无标题-4

|  |
| --- |
|  |



文档版本： ()

|  |
| --- |
| © 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](#_Toc392247288)

[1 典型部署 3](#_Toc392247289)

[1.1 直通部署方式 3](#_Toc392247290)

[1.1.1 单路部署 3](#_Toc392247291)

[1.1.2 多路部署 7](#_Toc392247292)

[1.2 非对称路由部署方式 12](#_Toc392247293)

[1.3 高可用性配置 14](#_Toc392247294)

[1.3.1 一路直通 15](#_Toc392247295)

[1.3.2 两路直通 20](#_Toc392247296)

[1.4 端口聚合模式 25](#_Toc392247297)

[2 其他典型配置示例 27](#_Toc392247298)

[2.1 入侵防护策略配置 27](#_Toc392247299)

[2.2 应用管理策略配置 29](#_Toc392247300)

[2.3 流量管理策略配置 31](#_Toc392247301)

[2.3.1 流量管理策略配置示例 31](#_Toc392247302)

[2.3.2 流量分析策略配置示例 35](#_Toc392247303)

[2.4 与NSFOCUS ESPC连接配置示例 37](#_Toc392247304)

[A 出厂参数 44](#_Toc392247305)

[A.1 初始网络设置 44](#_Toc392247306)

[A.2 初始管理员 44](#_Toc392247307)

[A.2.1 Web操作员初始帐号 44](#_Toc392247308)

[A.2.2 Web审计员初始帐号 44](#_Toc392247309)

[A.2.3 Console口管理员初始帐号 45](#_Toc392247310)

[A.3 NSFOCUS ESPC管理员初始帐号 45](#_Toc392247311)

[A.4 串口通讯参数 45](#_Toc392247312)

[A.5 CLI管理员初始帐号 45](#_Toc392247313)

插图

[图1-1 单路部署 4](#_Toc392247314)

[图1-2 单路部署 – 配置G1/1接口 5](#_Toc392247315)

[图1-3 单路部署 – 配置G1/2口 6](#_Toc392247316)

[图1-4 单路部署 – 配置M接口 7](#_Toc392247317)

[图1-5 多路部署 8](#_Toc392247318)

[图1-6 多路部署 – 配置G1/1接口 9](#_Toc392247319)

[图1-7 多路部署 – 配置G1/2接口 10](#_Toc392247320)

[图1-8 多路部署 – 配置G1/3接口 11](#_Toc392247321)

[图1-9 多路部署 – 配置G1/4接口 12](#_Toc392247322)

[图1-10 非对称路由网络拓扑 13](#_Toc392247323)

[图1-11 新建非对称路由支持策略 14](#_Toc392247324)

[图1-12 高可用性 – 一路直通 15](#_Toc392247325)

[图1-13 一路直通 – 主设备HA公共参数 16](#_Toc392247326)

[图1-14 一路直通 – 从设备HA公共参数 17](#_Toc392247327)

[图1-15 一路直通 – 主设备直通HA参数 18](#_Toc392247328)

[图1-16 一路直通 – 从设备直通HA参数 19](#_Toc392247329)

[图1-17 高可用性 – 两路直通 20](#_Toc392247330)

[图1-18 两路直通 – 主设备HA公共参数 22](#_Toc392247331)

[图1-19 两路直通 – 从设备HA公共参数 22](#_Toc392247332)

[图1-20 两路直通 – 主设备直通HA参数 23](#_Toc392247333)

[图1-21 两路直通 – 从设备直通HA参数 24](#_Toc392247334)

[图1-22 端口聚合部署 25](#_Toc392247335)

[图2-1 入侵防护策略 – 新建阻断内网客户端相关所有事件的入侵防护策略 28](#_Toc392247336)

[图2-2 应用管理策略 – 自定义时间对象 30](#_Toc392247337)

[图2-3 应用管理策略 – 配置应用管理策略 30](#_Toc392247338)

[图2-4 典型拓扑部署 31](#_Toc392247339)

[图2-5 流量管理策略配置 – 配置线路 32](#_Toc392247340)

[图2-6 流量管理策略配置 – 新建IP池 33](#_Toc392247341)

[图2-7 流量管理策略配置 – 新建自定义时间 33](#_Toc392247342)

[图2-8 流量管理策略配置 – 新建流量通道 34](#_Toc392247343)

[图2-9 流量管理策略配置 – 新建流量管理策略 35](#_Toc392247344)

[图2-10 新建流量分析策略 36](#_Toc392247345)

[图2-11 与NSFOCUS ESPC连接配置 37](#_Toc392247346)

[图2-12 与NSFOCUS ESPC连接 39](#_Toc392247347)

[图2-13 ESPC本地IP设置 40](#_Toc392247348)

[图2-14 设备识别提示 40](#_Toc392247349)

[图2-15 安全设备列表 40](#_Toc392247350)

[图2-16 添加设备 41](#_Toc392247351)

[图2-17 重启服务 42](#_Toc392247352)

[图2-18 验证配置结果 43](#_Toc392247353)

前言

概述

本文介绍绿盟网络入侵防护系统（NSFOCUS Network Intrusion Prevention System，以下简称NIPS）的部署方式和典型配置。

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 典型部署 | 介绍NIPS在网络中的部署方式及配置方法。 |
| 2 其他典型配置示例 | 介绍NIPS的各类防护配置的典型示例。 |
| A 出厂参数 | 介绍NIPS的默认出厂参数设置。 |

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)

# 典型部署

针对不同网络规模、不同安全级别和不同拓扑复杂程度的网络，NIPS提供以下几类典型的网络部署方式。

| 功能 | 描述 |
| --- | --- |
| 直通部署方式 | 介绍直通部署方式下设备的配置方法。 |
| 非对称路由部署方式 | 介绍非对称路由部署方式及配置方法。 |
| 高可用性配置 | 介绍高可用性配置的方法。 |
| 端口聚合模式 | 介绍端口聚合模式下设备端口的配置。 |

## 直通部署方式

直通部署方式分为单路部署和多路部署。

### 单路部署

* + - * 1. 应用场景

目前，很多企业从公司内网到外网有一条链路，通过单路部署NIPS的方式，可以保护内网客户不受到来自Internet的攻击。

单路部署，即选择一对Direct模式的接口（一组IN、OUT接口）作为工作口，任选一个未使用的接口为管理口，部署结构如图1-1所示。

单路部署



* + - * 1. 配置准备
* G1/1连接外网，G1/2连接内网，M为管理口。
* 管理口IP地址：192.168.3.1
* 默认网关：192.168.3.254
* 内网安全区：NIPS设备上线后默认将G1/1和G1/2置为一对直通接口，同属安全区Direct-A
  + - * 1. 配置思路

在本示例中，设备的接口可如下配置：

* G1/1接口：属安全区Direct-A，无需配置接口IP地址，对原有网络拓扑无任何影响，只是增加了对连接外部出口的主干链路的检测与防护。如配置了接口IP地址，并且选中了“可管理”，则也可以做管理口使用。
* G1/2接口：属安全区Direct-A，无需配置接口IP地址，与G1/1是一对直通接口，配置完全一样。
* M接口：安全区为管理（mgt）模式，配置接口IP地址，保证以Web方式就可以操作、配置设备。

|  |  |
| --- | --- |
| 提示 | Direct接口IP在通讯中不起作用。建议G1/1和G1/2不用做管理口时设置IP为0.0.0.0。 |

* + - * 1. 配置步骤

请在设备上进行如下配置：

选择菜单 网络 > 接口，进入接口列表的页面。

配置G1/1接口，如图1-2所示。

单路部署 – 配置G1/1接口



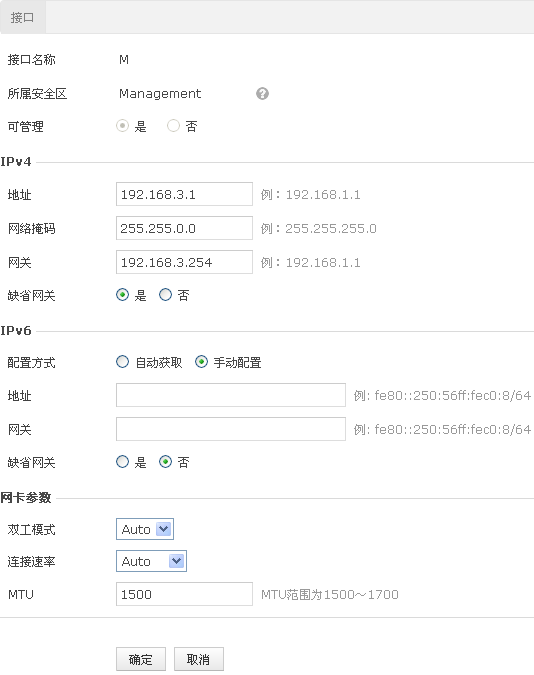
配置G1/2接口，如图1-3所示。

单路部署 – 配置G1/2口



配置M接口，如图1-4所示。

单路部署 – 配置M接口



选择菜单 系统 > 系统控制，进入系统控制页面，单击【重启引擎】按钮，使以上所有配置生效。

----结束

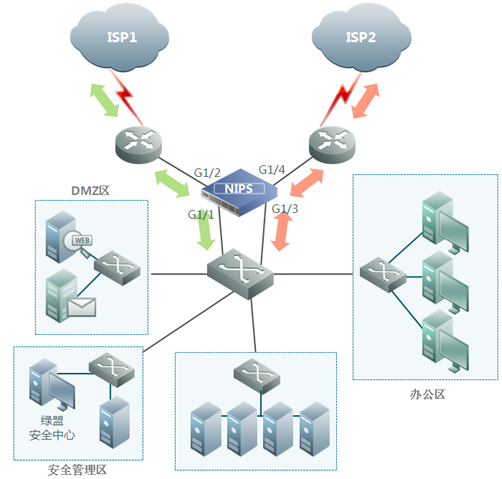
### 多路部署

* + - * 1. 应用场景

目前，很多企业为了保证网络带宽资源的充足和网络冗余，网络出口采用多链路连接方式，连接到两个或更多ISP服务商。针对这种连接方式，可以在网络出口处部署一台NIPS，采用多链路防护的部署方式。

多路部署，即选择两对Direct模式的接口，同时配置管理接口IP地址，部署结构如图1-5所示。

多路部署



* + - * 1. 配置准备
* G1/1和G1/3连接内网，G1/2和G1/4连接外网，G1/3同时作为管理口。
* 管理IP地址：192.168.3.1
* 默认网关：192.168.3.254
* 内网安全区：NIPS设备上线后默认将G1/1和G1/2置为一对直通接口，同属安全区Direct-A；G1/3和G1/4置为一对直通接口，同属安全区Direct-B。
  + - * 1. 配置思路

在本示例中，设备的接口可如下配置：

* G1/1接口：属安全区Direct-A，无需配置接口IP地址，对原有网络拓扑无任何影响，只是增加了对连接外部出口的主干链路的检测与防护。
* G1/2接口：属安全区Direct-A，无需配置接口IP地址，与G1/1是一对直通接口，配置完全一样。
* G1/3接口：属于安全区Direct-B，作为管理口配置接口IP为192.168.3.1，保证以Web方式就可以操作、配置设备，与G1/4是一对直通接口。
* G1/4接口：属于安全区Direct-B，无需配置接口IP地址，与G1/3是一对直通接口。
  + - * 1. 配置步骤

请在设备上进行如下配置：

选择菜单 网络 > 接口，进入接口列表的页面。

配置G1/1接口，如图1-6所示。

多路部署 – 配置G1/1接口



配置G1/2接口，如图1-7所示。

多路部署 – 配置G1/2接口



配置G1/3接口，如图1-8所示。

多路部署 – 配置G1/3接口



配置G1/4接口，如图1-9所示。

多路部署 – 配置G1/4接口



选择菜单 系统 > 系统控制，进入系统控制页面，单击【重启引擎】按钮，使以上所有配置生效。

----结束

## 非对称路由部署方式

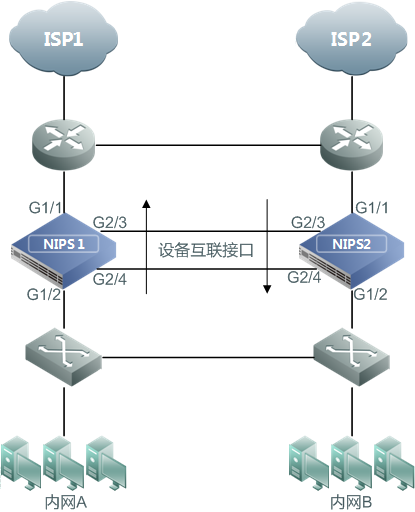
* + - * 1. 应用场景

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。

内网A和内网B通过不同路由器访问ISP1或ISP2，NIPS1和NIPS2之间连接流量数据线，通过配置两台NIPS的非对称路由支持实现对非对称路由数据包进行转发，如图1-10所示。

|  |  |
| --- | --- |
| 注意 | 在对两台NIPS设备接口进行直通配置时，需确保NIPS设备间的IN口和OUT口方向一致。 |

非对称路由网络拓扑



* + - * 1. 配置准备
* NIPS1和NIPS2的G1/1和G1/2分别连接外网和内网。
* NIPS设备上线后默认将G1/1和G1/2置为一对直通接口，同属安全区Direct-A。
* NIPS1和NIPS2的G2/3和G2/4作为非对称路由设备组之间的互联接口，属于interconnect类型的安全区。
* NIPS1管理口H1：IP地址为2.2.3.2，网络掩码为255.255.0.0。
* NIPS2管理口H2：IP地址为2.2.2.2，网络掩码为255.255.0.0。
  + - * 1. 配置思路
        2. 启用NIPS1、NIPS2设备的非对称路由支持功能。
        3. 配置NIPS1、NIPS2设备的非对称路由支持策略。
        4. 配置步骤

以管理员weboper登录，进行如下配置。

启用NIPS1、NIPS2设备的非对称路由支持功能。

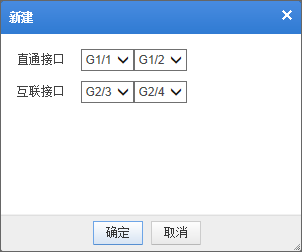
选择菜单 网络 > 高可用设置 > 非对称路由支持，进入非对称路由支持页面。

单击【启动】按钮，启动非对称路由支持功能。

配置NIPS1、NIPS2设备的非对称路由支持策略。

单击【新建】按钮，新建非对称路由支持策略，如图1-11所示。

新建非对称路由支持策略



选择菜单 系统 > 系统控制，单击【应用配置】或者单击页面右上角的“应用配置”，使配置生效。

----结束

## 高可用性配置

为了满足客户不间断业务访问需求，在直通部署下，NIPS支持高可用性（High Availability，简称HA），具备高可靠性，能够在设备、链路以及互连设备出现故障的情况下，提供网络访问路径无缝切换，保障重要的业务数据流的正常通讯。

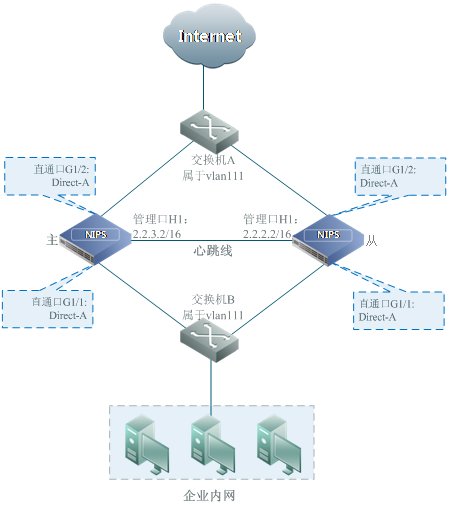
高可用性配置中，作为主、从设备的NIPS设备必须是完全相同的配置，包括硬件型号、软件版本以及相关配置信息等。

### 一路直通

* + - * 1. 应用场景

主、从设备都有一对直通口连接两端的交换机，并且同一交换机的接口需要在同一VLAN中。两台设备之间通过一个管理口（作为心跳口）相连，如图1-12所示。

高可用性 – 一路直通



* + - * 1. 配置准备

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、会话信息以及同步配置文件。

* 主、从设备中，G1/1连接内网，G1/2连接外网，H1为管理口。
* 主设备管理口H1：IP地址为2.2.3.2，网络掩码为255.255.0.0。
* 从设备管理口H1：IP地址为2.2.2.2，网络掩码为255.255.0.0。
* NIPS设备上线后默认将G1/1和G1/2置为一对直通接口，同属安全区Direct-A。
  + - * 1. 配置思路
        2. 配置主、从设备的HA公共参数。
        3. 配置主、从设备的直通HA参数。
        4. 启用主、从设备的直通HA功能。
        5. 配置步骤

配置主、从设备的HA公共参数。

分别在主设备和从设备中选择菜单 网络 > 高可用性设置，然后在右侧界面的“基本配置”页签中配置HA的公共参数。

主设备中，将“心跳接口”设置为“H1”；“对端IP地址”设置为“2.2.2.2”；如果要启动会话同步需要选中相应的单选按钮“是”，如图1-13所示。

一路直通 – 主设备HA公共参数



从设备中，将“心跳接口”设置为“H1”；“对端IP地址”设置为“2.2.3.2”；如果要启动会话同步需要选中相应的单选按钮“是”，如图1-14所示。

一路直通 – 从设备HA公共参数



|  |  |
| --- | --- |
| 注意 | 主、从设备中，会话同步的配置必须保持一致。 |

配置主、从设备的直通HA参数。

分别在主设备和从设备中选择菜单 网络 > 高可用性设置，然后在右侧界面中激活“直通配置”页签，配置直通HA参数。

主设备中，将“工作模式”设置为“主机”；抢占模式保持默认，即“是”；“心跳时间间隔”保持默认配置，即“1000毫秒”；“失去心跳次数”保持默认配置，即“3”，如图1-15所示。

一路直通 – 主设备直通HA参数



从设备中，将“工作模式”设置为“从机”；抢占模式保持默认配置，即“是”；“心跳时间间隔”保持默认配置，即“1000毫秒”；“失去心跳次数”保持默认配置，即“3”，如图1-16所示。

一路直通 – 从设备直通HA参数



启用主、从设备的直通HA功能。

分别在主设备和从设备的如图1-15和图1-16所示界面中，单击【启动】按钮，系统将自动重启引擎。

启动直通HA后，可以看到状态的变化：

* 在主设备的“直通配置”页签中，“工作状态”显示为“正常”；“本机系统状态”显示为“激活”；“对端系统状态”显示为“非激活”；“配置”中的选择均变成灰色不可变状态。

在主设备的“基本配置”页签中，“心跳口状态”显示为“正常”；“HA配置”中的信息为灰色不可变状态；单击【对端 >> 本机】按钮或者【本地 >> 对端】按钮，可以在主从设备之间同步配置。

* 在从设备“直通配置”页签中，“工作状态”显示为“正常”；“本机系统状态”显示为“非激活”；“对端系统状态”显示为“激活”。

在从设备的“基本配置”页签中，“心跳口状态”显示为“正常”；“HA配置”中的信息为灰色不可变状态；单击【对端 >> 本机】按钮或者【本地 >> 对端】按钮，可以在主从设备之间同步配置。

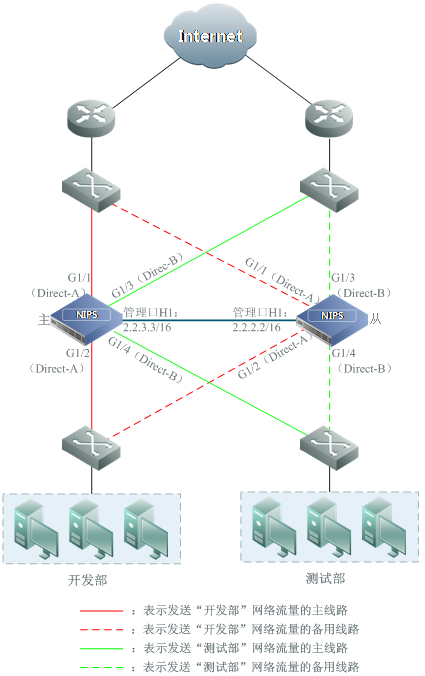
----结束

### 两路直通

* + - * 1. 应用场景

主设备与从设备都有两对直通口连接两端的交换机，两台设备之间各通过一个管理口（作为心跳口）相连，如图1-17所示。

高可用性 – 两路直通



* + - * 1. 配置准备

直通口用于连接两端的交换机、转发数据和故障切换，设备两端相连的交换机要处于同一VLAN中；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。

* 主、从设备中，G1/2和G1/4连接内网，G1/1和G1/3连接外网，H1为管理口。
* 主设备管理口H1：IP地址为2.2.3.3，网络掩码为255.255.0.0。
* 从设备管理口H1：IP地址为2.2.2.2，网络掩码为255.255.0.0。
* NIPS设备上线后默认将G1/1和G1/2置为一对直通接口，同属安全区Direct-A，G1/3和G1/4置为一对直通接口，同属安全区Direct-B。
* 主设备中G1/1和G1/2作为转发“开发部”网络流量的主线路；从设备中G1/1和G1/2作为转发“开发部”网络流量的从线路。
* 主设备中G1/3和G1/4作为转发“测试部”网络流量的主线路；从设备中G1/3和G1/4作为转发“测试部”网络流量的从线路。
  + - * 1. 配置思路
        2. 配置主、从设备的HA公共参数。
        3. 配置主、从设备的直通HA参数。
        4. 启用主、从设备的直通HA功能。
        5. 配置步骤

配置主、从设备的HA公共参数。

分别在主设备和从设备中选择菜单 网络 > 高可用性设置，然后在右侧界面的“基本配置”页签中配置HA的公共参数。

主设备中，将“心跳接口”设置为“H1”；“对端IP地址”设置为“2.2.2.2”；如果要启动会话同步需要选中相应的单选按钮“是”，如图1-18所示。

两路直通 – 主设备HA公共参数



从设备中，将“心跳接口”设置为“H1”；“对端IP地址”设置为“2.2.3.3”；如果要启动会话同步需要选中相应的单选按钮“是”，如图1-19所示。

两路直通 – 从设备HA公共参数



|  |  |
| --- | --- |
| 注意 | 主、从设备中，会话同步的配置必须保持一致。 |

配置主、从设备的直通HA参数。

分别在主设备和从设备中选择菜单 网络 > 高可用性设置，然后在右侧界面中激活“直通配置”页签，配置直通HA参数。

主设备中，将“工作模式”设置为“主机”；抢占模式保持默认，即“是”；“心跳时间间隔”保持默认配置，即“1000毫秒”；“失去心跳次数”保持默认配置，即“3”，如图1-20所示。

两路直通 – 主设备直通HA参数



从设备中，将“工作模式”设置为“从机”；抢占模式保持默认，即“是”；“心跳时间间隔”保持默认配置，即“1000毫秒”；“失去心跳次数”保持默认配置，即“3”，如图1-21所示。

两路直通 – 从设备直通HA参数



启用主、从设备的直通HA功能。

分别在主设备和从设备中，在图1-20和图1-21所示界面中，单击【启动】按钮，系统将自动重启引擎。

启动直通HA后，可以看到状态的变化：

* 在主设备的“直通配置”页签中，“工作状态”显示为“正常”；“本机系统状态”显示为“激活”；“对端系统状态”显示为“非激活”；“配置”中的选择均变成灰色不可变状态。

在主设备的“基本配置”页签中，“心跳口状态”显示为“正常”；“HA配置”中的信息为灰色不可变状态；单击【对端 >> 本机】按钮或者【本地 >> 对端】按钮，可以在主从设备之间同步配置。

* 在从设备的“直通配置”页签中，“工作状态”显示为“正常”；“本机系统状态”显示为“非激活”；“对端系统状态”显示为“激活”。

在从设备的“基本配置”页签中，“心跳口状态”显示为“正常”；“HA配置”中的信息为灰色不可变状态；单击【对端 >> 本机】按钮或者【本地 >> 对端】按钮，可以在主从设备之间同步配置。

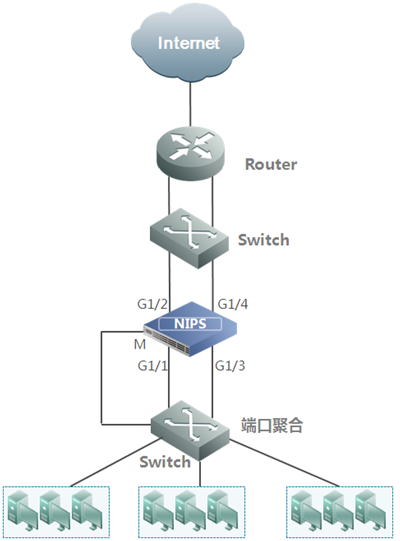
|  |  |
| --- | --- |
| 注意 | 在两路直通模式下，只要当前激活设备的某一个接口不起作用了（down掉或者异常），比如主机的一个直通口down了，主机所有直通口都会down，切换到备机。 |

----结束

## 端口聚合模式

支持端口聚合的交换机可以支持多路同时连接NIPS，以扩展带宽。

端口聚合部署



在本示例中，设备的端口可如下配置：

* G1/1接口：零配置上线后，NIPS设备默认G1/1接口属于安全区Direct-A，与G1/2为一对直通口，无需配置接口IP地址。
* G1/2接口：零配置上线后，NIPS设备默认G1/2接口属于安全区Direct-A，与G1/1为一对直通口，无需配置接口IP地址。
* G1/3接口：零配置上线后，NIPS设备默认G1/3接口属于安全区Direct-B，与G1/4为一对直通口，无需配置接口IP地址。
* G1/4接口：零配置上线后，NIPS设备默认G1/4接口属于安全区Direct-B，与G1/3为一对直通口，无需配置接口IP地址。
* M接口：安全区为管理（mgt）模式，配置接口IP地址，保证以Web方式就可以操作、配置设备。

|  |  |
| --- | --- |
| 注意 | 配置接口后，需要重启引擎使配置生效。 |

其中，G1/1与G1/3与下行交换机相连，G1/2与G1/4与上行交换机相连，上行交换机和下行交换机均配置了端口聚合，NIPS设备即使不接入网络，交换机间的端口聚合同样生效，通信正常，NIPS设备接入网络使得两路流量都可以接受NIPS的检查，增加总的负载流量。例如，G1/1上有100Mbps流量，G1/3上有100Mbps流量，两路接入NIPS后总流量负载为200Mbps。不配置端口聚合的时候，交换机会禁止其中一路的数据传输。

# 其他典型配置示例

管理员需要手动添加各种类型策略，确保NIPS设备对目标网络的防护。策略由安全区、对象、动作等元素共同组成，是指示引擎检测哪些事件以及事件发生时如何响应的规则集。

配置策略时，需注意以下情况：

* 多个策略之间具有优先级顺序，这个特性按照策略排列的先后顺序来确定，要注意的是前一条策略的动作（例如：当策略设置为阻断的时候，匹配策略的通讯数据会在触发策略后被丢弃）可能会影响后续策略的实现，建议您将需要明确阻断策略的优先级提前，这样可以有效减少NIPS的规则匹配次数，提高性能。
* NIPS的策略允许用户定义告警的响应方式，方便用户根据不同的区域或者事件种类等条件对告警进行处理。建议用户根据策略中所包含规则的分类、级别等对策略实行不同的响应方式。例如：对于漏洞攻击需要实时进行阻止，而对于一些应用的使用只需要进行记录。
* 需要注意告警事件的数量，数量多时建议使用事件过滤规则，推荐每一级把中、低风险事件过滤掉，只向高层NSFOCUS ESPC转发高风险事件。避免大量无用的告警事件把真正的攻击告警淹没了。

本章介绍了NIPS安全防护的各类典型示例，具体包括以下内容：

| 功能 | 描述 |
| --- | --- |
| 入侵防护策略配置 | 介绍入侵防护策略的配置示例。 |
| 应用管理策略配置 | 介绍应用管理策略的配置示例。 |
| 流量管理策略配置 | 介绍流量管理策略的配置示例。 |
| 与NSFOCUS ESPC连接配置示例 | 介绍系统与NSFOCUS ESPC设备连接的配置方法。 |

## 入侵防护策略配置

* + - * 1. 应用场景

在如图1-1所示的企业网络环境中，配置入侵防护策略，用以阻断内网客户端相关的所有事件。

* + - * 1. 配置准备

G1/1连接外网，G1/2连接内网，M为管理口，具体的参数配置如下：

* 管理口IP地址是192.168.3.1，网关是 192.168.3.254；
* 将G1/1和G1/2设置为一路Direct-A部署方式，Direct接口IP在通讯中不起作用，但不能和管理口IP在同一网段。
  + - * 1. 配置思路
        2. 配置阻断内网客户端相关所有事件的入侵防护策略。
        3. 应用配置，使配置生效。
        4. 配置步骤

请在设备上进行如下配置：

配置阻断内网客户端相关所有事件的入侵防护策略。选择菜单 策略 > 入侵防护，新建入侵防护策略，【规则模板】选择 内网客户端，【防护模式】保持默认设置（默认设置为 启用），如图2-1所示。

入侵防护策略 – 新建阻断内网客户端相关所有事件的入侵防护策略



入侵防护策略配置完毕，选择菜单 系统 > 系统控制，单击【应用配置】或者单击页面右上角的“应用配置”，使策略配置生效。

----结束

* + - * 1. 验证结果

当被保护服务器遭遇入侵攻击时，选择菜单 首页 > 入侵防护事件，可查看入侵防护事件记录信息。

|  |  |
| --- | --- |
| 说明 | 由于入侵防护事件页面会根据设定的自动刷新时间刷新，若遇查看不到入侵防护事件的情况，还可以在菜单“日志分析 > 入侵防护”中进行验证。 |

## 应用管理策略配置

* + - * 1. 应用场景

在如图1-1所示的企业网络环境中，配置应用管理策略，实现工作时间（9:00—12:00，13:00—18:00）阻断系统定义的应用对象，如“酷我音乐盒”。

* + - * 1. 配置准备

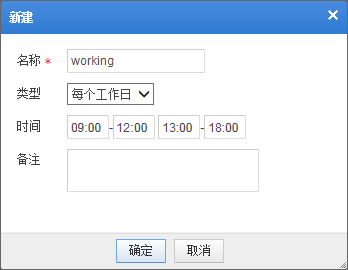
G1/1连接外网，G1/2连接内网，M为管理口，具体的参数配置如下：

* 管理口IP地址是192.168.3.1，网关是 192.168.3.254；
* 将G1/1和G1/2设置为一路Direct-A部署方式，Direct接口IP在通讯中不起作用，但不能和管理口IP在同一网段。
  + - * 1. 配置思路
        2. 创建工作时间对象“working”。
        3. 配置应用管理策略，以阻断该应用。
        4. 应用配置，使配置生效。
        5. 配置步骤

请在设备上进行如下配置：

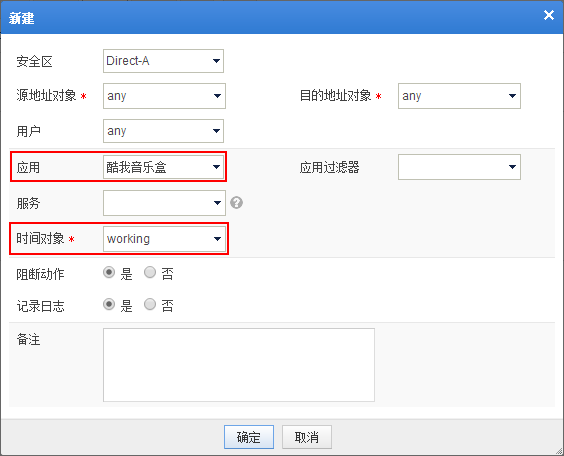
配置时间对象。选择菜单 对象 > 时间 > 自定义，新建名为“working”的工作时间对象，如图2-2所示。

应用管理策略 – 自定义时间对象



配置应用管理策略，以阻断系统定义的应用“酷我音乐盒”。选择菜单 策略 > 应用管理，然后单击【新建】按钮，配置应用管理策略，如图2-3所示。

应用管理策略 – 配置应用管理策略



时间对象和应用管理策略配置完毕，选择菜单 系统 > 系统控制，单击【应用配置】或者单击页面右上角的“应用配置”，使策略配置生效。

* + - * 1. 验证结果

当应用管理策略中配置的条件被触发时，选择菜单 日志分析 > 应用管理，可查看应用管理日志信息。

## 流量管理策略配置

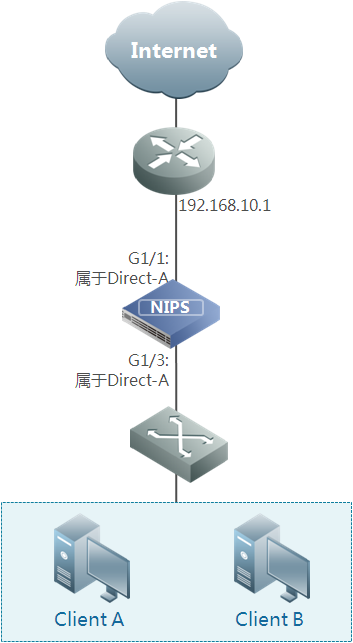
NIPS设备支持流量管理策略和流量分析策略。

### 流量管理策略配置示例

* + - * 1. 应用场景

在如图2-4所示的企业网络环境中，配置一条流量管理策略，实现上班时间（9:00—12:00，13:00—18:00）限制内网的每个用户IP访问外网的速率为100Kb/s。

典型拓扑部署



* + - * 1. 配置准备

内网用户的IP网段：192.168.10.190至192.168.10.199，网关指向路由器的内网地址。

* + - * 1. 配置思路
        2. 配置线路，设定流量管理策略应用到某条具体线路。
        3. 配置网络对象，设定要进行网络监控的IP池。
        4. 配置时间对象，设定要监控的时间段。
        5. 配置流量通道对象，设定监控的流量通道。
        6. 配置流量策略。
        7. 应用配置，使配置生效。

|  |  |
| --- | --- |
| 说明 | 配置线路、流量通道对象的具体步骤请参见《绿盟网络入侵防护系统用户手册》的相关章节，此处不再赘述。 |

* + - * 1. 配置步骤

请在设备上进行如下配置：

配置线路。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中单击【编辑线路】按钮，配置线路，如图2-5所示。

流量管理策略配置 – 配置线路



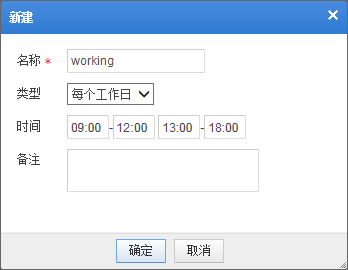
配置IP池对象。选择菜单 对象 > 网络 > IP池，新建IP池对象（包含了部门A中每个用户的内网IP地址），如图2-6所示。

流量管理策略配置 – 新建IP池



配置时间对象。选择菜单 对象 > 时间 > 自定义，新建自定义时间对象，如图2-7所示。

流量管理策略配置 – 新建自定义时间



配置流量通道。选择菜单 对象 > 流量通道，新建流量通道对象，如图2-8所示。

流量管理策略配置 – 新建流量通道



配置流量策略。选择菜单 策略 > 流量管理，新建流量管理策略，如图2-9所示。

流量管理策略配置 – 新建流量管理策略



|  |  |
| --- | --- |
| 提示 | 此时也可在策略设置中同时勾选流量分析，对流量管理的对象同时进行流量分析。更详细的流量分析配置请参见。 |

选择菜单 系统 > 系统控制，进入系统控制页面，单击【应用配置】或者单击页面右上角的“应用配置”，使策略配置生效。

----结束

### 流量分析策略配置示例

* + - * 1. 应用场景

在如图2-4所示的企业网络环境中，配置一条流量分析策略，实现对网络流量的详细分析。

* + - * 1. 配置准备

内网用户的IP网段：192.168.10.190至192.168.10.199，网关指向路由器的内网地址。

* + - * 1. 配置思路
        2. 配置流量分析策略。
        3. 应用配置，使配置生效。
        4. 配置步骤

请在设备上进行如下配置：

配置流量分析策略。选择菜单 策略 > 流量管理，新建流量分析策略，如图2-10所示。

新建流量分析策略



选择菜单 系统 > 系统控制，进入系统控制页面，单击【应用配置】或者单击页面右上角的“应用配置”，使策略配置生效。

* + - * 1. 验证结果

当有相应的流量通过设备时，可以选择菜单 首页 > 流量分析 > 流量/应用流量监控/IP流量监控”，查看流量分析的情况。

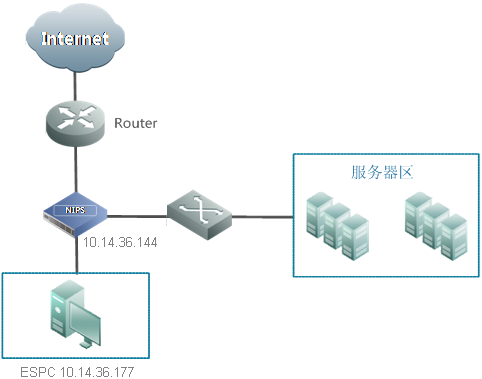
|  |  |
| --- | --- |
| 提示 | * 系统流量分析的报表详情需要通过NSFOCUS ESPC才能查看，请在查看前确认NIPS和NSFOCUS ESPC已经连接。 * 在配置NIPS和NSFOCUS ESPC连接时，必须配置ftp密码，才能确保流量分析日志送达NSFOCUS ESPC，与NSFOCUS ESPC连接的详细配置请参见。 |

## 与NSFOCUS ESPC连接配置示例

* + - * 1. 应用场景

在图2-11所示的网络环境中，NSFOCUS ESPC与NIPS联动部署。当绿盟NSFOCUS ESPC与NIPS连接后，可以接收NIPS更详细的日志信息，并长期保存。

与NSFOCUS ESPC连接配置



* + - * 1. 配置准备

NSFOCUS ESPC的IP地址10.14.36.177；

NIPS的数据传输地址10.14.36.144；

* + - * 1. 配置思路
        2. 配置NIPS与NSFOCUS ESPC的连接配置。
        3. 配置NSFOCUS ESPC与NIPS的连接配置。
        4. 验证配置结果。
        5. 配置步骤

在NIPS上进行如下配置

选择菜单 系统 > 安全中心，配置NIPS与NSFOCUS ESPC连接，本地IP地址、企业安全中心地址配置完成后，勾选“启动”，单击【确定】按钮，再进入系统控制页面，单击【重启引擎】按钮，使NIPS与NSFOCUS ESPC的连接配置生效，配置结果如图2-12所示。

|  |  |
| --- | --- |
| 说明 | 在NSFOCUS ESPC检测到设备并添加之前，显示状态为“正在连接”。 |

与NSFOCUS ESPC连接



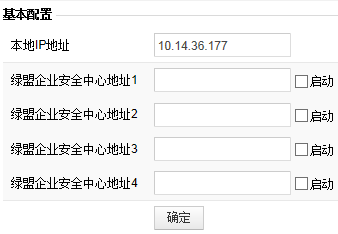
|  |  |
| --- | --- |
| 注意 | 如果需要在企业安全中心处查看NIPS的流量日志报表以及应用管理日志报表，必须配置FTP端口及FTP密码，且密码配置必须与企业安全中心的密码配置一致。 |

在NSFOCUS ESPC上进行如下配置

登录NSFOCUS ESPC（登录NSFOCUS ESPC的操作员用户名和密码均为admin）。

绑定NSFOCUS ESPC用于和NIPS设备通信的本地IP地址，选择菜单 系统 > 企业安全中心设置 > 基本设置，设置ESPC的本地IP地址，如图2-13所示。

ESPC本地IP设置



在NIPS设备上完成与NSFOCUS ESPC的连接配置后，ESPC的web管理界面会弹出设备识别提示框，如图2-14所示。

设备识别提示



单击提示框中的链接文字“点击此处”，跳转到NSFOCUS ESPC安全设备列表页面，如图2-15所示。

安全设备列表



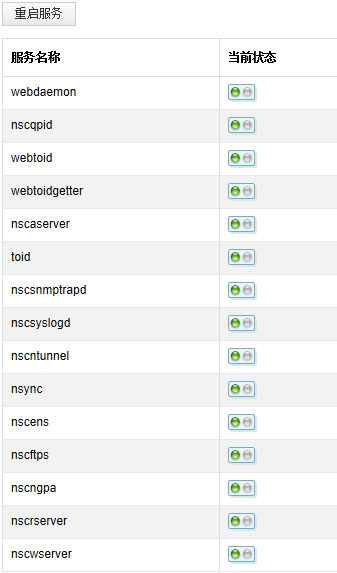
在“未添加设备列表”中可见ESPC识别到的申请建立连接的设备，单击设备列表操作栏中的添加图标，即可进入添加设备页面，如图2-16所示。

添加设备



在如图2-16所示的页面中输入设备名称后，单击【确定】按钮，ESPC将提示用户返回重启服务。选择菜单 系统 > 系统控制，进入系统控制页面，单击【重启服务】按钮即可，如图2-17所示。

重启服务



|  |  |
| --- | --- |
| 说明 | 手册以V5.6.9版本的NIPS与NSFOCUS ESPC建立连接为例，仅适用于V5.6.6及其以上版本的NIPS设备。 |

* + - * 1. 验证结果

如果NSFOCUS ESPC成功识别NIPS。在NSFOCUS ESPC的Web页面，选择菜单 设备管理 > 设备状态，可以看到如图2-18所示信息，同时NIPS的日志信息会及时同步上传到NSFOCUS ESPC。

验证配置结果



1. 出厂参数
   1. 初始网络设置

| 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. 初始管理员
     1. Web操作员初始帐号

| 管理员名 | weboper |
| --- | --- |
| 密码 |

* + 1. Web审计员初始帐号

| 管理员名 | webaudit |
| --- | --- |
| 密码 |

* + 1. Console口管理员初始帐号

| 管理员名 | conadmin |
| --- | --- |
| 密码 |

* 1. NSFOCUS ESPC管理员初始帐号

| 管理员名 | admin |
| --- | --- |
| 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

| 管理员名 | shell |
| --- | --- |
| 密码 |