)  [2.4 查看防护结果 39](#_Toc386549288)  [2.4.1 首页 39](#_Toc386549289)  [2.4.2 日志 40](#_Toc386549290)  [2.4.3 报表 40](#_Toc386549291)  [附录A 出厂参数 42](#_Toc386549292)  [A.1 管理口初始配置 42](#_Toc386549293)  [A.2 初始用户帐号 42](#_Toc386549294)  [A.3 串口通讯参数 42](#_Toc386549295)  [A.4 CLI管理员初始帐号 43](#_Toc386549296) |

本文档针对初次使用绿盟网络入侵防护系统的用户，介绍产品的基础配置和主要功能的使用方法。

1. 使用向导
   1. 典型部署

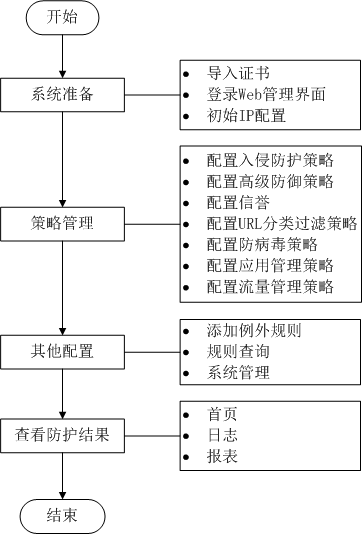
NIPS设备一般采用直通部署方式部署在实际网络环境中，M为管理口，G1/1和G1/2为一对直通接口，如所示。



典型部署

* 1. 配置流程

NSFOCUS NIPS设备部署到实际网络环境中后，主要的配置流程如所示，更加详细的功能介绍和操作步骤请参见《绿盟网络入侵防护系统用户手册》中的相关章节。



NIPS快速配置流程

1. 操作简介
   1. 系统准备阶段
      1. 导入证书

初次登录NIPS系统，必须首先导入证书，否则无法使用NIPS设备。

初次登录系统时，弹出导入证书对话框，如所示。



导入证书

证书导入后，NIPS设备自动进行接口配置、启用默认安全策略模板，并启用阻断。

* + 1. 登录Web管理界面

管理口IP配置完毕，选择一台管理主机，打开IE浏览器，用HTTPS方式连接NIPS的管理口IP地址，例如：https://192.168.1.1。

回车后出现安全报警信息，单击“继续浏览此网站（不推荐）”，接受NIPS证书加密的通道，跳转到NIPS的Web管理登录页面，如所示。



Web管理登录界面

输入正确的用户名和密码（初次登录使用weboper/weboper，登录后需立即按照密码复杂度修改密码）即可进入Web管理界面，对NIPS设备进行管理。

* + 1. 配置管理口IP

登录Web管理界面后，选择菜单 **网络** > **接口**，单击接口列表中M口对应的编辑图标，设置管理口的IP地址，如所示。管理口IP设定后，必须“重启引擎”使之生效。



配置管理口IP地址

* 1. 策略管理阶段

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。对象的配置请参见《绿盟网络入侵防护系统用户手册》中5 对象。

|  |  |
| --- | --- |
| 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。  对接口、安全区进行操作后必须进行“重启引擎”操作，新的配置才会生效。 |

* + 1. 配置入侵防护策略

入侵防护策略主要包括：入侵防护策略和DoS防护。

* 入侵防护策略

选择菜单 **策略** > **入侵防护** > **入侵防护策略**，在入侵防护策略页面中单击【新建】按钮，弹出新建入侵防护策略对话框，如所示。



新建入侵防护策略

入侵防护策略参数如所示。

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/目的地址对象 | 对来自/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、信任用户、非信任用户和自定义用户。 |
| 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。NIPS设备中规则模板包括系统规则模板、用户规则模板。其中系统规则模板又分为内置模板和派生模板。 |
| 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。 |

* DoS防护

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。

选择菜单 **策略** > **入侵防护** > **DoS防护**，配置各类DoS防护策略参数。

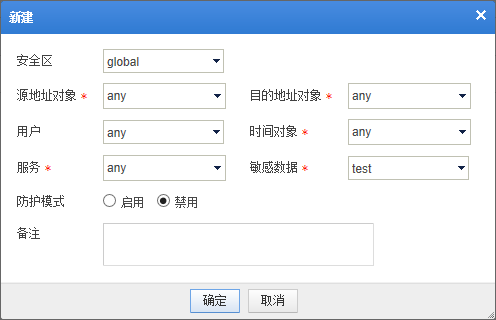
* + 1. 配置高级防御策略

高级防御策略主要包括：敏感数据保护策略、文件识别策略和服务器异常防护策略。

* 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。

选择菜单 **策略** > **高级威胁防御** > **敏感数据保护**，在敏感数据保护策略页面中单击【新建】按钮，弹出新建敏感数据保护策略对话框，如所示。



新建敏感数据保护策略

敏感数据保护策略参数如所示。

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策略。  “global”表示来自任何安全区的报文均匹配该策略。 |
| 源/目的地址对象 | 对来自/发往哪些地址的报文应用该敏感数据保策略。  “any”表示任意地址。 |
| 用户 | 敏感数据保策略的用户对象，分为如下四类：any、信任用户、非信任用户和自定义用户。 |
| 时间对象 | 敏感数据保策略生效的时间段。“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。 |

* 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。

选择菜单 **策略** > **高级威胁防御** > **文件识别**，在文件识别策略页面中单击【新建】按钮，弹出新建文件识别策略对话框，如所示。



新建文件识别策略

文件识别策略参数如所示。

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/目的地址对象 | 对来自/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、信任用户、非信任用户和自定义用户。 |
| 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。 |

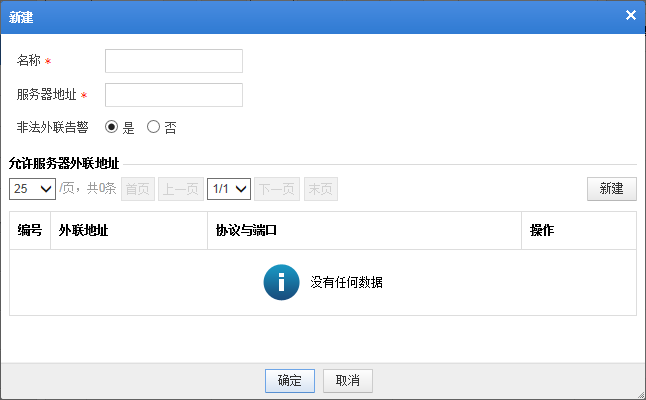
* 服务器异常防护策略

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个服务器的外联行为进行防护。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**，在服务器异常防护策略页面中单击【新建】按钮，弹出新建服务器异常防护策略对话框，如所示。

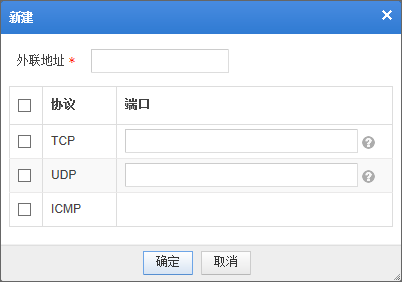


新建服务器异常防护策略

服务器异常防护策略参数如所示。

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，弹出如所示的新建正常外联行为对话框，配置参数后单价【确定】按钮保存配置，参数说明如所示。 |



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，允许服务器访问ICMP服务。 |

* + 快速新建

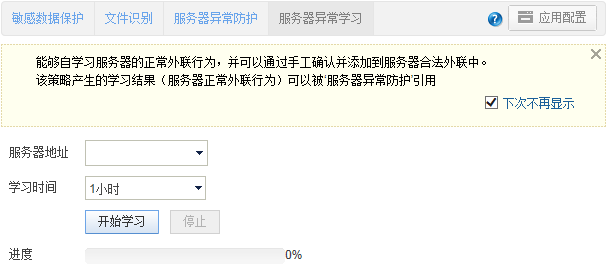
通过NIPS设备自学习到的外联信息，管理员可以快速新建服务器异常防护策略。

选择菜单 **策略** > **高级威胁防御** > **服务器异常学习**，在服务器异常学习页面的服务器列表中，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。

* 服务器异常学习

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。

选择菜单 **策略** > **高级威胁防御** > **服务器异常学习**，在服务器异常学习页面中配置服务器学习参数，如所示。



配置服务器学习参数

服务器学习参数如所示。

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。 |
| 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。 |

* + 1. 配置信誉

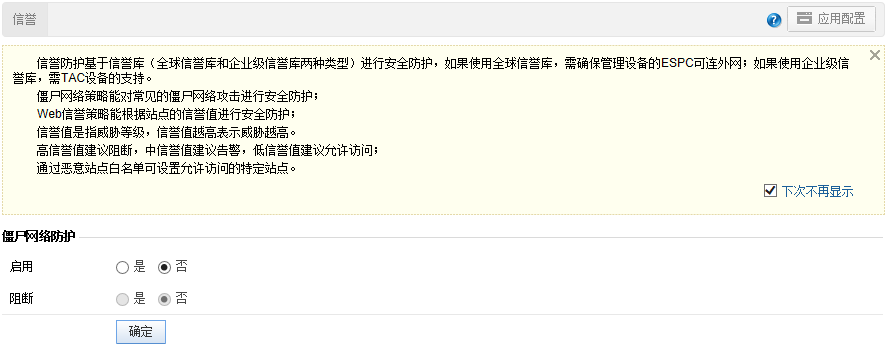
NIPS信誉包括僵尸网络防护和Web信誉。

* 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。

选择菜单 **策略** > **信誉** > **信誉**，在僵尸网络防护页面配置是否启用僵尸网络检测功能，以及启用后是否阻断僵尸网络连线，如所示。

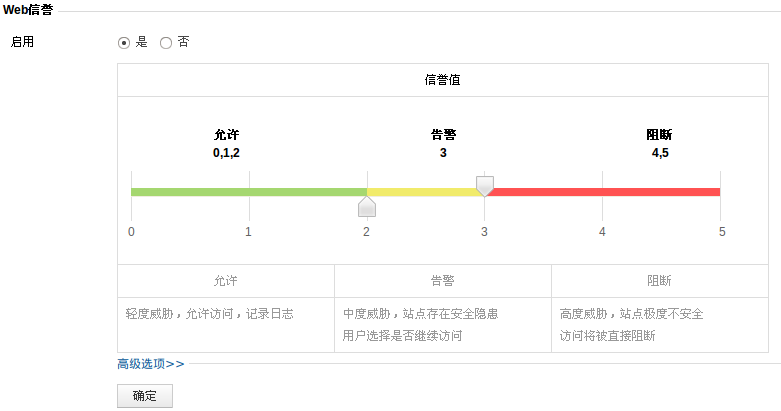


僵尸网络防护

* Web信誉策略

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，从而达到站点过滤的目的。

选择菜单 **策略** > **信誉** > **信誉**，配置Web信誉参数，如所示。



Web信誉

1. 启用Web信誉。
2. 配置Web信誉策略。
   1. 鼠标移动上方游标，设置进行告警、阻断的站点信誉值。
   2. 鼠标移动下方游标，设置允许访问的站点信誉值。
   3. 单击“高级选项>>”，配置允许访问的站点白名单。
      1. 配置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内置了一些系统URL分类规则，管理员也可以从在线服务器上获取更多的URL分类规则，管理员还可以根据实际情况手动配置需要过滤的站点URL分类。下面介绍如何新建URL过滤策略。

选择菜单 **策略** > **URL分类** > **URL分类**，在URL分类页面中单击【新建】按钮，弹出新建URL过滤策略对话框，如所示。



新建URL过滤策略

URL过滤策略参数如所示。

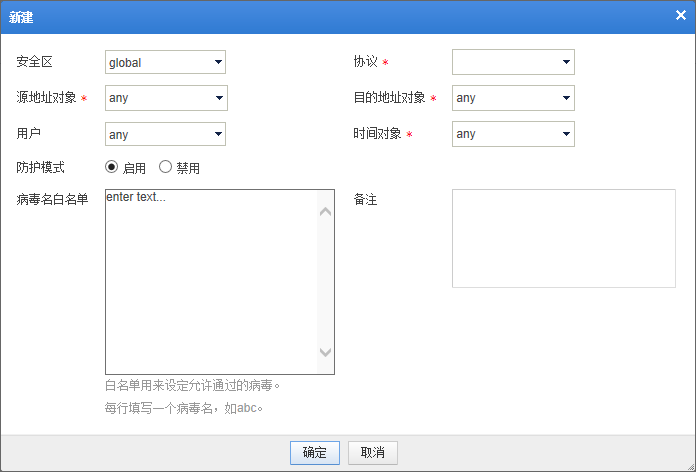
URL过滤策略参数

| 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。  若不指定，表示来自任何安全区的报文均匹配该策略。 |
| 源/目的地址对象 | 对来自/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 | URL过滤策略的用户对象，分为如下四类：any、信任用户、非信任用户和自定义用户。 |
| 时间对象 | URL过滤策略生效的时间段。“any”表示所有时间。 |
| 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。 |

* + 1. 配置防病毒策略

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。

选择菜单 **策略** > **防病毒** > **防病毒策略**，在防病毒策略页面单击【新建】按钮，弹出新建防病毒策略对话框，如所示。



新建防病毒策略

防病毒策略参数如所示。

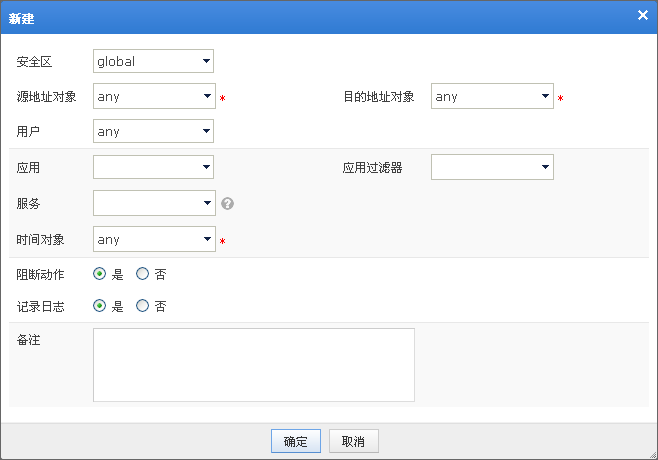
防病毒策略参数

| 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。  若不指定，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。 |
| 源/目的地址对象 | 对来自/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、信任用户、非信任用户和自定义用户。 |
| 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 | 白名单中病毒名不会被防病毒引擎扫描。多个病毒名之间用空行分隔。 |

* + 1. 配置应用管理策略

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。

选择菜单 **策略** > **应用管理**，在应用管理策略页面单击【新建】按钮，弹出新建应用管理策略对话框，如所示。



新建应用管理策略

应用管理策略参数如所示。

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。  若不指定，表示来自任何安全区的报文均匹配该策略。 |
| 源/目的地址对象 | 对来自/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、信任用户、非信任用户和自定义用户。 |
| 应用 | 策略要匹配的应用对象。应用对象的配置请参见《绿盟网络入侵防护系统用户手册》中的5.4.1 系统应用对象和5.4.2 自定义应用对象。  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《绿盟网络入侵防护系统用户手册》中5.4.3 配置过滤器。  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。  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。 |

* + 1. 配置流量管理策略

NIPS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

选择菜单 **策略** > **流量管理** > **流量管理策略**，在流量管理策略页面单击【新建】按钮，弹出新建流量管理策略对话框，如所示。



新建流量管理策略

流量管理策略参数说明如所示。

流量管理策略参数

| 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 | 选择**流量管理**。 |
| 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源地址对象。 |
| 用户 | 流量管理策略的用户对象，分为如下四类：any、信任用户、非信任用户和自定义用户。 |
| 应用 | 流量管理策略的应用对象。 |
| 时间对象 | 流量管理策略匹配的时间对象。“any”表示所有时间。 |

* 流量分析策略

选择菜单 **策略** > **流量管理** > **流量管理策略**，在流量管理策略页面单击【新建】按钮，弹出新建流量分析策略对话框，如所示。



新建流量分析策略

流量分析策略参数说明如所示。

* 1. 其他配置
     1. 添加例外规则

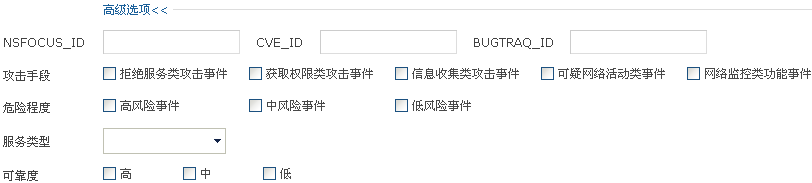
当用户需要对首页中某条规则的实时告警忽略不检测时，可以使用添加例外功能。

选择菜单 **首页** > **入侵防护事件**，当鼠标指向入侵防护事件列表中某一入侵防护事件时，入侵防护事件名称后显示“添加例外”，单击“添加例外”即可将该入侵防护事件添加到例外规则中。

* + 1. 规则查询

选择菜单 **对象** > **规则** > **规则查询**，在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。

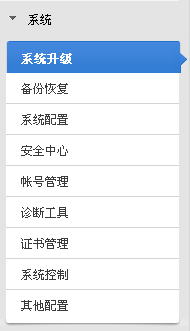
管理员除可以按照**规则编号**或**规则名称**进行搜索外，还可以配置查询条件的高级选项，进一步缩小规则搜索范围，使得查询结果更加准确，高级选项如所示。



规则查询高级选项

* + 1. 系统管理

NIPS设备系统管理的主要内容如所示。



系统管理

* 1. 查看防护结果

NIPS设备可以通过首页、日志以及报表查看各种防护结果。

* + 1. 首页

选择菜单 **首页**，管理员除可以查看NIPS设备的基本状态信息外，还可以查看入侵防护事件、高级威胁事件、信誉事件、URL分类事件、防病毒事件、流量分析和在线用户信息。

* + 1. 日志

选择菜单 **日志报表** > **日志分析**，管理员可以查看的日志类型有：入侵防护、高级威胁、信誉、应用管理、URL分类、防病毒、认证、认证状态、运行和系统日志。

* + 1. 报表

选择菜单**日志报表** >**统计报表**，管理员可以查看以下6种类型事件的报表：入侵防护、高级威胁、应用管理、信誉、URL分类和防病毒。

1. 出厂参数
   1. 管理口初始配置

|  |  |
| --- | --- |
| 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. 初始用户帐号

|  |  |  |  |
| --- | --- | --- | --- |
|  | Web操作员 | Web审计员 | Console口管理员 |
| 用户名 | weboper | webaudit | conadmin |
| 密码 |

* 1. 串口通讯参数

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

* 1. CLI管理员初始帐号

|  |  |
| --- | --- |
| 用户名 | shell |
| 密码 |