Neusoft

东软 NetEye 集成安全网关入侵防御系统 V4.2
用户使用指南

东软联系信息

网站：http://neteye.neusoft.com

电子信箱：servicedesk@neusoft.com

服务电话：400 655 6789

目录

前言

本手册介绍东软 NetEye 集成安全网关入侵防御系统 （以下简称 NISG-IPS），由以下部分组成：

- 第 1 章，快速向导，介绍 NISG-IPS 初始化配置和验证，包括向导、WebUI 和 CLI 三种方式。
- 第 2 章，功能概述，介绍 NISG-IPS 各模块功能 （第 3 章到第 15 章）。
- 第 3 章，系统配置，介绍与系统相关的配置。
- 第 4 章，网络配置，介绍 NISG-IPS 的接口、安全域、STP、DHCP、DNS、IPv6 功能。
- 第 5 章，路由，介绍路由特性。
- 第 6 章， ISP 智能选路，介绍 ISP 智能选路特性。
- 第 7 章，多播，介绍多播特性。
- 第 8 章，地址转换，介绍源地址转换 （SNAT）、目的地址转换 （ DNAT）和地址映射 （MIP）。
- 第 9 章，服务质量，介绍 QoS 特性、配置和范例。
- 第 10 章，策略，介绍访问策略、会话策略、多播策略、IP-MAC 绑定以及默认策略配置。
- 第 11 章，攻击防御，介绍攻击探测和防御机制。
- 第 12 章，入侵防御系统，介绍出口控制、客户端保护和服务器保护。
- 第 13 章，虚拟专用网，介绍 IPSec VPN 和 SSL VPN（包括 SSL VPN Web 入口页面和 SSL VPN 隧道）。
- 第 14 章，高可用性，介绍标准 VRRP 和增强功能。
- 第 15 章，虚拟系统，介绍虚拟系统和虚拟网络。
- 第 16 章，监控，介绍信息监控功能。
- 第 17 章，报表，介绍生成报表的功能。
- 第 18 章，旁路 IPS，介绍 NISG-IPS 部署在旁路模式下的功能配置并给出配置范例。

文档约定

表 1 图标约定

 路由器	 服务器	 用户
 交换机	 数据库	 用户
 NISG-IPS	 个人电脑	 笔记本

相关手册

除了本手册，管理员还可获得产品附带的以下文档：

- *东软 NetEye 集成安全网关入侵防御系统 V4.2 配置案例集*
- *东软 NetEye 集成安全网关入侵防御系统 V4.2 命令参考指南*
- *东软 NetEye 集成安全网关入侵防御系统 V4.2 日志参考指南*
- *东软 NetEye 集成安全网关入侵防御系统 V4.2 SNMP MIB 参考指南*

1 快速向导

本章描述以下内容：

1.1 安装硬件设备和系统

关于硬件安装的详细信息，请参见*东软 NetEye 集成安全网关入侵防御系统安装向导*。

NISG-IPS 出厂时已经安装好系统，用户无需自己安装。

不同的硬件型号配备的接口不同，接口的编号方式也有所不同，包括：

- MGT 口：该接口为管理接口，只能转发管理流量，不转发业务流量。
- ETH x：表示板载接口， x 表示接口编号。
- ETH-sxpx：表示接口卡接口。 sxpx 表示接口板上的接口编号， sx 表示接口所在接口板编号， px 表示接口编号。

MGT 口为一个物理接口，专门转发管理流量。板载接口和接口卡接口都可在 WebUI 上设置为逻辑上的管理接口。

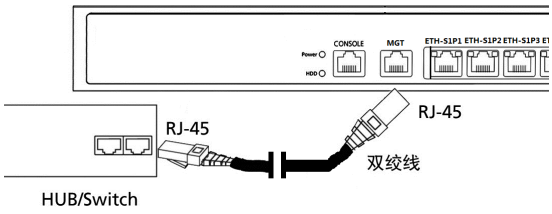
本章以含有 MGT 口和 ETH-sxpx 接口为例进行阐述。

1.2 连接设备和管理 PC

1.2.1. 连接以太网接口

1. 使用 RJ-45 网线连接管理 PC 至 NISG-IPS 的管理接口，或直接连接 NISG-IPS 的管理接口到 LAN。

   如下图所示，使用一根 5 类、超 5 类或 6 类的非屏蔽双绞线或屏蔽双绞线连接设备，两端均使用 RJ-45 接头。其中一端连接 NISG-IPS 设备的以太网接口，另一端连接局域网 HUB 或交换机设备的以太网接口。



2. 在管理 PC 上添加 IP 地址 192.168.1.200，掩码设为 255.255.255.0。

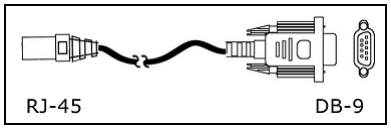
用于管理 NISG-IPS 的管理 PC 上至少应安装有以下一种浏览器：

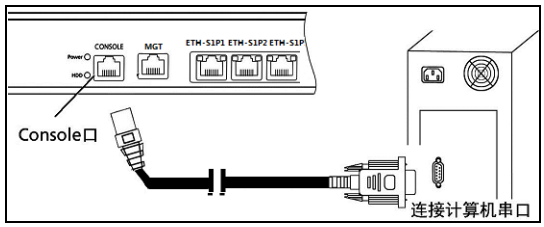
- Microsoft Internet Explorer （7.0 或更高版本）
- Mozilla Firefox （10.0 或更高版本）
- Google Chrome （9.0 或更高版本）
- Opera （11.x 或更高版本）
- Safari （5.0 或更高版本）

1.2.2. 连接 Console 口

Console 访问默认是允许的，管理员可以通过 Conole 口管理 NISG-IPS。

将 Console 线带有 RJ-45 连接头的一端连接到 Console 口，带有 DB-9 连接头的一端连接到管理终端的串口。





选用任何兼容标准 VT100 并带有 RS-232 接口 （标准 DTE 接口）的终端或模拟终端，并进行如下配置：

- 波特率：9600
- 数据位：8
- 奇偶校验位：无
- 停止位：1

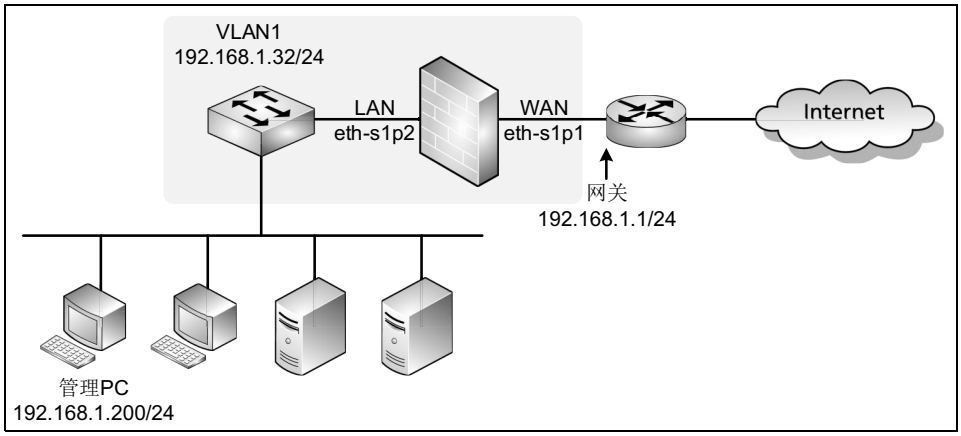
1.3 部署 NISG-IPS 到网络

在部署 NISG-IPS 时，需选择一种工作模式，并将 NISG-IPS 部署到网络中：

提示：后续小节都按照此处三种模式的拓扑描述如何对 NISG-IPS 进行配置。

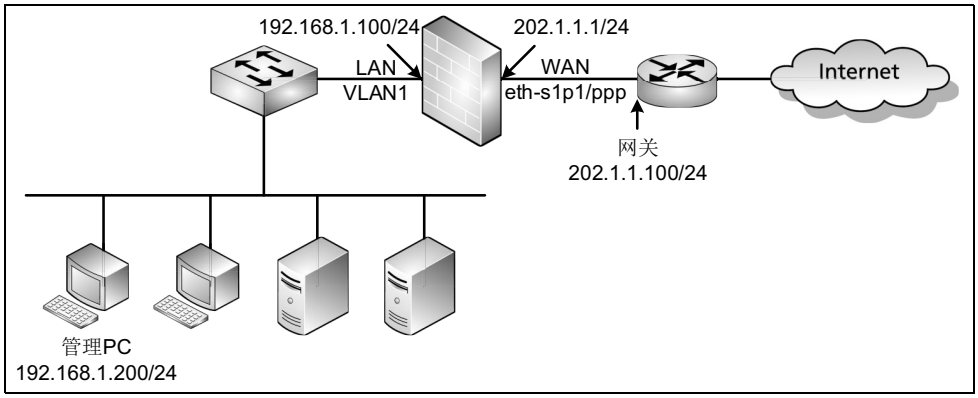
1.3.1 透明模式

NISG-IPS 可部署在私有网络的现有网关后面，无缝集成到现有网络中。透明模式下，NISG-IPS 主要用于数据的二层转发。当客户需要在不改变网络拓扑的情况下提供安全保护时，可使用此工作模式。



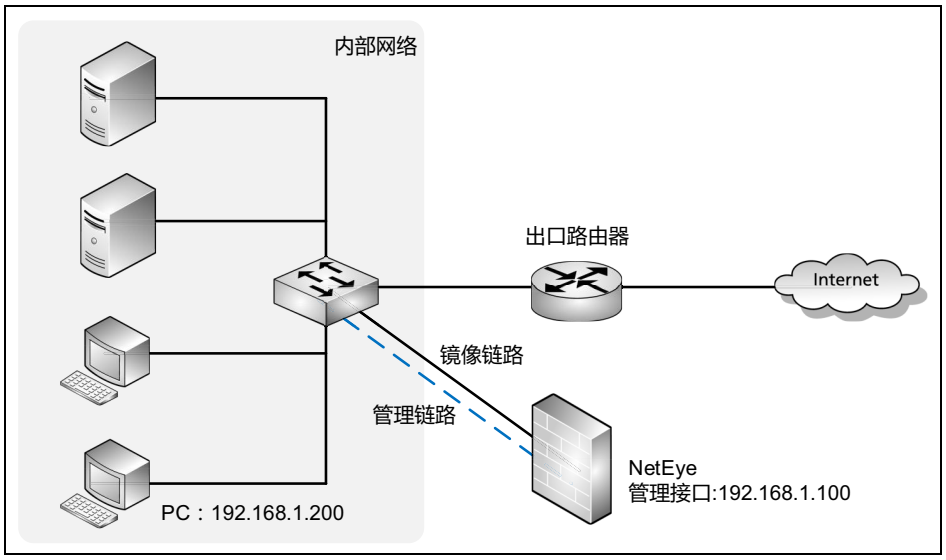
1.3.2 路由模式

NISG-IPS 可部署在公网和私网之间，作为局域网内主机的默认网关。路由模式下，NISG-IPS 可以让工作在不同网段之间的主机以三层路由的方式进行通信。



1.3.3 旁路模式

NISG-IPS 可旁路模式部署与网络中，对网络进行监控。流量经外部设备镜像至 NISG-IPS， NISG-IPS 对其进行监控检测。



1.4 使用向导进行初始化配置

NISG-IPS 提供一个 WebUI 向导用于完成初始化。本节介绍以下内容：

提示：旁路模式受 License 控制，如系统未被上载 License，或上载的 License 不包含旁路模式特性，则在配置向导中不会出现有关旁路模式的显示。

1.4.1 登录

在产品出厂、系统重置或重装后，当管理员首次通过 WebUI 登录 NISG-IPS 时，配置向导会自动弹出。管理员也可以点击 WebUI 界面右上角的按钮，随时开启向导功能。本文中以产品出厂后管理员首次登录为例进行阐述。

1. 启动 NISG-IPS 设备。
2. 在管理主机上打开浏览器，输入 https://192.168.1.100。出现一个证书错误提示页面。点击“继续浏览此网站（不推荐）”选择信任 NISG-IPS 证书。

3. 出现登录页面，在文本框中输入缺省用户名 admin，密码 neteye 以及验证码，点击**登录**按钮。

提示：如果连续输入密码错误达到 5 次，账号将被锁定 20 分钟。

1.4.2 基础设置

4. 登录后系统弹出**欢迎**页面。在下拉框中选择相应的语言，点击**后一页**。

提示：在首次登录且不愿使用配置向导进行初始化时，您可以点击**跳过**按钮，跳过配置向导，采用其他方式配置系统。

5. 修改管理员密码，点击**后一页**。

提示：您也可选择点击**跳过**按钮，跳过密码设置步骤，使用缺省密码。但是，为了安全考虑，我们建议您不要使用初始缺省密码。

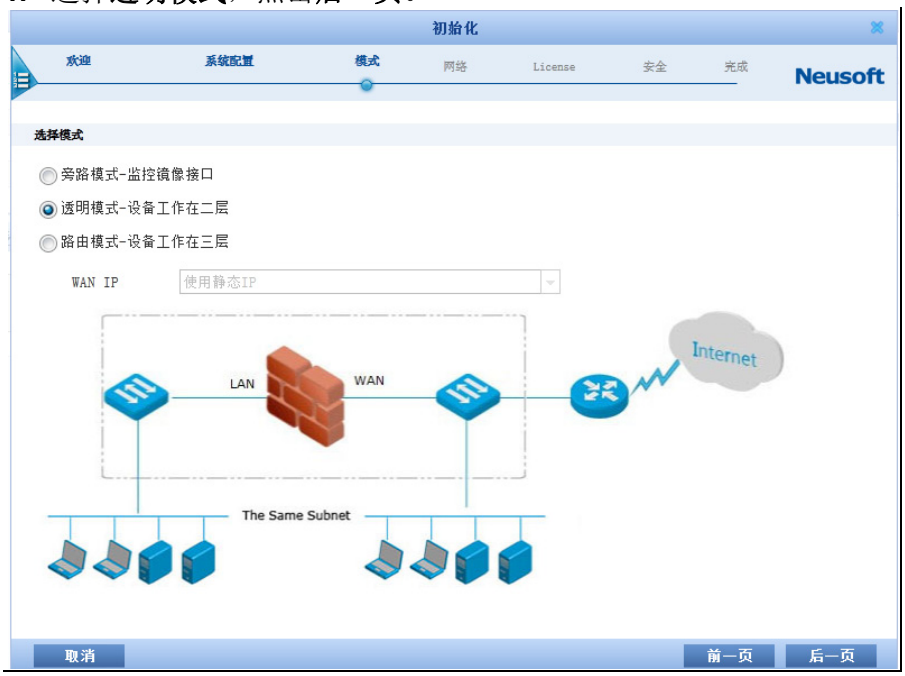
6. 根据需要配置主机名、系统时间和 NTP 服务器地址等内容，点击**后一页**。

7. 选择一种工作模式
   - 1.4.3 配置透明模式
   - 1.4.4 配置路由模式
   - 1.4.5 配置旁路模式

1.4.3 配置透明模式

1.4.3.1 网络和安全设置

1. 选择**透明模式**，点击**后一页**。



2. 配置设备端口分配，点击**后一页**。

   设备端口分配有两种方案可供选择，默认 WAN/LAN 和 WAN/LAN/OPT。如果选择 WAN/LAN，则第一个带编号的端口为 WAN 域，剩下的所有端口为 LAN 域；如果选择 WAN/LAN/OPT，则带编号的端口中第一个端口划分为 WAN 域，最后一个端口划分为 OPT 域，中间所有端口划分为 LAN 域。

3. 配置网络设置，点击**后一页**。

- VLAN 设置：
  - IP 地址 / 掩码：创建 VLAN，并为 VLAN 配置 IP 地址和掩码。创建 VLAN 后所有带编号的接口都处于 VLAN 中。
  - 网关：VLAN 的网关。
  - DNS 服务器：用于解析 NISG-IPS 到 Internet 的域名请求。
  - VLAN 服务：启用或禁用可连接 NISG-IPS 的服务。勾选表示启用。
- 带外管理接口配置 （如为没有 MGT 口的机型，在配置向导处不会显示此项）：
  - IP 地址 / 掩码：配置带外管理口的 IP 地址和掩码。
  - 服务配置：启用或禁用可连接 NISG-IPS 的服务。勾选表示启用。

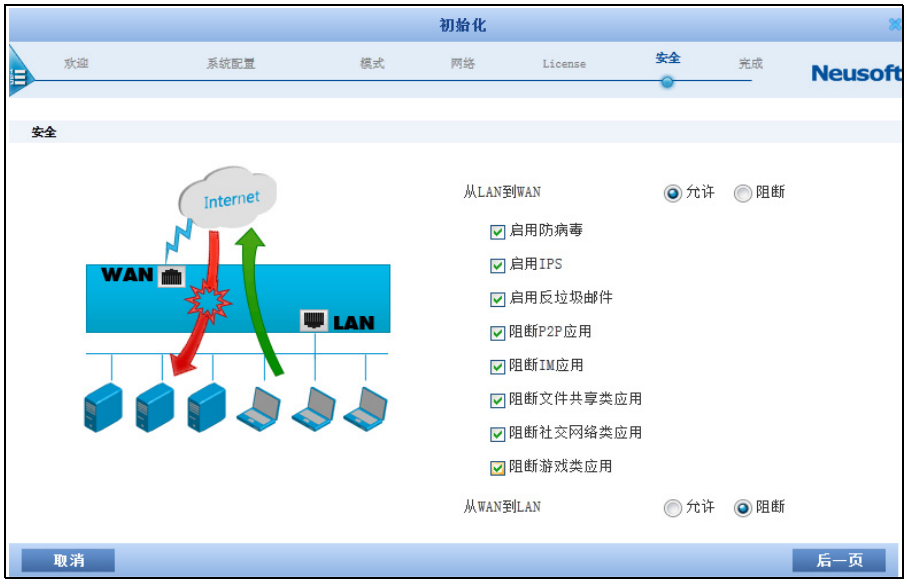
4. 点击**是**，然后点击**结束**，提交所做的基本配置并继续进行安全配置；或者点击**否**，然后点击**结束**，提交所做的基本配置并退出向导。

提示：点击**结束**后，将无法点击**前一页**返回基本配置页面进行修改。

5. （可选）如果系统中不存在 License，向导将跳转到 License 激活页面。您必须在激活 License 后才可做后续安全配置。 License 激活支持自动和手动两种方式：
   - **自动**：选择**自动获取 License**，点击**激活**按钮。点击按钮前，请确保 NISG-IPS 可以访问互联网。
   - **手动**：选择**手动输入 License**，输入 License 字符串，然后点击**激活**按钮。

提示：如果设备已有可用 License，向导会跳过此步，请直接执行步骤 6。

6. 设置访问安全控制动作，启用或禁用安全功能，点击**后一页**。



提示：具体可配置安全功能由 License 控制，上图显示所有安全功能。

7. 检查详细配置信息，点击**结束**。

8. 初始化成功后，点击**关闭**按钮退出向导。

提示：如果在向导中执行了激活 License 操作，系统将出现重启提示，请根据提示重启系统。否则， License 将不会生效。重启过程将持续三分钟左右，请三分钟后再进行登录。

1.4.3.2 通过 WebUI 确认初始化配置

要确认初始化配置是否生效，请执行以下操作：

1. 输入用户名和密码进行登录。
2. 查看主页上方的主机名和系统时间，可以看到新的主机名和系统时间已生效。

3. 选择**网络** > **接口**查看接口配置。可以看到新建 VLAN 接口 vlan1 包含 eth-s1p1 和 eth-s1p2。

4. 选择**网络** > **安全域**查看安全域配置 。可以看到新建二层安全域 LAN 和 WAN，WAN 包含 eth-s1p1， LAN 包含 eth-s1p2。安全域被缺省访问策略引用。

5. 选择**网络** > **路由** > **缺省路由**查看默认网关是否已经修改。下面是缺省配置。

6. 选择**防火墙** > **访问策略**。可以看到系统已经添加两条缺省访问策略，允许 LAN 到 WAN 的访问，同时拒绝 WAN 到 LAN 的访问。

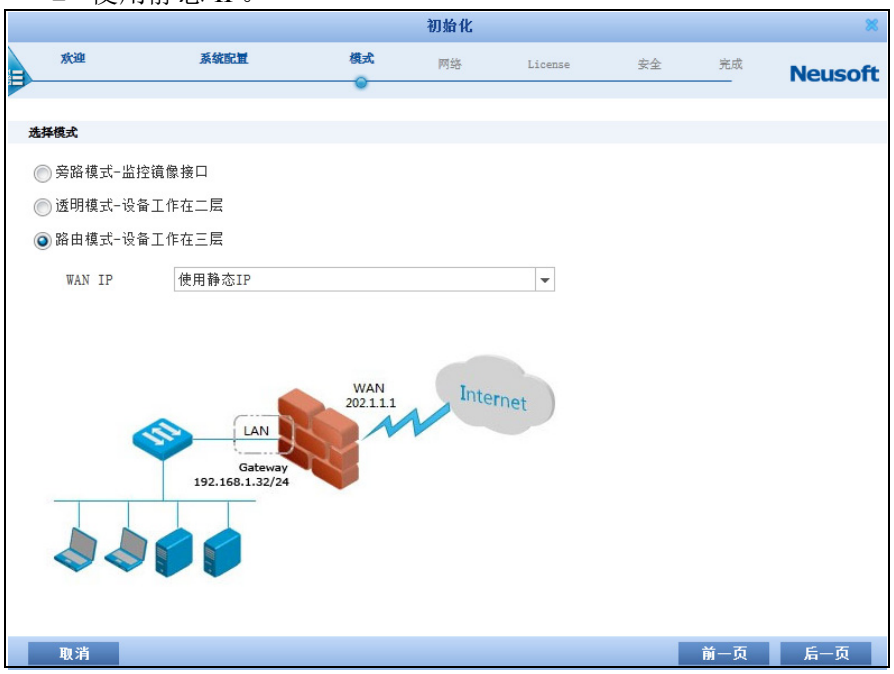
7. 选择**系统** > **服务配置** > **访问设置**查看服务是否已被启用或禁用。

提示：访问服务允许的 IP 地址范围默认为 0.0.0.0-255.255.255.255，管理员应根据实际情况修改允许访问的 IP 地址范围。

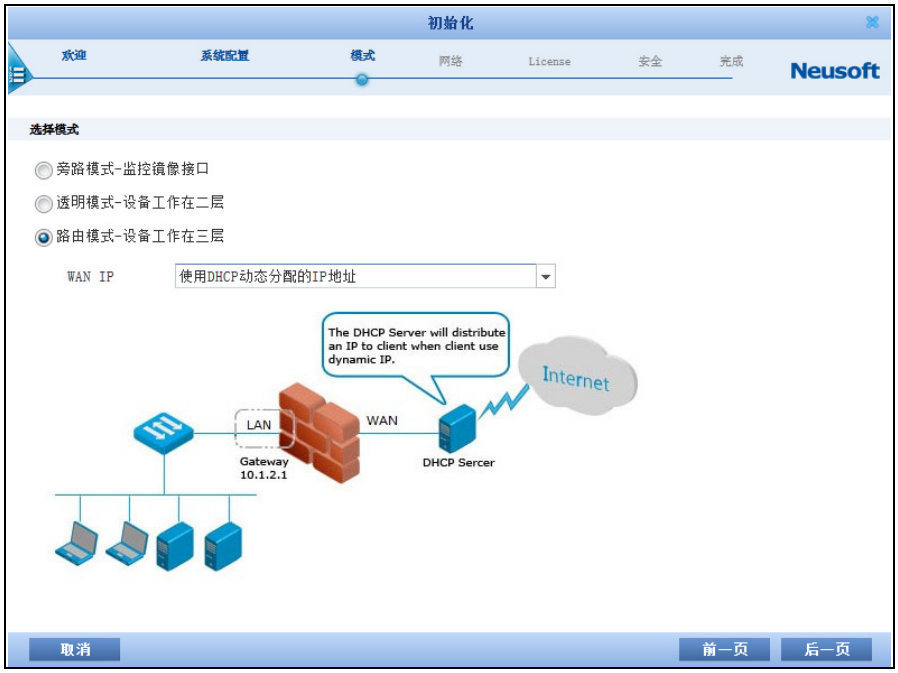
1.4.4 配置路由模式

1.4.4.1 网络和安全配置

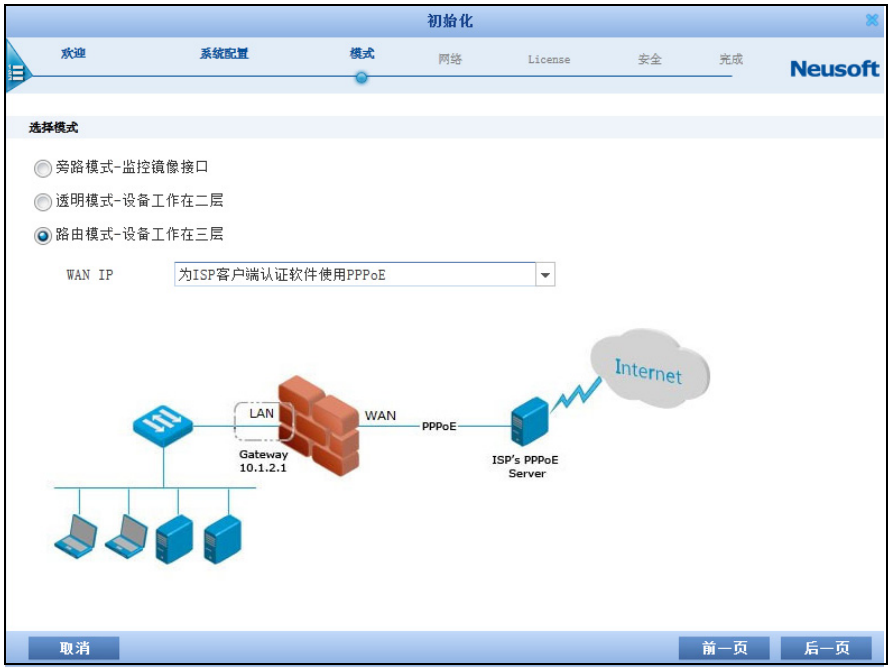
1. 选择**路由模式**。选择以下任意一种 WAN 接口获取 IP 地址的方式。点击**后一页**。
   - 使用静态 IP。



- 使用 DHCP 动态分配的 IP 地址。



- 为 ISP 客户端认证软件使用 PPPoE。



2. 配置设备端口分配，点击**后一页**。

   设备端口分配有两种方案可供选择，默认 WAN/LAN 和 WAN/LAN/OPT。如果选择 WAN/LAN，则第一个带编号的端口为 WAN 域，剩下的所有端口为 LAN 域；如果选择 WAN/LAN/OPT，则带编号的端口中第一个端口划分为 WAN 域，最后一个端口划分为 OPT 域，中间所有端口划分为 LAN 域。

3. 配置 WAN 设置，点击**后一页**。

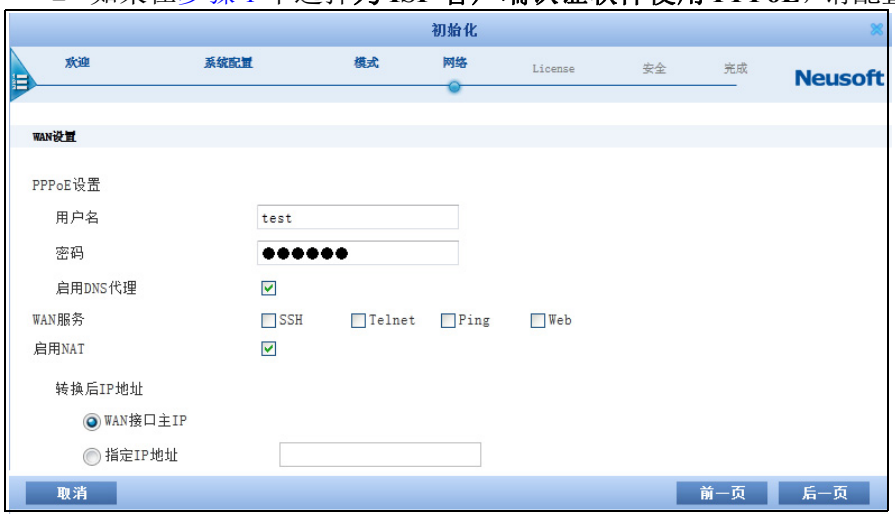
   - 如果在步骤 1 中选择**使用静态 IP**，请配置以下 WAN 页面。

   - IP 地址/掩码：WAN 接口的 IP 地址。此处的静态 IP 地址由上游网络管理员分配，请向上游网络管理员索取，请不要私自配置 IP 地址。
   - WAN 服务：WAN 服务表示在外网可使用的能够管理系统的服务，缺省情况下，不允许外网终端管理系统。
   - 网关：WAN 接口的网关。
   - DNS：DNS 服务器 IP 地址。
   - 启用 NAT：如果此处选择启用 NAT，系统将自动生成一条名为 def_lw 的 SNAT 规则，将数据包的源 IP 地址转换为指定的转换后 IP 地址。该指定 IP 地址不能为 192.168.255.254。

- 如果在步骤 1 中选择**使用 DHCP 动态分配的 IP 地址**，请配置以下 WAN 页面。

  - 启用 DNS 代理：NISG-IPS 设备代理 DNS 服务器。
  - WAN 服务：WAN 服务表示在外网可使用的能够管理系统的服务，缺省情况下，不允许外网终端管理系统。
  - 启用 NAT：如果此处选择启用 NAT，系统将自动生成一条名为 def_lw 的 SNAT 规则，将数据包的源 IP 地址转换为指定的转换后 IP 地址。该指定 IP 地址不能为 192.168.255.254。

- 如果在步骤 1 中选择**为 ISP 客户端认证软件使用 PPPoE**，请配置以下 WAN 页面。



  - 用户名、密码：PPPoE 登录时需要的用户名和密码。
  - 启用 DNS 代理：NISG-IPS 设备代理 DNS 服务器。
  - WAN 服务：WAN 服务表示在外网可使用的能够管理系统的服务，缺省情况下，不允许外网终端管理系统。
  - 启用 NAT：如果此处选择启用 NAT，系统将自动生成一条名为 def_lw 的 SNAT 规则，将数据包的源 IP 地址转换为指定的转换后 IP 地址。该指定 IP 地址不能为 192.168.255.254。

4. 配置 LAN 设置，点击**后一页**。

如果管理员选择在 LAN 上启用 DHCP 服务器角色为内网 DHCP 客户端分配 IP 地址，需要设置 DHCP IP 地址池的起始和终止 IP 地址。还可以设置为 DHCP 客户端分配的网关地址和 DNS 服务器地址。

起始和终止 IP 地址必须和配置的 LAN 的 IP 地址在同一网段上。

提示：如设备没有 MGT 口，在配置向导处不会显示**带外管理接口配置**相关内容。

5. 点击**是**，然后点击**结束**，提交所做的基本配置并继续进行安全配置；或者点击**否**，然后点击**结束**，提交所做的基本配置并退出向导。

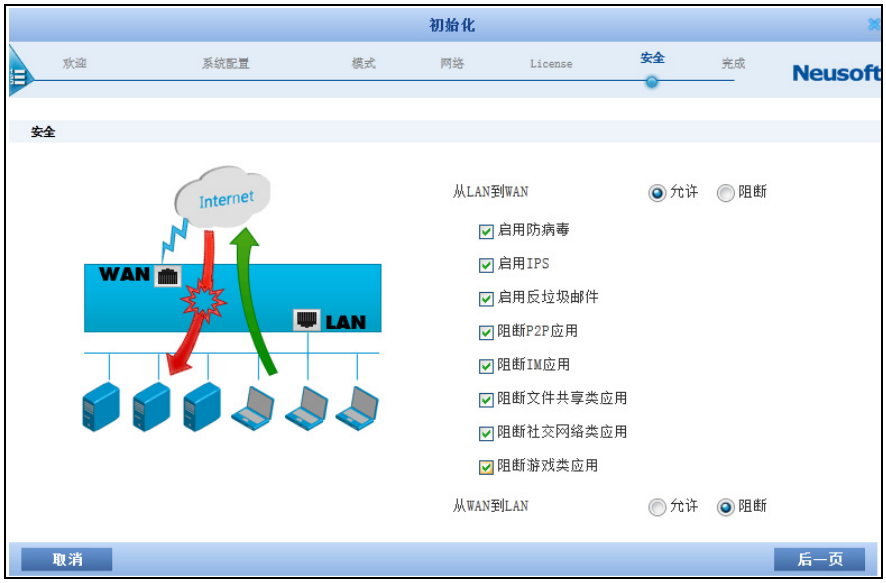
提示：点击**结束**后，将无法点击**前一页**返回基本配置页面进行修改。

6. （可选）如果系统中不存在 License，向导将跳转到 License 激活页面。您必须在激活 License 后才可做后续安全配置。 License 激活支持自动和手动两种方式：

- **自动**：选择**自动获取 License**，点击**激活**按钮。点击按钮前，请确保 NISG-IPS 可以访问互联网。
- **手动**：选择**手动输入 License**，输入 License 字符串，然后点击**激活**按钮。

提示：如果设备已有可用 License，向导会跳过此步，请直接执行步骤 7。

7. 设置访问安全控制动作，启用或禁用安全功能，点击**后一页**。



提示：具体可配置安全功能由 License 控制，上图显示所有安全功能。

8. 检查详细配置信息，点击**结束**。

9. 初始化成功后，点击**关闭**按钮退出向导。

提示：如果执行了激活 License 操作，系统将出现重启提示，请根据提示重启系统。否则， License 将不会生效。重启过程将持续三分钟左右，请三分钟后再进行登录。

1.4.4.2 通过 WebUI 确认初始化配置

要确认初始化配置是否生效，请执行以下操作：

1. 输入用户名和密码进行登录。
2. 查看主页上方的主机名和系统时间，可以看到新的主机名和系统时间已生效。

3. 选择**网络** > **接口**查看接口配置。
   - 如果选择**使用静态 IP**，显示如下：

接口	链路状态	接口状态	模式	MAC地址	属于	IP地址
eth-s1p1			Layer3	00:0C:29:A8:AF:0D		202.1.1.1/24(静态)
eth-s1p2			Layer2 (Access)	00:0C:29:A8:AF:17	vlan1	
eth-s1p3			Layer2 (Access)	00:0C:29:A8:AF:21	vlan1	
eth-s1p4			Layer2 (Access)	00:0C:29:A8:AF:2B	vlan1	
mgt			Layer3	00:0C:29:A8:AF:2E		10.1.3.127/21(静态)
vlan1			Layer3	00:0C:29:A8:AF:2F		192.168.1.100/24(静态)

   - 如果选择**使用 DHCP 动态分配的 IP 地址**，显示如下：

接口	链路状态	接口状态	模式	MAC地址	属于	IP地址
eth-s1p1			Layer3	00:0C:29:A8:AF:0D		202.1.1.1/24(DHCP)
eth-s1p2			Layer2 (Access)	00:0C:29:A8:AF:17	vlan1	
eth-s1p3			Layer2 (Access)	00:0C:29:A8:AF:21	vlan1	
eth-s1p4			Layer2 (Access)	00:0C:29:A8:AF:2B	vlan1	
mgt			Layer3	00:0C:29:A8:AF:2E		10.1.3.127/21(静态)
vlan1			Layer3	00:0C:29:A8:AF:2F		192.168.1.100/24(静态)

   - 如果选择**为 ISP 客户端认证软件使用 PPPoE**，显示如下：

接口	链路状态	接口状态	模式	MAC地址	属于	IP地址
eth-s1p1			Layer2 (Access)	00:0C:29:A8:AF:0D		
eth-s1p2			Layer2 (Access)	00:0C:29:A8:AF:17	vlan1	
eth-s1p3			Layer2 (Access)	00:0C:29:A8:AF:21	vlan1	
eth-s1p4			Layer2 (Access)	00:0C:29:A8:AF:2B	vlan1	
mgt			Layer3	00:0C:29:A8:AF:2E		10.1.3.127/21(静态)
vlan1			Layer3	00:0C:29:A8:AF:2F		192.168.1.100/24(静态)
ppp0			Layer3			202.1.1.1

4. 选择**网络** > **安全域**查看新建的三层安全域 LAN 和 WAN 。
   - 在选择**使用静态 IP** 和**使用 DHCP 动态分配的 IP 地址**，显示如下：

名称	类型	接口	引用
WAN	基于三层接口	eth-s1p1	
LAN	基于三层接口	vlan1	

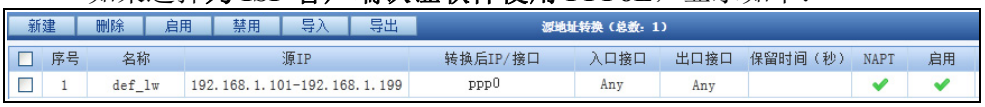
   - 在选择**为 ISP 客户端认证软件使用 PPPoE**，显示如下：

名称	类型	接口	引用
WAN	基于三层接口	ppp0	
LAN	基于三层接口	vlan1	

5. 选择**网络 > 地址转换 > 源地址转换**，查看系统是否已按初始化配置创建了一条 SNAT 规则。

   - 如果选择**使用静态 IP** 和**使用 DHCP 动态分配的 IP 地址**，显示如下：

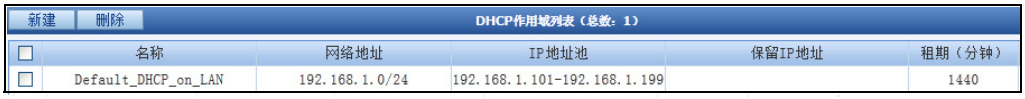
   - 如果选择**为 ISP 客户端认证软件使用 PPPoE**，显示如下：



6. 选择**网络 > 路由 > 缺省路由**，查看缺省路由是否已按初始化配置修改。

7. 选择**防火墙 > 访问策略**，查看系统是否已创建了两条访问策略，允许 LAN 到 WAN 的访问，同时拒绝 WAN 到 LAN 的访问。

8. 选择**网络 > DHCP > DHCP 作用域**，查看是否创建成功缺省的 DHCP 作用域。



9. 选择**系统 > 服务配置 > 访问设置**，查看相关服务是否已经启用或禁用。

提示：访问服务允许的 IP 地址范围默认为 0.0.0.0-255.255.255.255，管理员应根据实际情况修改允许访问的 IP 地址范围。

1.4.5 配置旁路模式

1.4.5.1 网络设置

1. 选择**旁路模式**，点击**后一页**。

2. 设置网络参数，点击**后一页**。

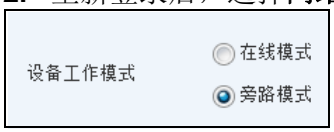
提示：此处的 IP 地址缺省配置在现有的管理接口上，如需另外增加或改变管理接口，需在初始化之后，在**网络 > 接口**处进行配置。

3. 点击**结束**，提交所做的基本配置。

提示：点击**结束**后，配置生效，您需要激活 License 后才能正常使用。激活 License 具体步骤请参见 1.5.8 导入 License。

1.4.5.2 通过 WebUI 确认初始化配置

1. 检查系统时间等项是否正确。
2. 重新登录后，选择**网络 > 工作模式**，检验是否为旁路模式。



3. 选择**网络 > 接口**，检查管理接口的 IP 地址是否为所配置 IP 地址。

1.5 使用 WebUI 进行初始化配置

选择配置以下任意一种工作模式：

要配置功能，需要导入有效的 License：

1.5.1 登录

1. 通过 WebUI 向导登录，步骤同 1.4.1 登录。
2. 在**欢迎**页面选择**简体中文**，点击**跳过**，弹出 WebUI 页面。

1.5.2 WebUI 概述

WebUI 操作按钮如下表所示。

表 2 WebUI 操作按钮

按钮	描述	按钮	描述
	配置锁 （同一时间只能有一个管理用户拥有配置锁）		切换虚拟系统
	保存		编辑系统日期时间
	在线帮助		被引用 （查看引用某条目的策略或防护配置）
	退出 （系统）		移动策略以改变其优先级
	刷新		克隆
	恢复 （系统设置）		（条目）启用状态
	查看		（条目）禁用状态
	下载		过滤条件被启用 （过滤条件用于设置要显示的参数项）
	导出		过滤条件被禁用
	修改密码		添加条目到列表框
	编辑		从列表框删除条目
	关闭窗口 （或删除条目）		向上移动列表中的条目
	调出配置向导		向下移动列表中的条目
	调出 Webshell		

1.5.3 重置密码

要修改缺省登录密码，请执行以下操作：

1. 选择**系统** > **认证** > **管理用户**。

2. 点击 修改密码。

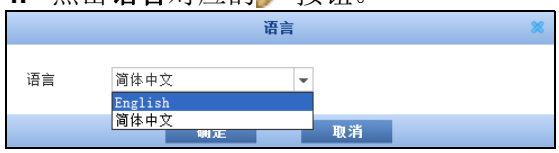
3. 点击**确定**。新密码在下次登录时生效。

1.5.4 设置系统语言 / 主机名 / 系统时间

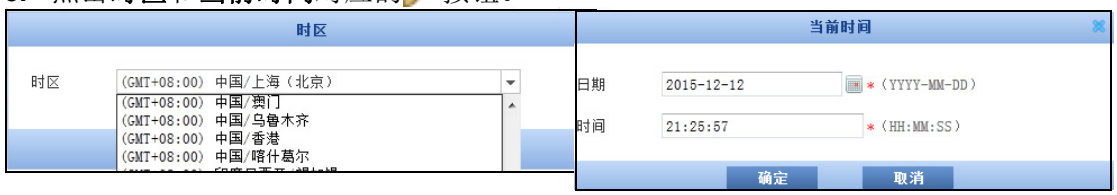
1. 选择**系统** > **概述**。

2. 点击**主机名**对应的按钮，修改主机名。

3. 点击**确定**。
4. 点击**语言**对应的按钮。



5. 选择一种语言，点击**确定**。
6. 点击**时区**和**当前时间**对应的按钮。



7. 编辑系统时间，点击**确定**。
8. 点击。

1.5.5 配置透明模式

1. 选择**网络** > **接口**。设置接口如下：

新建	删除	接口列表				
接口	链路状态	接口状态	模式	MAC地址	属于	IP地址
eth-s1p1			Layer2 (Access)	00:0C:29:A8:AF:0D	vlan1	
eth-s1p2			Layer2 (Access)	00:0C:29:A8:AF:17	vlan1	
mgt			Layer3	00:0C:29:A8:AF:21		10.10.1.10/24(静态)
vlan1			Layer3	00:0C:29:A8:AF:2B		192.168.1.32/24(静态)

设置接口的具体方法：

a. 点击**新建 > VLAN**，创建 VLAN 接口 vlan1 ；

b. 添加 eth-s1p1 和 eth-s1p2 接口到 vlan1。

2. 选择**网络** > **安全域**，创建二层安全域 LAN 和 WAN。添加 eth-s1p2 到 LAN，添加 eth-s1p1 到 WAN。

新建	删除	安全域列表（总数：2）	
	名称	类型	接口
	WAN	基于二层接口(vlan1)	eth-s1p1
	LAN	基于二层接口(vlan1)	eth-s1p2

3. 选择**防火墙** > **访问策略**，创建如下访问策略：

新建	删除	启用	禁用	导入	导出	访问策略列表（总数：2）						
	序号	名称	源安全域	源IP	目的安全域	目的IP/域名	服务	动作	启用
	1	def_lw	LAN	任意	WAN	任意	任意	允许	
	2	def_wl	WAN	任意	LAN	任意	任意	拒绝	

4. 点击 。

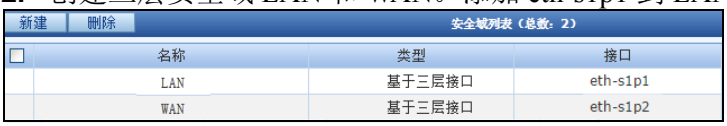
1.5.6 配置路由模式

此处 eth-s1p1 为连接内部的接口， eth-s1p2 为连接外部的接口。

1.5.6.1 以太网连接

1. 选择**网络** > **接口**。设置接口如下：

2. 创建三层安全域 LAN 和 WAN。添加 eth-s1p1 到 LAN，添加 eth-s1p2 到 WAN。



3. 修改缺省网关为 202.1.1.100。

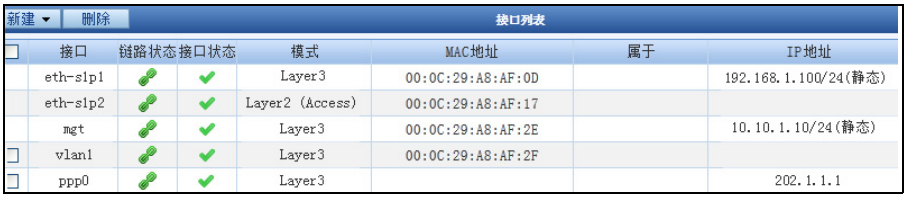
4. 创建 SNAT 规则，将 192.168.1.0/24 转换成 eth-s1p2 的 IP 地址：

5. 创建访问策略，允许 LAN 到 WAN 的访问，拒绝 WAN 到 LAN 的访问。

6. 点击 。

1.5.6.2 PPPoE 连接

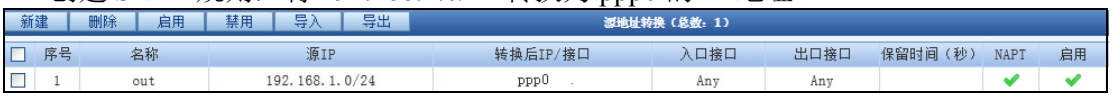
1. 选择**网络** > **接口**。设置接口如下：



2. 创建三层安全域 LAN 和 WAN，添加 eth-s1p1 到 LAN，添加 ppp0 到 WAN。

3. 修改缺省网关为 202.1.1.100。

4. 创建 SNAT 规则，将 192.168.1.0/24 转换为 ppp0 的 IP 地址。

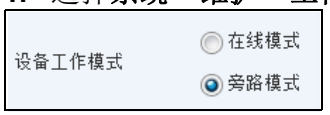


5. 创建访问策略，允许 LAN 到 WAN 的访问，拒绝 WAN 到 LAN 的访问。

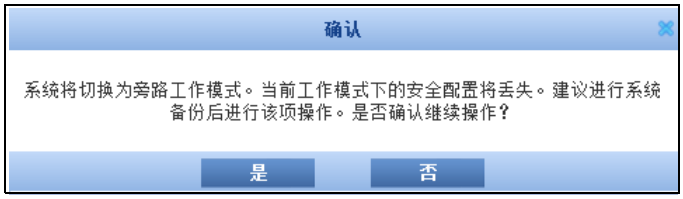
6. 点击 。

1.5.7 配置旁路模式

1. 选择**系统 > 维护 > 工作模式**，选择旁路模式。



2. 系统弹出提示框，点击**确定**。



3. 选择**网络 > 接口**，在接口页面修改接口模式和 IP 地址。

1.5.8 导入 License

在进行以下步骤之前，请确认您已将有效 License 文件存放到本地 PC。

1. 选择**系统 > 维护 >License**。点击**导入**，上载 License 文件。系统提示重启，点击**是**。

提示：您也可以点击**自动获取 License** 按钮在线激活 License，但前提是您的 NISG-IPS 设备与 License 服务器之间是互通的。

2. 系统重启后自动跳转到登录页面，您可以登录后通过 WebUI 继续配置 NISG-IPS。

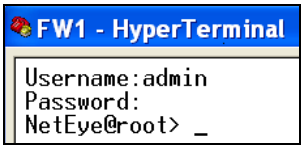
1.6 使用 CLI 进行初始化配置

1.6.1. 通过 Console 登录

1. 在管理 PC 上选择**开始** > **所有程序** > **附件** > **通讯** > **超级终端**。
   a. 输入区域码和连接名称，并在下面的对话框中依次点击**确定**。

   b. 在第一个下拉框中选择 9600，点击**确定**。

2. 按 **Enter** 键，根据下面的提示输入缺省管理用户名和密码登录 NISG-IPS。



如果连续输入密码错误达到 5 次，账号将被锁定 20 分钟。

1.6.2 CLI 基本信息

首次登录 CLI 会出现如下提示符：

NetEye@root>

在提示符下可输入以下命令：

- **show 命令**：用于查看系统配置信息，如 **show system info**、 **show interface brief**、**show service** 和 **show route**。
- 简单操作命令，如 **clear**、 **halt**、 **debug** 和 **save config**。
- **configure mode override**：如果输入此命令，其他管理员将不能继续配置 NISG-IPS，除非他们重新抢占配置锁，不过他们已经提交的修改不会丢失。执行此命令后，系统提示如下提示符：NetEye@root-system]。您可以在此命令符下输入下表中的命令进入相应的配置模式。

命令	配置项	提示符
vlan *vlan_id*	VLAN 接口	NetEye@root-system-vlan1]
interface ethernet *interface_id*	以太网接口	NetEye@root-system-if-eth-s1p1]
channel *channel_id*	以太网通道接口	NetEye@root-system-if-ch1]
tunnel *tunnel_id*	VPN 隧道接口	NetEye@root-system-tunnel1]
rint *rint_id*	冗余接口	NetEye@root-system-rint1]
veth *veth_id*	虚拟接口	NetEye@root-system-veth1]
loopback *lo_id*	环回接口	NetEye@root-system-lo1]
pppoe *pppoe_id*	PPPoE 接口	NetEye@root-system-pppoe1]
cluster	集群	NetEye@root-system-cluster]
virtual router *vrid*	虚拟路由器	NetEye@root-system-vr1]
detection group *group_id*	虚拟路由器探测组	NetEye@root-system-dg1]
policy route *policy_name*	基于策略的路由	NetEye@root-system-routepolicy-test]
vpn	VPN	NetEye@root-system-vpn]
sslvpn	SSL VPN	NetEye@root-system-sslvpn]
vsys *vsys _id*	虚拟系统	NetEye@root-system-vsys1]
vnet *vnet_id*	虚拟网络	NetEye@root-system-vnet1]

输入以上任意一种命令，您可以对相应的配置项进行配置，如接口、集群 / 虚拟路由器、 VPN、 Vsys 等。在上面的例子中，你可以用 **ip address** 为接口配置 IP 地址。

CLI 支持：

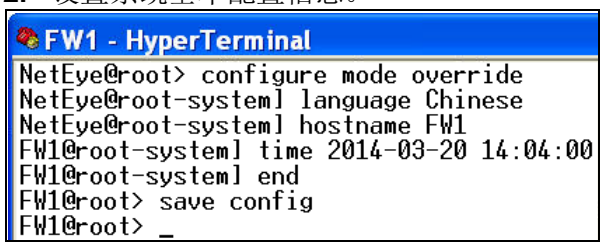
- 在关键字或参数后输入 "**?**"，系统会提示该关键字或参数的帮助信息。
- 在关键字或参数后面加空格，然后再输入 "**?**"，系统会提示下一个关键字或参数。
- 可以通过按 Tab 键，补齐当前输入的关键字。如果有多个可选关键字，按 Tab 键则显示所有关键字。
- 支持缩写。例如，可以将命令 **configure mode** 缩写为 **con mo**。

下面是如何使用 CLI 为 VLAN 接口配置 IP 地址的例子：

```
Username:admin
Password:
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] ip address 192.168.1.32 255.255.255.0
NetEye@root-system-vlan1] end
NetEye@root> save config
NetEye@root> _
```

1.6.3 设置系统语言 / 主机名 / 系统时间

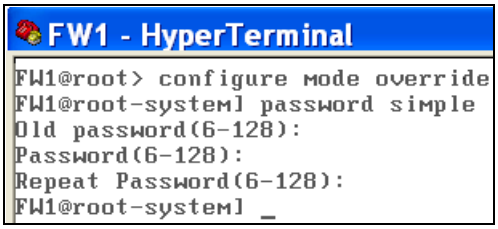
1. 使用 **show system info** 命令查看系统信息。
2. 设置系统基本配置信息。



1.6.4 重置密码

通过以下命令重置缺省登录密码：

1. 输入 **configure mode override** 命令，按 Enter 键。
2. 执行 **password simple** 命令。
3. 输入旧密码。
4. 输入新密码。
5. 重复新密码。



1.6.5 配置透明模式

1. 配置 NISG-IPS 工作在透明模式：

```
FW1 - HyperTerminal
FW1@root-system] interface ethernet mgt
FW1@root-system-if-mgt] ip address 10.10.1.10 255.255.255.0
FW1@root-system-if-mgt] exit
FW1@root-system] vlan 1
FW1@root-system-vlan1] hold ethernet eth-s1p1
FW1@root-system-vlan1] hold ethernet eth-s1p2
FW1@root-system-vlan1] ip address 192.168.1.32 255.255.255.0
FW1@root-system-vlan1] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] zone LAN based-layer2 vlan 1 eth-s1p1
FW1@root-system] zone WAN based-layer2 vlan 1 eth-s1p2
FW1@root-system] policy access LANtoWAN LAN any WAN any any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any any deny enable
FW1@root-system] end
FW1@root> save config
FW1@root> _
```

2. 查看接口配置信息：

```
FW1 - HyperTerminal
FW1@root> show interface brief
Name       Active     IP Address                    MAC               Held In
terfaces      MTU  Vsys
mgt        on         10.10.1.10/24(Static)         00:0C:29:DB:68:F0
              1500 root
vlan1      on         192.168.1.32/24(Static)       00:0C:29:DB:69:11 eth-s1p
1~            1500 root

Name       Active     Status     Speed      Duplex     Mode              Vlan Li
st
eth-s1p1   on         up         1000Mb/s   Full       Layer2 Access     vlan1

eth-s1p2   on         up         1000Mb/s   Full       Layer2 Access     vlan1

mgt        on         up         1000Mb/s   Full       Layer3
```

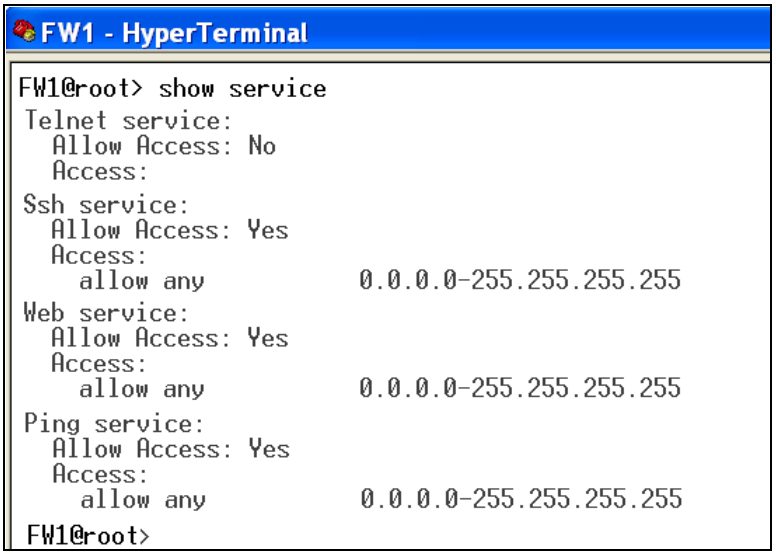
3. 查看安全域信息：

```
FW1@root> show zone
Name              Refcount  Policy                                Descriptio
n
LAN               2         Access Policies
WAN               2         Access Policies
FW1@root> _
```

4. 查看访问策略：

```
FW1@root> show policy access
Number Name                From      To        Source ip       Destination ip
Source users Services      Action State  Tunnel
1      LANtoWAN            LAN       WAN       Any Ip          Any Ip
any user     any           permit enable
2      WANtoLAN            WAN       LAN       Any Ip          Any Ip
any user     any           deny   enable
FW1@root> _
```

5. 查看服务设置：



提示：访问服务允许的 IP 地址范围默认为 0.0.0.0-255.255.255.255，管理员应根据实际情况修改允许访问的 IP 地址范围。

1.6.6 配置路由模式

此处 eth-s1p1 为连接内部的接口， eth-s1p2 为连接外部的接口。

1.6.6.1 以太网连接

1. 设置 NISG-IPS 工作在路由模式并通过以太网接口访问 Internet：

FW1 - HyperTerminal

```
FW1@root-system] interface ethernet eth-s1p2
FW1@root-system-if-eth-s1p2] working-type layer3-interface
FW1@root-system-if-eth-s1p2] ip address 202.1.1.1 255.255.255.0
FW1@root-system-if-eth-s1p2] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] interface ethernet eth-s1p1
FW1@root-system-if-eth-s1p1] working-type layer3-interface
FW1@root-system-if-eth-s1p1] exit
FW1@root-system] zone LAN based-layer3 eth-s1p1
FW1@root-system] zone WAN based-layer3 eth-s1p2
FW1@root-system] route default gateway 10.1.1.1 interface eth-s1p2
FW1@root-system] policy access LANtoWAN LAN any WAN any any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any any any deny enable
FW1@root-system] policy snat out netmask 192.168.1.0 255.255.255.0 interface eth
-s1p2 napt enable
FW1@root-system] interface ethernet mgt
FW1@root-system-if-mgt] ip address 10.10.1.10 255.255.255.0
FW1@root-system-if-mgt] exit
FW1@root-system] interface ethernet eth-s1p1
FW1@root-system-if-eth-s1p1] ip address 192.168.1.100 255.255.255.0
FW1@root-system] end
FW1@root> save config
```

2. 查看接口信息：

```
FW1@root> show interface brief
Name       Active     IP Address                      MAC               Held In
terfaces      MTU  Vsys
eth-s1p1   on         192.168.1.100/24(Static)        00:0C:29:DB:00:F0
              1500 root
eth-s1p2   on         202.1.1.1/24(Static)            00:0C:29:DB:01:F0
              1500 root
mgt        on         10.10.1.10/24(Static)           00:0C:29:DB:68:F0
              1500 root

Name       Active     Status     Speed      Duplex     Mode              Vlan Li
st
eth-s1p1   on         up         1000Mb/s   Full       Layer3

eth-s1p2   on         up         1000Mb/s   Full       Layer3

mgt        on         up         1000Mb/s   Full       Layer3
```

3. 查看安全域信息：

```
FW1@root> show zone
Name              Refcount  Policy                                  Descriptio
n
LAN               2         Access Policies
WAN               2         Access Policies
FW1@root> _
```

4. 查看访问策略：

```
FW1@root> show policy access
Number Name                From      To        Source ip       Destination ip
Source users Services      Action State  Tunnel
1      LANtoWAN             LAN       WAN       Any Ip          Any Ip
any user     any           permit enable
2      WANtoLAN             WAN       LAN       Any Ip          Any Ip
any user     any           deny   enable
FW1@root> _
```

5. 查看 SNAT 规则：

```
FW1@root> show policy snat

Num  Policy-Name         In-Interface Out-Interface Before-Trans        After-T
rans        Napt  State
1    out                 Any          Any           192.168.1.0/24      eth-s1p2
            True  Enable

FW1@root> _
```

6. 查看服务设置：

FW1 - HyperTerminal

```
FW1@root> show service
Telnet service:
  Allow Access: No
  Access:
Ssh service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
Web service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
Ping service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
FW1@root>
```

提示：访问服务允许的 IP 地址范围默认为 0.0.0.0-255.255.255.255，管理员应根据实际情况修改允许访问的 IP 地址范围。

1.6.6.2 PPPoE 连接

1. 设置 NISG-IPS 工作在路由模式并通过 PPPoE 接口访问 Internet：

```
FW1 - HyperTerminal
FW1@root-system] pppoe 0
FW1@root-system-pppoe0] hold ethernet eth-s1p2
FW1@root-system-pppoe0] username test password neteye
FW1@root-system-pppoe0] active on
FW1@root-system-pppoe0] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] zone LAN based-layer3 eth-s1p1
FW1@root-system] zone WAN based-layer3 ppp0
FW1@root-system] route default gateway 202.1.1.100 interface ppp0
FW1@root-system] policy access LANtoWAN LAN any WAN any any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any any deny enable
FW1@root-system] policy snat out netmask 192.168.1.0 255.255.255.0 interface ppp0
napt enable
FW1@root-system] end
FW1@root> save config
FW1@root> _
```

2. 查看接口信息：

```
FW1@root> show interface brief
Name       Active     IP Address                      MAC               Held In
terfaces      MTU  Vsys
eth-s1p1   on         192.168.1.100/24(Static)        00:0C:29:DB:00:F0
              1500 root
eth-s1p3   on         -                               00:0C:29:DB:02:F0
              1500 root
mgt        on         10.10.1.10/24(Static)           00:0C:29:DB:68:F0
              1500 root

Name       Active     IP Address                      MAC               Held In
terfaces      MTU  Vsys
ppp0       on         202.1.1.1                       -                 eth-s1p2
              1454 root

Name       Active     Status     Speed      Duplex     Mode              Vlan Li
st
eth-s1p1   on         up         1000Mb/s   Full       Layer3

eth-s1p2   on         up         1000Mb/s   Full       Layer2 Access
```

3. 查看安全域信息：

```
FW1@root> show zone
Name              Refcount  Policy                                  Descriptio
n
LAN               2         Access Policies
WAN               2         Access Policies
FW1@root> _
```

4. 查看访问策略：

```
FW1@root> show policy access
Number Name                From      To        Source ip       Destination ip
Source users Services      Action State  Tunnel
1      LANtoWAN             LAN       WAN       Any Ip          Any Ip
any user     any           permit enable
2      WANtoLAN             WAN       LAN       Any Ip          Any Ip
any user     any           deny   enable
FW1@root> _
```

5. 查看 SNAT 规则：

```
FW1@root> show policy snat

Num   Policy-Name         In-Interface Out-Interface Before-Trans        After-T
rans          Napt  State
1     out                 Any          Any           192.168.1.0/24      ppp0
              True  Enable

FW1@root> _
```

6. 查看服务设置：

FW1 - HyperTerminal

```
FW1@root> show service
Telnet service:
  Allow Access: No
  Access:
Ssh service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
Web service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
Ping service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
FW1@root>
```

提示：访问服务允许的 IP 地址范围默认为 0.0.0.0-255.255.255.255，管理员应根据实际情况修改允许访问的 IP 地址范围。

1.6.7 导入 License

1. 在管理 PC 上搭建一个 TFTP 服务器，并将 License 文件放在下载路径。
2. 使用 **`license import`** 命令导入 License，根据提示输入 **`y`** 重启系统：

FW1 - HyperTerminal

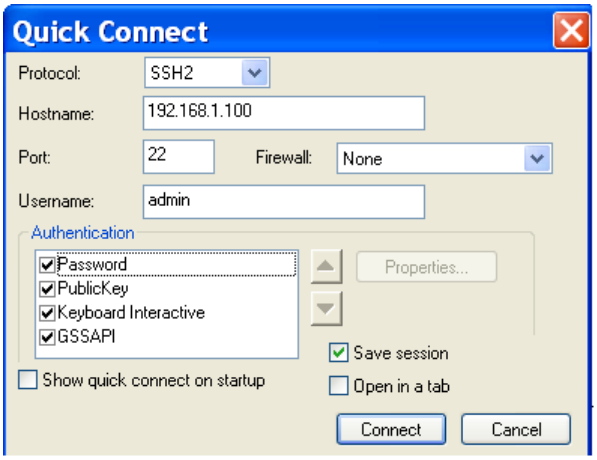
```
FW1@root-system] license import from tftp 192.168.1.200 FW1.dat

License upload succeeded. System needs to reboot.
Continue? (y/n)y
```

如果重启系统前不保存配置，所有配置将在重启系统后丢失。

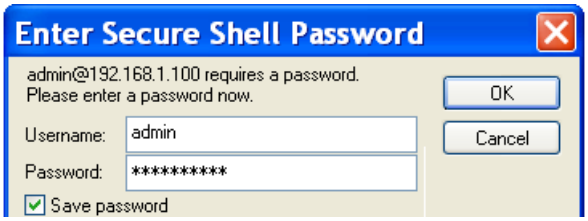
3. 重启后重新登录，并继续通过 CLI Console 配置 NISG-IPS。

1.6.8 使用 SSH 登录

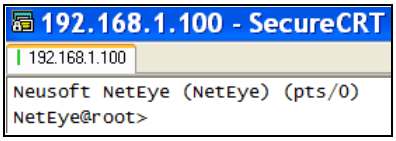
1. 打开 SecureCRT，点击 **Quick Connect**。在 **Hostname** 文本框中输入 NISG-IPS 的管理 IP 地址，在 **Username** 文本框中输入缺省用户名。点击 **Connect**。



2. 输入密码，点击 **OK**。



3. 登录后配置 NISG-IPS，配置方式同使用 CLI Console。



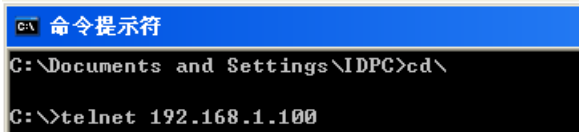
1.6.9 使用 Telnet 登录

Telnet 服务默认是关闭的。

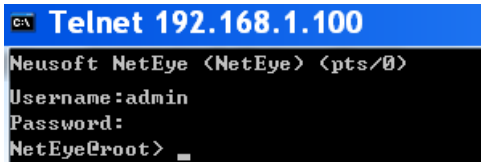
1. 使用 Telnet 连接之前，需要先通过 CLI Console 启用 Telnet 服务：

```
NetEye@root> configure mode override
NetEye@root-system] service telnet on
NetEye@root-system] service telnet allow zone any 0.0.0.0 255.255.255.255
```

2. 在管理PC上选择**开始**>**所有程序**>**附件**>**命令提示符**，打开命令提示窗口，通过Telnet命令远程登录 NISG-IPS：



3. 登录后配置 NISG-IPS，配置方式同使用 CLI Console。



1.7 验证初始化配置

初始化之后，执行以下步骤测试网络的连通性：

1. Ping 管理接口。如果 Ping 失败：
   a. 检查管理 IP。（缺省为 192.168.1.100/24。）
      - WebUI：选择**网络** > **接口**。
      - CLI：运行 **show interface brief** 命令。
   b. 检查相关服务是否开启。运行 **show service** 和 **show service port** 命令查看服务和端口配置。 Telnet 服务默认关闭，若使用 Telnet 登录，需要先开启 Telnet 服务。

```
FW1@root> show service
Telnet service:
  Allow Access: No
  Access:
Ssh service:
  Allow Access: Yes
  Access:
    allow any              0.0.0.0-255.255.255.255
Web service:
  Allow Access: Yes
  Access:
    allow any              0.0.0.0-255.255.255.255
Ping service:
  Allow Access: Yes
  Access:
    allow any              0.0.0.0-255.255.255.255

FW1@root> _
```

```
FW1@root> show service port

Telnet port: 23
   SSH port: 22
   Web port: 443

FW1@root> _
```

   c. 检查是否存在 IP 冲突。
      将 NISG-IPS 设备从网络中移除，从管理 PC 上 Ping NISG-IPS 的管理 IP 地址。如果收到应答，表明存在 IP 冲突。
   d. 使用 HTTPS 而非 HTTP 访问 NISG-IPS WebUI （输入 “https://” 和管理 IP 地址）。
   e. 换一个浏览器或 PC 访问 NISG-IPS。
   f. 检查管理 PC 和 NISG-IPS 设备之间的网线连接。
      应使用 RJ45 网线连接管理 PC 和 NISG-IPS 的接口。
      检查接口是否是 Up 状态。
   g. 检查路由设置。
      如果管理 PC 和 NISG-IPS 设备之间有路由设备，检查管理 PC、 NISG-IPS 和路由设备上是否正确配置了路由信息。
      在 NISG-IPS 上启用 Ping 服务，从管理 PC 上 Ping NISG-IPS 的管理 IP 地址。

```
FW1@root-system] service ping on
FW1@root-system] service ping allow zone any 0.0.0.0 255.255.255.255
```

      如果 Ping 失败，检查路由设置和网络拓扑。在 NISG-IPS 上执行 **show route** 命令查看路由信息。
2. Ping 外网口 WAN 接口。如果 Ping 失败：
   - 透明模式下，检查 NISG-IPS 的安全域和访问策略配置。
   - 路由模式下，检查 NISG-IPS 的安全域、访问策略、路由、NAT 规则配置，以及管理 PC 上的网关配置。
     访问策略按优先级从高到低进行匹配。一旦匹配到一条策略，其他策略不再进行匹配。

3. Ping NISG-IPS 的网关。如果 Ping 失败：
   - 检查 NISG-IPS 上的缺省路由。
   - 检查 NISG-IPS 和其网关之间的网线连接。
4. 访问 Internet。如果访问失败：
   - 检查以上步骤。如果能Ping通NISG-IPS的网关，Traceroute被访问网站来定位问题所在。
   - 如果出现在重启系统后，检查重启系统前是否忘记保存配置。

提示：详细信息请参见前一小节相关步骤。

1.8 常见问题

疑难 1

初始化之后访问不了 NISG-IPS。

解决办法

- 检查管理接口或 IP 是否在初始化过程中被修改。
- 检查 NISG-IPS 网关是否在初始化过程中被修改。

疑难 2

能登录，但访问的页面不正确。

解决办法

- 清空浏览器缓存再访问。
- 检查是否存在 IP 冲突。

疑难 3

登录后不能配置 NISG-IPS 功能。

解决办法

- 没有配置锁。点击 WebUI 右上角的 按钮获取配置锁，或在 CLI 下执行 **`configure mode override`** 命令获取配置锁。
- 未上载相关功能的 License。要上载 License，请参见 1.6.7 导入 License。

疑难 4

不能激活 License。

解决办法

- 检查 NISG-IPS 的 IP 是否同 License 服务器是否连通。
- 为 NISG-IPS 配置 DNS 服务器地址，用于解析 DNS 请求。
- 检查 NISG-IPS 和 Internet 之间的连通性。

疑难 5

不能通过 WebUI 登录 NISG-IPS。

解决办法

- 检查 Web 服务是否开启。
- 如果您连续 5 次输入密码错误，登录账号将被锁定 20 分钟。
- 在 CLI 下执行 **df** 命令，确保有足够的存储空间。

疑难 6

不能通过 PPPoE 接口访问 Internet。

解决办法

- 检查 NISG-IPS 上的 PPPoE 接口是否开启，所绑定的二层以太网接口是否连接正确。
- 检查 NISG-IPS 上为 PPPoE 接口配置的用户名和密码是否正确。
- 检查 PPPoE 接口和 Internet 之间的连通性。

1.9 后续配置步骤

下面是初始化之后的推荐配置步骤：

表 3 推荐配置步骤

WebUI 菜单路径	描述信息	用户指南章节
系统配置 （用户）		
系统 > 认证 > 管理用户	如使用 Vsys，创建 Vsys 管理员。	3.15 管理用户
系统 > 认证 > 用户	创建网络用户，允许其通过 NISG-IPS 访问网络资源。	3.16 网络用户
网络配置 （接口 & 安全域） & 路由配置 （仅针对路由模式）		
网络 > 接口	根据网络拓扑配置接口 IP 地址，并选择是否开启 IPv6。	从 4.1 接口到 4.1.4.8 配置隧道接口
网络 > 安全域	根据网络拓扑创建安全域，以便根据安全域创建策略控制访问流量和安全。	4.6 安全域
网络 > 路由 / 多播	添加静态、策略和多播路由，使 NISG-IPS 可以成功转发流经 NISG-IPS 的数据流。	第 5 章 , 路由
安全配置 （策略，攻击防御 &UTM）		
防火墙 > 访问策略 / 多播策略	创建相关策略允许指定流量经过 NISG-IPS 转发。	10.2.1 创建访问策略和 10.2.2 创建多播策略
防火墙 > 缺省策略设置	设置缺省域间和域内策略的动作。	10.2.5 配置缺省访问策略
防火墙 >IP-MAC 绑定策略 / 会话策略	配置 IP-MAC 绑定策略和会话策略，防止 IP 欺骗和会话泛滥攻击。	10.2.4 配置 IP-MAC 绑定和 10.2.3 创建会话策略
防火墙 > 攻击防御	配置攻击防御设置防御网络层攻击。	第 11 章 , 攻击防御
UTM	更新 UTM 规则，包括应用库、 URL 分类、防病毒规则、反垃圾邮件规则和攻击签名规则。 配置 UTM 策略和设置提供深层安全防护。	第 12 章 , 入侵防御系统
VPN，高可用性， Vsys		
VPN （IPSec VPN，SSL VPN 入口页面，SSL VPN 隧道）	配置 VPN，为两个站点之间或远程用户和站点之间的通讯提供安全通道。	第 13 章 , 虚拟专用网
系统 > 高可用性	配置高可用性，确保 NISG-IPS 的可用性。	第 14 章 , 高可用性
系统 > 虚拟系统	将根系统划分为多个虚拟系统，可以节省设备开销和降低根系统管理员的工作量。	第 15 章 , 虚拟系统

2 功能概述

本章简要介绍 NISG-IPS 功能特性，旨在方便您能够快速了解产品特性，更好地使用 NISG-IPS 产品。本文将从以下六个方面进行描述：

- 数据包处理流程
- 系统配置
- 网络配置
- 安全特性
- 监控及报表
- 虚拟系统和旁路 IPS 检测

数据包处理流程

2.1. 数据包处理流程	介绍 NISG-IPS 中数据包的处理流程，帮助管理员了解数据包通过各个模块的先后顺序。了解该顺序后，能够最大程度防止各个特性间的配置冲突。

系统配置

2.2. 系统配置	介绍设置系统基本信息的路径，并给出文档相关章节的链接。可设置的系统信息有：系统时间、本地访问控制、 License、用户和认证、证书、对象、系统升级、备份和恢复、系统诊断、技术支持、集中管理、日志、 SNMP 配置以及报警设置等。

网络配置

2.3. 网络配置	介绍配置网络的路径，并给出文档相关章节的链接。可配置的网络内容有：接口、ARP/CAM、 STP、安全域、 DNS、 DHCP、在线模式旁路模式切换以及 IPv6（DHCPv6 和邻居发现）等。
2.4. 路由及多播	介绍 NISG-IPS 静态路由中策略和路由条目的匹配原则，支持的动态路由协议种类及对多播的支持情况等内容。
2.5. ISP 智能选路	NISG-IPS 支持基于 IP 地址库、可用带宽的负载均衡和带宽利用率的负载均衡三种规则进行选取路由。
2.6. 高可用性	介绍 NISG-IPS 高可用性简单原理及在网络中支持的部署方式。
2.7. 地址转换（NAT）	介绍 NISG-IPS 支持的源地址转换、目的地址转换和地址映射功能。

安全特性

2.8. 服务质量（QoS）	介绍 NISG-IPS 的流量控制功能。能够分别控制整体带宽和单 IP 单用户的带宽使用。
2.9. 策略	通过策略控制流量转发，包括访问策略、缺省策略设置、多播策略、会话策略以及 IP-MAC 绑定。系统可自动探测 IP-MAC 绑定关系和自学习访问策略。
2.10. 攻击防御	介绍 NISG-IPS 可防御的攻击类型及系统的处理手段。可防御的攻击类型包括 ARP 攻击、 DoS 攻击、探测攻击、 TCP 逃避控制、 IP 选项校验和 ICMP 攻击等。
2.11. 入侵防御（IPS）	NISG-IPS 能够实现应用控制、 URL 过滤、入侵防御等功能，提供全面的安全防护。
2.12. 虚拟专用网（VPN）	介绍 NISG-IPS 支持的 VPN 种类及部署场景，包括 IPSec VPN、 SSL VPN (Web 入口页面 / 隧道）、 GRE 隧道。

监控及报表

2.13. 监控	监控系统运行信息、提供日志查询。
2.14. 报表	可通过设定报表计划生成有关以下信息的报表：系统、流量、 Web 安全、攻击、应用以及用户的统计信息。

虚拟系统和旁路 IPS 检测

2.15. 虚拟系统和虚拟网络	NISG-IPS 支持将其划分为多个虚拟系统。每个虚拟系统拥有独立的资源，可独立对外提供服务，大大降低了管理和硬件成本。 NISG-IPS 支持虚拟网络，虚拟系统之间可以通过虚拟网络通信。
2.16. 旁路 IPS 检测	介绍当旁路部署 NISG-IPS 设备时 NISG-IPS 可实现的功能和使用场景。

2.1. 数据包处理流程

数据包在 NISG-IPS 中的处理流程如下图 1 所示。图中标注的编号在下一页会有更加详细的解释。

图 1 数据包处理流程

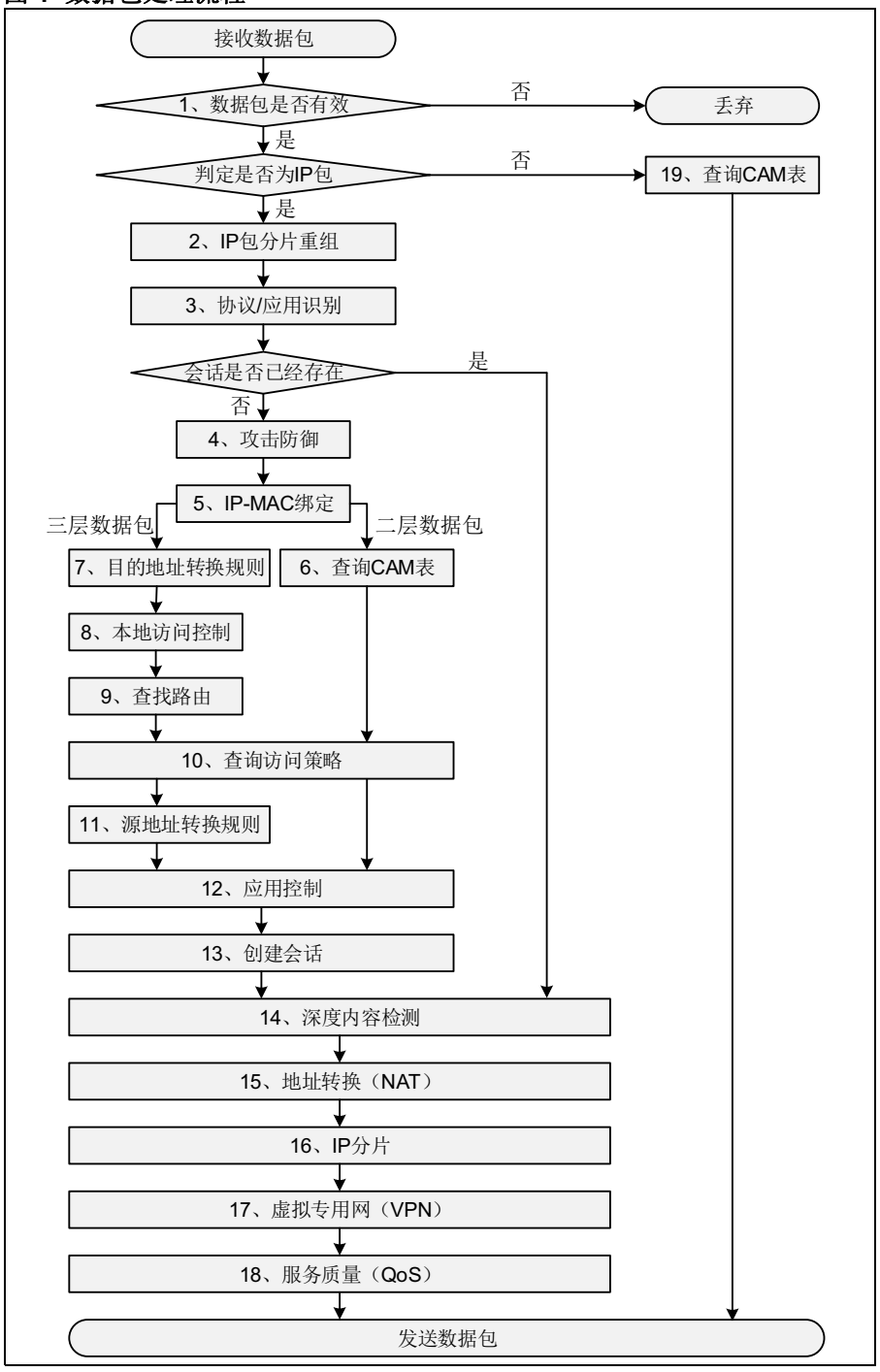


表 1 给出了上图中各个步骤的描述信息。No. 表示图中标识的编号，“ 参考章节 ” 指出了可以查找更详细信息的手册章节。

表 1 数据包处理流程

No.	NISG-IPS 处理数据包的功能	本章节	参考章节
1.	**数据包是否有效**。在数据包进入接口后， NISG-IPS 对数据包的合法性进行检查，即对数据包信息中的常规性错误进行检查，如：IP 地址全零、MAC 地址全零等。（无需配置）	---	---
2.	**IP 包分片重组**。接收完数据包所有分片后，NISG-IPS 会对数据包进行重组。	---	---
3.	**协议 / 应用识别 （DPI）**。 NISG-IPS 首先识别数据包使用的协议或应用，然后发送相关引擎进行检查。	---	---
4.	运行**攻击防御**。检查 DoS、 Reconnaissance、ICMP 等攻击，进行 IP 选项校验和 TCP 逃避控制。	2.10. 攻击防御	第 11 章，攻击防御
5.	匹配 **IP-MAC 地址绑定**策略，防止 IP 欺骗或地址伪装。	2.9. 策略	10.1.4 IP-MAC 绑定
6.	根据数据包的目的 IP 地址**查询 CAM 表**，然后进行一系列检测，最后将数据包通过对应的出口接口转发给目的 IP。	2.3. 网络配置	4.4 CAM
7.	查找目的地址转换 （**DNAT**）规则。	2.7. 地址转换 （NAT）	8.2.2 创建 DNAT 规则
8.	进行**本地访问控制** （如访问设置、网关设置等）。	2.2. 系统配置	3.12 访问设置
9.	**查询路由表**，查找到达目的地址的路由。	2.4. 路由及多播	5.2 基本配置步骤
10.	**查询访问策略**，进行 IP 包过滤检测。	2.9. 策略	10.2.1 创建访问策略
11.	查找源地址转换 （**SNAT**）规则。	2.7. 地址转换 （NAT）	8.2.1 创建 SNAT 规则
12.	对应用层数据包进行**应用控制**。	2.11. 入侵防御 （IPS）	12.2 基本配置步骤
13.	**创建会话**。保存会话信息到会话表，转发会话请求。	---	---
14.	进行**深度内容检测**，如 IPS 攻击签名检测 （IPS）等。	2.11. 入侵防御 （IPS）	12.2 基本配置步骤
15.	进行地址转换 （**NAT**）。	2.7. 地址转换 （NAT）	8.1 概述
16.	进行 **IP 分片**。	---	---
17.	**虚拟专用网 （VPN）**，封装数据包并引入 VPN 隧道。	2.12. 虚拟专用网 （VPN）	13.2 基本配置步骤
18.	**服务质量 （QoS）**，对数据流量进行带宽控制。	2.8. 服务质量 （QoS）	9.2 基本配置步骤
19.	根据数据包的目的 IP 地址**查询 CAM 表**，将数据包通过对应的出口接口转发给目的 IP。	2.3. 网络配置	4.4 CAM

2.2. 系统配置

表 2 提供系统配置相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 2 系统配置

	WebUI 菜单路径	描述信息	手册章节
系统基本信息			
1.	**主页**或 **系统 > 概述 > 系统信息**	查看系统概要信息参数。	3.3 WebUI 主页 3.4 系统概述
2.	**系统 >** **服务配置 > 标题信息**	设置系统标题信息。	3.13 标题信息
3.	**系统 >** **资产信息 >** **资产汇总 , 版权信息**	查看系统资产和版权信息。	3.5 资产汇总 3.6 版权信息
4.	**系统 >** **维护 > 日期时间**	设置系统日期、时间。	3.7 系统时间
License 和系统升级			
5.	**系统 >** **维护 > License**	License 概要信息，支持自动和手动激活。	3.8 License
6.	**系统 >** **系统升级 >** **安装升级包 , 管理安装升级包 ,** **管理增强升级包**	手动或自动加载升级包，包括安装包和增强升级包。	3.9 系统升级 3.10 安装升级包管理 3.11 增强升级包管理
访问设置			
7.	**系统 >** **服务配置 >** **访问设置 ,SNMP 配置**	设置对 Telnet、SSH、Web、Ping 和 root 用户的访问控制，配置 SNMP。	3.12 访问设置和 3.14 SNMP
授权和认证			
8.	**系统 >** **认证 >** **管理用户，网络用户**	管理用户的登录方式包括 Telnet、 SSH 和 Web。网络用户的类型包括 WebAuth、IPSec VPN 和 SSL VPN。	3.15 管理用户和 3.16 网络用户
9.	**系统 >** **认证 >** **认证配置，认证服务器，** **WebAuth 配置**	网络用户认证。	3.17 用户认证和 3.18 WebAuth 配置
10.	**系统 >** **认证 >** **管理用户**	启用 E-Key 认证后，用户在登录时，需要插入绑定的 USB Key 设备并输入 PIN 码才可以成功登录。	3.19 E-Key 认证
11.	**系统 >** **认证 >** **OTP 硬件令牌**	OTP 认证为对登录用户的增强认证，保证系统的安全性。	3.20 OTP 认证
系统维护			
12.	**系统 >** **维护 > 备份 / 恢复**	备份整机或根系统配置到备份文件，从备份文件恢复系统配置。	3.21 备份恢复
13.	**系统 >** **维护 > 技术支持**	生成系统诊断文件。	3.22 技术支持
14.	**系统 > 维护 > 诊断工具**	通过界面操作进行相关命令的输入，使命令使用简单化。	3.23 诊断工具

表 2 系统配置 (*续*)

	WebUI 菜单路径	描述信息	手册章节
15.	系统 > 维护 > 集中管理	配置是否允许被集中管理系统管理。	3.25 集中管理
16.	系统 > 日志配置 > 报警配置 , 日志维护	配置本地日志、 Syslog、 SNMP 和 Email 报警策略，下载日志文件和导出日志文件到 USB 设备。	3.26 报警配置和 3.27 日志维护
供系统全局使用的配置			
17.	系统 > 证书 > 本地证书 ,CA 证书	导入和管理 CA 和本地证书，用于用户认证和 VPN 隧道协商。	3.28 证书
18.	系统 > 证书 >CA 中心	创建本地证书中心，签发或撤回证书。	3.28 证书
19.	系统 > 对象 >IP 地址 , 服务	为策略和规则添加 IP 和服务对象。	3.29 对象

2.3. 网络配置

表 3 提供网络配置相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 3 网络配置

	WebUI 菜单路径	描述信息	手册章节
接口			
1.	网络 > 接口	用于接收和发送数据包。	4.1 接口
工作模式			
2.	网络 > 工作模式	能够调整系统的部署模式，选择在线模式或者旁路模式。	4.2 工作模式
STP			
3.	网络 > STP	生成树协议 （STP）在提供路径冗余的同时可以避免二层网络环路。	4.5 STP
ARP 和 CAM			
4.	-	通过命令行配置 ARP 和 CAM 表。	4.3 ARP 和 4.4 CAM
安全域			
5.	网络 > 安全域	安全域是接口的集合。将接口绑定在一起使得 NISG-IPS 可以对一个逻辑网络进行统一的安全控制。	4.6 安全域
DNS 和 DHCP			
6.	网络 > DNS > 主机 DNS 代理 静态缓存	配置 NISG-IPS 作为 DNS 主机或代理工作时使用的 DNS 服务器，为 NISG-IPS 配置 DNS 静态缓存。支持 DNSv6。	4.7 DNS 主机、 4.8 DNS 代理和 4.9 DNS 缓存

表 3 网络配置 (*续*)

	WebUI 菜单路径	描述信息	手册章节
7.	网络 > DNS > 入站智能 DNS	系统能够解析出访问者的 IP 地址的所属 ISP，进而帮助访问者访问到本运营商的服务器。入站智能 DNS 还可帮助运营商服务器进行负载均衡，使流量分布更合理。	4.10 入站智能 DNS
8.	网络 >DDNS	可以把动态变化的 IP 地址映射到一个固定的域名。访问域名时，即可访问到 NISG-IPS，不会感知到其 IP 地址的变化。	4.11 动态 DNS
9.	网络 > DHCP > DHCP 服务器 DHCP 作用域	设置 NISG-IPS 的 DHCP 工作模式，包括 DHCP 服务器、中继代理和客户端。工作模式为 DHCP 服务器时需要设置 DHCP 作用域。	4.12 DHCP 服务器和 4.13 DHCP 作用域
10.	网络 > IPv6 > DHCPv6	包括有状态 DHCPv6 （为主机分配 IPv6 前缀）和无状态 DHCPv6 （为主机分配域名和服务器地址）。	4.15 DHCPv6
邻居发现			
11.	网络 > IPv6 > 邻居发现配置	邻居发现 （ND）协议用于发现相同链路上的相邻节点（主机或路由器）。	4.16 邻居发现

2.4. 路由及多播

NISG-IPS 提供静态路由、动态路由和多播的特性。具体内容如下：

- 2.4.1. 静态路由，其中包括缺省路由和策略路由。
- 2.4.2. 动态路由，系统支持 OSPF、 RIP 和 BGP 三种动态路由协议。
- 2.4.3. 多播，系统支持二层和三层的多播。

2.4.1. 静态路由

静态路由包含策略路由和缺省路由。系统先进行策略路由匹配，再进行缺省路由匹配。

2.4.1.1. 匹配原则

策略匹配

当接收到新的数据包时，系统按如下顺序将其与路由进行匹配：

- 如果找到匹配的直连路由，系统直接转发数据包。
- 如果没有直连路由，系统会将数据包与所有在用的策略进行匹配，并按照策略的优先级由高到低进行匹配。匹配依据为以下参数：
  - 策略中定义的入口接口、 TOS、源 IP 地址和服务。
  - 策略路由表中的目的 IP 地址。

路由匹配

如果策略路由表或缺省路由表中包含多条可选路由，则按照以下规则进行匹配：

- 如果多条路由都包含数据包的目的 IP 地址，则选择掩码或者前缀长度较长的路由。
- 如果匹配的路由目的 IP 地址、掩码或前缀长度相同，则选择 Metric 值较小的路由。
- 如果 IP 地址、掩码或前缀及 Metric 值都相同，则选择最先添加的路由。

表 4 提供了静态路由相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 4 静态路由相关配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	网络 > 路由 > 策略路由	为系统配置路由策略及其中的路由表。	5.1.2 策略路由
2.	网络 > 路由 > 缺省路由	为系统配置缺省路由表。	5.1.1 缺省路由

2.4.2. 动态路由

NISG-IPS 支持动态路由。动态路由适用于具有一定规模的网络。

NISG-IPS 支持内部网关协议 OSPF 和 RIP，同时也支持外部网关协议 BGP。 NISG-IPS 只提供 CLI 方式配置动态路由。关于如何配置动态路由，参见*东软 NetEye 集成安全网关入侵防御系统 V4.2 命令参考手册*。

2.4.3. 多播

NISG-IPS 提供静态和动态多播路由功能。静态多播路由是由管理员手动设置的路由。动态多播路由是通过多播路由协议学到的路由。

在三层，动态多播路由支持 DVMRP 协议并兼容 PIM 协议的邻居发现。

在二层，系统通过 IGMP Snooping 防止广播风暴。

表 5 提供多播相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 5 多播相关配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	网络 > 多播 > DVMRP	配置 DVMRP 接口和参数，启用多播路由功能。	7.1.1 DVMRP
2.	网络 > 路由 > 多播路由	配置静态多播路由。	5.1.4 多播路由
3.	网络 > 多播 > IGMP Snooping	为系统配置 IGMP Snooping 功能。	7.1.2 IGMP Snooping

2.5. ISP 智能选路

在多条 ISP 线路环境中，当用户访问网络时， NISG-IPS 的 ISP 智能选路特性可以为用户选择最合适的 ISP 线路，充分利用出口链路资源，提高用户的访问速度。

开启该功能后，可配置 ISP 线路和选路规则等。

选路规则包含以下三种：

- 基于 IP 地址库选路。

  将数据包的目的 IP 地址与 IP 地址归属列表和地址库进行匹配，查询对应的运营商的首选线路进行转发。

- 基于可用带宽的负载均衡选路。

  在所有 ISP 线路中，选择可用带宽最大的 ISP 线路转发数据包。

- 基于带宽利用率的负载均衡选路。

  在所有 ISP 线路中，选择带宽利用率最小的 ISP 线路转发数据包。

表 6 提供 ISP 智能选路相关 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 6 ISP 智能选路相关配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**网络 >ISP 智能选路 > 策略**	为 ISP 智能选路配置策略。	6.2.1 设置 ISP 智能选路策略
2.	**网络 >ISP 智能选路 > IP 地址归属**	为指定 IP 地址配置所属的运营商。	6.2.2 设置 IP 地址归属
3.	**网络 >ISP 智能选路 > 地址库和更新**	配置地址库的更新策略。	6.2.3 设置地址库更新

2.6. 高可用性

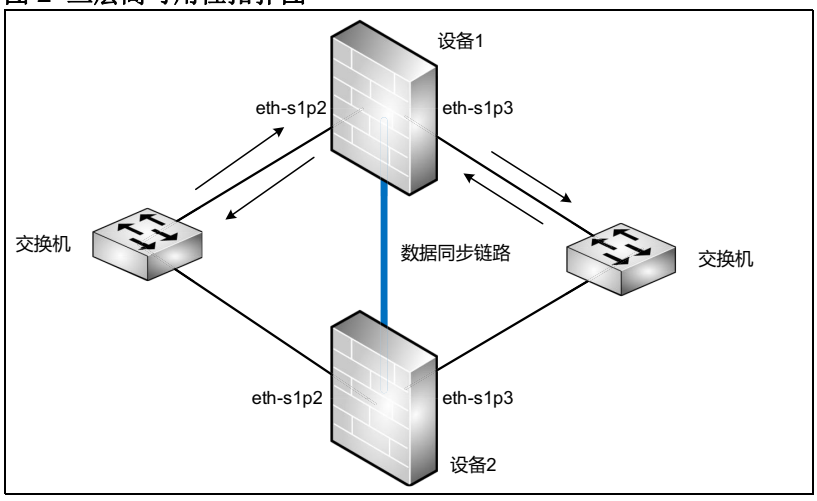
很多重要的网络终端不能长时间对外停止服务，一旦长时间停止，将造成重大损失。但单设备宕机导致网络中断不可避免，所以需要对安全设备进行高可用冗余部署。

NISG-IPS 支持三层和二层高可用性部署。

三层高可用性

NISG-IPS 通过虚拟路由器冗余协议 (Virtual Router Redundancy Protocol, VRRP) 实现三层高可用性。当需要进行三层高可用配置时，需要进行如图 2 拓扑部署。

图 2 三层高可用性拓扑图

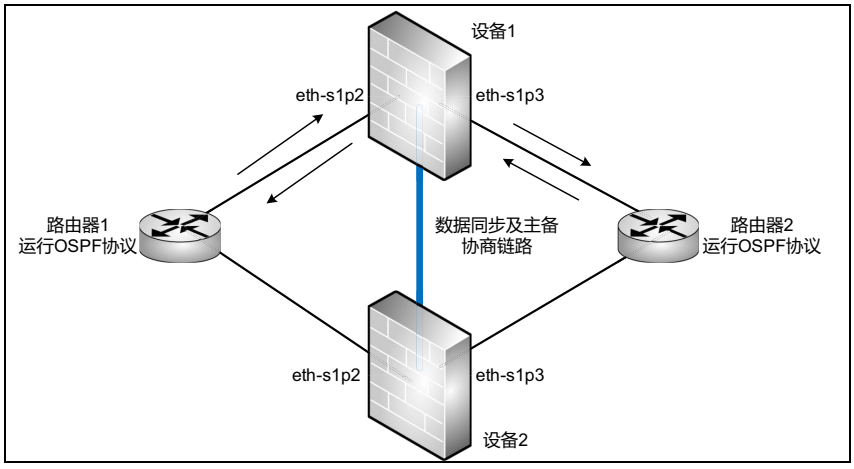


此种拓扑部署时，支持主主模式和主备模式运行。主主模式即两设备都处理业务流量，当一台宕机时，另一台接管全部流量。主备模式即只有主设备处理业务流量。备设备只进行配置同步和监听，一旦主设备出现故障则接替主设备处理业务流量。

二层高可用性

NISG-IPS 能够部署在两台路由器之间提供二层高可用性。在此种情况下，两端路由器需运行 OSPF 协议，需进行如下拓扑部署。

图 3 二层高可用性拓扑图



此种拓扑情况下， NISG-IPS 只支持主备模式部署，即只有主设备处理业务流量。备设备只进行配置同步和监听，一旦主设备出现故障则接替主设备处理业务流量。

表 7 提供高可用性相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

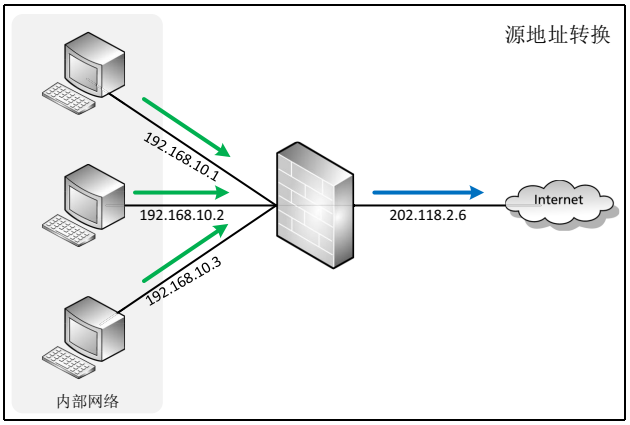
表 7 高可用性配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	系统 > 高可用性 > 虚拟路由器	使用 VRRP 协议达到备份和冗余的目的。一个虚拟路由器可以代表一组路由器作为缺省网关工作。如果一个路由器被选举为主设备，则其他路由器则作为备设备工作。	14.2.1 配置虚拟路由器
2.	系统 > 高可用性 > 虚拟路由器探测组	增强的 VRRP 功能。一个探测组将多个虚拟路由器绑定在一起，以达到整体切换的目的。	14.2.2 配置虚拟路由器探测组
3.	系统 > 高可用性 > 集群	一个集群由配置相同的设备组成。任何成员设备的配置修改都将被同步到组内其他成员设备上。	14.2.3 配置集群

2.7. 地址转换 （NAT）

随着网络迅猛发展， IPv4 地址资源越来越紧缺。地址转换功能能够帮助网络用户通过很少的公网 IP 地址接入到互联网中。与此同时，地址转换能够隐藏内部主机的 IP 地址及网络拓扑，一定程度上避免遭受外部攻击，保证内部网络安全。

NISG-IPS 提供三种 NAT 方式：

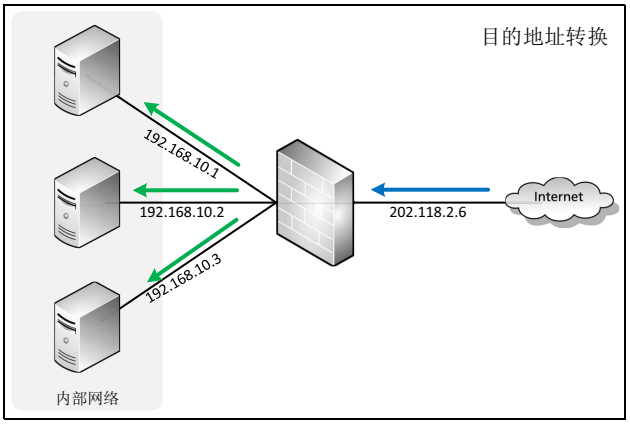


源地址转换可完成私有 IP 地址到公有 IP 地址的转换，使内网用户访问外网。

根据映射的 IP 地址数量，SNAT 可分为：

- 单 IP 地址转换为单 IP 地址。
- 多 IP 地址转换为单 IP 地址。
- 多 IP 地址转换为多 IP 地址。

当进行后两种转换时，需开启 NAPT 功能。



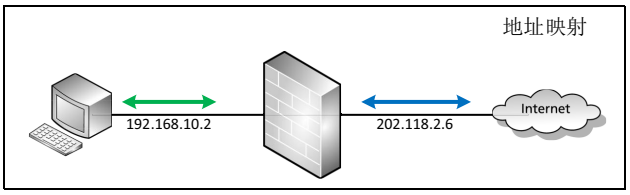
目的地址转换可完成公有 IP 地址到私有 IP 地址的转换，能够减小内网被外网攻击的可能性。

根据映射的 IP 地址数量，DNAT 可分为：

- 单 IP 地址转换为单 IP 地址。
- 单 IP 地址转换为多 IP 地址。

当进行单 IP 地址转换为多 IP 地址时，需开启 NAPT 功能，同时，可实现内部服务器的负载均衡。

NISG-IPS 支持对目的 IP 地址对应的域名的转换。



地址映射可完成内网 IP 地址和外网 IP 地址一对一的映射。

进行地址转换匹配时，地址映射优先于源地址转换和目的地址转换。

表 8 提供地址转换相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

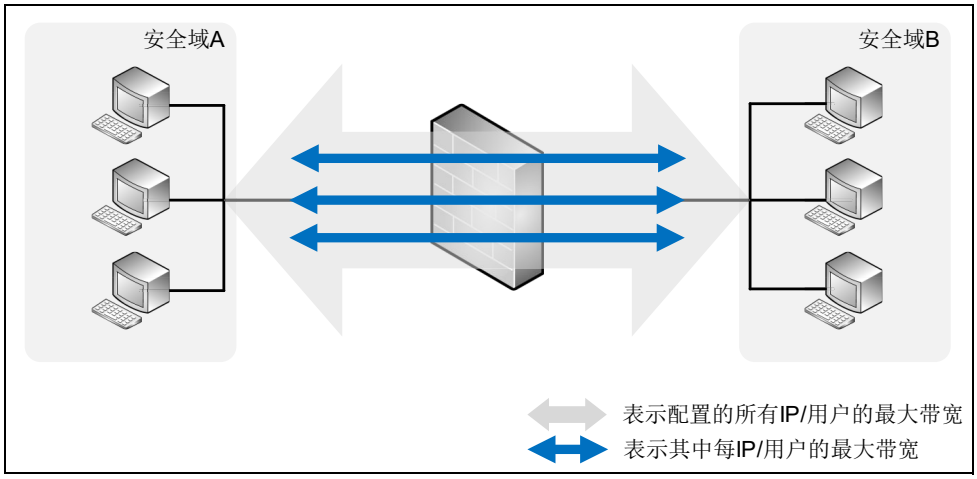
表 8 地址转换配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	网络 > 地址转换 > 源地址转换	源地址转换 （SNAT）。	8.2.1 创建 SNAT 规则
2.	网络 > 地址转换 > 目的地址转换	目的地址转换 （DNAT）。	8.2.2 创建 DNAT 规则
3.	网络 > 地址转换 > 地址映射	地址映射 （MIP）。	8.2.3 创建 MIP 规则

2.8. 服务质量 （QoS）

网络流量迅猛增长的今天，网络延迟和阻塞越来越多。在这种情况下，网络流量的精细化管理显得越来越重要。服务质量 （QoS）功能能够帮助管理员更好地管理网络流量，最大程度地避免网络延迟和拥塞的出现，保证重要流量通行和网络高效运行。

NISG-IPS 支持对整个网络中的流量根据应用协议等进行限速，同时也支持对单 IP 地址、单用户的流量管控。



NISG-IPS 还支持正向和反向使用不同的防护配置策略。例如，上图中可配置从安全域 A 到安全域 B 针对视频应用限速 100M，但从安全域 B 到安全域 A 可对视频应用限速 50M。

表 9 提供 QoS 相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 9 QoS 配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	IPS > QoS > QoS 防护配置	创建全局 QoS 防护配置，用于决定流量的最大带宽和 DSCP 值。	9.2.1 创建普通 QoS 防护配置
2.	IPS > QoS > 每 IP/ 用户 QoS 防护配置	创建每 IP/ 用户 QoS 防护配置，用于决定每 IP、用户流量的最大带宽。	9.2.2. 创建每 IP/ 用户 QoS 防护配置
3.	IPS > QoS > QoS 策略	创建 QoS 策略，用于决定哪些流量要进行带宽控制。	9.2.3 创建 QoS 策略

2.9. 策略

各安全域间的访问可以通过策略来控制，合适的策略能够更好的隔离域间和域内的恶意流量。

NISG-IPS 设备支持多种策略的配置，包括访问策略、多播策略、会话策略、 IP-MAC 绑定和缺省策略。

访问策略

访问策略主要用于允许或拒绝与指定条件相匹配的数据包。访问策略也可用于启用 DNS 透明代理和将满足条件的数据包引入 VPN 隧道。关于 DNS 透明代理的内容，请参见 4.8 DNS 代理。关于策略在 VPN 中的应用，请参见第 13 章，虚拟专用网。

NISG-IPS 提供策略自学习功能。通过在有限时间内的学习，系统可生成策略。管理员可以直接使用生成策略，也可根据情况编辑生成策略。

多播策略

多播策略可允许指定源安全域、源 IP 地址的流量通过指定的多播 IP 地址转发到特定的安全域。

会话策略

会话策略能够限制会话的数量，防止会话泛滥攻击的发生。 NISG-IPS 提供三种会话控制策略：

- 基于策略的会话限制：用于限制符合指定源和目的 IP 地址条件的并发会话数。
- 基于源 IP 的会话限制：用于限制符合每个源 IP 地址的并发会话数。
- 基于目的 IP 的会话限制：用于限制符合每个目的 IP 地址的并发会话数。

IP-MAC 绑定

IP-MAC 绑定功能用于检查数据包中主机 IP 地址与网卡 MAC 地址的映射关系是否为已配置的绑定关系，以此防止非法主机冒用合法主机的 IP 地址造成网络安全隐患。

IP-MAC 绑定支持自动探测功能。 NISG-IPS 可探测与其三层接口同网段的 IP 地址段中的 IP 地址与 MAC 地址的对应关系。管理员可以根据需要将生成的映射关系添加到绑定策略之中。

配置完 IP-MAC 绑定策略之后， NISG-IPS 只允许 IP 和 MAC 地址同时匹配管理员配置的绑定关系的数据包通过。如果只有 IP 地址或 MAC 地址不能完全匹配，则该数据包会根据配置被允许通过或被拒绝。

IP-MAC 绑定功能可关联 DHCP IP 地址绑定状态列表。关联后，系统除查询绑定策略外，还将查询 DHCP IP 地址绑定状态列表。

缺省策略

当数据包未匹配到管理员添加的策略时，系统会按照缺省策略中的配置处理数据包。可配置的缺省策略包括域间缺省策略、域内缺省策略和会话缺省超时时间。

在没有安全域的情况下，系统会按照域间缺省策略处理流量。

表 10 提供防火墙策略相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 10 策略配置步骤

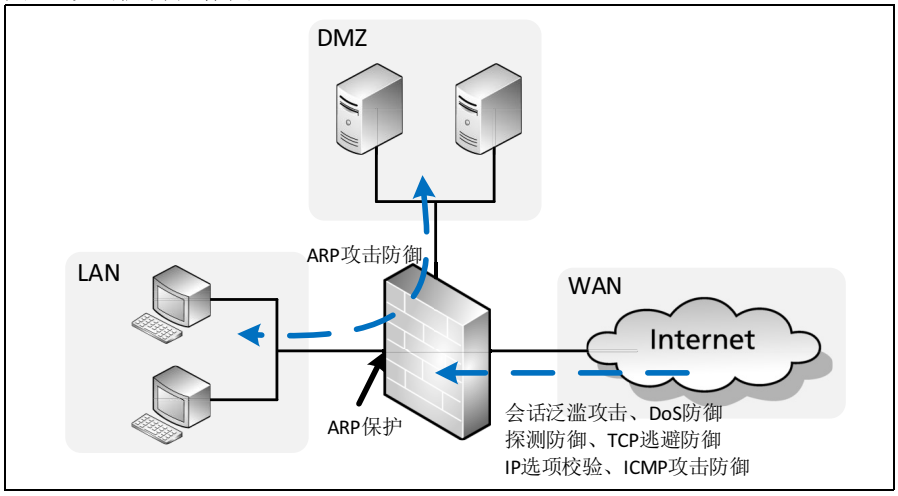
	WebUI 菜单路径	描述信息	手册章节
1.	**防火墙 > 访问策略**	安全域到安全域。	10.2.1 创建访问策略
2.	**防火墙 > 多播策略**	允许转发多播数据包的安全域。	10.2.2 创建多播策略
3.	**防火墙 > 会话策略**	安全域到安全域的会话限制。	10.2.3 创建会话策略
4.	**防火墙 > IP-MAC 绑定**	配置 IP-MAC 绑定关系。	10.2.4 配置 IP-MAC 绑定
5.	**防火墙 > 缺省策略设置**	所有安全域。	10.2.5 配置缺省访问策略

2.10. 攻击防御

网络攻击能够获取网络及其主机信息或降低网络处理流量的性能。NISG-IPS 的攻击防御功能能够帮助您防御绝大多数的恶意网络攻击。

攻击防御功能多用于图 4 中场景。

图 4 攻击防御拓扑图



NISG-IPS 支持防御以下攻击，具体攻击形式及 NISG-IPS 的应对措施，请参见第 11 章，攻击防御中的 11.3 配置参数说明。

局域网保护	接口级	• ARP 过滤 （防主机欺骗） • ARP 网关保护 （防仿冒网关攻击）
	安全域级	ARP 攻击防御
防御来自外网的网络攻击	策略级	会话泛滥攻击防御 关于会话泛滥攻击的防御措施，请参见 10.1.3 会话策略。
	安全域级	• DoS 防御 • 探测防御 • TCP 逃避控制 • IP 选项校验 • ICMP 攻击防御

对于以上攻击， NISG-IPS 可对判断为攻击的流量进行**丢弃**和**报警**处理，管理员可根据需要进行配置。

表 11 提供攻击防御相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 11 攻击防御配置步骤

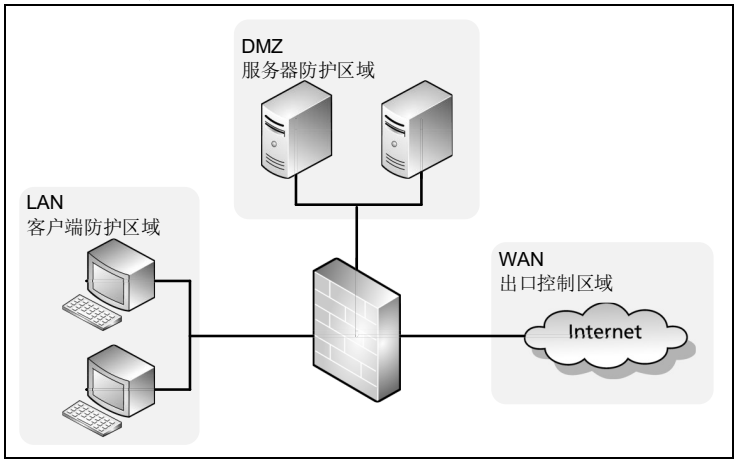
	WebUI 菜单路径	描述信息	手册章节
1.	防火墙 > 攻击防御 > ARP 保护 ARP 攻击防御	配置局域网内部 ARP 相关的防护功能。	11.2.1 配置 ARP 攻击防御和保护
2.	防火墙 > 攻击防御 > DoS 防御 探测防御 TCP 逃避控制 IP 选项校验 ICMP 攻击防御	对于网络攻击的安全域级别的检测和防御机制。	11.2.2 配置其他类型攻击防御

2.11. 入侵防御 （IPS）

随着网络的发展，越来越多的攻击行为和恶意信息隐藏在应用层数据中。 NISG-IPS 的 IPS 功能针对应用层数据进行解析，并对其内容进行安全性检测和控制。

IPS 功能多用于图 5 中场景。

图 5 IPS 拓扑图



出口控制

IPS 提供出口控制功能，该功能能够在出口安全域处对用户流量进行安全检测和控制。出口控制包含以下功能：

- 应用控制：能够控制用户访问的应用。
- URL 过滤：能够限制用户访问的 URL。
- DNS 域名黑名单：对用户的 DNS 请求进行限制，阻断匹配黑名单的域名解析请求。
- 页面过滤：可对页面中的敏感词设置分值，并对敏感词分值达到一定阈值的页面进行阻断、生成日志等操作。

表 12 提供出口控制相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 12 应用控制配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**IPS > 出口控制 > 应用控制 > 应用知识库，自定义应用**	自定义应用匹配条件。	12.2.1.2.2 添加自定义应用（2b）
2.	**IPS > 出口控制 > 应用控制 > 防护配置**	根据需要创建防护配置。每个防护配置指定了要控制的应用、针对每种应用的动作以及未指定应用的缺省动作。	12.2.1.2.3 创建应用控制防护配置（2c）
3.	**IPS > 出口控制 > 策略 > 应用控制**	针对每个出口安全域： ■ 根据需要创建应用控制策略。 ■ 开启应用控制功能。	12.2.1.2.4 创建应用控制策略（2d）
4.	**IPS > 出口控制 > URL 过滤 > 常规设置**	设置 URL 过滤引擎失效时 NISG-IPS 的处理动作。	12.2.1.3.2 配置 URL 过滤常规设置（3b）
5.	**IPS > 出口控制 > URL 过滤 > 黑白名单**	配置 URL 黑白名单。	12.2.1.3.3 创建 URL 过滤防护配置：黑白名单（3c）
6.	**IPS > 出口控制 > URL 过滤 > 防护配置**	URL 过滤防护配置指定了黑白名单、要过滤的 URL 分类、针对分类执行的动作，以及对未知分类的缺省处理动作。	12.2.1.3.4 创建 URL 过滤防护配置（3d）
7.	**IPS > 出口控制 > 策略 > URL 过滤**	针对每个出口安全域： • 创建 URL 过滤策略。 • 开启 URL 过滤功能。	12.2.1.3.5 创建 URL 过滤策略（3e）
8.	**IPS > 出口控制 > DNS 域名黑名单** **IPS > 出口控制 > 策略 > DNS 域名黑名单**	配置全局 DNS 域名黑名单功能。需要为每个出口安全域单独开启该功能。	12.2.1.5 配置 DNS 域名黑名单
9.	**IPS > 出口控制 > 页面过滤** **IPS > 出口控制 > 策略 > 页面过滤**	配置全局页面过滤功能。需要为每个出口安全域单独开启该功能。	12.2.1.4 配置页面过滤

客户端及服务器防护

IPS 可以根据内网主机类型不同进行不同防护，可进行客户端防护和服务器防护。

防护特性包括：

- 入侵防御系统 （IPS）：NISG-IPS 能够深度检测报文，检测七层威胁，并阻止其中的威胁或攻击。
- SSL 检测：NISG-IPS 提供对 SSL VPN 中的数据包进行解密、检测再加密发送的功能。
- 协议异常检测：NISG-IPS 能够检测流量协议的异常，并根据配置阻断异常流量。

表 13 提供客户端防护相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 13 客户端防护配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**IPS > IPS > 协议限制**	设置全局 SMTP/POP3/IMAP/DNS 协议限制。	12.2.2.3 配置 IPS SMTP/POP3/IMAP/DNS 协议限制 （客户端）
2.	**IPS > IPS > 防护配置**	配置全局 IPS 防护配置。	12.2.2.5 创建 IPS 防护配置
3.	**IPS > 客户端防护 > DNS 缓存中毒防御**	配置全局 DNS 缓存中毒防御功能，为指定安全域启用该功能。	12.2.2.4 配置 DNS 缓存中毒防御
4.	**IPS > 客户端防护 > 策略**	为指定安全域配置客户端保护策略，指定： • 受保护的客户端 • IPS 防护配置 • 其他检测动作	12.2.2.6 创建客户端防护策略
5.	**IPS > 客户端防护 > 策略 信任服务器列表，信任邮件地址列表**	为指定安全域创建信任服务器和邮件地址列表。	12.2.2.7 创建信任服务器 / 邮件列表
6.	**IPS > 服务器防护 > Web 防护 , 邮件防护**	为所有安全域配置 Web 和邮件防护。	12.2.3.4 配置 Web/ 邮件防护
7.	**IPS > 服务器防护 > 策略**	为指定安全域配置服务器防护策略，指定： • 受保护服务器 • IPS 防护配置 • 其他检测动作	12.2.3.6 创建服务器防护策略
8.	**IPS > 服务器防护 > 策略 信任客户端列表 信任邮件地址列表**	为指定安全域创建信任客户端和邮件地址列表。	12.2.3.7 创建信任客户端 / 邮件列表

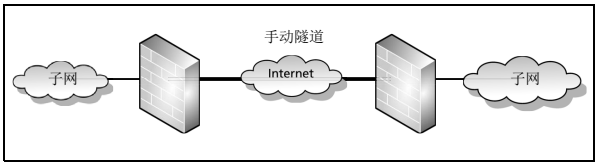
2.12. 虚拟专用网 （VPN）

虚拟专用网功能利用公共网络建立虚拟专用网络，能够帮助远程用户、公司分支机构、商业伙伴等同公司内部网络建立可信的安全连接，并保证数据的安全传输。

NISG-IPS 支持以下 VPN 类型：

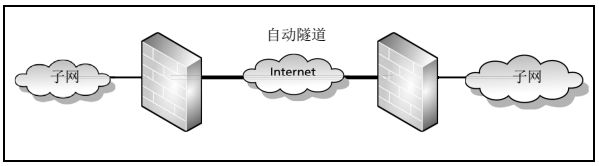
- IPSec VPN
- GRE VPN
- SSL VPN

IPSec VPN



网段到网段手动密钥隧道

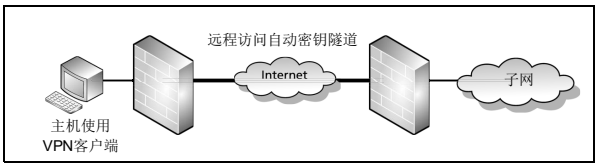
通过手动生成密钥建立隧道，仅支持网段到网段的 IPSec VPN。一般用于小型或静态网络。



网段到网段自动密钥隧道

指两个网关设备之间通过自动生成密钥方式建立 IPSec VPN 隧道。

NISG-IPS 支持多 SA 功能，即一个网关设备可保护多个子网，可以对每条隧道从本端特定子网到对端特定子网之间的数据流进行精准的安全控制。



远程访问自动密钥隧道

指远程用户 / 用户组与 VPN 网关之间建立 IPSec VPN 隧道，用户 / 用户组可以通过该隧道安全地访问受网关保护的内部子网。

NISG-IPS 支持 IPSec VPN 的 NAT 穿越和隧道组功能。

当 IPSec VPN 中间网络出现 NAT 设备时，会导致两端协商失败。这时需要 NAT 穿越功能来确保 IPSec VPN 隧道搭建成功。详细信息，请参见 13.1.1 NAT 穿越。

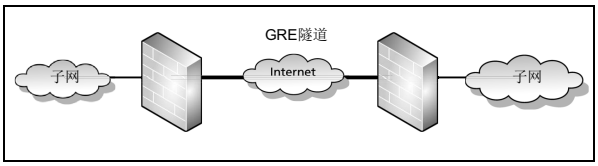
隧道组是一组自动密钥隧道的集合，可以起到冗余备份的作用。一个隧道组中只有一个成员隧道处于工作状态，其余隧道处于备份状态。当处于工作状态的隧道发生故障时，将从其余可用的隧道中协商选出一个优先级最高的隧道，来继续工作。

表 14 提供 IPSec VPN 相关的 WebUI 菜单路径、简短描述以及到相关手册章节链接。

表 14 IPSec VPN 配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**系统 >** **证书 >** **本地证书，CA 证书**	导入证书。	导入证书
2.	**系统 >** **认证 >** **网络用户 （Auto IKE)**	创建 IPSec VPN 用户或用户组 （远程拨号自动密钥隧道）	创建 IPSec VPN 用户
3.	**VPN >** **IPSec VPN >** **自动 / 手动密钥隧道**	创建自动或手动隧道。	创建手动密钥隧道 创建自动密钥隧道
4.	**网络 >** **路由 >** **缺省路由，策略路由** **防火墙 >** **访问策略**	创建路由或访问策略并指定引用隧道。	配置路由 / 配置访问策略
5.		配置对端 （仅针对拨号访问）。	配置远程 VPN 客户端

GRE VPN



GRE 隧道

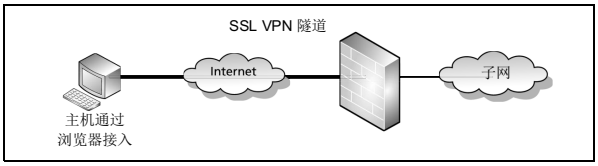
通过将一种协议的报文封装在另一种协议报文中，使被封装的报文能够在网络中传输。其实现机制简单，通常用于对安全性要求不高的场景。

表 15 提供 GRE 隧道相关的 WebUI 菜单路径、简短描述以及到相关手册章节链接。

表 15 GRE 隧道配置步骤

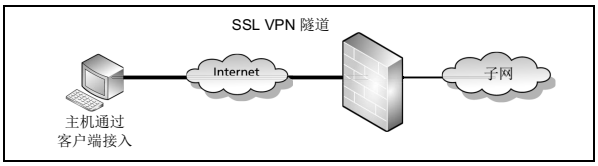
	WebUI 菜单路径	描述信息	手册章节
1.	**VPN >** **GRE 隧道**	配置接口 IP 地址和缺省路由。	创建 GRE 隧道
2.	**防火墙 >** **访问策略**	创建访问策略并指定引用隧道。	配置访问策略
3.	**网络 >** **路由 >** **缺省路由，策略路由**	创建路由或并指定引用隧道。	同表 14 中的 配置路由。

SSL VPN



SSL VPN Web 入口访问

远程用户可以通过浏览器登录到入口网页，方便快捷地访问受保护的内网资源。这种连接方式只能访问 HTTP/HTTPS 的 Web 服务，所以也称为 Web-Only 型 SSL VPN。



SSL VPN 隧道

指 SSL VPN 客户端与 NISG-IPS 之间利用 SSL 建立隧道，客户端通过这条隧道与受保护的子网或网站进行安全通信。这种通信方式称为隧道型 SSL VPN。

表 16 提供 SSL VPN 相关的 WebUI 菜单路径、简短描述以及到相关手册章节链接。

表 16 SSL VPN 配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**VPN>** **IP 地址池** **系统 >** **认证 > 网络用户** **VPN >** **SSL VPN > 用户组**	创建 IP 地址池、 SSL VPN 用户和用户组。	创建 IP 地址池 创建 SSL VPN 用户 创建 SSL VPN 用户组
2.	**系统 >** **证书 >** **本地 / CA 证书**	导入 CA/ 本地证书。	导入 CA/ 本地证书
3.	**VPN >** **SSL VPN Web 入口页面 >** **应用 / 页面模板**	应用包括 HTTP 和 HTTPs。 入口页面模板包括内容、布局和风格。	创建 SSL VPN 应用 创建 SSL VPN 页面模板
4.	**VPN >SSL VPN** **SSL VPN 隧道 > 隧道**	在服务器和客户端之间创建 SSL VPN 隧道。	创建 SSL VPN 隧道
5.	**VPN >** **SSL VPN Web 入口页面 >** **页面服务**	启用 HTTPS 服务，在指定 IP 地址和端口为用户组提供服务。	创建 SSL VPN 页面服务
6.		安装 SSL VPN 客户端软件。	添加 SSL VPN 连接

2.13. 监控

通过 NISG-IPS 的监控功能，能够实时查看运行数据信息。

表 17 提供监控和日志相关的 WebUI 菜单路径。

表 17 监控 / 日志查看路径

	WebUI 菜单路径	描述信息	手册章节
1.	**监控 > 拓扑 / 流量统计数据 / 虚拟系统 /STP/ 路由 / 地址转换 /ARP/ CAM/DHCP IP 地址绑定状态 /DHCPv6 客户端 /DNS 缓存 / 高可用性 / 系统利用率 / 在线用户 /IPSec VPN 隧道 /GRE 隧道 / 多播 / 报警 / 日志**	所有功能的实时监控信息。	第 16 章 , 监控

2.14. 报表

NISG-IPS 能够记录的实时数据，并以图表 （线图、条形图、圆饼图和表格）的形式展现给用户。

报表可记录以下类别相关的数据：系统、流量、 Web 安全、攻击、应用和用户。管理员可以制定具体的报表生成计划，使 NetEye 按照计划在规定的时间自动地生成报表，并可以通过 SMTP 服务器将生成的报表以邮件方式发送给特定用户。

表 18 提供报表相关的 WebUI 菜单路径、简短描述以及到相关手册章节链接。

表 18 报表配置路径

	WebUI 菜单路径	描述信息	手册章节
1.	**监控 > 报表 > 常规设置**	所有报表的全局设置。	17.2.1 配置常规设置
2.	**监控 > 报表 > 计划**	创建报表模板。	17.2.2 创建报表生成计划
3.	**监控 > 报表 > 结果**	查看生成的报表。	17.2.3 管理报表结果

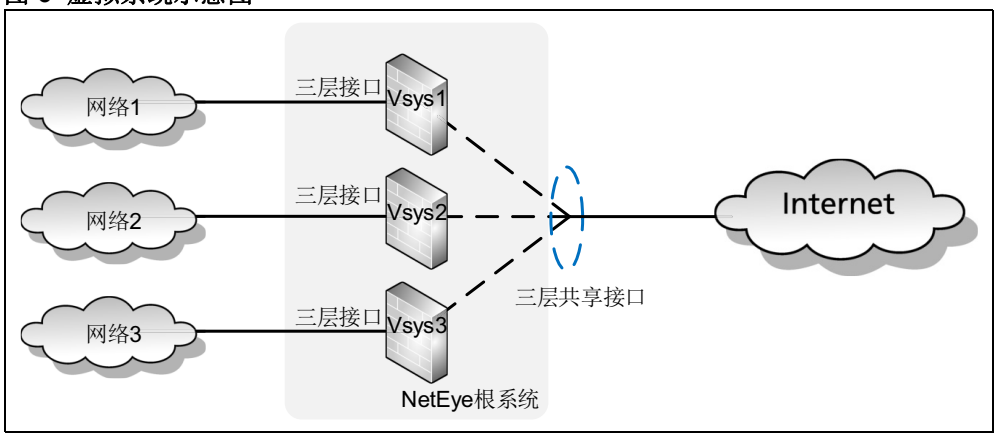
2.15. 虚拟系统和虚拟网络

缺省状态下， NISG-IPS 是一个单独的系统，虚拟系统功能可以帮助管理员将 NISG-IPS 逻辑上划分为多个独立的虚拟系统。每个虚拟系统可有独立的管理员、审计员、策略、用户认证数据库等，可独立对外提供服务。当管理员需要对网络内部的某一部分网络单独管理，可使用此功能。

系统提供三层共享接口，此接口可用于多个虚拟系统通过一个接口与 NISG-IPS 设备外部连接，提升接口使用效率，减少接口使用数量。

虚拟系统基本使用场景如图 6 所示。

图 6 虚拟系统示意图



除了虚拟系统之外，还支持虚拟网络，虚拟网络用于虚拟系统间的互相通信。其工作原理如下。

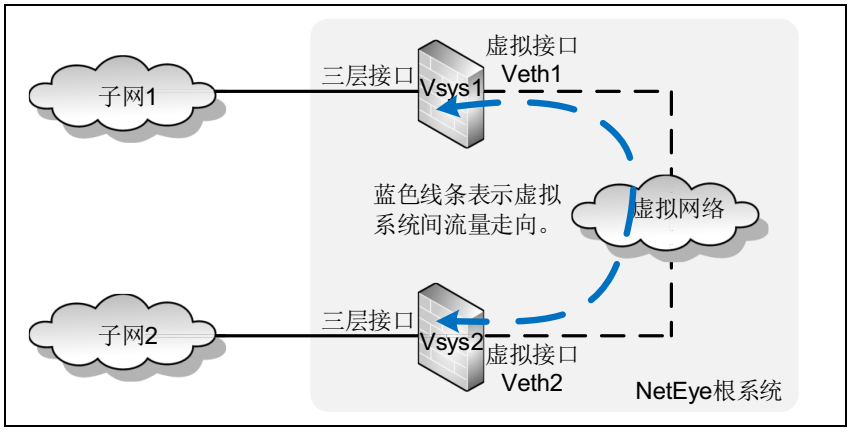


表 19 提供虚拟系统相关的 WebUI 菜单路径、简短描述以及到相关手册章节链接。

表 19 虚拟系统配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**网络 > 接口**	创建三层接口，如 VLAN 和 Channel 接口，用于划分到 Vsys 中。	15.3.1 创建三层接口
2.	**系统 > 虚拟系统 > 虚拟系统**	创建虚拟系统，指定最大资源限制、包含的三层接口、管理接口 /IP、 IPS 功能。	15.3.2 创建虚拟系统 （资源限制 / 接口 / 管理 IP/IPS）
3.	**系统 > 认证 > 管理用户**	创建 Vsys 管理员。	15.3.3 创建虚拟系统管理员
4.	在浏览器中输入 https://+vsys_management_IP 登录虚拟系统。	登录并管理 Vsys。每个 Vsys 都有自己的管理员和策略等配置。	15.3.4 登录 / 切换虚拟系统和 15.3.5 管理虚拟系统
5.	**系统 > 虚拟系统 > 虚拟网络**	创建虚拟网络连接虚拟系统。需要将虚拟接口提前划分指定的虚拟系统。	15.3.6 创建虚拟网络

2.16. 旁路 IPS 检测

当管理员仅想监听并检测网络流量时，可以选择旁路部署 NISG-IPS 设备。在旁路部署时，设备可以通过监听接口获取网络流量镜像，并对镜像流量进行 IPS 检测。

管理员可以检测多个网络， NISG-IPS 最多支持检测 64 个网络。

提示：如果需使用旁路 IPS 检测功能，需旁路部署 NISG-IPS 设备，并且选择**网络 > 工作模式**切换为旁路模式。

详细信息，请参见第 18 章 , 旁路 IPS。

3 系统配置

本章介绍 NISG-IPS 提供的如下管理功能：

3.1 管理方式

管理员可以将管理主机连接到 NISG-IPS 的 Console 口、带外管理口 （MGT）、以太网专用管理接口或任意一个三层以太网接口，通过 Console、Web、SSH 或 Telnet 方式登录 NISG-IPS，对设备进行管理。

NISG-IPS 支持 WebUI 和 CLI 两种配置方式：

- WebUI 提供图形化操作界面，管理员可以通过在浏览器中输入 NISG-IPS 的管理 IP 地址进入 WebUI 操作界面。
- CLI 提供命令行操作界面，管理员可以通过 Console、SSH、Telnet 和 WebShell 方式进入 CLI 操作界面。

管理员可以通过 WebUI 方式完成首次登录，并使用初始化向导对 NISG-IPS 进行初始配置。关于初始配置的具体步骤，请参见第 1 章，快速向导。

3.2 页面布局

通过 WebUI 登录后，可看到如下管理界面：

页面上方是产品 Logo、主机名、管理用户名、功能菜单和快捷菜单，左侧是导航菜单，右侧是查看和配置区域。

NISG-IPS 提供如下快捷菜单：

WebShell 快捷菜单，可以随时调出 CLI 操作界面。
如果连接超时，可以通过点击窗口上显示的 **Connect** 按钮重新连接。

可以随时调出初始化向导界面。

点击保存所做修改。拥有配置锁的管理用户才具有保存配置的权限。
配置锁被抢时显示为配置锁图标 ，点击该图标可抢回配置锁。

点击查看当前界面的帮助信息。

点击退出系统。

3.3 WebUI 主页

WebUI 主页缺省显示 NISG-IPS 系统基本信息、资源使用情况、接口状态等信息，上载 License 后显示更多详细信息。

点击**主页**选项卡查看系统详细信息。

- 管理员可以根据需要点击左边目录树节点查看具体页面。
- 可以点击 手动刷新页面，点击 关闭当前信息窗口，或点击 编辑刷新频率、刷新方式、显示的信息条数、显示格式等。
- 当鼠标指针变为 时，可以将该栏目拖到任意位置，改变页面布局。
- 可以点击**更多**进入相应配置页面进行更多配置。

表 20 主页信息

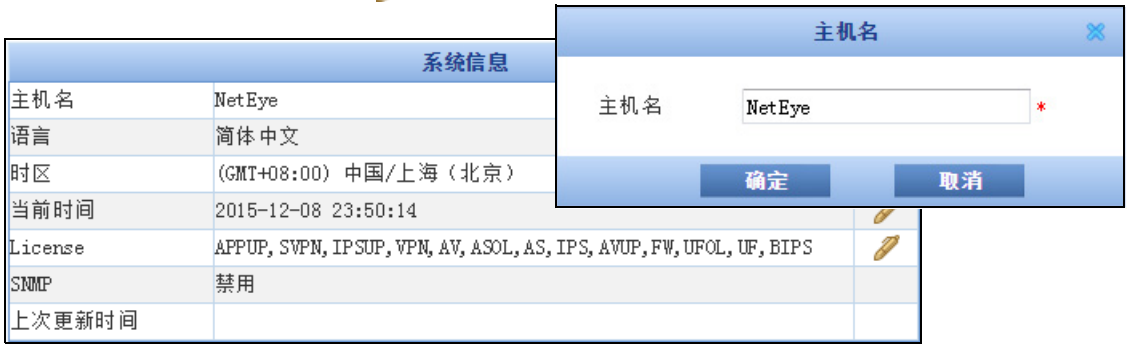
参数	说明
系统信息	显示系统信息，包括型号、软件名称、软件版本、释放时间、序列号、内存和系统运行时间。
资源使用情况	显示系统资源使用情况，包括 CPU、内存、日志存储空间、会话、策略、 VPN 和 NAT 资源。
接口状态	显示接口状态。已启用处于连通状态的接口显示为绿色，被禁用的接口显示为灰色。鼠标指向接口时会弹出该接口的详细信息。
系统日志	显示生成的不同安全级别的日志信息。 Emergency 和 Alert 以红色标示， Critical 和 Error 黄色标示， Warning 和 Notice 绿色标示， Informational 和 Debugging 蓝色标示。
URL 排名	显示 URL 排名相关信息。
用户排名	显示用户排名相关信息。
IP 地址排名	显示 IP 地址排名相关信息。
应用排名	显示应用排名相关信息。
WebAuth 用户	显示在线 WebAuth 用户相关信息，包括用户、 IP 地址、在线时间、实时流量、总流量及空闲时间。
SSL VPN 用户	显示在线 SSL VPN 用户相关信息，包括用户、登录类型、 IP 地址、在线时间、接收和发送字节数及空闲时间。

3.4 系统概述

系统概述页面显示系统信息、访问设置及系统重启关闭等相关内容。

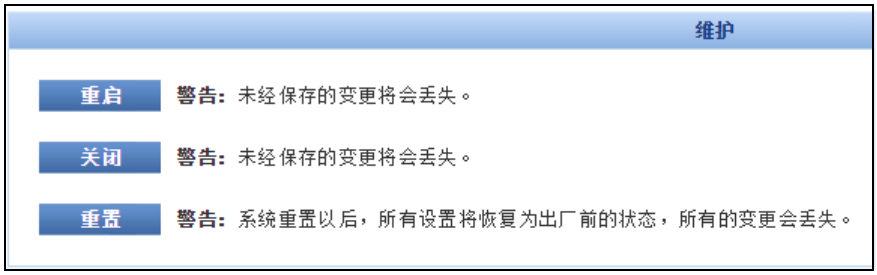
3.4.1 基本配置步骤

1. 选择**系统** > **概述**。
2. 点击系统信息参数对应的编辑系统信息。



3. 在**访问设置**区域查看访问服务的状态，点击进入**系统** > **服务配置** > **访问设置**页面配置访问服务。关于访问服务的更多信息，请参见 3.12 访问设置。

4. 在**维护**区域重启、关闭或重置系统。



配置注意事项

- 只有根管理员和根系统管理员可以重启和关闭系统。只有根系统管理员可以重置系统。
- 当系统重启、关闭或者重置时，未经保存的配置信息将会丢失。系统重置后，之前的日志会清除。请在执行该操作前，确认重要配置信息已经保存，避免信息丢失。

表 21 系统信息命令

show system info	查看系统信息。
hostname *name*	修改主机名。
language {**Chinese** | **English**}	设置系统语言。
timezone *timezone_id*	设置系统时区。
time *date time*	手动设置系统时间。
license import from	上载 License 文件。

表 22 重启和关闭命令

reboot	重启系统。
halt	关闭系统。
reset	重置系统。

3.4.2 配置参数说明

表 23 系统信息参数

参数	说明
主机名	系统主机名。长度 1-24 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。不能以 “-” 开头。
语言	当前系统语言，包括简体中文和英语。
时区	当前系统所在时区。
当前时间	当前系统时间。
License	当前系统的 License 信息。
SNMP	SNMP 服务状态。
上次更新时间	上次系统更新时间。

3.5 资产汇总

1. 选择**系统** > **资产信息** > **资产汇总**。
2. 查看硬件和操作系统信息。

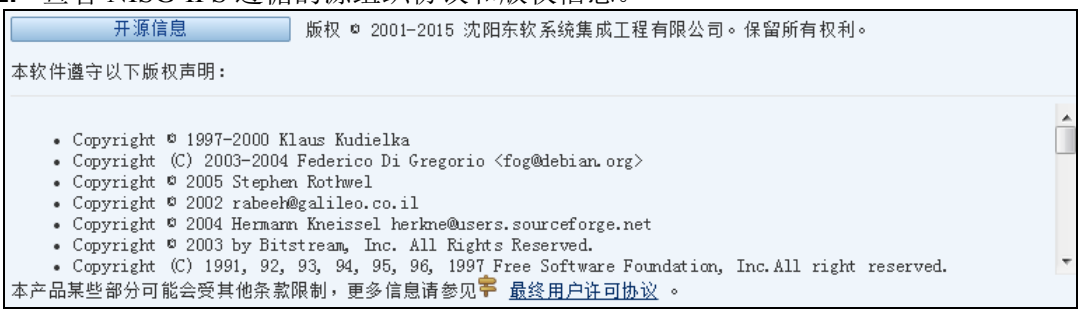
硬件信息	
平台	5000
机箱序列号	000C29A1BCEE
CPU制造商	GenuineIntel
CPU型号	Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz
CPU频率	3.09GHz
内存	3072 MB
磁盘0容量	8192 MB
磁盘0型号	VMware Virtual S
磁盘1容量	0 MB
磁盘1型号	Not installed
主板型号	VMware Virtual Platform
主板修订版	None
BIOS制造商	Phoenix Technologies LTD
BIOS版本	6.00
BIOS日期	07/31/2013
系统信息	
产品型号	5000
内部版本	4.2-BUILD700200

表 24 资产信息命令

show assetinfo	查看资产信息。

3.6 版权信息

1. 选择**系统** > **资产信息** > **版权信息**。
2. 查看 NISG-IPS 遵循的源组织协议和版权信息。



3. 点击页面上方的按钮查看开源信息。
4. 点击页面下方的链接查看最终用户许可协议。

3.7 系统时间

3.7.1 概述

系统时间即 NISG-IPS 系统时钟的时间。管理员可以通过手动校时或者 NTP 校时的方式来设置 NISG-IPS 系统时间。此外，管理员还可以设置 NISG-IPS 设备当前所在的时区。

3.7.2 基本配置步骤

1. 选择**系统** > **维护** > **日期时间**。
2. 手动校时。点击**当前时间**所对应的，在弹出的**当前时间**窗口手动设置系统时间。

系统时间范围为 1970 年 1 月 1 日 0 时 0 分 0 秒至 2037 年 12 月 31 日 23 时 59 分 59 秒。

3. 进行 NTP 校时。

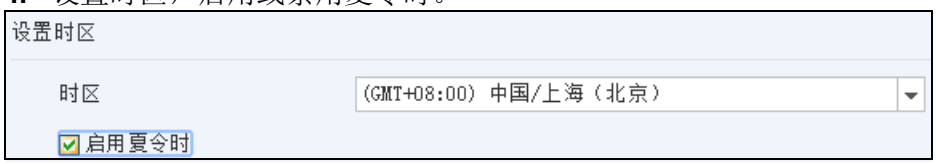
在启用 NTP 校时前，需要先设置 NTP 服务器地址。 NISG-IPS 支持一个主服务器和两个备份服务器。进行 NTP 校时时， NISG-IPS 最先向主 NTP 服务器发出校时请求。

NTP 校时支持系统立即校时或自动周期性校时。

- 设置 NTP 服务器地址，点击**立即同步**，可立即进行系统校时。
- 勾选**自动同步**启用自动校时。除了 NTP 服务器地址，还需要设置同步周期及最大时间误差。

NISG-IPS 支持 NTP 同步认证功能。启用此功能前，需要与 NTP 服务器管理员确定与每个 NTP 服务器对应的唯一密钥 ID 和预共享密钥。

4. 设置时区，启用或禁用夏令时。



5. 点击**确定**。
6. 点击 。

配置注意事项：

- 要设置系统时间，需要以根系统管理员身份登录。
- 完成时区配置后，需要保存当前配置并重新启动系统，以保证时区配置生效。

表 25 系统时间命令

time *date time*	手动同步系统时间。
ntp auto-syn {**enable** | **disable**}	启用或禁用 NTP 周期性校时。
ntp synchronize	启用或禁用 NTP 立即校时。
ntp authentication {**enable** | **disable**}	启用或禁用 NTP 认证。
ntp server {**server1** | **server2** | **server3**} {*ipv4* | *domain_name*} [**key_id** *id_num* **key** *password*]	添加 NTP 服务器。
unset ntp server {**server1** | **server2** | **server3**}	删除 NTP 服务器。
ntp auto-syn adjust *max_adjustment*	设置最大时间误差。
timezone *timezone_id*	设置系统时区。
timezone dst {**on default** | **off**}	启用或禁用夏令时。

3.7.3 配置参数说明

表 26 手动校时配置信息

参数	说明
当前时间	点击 修改系统当前时间。 日期输入格式为 YYYY-MM-DD。 时间输入格式为 HH:MM:SS。 • 小时的取值范围是 0-23。 • 分的取值范围是 0-59。 • 秒的取值范围是 0-59。
上次校时时间	上次执行校时的时间。
上次校时方式	上次执行校时的方式，包括： • **Not set**：尚未执行过系统校时。 • **Set (manually)**：上次校时方式为手动校时 （管理员手动设置）。 • **NTP (manually)**：上次校时方式为 NTP 立即校时。 • **NTP (automatic)**：上次校时方式为 NTP 自动周期性校时。 • **HA (changed)**：上次校时方式为 HA 同步引起的时间更新。

表 27 NTP 校时配置信息

参数	说明
NTP 校时	启用 NTP 校时，需要设置主备服务器 IP 地址或域名： • IP 地址的范围为 [1-223].[0-255].[0-255].[0-255]。 • 域名长度为 2-255 字节。 NTP 校时支持**自动同步**和**立即同步**两种方式。启用自动同步时，除了设置 NTP 服务器地址，还需要设置更新周期和最大时间误差。
认证	当开启同步认证时，需要设置主备服务器密钥 ID 和预共享密钥： • **密钥 ID**：取值范围为 1-65535。 • **预共享密钥**：字符串，长度为 1-32 字节。 密钥 ID 和预共享密钥必须成对出现。
更新系统时钟	NTP 自动校时周期，可以选择每月、每周、每天。
最大时间误差	系统当前时间与 NTP 服务器时间的最大允许差值。最大时间误差取值范围为 0-3600 秒。 • 仅当系统时钟与 NTP 服务器时间的差值小于最大时间误差时， NISG-IPS 才会按照 NTP 服务器的时间校时。 • 当最大时间误差值为 0 时，只要系统时钟与 NTP 服务器时间存在差值， NISG-IPS 就会按照 NTP 服务器时间调整系统时间。

表 28 时区配置信息

参数	说明
时区	当前系统所设置的时区。缺省时区为 GMT+8:00 中国 / 上海 （北京）。
启用夏令时	启用或禁用夏令时。

3.8 License

3.8.1 概述

License 可以控制的 NISG-IPS 功能如下表所示：

表 29 NISG-IPS License 的控制对象

功能	详细信息
防火墙	虚拟系统、用户、规则 / 策略、会话的最大数目及有效期。
IPSec VPN	IPSec VPN 隧道及隧道接口的最大数目及有效期，以及最大用户接入点数（Maximum User Access Points，缩写为 UAP）。
SSL VPN	SSL VPN 隧道及 SSL VPN 并发用户的最大数目及有效期。
IPS 相关	IPS 和 URL 过滤功能，以及 IPS、应用控制和 URL 过滤功能的规则更新。
旁路 IPS	旁路 IPS 功能及最大监听接口数目。
SMC 相关（CL）	SMC 能管理的客户端数目。

若要申请 License，需要获取 NISG-IPS 的序列号和型号信息（选择**主页** > **系统信息**）。

要成功上载其他功能的 License，必须先上载 FW 功能的 License。 NISG-IPS 最多可以上载 20 个 License。如果不同的 License 限制了同一功能，该功能的参数以后上载的 License 为准。

提示：必须上载相应的 License，才能使用相应的功能。

3.8.2 基本配置步骤

3.8.2.1 首次激活 License

1. 选择**主页** > **系统信息**。
2. 点击**序列号**对应的**激活**按钮。

- 点击**自动获取 License**，在线激活 License。自动激活要求设备已正确接入 Internet。
- 点击**输入 License**，在文本框中手动输入 License 字符串，手动激活 License。

3. 点击**确定**。

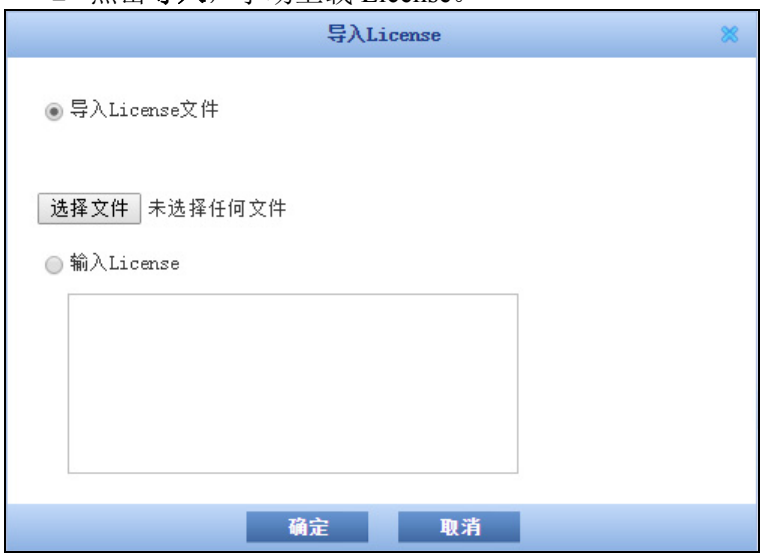
3.8.2.2 管理 License 文件

1. 选择**系统 > 概述 > 系统信息**并点击 **License** 对应的，或选择**系统** > **维护** > **License**。
2. 查看 License 信息。

系统License信息			
功能	参数	值	有效期
防火墙	虚拟系统	2	永久
	用户	50000	永久
	规则	10000	永久
	会话	1000	永久
IPSec VPN	IPSec VPN隧道接口	1000	永久
	IPSec VPN隧道	1000	永久
	最大用户接入点数	15000	永久
SSL VPN	SSL VPN隧道	1000	永久
	SSL VPN并发用户	1000	永久
IPS			2011-10-20
URL过滤			2011-10-20
IPS更新			2011-10-20
URL过滤更新			2011-10-20
应用更新			2011-10-20
旁路IPS	监听接口数	2	永久

3. 管理 License 文件：

- 点击**自动获取 License**，在线激活 License。
- 点击**导入**，手动上载 License。



4. 点击 。

配置注意事项

- 要下载 License 到本地或指定的 TFTP/SFTP 服务器对 License 进行备份，请以根管理员或根系统管理员身份登录。
- 通过 CLI 上载 License 时， License 文件名不能包含空格。
- 上载带有 FW 和 VPN 功能的 License 后需要重启系统才能生效。
- 在线激活 License 前，请确保设备已连接到 Internet 并正确配置了 DNS 主机地址。在线激活后，系统将重启。

表 30 License 命令

show license	查看 License 信息。
license import from {**x/zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *password file_name*}	上载 License 文件。
license word import *string*	上载 License 字符串。
unset license word *trait_name*	删除 License 文件。
license download to {**x/zmodem** *trait_name* | **tftp** *ip_tftp trait_name* | **sftp** *ip_sftp* **username** *user_name* **password** *password file_name*}	下载 License 文件。
license automatic activate	自动激活 License。

3.8.3 配置参数说明

表 31 无 License 时的操作权限

模块	权限
初始化向导	通过向导完成透明或路由模式部署以及初始化配置。
系统	• 查看系统基本信息（包括型号、序列号、内存、软件名称、软件版本和运行时间）、资源使用情况和接口状态信息。 • 激活 License。 • 查看和设置主机名、系统语言、时区和系统时间、 License、管理用户及访问服务。 • 修改根管理员和根系统管理员密码。 • 重启、重置和关闭系统。 • 使用 ping、 ping6、 nslookup 和 traceroute 诊断工具。 • 配置设备是否可以被集中管理系统管理。 • 查看资产及版权信息。
网络	查看和配置接口、STP、安全域、DNS 主机、DNS 代理、DDNS、DHCP 服务器、DHCP 作用域、缺省路由、多播路由、源 / 目的地址转换、地址映射、 DVMRP、 IGMP Snooping、邻居发现、 DHCPv6 配置。
防火墙	查看和配置访问策略、多播策略和缺省策略。
监控	查看拓扑、接口流量、实时接口流量、 STP、路由、地址转换、 GRE 隧道、 DVMRP 邻居和 IGMP Snooping 状态等监控信息。

3.9 系统升级

3.9.1 概述

系统升级通过加载安装升级包和增强升级包实现弥补自身缺陷或增强功能的目的。安装升级包仅用于手动升级，增强升级包用于手动和自动升级。

- 手动升级

  管理员通过 WebUI 或者 CLI 将获取的升级包手动上载到系统，完成升级。

- 自动升级

  NISG-IPS 支持立即升级和自动周期性升级。启用自动周期性升级，管理员需要设置升级模式和升级周期。

- 升级历史

  NISG-IPS 最多支持 50 条升级记录。

NISG-IPS 支持无缝升级，即通过自动或者手动方式进行系统更新后，原系统内所有的配置及日志完整保留，不会丢失或者损坏。

3.9.2 基本配置步骤

1. 选择**系统** > **系统升级** > **安装升级包**。

2. 手动升级：
   - 通过 WebUI 将本地升级包通过 HTTPS 上载。
   - 通过 CLI 将本地升级包通过 X/Zmodem 或者 SFTP/TFTP 上载。
3. 自动升级：
   - 点击**立即更新**立即升级系统。
   - 设置升级服务器地址、升级模式及升级周期进行自动周期性升级。

4. 查看或导出升级记录。
5. 点击 。

配置注意事项

- 使用自动升级方式前，需要配置 DNS 主机地址，确保 NISG-IPS 可以访问升级服务器域名。
- 如需修改升级服务器地址，请保存修改后再执行立即升级操作。
- 当系统无法连接升级服务器时，自动升级模式下会重试 3 次，立即升级模式下只重试 1 次。如果仍然无法连接，那么系统将等待至下一次升级周期开始。
- 当更新多个增强升级包时，系统将一次完成所有的升级操作。有些增强升级包安装后重启才能生效，此时 NISG-IPS 会提示用户重启系统。请在执行该操作前，确认已保存了重要的配置信息，以防配置丢失。

表 32 系统升级命令

show package upgrade config	查看系统升级配置。
package upgrade immediately	立即进行系统升级。
package upgrade from {**x/zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *password file_name* | **internal** *file_name*}	安装系统升级包。
package upgrade server {*server_name* | *server_ip*}	设置系统升级服务器。
package upgrade mode {**install update-schedule** {**daily** *time* | **weekly** *weekday* | **monthly** *date*} | {**download** | **check**} **check-schedule** {**daily** *time* | **weekly** *weekday* | **monthly** *date*} | **never**}	设置系统升级模式。
show package upgrade config	查看系统升级配置。

3.9.3 配置参数说明

表 33 系统升级配置信息

参数	说明
更新信息	• **系统版本**：当前升级包的版本信息。 • **信息**：可用升级包信息。
更新模式	可以选择通过 Internet 自动更新或手动上载升级包更新。选择自动更新，需设置： • **更新服务器 URL**：缺省的升级服务器地址为 nts.neusoft.com/autoupdate。 • **更新模式**：NISG-IPS 支持四种自动更新模式： - **下载更新，允许我选择是否安装更新。** - **自动安装更新 （推荐）。** - **检查更新，并允许我选择是否下载和安装更新。** - **从不检查更新。** • **检查时间表**：自动安装升级包的周期。周期可以设置为每天、每周或者每月中的某一固定时刻。

3.10 安装升级包管理

1. 选择**系统** > **系统升级** > **管理安装升级包**。
2. 切换安装升级包。
3. 删除安装升级包。

4. 点击 。

配置注意事项

- 只有根系统管理员可以切换或删除安装升级包。
- 切换安装升级包版本后，系统将重启，请在系统重新启动之前，确认已保存了重要的配置信息，以防配置丢失。
- NISG-IPS 同时只能启用一个安装升级包。正在使用的安装升级包不能被删除。

表 34 安装升级包命令

system switch *file_name*	切换系统版本。
delete system *file_name*	删除非启用状态的安装升级包。

3.11 增强升级包管理

1. 选择**系统** > **系统升级** > **管理增强升级包**。
2. 启用或禁用增强升级包。
3. 删除增强升级包。

4. 点击 。

配置注意事项

- 只有根管理员和根系统管理员能够查看增强升级包信息。
- 根系统管理员可以启用、禁用以及删除增强升级包。
- 手动升级中，每次只允许上载一个增强升级包。自动升级中，升级服务器可以一次上载多个增强升级包。
- 增强升级包分为系统增强升级包和规则库增强升级包。启用或删除系统增强升级包之后，系统可能会提示重新启动。请在执行该操作前，确认已保存了重要的配置信息。
- 通过禁用增强升级包，管理员可以将 NISG-IPS 系统回退到升级之前的版本。最多可保留一个增强升级包，支持回退一次。

表 35 增强升级包命令

patch {enable | disable}	启用或禁用增强升级包。
delete patch *file_name*	删除增强升级包。

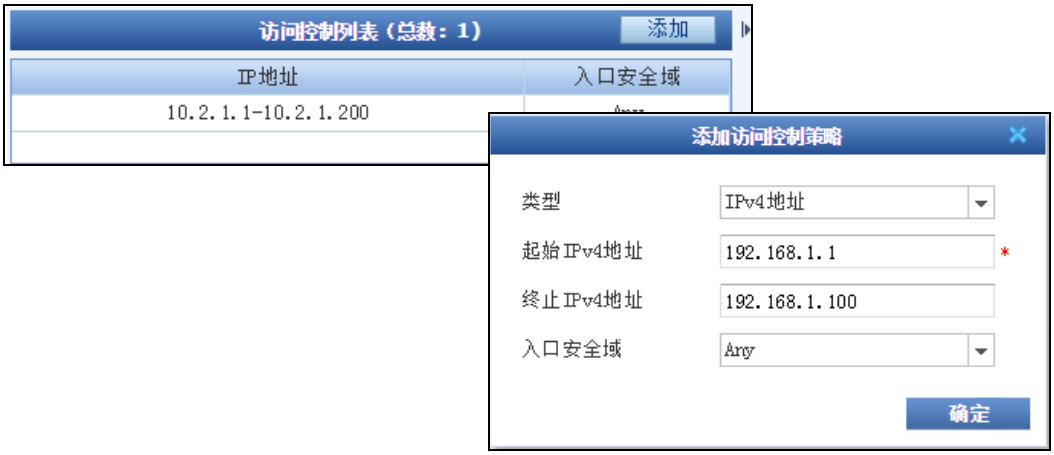
3.12 访问设置

NISG-IPS 为远程主机提供多种服务，包括支持远程主机以 Telnet、 SSH、 Web 方式访问 NISG-IPS，使用 Ping 服务测试远程主机和 NISG-IPS 之间的连通性，以及支持根管理员远程访问 NISG-IPS。

3.12.1 基本配置步骤

1. 选择**系统** > **服务配置** > **访问设置**。
2. 启用访问服务并设置服务端口号。

3. 创建访问控制策略，设置允许访问的 IP 地址范围。



提示：旁路模式下，不对入口安全域进行限制。

4. 允许或拒绝根管理员远程登录。

5. 点击**确定**。
6. 点击 。

表 36 访问服务命令

show service [**telnet** | **web** | **ping** | **ssh**]	查看访问服务信息。
show root-net-login	查看根管理员远程访问控制。
service {**telnet** | **web** | **ping** | **ssh**} {**on** | **off**}	启用或禁用 Telnet、Web、Ping 或 SSH 服务。
service {**telnet** | **ssh** | **web**} **port** *num*	设置服务端口号。
service {**telnet** | **web** | **ping** | **ssh**} **allow** {**mgt-interface** | **zone** {*zone_name* | **any**}} *start_ip* [*end_ip*]	添加访问控制策略。
unset service {**telnet** | **web** | **ping** | **ssh**} [**allow** {**mgt-interface** | **zone** {*zone_name* | **any**}} *start_ip* [*end_ip*]]	删除访问控制策略。
service root-net-login {**enable** | **disable**}	允许或阻断根管理员远程登录。

3.12.2 配置参数说明

表 37 访问服务配置信息

参数	说明
服务状态	启用或禁用访问服务。
端口号	Telnet、 SSH 和 Web 端口范围均为 1-65535。
访问控制列表	包含访问控制策略。每个访问控制列表最多支持 32 条策略。每条策略限定了 IP 地址范围和入口安全域。 IP 地址范围和入口安全域范围内的主机可以通过访问服务访问 NISG-IPS。
root 用户访问控制	允许或阻断根管理员远程访问 NISG-IPS。

表 38 访问服务缺省配置

服务名称	描述
Web	为管理用户提供可视化管理界面。 默认使用 HTTPS 连接、 443 端口，允许任意 IP 地址访问，建议根据实际需求修改访问控制列表。
Telnet	当没有配置线或设备不在身边时，允许管理用户通过 Telnet 方式远程访问 NISG-IPS。 由于 Telnet 是明文传输，为保证设备安全， Telnet 服务默认关闭，缺省端口 23。
SSH	当没有配置线或设备不在身边时，允许管理用户通过 SSH 方式远程访问 NISG-IPS。 SSH 是密文传输，较 Telnet 更为安全。 SSH 服务默认开启，缺省端口 22，允许任意 IP 地址访问，建议根据实际需求修改访问控制列表。
Ping	用于测试远程主机和 NISG-IPS 之间的联通性。 当管理用户使用 Telnet 或 SSH 远程访问 NISG-IPS 时，需要保证管理主机和 NISG-IPS 之间的联通性，此时需要开启 Ping 服务。 Ping 服务默认开启，允许任意 IP 地址访问，建议根据实际需求修改访问控制列表。
Root 用户远程登录	允许 root 用户远程访问 NISG-IPS。 NISG-IPS 默认允许 root 用户远程登录，为保证设备安全，非必要情况下建议关闭该服务。

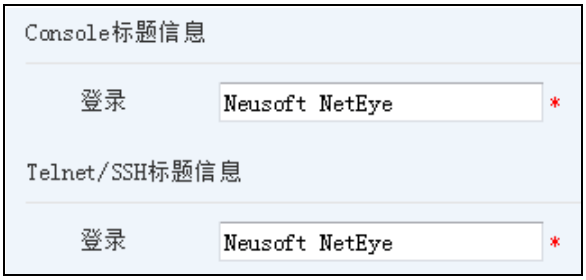
3.13 标题信息

3.13.1 概述

标题信息是在以 CLI 方式登录 NISG-IPS 时， NISG-IPS 所显示的标识信息。

3.13.2 基本配置步骤

1. 选择**系统** > **服务配置** > **标题信息**。
2. 设置 Console 或 Telnet/SSH 登录标题信息。标题信息的长度范围是 1-64 字节。



3. 点击**确定**。
4. 点击 。

表 39 标题信息命令

banner {**console** | **vty**} *string*	设置 NISG-IPS 的标题信息。

3.14 SNMP

3.14.1 概述

NISG-IPS 支持 SNMP 管理，允许网络管理站 （Network Management Station，简称 NMS）查询 NISG-IPS 的状态信息，但不允许其修改 NISG-IPS 的配置信息。

- 支持的 SNMP 版本

  NISG-IPS 支持 SNMP v1、 v2 和 v3。

- SNMP 用户

  在 SNMP v1 和 SNMP v2 中，管理站和被管设备之间通过团体字符串进行认证，数据通过明文传输。为保证管理数据安全，建议使用 SNMPv3 进行 SNMP 管理。

  在 SNMP v3 中，管理站和被管设备之间通过 SNMP 用户信息进行认证。 NISG-IPS 作为被管设备接受管理站的访问时，会根据 NISG-IPS 保存的 SNMP 用户信息对管理站进行认证。

  SNMP 用户信息与系统用户信息分别保存， SNMP 用户可以和系统用户重名。

NISG-IPS 提供管理信息数据库 （MIB），管理站可以通过调用 MIB 中的数据对象查询 NISG-IPS 的状态信息。 NISG-IPS 支持 RFC 定义的公有 MIB 库和东软的私有 MIB 库，详细信息请参见*东软 NetEye 集成安全网关 SNMP MIB 信息参考指南*。

提示：旁路模式下，不支持私有 MIB 库，所以 NMS 无法获取 IPS 检测信息。

3.14.2 基本配置步骤

1. 选择**系统** > **服务配置** > **SNMP 配置**。
2. 查看、启用或禁用 SNMP。启用 SNMP 后，需要设置端口号、团体字符串、物理位置字符串及联系信息字符串。

提示：NISG-IPS 和 NMS 上设置的团体字符串必须保持一致。

3. NISG-IPS 与 NMS 通过 SNMPv3 进行通讯时，需要添加 SNMP 用户。

提示：如果配置了 SNMP 用户认证或加密，则管理站上也要进行相应的设置。

4. 点击**确定**。
5. 点击 。

表 40 SNMP 命令

show snmp {**daemon** | **port** | **community** {**read-only** | **read-write**} | **location** | **contact**}	查看 SNMP 配置信息。
snmp daemon {**on** | **off**}	启用或禁用 SNMP。
snmp port *port_num*	设置 SNMP 服务端口号。
snmp community *string* {**read-only** | **read-write**}	添加指定权限的团体字符串。
snmp {**location** | **contact**} *string*	添加物理位置或联系信息字符串。
unset snmp {**community** {**read-only** | **read-write**} | **location** | **contact**}	删除团体、物理位置或联系信息字符串。
show snmp usm user [*user_name*]	查看 SNMP 用户信息。
snmp usm user *user_name* **seclvl authNoPriv authpro MD5 authpassphrase** *auth_password* {**read-only** | **read-write**}	添加安全级别为认证但不加密的 SNMP 用户。
snmp usm user *user_name* **seclvl authPriv authpro MD5 authpassphrase** *auth_password* **privpro DES privpassphrase** *privacy_password* {**read-only** | **read-write**}	添加安全级别为认证并加密的 SNMP 用户。
unset snmp usm user [*user_name*]	删除 SNMP 用户。

3.14.3 配置参数说明

表 41 SNMP 配置信息

参数	说明
启用 SNMP	启用或禁用 SNMP 功能。
SNMP 版本	NISG-IPS 支持 SNMP v1、 SNMP v2 和 SNMP v3。
端口	端口范围为 1-65535。
团体字符串	管理站和 NISG-IPS 之间进行身份识别的字符串。 团体字符串包括两种类型：只读和读写。由字母、数字、 @、下划线、连字符或句点构成，长度为 0-128 字节。
SNMP 物理位置字符串	描述 NISG-IPS 设备物理位置的信息。 由字母、数字、 @、下划线、连字符或句点构成，长度为 0-128 字节。
SNMP 联系信息字符串	管理员的联系信息。 由字母、数字、 @、下划线、连字符或句点构成，长度为 0-128 字节。

表 42 SNMP 用户配置信息

参数	说明
名称	SNMP v3 用户的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：* ? , " ' \ < > & #。 NISG-IPS 最多支持 5 个 SNMP v3 用户。
权限	SNMP v3 用户的权限： • **只读**：只可以查询 NISG-IPS 的状态信息。 • **读写**：既可以查询 NISG-IPS 的状态信息，又可以修改 NISG-IPS 的部分配置信息。可修改的配置信息包括团体字符串、物理位置字符串和联系信息字符串。
安全级别	SNMP 数据包在网络上传输的安全级别，包括认证并加密和认证但不加密。
认证	用于确认身份的字符串。长度 8-128 字节， ASCII 字符。不能包含空格和以下字符：? " ' < > &。 启用 SNMP 用户认证可以保证 NMS 接收数据来源的可靠性。
认证算法	认证所使用的算法。 NISG-IPS 将 MD5 作为认证算法。
密钥	用于信息加密的字符串。长度 8-128 字节， ASCII 字符。不能包含空格和以下字符：? " ' < > &。 启用加密可以保证 NISG-IPS 和 NMS 之间数据传输的安全性。
加密算法	加密使用的算法。 NISG-IPS 将 DES 作为加密算法。

3.15 管理用户

3.15.1 概述

3.15.1.1 管理用户

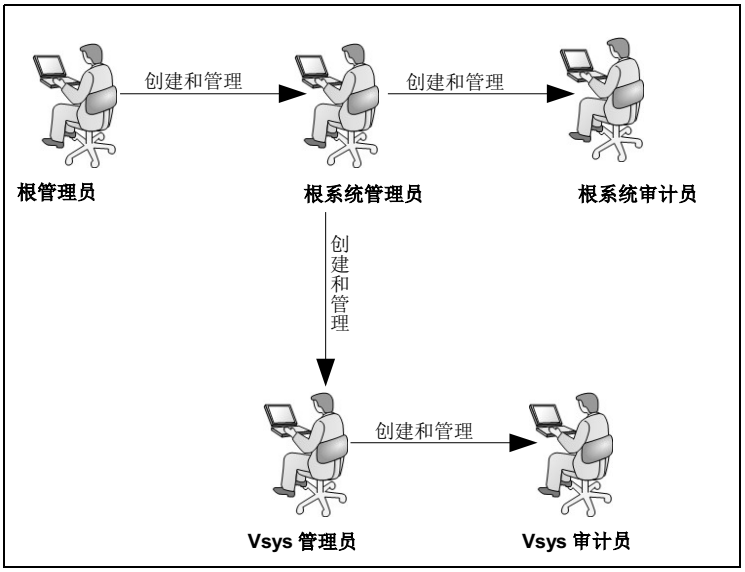
NISG-IPS 的管理角色如表 43 所示：

表 43 管理用户角色

管理角色	描述
根管理员	初始管理用户，不能被删除。其缺省用户名和初始口令分别为 “root” 和 “neteye”。具有只读权限，只能查看系统的配置信息。
根系统管理员	由根管理员创建和管理。具有读 / 写权限，可以查看和设置整个系统的配置信息。缺省根系统管理员名称为 “admin”，初始密码为 “neteye”。
根系统审计员	由根系统管理员创建和管理。具有只读权限，只能查看系统的配置信息。
Vsys 管理员	由根系统管理员创建和管理。具有读 / 写权限，可以查看和设置一个或者多个虚拟系统的配置信息。
Vsys 审计员	由 Vsys 管理员设置和管理。具有只读权限，只能查看系统的配置信息。

管理角色之间的关系如图 7 所示：

图 7 管理角色关系



3.15.1.2 配置锁

为了防止配置冲突， NISG-IPS 采用了配置锁机制。同一时间只允许一个管理用户对 NISG-IPS 进行配置操作。

- WebUI 中的配置锁

  以 WebUI 方式管理 NISG-IPS 时，如果想要修改 NISG-IPS 的配置信息，在登录成功后，需选择覆盖配置锁。如果没有选择覆盖配置锁，那么在 WebUI 界面的右上方可以看到，可以点击该图标获得配置锁。之前已获得配置锁的管理员将立即失去配置锁，只能进行查看操作。

  点击退出登录，即可自动释放配置锁。如果获得了配置锁但未退出登录而直接关闭浏览器，那么配置锁会一直有效，直到会话超时或者配置锁被覆盖。所以修改配置完成后，退出登录时，建议释放配置锁，以使其他用户能够及时申请到配置锁。

  以 WebUI 方式管理 NISG-IPS 时，获得配置锁后如果 30 分钟内无任何操作， NISG-IPS 将自动断开本次连接，同时释放配置锁。

- CLI 中的配置锁

  以 CLI 方式管理 NISG-IPS 时，管理员登录后，如果配置锁未被其他管理员占用，则可以通过 CLI 命令 “**configure mode**” 进入全局配置模式，进行配置操作。如果配置锁正在被其他管理用户占用，可以通过 CLI 命令 “**configure mode override**” 覆盖其他管理员的配置锁。管理员退出全局配置模式时，可以通过 CLI 命令 “**exit**”，释放配置锁。

3.15.2 基本配置步骤

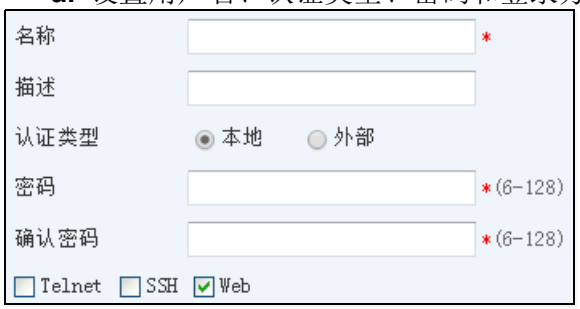
1. 选择**系统** > **认证** > **管理用户**。
2. 查看、编辑或删除管理用户，修改管理用户密码。
   - 如果以根管理员身份登录，可以查看和编辑根系统管理员，重置根管理员自身的密码。

   - 如果以根系统管理员身份登录，可以查看和编辑审计员和 Vsys 管理员，重置当前登录的根系统管理员密码。

- 如果以 Vsys 管理员身份登录，可以查看和编辑 Vsys 审计员，重置当前登录的 Vsys 管理员密码。

3. 点击**新建**，创建管理用户。

a. 设置用户名、认证类型、密码和登录方式。管理用户名称须唯一。

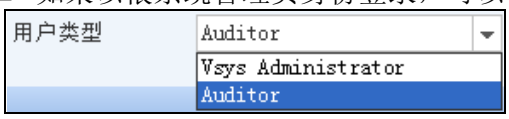


- 如果选择本地认证，需要设置密码，两次输入密码必须一致；如果选择外部认证，需要到**系统 > 认证 > 认证配置**页面指定管理用户的认证服务器。
- 系统默认允许管理用户通过 Web 登录，可根据需要开启 Telnet 和 SSH 服务。

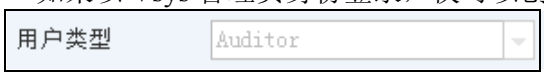
b. 设置用户类型。

- 如果以根管理员身份登录，仅可以创建根系统管理员。

- 如果以根系统管理员身份登录，可以创建审计员和 Vsys 管理员。



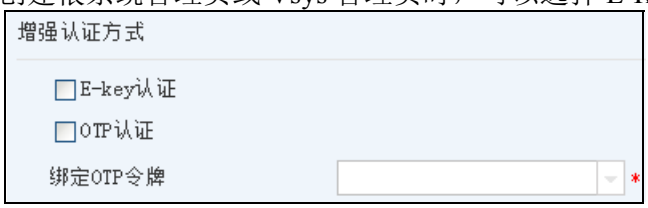
- 如果以 Vsys 管理员身份登录，仅可以创建 Vsys 审计员。



c. 创建 Vsys 管理员时，需要指定可管理的虚拟系统。

根系统管理员缺省从属于根系统。也可以为根系统管理员分配多个虚拟系统，使之获得相应 Vsys 的管理权限。

d. 创建根系统管理员或 Vsys 管理员时，可以选择 E-Key 或 OTP 增强认证方式。



- 若要使用 E-Key 认证，需要插入存储有客户端证书的 USB Key 硬件设备，还需要将签发客户端证书的 CA 证书上传到 NISG-IPS。关于如何使用 E-Key 认证，请参见 3.19 E-Key 认证。
- 如果为管理用户启用 OTP 认证，需要同时绑定一个 OTP 令牌，并在登录时输入 OTP 设备上显示的密码。关于如何使用 OTP 认证，请参见 3.20 OTP 认证。
- 以根管理员身份登录，可以为根系统管理员启用、禁用 E-Key 或 OTP 认证。
- 以根系统管理员身份登录，可以为 Vsys 管理员启用、禁用 E-Key 或 OTP 认证。
- 根系统管理员也可以启用、禁用自身的 E-Key 或 OTP 认证。

4. 点击**确定**。

5. 点击 。

表 44 管理用户命令

show user administrator	查看管理用户信息。
password	修改管理用户口令。
user administrator	创建或编辑管理用户。
unset user administrator	删除管理用户。

3.15.3 配置参数说明

表 45 管理角色配置权限

管理角色	配置权限
根管理员	• 设置管理用户 - 创建、删除和编辑根系统管理员 - 修改根管理员和根系统管理员口令 • 设置 NISG-IPS - 上载、下载和删除 License - 重启和关闭 NISG-IPS - 为管理用户设置本地认证 - 切换语言 • 查看系统配置信息
根系统管理员	• 设置管理用户 - 创建、删除和编辑根系统审计员和 Vsys 管理员 - 修改根系统审计员和 Vsys 管理员口令 - 指定根系统管理员为 Vsys 管理员 • 设置 NISG-IPS - 切换及配置 Vsys - 设置系统维护、服务配置、用户与认证、证书、日志配置、系统升级、高可用性 - 进行网络配置、路由、地址转换 - 设置策略、对象、虚拟专用网、攻击防御及入侵防御 • 查看系统配置信息
根系统审计员	• 修改根系统审计员的口令 • 查看系统配置信息
Vsys 管理员	• 设置管理用户 - 创建、删除和修改当前 Vsys 的审计员 - 修改 Vsys 审计员和 Vsys 管理员的口令 • 设置虚拟系统 - 切换到其他 Vsys - 设置当前 Vsys • 查看当前虚拟系统配置信息
Vsys 审计员	• 修改 Vsys 审计员的口令 • 查看当前虚拟系统配置信息

表 46 管理用户配置信息

参数	说明
名称	管理用户名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：* ? , " ' \ < > & #。
描述	管理用户的描述信息。长度 0-255 字节， UTF-8 字符。不能包含以下字符：? " ' \ < > &。
认证类型	管理用户的认证类型，包括本地认证和外部认证。
密码	根系统管理员或 Vsys 管理员登录 NISG-IPS 的密码。长度范围为 6-128 个字符。
登录方式	管理用户登录方式，包括 Telnet、 SSH 和 Web。

表 46 管理用户配置信息 (*续*)

参数	说明
用户类型	管理用户的类型。 • 如果以根管理员身份登录，仅能够创建根系统管理员 （Administrator）。 • 如果以根系统管理员身份登录，可以创建根系统审计员 （Auditor）和 Vsys 管理员（Vsys Administrator）。 • 如果以 Vsys 管理员身份登录，仅可以创建本 Vsys 的审计员。 审计员仅具备查看权限。
虚拟系统列表	创建 Vsys 管理员时需要设置所能管理的虚拟系统。 一个 Vsys 管理员可管理多个 Vsys。
增强认证方式	• **E-key 认证**：开启 E-Key 认证后，管理用户需要输入用户名、密码、验证码并且插入对应的 USB Key 才能登录。 USB Key 是一个存储客户端证书的 USB 硬件设备。 • **OTP 认证**：开启 OTP 认证的同时需要为管理用户选择绑定的 OTP 令牌。 开启 OTP 认证后，管理用户需要输入用户名、密码、验证码并且输入 OTP 硬件设备上显示的动态密码才能登录。

3.16 网络用户

3.16.1 概述

网络用户指通过 NISG-IPS 认证和授权后可访问网络资源的用户。 NISG-IPS 网络用户包括：

- WebAuth 用户

  管理员需要为 NISG-IPS 上集成的 WebAuth 服务器指定 IP 地址和端口以供 WebAuth 用户登录。 WebAuth 用户需要预先知道认证服务器的访问方式和合法的用户名和口令，才可以进行网络访问。 WebAuth 用户可以通过主动或被动认证登录。关于 WebAuth 认证的详细信息，请参见 3.18 WebAuth 配置。

- IPSec VPN 用户

  IPSec VPN 用户包括 Xauth 用户和 L2TP 用户，可以通过外部认证服务器认证或本地认证。 NISG-IPS 将 IPSec VPN 用户定义为远程拨号用户来进行管理。 IPSec VPN 用户要接入 VPN 前，必须接受 NISG-IPS 对其进行的身份认证。认证通过后，方可接入 VPN。

- SSL VPN 用户

  SSL VPN 用户指通过 SSL VPN 服务接入访问的用户。 SSL VPN 用户可以划入 SSL VPN 用户组成为组内成员。 SSL VPN 用户可通过本地数据库或外部认证服务器进行认证。

NISG-IPS 允许网络用户进行多点登录。网络用户可以通过单点或多点登录到 NISG-IPS。

NISG-IPS 对网络用户的在线时间和流量进行记录，通过 RADIUS 服务器对用户产生的流量进行计费。如果一个网络用户在规定的超时时间内没有流量， NISG-IPS 则会认为其下线。超时时间可以针对用户单独配置。如果不配置，则超时时间取网络用户所在虚拟系统默认配置的时间。

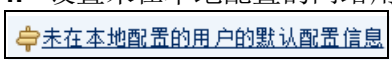
对未在本地配置的网络用户， NISG-IPS 提供默认配置。管理员可以通过点击超链接设置未在本地配置的用户的默认配置，包括用户超时时间及用户类型等信息。

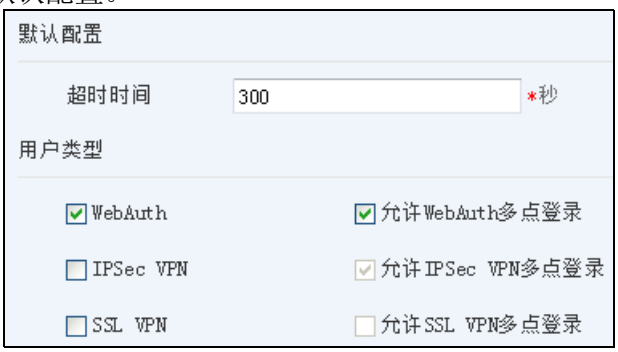
3.16.2 基本配置步骤

1. 选择**系统** > **认证** > **网络用户**。
2. 查看、删除、启用或禁用网络用户，修改用户密码。

3. 创建或编辑网络用户。

4. 设置未在本地配置的网络用户的默认配置。





5. 点击**确定**。
6. 点击 。

表 47 网络用户命令

show user authuser	查看网络用户信息。
user authuser enable, disable	启用或禁用网络用户。
user authuser password	修改网络用户密码。
user authuser	创建网络用户。
unset user authuser	删除网络用户。

3.16.3 配置参数说明

表 48 网络用户配置信息

参数	说明
名称	网络用户名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：* ? , " ' \ < > & #。
认证类型	网络用户的认证类型，包括本地认证和外部认证。
用户类型	网络用户的类型，包括 WebAuth、 IPSec VPN 和 SSL VPN。
超时时间	网络用户的超时时间，范围是 0-3600 秒。 如果配置为 0 秒，则不限制该网络用户的超时时间，只要用户不主动下线，则永远不会下线（管理员强制其下线除外）。 IPSec VPN 用户暂不支持超时时间。
时间表	网络用户拥有指定访问权限的有效时间段，包括起始日期和终止日期。
引用	引用该用户的访问策略列表。
启用	启用或禁用网络用户。只有启用后，网络用户才能通过 NISG-IPS 访问网络资源。
密码	网络用户的认证密码。长度 1-127 个字节。

表 48 网络用户配置信息 (*续*)

参数	说明
分配的 IP	为 IPSec VPN 和 SSL VPN 用户分配地址，包括用户 IP 地址、主备 DNS 服务器地址及主备 WINS 服务器地址。用户地址可以是静态 IP 或从 IP 地址池获得。
IPSec VPN 配置	IPSec VPN 用户配置： • **用户类型**：包括 Xauth 和 L2TP。 •如果选择 Xauth 类型， VPN 用户必须使用 Greenbow 客户端。 •如果选择 L2TP 类型，必须为 VPN 用户配置静态 IP 地址或 IP 地址池。 • **ID 类型**：设置远程拨号 VPN 用户的 IKE 身份标识类型，支持以下几种： •**IPV4_ADDR**：VPN 客户端的 IP 地址。 •**FQDN**：VPN 用户的完全合格域名，例如 www.abcd.com。也可以是 VPN 客户端的计算机名。 •**USER_FQDN**：VPN 用户的邮件地址。 •**DER_ASN1_DN**：VPN 用户使用的证书的主题信息，例如：“C=CN, ST=LiaoNing, O=abcd, OU=Network Security Department, CN=149,E=149@abcd.com”。DER_ASN1_DN 格式的 ID 可以从证书中获取。 •**KEY_ID**：标识 VPN 用户身份的一个字符串。 ASCII 码 32-126 能够表示的所有字符，除 ? , " ' \ < > & 以及空格。最大支持 1023 个字节。 当 VPN 客户端配置了静态 IP 地址时，五种类型的 ID 都可以使用；当 VPN 客户端使用动态 IP 地址时，只能使用 FQDN、 USER FQDN、 DER ASN1 DN 或 KEY ID 类型的 ID。 如果客户端与 VPN 网关之间存在 NAT 设备或者用户通过 PPPoE 拨号连接，则用户的 ID 类型不能设置为 IPV4_ADDR。在此种场景下，当 VPN 的认证方式为预共享密钥认证时，ID 类型需设置为 FQDN、 USER_FQDN 或 KEY_ID （Windows 的 VPN 客户端需设置为 FQDN）；当 VPN 的认证方式为证书认证时， ID 类型需设置为 DER_ANS1_DN。

3.17 用户认证

3.17.1 概述

3.17.1.1 本地 / 外部认证

在 NISG-IPS 中，管理用户及网络用户的认证方式分为两种，可以通过本地数据库或外部认证服务器进行认证。

- 本地数据库认证

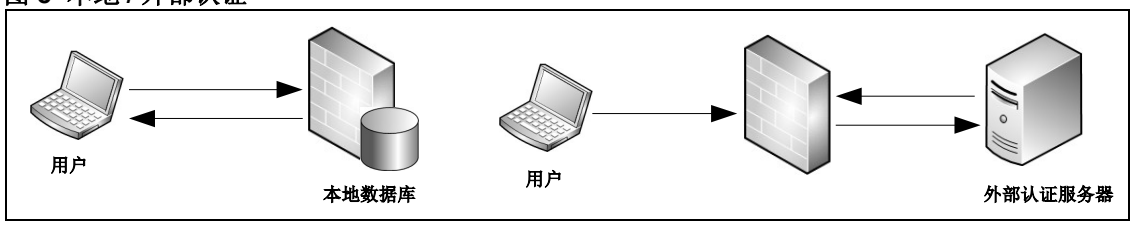
  用户认证信息保存在 NISG-IPS 本地数据库中。用户登录时需要向 NISG-IPS 提供用户名和密码。 NISG-IPS 将用户信息与本地数据库中保存的用户信息进行匹配。如果一致，则认证成功。

- 外部服务器认证

  用户认证信息保存在管理员配置的外部认证服务器中。 NISG-IPS 收到用户的登录请求后，会向配置的外部认证服务器发出验证请求。服务器将用户提供的信息与存储的信息进行匹配。如果一致，则认证成功。

本地认证的优先级高于外部认证。本地创建的管理用户，即使认证方式设为外部，NISG-IPS 仍然首先查找本地数据库进行本地认证，本地无身份信息后查找外部认证服务器。本地认证和外部认证如图 8 所示。

图 8 本地 / 外部认证



3.17.1.2 认证服务器

NISG-IPS 支持以下四种外部认证服务器：

- RADIUS 服务器

  在线模式下， NISG-IPS 还可以通过 RADIUS 服务器实现实现对网络用户的计费功能。

- LDAP 服务器
- Active Directory 服务器
- eDirectory 服务器

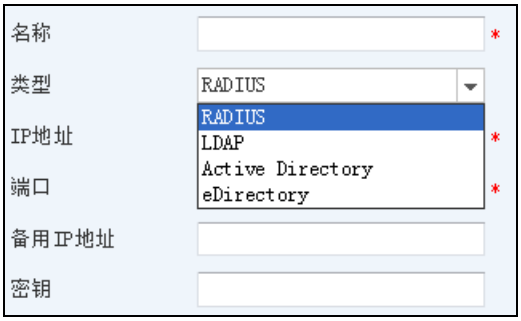
LDAP、 Active Directory 及 eDirectory 服务器认证过程基于 LDAPv3。

NISG-IPS 支持备用服务器。当 NISG-IPS 与主服务器无法建立连接或者主服务器在默认超时时间 （30 秒）内无应答时，启用备用服务器。主备服务器端口必须一致。

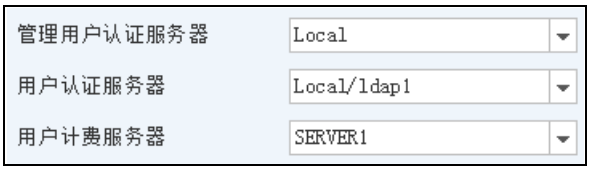
3.17.2 基本配置步骤

1. 选择**系统** > **认证** > **认证服务器**。
2. 查看或删除认证服务器。

3. 添加或编辑认证服务器。



4. 选择**系统** > **认证** > **认证配置**。选择用户认证服务器。



5. 点击**确定**。
6. 点击 。

配置注意事项

- 外部认证服务器名称须唯一。
- NISG-IPS 最多支持四个外部认证服务器。
- 正在被使用的服务器不可被直接删除。如果要删除，请先指定其他外部认证服务器。
- 修改认证服务器的配置参数，不影响已经完成认证的连接，只对更改之后发起的认证生效。
- 根管理员仅可以设置管理用户的认证方式，且只能将认证方式设置为本地。

表 49 认证配置命令

server authentication type administrator | authuser	指定管理用户或网络用户的认证服务器。
show server authentication	查看认证服务器。

表 49 认证配置命令 (*续*)

server account	指定网络用户的计费服务器。
unset server account	删除计费服务器。
show server account	查看计费服务器。

表 50 认证服务器命令

radius | ldap | active-directory | edirectory server	添加 RADIUS、 LDAP、 Active Directory 或 eDirectory 服务器。
unset radius | ldap | active-directory | edirectory server	删除 RADIUS、 LDAP、 Active Directory 或 eDirectory 服务器。
show radius | ldap | active-directory | edirectory server	查看 RADIUS、 LDAP、 Active Directory 或 eDirectory 服务器。

3.17.3 配置参数说明

表 51 认证服务器和计费服务器配置信息

参数	说明
管理员认证服务器	为管理用户指定认证服务器，可以是本地或者指定的外部服务器。
用户认证服务器	为网络用户指定认证服务器，可以是本地或者指定的外部服务器。
用户计费服务器	为网络用户指定计费服务器， RADIUS 服务器有计费功能。

表 52 认证服务器配置信息

参数	说明
名称	认证服务器名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #。
IP 地址 / 域名	认证服务器的 IPv4 地址或域名。 NISG-IPS 将向此 IP 地址或域名发送认证请求。域名长度为 2-255 字节。
端口	认证服务器端口号。 NISG-IPS 将向此端口发送认证请求。端口的取值范围为 1-65535。
备用 IP 地址 / 域名	认证服务器的备用 IPv4 地址或域名。域名长度为 2-255 字节。
安全连接	如果传输需要使用 SSL 加密，则需启用安全连接。安全连接类型包括 SSL/TLS 和 STARTTLS。
证书	启用安全连接后服务器使用的 CA 证书。
公共名标识符	用来识别在 LDAP 服务器中输入的个体的标识符。由除空格和问号外的任意 UTF-8 字符组成。取值范围为 0-80 字节。
识别名称	认证服务器在使用公共名标识符搜索具体条目前使用的路径。由除空格和问号外的任意 UTF-8 字符组成。取值范围为 0-511 字节。

表 52 认证服务器配置信息 (*续*)

参数	说明
管理员识别名称	具有管理员权限的用户 DN，用来与认证服务器绑定以获取查询权限。由除空格和问号外的任意 UTF-8 字符组成。取值范围为 0-511 字节。
密钥	• RADIUS：服务器与 NISG-IPS 协商的共享密钥，用来验证 RADIUS 数据包的合法性。只有在密钥一致的情况下，彼此才能接收对方发来的数据包，并作出响应。长度范围为 0-64 字节。 • LDAP/Active Directory/eDirectory：具有管理员权限的用户密码。长度范围为 0-127 字节。
状态	认证服务器当前的使用状态。如果正在被使用，其状态显示为 In Use。

3.18 WebAuth 配置

3.18.1 概述

WebAuth 认证是一种对用户上网权限进行控制的身份认证方式，通过普通的浏览器软件即可进行认证。 NISG-IPS 的 WebAuth 认证主要通过 HTTP 拦截和 HTTP 重定向实现。

3.18.1.1 认证过程

1. 在认证之前， NISG-IPS 将用户发出的所有 HTTP 请求都拦截下来，并重定向到 WebAuth 认证服务器，在用户的浏览器上将弹出一个认证页面；
2. 在认证过程中，用户在认证页面上输入认证信息 （用户名、口令等）与 WebAuth 认证服务器交互，完成身份认证。
   - 用户名和密码存在 NISG-IPS 本地时，只需要与 NISG-IPS 本地交互；
   - 用户名和密码存在外部服务器 （如 Radius）时，需要 NISG-IPS 与外部服务器交互，进行用户认证。
3. 在认证通过后，WebAuth 认证服务器将通知 NISG-IPS 该用户已通过认证，NISG-IPS 将允许用户访问互联网资源。

3.18.1.2 配置要点

1. 在接口上启用 WebAuth 认证。
2. 创建自动重定向策略。

实现 WebAuth 认证需满足以下条件：

1. WebAuth 认证已启用，用户通过认证接口访问网络。
2. 用户数据包匹配自动重定向策略。

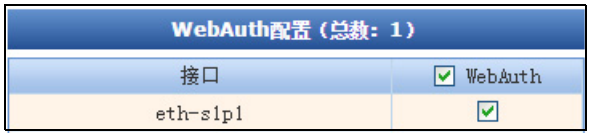
WebAuth 认证成功后，用户可以实现网络访问。

3.18.1.3 应用场景

NISG-IPS 部署在内外网边界处，内网主机的网关指向 NISG-IPS 内网口，内网用户需要进行身份认证才能允许访问外网。通过配置 WebAuth 认证，NISG-IPS 可以有效控制用户上网权限，保护内网安全。

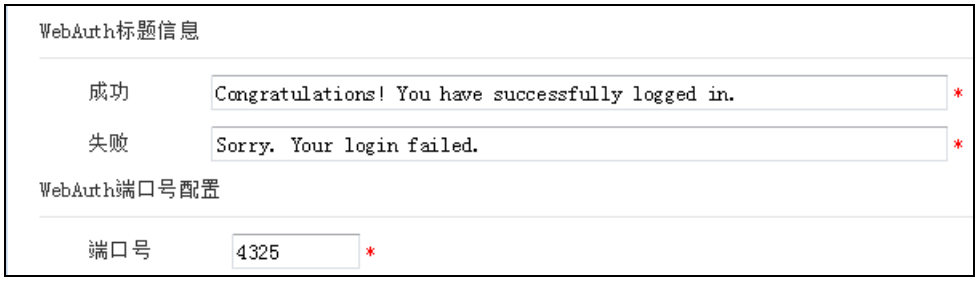
3.18.2 基本配置步骤

1. 选择**系统** > **认证** > **WebAuth 配置**。
2. 三层接口上开启 WebAuth 认证。



提示：WebAuth 认证可以在以下三层接口上开启：以太网接口、 Channel 接口、冗余接口、 PPPoE 接口和 VLAN 接口。

3. 设置 WebAuth 认证成功或失败的标题信息和认证端口号。



4. 点击**对未标识会话进行被动 WebAuth 认证**前面的 图标，查看或删除 WebAuth 自动重定向策略。

5. 创建或编辑 WebAuth 自动重定向策略。

6. 点击**确定**。

7. 点击 。

配置注意事项

- 每个虚拟系统最多支持 64 条自动重定向策略。
- 每条策略中最多可以添加 4096 个源 IP 地址条目和 4096 个目的 IP 地址条目。

表 53 WebAuth 认证命令

webauth banner	设置 WebAuth 标题信息。
webauth auth-port	设置 WebAuth 端口号。
webauth on,off	启用或禁用 WebAuth 认证。
webauth policy	创建 WebAuth 自动重定向策略。
unset webauth policy	删除 WebAuth 自动重定向策略。

3.18.3 配置参数说明

表 54 WebAuth 自动重定向策略配置信息

参数	说明
名称	WebAuth 自动重定向策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。每条策略都有独特的名称，在创建后不能修改。
源安全域	发出数据包的安全域。
目的安全域	接收数据包的安全域。
源 IP 地址	发出数据包的 IPv4 或 v6 地址。
目的 IP 地址	接收数据包的 IPv4 或 v6 地址。
服务	进行被动认证连接的端口号，可以是 HTTP 服务对象 （目的端口为 80）或目的端口 （端口范围 1-65535）。

表 55 WebAuth 认证配置信息

参数	说明
WebAuth 标题信息	用户经过 WebAuth 服务器验证身份后返回的提示信息。长度 1-220 字节， UTF-8 字符。不能包含空格和以下字符：？" ' \ < > &。
WebAuth 端口号配置	连接 WebAuth 服务器的端口号。端口号取值范围为 1-65535。
接口	启用 WebAuth 功能的接口。此接口可以是除环回接口和隧道接口外的其他所有三层接口。
WebAuth	启用或禁用 WebAuth 功能。

3.19 E-Key 认证

本节内容包括：

3.19.1 概述

为了解决静态口令认证方式的安全性问题， NISG-IPS 引入了 E-Key 增强认证方式。即用户在登录时，需要插入绑定的 USB Key 设备并输入 PIN 码才可以成功登录。

提示：NISG-IPS 使用 E-Key 认证的同时，保留了传统的静态口令认证，以达到多重认证效果。

E-Key 支持的操作系统包括 （英文和简体中文版）：

- Windows 2000/XP/Vista/7/8
- Windows Server 2003/2008
- Linux
- Mac OS X

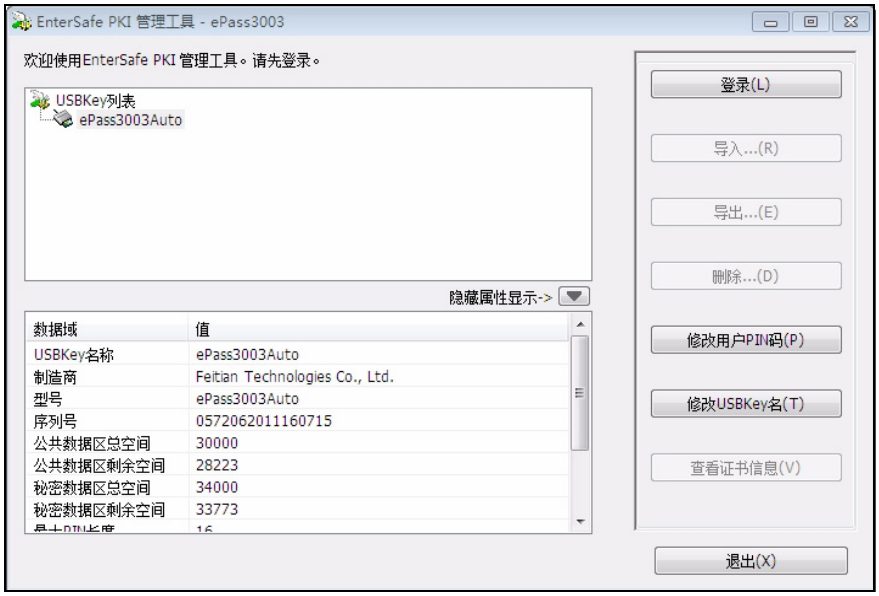
NISG-IPS 的 E-Key 支持 USB1.1 和 USB2.0。 USB Key 用于存储用户证书。

3.19.2 基本配置步骤

提示：NISG-IPS 的 E-Key 认证目前只支持对根系统管理员和 Vsys 管理员的认证。

3.19.2.1 制作 USB Key

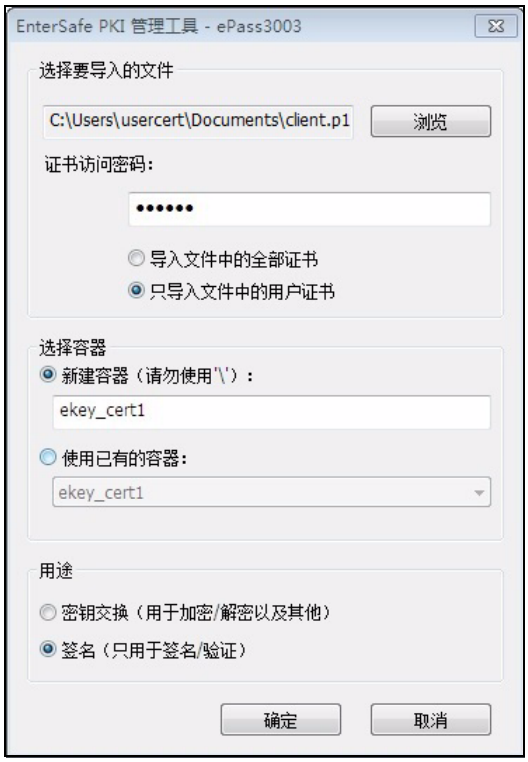
1. 在登录 PC 上插入定制的 USB 设备。
2. 双击系统中出现的 USB 驱动图标，完成驱动安装。
3. 电脑右下角的通知区域出现一个图标，双击该图标打开 USB 管理软件。



提示：您可以根据需要点击右侧的操作按钮修改 PIN 码和 USB Key （令牌）名称。

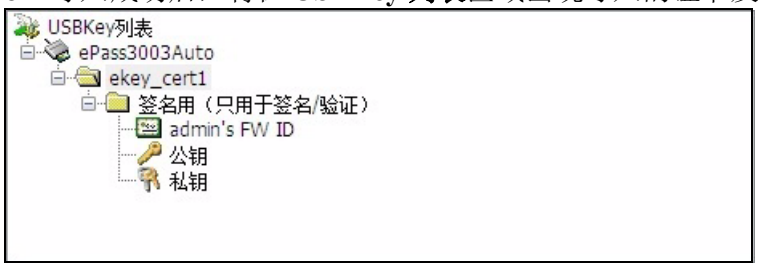
4. 在 **USBKey 列表**区域选择要进行操作的 USB 设备，点击右侧的**登录**按钮，输入 PIN 码（缺省为 123456）。

5. 登录后，右侧置灰的操作按钮变为可用状态。点击**导入**按钮，选择要用于 E-Key 认证的用户证书，输入证书的访问密码，用途选择“签名”。



提示：仅允许导入 pfx/p12 格式的证书。要导入的证书应事先存储在本地。

6. 导入成功后，将在 **USBKey 列表**区域出现导入的证书及详细信息。



3.19.2.2 导入 CA 证书

要使用 E-Key 认证，需要将签发 E-Key 用户个人证书的 CA 证书上载至 NISG-IPS，用于对用户的个人证书进行验证。

如果 CA 证书由第三方 CA 中心颁发：

1. 选择**系统 > 证书 > CA 证书**。
2. 点击 **CA 证书列表**上方的**导入**按钮，导入要用于 E-Key 认证的 CA 证书。

3. 点击 。

如果 CA 证书由本地 CA 中心颁发：

1. 选择**系统 > 证书 > CA 中心**。
2. 选择要使用的 CA 证书，点击列表上方的**复制到 CA 证书列表**按钮。

3. 点击 。

提示：推荐使用本地 CA 中心颁发 E-Key 用户的个人证书。个人证书的所有者字段 （**公共名**）必须是使用此证书的管理用户的用户名，以标识用户与证书的绑定关系。关于本地 CA 中心颁发证书的过程，请参见 3.28.2.2 颁发、续订和吊销证书。

3.19.2.3 启用 E-Key 认证

1. 选择**系统 > 认证 > 管理用户**，点击管理用户对应的图标，进入管理用户编辑页面。
2. 在**增强认证方式**区域，勾选 **E-Key 认证**复选框。

3. 点击**确定**。
4. 点击。

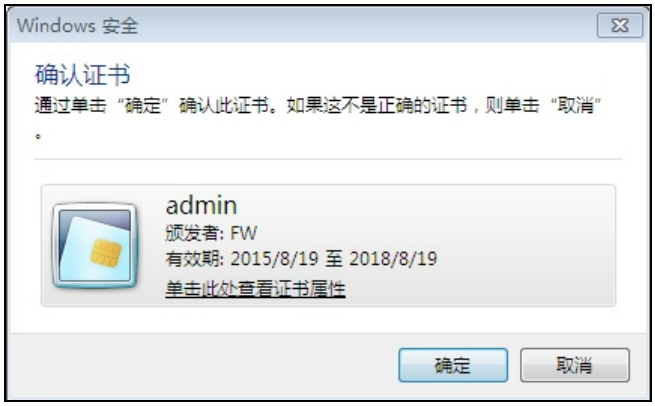
配置注意事项：

- 根管理员可以为根系统管理员启用、禁用 E-Key 认证。
- 根系统管理员可以为 Vsys 管理员启用、禁用 E-Key 认证。
- 根系统管理员也可以启用或禁用自身的 E-Key 认证状态。

3.19.2.4 使用 USB Key 登录

在 NISG-IPS 上完成 E-Key 认证配置后，启用了 E-Key 认证的管理用户可以通过以下方式进行登录：

1. 在 PC 上插入存储 E-Key 用户证书的 USB Key，打开浏览器，输入 NISG-IPS 的管理地址。
2. 选择使用的证书。



3. 在弹出的验证窗口输入 USB Key 的 PIN 码。

提示：如果不弹出验证窗口，请关闭浏览器后重新打开，输入管理地址。

4. 输入管理用户名、密码和验证码，点击**登录**。

3.20 OTP 认证

3.20.1 概述

为了解决静态口令认证方式的安全性问题， NISG-IPS 引入了 OTP 增强认证方式。即用户在登录时，需要输入 OTP 设备上显示的动态密码才可以成功登录。

提示：NISG-IPS 使用 OTP 认证的同时，保留了传统的静态口令和验证码认证，以达到多重认证效果。

本节内容包括：

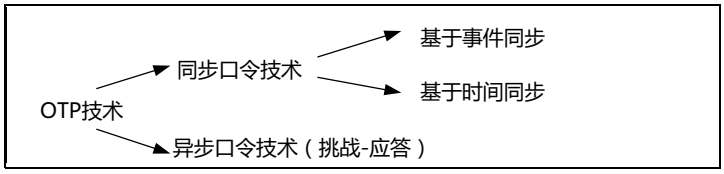
3.20.1.1 名词解释

OTP 相关名词解释：

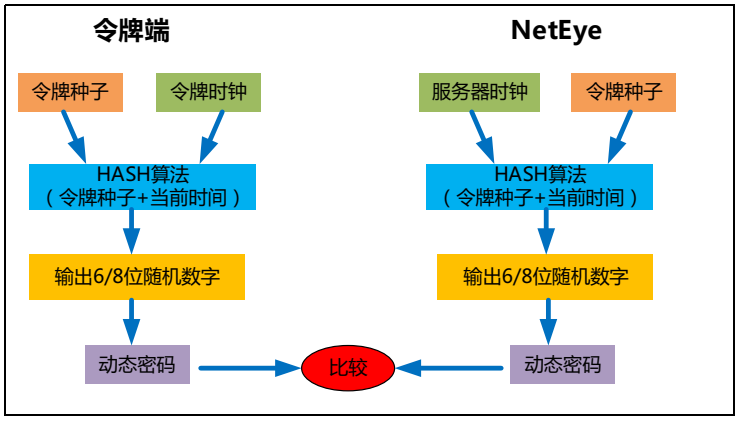
- **动态口令技术：**One-Time Password （OTP），是一种安全便捷的帐号防盗技术，根据专门的算法每隔 60 秒生成一个与时间相关的、不可预测的随机数字组合，每个口令只能使用一次。
- **动态令牌：**用于生成并显示动态口令的终端硬件或软件，供用户登录时使用。
- **令牌种子：**即令牌密钥，同时存储于令牌终端和认证服务器（NISG-IPS）中，与“时间 / 事件 / 挑战值”数据组装，通过特定算法获得当前口令。

3.20.1.2 OTP 技术

按动态口令生成方式不同， OTP 技术可分为三种类型，即基于事件同步、基于时间同步、挑战 - 应答。



NISG-IPS 采用基于时间同步的 OTP 技术：



将两端的时间及相同的种子作为输入，由特定算法运算出一致的密码。如果令牌端与服务器端 （NISG-IPS）时间存在偏差，可通过设定认证窗口，计算出认证窗口时间范围内所有可能的动态口令，只要其中有一个与传递过来的口令匹配，则认证通过。

虽然认证窗口的机制可以保证硬件令牌与服务器端存在失步时仍能认证成功，但某些极端情况下仍有可能出现严重失步 （如硬件令牌受强磁干扰等非正常情况），以致超出了认证窗口所能保证的范围。这时需要对该令牌进行时间同步操作。该操作仅在硬件令牌疑似严重失步而无法认证成功时才需执行。

基于时间同步的 OTP 技术具有较强的可靠性且易于使用，不过要求系统时钟十分精确。

3.20.1.3 动态令牌

动态令牌是生成并显示动态口令的载体。按照具体的实现方式不同，主流动态令牌通常有“硬件令牌”、“手机令牌”、“短信令牌”、“软件令牌”几种形式。

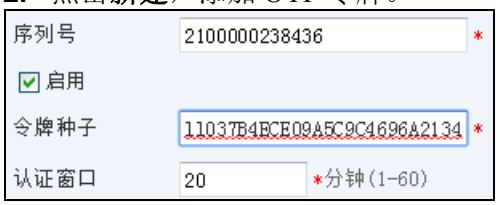
NISG-IPS 采用硬件令牌技术，该技术成熟，是目前主流的终端形式。采用相同算法（OATH 国际标准组织的 TOTP 等算法）的不同厂商令牌可以相互通用。采用硬件令牌技术，业务响应度高，认证可靠性高，无时区影响。

3.20.2 基本配置步骤

提示：NISG-IPS 的 OTP 认证目前只支持对根系统管理员及 Vsys 管理员的登录认证，仅允许根系统管理员对 OTP 令牌进行操作。

3.20.2.1 添加 OTP 令牌

1. 选择**系统 > 认证 > OTP 令牌**。
2. 点击**新建**，添加 OTP 令牌。



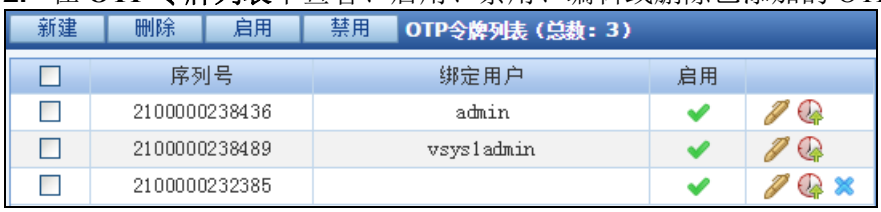
3. 点击**确定**。
4. 点击 。

配置注意事项：

- OTP 令牌的序列号即令牌硬件后端贴的条形码数值。
- 令牌种子由 OTP 硬件厂商供货时随机提供，令牌种子和令牌硬件是一一对应的。

3.20.2.2 编辑 OTP 令牌

1. 选择**系统 > 认证 > OTP 令牌**。
2. 在 **OTP 令牌列表**中查看、启用、禁用、编辑或删除已添加的 OTP 令牌。



配置注意事项：

- 若令牌被禁用，则绑定该令牌的用户登录时将不能认证成功。
- 若令牌已被绑定至某个用户，则需解除用户的绑定关系后方可删除。

- 编辑令牌时，令牌名称、令牌种子和绑定用户不可更改，令牌种子不可查看，显示为“******”。若要修改令牌绑定关系，请参见 3.20.2.3 启用 OTP 认证和绑定令牌。
- 如果 OTP 认证失败，说明令牌端和 NISG-IPS 的时间偏差过大，可以点击进行时间同步。

3.20.2.3 启用 OTP 认证和绑定令牌

1. 选择**系统 > 认证 > 管理用户**。
2. 点击管理员对应的图标，进入编辑页面。
3. 在**增强认证方式**区域，勾选 **OTP 认证**，选择绑定的 OTP 令牌。

4. 点击**确定**。
5. 点击。

配置注意事项：

- 一个管理用户只能绑定一个 OTP 令牌。
- 根管理员可以为根系统管理员启用、禁用 OTP 认证。
- 根系统管理员可以为 Vsys 管理员启用、禁用 OTP 认证。
- 根系统管理员也可以启用或禁用自身的 OTP 认证状态。

3.20.2.4 使用 OTP 令牌登录

完成 OTP 配置后，拥有 OTP 设备的管理用户即可通过 OTP 认证登录 NISG-IPS：

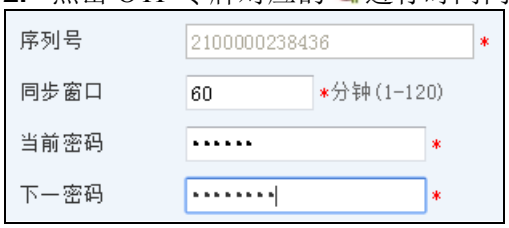
1. 在浏览器中输入 NISG-IPS 的管理地址，弹出认证界面。
2. 输入用户名、密码和验证码，出现 OTP 密码文本框。

3. 输入 OTP 设备上显示的动态密码，即可成功登录。

3.20.2.5 时间同步

如果登录时 OTP 认证失败且输入密码无误，则说明令牌端和服务器端的时间偏差过大，超出了认证窗口的范围，可以执行时间同步操作：

1. 选择**系统 > 认证 > OTP 令牌**。
2. 点击 OTP 令牌对应的进行时间同步。



3. 点击**确定**。
4. 点击。

配置注意事项：

- 进行时间同步需要设置同步窗口大小和动态认证密码 （OTP 硬件设备上连续两次显示的密码）。 OTP 设备每隔一分钟变化一次密码。
- 进行时间同步时，要求 NISG-IPS 系统时间必须准确，否则 OTP 与 NISG-IPS 时间误差过大 （超过设定的同步窗口的 1/2）会导致同步失败。

3.20.2.6 令牌挂失

如果令牌丢失，需要解除原有令牌的绑定关系，绑定新的令牌：

- 如果根系统管理员的令牌丢失，必须以根管理员 root 身份登录系统。
- 如果是 Vsys 管理员的令牌丢失，必须以根系统管理员身份登录系统。

1. 选择**系统 > 认证 > OTP 令牌**。
2. 在 **OTP 令牌列表**中禁用丢失的 OTP 令牌。
3. 选择**系统 > 认证 > 管理用户**。进入编辑页面绑定新的令牌。
4. 点击**确定**。
5. 点击。

表 56 OTP 令牌命令

show otp-token	显示指定 OTP 令牌的相关信息或所有 OTP 令牌的信息。
otp-token key authwnd	添加 OTP 令牌，或编辑指定 OTP 令牌的令牌种子和认证窗口大小。
otp-token sync syncwnd password1 password2	为指定 OTP 令牌设置同步窗口大小和动态口令。
otp-token enable, disable	启用或禁用指定的 OTP 令牌。
unset otp-token	删除指定 OTP 令牌的相关信息或删除所有 OTP 令牌。

3.20.3 配置参数说明

表 57 OTP 令牌配置参数

参数	说明
序列号	OTP 令牌的唯一标识，即每一个令牌硬件后端贴的条形码数值。
启用	启用或禁用 OTP 令牌。
令牌种子	即令牌密钥。长度 1-512 字节，只能由字母和数字组成。
认证窗口	进行 OTP 认证时，允许出现的时间误差。范围 1-60 分钟，默认 20 分钟。 默认值 20 代表在当前时间点的前后 10 分钟内计算出所有口令，只要其中有一个与来自客户端的口令匹配，则认证通过。其值不宜过大，否则会加重 NISG-IPS 负担。
绑定用户	绑定该令牌的管理用户名称。
	点击该图标对 OTP 令牌进行时间同步。需要设置如下信息： • **同步窗口**：进行时间同步允许的时钟误差。范围 1-120 分钟，默认 60 分钟。 默认值 60 表示只有当令牌时间与服务器端当前时间差在 30 分钟内，才可以同步成功。 • **当前密码**：输入令牌终端上显示的当前动态口令， 6 个数字字符 （0-9），不可为空。 • **下一个密码**：输入令牌终端上显示的下一个动态口令， 6 个数字字符 （0-9）。

3.21 备份恢复

3.21.1 概述

NISG-IPS 支持对除系统日志、诊断文件和 License 文件之外的系统配置文件进行备份。

- 备份系统配置

  管理员应定期对 NISG-IPS 系统配置进行备份。

- 管理备份文件

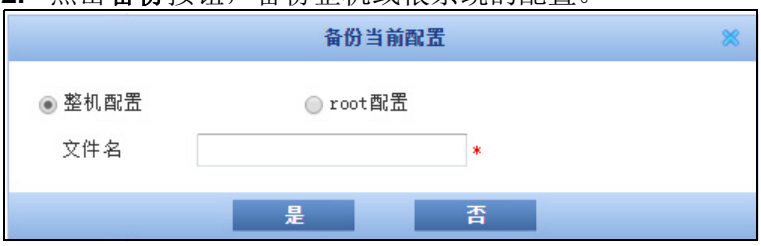
  管理员可以查看、删除和下载系统备份文件，也可以将备份文件复制到本地存储介质上（仅在 CLI 下支持此操作）。一个 Vsys 的备份文件不能被复制到另一 Vsys。

- 恢复系统配置

  管理员可以通过保存在本地或远程主机上的备份文件进行系统恢复。远程恢复时，远程主机上的备份文件会被临时上载到本地。系统恢复结束后，该备份文件将被自动删除。

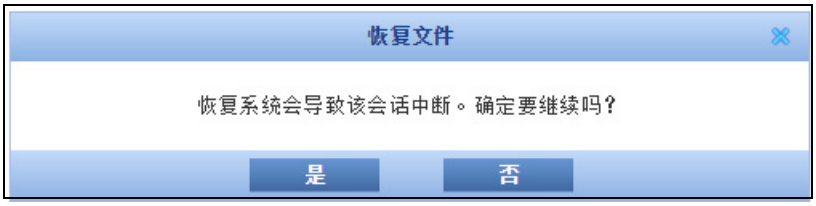
3.21.2 基本配置步骤

1. 选择**系统** > **维护** > **备份 / 恢复**。
2. 点击**备份**按钮，备份整机或根系统的配置。

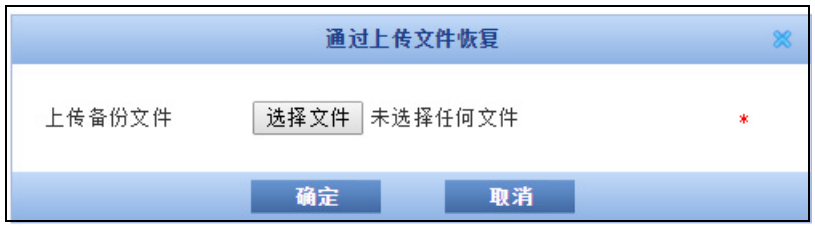


3. 点击 下载备份文件或点击 删除备份文件。

4. 点击 通过本地备份文件恢复系统配置。



5. 点击**通过上传文件恢复**按钮，上传文件恢复系统配置。



6. 点击**确定**。
7. 点击 。

配置注意事项

- 备份文件名由字母、数字和下划线组成，并且不能以下划线开头。文件名的长度范围是 1-128 字节。备份文件名称不能重复。
- 根系统最多支持 5 个整机配置备份文件和 5 个根系统配置备份文件，每虚拟系统最多支持 5 个备份文件。
- 只有根系统管理员和 Vsys 管理员才能备份系统。根系统管理员可以备份根系统和整机的配置信息，而 Vsys 管理员只能备份其所登录管理的 Vsys 的配置信息。

表 58 备份恢复命令

backup	备份系统配置。
copy backup	下载系统备份文件。
delete backup	删除备份文件。
restore from internal	用本地保存备份文件恢复系统。
restore from	通过上载备份文件恢复系统。

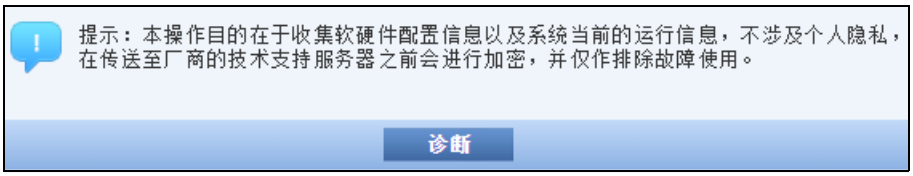
3.22 技术支持

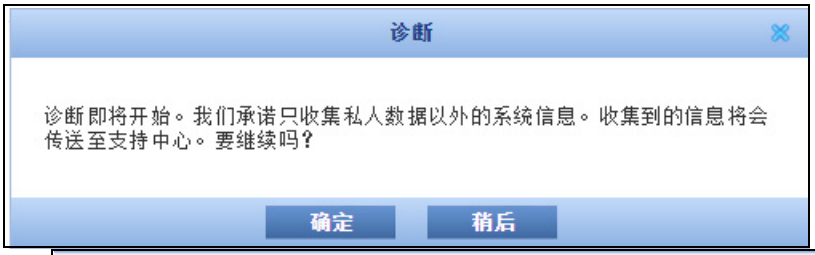
3.22.1 概述

管理员可以通过一键式操作，方便地将诊断文件发送给 NISG-IPS 的技术支持中心，尽快地解决问题。诊断信息的内容包括配置文件信息、系统状态信息、事件日志信息等。诊断文件保存在 NISG-IPS 上，可以查看、删除或下载。当生成新的诊断文件时，旧文件会被覆盖。

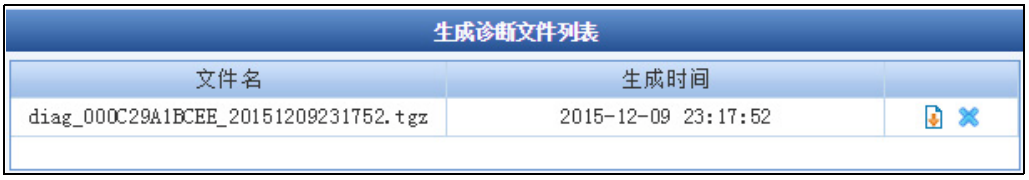
3.22.2 基本配置步骤

1. 选择**系统** > **维护** > **技术支持**，进入**技术支持**页面。
2. 点击**诊断**按钮，开启诊断功能。





3. 查看、删除或下载生成的诊断文件。



4. 点击 。

3.23 诊断工具

3.23.1 概述

NISG-IPS 提供以下诊断工具：

- **Ping/Ping6**：测试 NISG-IPS 与远程主机之间的连通性。
- **Traceroute**：探测数据包在传输过程中所经过的路径。
- **Nslookup**：诊断和排查 DNS 系统故障。
- **Tcpdump**：截获数据包头用于网络问题分析。

为了方便管理员进行远程调试， NISG-IPS 支持：

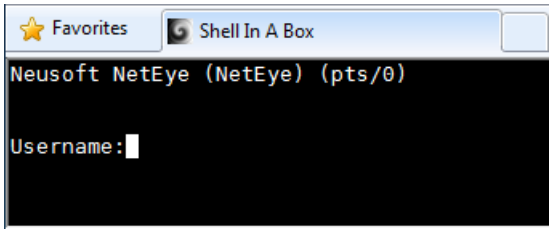
- 通过 WebShell 执行 Ping/Ping6、 Traceroute 和 Nslookup 命令。
- 通过 WebUI 执行 Tcpdump 诊断命令。

3.23.2 基本配置步骤

3.23.2.1 通过 WebShell 执行诊断命令

通过 WebShell （CLI）执行 Ping、 Traceroute 和 Nslookup 诊断命令：

1. 点击页面右上方的 WebShell 快捷菜单，打开 WebShell 窗口。

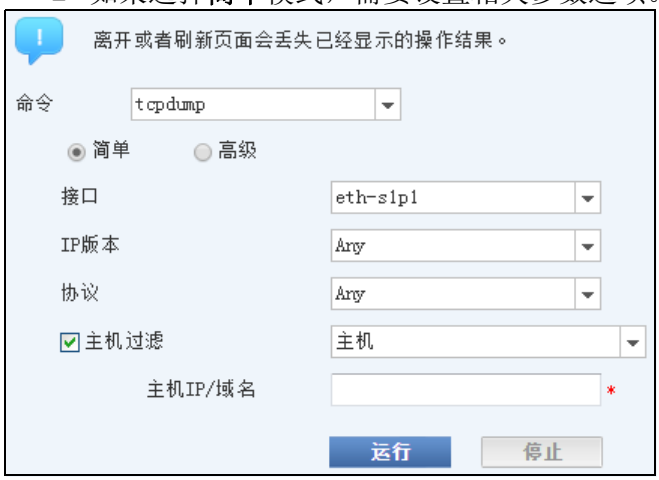


2. 输入管理用户名和密码登录 CLI。
3. 执行 Ping/Ping6、 Traceroute 或 Nslookup 命令。

3.23.2.2 通过 WebUI 执行诊断命令

通过 WebUI 执行 Tcpdump 命令：

1. 选择**系统 > 维护 > 诊断工具**。
2. 从**命令**下拉列表中选择 tcpdump 命令并配置相关参数。
   - 如果选择**简单**模式，需要设置相关参数选项。



   - **接口**：选择一个三层以太网接口，截获经过此接口的数据包。
   - **IP 版本**：用于区分 IPv4 和 IPv6 协议。选择 Any 时代表不区分 IPv4 和 IPv6。
   - **协议**：指定要抓取数据包使用的协议，包括 TCP、UDP、ICMP、ARP、RARP 和 Any。 Any 表示所有协议。
   - **端口过滤**：选择 TCP 或 UDP 协议时，可以选择设置端口过滤条件。端口过滤条件包括：
     - **端口**：抓取源或目的端口为指定端口号的数据包。
     - **源端口**：抓取源端口为指定端口号的数据包。
     - **目的端口**：抓取目的端口为指定端口号的数据包。
   - **主机过滤**：选择一种主机过滤条件并指定主机 IP 地址或域名。主机过滤条件包括：
     - **主机**：抓取源或目的为指定主机 IP 或域名的数据包。
     - **源主机**：抓取源主机为指定主机 IP 或域名的数据包。
     - **目标主机**：抓取目的主机为指定主机 IP 或域名的数据包。
     - **源主机和目标主机**：抓取源主机为指定源主机 IP/ 域名并且目的主机为指定目的主机 IP/ 域名的数据包。
     - **源主机或目标主机**：抓取源主机为指定源主机 IP/ 域名或者目的主机为指定目的主机 IP/ 域名的数据包。
     - **主机和主机**：抓取指定的两个主机之间的双向数据包。

- 如果选择**高级**模式，只需要在**命令行**文本框中输入 tcpdump 和相关命令参数即可。

提示：系统自动添加 -w 参数并将抓取数据保存在一个 pcap 文件中，所以无需指定 -w 和 -C 参数。

3. 点击**运行**按钮开始执行命令。

   结果区域显示正在抓包且命令执行结果将保存在一个 pcap 文件中的提示信息。

4. 点击**停止**按钮并在**结果**区域点击链接下载输出结果。抓取的数据信息保存在一个 pcap 文件中，并打包为一个 zip 压缩文件。

配置注意事项：

- 根管理员、根系统管理员和审计员无需获得配置锁即可使用诊断工具。
- 在 WebUI 上，诊断工具不能和技术支持功能同时使用。当进行技术支持诊断操作时，所有正在运行的诊断命令都将被终止，并且诊断结果将丢失。
- 在 WebUI 上，当管理员离开或刷新页面时，系统将终止正在执行的诊断命令，且执行的诊断命令结果将丢失。
- 在一个 Web 界面中，同一时间只能执行一个诊断命令。如果管理员需要同时执行多个命令，需要打开多个 Web 页面。管理员最多可以同时执行五个诊断命令。

表 59 诊断命令

ping {*host_name* | *ipv4_address*} [*num*]	检查 NISG-IPS 与目的 IPv4 地址之间是否连通。
ping6 {*host_name* | *ipv6_address* [**interface** *interface_name*]} [*num*]	检查 NISG-IPS 与目的 IPv6 地址之间是否连通。
traceroute {*ipv4_address* | *domain name*}	探测到达路由器或服务器的路径。
nslookup {*domain_name*} [*dns_server_address*]	将域名解析为 IP 地址。

3.23.3 配置参数说明

表 60 Tcpdump 诊断命令配置信息

参数	描述
命令	选择执行的诊断命令。
类型	为不同的用户提供不同的配置方式： • **简单**：为不熟悉命令行的初级管理用户提供。管理用户可通过 WebUI 选取命令和相关参数，执行诊断命令。 选取 tcpdump 诊断命令和简单模式后，管理员需要设置监听接口、 IP 版本、协议、端口过滤、主机过滤等参数。 • **高级**：为熟悉命令行配置参数的高级管理用户提供。管理用户可直接输入诊断命令和相关参数。命令行参数同 Linux 下的命令行参数一致。
运行 / 停止	点击按钮开始或终止执行诊断命令。
结果	显示诊断命令执行状态并提供输出结果。

3.24 调试工具

管理员可使用 NISG-IPS 提供的调试 （Debug）工具对数据包包进行监听和跟踪。

3.24.1 通用 Debug

下表给出通用 Debug 的相关命令：

- 基本命令：如 **show debug**、 **debug clear** 等。
- **debug dump hook**：通过此命令设置监听对象。
- **debug match**：通过此命令设置匹配条件监听指定数据包。
- **debug dump**：通过此命令设置诊断信息的输出条件。

表 61 Debug 命令

show debug	查看 Debug 配置信息。
debug start *time* [*file_name*]	设置监听数据包时长 （3-14400 秒）。
debug stop	停止监听数据包。
debug file remove [*file_name*]	删除 Debug 文件。
debug file download	下载 Debug 文件。
debug clear	停止 Dump 并重置监听匹配条件。
debug dump hook all	监听所有数据包。
debug dump hook dnat	监听执行过 DNAT 的数据包。
debug dump hook error	监听传输中出错的数据包。
debug dump hook input	监听接收的数据包。
debug dump hook input_error	监听接收的数据包和出错的数据包。
debug dump hook input_output	监听接收和成功发送的数据包。
debug dump hook output	监听成功发送的数据包。
debug dump hook output_error	监听发送的数据包和出错的数据包。
debug dump hook policy	监听匹配策略的数据包。
debug dump hook route	监听匹配路由的数据包。
debug dump hook snat	监听执行过 SNAT 的数据包。
debug match **bidir**	设置是否进行双向监听。
debug match **input**	设置入口接口，包括任意接口、以太网通道、以太网接口、本地接口、 PPPoE 接口、冗余接口及 VLAN 接口。
debug match ip	设置源和目的 IP 地址。此地址可以为 IPv4 或 IPv6 地址。
debug match mac	设置源和目的 MAC 地址。
debug match output	设置出口接口，包括任意接口、以太网通道、以太网接口、本地接口、 PPPoE 接口、冗余接口及 VLAN 接口。

表 61 Debug 命令 (*续*)

debug match port	设置源和目的端口。
debug match protocol	设置协议类型，包括指定协议号、任意协议、 ARP、 ICMP、 ICMPv6、 TCP 及 UDP。
debug match tunnel	设置 VPN 隧道。
debug dump bytes	设置单个数据包内容的最大输出字节数。
debug dump session	设置是否输出会话信息。
debug dump complex	设置是否输出数据包包头的详细标记信息。

3.24.2 VPN Debug

开启 VPN Debug 对指定或所有自动密钥隧道进行调试。

输出的调试信息包含以下数据：

- 协商结果和协商状态
- 当前信息所属隧道
- 协商包的每个字段的信息

表 62 VPN Debug 命令

show debug vpn [**all-tty**]	查看当前或所有终端的 VPN Debug 配置信息。
unset debug vpn [**all-tty**]	取消输出当前或所有终端的 VPN Debug 信息。
debug vpn ipsec *timeout*	输出 IPSec Debug 信息
debug vpn isakmp [**peerip** *ip_address* | **tunnel** *tunnel_name*] {**error** | **basic** | **detail**}	输出不同级别的 ISAKMP Debug 信息。
unset debug vpn isakmp [**peerip** *ip_addr*ess | **tunnel** *tunnel_name*]	取消输出 ISAKMP Debug 信息。
debug vpn l2tp	输出所有隧道的 L2TP Debug 信息。
unset debug vpn l2tp	取消输出隧道的 L2TP Debug 信息。
debug sslvpn {**on** | **off**}	输出或取消输出 SSL VPN Debug 信息。

3.24.3 PPPoE Debug

管理员可以通过相关命令设置和查看 PPPoE Debug 的相关信息。

表 63 PPPoE Debug 命令

show debug pppoe [all-tty]	查看 PPPoE Debug 配置信息。
debug pppoe	输出 PPPoE Debug 信息。
unset debug pppoe [**all-tty**]	取消输出 PPPoE Debug 信息。
show debug pppoev6 [**all-tty**]	查看 PPPoEv6 Debug 配置信息。
debug pppoev6	输出 PPPoEv6 Debug 信息。
unset debug pppoev6 [**all-tty**]	取消输出 PPPoEv6 Debug 信息。

3.25 集中管理

3.25.1 概述

集中管理系统提供对网络安全产品的集中管理，对被管理设备提供报警、监控、日志和报表等功能。 NISG-IPS 支持集中管理服务器的管理，但一台 NISG-IPS 设备同时只能接受一台服务器的管理。 NISG-IPS 上不上载任何 License 时也能够接受集中管理服务器的管理。

NISG-IPS 上开启允许集中管理后，会对向其发出管理请求的集中管理服务器进行认证，通过认证的服务器才能对 NISG-IPS 进行管理。集中管理服务器进行管理后，可以配置系统，但需要临时抢占配置锁。配置完成后，会自动释放配置锁。

3.25.2 基本配置步骤

1. 选择**系统** > **维护** > **集中管理**，进入**集中管理**页面。
2. 开启集中管理服务器管理功能。

3. 点击**确定**。
4. 点击 。

3.26 报警配置

3.26.1 概述

当有事件发生时， NISG-IPS 会检查报警策略，如果匹配了报警策略，那么 NISG-IPS 将根据管理员设置以简体中文或英语生成日志，并将日志发送到对应的服务器。

NISG-IPS 支持如下报警策略：

- 本地日志报警策略

  NISG-IPS 缺省提供了名称为 “internal” 的本地日志类型的报警策略。管理员可以查看和编辑缺省策略，但不能删除。

- Syslog 报警策略

  NISG-IPS 将系统日志信息发送到远程 Syslog 服务器。

- 邮件报警策略

  NISG-IPS 可以采用电子邮件方式将报警信息通过邮件服务器发送给指定的邮件地址。

- SNMP Trap 报警策略

  NISG-IPS 可以利用 SNMP Trap 方式，将系统日志发送给 SNMP 服务器。也支持向多个 SNMP Trap 服务器发送日志信息。 SNMP Trap 中有两个协议版本， v1 和 v2c。

- 终端输出报警策略

提示：Syslog 报警策略、电子邮件报警策略和 SNMP Trap 报警策略，每种策略最多支持 15 条。

3.26.2 基本配置步骤

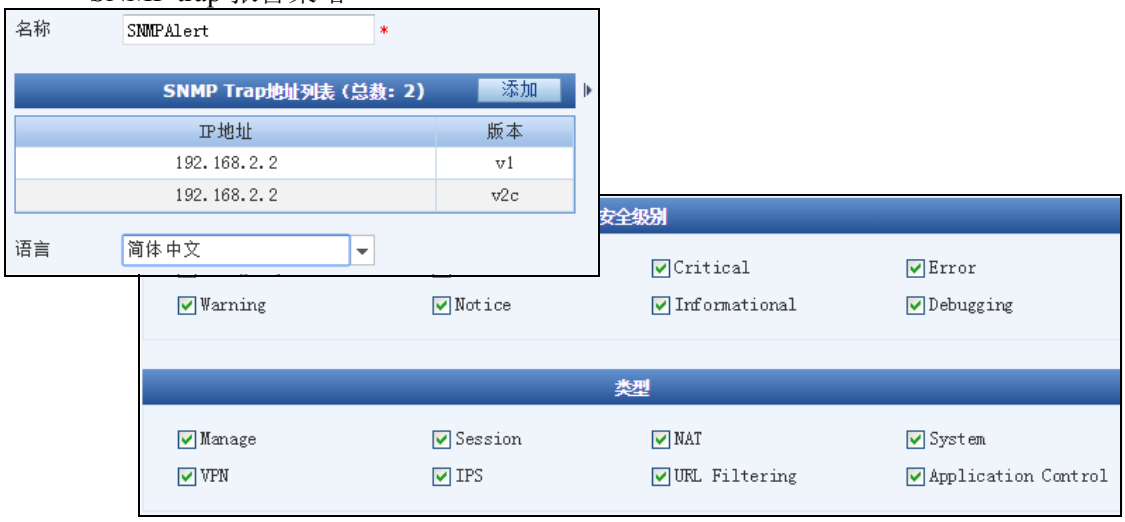
1. 选择**系统** > **日志配置** > **报警配置**。
2. 查看或删除报警策略。

3. 编辑本地日志报警策略。

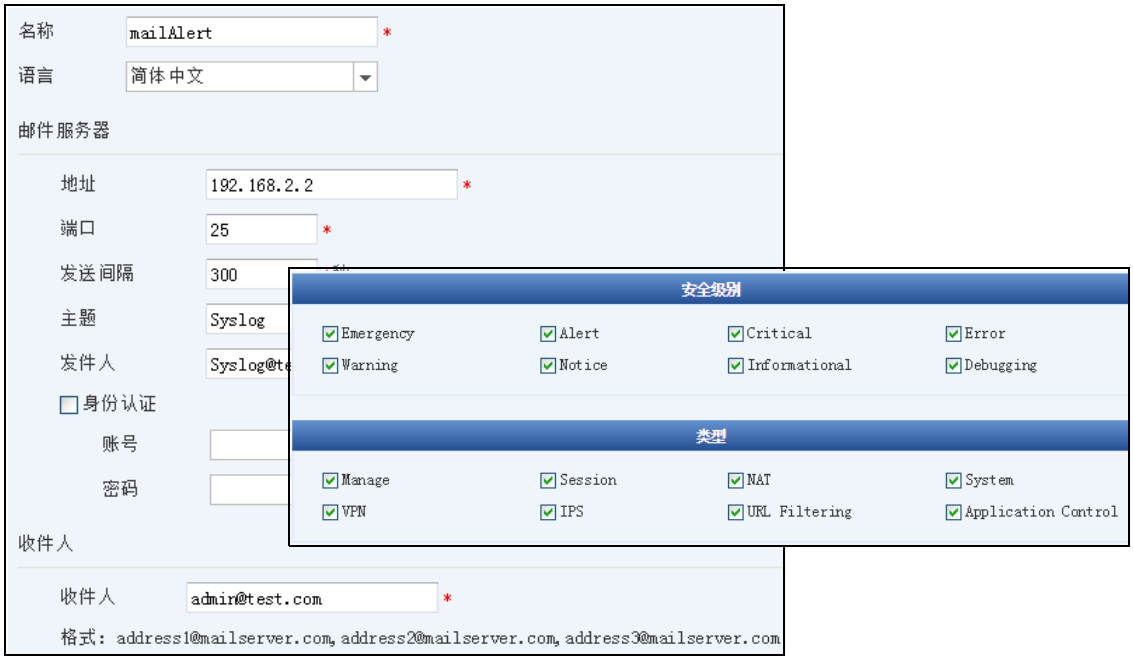
4. 创建或编辑报警策略：

- Syslog 报警策略

- SNMP trap 报警策略



- 邮件报警策略



5. 点击**确定**。
6. 点击 。

表 64 报警策略命令

show alert-config	查看报警策略。
alert-config local-syslog | syslog | snmp-trap | mail	编辑本地日志报警策略或创建 Syslog、SNMP Trap 或邮件报警策略。
unset alert-config syslog | snmp-trap | mail	删除 Syslog、 SNMP Trap 或邮件报警策略。

3.26.3 配置参数说明

表 65 本地日志报警策略配置信息

参数	说明
名称	本地日志报警策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。
存储介质	系统日志的存储介质，不允许切换存储介质。
日志存储区已满时	设置日志存储策略，覆盖或停止产生日志。
安全级别	系统日志输出事件的安全级别，包括 Emergency、 Alert、 Critical、 Error、 Warning、 Notice、 Informational 和 Debugging。
类型	系统日志的来源类型，包括 Manage、 Session、 NAT、 System、 VPN、 IPS、 URL Filtering 和 Application Control。

表 66 Syslog 报警策略配置信息

参数	说明
名称	Syslog 报警策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。
Syslog 服务器	设置 Syslog 服务器 IP 地址和端口： • **IP 地址**：取值范围为 [0-223].[0-255].[0-255].[0-255]。 • **端口**：取值范围为 1-65535。
输出方式	日志输出到 Syslog 服务器的方式： • **完整输出**：将整条系统日志完整地输出，包括事件头和事件内容。输出格式： <pri> 月份 + 日期 + 时间 + 主机名：虚拟系统名 + 事件库版本 - 语言标识 - 模块 ID - 事件 ID + 日志等级 + 模块类型 + 用户名 + rep= 重复次数 | 消息体 • **精简输出**：将系统日志部分地输出。输出格式： <pri> 月份 + 日期 时间 + 主机名：虚拟系统名 + 事件库版本 - 语言标识 - 模块 ID - 事件 ID + 日志等级 + 模块类型
语言	日志输出语言，简体中文或英语。
安全级别	系统日志输出事件的安全级别。
类型	系统日志的来源类型。

表 67 邮件报警策略配置信息

参数	说明
名称	邮件报警策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #。
语言	日志输出语言，简体中文或英语。
邮件服务器	设置接收邮件的邮件服务器： • **地址**：IP 地址或域名。 IP 地址的范围为 [0-255].[0-255].[0-255].[0-255]。域名长度范围为 2-255 字节。 • **端口**：1-65535。 • **发送间隔**：取值范围为 1-2678400 秒。 • **主题**：0-64 字节， UTF-8 字符。不能包含空格和以下字符：? ' \ 。NISG-IPS 以邮件形式发送系统日志时，会在邮件主题前添加产品序列号。 • **发件人**：NISG-IPS 用于发送邮件的邮件地址。 • **身份认证**：邮件服务器对邮件发送者进行身份验证。当启用身份验证时必须设置账号及密码。密码长度为 1-255 字节。
收件人	接收报警信息的邮件地址，最多添加 10 个邮件地址。多个地址以逗号分隔。
安全级别	系统日志输出事件的安全级别。
类型	系统日志的来源类型。

表 68 SNMP Trap 报警策略配置信息

参数	说明
名称	SNMP Trap 报警策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #。
SNMP Trap 地址	设置 SNMP Trap 地址： • **IP 地址**：接收 SNMP Trap 格式日志的 SNMP 服务器 IP 地址。范围为 [0-223].[0-255].[0-255].[0-255]。 • **版本**：SNMP 服务器接收 SNMP 的版本号， v1 和 v2c。
语言	日志输出语言，简体中文或英语。
安全级别	系统日志输出事件的安全级别。
类型	系统日志的来源类型。

3.27 日志维护

3.27.1 概述

当有事件发生时， NISG-IPS 会根据报警策略生成日志。当日志文件大小超过存储空间时， NISG-IPS 会覆盖产生时间最早的日志文件或停止产生新日志。

不同报警策略类型的日志输出格式如表 69 所示：

表 69 报警策略的日志输出格式

策略类型	日志输出格式
本地日志	输出格式： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型 用户名 rep= 重复次数 | 消息体** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage N/A rep=1| 管理用户 root 通过 Web 登录成功， IP 为 10.2.1.119。
Syslog	Syslog 报警策略包含两种系统日志输出格式： • **完整输出**：将整条系统日志完整地输出： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型 用户名 rep= 重复次数 | 消息体** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage N/A rep=1| 管理用户 root 通过 Web 端登录成功， IP 为 10.2.1.119。 • **精简输出**：将整条系统日志部分地输出 （不包含日志的重复次数和消息体部分）： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage
邮件	输出格式： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型 用户名 rep= 重复次数 | 消息体** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage N/A rep=1| 管理用户 root 通过 Web 登录成功， IP 为 10.2.1.119。 报警邮件的邮件名格式： [syslog] + MAC + 用户自定义主题 示例：当 MAC 地址为 000C29FB8FF0 的 NISG-IPS 设备发送一封自定义主题为 test 的系统日志报警邮件时，邮件主题为： [syslog]000C29FB8FF0test
SNMP Trap	输出格式： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型 用户名 rep= 重复次数 | 消息体** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage N/A rep=1| 管理用户 root 通过 Web 登录成功， IP 为 10.2.1.119。

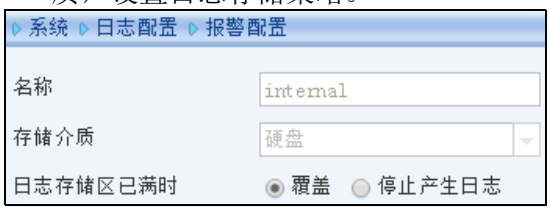
3.27.2 基本配置步骤

3.27.2.1 切换日志存储介质

只有硬盘才能存储日志信息。系统默认只有 Flash 卡，不能存储日志。如果挂载了硬盘，可以格式化硬盘后，切换存储介质为硬盘，进行日志存储。

如果设备选配自带硬盘，则系统日志可以直接存储在硬盘中。

1. 选择**系统** > **日志配置** > **报警配置**。
2. 点击缺省的本地日志报警策略 “internal” 所对应的，进入编辑页面，切换存储介质，设置日志存储策略。



3. 点击**确定**。
4. 点击。
5. 选择**系统** > **日志配置** > **日志维护**，查看日志存储介质的使用情况。

3.27.2.2 下载日志文件

1. 选择**系统** > **日志配置** > **日志维护**。
2. 在**下载日志文件**区域，设置日志生成时间范围，点击**压缩**按钮，压缩完成后点击**导出**按钮，将指定时间段内生成的日志信息下载到本地进行查看。

3.27.2.3 导出日志到 USB 设备

1. 选择**系统** > **日志配置** > **日志维护**。
2. 在 **USB** 区域，设置日志生成时间范围，点击**导出**按钮，导出日志到 USB 设备。导出完成后，点击**结束**。

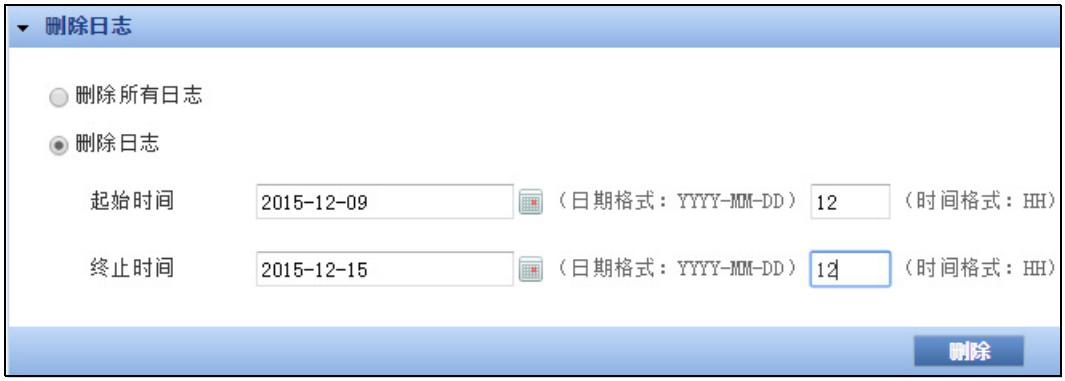
如果 USB 的文件系统无法识别，系统会提示先进行格式化。

3. 管理员可以对导出的日志信息进行加密。启用加密功能后，需要输入密码，长度 6-64 字节。

提示：日志导出到 USB 设备过程中请不要重启或关闭系统。

3.27.2.4 删除日志信息

1. 选择**系统** > **日志配置** > **日志维护**。
2. 在**删除日志**区域，点击**删除所有日志**删除全部日志信息，或设置日志生成时间范围并点击**删除**按钮，删除指定时间段内生成的日志信息。



3. 点击 。

表 70 系统日志命令

logging media	切换日志存储介质。
logging policy	设置系统日志存储策略。
delete log all,time	删除系统日志。

3.27.3 配置参数说明

表 71 系统日志参数信息

参数	说明
优先级	日志信息的优先级。
日期时间	系统日志产生的时间。 显示格式为：**YYYY-MM-DD hh:mm:ss**
Vsys 和主机名	产生系统日志的 NISG-IPS 的主机名及 Vsys。 显示格式为：**主机名 :Vsys 名称** 示例： 如主机名是 henry， Vsys 是根系统 (root)，即为：henry:root。
基本信息	系统日志的基本信息，包括事件库版本、语言标识、模块 ID、事件 ID。 显示格式为： **事件库版本 - 语言标识 - 模块 ID- 事件 ID** • 事件库 （主）版本为两字节整数，当前事件库主版本号为 03。 • 语言标识为两字节整数， 01 代表简体中文， 02 代表英文。 • 模块 ID 为两字节整数。 • 事件 ID 为四字节整数。
级别	系统日志的安全级别： • **Emergency**：代表内存不足或者电源、 CPU 等硬件异常情况。该级别 ID 为 0。 • **Alert**：代表根据当前的情形需要立即做出响应的事件。如，攻击防御部分收到攻击包或 IP 分片中收到了类似的攻击包。该级别 ID 为 1。 • **Critical**：代表影响设备功能的条件信息，如拔插网线、启用 / 禁用网卡。该级别 ID 为 2。 • **Error**：代表所有添加、删除、修改动作失败的信息，包重组失败信息以及所有的匹配策略失败的错误信息。该级别 ID 为 3。 • **Warning**：代表可能影响系统功能的条件信息。如，连接邮件服务器失败或者认证失败、超时。该级别 ID 为 4。 • **Notice**：代表对普通事件的通告。如，由管理员进行添加、删除和修改操作的成功信息。该级别 ID 为 5。 • **Informational**：代表系统操作的通用信息。该级别 ID 为 6。 • **Debugging**：代表与调试相关的信息。该级别 ID 为 7。
类型	产生系统日志的模块类型，包括 Manage （管理）、 System （系统）、 Session （会话）、 NAT （地址转换）、 VPN （虚拟专用网）、 IPS （入侵防御系统）、 URL Filtering （URL 过滤）和 Application Control （应用控制）。
用户	触发系统日志产生的用户名称 （包括管理用户、网络用户、系统自身）。
重复次数	系统日志的重复次数。 NISG-IPS 可以对一定时间内内容重复的系统日志进行合并，以标明重复次数的方式提醒管理员注意。
日志信息	系统日志的主体部分，具体介绍发生了什么。内容包括系统日志的主体描述和参数等。

3.28 证书

3.28.1 概述

数字证书是一个经证书授权中心 （Certificate Authority， CA）数字签名的文件，包含公开密钥拥有者信息以及公开密钥。

在 NISG-IPS 中，管理员可以创建本地 CA 中心并通过本地 CA 中心申请、颁发和吊销证书，也可以直接导入由第三方颁发的证书。

3.28.1.1 CA 中心

NISG-IPS 可作为本地 CA 中心颁发和管理证书。

- 本地 CA 中心

  本地 CA 中心分为根 CA 中心和从属 CA 中心两种。 NISG-IPS 最多支持三级 CA 中心：根 CA 中心、二级从属 CA 中心、三级从属 CA 中心。根 CA 中心为二级从属 CA 中心颁发 CA 证书，二级从属 CA 中心为三级从属 CA 中心颁发 CA 证书。上一级 CA 中心是下一级 CA 中心的父 CA 中心。

  根系统下最多允许创建 8 个 CA 中心，每个虚拟系统仅允许创建一个 CA 中心。

- 证书管理

  CA 中心颁发的证书包括从属 CA 证书和个人 / 服务器证书。管理员可对本地 CA 中心颁发的证书进行管理 （包括吊销、续订、复制、删除、导出等操作）。

  从属 CA 证书可用于验证其 CA 中心颁发的个人 / 服务器证书是否合法，也可用于创建本地从属 CA 中心。从属 CA 证书可复制到 NISG-IPS 的 CA 证书列表，用于 NISG-IPS 与对端设备通信时验证对端身份。

  个人 / 服务器证书用于验证证书持有者的身份。个人 / 服务器证书可复制到 NISG-IPS 的本地证书列表，用于 NISG-IPS 与对端通信时证明 NISG-IPS 本端的身份，或发送给证书申请者，用于验证证书申请者的身份。

3.28.1.2 NISG-IPS 证书管理

NISG-IPS 与对端设备通信时所使用的证书称为 NISG-IPS 证书，需要事先申请并存储在 NISG-IPS 本地。 NISG-IPS 证书分为本地证书和 CA 证书。管理员可以管理 （导入、查看、删除等） NISG-IPS 本地证书和 CA 证书，并查询证书状态。

- 本地证书

  本地证书用于 NISG-IPS 与对端通讯时证明本端身份或加解密通讯数据：

  - 在 IPSec VPN 协商过程中，用于本端身份认证。
  - 在 SSL VPN 通讯过程中，用于加解密隧道数据。

- 在 SSL 检测过程中，用于加解密 SSL 数据或颁发仿冒证书。
- 在 HTTPS （WebUI）管理过程中，用于加密管理通讯数据。

NISG-IPS 的本地证书可以通过本地 CA 中心签发，也可以由第三方 CA 中心签发。

- 本地 CA 中心颁发的个人 / 服务器证书，可以直接复制到 NISG-IPS 本地证书列表，作为本地证书使用。
- 要向第三方 CA 中心申请本地证书，必须先创建证书请求文件，然后通过手动或自动方式获取本地证书。
  - 手动获取本地证书

    保存生成的证书请求文件到本地，联系 CA，获取本地证书。
  - 自动获取本地证书

    NISG-IPS 支持简单证书注册协议 （SCEP），通过与 SCEP 服务器进行交互，实现证书自动注册和自动更新。启用证书自动更新功能后， NISG-IPS 会在证书过期之前的指定时间内，向 CA 服务器发出证书自动更新请求。

- CA 证书

  CA 证书用于检查证书持有者身份的合法性。 NISG-IPS 的 CA 证书用于 NISG-IPS 与对端通讯时验证对端身份：

  - 在 IPSec VPN 协商过程中，用于对隧道对端的证书进行身份验证。
  - 在 LDAP 认证过程中，用于验证对端 LDAP 服务器的证书。

  NISG-IPS 的 CA 证书可以通过本地 CA 中心签发，也可以由第三方 CA 中心签发。本地 CA 中心颁发的 CA 证书，可以直接复制到 NISG-IPS 本地的 CA 证书列表。第三方 CA 中心签发的 CA 证书，需要手动导入本地 CA 证书列表。

- 证书撤销状态查询

  NISG-IPS 支持以下两种方法验证 NISG-IPS 证书的有效性：

  - 证书吊销列表 (CRL)

    CRL 列表中包含 CA 签发的所有无效或已过期的证书。
  - 在线证书状态协议 (OCSP)

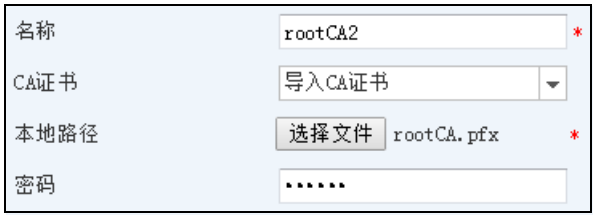
    NISG-IPS 使用 OCSP 验证证书有效性时，作为 OCSP 客户端，向 OCSP 服务器发送验证请求，当 OCSP 服务器收到请求后，将确认证书的状态，并向 NISG-IPS 返回证书状态信息。

3.28.2 基本配置步骤

3.28.2.1 配置本地 CA 中心

1. 选择**系统 > 证书 > CA 中心**。
2. 点击**新建**，选择**根 CA**，创建根 CA 中心。
   - 在**CA 证书**下拉框中选择**生成根 CA 证书**，直接生成自签名的根 CA 证书。此时需要配置证书有效期、证书信息和密钥对。

   - 在 **CA 证书**下拉框中选择**导入 CA 证书**，导入 pfx 格式的根 CA 证书。

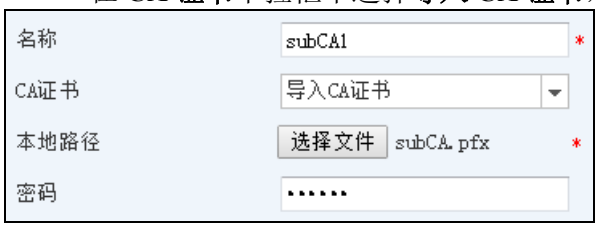


提示：新建 CA 中心或导入 CA 证书时，证书主题不能与已有证书主题相同。

3. 点击**新建**，选择**从属 CA**，创建从属 CA 中心。

   - 可以通过导入 CA 证书的方式创建从属 CA 中心。

     在 **CA 证书**下拉框中选择**导入 CA 证书**，导入 pfx 格式的从属 CA 证书。

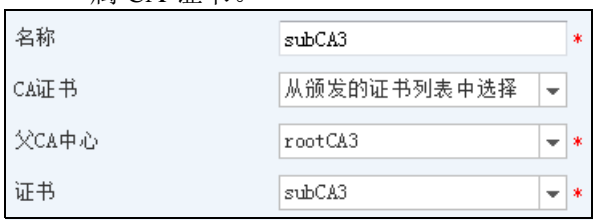


   - 如果本地已经存在父CA中心，可以由父CA中心直接颁发一个从属CA证书用于创建从属 CA 中心。

     在 **CA 证书**下拉框中选择**本地 CA 中心颁发**，选择对应的父 CA 中心，配置证书有效期、证书信息、密钥对。

   - 如果本地已经存在父CA中心，并且父CA中心已经颁发了从属CA证书，可以从父 CA 中心已经颁发的从属 CA 证书中选择一个证书用于创建从属 CA 中心。

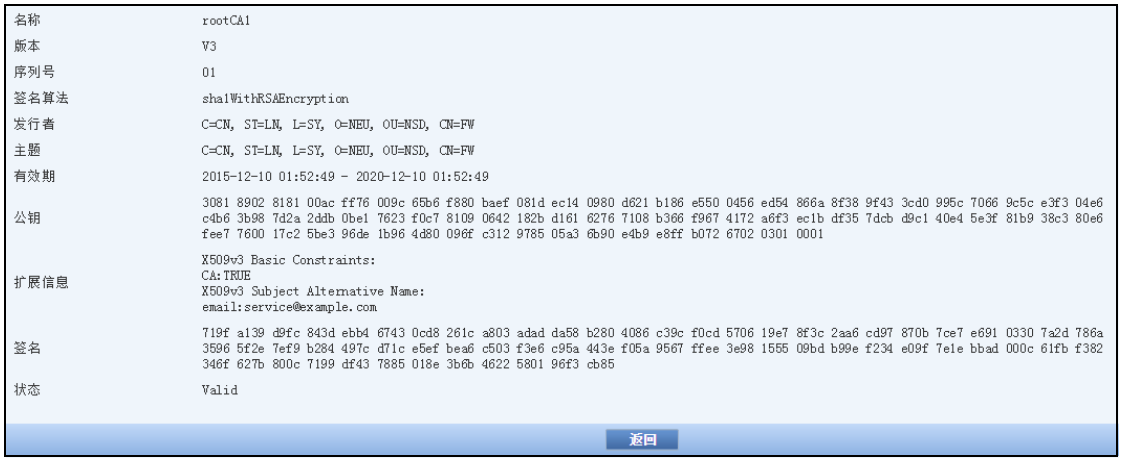
     在 **CA 证书**下拉框中选择**从颁发的证书列表中选择**，选择相应的父 CA 中心和从属 CA 证书。



4. 在 CA 中心列表中，可以查看 CA 中心的基本信息：

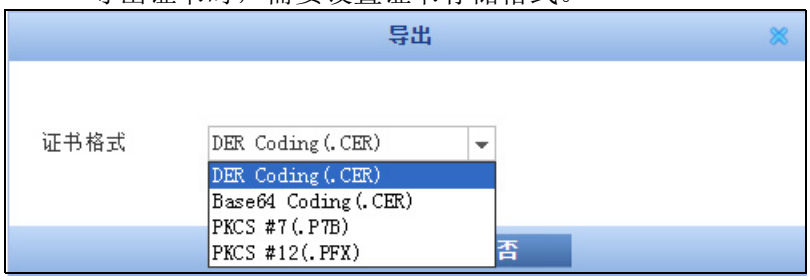
名称	类型	主题	有效期	状态	
rootCA1	根CA	C=CN, ST=LN, L=SY, O=NEU, OU=NSD, CN=FW	2015-12-10 00:29:21 - 2020-12-10 00:29:21	Valid	证书管理
rootCA2	根CA	C=cn, CN=test	2015-07-27 15:25:42 - 2020-07-27 15:35:15	Valid	证书管理
rootCA3	根CA	C=CN, ST=LN	2015-12-10 00:35:06 - 2018-12-10 00:35:06	Valid	证书管理
subCA1	从属CA	CN=subCA	2015-07-31 08:44:49 - 2016-07-31 08:54:49	Valid	证书管理
subCA2	从属CA	C=CN, ST=BJ, L=BJ, O=NEU, OU=SALES, CN=FW	2015-12-10 00:34:19 - 2018-12-10 00:34:19	Valid	证书管理
subCA3	从属CA	C=CN, ST=HZ	2015-12-10 00:35:41 - 2017-12-10 00:35:41	Valid	证书管理

- 点击图标，查看指定 CA 中心的 CA 证书详细信息。



- 点击图标，导出指定 CA 中心的 CA 证书。

  导出证书时，需要设置证书存储格式。



- 点击图标，复制指定 CA 中心的 CA 证书到 NISG-IPS 本地的 CA 证书列表。

  管理员也可通过列表上方的**复制到 CA 证书列表**按钮复制 CA 中心证书：

  - 勾选多个 CA 中心的复选框，点击**复制到 CA 证书列表**，复制多个 CA 中心的 CA 证书到 NISG-IPS 本地的 CA 证书列表。
  - 勾选列表表头的复选框，点击**复制到 CA 证书列表**，复制全部 CA 中心的 CA 证书到 NISG-IPS 本地的 CA 证书列表。

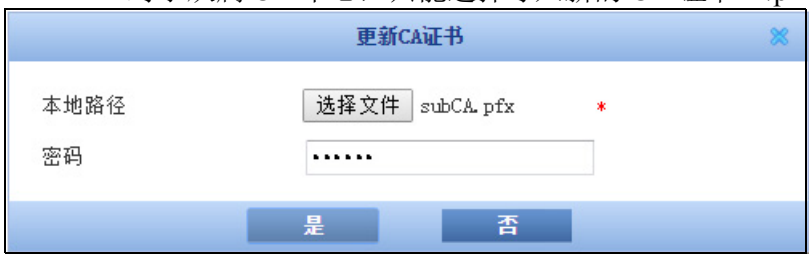
  选择**系统 > 证书 > CA 证书**，查看复制的 CA 证书出。

- 点击图标，更新 CA 中心证书。

- 对于根 CA 中心，可以选择续订原有证书或导入新的证书。
  - 如果选择**续订**，需要设置证书有效期，选择生成新密钥对或使用原有密钥对。证书其他信息与原证书保持一致。

  - 如果选择**导入**，需要指定证书本地存储路径，并输入证书导入密码。

- 对于从属 CA 中心，只能选择导入新的 CA 证书 （pfx 格式）。



- 点击 ✖ 图标，删除指定 CA 中心。

5. 点击 。

提示：删除 CA 中心后，该 CA 中心下颁发的证书、 CRL、证书申请也全部删除。

3.28.2.2 颁发、续订和吊销证书

提示：CA 中心证书未生效或过期时，不能颁发、吊销或续订证书。

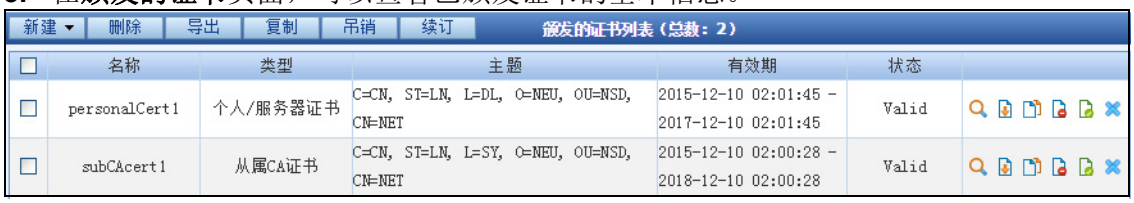
1. 选择**系统 > 证书 > CA 中心**。点击对应 CA 中心的**证书管理**链接，进入证书管理页面。
2. 在页面上方的下拉框中选择**颁发的证书**，打开证书颁发页面。

   颁发的证书支持两种类型：具有证书颁发权限的从属 CA 证书，以及普通的个人 / 服务器证书。颁发证书的有效期不能超出 CA 中心证书的有效期。

   - 点击**新建**，选择**从属 CA 证书**，新建从属 CA 证书。

   - 点击**新建**，选择**个人 / 服务器证书**，创建个人或服务器证书。配置参数同从属 CA 证书。

3. 在**颁发的证书**页面，可以查看已颁发证书的基本信息。



   - 点击 图标，可查看对应的从属 CA 证书或个人 / 服务器证书的详细信息。
   - 点击 图标下载指定证书。导出证书时，需要设置证书存储格式。
   - 点击从属CA证书或个人/服务器证书对应的 图标复制证书到CA证书列表或本地证书列表。可选择**系统 > 证书 > CA 证书**或**系统 > 证书 > 本地证书**进行查看。

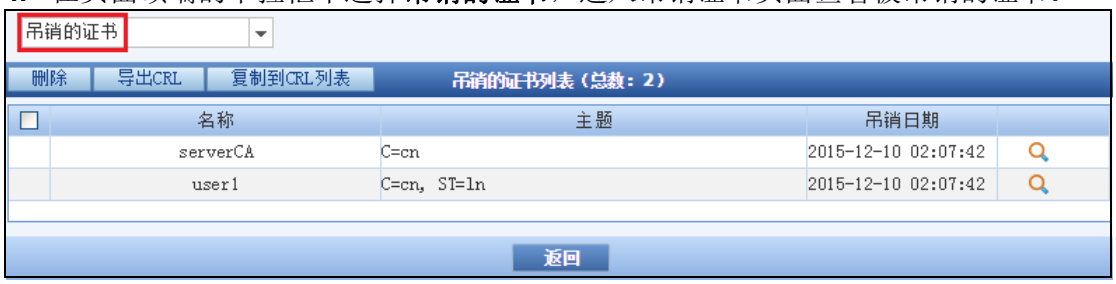
提示：复制个人 / 服务器证书前须先复制其对应的 CA 证书到 NISG-IPS 的 CA 证书列表。

   - 点击 图标吊销指定证书。

- 点击图标续订指定证书。续订证书时需要指定新的有效期，选择生成新密钥对或使用原有密钥对。证书其他信息与原证书保持一致。

- 点击删除指定证书。

4. 在页面顶端的下拉框中选择**吊销的证书**，进入吊销证书页面查看被吊销的证书。



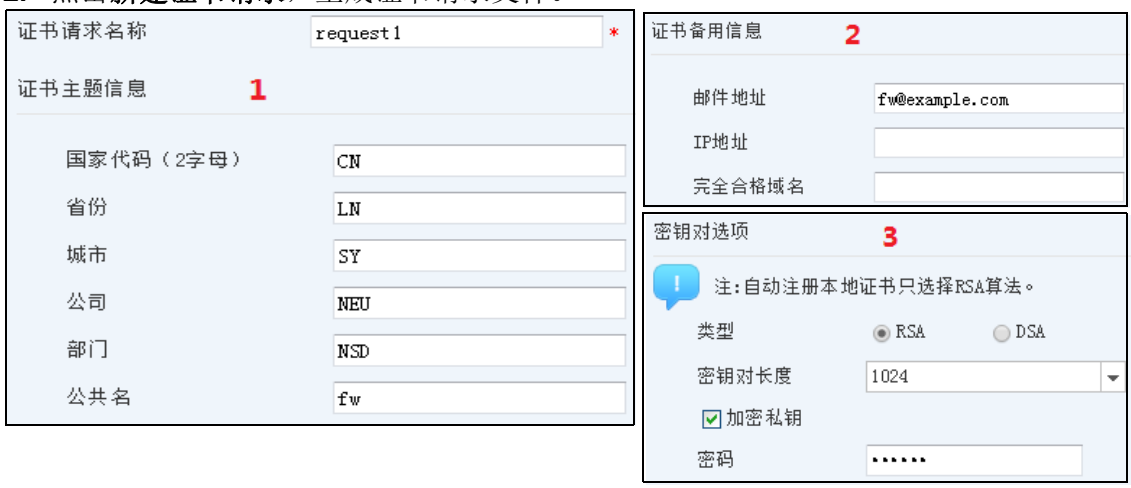
- 当被吊销的证书过期时，可以选择过期证书并点击**删除**按钮将其从**吊销的证书列表**中删除。
- 点击**导出 CRL** 按钮，可以导出吊销证书列表。
- 点击**复制到 CRL 列表**按钮，可以将吊销证书信息同步到 NISG-IPS 本地 CRL 列表。

5. 点击。

提示：续订或吊销证书后，需要手动复制证书或 CRL 到本地证书或 CRL 列表。

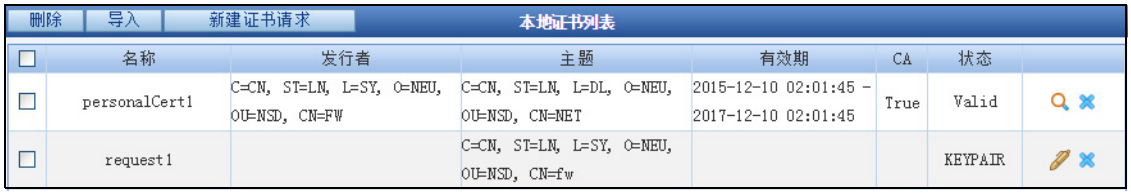
3.28.2.3 管理本地证书

1. 选择**系统 > 证书 > 本地证书**。
2. 点击**新建证书请求**，生成证书请求文件。



3. 保存证书请求文件至本地手动申请或启用证书自动注册。

4. 查看、删除或导入本地证书。



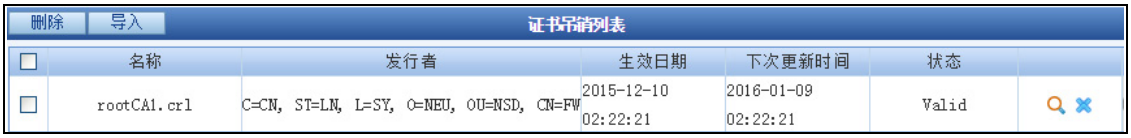
提示：被 VPN 隧道引用的本地证书不可以被删除。

5. 点击 。

3.28.2.4 管理 CA 证书

1. 选择**系统 > 证书 > CA 证书**。
2. 查看、删除或导入 CA 证书。

3. 将证书导入证书吊销列表或从证书吊销列表中删除。



4. 点击 。

配置注意事项

- 当首次向CA服务器申请注册证书时，系统提示确认CA证书的“指纹”。如果确认此“指纹”，则继续进行证书注册。
- 上载证书的顺序是CA证书、CRL和本地证书。因为CA证书和CRL用于检验本地证书是否由 CA 签发以及是否有效。

表 72 证书命令

generate certificate-request	生成本地证书请求。
enroll request ca	发送本地证书请求至 CA。
enroll request accept-ca-certificate	接受或拒绝 CA 证书指纹。
ca certificate checkmethod	设置本地证书检测方式。
delete certificate req	删除本地证书请求。
delete certificate ca, crl, local	删除 CA 证书、 CRL 或本地证书。
import certificate	上载 CA 证书或本地证书。
import certificate crl	上载 CRL。

3.28.3 配置参数说明

3.28.3.1 CA 中心参数

表 73 CA 中心配置信息

参数	说明
名称	CA 中心的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。
类型	CA 中心的类型，包括根 CA 和从属 CA 两种类型。
CA 证书	CA 中心所使用的 CA 证书。 • 新建根 CA 中心时，可以选择**生成根 CA 证书**，也可以选择**导入 CA 证书**。 • 新建从属 CA 中心时，可以有三种选择：**导入 CA 证书**、**从颁发的证书列表中选择**、**本地 CA 中心颁发**。
主题	CA 中心自身 CA 证书的主题信息。 关于证书主题信息和备用信息的输入限制，请参见表 76。
有效期	CA 中心自身 CA 证书的有效时间。 有效时间范围：1-100 年， 1-1200 月， 1-5200 周， 1-36500 天。
状态	CA 中心自身 CA 证书是否有效，包括 valid、 not yet valid、 expired 和 revoked。 CA 中心证书未生效、过期时，不能颁发、吊销或续订证书。
证书管理	点击该链接进入证书颁发和管理页面。
	点击该图标查看 CA 中心自身 CA 证书的详细信息。
	点击该图标导出 CA 中心自身的 CA 证书。 导出 CA 证书时，可以选择证书存储格式，包括 DER Coding (.CER)、Base64 Coding (.CER)、 PKCS #7 (.P7B)、 PKCS #12 (.PFX)。选择 .PFX 格式时，可以设置访问密码。
	点击该图标可将 CA 中心自身的 CA 证书复制到 NISG-IPS 的 CA 证书列表。（可选择**系统 > 证书 > CA 证书**进行查看。）
	点击该图标更新 CA 中心的 CA 证书。 对于根 CA 中心，可以选择**续订**并延长有效期，或选择**导入**并导入新的证书；对于从属 CA 中心，只能选择**导入**并导入新的证书。 续订根 CA 中心证书时，可以选择使用原有的密钥对，也可以设置新的密钥对。密钥对选项包括： • **类型**：包括 RSA 和 DSA，自动注册证书只能选择 RSA 算法。 • **密钥对长度**：密钥越长，越安全，但加密和解密速度越慢。密钥对长度可以为 768、 1024、 1536 和 2048。

表 74 颁发的证书配置信息

参数	说明
名称	颁发的证书名称。
类型	颁发的证书类型，包括从属 CA 证书和个人 / 服务器证书两种类型。
主题	颁发的证书主题信息。
有效期	颁发的证书的有效时间。 颁发证书的有效期不能超出 CA 中心证书的有效期。
状态	颁发的证书状态，包括 valid、 not yet valid 和 expired。
	点击该图标查看颁发的证书详细信息。
	点击该图标导出颁发的证书。 导出证书时，可以选择证书存储格式，包括 DER Coding (.CER)、Base64 Coding (.CER)、PKCS #7 (.P7B)、 PKCS #12 (.PFX)。选择 .PFX 格式时，可以设置访问密码。
	点击该图标可将颁发的从属 CA 证书复制到 CA 证书列表 （**系统 > 证书 > CA 证书**），或者将颁发的个人 / 服务器证书复制到本地证书列表 （**系统 > 证书 > 本地证书**）。
	点击该图标吊销颁发的证书。
	点击该图标续订颁发的证书。 续订证书时，可以选择使用原有的密钥对，也可以设置新的密钥对。密钥对选项包括： • **类型**：包括 RSA 和 DSA，自动注册证书只能选择 RSA 算法。 • **密钥对长度**：密钥越长，越安全，但加密和解密速度越慢。密钥对长度可以为 768、 1024、1536 和 2048。

表 75 吊销的证书配置信息

参数	说明
名称	吊销的证书名称。
主题	吊销的证书主题信息。
吊销日期	证书被吊销的日期。
	点击该图标查看被吊销证书的详细信息。
导出 CRL	点击该按钮导出指定 CA 中心的 CRL 列表，即吊销证书列表。
复制到 CRL 列表	点击该按钮将 CA 中心的吊销证书列表复制到 NISG-IPS 的 CRL 列表。

3.28.3.2 本地证书参数

表 76 本地证书请求配置信息

参数	说明
证书请求名称	长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。
证书主题信息	证书主题信息包括： • **国家代码**：由两个英文字母组成，代表 NISG-IPS 设备所在的国家。 • **省份**：长度 0-127 字节， UTF-8 字符。不能包含空格和以下字符：`？, " ' \ < > &。 • **城市**：长度 0-127 字节， UTF-8 字符。不能包含空格和以下字符：`？, " ' \ < > &。 • **公司**：长度 0-64 字节， UTF-8 字符。不能包含空格和以下字符：`？, " ' \ < > &。 • **部门**：长度 0-64 字节， UTF-8 字符。不能包含空格和以下字符：`？, " ' \ < > &。 • **公共名**：长度 0-64 字节， UTF-8 字符。不能包含空格和以下字符：`？, " ' \ < > &。
证书备用信息	证书备用信息包括： • **邮件地址**：对证书负责的联系人的邮件地址。长度 5-64 字节。 • **IP 地址**：使用证书的安全设备的 IPv4 地址。最大长度 64 字节。 • **完全合格域名**：使用证书的安全设备的完全合格域名。长度 2-64 字节。可以输入不带点 （.）的域名。 证书主题信息和证书备用信息部分至少需要设置一项。
密钥对选项	密钥对选项包括： • **类型**：包括 RSA 和 DSA，自动注册证书只能选择 RSA 算法。 • **密钥对长度**：密钥越长，越安全，但加密和解密速度越慢。密钥对长度可以为 768、 1024、 1536 和 2048。 • **加密私钥**：选择是否加密证书私钥。 • **密码**：个人密钥，长度 0-127 字节。

表 77 证书自动注册和更新配置信息

参数	说明
自动注册 (SCEP)	启用或禁用自动注册证书功能。
选择 CA 服务器	用于注册证书的 CA 服务器的 CA 证书，可以选择 NISG-IPS 上已经存在的 CA 证书或手动输入 CA 证书名称。 NISG-IPS 支持下列 CA 服务器：Baltimore、 Entrust、 Microsoft、 Netscape、 RSA Keon 和 Verisign。
CA 服务器地址	签发证书的 CA 服务器的 URL 地址。长度范围为 2-255 字节。
CA 证书标识	所生成的 CA 证书的 ID，是证书在 NISG-IPS 上的唯一标识。最大长度为 255 字节。
挑战码	当 CA 采用预共享密钥方式认证证书请求者身份时，挑战码用于 CA 对证书请求者的身份进行验证。最大长度为 127 字节。
轮询	如果管理员启用轮询功能，在等待 CA 服务器认证证书注册请求的过程中，作为请求的发送方， NISG-IPS 会不断地发送轮询消息，直到达到最大轮询次数或 CA 服务器返回状态标识为止。 • **轮询间隔**：连续两次发送轮询的间隔时间。取值范围为 1-600 分钟。 • **轮询次数**：最多可发送轮询消息的次数，取值范围为 1-1000。
自动更新	启用证书自动更新功能时，需要设置在证书到期前多长时间执行自动更新。 启用证书自动更新的前提是配置了正确的 CA 服务器地址并且服务器可达。

表 78 本地证书配置信息

参数	说明
名称	本地证书名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。
发行者	发放、管理和撤消本地证书的机构。
主题	本地证书的主题信息。
有效期	本地证书的有效期。
CA	本地证书是否可以被用作 CA 证书颁发用于 SSL 检测的仿冒证书。 • **True**：表示可以颁发仿冒证书。 • **False**：表示不可以颁发仿冒证书。 建议使用从属 CA 证书颁发用于 SSL 检测的仿冒证书。
状态	本地证书注册过程中的各个状态： • **Valid**：证书有效。 • **Pending**：证书注册处于轮询状态，一般发生在 CA 服务器采用手动认证的情况。 • **Keypair**：证书请求标识。 • **Expired**：证书已经过期。 • **Not yet valid**：证书尚未生效。

3.28.3.3 CA 证书参数

表 79 CA 证书配置信息

参数	说明
名称	CA 证书名称。不能为 any （不区分大小写）。
主题	CA 证书的主题信息。
有效期	CA 证书的有效期。
状态	CA 证书的状态： • **Valid**：在有效期内的本地证书。 • **Expired**：标识证书已经过期失效。 • **Not yet valid**：该证书还未生效。
CA 服务器	点击 编辑 CA 服务器的配置，包括**设置证书撤销检测方式**和 **SCEP 设置**。 证书撤销检测方式的配置参数请见表 80。 SCEP 设置的配置参数请参见表 77。

表 80 证书撤销检测方式配置信息

参数	说明
检查方式	证书撤销检查方法，包括 CRL、 OCSP 或 None。 None 表示不进行检测。

表 80 证书撤销检测方式配置信息 (*续*)

参数	说明
严格检查	• 当使用 OCSP 验证证书状态时，如果 NISG-IPS 与 OCSP 服务器连接失败，或者 OCSP 服务器返回检查结果为“未知”时，在勾选**严格检查**复选框的情况下，证书无效；在不选**严格检查**复选框的情况下，证书合法。 • 当使用 CRL 方法验证证书状态时，如果 NISG-IPS 中不存在 CRL，在勾选**严格检查**复选框的情况下，证书无效；在不选**严格检查**复选框的情况下，证书合法。
OCSP 地址	OCSP 服务器的 URL 地址，例如：http://ocsp.test.com。 也可以在设置 OCSP 服务器的 URL 时，设置端口号，例如：http://ocsp.test.com:8080。 NISG-IPS 支持以下 OCSP 服务器：Entrust、 microsoft、 RSA Keon 和 Verisign。

表 81 CRL 列表配置信息

参数	说明
名称	CRL 列表名称。
发行者	发布 CRL 列表的 CA 中心的 CA 证书主题信息。
生效日期	CRL 列表的起始生效时间。 • 如果是从本地 CA 中心复制的 CRL 列表，其起始生效时间即复制 CRL 列表的时间。 • 如果是从第三方 CA 中心导出的 CRL 列表，其起始生效时间以 CRL 文件本身的生效时间为准。
下次更新时间	CRL 列表的终止生效时间。管理员应在此时间之前再次复制或导入 CA 中心最新发布的 CRL 列表。 • 如果是从本地 CA 中心复制的 CRL 列表，其有效期为一个月，管理员应在一个月内再次复制本地 CA 中心发布的 CRL 列表。 • 如果是从第三方 CA 中心导出的 CRL 列表，其有效期以发布该 CRL 列表的 CA 中心系统配置为准，管理员应在规定的有效期内再次导入第三方 CA 中心新发布的 CRL 列表。
状态	CRL 列表的状态，包括 Valid、 Expired 和 Not yet valid。

3.29 对象

为了方便管理员配置， NISG-IPS 引入了对象的概念。

管理员可以将一个或多个 IP 地址定义为一个对象，也可以将一个或多个服务定义为一个对象，还可以将相同类型的对象划分到一个对象组中。

配置完对象或对象组后，可以在以下策略中引用：

表 82 可以引用对象的策略类型

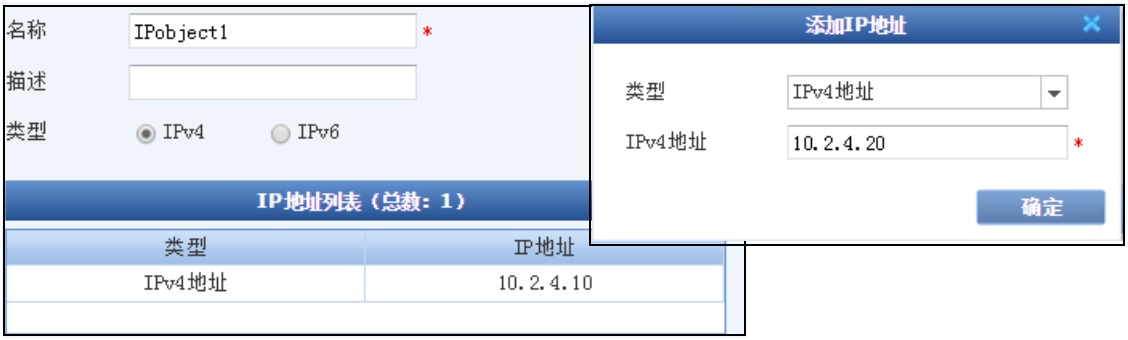
策略类型	引用对象类型	操作路径
WebAuth 重定向策略	IP 对象和对象组	系统 > 认证 >WebAuth 配置 > 对未标识会话进行被动认证 > 新建 > 源 / 目的 IP 地址
策略路由	• IP 对象和对象组 • 服务对象和对象组	网络 > 路由 > 策略路由 > 新建 > 源 IP 地址 / 服务
地址映射	• IP 对象和对象组 • 服务对象和对象组	网络 > 地址转换 > 地址映射 > 新建 > 高级设置 > 目的 IP 地址 / 服务
源地址转换	• IP 对象和对象组 • 服务对象和对象组	网络 > 地址转换 > 源地址转换 > 新建 > 源 IP 地址 / 高级设置 （目的 IP 地址 / 服务）
目的地址转换	IP 对象和对象组	网络 > 地址转换 > 目的地址转换 > 新建 > 高级设置 > 源 IP 地址
访问策略	• IP 对象和对象组 • 服务对象和对象组	防火墙 > 访问策略 > 新建 > 源 IP 地址 / 目的 IP 地址 / 服务
多播策略	IP 对象和对象组	防火墙 > 多播策略 > 新建 > 源 IP 地址 / 多播组 IP 地址
会话策略	• IP 对象和对象组 • 服务对象和对象组	防火墙 > 会话策略 > 新建 > 源 IP 地址 / 目的 IP 地址 / 服务
IP-MAC 绑定	IP 对象和对象组	防火墙 >IP-MAC 绑定 > 新建 > 绑定 IP 地址列表
IPS 策略	IP 对象和对象组	• IPS> 出口控制 > 策略 > 应用控制 /URL 过滤 > 新建 > 源 IP 地址 • IPS> 客户端防护 > 策略 > 新建 > 客户端 IP 地址 • IPS> 服务器防护 > 策略 > 新建 > 受保护的服务器列表
QoS 策略	• IP 对象和对象组 • 服务对象和对象组	IPS>QoS>QoS 策略 > 新建 > 源 IP 地址 / 目的 IP 地址 / 服务
SSL 检测证书策略	IP 对象和对象组	IPS>SSL 检测 > 新建 > 目的 IP 和端口列表

3.29.1 IP 地址

可以将一个或多个 IP 地址定义为一个对象。还可以将相同类型的 IP 地址对象划分到一个 IP 地址对象组中，以简化配置。

3.29.1.1 基本配置步骤

1. 选择**系统** > **对象** > **IP 地址** > **IP 地址对象**。
2. 点击**新建**创建一个对象。点击**添加**编辑该对象包含的 IP 地址。



3. 选择**系统** > **对象** > **IP 地址** > **IP 地址对象组**。
4. 点击**新建**创建 IP 地址对象组。从**备选对象**中选择 IP 地址对象加入对象组。

5. 点击**确定**。
6. 点击 。

配置注意事项

- 被策略引用的 IP 地址对象或对象组不能被删除。
- 最多可创建 1024 个 IP 地址对象，每个 IP 地址对象最多可包含 128 个 IP 地址条目。

- 最多可创建1024个IP地址对象组，每个IP地址对象组最多可包含128个IP地址对象。IP 地址对象组不能和其对象成员重名。

表 83 IP 地址对象 /IP 地址对象组命令

object ipaddr *object_name* **description** *string*	设置指定 IP 地址对象的备注信息。
object group *group_name* **type ipaddr** [**object** *object_list*]	添加 IP 地址对象组 , 或者向已存在的 IP 地址对象组中添加对象成员。
object group *group_name* **type ipaddr description** *string*	设置指定 IP 地址对象组的备注信息。
object ipaddr *object_name* [*ipv4_list* | *ipv6_list*]	添加 IP 地址对象或向已存在的 IP 地址对象中添加 IP 地址。
unset object ipaddr [*object_name*]	删除 IP 地址对象。
unset object group type ipaddr [*group_name*]	删除 IP 地址对象组。
unset object group type ipaddr *group_name* **object** *object_name*	删除 IP 地址对象组的指定成员。
unset object ipaddr *object_name* {*ipv4_list* | *ipv6_list*}	删除指定 IP 地址对象中的 IP 地址。

3.29.1.2 IP 地址对象参数

表 84 IP 地址对象参数

参数	说明
名称	IP 地址对象名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
描述	IP 地址对象备注信息，长度 0-255 字节， UTF-8 字符。不能包含以下字符：? " ' \ < > &
类型	IP 类型，包括 IPv4 和 IPv6。
IP 地址	IP 地址对象包含的 IP 地址，可以为单个 IPv4 或 IPv6 地址、 IPv4 或 IPV6 地址范围、 IPv4 地址 / 掩码、 IPv6 地址 / 前缀。
引用	显示引用 IP 地址对象的策略。

3.29.1.3 IP 地址对象组参数

表 85 IP 地址对象组参数

参数	说明
组名称	IP 地址对象组名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
描述	IP 地址对象组备注信息。长度 0-255 字节， UTF-8 字符。不能包含以下字符：? " ' \ < > &
包含对象	IP 地址对象组包含的 IP 地址对象。
引用	显示引用 IP 地址对象组的策略。

3.29.2 服务

可以将一个或多个服务定义为一个对象。还可以将多个服务对象划分到一个服务对象组中，以简化配置。

3.29.2.1 基本配置步骤

1. 选择**系统** > **对象** > **服务** > **服务对象**。
2. 点击**新建**创建一个对象。点击**添加**编辑该对象包含的服务。

3. 选择**系统** > **对象** > **服务** > **服务对象组**。
4. 点击**新建**创建服务对象组。从**备选对象**中选择服务对象加入服务对象组。

5. 点击**确定**。
6. 点击 。

配置注意事项

- 被策略引用的服务对象或对象组不能被删除。
- 最多可创建 1024 个服务对象，每个服务对象最多可包含 128 个服务条目。
- 最多可创建 1024 个服务对象组，每个服务对象组最多可包含 128 个服务对象。服务对象组不能和其对象成员重名。

表 86 服务对象 / 服务对象组命令

object service *object_name* **description** *string*	设置指定服务对象的备注信息。
object group *group_name* **type service** [**object** *object_list*]	添加服务对象组 , 或者向已存在的服务对象组中添加对象成员。
object group *group_name* **type service description** *string*	设置指定服务对象组的备注信息。
object service *object_name* [{**tcp	udp**} {*src_port*	*src_port_range*} {*dst_port* **|** *dst_port_range*}	**icmp** {*icmp_type*	*icmp_list*	**Any** }	**icmpv6** {*icmpv6_type*	*icmpv6_list*	**Any**}	**other** *protocol_num*]	添加服务对象或者向已存在的服务对象中添加服务列表。
unset object service [*object_name*]	删除服务对象。
unset object group type service [*group_name*]	删除服务对象组。
unset object group type service *group_name* **object** *object_name*	删除服务对象组的指定成员。
unset object service *object_name* {{**tcp	udp**} {*src_port*	*src_port_range*} {*dst_port* **|** *dst_port_range*}	**icmp** {*icmp_type*	*icmp_list*	**Any**}	**icmpv6** {*icmpv6_type*	*icmpv6_list*	**Any**}	**other** *protocol_num*}	删除指定服务对象中的服务。

3.29.2.2 服务对象参数

表 87 服务对象参数

参数	说明
名称	服务对象名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
描述	服务对象备注信息。长度 0-255 字节， UTF-8 字符。不能包含以下字符：? " ' \ < > &
服务	网络协议类型和与之对应的 ICMP 协议类型、端口号或者协议号。网络协议类型包括 ICMP、ICMPv6、TCP、UDP 和 Other，其中 Other 是除了 ICMP、ICMPv6、TCP、UDP 之外的协议。
引用	显示引用服务对象的策略。

表 88 服务对象缺省配置信息

服务对象	缺省配置信息
AOL	协议：TCP ；源端口：1-65535 ；目的端口：5190-5194
BGP	协议：TCP ；源端口：1-65535 ；目的端口：179
CHARGEN	• 协议：TCP ；源端口：1-65535 ；目的端口：19 • 协议：UDP ；源端口：1-65535 ；目的端口：19
DHCP-Relay	• 协议：UDP ；源端口：1-65535 ；目的端口：67 • 协议：UDP ；源端口：1-65535 ；目的端口：68
DISCARD	• 协议：TCP ；源端口：1-65535 ；目的端口：9 • 协议：UDP ；源端口：1-65535 ；目的端口：9

表 88 服务对象缺省配置信息 (*续*)

服务对象	缺省配置信息
DNS	• 协议：UDP；源端口：1-65535；目的端口：53 • 协议：TCP；源端口：1-65535；目的端口：53
ECHO	• 协议：UDP；源端口：1-65535；目的端口：7 • 协议：TCP；源端口：1-65535；目的端口：7
FINGER	协议：TCP；源端口：1-65535；目的端口：79
FTP	协议：TCP；源端口：1-65535；目的端口：21
GNUTELLA	• 协议：UDP；源端口：1-65535；目的端口：6346-6347 • 协议：TCP；源端口：1-65535；目的端口：6346-6347
GOPHER	协议：TCP；源端口：1-65535；目的端口：70
GRE	协议：Other；协议号：47
GTP	协议：UDP；源端口：1-65535；目的端口：2123
HTTP	协议：TCP；源端口：1-65535；目的端口：80
HTTPS	协议：TCP；源端口：1-65535；目的端口：443
HTTP_EXT	• 协议：TCP；源端口：1-65535；目的端口：7001 • 协议：TCP；源端口：1-65535；目的端口：8000-8001 • 协议：TCP；源端口：1-65535；目的端口：8080-8081 • 协议：TCP；源端口：1-65535；目的端口：8100 • 协议：TCP；源端口：1-65535；目的端口：8200 • 协议：TCP；源端口：1-65535；目的端口：9080
H_323	• 协议：TCP；源端口：1-65535；目的端口：1720 • 协议：UDP；源端口：1-65535；目的端口：1718-1719
ICMP 类对象 (协议：ICMP)	• ICMPv4 类： •ICMP_Any •ICMP_ADDRESS_and_ADDRESSREPLY •ICMP_DEST_UNREACH •ICMP_ECHO_and_ECHOREPLY •ICMP_INFO_REQUEST_and_INFO_REPLY •ICMP_PARAMETERPROB •ICMP_REDIRECT •ICMP_ROUTER_ADVERTISEMENT •ICMP_ROUTER_SOLICITATION •ICMP_SOURCE_QUENCH •ICMP_TIMESTAMP_and_TIMESTAMPREPLYICMP •ICMP_TIME_EXCEEDEDICMP • ICMPv6 类： •ICMPv6_ANY •ICMPv6_DST_UNREACH •ICMPv6_PACKET_TOO_BIG •ICMPv6_TIME_EXCEEDED •ICMPv6_PARAM_PROB •ICMPv6_ECHO_and_ECHOREPLY
IDENT	协议：TCP；源端口：1-65535；目的端口：113
IKE	协议：UDP；源端口：1-65535；目的端口：500

表 88 服务对象缺省配置信息 (*续*)

服务对象	缺省配置信息
IKE_NAT	协议：UDP；源端口：500；目的端口：500
IMAP	协议：TCP；源端口：1-65535；目的端口：143
IRC	协议：TCP；源端口：1-65535；目的端口：6660-6669
Internet_Locator_Service	• 协议：TCP；源端口：1-65535；目的端口：389 • 协议：TCP；源端口：1-65535；目的端口：522 • 协议：TCP；源端口：1-65535；目的端口：636
L2TP	协议：UDP；源端口：1-65535；目的端口：1701
LDAP	协议：TCP；源端口：1-65535；目的端口：389
LPR	协议：TCP；源端口：1-65535；目的端口：515
MAIL	协议：TCP；源端口：1-65535；目的端口：25
MGCP_CA	协议：UDP；源端口：1-65535；目的端口：2727
MGCP_UA	协议：UDP；源端口：1-65535；目的端口：2427
MSN	协议：TCP；源端口：1-65535；目的端口：1863
MS_RPC_EPM	• 协议：UDP；源端口：1-65535；目的端口：135 • 协议：TCP；源端口：1-65535；目的端口：135
MS_SQL	协议：TCP；源端口：1-65535；目的端口：1433
NBDS	协议：UDP；源端口：1-65535；目的端口：138
NBNAME	协议：UDP；源端口：1-65535；目的端口：137
NFS	• 协议：UDP；源端口：1-65535；目的端口：111 • 协议：TCP；源端口：1-65535；目的端口：111 • 协议：UDP；源端口：1-65535；目的端口：2049 • 协议：TCP；源端口：1-65535；目的端口：2049
NNTP	协议：TCP；源端口：1-65535；目的端口：119
NTP	协议：UDP；源端口：1-65535；目的端口：123
NetMeeting	• 协议：TCP；源端口：1-65535；目的端口：1720 • 协议：TCP；源端口：1-65535；目的端口：1503 • 协议：TCP；源端口：1-65535；目的端口：389 • 协议：TCP；源端口：1-65535；目的端口：522 • 协议：TCP；源端口：1-65535；目的端口：1731 • 协议：UDP；源端口：1-65535；目的端口：1719
ORACLE	协议：TCP；源端口：1-65535；目的端口：1521
OSPF	协议：Other；协议号：89
PC_Anywhere	• 协议：UDP；源端口：1-65535；目的端口：5632 • 协议：UDP；源端口：1-65535；目的端口：22 • 协议：TCP；源端口：1-65535；目的端口：5631
PING	协议：ICMP；类型：ECHO_and_ECHOREPLY
POP3	协议：TCP；源端口：1-65535；目的端口：110

表 88 服务对象缺省配置信息 (*续*)

服务对象	缺省配置信息
PPTP	协议：TCP；源端口：1-65535；目的端口：1723
RADIUS	协议：UDP；源端口：1-65535；目的端口：1812-1813
REXEC	协议：TCP；源端口：1-65535；目的端口：512
RIP	协议：UDP；源端口：1-65535；目的端口：520
RLOGIN	协议：TCP；源端口：1-65535；目的端口：513
RSH	协议：TCP；源端口：1-65535；目的端口：514
RTSP	协议：TCP；源端口：1-65535；目的端口：554
Real_Media	• 协议：TCP；源端口：1-65535；目的端口：7070 • 协议：TCP；源端口：1-65535；目的端口：554
SCCP	协议：TCP；源端口：1-65535；目的端口：2000
SCTP_ANY	协议：Other；协议号：132
SIP	协议：UDP；源端口：1-65535；目的端口：5060
SMB	• 协议：TCP；源端口：1-65535；目的端口：139 • 协议：TCP；源端口：1-65535；目的端口：445
SMTP	协议：TCP；源端口：1-65535；目的端口：25
SNMP	• 协议：UDP；源端口：1-65535；目的端口：161 • 协议：TCP；源端口：1-65535；目的端口：161 • 协议：UDP；源端口：1-65535；目的端口：162 • 协议：TCP；源端口：1-65535；目的端口：162
SQL_Monitor	协议：UDP；源端口：1-65535；目的端口：1434
SQL_Net_V1	协议：TCP；源端口：1-65535；目的端口：1525
SQL_Net_V2	协议：TCP；源端口：1-65535；目的端口：1521
SSH	协议：TCP；源端口：1-65535；目的端口：22
SUN_RPC_PORTMAPPER	• 协议：UDP；源端口：1-65535；目的端口：111 • 协议：TCP；源端口：1-65535；目的端口：111
SYSLOG	协议：UDP；源端口：1-65535；目的端口：514
TALK	协议：UDP；源端口：1-65535；目的端口：517-518
TCP_ANY	协议：TCP；源端口：1-65535；目的端口：1-65535
TELNET	协议：TCP；源端口：1-65535；目的端口：23
TFTP	协议：UDP；源端口：1-65535；目的端口：69
TRACEROUTE	协议：ICMP；类型：ECHO_and_ECHOREPLY
UDP_ANY	协议：UDP；源端口：1-65535；目的端口：1-65535
UUCP	协议：UDP；源端口：1-65535；目的端口：540

表 88 服务对象缺省配置信息 (*续*)

服务对象	缺省配置信息
VDO_Live	协议：TCP；源端口：1-65535；目的端口：7000-7010
VNC	• 协议：TCP；源端口：1-65535；目的端口：5800 • 协议：TCP；源端口：1-65535；目的端口：5900
WAIS	协议：TCP；源端口：1-65535；目的端口：210
WHOIS	协议：TCP；源端口：1-65535；目的端口：43
WINFRAME	协议：TCP；源端口：1-65535；目的端口：1494
X_WINDOWS	协议：TCP；源端口：1-65535；目的端口：6000-6063
YMSG	• 协议：TCP；源端口：1-65535；目的端口：5050 • 协议：TCP；源端口：1-65535；目的端口：443

3.29.2.3 服务对象组参数

表 89 服务对象组参数

参数	说明
对象组名称	服务对象组名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
描述	服务对象组备注信息。长度 0-255 字节，UTF-8 字符。不能包含以下字符：? " ' \ < > &
包含对象	服务对象组包含的服务对象。
引用	显示引用服务对象组的策略。

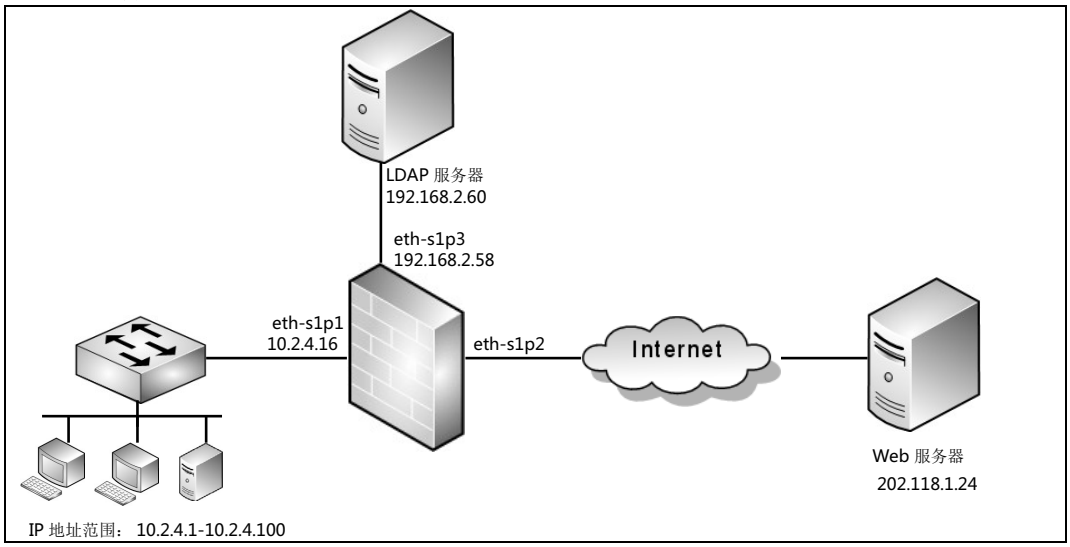
3.30 系统配置范例

3.30.1 范例：WebAuth 认证

基本需求

- 内网用户必须通过 WebAuth 认证才能访问外网。
- 重定向后的认证地址使用内网口 IP 地址，认证端口为 4325。

组网拓扑



配置要点

- 创建访问策略
- 设置 DNS 代理
- 创建 SNAT 规则
- 配置 LDAP 服务器
- 设定用户 WebAuth 角色
- 设置网络用户认证服务器
- 开启接口 WebAuth 认证
- 创建 WebAuth 自动重定向策略

配置步骤

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建访问策略。允许来自 10.2.4.1-10.2.4.100 网段的访问。
   - 名称：acpolicy1
   - 源 IP 地址：10.2.4.1-10.2.4.100
   - 目的 IP 地址：202.118.1.24
   - 动作：允许
3. 点击策略对应的图标，在策略中启用 DNS 透明代理。
4. 点击**确定**。
5. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access acpolicy1 any 10.2.4.1-10.2.4.100
any 202.118.1.24 any any permit enable
NetEye@root-system] policy access acpolicy1 dns-proxy enable
NetEye@root-system] end
NetEye@root> save config
```

设置 DNS 代理

1. 选择**网络** > **DNS** > **DNS 代理**。
2. 点击**新建**，设置 DNS 代理。
   - 域名：www.test.com
   - 接口：任意
   - 首选 DNS：202.96.1.20
3. 点击**确定**。
4. 点击。

也可以通过在 NISG-IPS 上添加静态缓存建立 IP 地址和域名的对应关系：

1. 选择**网络** > **DNS** > **静态缓存**。
2. 点击**新建**，添加静态 DNS 缓存条目：
   - 域名：www.test.com
   - 入口接口：任意
   - IP 地址：202.118.1.24
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] dns server-select www.test.com output-interface any primary 202.96.1.20
NetEye@root-system] dns cache www.test.com 202.118.1.24 input-interface any)
NetEye@root-system] end
NetEye@root> save config
```

创建 SNAT 规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**创建 SNAT 规则。
   - 名称：snat1
   - 源 IP：10.2.4.1-10.2.4.100
   - 转换后接口：eth-s1p2
   - 入口接口：eth-s1p1
   - 出口接口：eth-s1p2
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy snat snat1 iplist 10.2.4.1-10.2.4.100 interface eth-s1p2 napt enable
NetEye@root-system] policy snat snat1 matching input-interface eth-s1p1
NetEye@root-system] policy snat snat1 matching output-interface eth-s1p2
NetEye@root-system] end
NetEye@root> save config
```

配置 LDAP 服务器

1. Windows Server 2003 上安装 Active Directory 服务。
2. 将用户的认证信息存储至新建的 LDAP 服务器。
   - 用户名：testuser
   - 密码：test.12

提示：服务器配置信息需与以上创建的 LDAP 服务器配置一致。

---

3. 在 NISG-IPS 上选择**系统** > **认证** > **认证服务器**。
4. 点击**新建**设置 LDAP 服务器，输入以下服务器信息：
   - 名称：Server3
   - 类型：LDAP
   - IP 地址：192.168.2.60
   - 端口：389
   - 安全连接：无
   - 公共名标示符：sAMAccountName
   - 识别名称：dc=IDTest,dc=com
   - 管理员识别名称：cn=Administrator,cn=Users,dc=IDTest,dc=com
   - 密钥：123456 （即 LDAP 服务器管理员密码）
5. 点击**确定**。
6. 点击  。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] ldap server Server3 ip/domain 192.168.2.60 port
389 Secure_Connection none
NetEye@root-system] ldap server Server3 Admin_DN
cn=Administrator,cn=Users,dc=IDTest,dc=com
NetEye@root-system] ldap server Server3 Common_Name_Identifier
sAMAccountName
NetEye@root-system] ldap server Server3 Distinguished_Name
dc=IDTest,dc=com
NetEye@root-system] end
NetEye@root> save config
```

设定用户 WebAuth 角色

1. 选择**系统 > 认证 > 网络用户**，进入**网络用户**页面。
2. 点击**新建**创建 WebAuth 用户。
   - 用户名：testuser
   - 认证类型：外部
   - 勾选**启用**和 **WebAuth**。
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] user authuser testuser authtype external enable
NetEye@root-system] user authuser testuser auth
NetEye@root-system] user authuser testuser auth multipoint enable
NetEye@root-system] end
NetEye@root> save config
```

设置网络用户认证服务器

1. 选择**系统 > 认证 > 认证配置**。
2. 指定网络用户认证服务器为 “Server3”。
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] server authentication type authuser Server3
NetEye@root-system] end
NetEye@root> save config
```

开启接口 WebAuth 认证

1. 选择**系统 > 认证 > WebAuth 配置**。在 eth-s1p1 上启用 WebAuth 功能。
2. 点击**确定**。
3. 点击  。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] webauth ethernet eth-s1p1 on
NetEye@root-system] end
NetEye@root> save config
```

创建 WebAuth 自动重定向策略

1. 选择**系统 > 认证 > WebAuth 配置**。
2. 点击**对未标识会话进行被动 WebAuth 认证**。点击**新建**，创建 WebAuth 自动重定向策略。
   - 名称：authpolicy1
   - 源 IP 地址：10.2.4.1-10.2.4.100
   - 服务：HTTP
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] webauth policy authpolicy1 any 10.2.4.1-10.2.4.100 any any service http
NetEye@root-system] end
NetEye@root> save config
```

验证结果

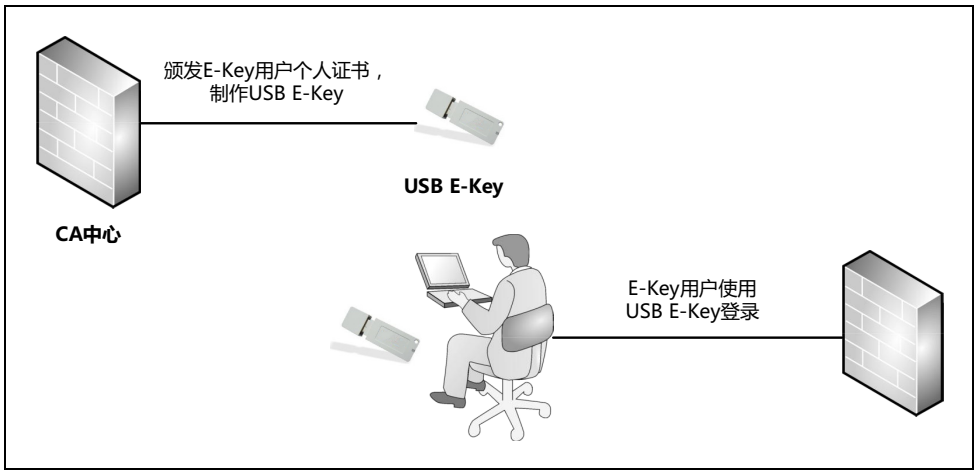
上述配置后，用户输入 http://www.test.com, 页面跳转至 WebAuth 认证登录页面 （https://10.2.4.16:4325/e/webauth/login/）。输入正确的用户名和密码后， NISG-IPS 显示如下登录成功的信息。之后用户可以输入 http://www.test.com 进行访问。

3.30.2 范例：使用本地 CA 中心颁发证书

基本需求

本范例介绍如何通过 NISG-IPS 的本地 CA 中心手动颁发证书，供 E-Key 用户 admin 登录时用于身份验证。

组网拓扑



配置要点

- 创建本地 CA 中心
- 颁发个人证书
- 验证颁发的证书
- 撤销个人证书

配置步骤

创建本地 CA 中心

1. 选择**系统 > 证书 > CA 中心**。
2. 点击**新建**按钮，选择**根 CA 中心**，创建本地根 CA 中心 **rootCA**，选择**生成根 CA 证书**（生成自签名 CA 证书），并设置证书各项信息。
   - 名称：rootCA
   - CA 证书：生成根 CA 证书
   - 有效期：5 年
   - 证书主题信息：
     - 国家代码 （2 字母）：CN
     - 省份：LN

- 城市：SY
- 公司：NEU
- 部门：NSD
- 公共名：FW

- 证书备用信息：（选填）
- 秘钥对选项：
  - 类型：RSA
  - 秘钥对长度：1024

3. 点击**确定**，查看生成的根 CA 中心以及根 CA 证书。
4. 勾选新建根 CA 中心前面的复选框，点击列表上方的**复制到 CA 证书列表**，将新建根 CA 中心的 CA 证书复制到 NISG-IPS 本地 CA 证书列表，用于在 E-Key 用户登录时验证用户的个人证书。
5. 选择**系统 > 证书 > CA 证书**，可以查看复制的 CA 证书。
6. 点击 。

颁发个人证书

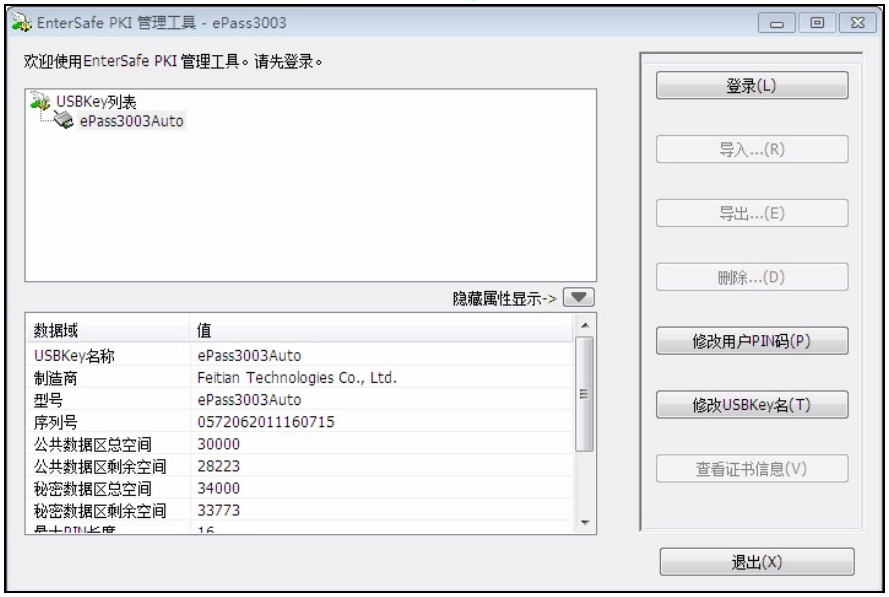
1. 在 **CA 中心**列表中，点击根证书 rootCA 对应的**证书管理**链接，进入证书颁发页面。
2. 点击**新建**按钮，选择**个人 / 服务器证书**，填写 E-Key 用户的证书信息。公共名必须填写该 E-Key 用户的用户名，标识该用户与证书的绑定关系。
   - 名称：admin_eKeyCert
   - 有效期：3 年
   - 证书主题信息：
     - 国家代码 （2 字母）：CN
     - 省份：LN
     - 城市：SY
     - 公司：NEU
     - 部门：NSD
     - 公共名：**admin**
   - 证书备用信息：（选填）
   - 秘钥对选项：
     - 类型：RSA
     - 秘钥对长度：1024
3. 点击**确定**，查看颁发的个人证书。
4. 勾选新颁发证书对应的 ，将证书导出到本地，用于制作 USB E-Key。
5. 点击 。

验证颁发的证书

- 制作 USB E-Key
- 启用 E-Key 认证
- 使用 E-Key 登录

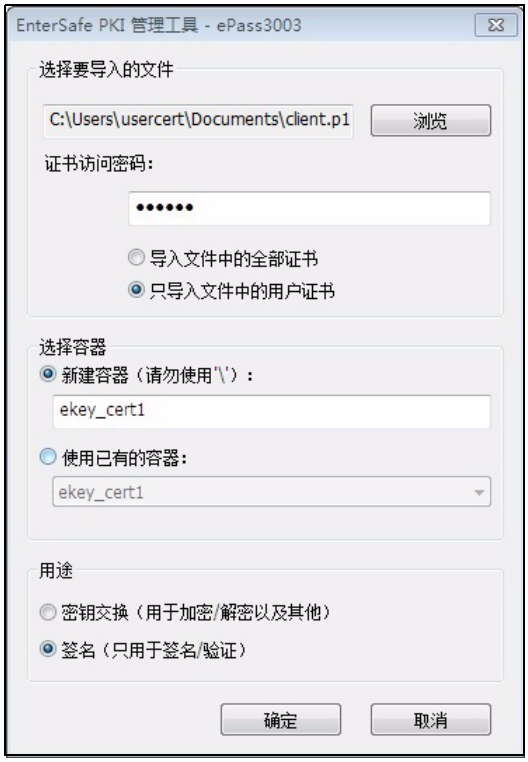
制作 USB E-Key

1. 插入定制的 USB 设备。
2. 双击系统中出现的 USB 驱动图标，完成驱动安装。
3. 电脑右下角的通知区域出现一个图标，双击该图标打开 USB 管理软件。



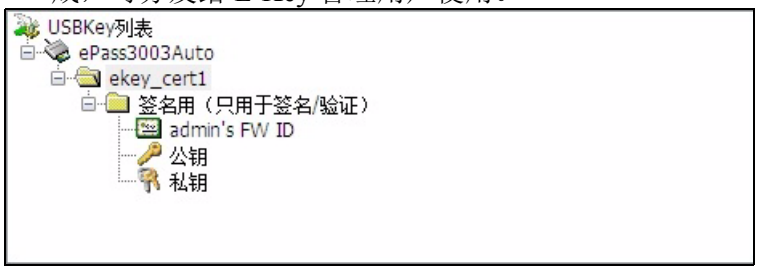
4. 在令牌列表区域选择要进行操作的 USB 设备，点击右侧的**登录**按钮，输入 PIN 码。

5. 登录后，右侧的操作按钮变为可用状态。点击**导入**按钮，选择要用于 E-Key 认证的用户证书，输入证书的访问 （导入 / 导出）密码，用途选择 “ 签名 ”。



提示：仅允许导入 pfx/p12 格式的证书。

6. 导入成功后，在令牌列表区域将出现导入证书的详细信息。至此，USB E-Key 制作完成，可分发给 E-Key 管理用户使用。

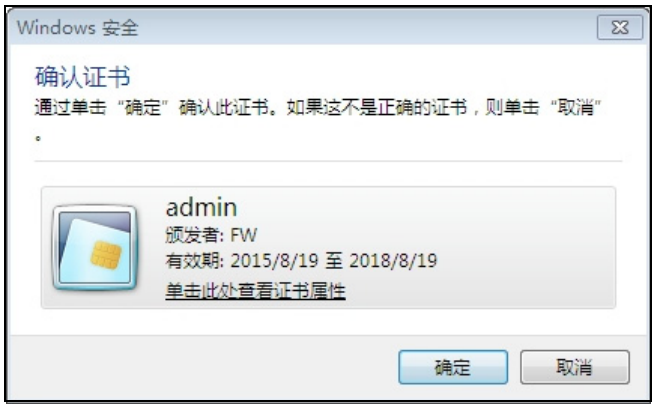


启用 E-Key 认证

1. 以根管理员 root 身份登录，选择**系统 > 认证 > 管理用户**，点击管理用户 admin 对应的 图标，进入管理用户编辑页面。
2. 在**增强认证方式**区域，勾选 **E-key 认证**复选框。
3. 点击**确定**。
4. 点击 。

使用 E-Key 登录

1. 插入 E-Key，打开浏览器，输入 NISG-IPS 的管理地址。
2. 选择使用的证书。



3. 在弹出的验证窗口输入 E-Key 的 PIN 码。

提示：如果不弹出验证窗口，请关闭浏览器后重新打开并输入管理地址。

4. 输入管理用户名、密码和验证码，点击**登录**。
5. 登录成功，则说明本地 CA 中心签发的证书生效；否则说明证书无效，请检查证书信息和签发过程。

撤销个人证书

如果不慎将证书私钥泄露，需要撤销证书后重新颁发证书。

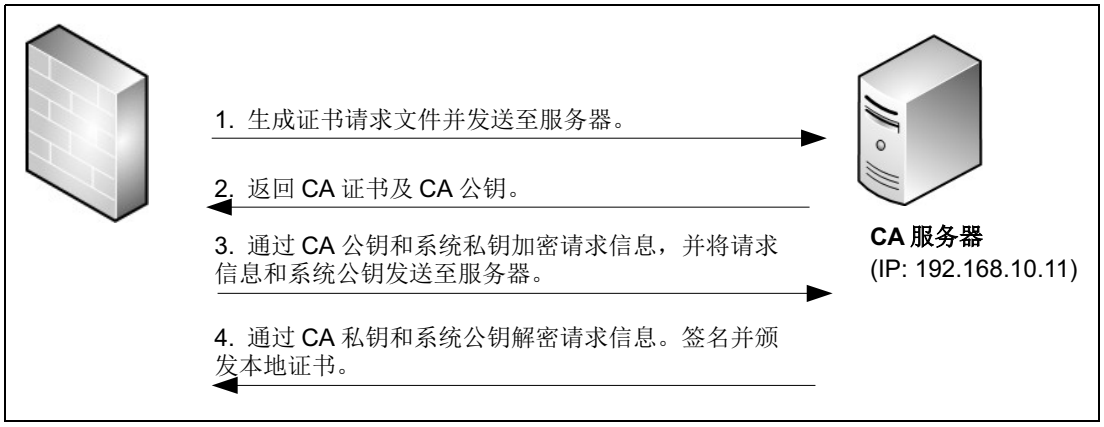
1. 在**颁发的证书**页面，勾选要撤销的证书，点击**吊销**按钮。
2. 在弹出的确认对话框中点击**是**，确认吊销证书。
3. 在页面上方的下拉框中选择**吊销的证书**，将发现被吊销的证书出现在**吊销的证书**列表中。
4. 点击 。

3.30.3 范例：通过第三方 CA 中心自动注册证书

基本需求

本范例介绍 NISG-IPS 如何通过 Windows 的 CA 服务器自动生成证书。

组网拓扑



配置要点

- 创建证书请求
- 自动注册证书

配置步骤

创建证书请求

1. 选择**系统** > **证书** > **本地证书**。
2. 点击**新建证书请求**进入**本地证书**页面。输入证书请求名称和证书主题及备用信息。
   - 证书请求名称：test
   - 证书主题信息：
     - 国家代码 （2 字母）：CN
     - 省份：LN
   - 证书备用信息：（选填）
   - 秘钥对选项：
     - 类型：RSA
     - 秘钥对长度：1024
     - 加密私钥：不勾选
3. 点击**确定**。

4. 在本地证书列表中查看已生成的证书请求文件。
5. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] generate certificate-request test country CN
state-or-province LN locality none organization none organizational-
unit none common-name none ip-address none email-address none dns
none rsa 1024
NetEye@root-system] end
NetEye@root> save config
```

自动注册证书

1. 点击新生成的证书请求文件所对应的进入**本地证书**页面。
2. 勾选**自动注册 （SCEP）**。输入 CA 服务器名、地址、 CA 证书标识及挑战码信息。
   - 选择 CA 服务器：CC
   - CA 服务器地址：http://192.168.10.11/certsrv/mscep/mscep.dll
   - 挑战码：8AE0AA7D70B3F623

提示：CA 服务器地址、挑战码及指纹信息从 CA 服务器获得。

---

3. 点击**确定**并验证 CA 证书指纹。如果指纹正确点击**接受**。
4. 证书已生成。点击**返回**在**本地证书列表**中查看生成的本地证书。
5. 在 **CA 证书列表**中查看生成的 CA 证书。
6. 点击。

CLI

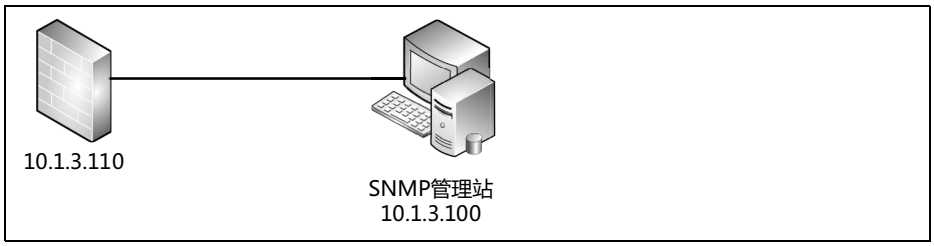
```
NetEye@root> configure mode override
NetEye@root-system] enroll request test ca CC url http://
192.168.10.11/certsrv/mscep/mscep.dll ident none challenge
8AE0AA7D70B3F623 polling disable
% Please contact the CA administrator to verify the finger print of CA
certificate:
        86:E3:BF:BF:14:46:57:0C:1A:D8:1E:9E:C2:F6:D2:78
NetEye@root-system] enroll request test accept-ca-certificate accept
% You have successfully generated the certificate.
Please check the certificates in the certificate list.
NetEye@root-system] end
NetEye@root> save config
```

3.30.4 范例：SNMP 管理

基本需求

当网络中已经部署了 SNMP 管理站，配置 NISG-IPS 的 SNMP 功能，使其可以被 SNMP 管理站管理。

组网拓扑



配置要点

- 配置 NISG-IPS 接口 IP 地址
- 在 NISG-IPS 上配置 SNMP 管理
- 配置 SNMP 管理站

配置步骤

配置 NISG-IPS 接口 IP 地址

1. 选择**网络 > 接口**。
2. 设置与管理站相连的接口的 IP 地址。
   - 接口名称：eth-s1p1
   - 模式：三层
   - IP 地址：（静态 IP） 10.1.3.110/24
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 10.1.3.110 255.255.255.0
NetEye@root-system-if-eth-s1p1] end
NetEye@root> save config
```

在 NISG-IPS 上配置 SNMP 管理

1. 选择**系统 > 服务配置 > SNMP 配置**。
2. 点击**是**按钮，开启 SNMP 管理功能，使用默认端口 161。
3. 配置只读团体字符串，以及物理位置和联系信息字符串。
   - 读写团体字符串：test
   - SNMP 物理位置字符串：shenyang
   - SNMP 联系信息字符串：nsd
4. 点击 **SNMP 用户列表**中的**新建**按钮，创建 SNMP 用户：
   - 名称：SNMPuser1
   - 权限：读写
   - 安全级别：认证并加密
   - 认证：12345678
   - 秘钥：87654321
5. 点击**确定**。
6. 点击  。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] snmp daemon on
NetEye@root-system] snmp community test read-only
NetEye@root-system] snmp location shenyang
NetEye@root-system] snmp contact nsd
NetEye@root-system] snmp usm user SNMPuser1 seclvl authPriv authpro
MD5 authpass phrase 12345678 privpro DES privpassphrase 87654321
read-write
NetEye@root-system] end
NetEye@root> save config
```

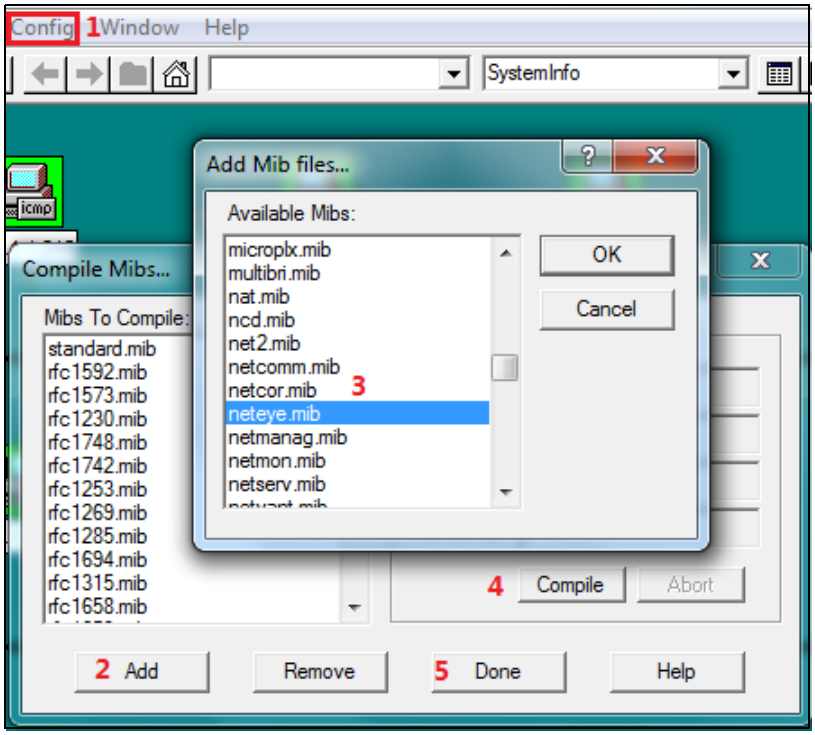
配置 SNMP 管理站

以下以 SNMPc Network Manager 软件为例，介绍 SNMP 管理站如何管理 NISG-IPS 设备。

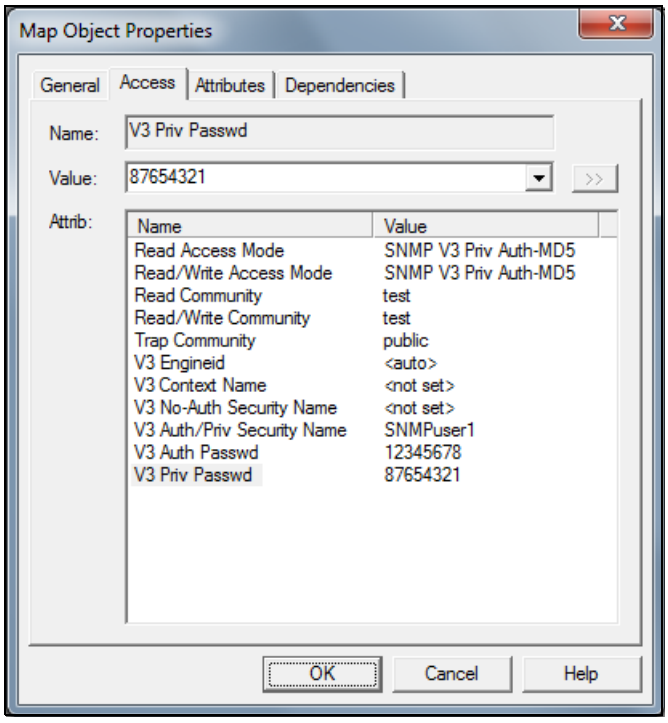
1. 在安装了SNMP管理软件的主机上，将NISG-IPS的MIB文件neteye.mib拷贝到SNMPc的安装路径下：SNMPc Network Manager\mibfiles。

   提示：关于如何获取 NISG-IPS 的 MIB 文件，请与技术支持工程师联系。

2. 选择**开始>程序> SNMPc Network Manager > Login Console**，打开SNMPc管理界面，输入用户名和密码登录。
3. 选择 **Config > Mib Database**，点击 **Add**，选中 neteye.mib，点击 **Compile**，编译完成后，点击 **Done**。

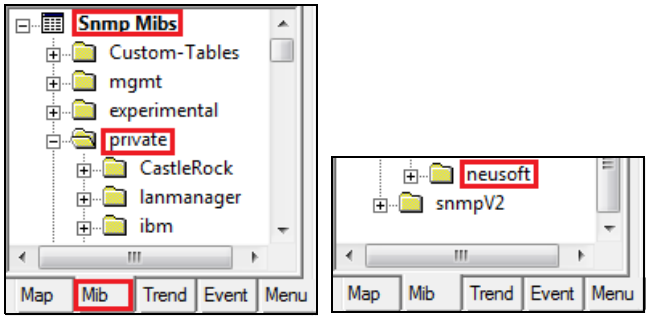


4. 打开左侧导航栏的 **Map** 页，找到 **Root Subnet** 下方的 10.1.3.110 节点，右键选择 **Properties**，点击 **Access**，设置各项数值（同 NISG-IPS 上的设置相匹配），点击 **OK**。

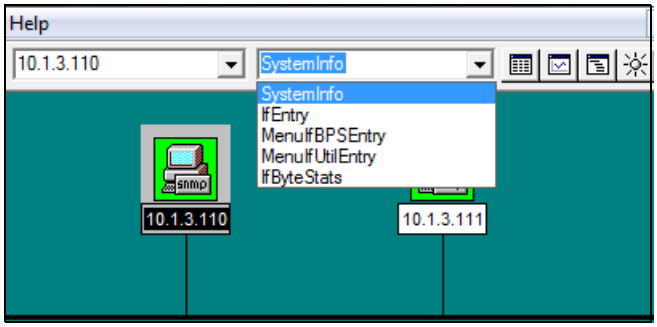


提示：由于 NISG-IPS 端启用了 SNMP 用户认证，这里需要选择 SNMPv3 并设置相应的认证和加密信息。

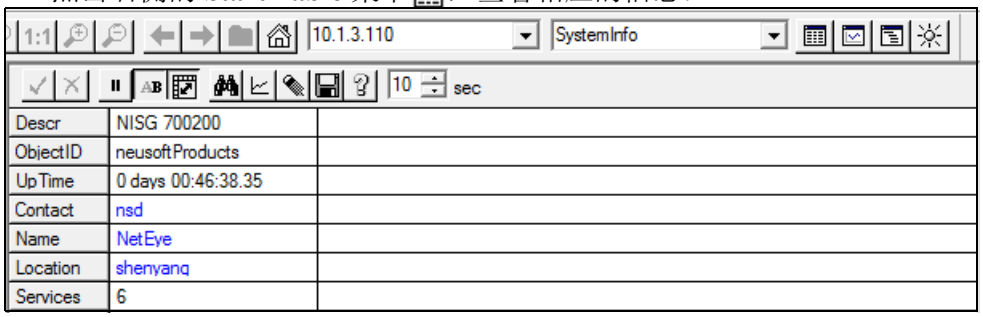
5. 打开左侧导航栏的 **Mib** 页，在 **Snmp Mibs > private** 节点下方，将出现一个 **neusoft** 子节点：



6. 在主菜单行的下拉框中选择NISG-IPS的IP地址，在右侧的下拉框中选择相应的选项：



7. 点击右侧的 **Start Table** 菜单，查看相应的信息：



8. 根据需要查看 NISG-IPS 的其他信息。

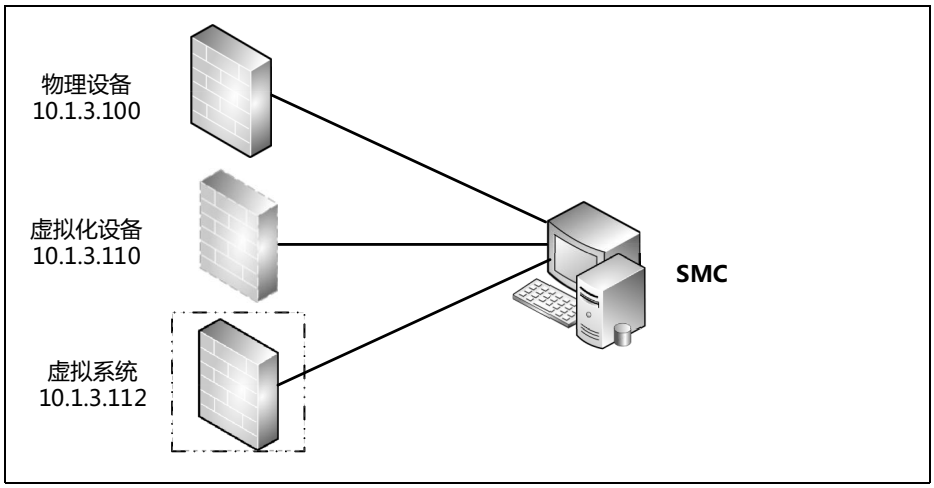
3.30.5 范例：SMC 管理

基本需求

网络中部署了多台 NISG-IPS 设备，需要统一管理和统一配置。此种情况下，可以使用东软 SMC 集中管理软件统一管理 NISG-IPS 设备，统一向 NISG-IPS 下发策略和 VPN 隧道配置，减轻管理员负担。

提示：SMC 可以管理多种形态的 NISG-IPS 设备，包括物理设备、虚拟化设备和虚拟系统。

组网拓扑



配置要点

- 在 NISG-IPS 上开启集中管理功能
- 在 SMC 设备上添加被管理设备

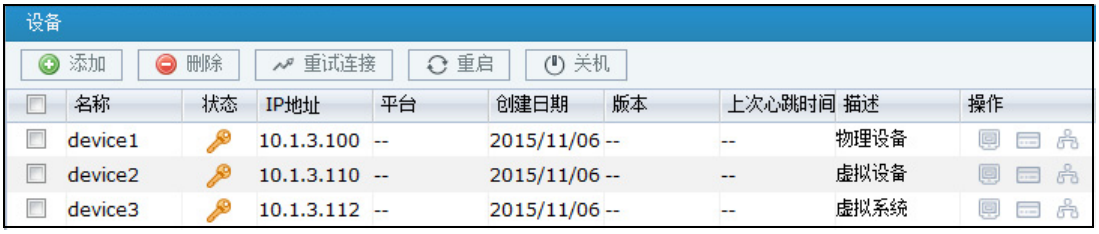
配置步骤

在 NISG-IPS 上开启集中管理功能

1. 以管理员身份登录 NISG-IPS。
2. 选择**系统** > **维护** > **集中管理**，开启集中管理功能，以使 NISG-IPS 接受 SMC 服务器的管理。
3. 点击**确定**。
4. 点击 。

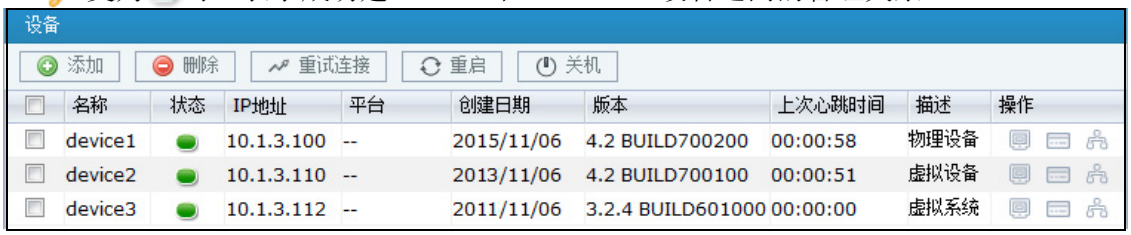
在 SMC 设备上添加被管理设备

1. 以超级管理员身份 （缺省用户名和密码：admin， neteyesmc）登录 SMC 设备。
2. 选择**设备管理 > 设备**，点击**添加**，添加要管理的 NISG-IPS 设备。
   - 名称：device1
   - IP 地址 / 域名：10.1.3.100
   - 端口：443
   - 用户名：admin （同被管理设备管理员名称）
   - 密码：（同被管理设备管理员密码）
   - 描述：物理设备
   - 收集报表数据：勾选
3. 添加更多被管理设备。



4. 如果SMC获取不到被管理NISG-IPS设备的信息，请检查被管理NISG-IPS设备的SMC功能是否已经开启；如果已经开启，双击被管理设备对应的🔑重新设置管理用户名和密码。

   🔑变为🟢时，表示成功建立 SMC 和 NISG-IPS 设备之间的管理关系。



验证结果

1. 在被管理 NISG-IPS 设备上选择**系统** > **维护** > **集中管理**。
2. 可以查看到 SMC 集中管理服务器的信息。

3.30.6 范例：本地查看报警日志

基本需求

本地查看 NISG-IPS 的报警日志。

配置要点

- 配置本地日志报警策略
- 本地查看报警日志

配置步骤

配置本地日志报警策略

1. 选择**系统** > **日志配置** > **报警配置**。
2. 点击本地日志策略 internal 对应的图标，设置本地报警策略。根据日志存储空间大小设置日志存储策略、开启相应的安全级别和日志类型。
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] alert-config local-syslog internal level any type any
NetEye@root-system] exit
NetEye@root> save config
```

本地查看报警日志

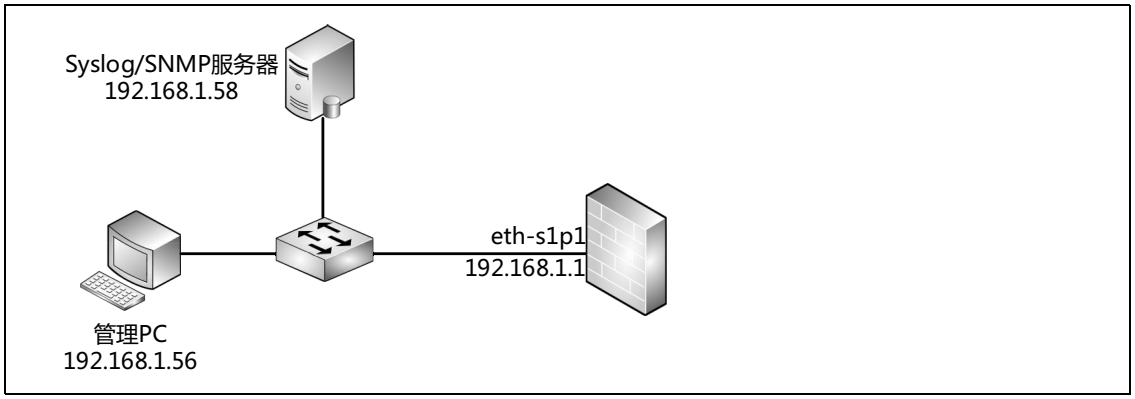
1. 选择**监控** > **报警 / 日志** > **系统日志**。
2. 点击**刷新**获取最新的系统日志信息。点击筛选日志信息。
3. 选择**监控** > **报警 / 日志** > **IPS 报警**，查看 IPS 报警信息。
4. 选择**监控** > **报警 / 日志** > **URL 过滤报警**，查看 URL 过滤报警信息。
5. 选择**监控** > **报警 / 日志** > **应用控制报警**，查看应用控制报警信息。
6. 选择**监控** > **流量统计数据**，查看应用排名和 URL 排名等信息。
7. 还可以选择**主页**，查看系统日志、应用排名和 URL 排名等信息。

3.30.7 范例：Syslog/SNMP 报警

基本需求

客户网络中通过 Syslog 服务器或 SNMP 服务器将所有安全设备的日志记录汇总，便于管理和查询。部署 NISG-IPS 设备后，需要配置 Syslog 或 SNMP 报警策略，允许 Syslog 服务器或 SNMP 服务器收集 NISG-IPS 的日志信息。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置日志报警策略
- 验证结果（采集日志）

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 设置接口 IP 地址。
   - 接口名称：eth-s1p1
   - 模式：三层
   - IP 地址：（静态 IP） 192.168.1.1/24
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] end
NetEye@root> save config
```

配置日志报警策略

1. 选择**系统 > 日志配置 > 报警配置**。
2. 点击**新建**，创建一条Syslog报警策略，允许IP地址为192.168.1.58的Syslog服务器可以实时获取 NISG-IPS 的日志信息。
   - 名称：syslog
   - Syslog 服务器：
     - IP 地址：192.168.1.58
     - 端口：514
   - 输出方式：完整输出
   - 语言：简体中文
   - 安全级别：全开
   - 类型：全开
3. 点击**确定**。
4. 点击**新建**，创建一条SNMP报警策略，允许IP地址为192.168.1.58的SNMP服务器可以通过 SNMPv2c 实时获取 NISG-IPS 的日志信息。
   - 名称：snmp
   - SNMP Trap 地址：
     - IP 地址：192.168.1.58
     - 版本：v2c

- 语言：简体中文
- 安全级别：全开
- 类型：全开

5. 点击**确定**。
6. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] alert-config syslog syslog server 192.168.1.58 514 level any type any language Chinese complete
NetEye@root-system] alert-config snmp-trap snmp v2c 192.168.1.58 level any type any language Chinese
NetEye@root-system] exit
NetEye@root> save config
```

验证结果 （采集日志）

在内网日志服务器上收集 NISG-IPS 报警日志信息：

1. 配置日志服务器的网关和 DNS 服务器地址如下：
   - IP 地址：192.168.1.56
   - 子网掩码：255.255.255.0
   - 默认网关：192.168.1.1
   - 首选 DNS 服务器：202.118.1.24
2. 打开 Syslog 服务器管理软件，获取 NISG-IPS 报警日志信息。

Date	Time	Priority	Hostname	Message
11-06-2015	12:08:19	Local7.Debug	192.168.1.1	community=NetEye enterprise=1.3.6.1.4.1.8596.0.206064000 uptime=11008611 agent_ip=192.168.1.58 version=Ver2 var01_oid=1.3.6.1.4.1.8596.1.206064000 var01_value="2015-11-07 04:08:19 root@NetEye [Informational] NAT->[NAT]:0 repeat:1 user[N/A] NAT转换前：192.168.1.58(56044)->202.118.1.24(53)，NAT转换后：202.204.1.6(64943)->202.118.1.24(53)，协议：UDP。"
11-06-2015	12:08:09	Local7.Debug	192.168.1.1	community=NetEye enterprise=1.3.6.1.4.1.8596.0.204400128 uptime=11007610 agent_ip=192.168.1.58 version=Ver2 var01_oid=1.3.6.1.4.1.8596.1.204400128 var01_value="2015-11-07 04:08:09 root@NetEye [Warning] System->[Update]:16128 repeat:1 user[admin] 防病毒规则库立即更新更新失败，当前版本为Anti-Virus:1.0.305，失败原因是网络连接失败。"

3. 打开 SNMP 服务器管理软件，获取 NISG-IPS 报警日志信息。

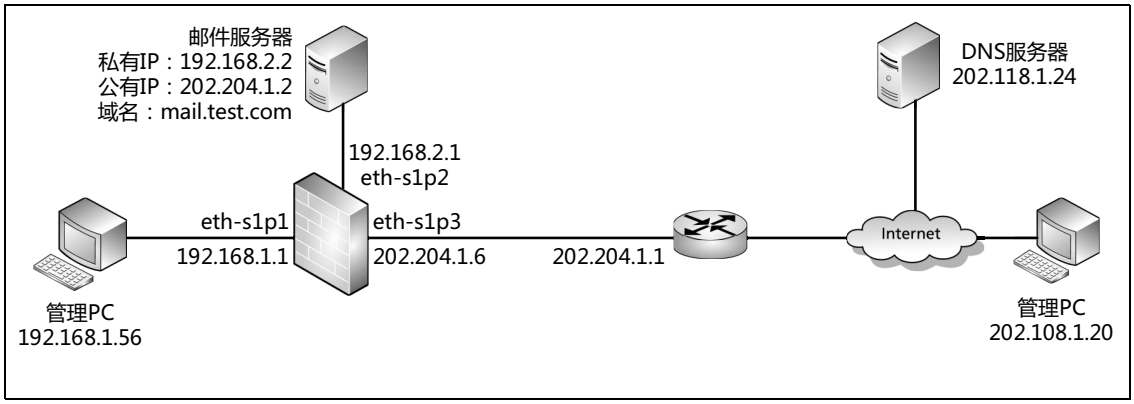
Date	Time	Priority	Hostname	Message
11-06-2015	12:05:24	Local7.Debug	192.168.1.1	community=NetEye enterprise=1.3.6.1.4.1.8596.0.206064000 uptime=10991110 agent_ip=192.168.1.58 version=Ver2 var01_oid=1.3.6.1.4.1.8596.1.206064000 var01_value="2015-11-07 04:05:24 root@NetEye [Informational] NAT->[NAT]:0 repeat:1 user[N/A] NAT转换前：192.168.1.58(52797)->202.118.1.24(53)，NAT转换后：202.204.1.6(64959)->202.118.1.24(53)，协议：UDP。"
11-06-2015	12:05:12	Local7.Debug	192.168.1.1	community=NetEye enterprise=1.3.6.1.4.1.8596.0.206064000 uptime=10989911 agent_ip=192.168.1.58 version=Ver2 var01_oid=1.3.6.1.4.1.8596.1.206064000 var01_value="2015-11-07 04:05:12 root@NetEye [Informational] NAT->[NAT]:0 repeat:1 user[N/A] NAT转换前：192.168.1.58(56703)->202.118.1.24(53)，NAT转换后：202.204.1.6(64960)->202.118.1.24(53)，协议：UDP。"
11-06-2015	12:05:07	Local7.Debug	192.168.1.1	community=NetEye enterprise=1.3.6.1.4.1.8596.0.204407296 uptime=10989447 agent_ip=192.168.1.58 version=Ver2 var01_oid=1.3.6.1.4.1.8596.1.204407296 var01_value="2015-11-07 04:05:07 root@NetEye [Warning] System->[Update]:23296 repeat:1 user[admin] 系统查询升级包更新失败，当前版本为4.2 BUILD700200，失败原因是网络连接失败。"

3.30.8 范例：邮件报警

基本需求

允许管理用户在任意位置通过邮件接收 NISG-IPS 报警日志。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置路由
- 配置访问策略
- 配置 SNAT 规则
- 配置 DNAT 规则
- 配置日志报警策略
- 验证结果 （收取日志邮件）

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 设置接口 IP 地址。
   - eth-s1p1：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.2.1/24
   - eth-s1p3：
     - 模式：三层
     - IP 地址：（静态 IP） 202.204.1.6/24
3. 点击  。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet eth-s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 202.204.1.6 255.255.255.0
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

配置路由

1. 选择**网络 > 路由 > 缺省路由**。
2. 点击缺省路由条目对应的，修改网关地址为 202.204.1.1。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route default gateway 202.204.1.1 1
NetEye@root-system] exit
NetEye@root> save config
```

配置访问策略

1. 选择**防火墙 > 访问策略**。
2. 点击**新建**，创建两条访问策略：
   - policy1：允许内网管理 PC 访问外网 DNS 服务器。
     - 源 IP 地址：192.168.1.0/24
     - 目的 IP 地址：任意
     - 服务：任意
     - 动作：允许
   - policy2：允许外网管理 PC 访问内网邮件服务器 （192.168.2.2）。
     - 源 IP 地址：任意
     - 目的 IP 地址：192.168.2.2
     - 服务：服务 =TCP ； 源端口 =1-65535 ； 目的端口 =25&110
     - 动作：允许
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access policy1 any 192.168.1.0/24 any any
any any permit enable 1
NetEye@root-system] policy access policy2 any any any 192.168.2.2 tcp
1-65535 25 any permit enable 2
NetEye@root-system] policy access policy2 protocol tcp 1-65535 110
NetEye@root-system] exit
NetEye@root> save config
```

配置 SNAT 规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建一条 SNAT 规则，使内网管理 PC 可以访问外网 DNS 服务器。
   - 名称：snat1
   - 启用：勾选
   - NAPT：勾选
   - 源 IP 地址：192.168.1.0/24
   - 转换后接口：eth-sp1p3
   - 入口接口：eth-s1p1
   - 出口接口：eth-s1p3
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy snat snat1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p3 napt enable
NetEye@root-system] policy snat snat1 matching input-interface eth-
s1p1
NetEye@root-system] policy snat snat1 matching output-interface eth-
s1p3
NetEye@root-system] policy snat snat1 matching dip any
NetEye@root-system] exit
NetEye@root> save config
```

配置 DNAT 规则

1. 选择**网络** > **地址转换** > **目的地址转换**。
2. 点击**新建**，创建两条 DNAT 规则：
   - dnat1：使内网管理 PC 可以通过内网邮件服务器收取报警邮件 （允许客户端通过域名访问邮件服务器）。
     - 序号：1
     - 启用：勾选
     - NAPT：不勾选
     - 目的 IP 地址：
       - IP 地址：202.204.1.2
       - 域名：mail.test.com
     - 转换后 IP 地址：192.168.2.2
     - 入口接口：eth-s1p1

- dnat2：使外网管理 PC 可以通过内网邮件服务器收取报警邮件。
  - 序号：2
  - 启用：勾选
  - NAPT：不勾选
  - 目的 IP 地址：
    - IP 地址：202.204.1.2
  - 转换后 IP 地址：192.168.2.2
  - 入口接口：eth-s1p3

3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy dnat dnat1 202.204.1.2 domain mail.test.com 192.168.2.2 enable 1
NetEye@root-system] policy dnat dnat1 matching input-interface eth-s1p1
NetEye@root-system] policy dnat dnat4 202.204.1.2 192.168.2.2 enable 2
NetEye@root-system] policy dnat dnat2 matching input-interface eth-s1p3
NetEye@root-system] exit
NetEye@root> save config
```

配置日志报警策略

1. 选择**系统** > **日志配置** > **报警配置**。
2. 点击**新建**，创建一条邮件报警策略，允许管理员 admin@test.com 在任意位置 （内网或外网）通过邮件实时获取 NISG-IPS 的日志信息。
   - 名称：mailAlert
   - 语言：简体中文
   - 邮件服务器：
     - 地址：192.168.1.58
     - 端口：25
     - 发送间隔：300 秒
     - 主题：Syslog
     - 发件人：syslog@test.com
     - 身份认证：（邮件服务器要求进行身份认证时才需要填写此项）
       - 账号：syslog@test.com
       - 密码：123
   - 收件人：admin@test.com （可以填写多个收件人）
   - 安全级别：全开
   - 类型：全开

3. 点击**确定**。
4. 点击 。

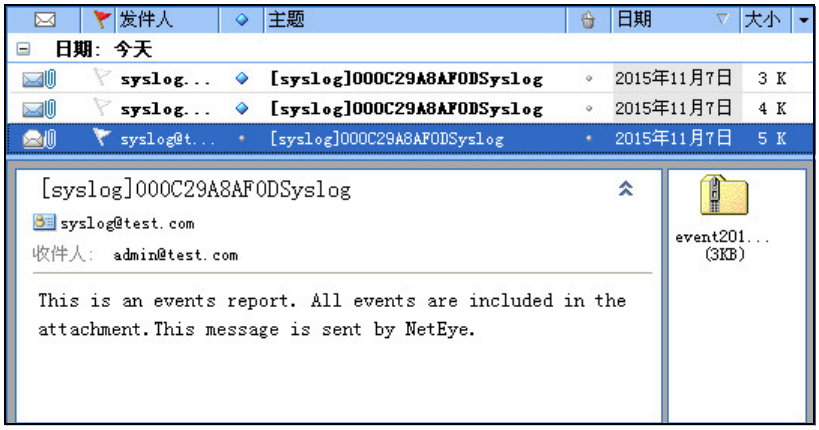
CLI

```
NetEye@root> configure mode override
NetEye@root-system] alert-config syslog syslog server 192.168.1.58 514 level any type any language Chinese complete
NetEye@root-system] alert-config snmp-trap snmp v2c 192.168.1.58 level any type any language Chinese
NetEye@root-system] alert-config mail mailAlert server 192.168.2.2 25 sender syslog@test.com user syslog@test.com password simple 123 subscriber admin@test.com interval 300 level any type any language Chinese subject Syslog
NetEye@root-system] exit
NetEye@root> save config
```

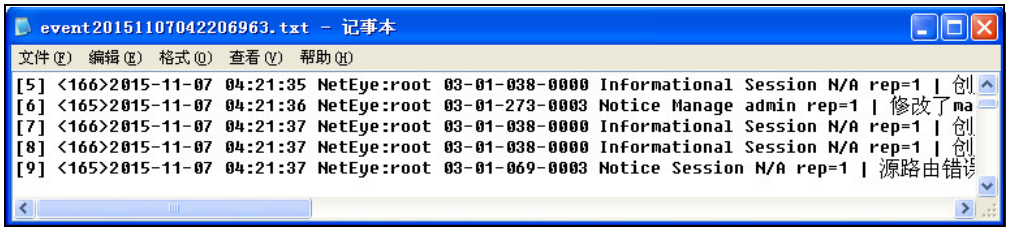
验证结果 （收取日志邮件）

在内网管理 PC 上收取 NISG-IPS 报警日志邮件：

1. 配置内网管理 PC 的 DNS 服务器地址为 202.118.1.24。
2. 配置邮件客户端如下：
   - 发送邮件服务器 (SMTP)：mail.test.com
     - SMTP 服务器需要身份验证：勾选
   - 接收邮件服务器 （POP3）：mail.test.com
   - POP3 邮件帐号：admin
   - 密码：123
3. 收取 NISG-IPS 报警日志邮件：



4. 打开附件查看具体的日志信息。



在外网管理 PC 上收取 NISG-IPS 报警日志邮件：

1. 配置外网管理 PC 的 DNS 服务器地址为 202.118.1.24。
2. 配置邮件客户端如下：
   - 发送邮件服务器 (SMTP)：mail.test.com
     - SMTP 服务器需要身份验证：勾选
   - 接收邮件服务器 （POP3）：mail.test.com
   - POP3 邮件帐号：admin
   - 密码：123
3. 收取 NISG-IPS 报警日志邮件。
4. 打开附件查看具体的日志信息。

3.30.9 范例：系统在线升级

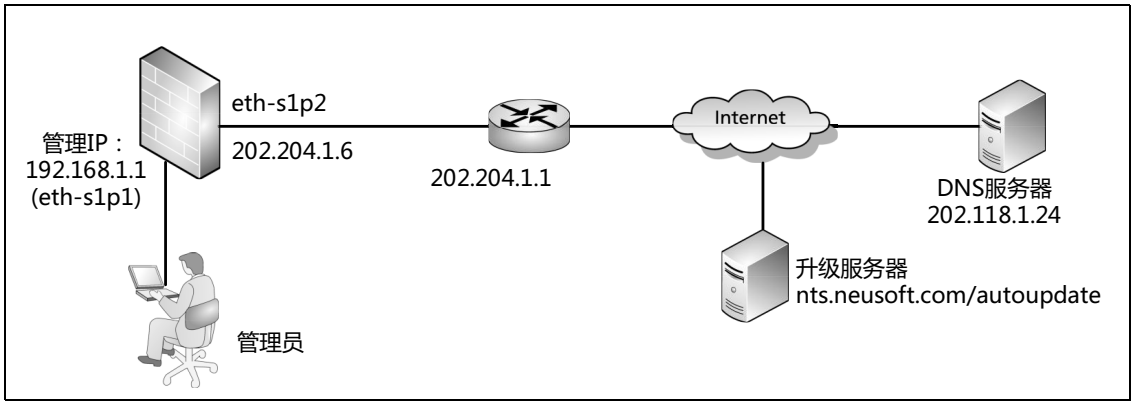
基本需求

在 NISG-IPS 设备联网情况下自动升级系统。

注意事项：

- 升级前必须准备配置线，以防在升级失败后能及时处理。
- 升级过程中请不要切换到其他界面，更不能断电或重启设备。
- 系统升级可能会造成网络中断，请避开业务高峰期执行升级操作。
- 有些系统升级包需要重启系统才能生效，执行升级操作前请保存系统配置。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置网关
- 配置 DNS 主机
- 在线升级系统
- 查看系统升级结果

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 设置接口 IP 地址。
   - eth-s1p1：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - IP 地址：（静态 IP） 202.204.1.6/24
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.204.1.6 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

配置网关

1. 选择**网络 > 路由 > 缺省路由**。
2. 点击缺省路由条目对应的，修改网关地址为 202.204.1.1，使 NISG-IPS 可以访问外网。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route default gateway 202.204.1.1 1
NetEye@root-system] exit
NetEye@root> save config
```

配置 DNS 主机

1. 选择**网络** > **DNS** > **主机**。
2. 设置 DNS 主机地址 202.118.1.24，使 NISG-IPS 可以访问升级服务器的域名地址。
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] dns host 202.118.1.24 primary
NetEye@root-system] exit
NetEye@root> save config
```

在线升级系统

1. 选择**系统** > **系统升级** > **安装升级包**。
2. 点击**立即更新**。
3. 根据提示点击**是**和**确定**，完成升级操作。

提示：有些系统升级包需要重启系统。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] package upgrade immediately
NetEye@root-system] exit
NetEye@root> save config
```

查看系统升级结果

1. 选择**系统** > **系统升级** > **安装升级包**。
2. 在**更新信息**区域查看升级结果信息。

CLI

```
NetEye@root> show system info
Build:                BUILD700201
```

3.30.10 范例：手动升级系统

基本需求

在 NISG-IPS 设备未联网或网络故障的情况下手动升级系统。

配置要点

- 获取系统升级包
- 手动上传系统升级包

配置步骤

获取系统升级包

1. 在管理 PC 的浏览器中输入 https://nts.neusoft.com/，按 Enter 键访问升级服务器。
2. 点击**登录**菜单进入登录页面。输入用户名、密码以及验证码，点击**登录**按钮，登录升级服务器。
3. 点击**下载中心**菜单，可以看到所有可用的系统升级包。
4. 点击要下载的升级包对应的**了解更多**链接，打开详细信息页面。点击**升级包下载**，下载当前升级包到本地。

提示：如果无法访问系统升级服务器，请联系技术支持工程师获取升级包文件。

手动上传系统升级包

1. 选择**系统** > **系统升级** > **安装升级包**。
2. 点击**上载升级包**，选择要上传的系统升级包。
3. 根据提示点击**确定**，完成升级操作。

提示：有些系统升级包需要重启系统才能生效。

CLI

提示：需要使用 SSH 软件 （如 SecureCRT）登录 CLI 上传升级包。

```
NetEye@root> configure mode override
NetEye@root-system] package upgrade from x/zmodem
```

查看系统升级结果

1. 选择**系统** > **系统升级 > 安装升级包**。
2. 在**更新信息**区域查看升级结果信息。

CLI

```
NetEye@root> show system info
Build:                    BUILD700201
```

4 网络配置

本章介绍网络配置的相关内容，包括：

4.1 接口

本节包括：

4.1.1 接口类型

NISG-IPS 的接口分为物理接口和逻辑接口。以太网接口为物理接口，其他接口均为逻辑接口。根据 OSI 网络模型的工作层次， NISG-IPS 的接口又可分为二层接口和三层接口。

下表列出 NISG-IPS 支持的所有接口的类型、每类接口的工作模式和 NISG-IPS 最多支持的逻辑接口数量：

表 90 接口类型

类型 / 数量	工作模式	说明
以太网接口	二层 三层 共享三层	用于接收和发送数据包。以太网接口的数量取决于 NISG-IPS 设备的机型。 NISG-IPS 提供接口卡槽位。可以在槽位插入接口卡，每个接口卡最多支持 8 个以太网接口。NISG-IPS 不支持热插拔功能。 管理接口是三层以太网接口，不转发数据，也不能被划分到任何安全域中。管理接口应用于如下：系统升级， Telnet、 SSH、 Web 和 Ping 访问控制， SNMP、接口 WebAuth 认证、外部服务器认证和 NTP 校时，发送 Syslog、报警邮件和 SNMP Trap 报警信息，与 SMC 服务器通讯。 NISG-IPS 支持两种类型的管理接口： • 带外管理口：部分机型的 NISG-IPS 设备会提供一个带外管理口。此接口名称为 “mgt”，缺省 IP 地址为 192.168.1.100/24。带外管理口是专门用于管理 NISG-IPS 的以太网接口，只能工作在三层模式，不可被创建或删除。管理员只能手动为此接口配置 IP 地址且最多能够添加 32 个 IPv4 地址和 32 个 IPv6 地址 （包括 1 个链路本地地址和 31 个全球单播地址）。 • 专用管理口：可以将三层以太网接口设置为管理接口 （以 “M” 标识）。当接口的工作模式或所属的 Vsys 改变时，该接口将自动转变为普通接口，可以进行数据转发。 通过专用管理口访问 NISG-IPS 时，受访问控制策略的限制。请参见 3.12 访问设置。
以太网通道 / 8 个	二层 三层 共享三层	多个以太网接口通过使用同一个 MAC 地址来扮演一个以太网通道的角色，可以增加带宽、提高容错能力。 • 以太网通道的传输速率是所包含的以太网接口的传输速率的总和。 • 当某一以太网接口出现故障时，其他以太网接口将继续转发数据包。
冗余接口 / 4 个	二层 三层 共享三层	两个二层以太网接口作为一个逻辑接口使用，实现了接口级的高可靠性。 • 主接口：承担所有流量。 • 备用接口：没有流量通过。当主接口发生故障时，备用接口自动成为主接口并接管流量。 当其中一个成员以太网接口被删除时，另外一个也会自动被删除。
虚拟接口 / 1023 个	二层 三层	用于连接不同的虚拟网络，使 Vsys 之间不必依赖以太网接口，就可以互相通信。更多信息，请参见 15.1.2 虚拟网络 （Vnet）。
VLAN 接口 / 4094 个	三层	VLAN （虚拟局域网）是将网络中的主机逻辑划分到一个广播域，而不关注这些主机的物理位置。 VLAN 接口实际就是一个包含二层接口的 VLAN。同一个 VLAN 内的成员通过二层交换模式直接通信，不同 VLAN 之间的成员则通过三层路由模式通信。

表 90 接口类型 (*续*)

类型 / 数量	工作模式	说明
环回接口 / 1023 个	三层	其链路状态永远处于已连接 （Up）状态，除非接口状态被禁用或 NISG-IPS 被关闭。 • 可以利用环回接口的链路状态来探测设备状态。例如，网络管理站可以使用 SNMP 协议，获取 NISG-IPS 的状态信息和监控信息。更多信息，请参见 3.14 SNMP。 • 当为环回接口正确配置了 IP 地址和相应路由信息后，可通过此 IP 地址对 NISG-IPS 进行管理。 • 通过环回接口的数据访问受访问控制策略的限制。
PPPoE 接口 / 8 个	三层	必须绑定一个二层以太网接口或者二层冗余接口。 NISG-IPS 可充当 PPPoE 客户端，通过 PPPoE 拨号功能，与 ISP 之间建立 PPP 连接。 NISG-IPS 支持两种 PPPoE 协议：基于 IPv4 的 PPPoEv4 和基于 IPv6 的 PPPoEv6。 PPPoE 接口可作为 PPPoEv6 的客户端，通过 DHCPv6-PD （前缀分配）功能获得前缀信息，形成 PPPoE 接口的 IPv6 地址。 同一个二层以太网接口或二层冗余接口可以同时用于 PPPoEv4 接口和 PPPoEv6 接口。 关于 PPPoE 接口的配置信息，请参见表 106 PPPoE 接口属性。
隧道接口	三层	不可以手动创建或删除隧道接口。在创建 IPSec VPN 隧道、 SSL VPN 和 GRE 隧道时，隧道接口自动被创建，用于建立 VPN 通信。当隧道被删除时，其关联的隧道接口也被删除。 • 在为隧道接口配置了静态 IP 地址后，系统将自动添加以该隧道接口为出口的直连路由，用于将数据流引入到对应的 IPSec、 SSL VPN 或 GRE 隧道中。 • 隧道接口可以借用其他三层或共享三层接口的 IP 地址作为自己的地址，既能完成隧道接口的路由交换，又能节省 IP 地址资源。 • 隧道接口不支持 IPv6 配置。 管理员可以为隧道接口配置静态 IP 地址，请参见表 108 隧道接口属性。更多信息，请参见第 13 章，虚拟专用网。

管理员可以将所有三层或共享三层接口 （除了环回接口和隧道接口）划分到虚拟系统中。

4.1.2 工作模式

接口的工作模式分为二层和三层。除了虚拟接口外，其他二层接口又有以下两种工作模式：

- Access（缺省模式）：工作在 Access 模式的接口是交换端口，负责二层数据交换，并通常作为接入端口，用来连接终端设备。处于 Access 模式下的接口可以被划分到一个 VLAN 中，且不能自动识别 802.1Q 数据包。
- Trunk：通过将二层接口设置为 Trunk 模式的接口 （即 Trunk 端口），可以实现多个 VLAN 在同一条链路上复用。 Trunk 模式一般应用于内网接口数量较少的情形。

  NISG-IPS 的 Trunk 端口采用 IEEE802.1Q 协议封装。管理员可以配置 Trunk 端口的 Native VLAN，以接收非 802.1Q 格式的数据包；否则未经 IEEE802.1Q 封装的数据包将被丢弃。

4.1.3 接口属性

接口具有一些通用属性，如接口名称、链路状态。此外，二层接口和三层接口还分别具有一些特有的属性。

4.1.3.1 通用属性

表 91 通用属性

配置信息	说明
接口	指接口的名称。每类接口都有相应的命名规范，不可以修改。如：以太网接口 eth-s1p2，以太网通道 ch1。
链路状态	指接口的链路状态。 • **绿色图标**：表示已连接，且链路协商成功。 • **红色图标**：表示已断开。 环回接口的链路状态永远是已连接的。
接口状态	指接口的活动状态。管理员可以手动激活或禁用接口 （除隧道接口）。 • **绿色图标 （开）**：表示接口已激活。 • **灰色图标 （关）**：表示接口已禁用。 隧道接口的活动状态由对应的隧道状态决定。
模式	接口的工作模式，包括： • **二层**：可以将二层接口设置为二层 Access 模式或 Trunk 模式。 • **三层**：可以为三层接口配置 MTU 值和 IP 地址信息。 • **共享三层**：可以将以太网接口、以太网通道和冗余接口设置为此模式。共享三层接口可被划分到多个虚拟系统中；一般应用于外网接口数量较少的情形。共享三层接口缺省不属于任何虚拟系统 （包括根系统）。关于共享三层接口在虚拟系统中的应用，请参见 15.5.1 范例：基于三层共享接口的多 Vsys 应用。
NIC 模式	包括三个属性，仅有以太网接口具有这些属性。 • **链路速率**：指接口的数据传输效率，包括 10 Mbps、 100 Mbps、 1000 Mbps 和自动四种模式。自动模式是指 NISG-IPS 根据实际情况自动调节接口的数据传输速率。 • **双工**：指接口的双工模式，包括如下三种： •**全双工**：同时发送和接收数据。 •**半双工**：同一时刻只能接收数据或发送数据。 •**自动**：自动协商双工模式。 • **流量控制**：指对接口流量的控制。当接口发生拥塞不能再接收数据包时， NISG-IPS 将通知接口的对端设备。对端设备收到信息后停止向该接口发送数据包，直到拥塞消失后再继续传输数据。**开**指该功能已启用，**关**指该功能已禁用。
MAC 地址	指接口的 MAC 地址。隧道接口、环回接口和 PPPoE 接口没有 MAC 地址。
引用	指引用相应接口的条目列表。引用中的接口不能被删除；要删除该接口，需要首先解除引用关系。
使用特定 MAC 地址	勾选该复选框，手动指定 MAC 地址。环回接口、隧道接口、虚拟接口和 PPPoE 接口不具有该属性。
连接到虚拟网络	指虚拟接口连接的虚拟网络。仅有虚拟接口具有此属性。
描述	接口的描述信息。为 0 ～ 255 个字节的 UTF-8 字符，不包含：?'\"<>&。

4.1.3.2 二层特有属性

表 92 二层特有属性

配置信息	说明
属于	指二层接口所属的 VLAN 接口、以太网通道或冗余接口。
二层高级设置	指二层接口的工作模式，分为 Access 模式 （缺省模式）和 Trunk 模式。 • 当接口工作在 Access 模式下，可将该接口划分到某个 VLAN 中，或者不属于任何 VLAN。 • 当接口工作在 Trunk 模式下，可配置该 Trunk 所允许的 VLAN 和它的 Native VLAN。

4.1.3.3 三层特有属性

表 93 三层特有属性

配置信息	说明
MTU	指最大传输单元 （Maximum Transmission Unit），单位为字节。三层接口的 MTU 只对出口接口的数据包起作用，即当数据包的长度大于三层接口的 MTU 时，在出口接口进行分片操作。 MTU 取值范围如下： • 在 IPv4 中，环回接口的为 68 ～ 65535， PPPoE 接口的为 68 ～ 1492，其他接口的为 68 ～ 1500。 • 在 IPv6 中，环回接口的为 1280 ～ 65535， PPPoE 接口的为 1280 ～ 1492，其他接口的为 1280 ～ 1500。 PPPoE 的 MTU 缺省为 1454 字节，其他三层接口的 MTU 缺省为 1500 字节。
二层接口列表	可以将二层 Access 模式的以太网接口、以太网通道、冗余接口以及虚拟接口划分到 VLAN 接口中或将二层以太网接口划分到以太网通道中。仅 VLAN 接口和以太网通道具有该属性。
IP 地址	三层接口的 IP 地址。可以为接口设置 IPv4 和 IPv6 地址。 IPv4 地址可以通过以下两种方式获取： • **静态 IP**：手动配置三层接口的 IP 地址和掩码长度。最多可以添加 32 个 IPv4 地址。主地址表示该接口的主 IP 地址。 • **DHCP**：从 DHCP 服务器上获得动态分配的 IP 地址。可以设置是否启用 DNS 代理。如果启用，系统将根据该接口通过 DHCP 方式获得的 DNS 服务器 IP 地址自动添加为代理。 勾选**启用 IPv6**，配置 IPv6 地址： • **链路本地地址**：包括自动生成 （缺省方式）和手动指定两种方式。 当勾选**自动配置链路本地地址**时， NISG-IPS 根据链路本地地址前缀及接口的 MAC 地址，自动为该接口生成链路本地地址。当取消勾选**自动配置链路本地地址**时，可以手动配置地址。 • **ULA 或全球单播地址**：当勾选**无状态自动配置**时，表示采用无状态自动配置方式。当取消勾选**无状态自动配置**时，表示采用手动配置方式 （缺省方式），需要在 **IP 地址列表**中配置 IPv6 地址。最多可以向列表中添加 31 个 IPv6 全球单播地址。 **类型**：表示手动配置 ULA 或全球单播地址的类型，包括手动和 EUI-64。 当指定**手动**时，表示不使用 EUI-64 格式的接口标识；当指定 **EUI-64** 时，表示使用 EUI-64 格式的接口标识。 **状态**：表示 IPv6 地址的状态，包括临时地址 （TENTATIVE）、重复地址 （DUPLICATE）、首选地址 （PREFERRED）、不推荐地址 （DEPRECATED）以及无效地址 （INVALID）。
IP 探测	用于探测 IP 地址。仅有冗余接口具有该属性。 • **IPv4 探测类型**：包括 None （不进行探测）， Ping 和 ARP Ping。 • **IPv6 探测类型**：包括 None （不进行探测）， Ping 和 NS Ping。 • **等待时间**：冗余接口恢复故障的时间。

4.1.4 配置接口

本节介绍如何配置每种类型的接口，包括：

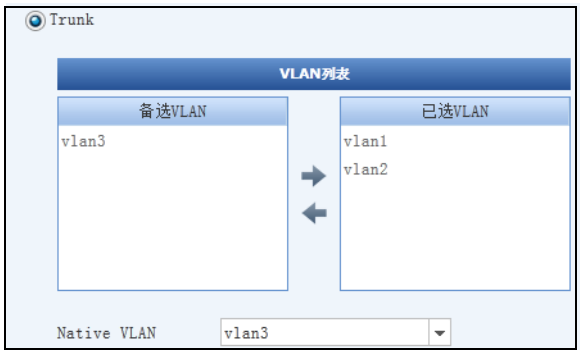
4.1.4.1 配置以太网接口

4.1.4.1.1 二层接口

1. 选择**网络** > **接口**。点击以太网接口所对应的 。
2. 将接口的工作模式设置为**二层**。

   - 将接口设置为 Access 模式，并将其划分到 VLAN 接口中。

   - 将接口设置为 Trunk 模式。在 **VLAN 列表**中选择允许的 VLAN，在 **Native VLAN** 下拉框中选择 Native VLAN。



3. 在**高级设置**区域，配置 NIC 模式。**使用特定 MAC 地址**功能对二层接口无效。
4. 点击**确定**。
5. 点击 。

表 94 二层以太网接口命令

interface ethernet *interface_id*	进入指定的以太网接口配置模式。
working-type layer2-interface	设置接口为二层工作模式。
shutdown	禁用接口。
unset shutdown	启用接口。
port mode {**access** | **trunk**}	设置二层接口 （虚拟接口除外）的工作模式。
port access vlan *vlan_id*	将二层接口划分到指定 VLAN 接口中。
unset port access vlan	删除二层接口所隶属的 VLAN 接口。
port trunk allowed vlan	设置指定 Trunk 端口所允许的 VLAN，即对允许的 VLAN 中的数据进行 802.1Q 封装。
unset port trunk allowed vlan	删除指定 Trunk 端口所允许的 VLAN。
port trunk native vlan *vlan_id*	设置指定 Trunk 端口所允许的 Native VLAN。即不对该 VLAN 中的数据进行 802.1Q 封装。
unset port trunk native	删除指定 Trunk 端口所允许的 Native VLAN。
hold ethernet *interface_id*	设置隶属于以太网通道的二层以太网接口。
unset hold ethernet *interface_id*	删除隶属于以太网通道的二层以太网接口。

4.1.4.1.2 三层接口

1. 选择**网络** > **接口**。点击以太网接口所对应的 。
2. 将接口的工作模式设置为**三层**。勾选**专用管理口**，可以将接口设置为专用管理接口。
3. 修改 MTU 值。

4. 为接口配置 IPv4 地址。
   - **静态 IP**：手动配置 IP 地址和掩码长度。**主**表示该地址作为主地址，优先被使用。最多能够配置 32 个 IPv4 地址。

   - **DHCP**：NISG-IPS 作为 DHCP 客户端从 DHCP 服务器自动获取 IP 地址。

     勾选**启用 DNS 代理**，可以为 DHCP 客户端接口自动添加 DNS 代理。点击**使用 DHCP 更新 IP 地址**，可以更新已获取的 IP 地址。

5. 勾选**启用 IPv6**，为接口配置 IPv6 地址。

   - 缺省情况下，链路本地地址为自动生成。取消勾选**自动配置链路本地地址**，可指定链路本地地址。
   - NISG-IPS 支持同时进行 IPv6 地址的自动配置和手动配置。勾选**无状态自动配置**，可以通过无状态地址自动配置的方式自动生成 IPv6 地址。在 **IPv6 地址列表**中，可以手动配置 IPv6 地址。一个接口最多支持 31 个全球单播地址。

6. 在**高级设置**区域，配置 MAC 地址和 NIC 模式。
7. 点击**确定**。
8. 点击。

提示：选择**网络 > 接口**。点击 “mgt” 对应的，对带外管理口进行设置，配置操作与以太网接口操作类似。

表 95 三层以太网接口命令

working-type layer3-interface	设置接口为三层工作模式。
management-only	设置三层以太网接口为专用管理口。
unset management-only	取消设置三层以太网接口为专用管理口。
mtu {*mtu_value* | **default**}	设置三层或共享三层接口的 MTU。
ip address *ipv4 netmask* [**secondary**]	为指定的三层或共享三层接口添加 IPv4 地址。
unset ip address [*ipv4*]	删除指定三层或共享三层接口的 IPv4 地址。
dhcp client	在三层或共享三层接口上启用 DHCP 客户端。该接口会通过 DHCP 服务器自动获得动态 IP 地址。
unset dhcp client	删除 DHCP 客户端的设置。
dhcp update ip address	重新获得动态 IP 地址。
dhcp enable-dns-proxy	启用为 IPv4 工作模式的 DHCP 客户端接口自动添加 DNS 代理的功能。
unset dhcp enable-dns-proxy	禁用为工作在 IPv4 模式的 DHCP 客户端接口自动添加 DNS 代理功能。
ipv6 enable	启用指定三层或共享三层接口的 IPv6 功能。
unset ipv6 enable	禁用指定三层或共享三层接口的 IPv6 功能。
ipv6 address {*ipv6* | **auto**} **link-local**	为指定的三层或共享三层接口设置链路本地地址。
ipv6 address autoconfig	启用指定三层或共享三层接口的无状态地址自动配置功能。
unset ipv6 address autoconfig	禁用指定三层或共享三层接口的无状态地址自动配置功能。
ipv6 address {*ipv6* | *ipv6/prefix*} [**eui-64**]	为指定的三层或共享三层接口手动添加 ULA 地址和全球单播地址。
unset ipv6 address	删除指定三层或共享三层接口的 ULA 地址和全球单播地址。
default mac	获取以太网接口、以太网通道、 VLAN 或冗余接口的缺省 MAC 地址。
mac address *mac_address*	修改以太网接口、以太网通道、 VLAN 或冗余接口的 MAC 地址。
show interface [**brief**]	显示所有接口信息。
show interface ethernet [*interface_id* | **brief**]	显示以太网接口信息。

4.1.4.1.3 共享三层接口

只有将接口划分到 Vsys 后，才可以为其添加地址。

1. 选择**网络** > **接口**。点击以太网接口所对应的 。
2. 将接口的工作模式设置为**共享三层**。

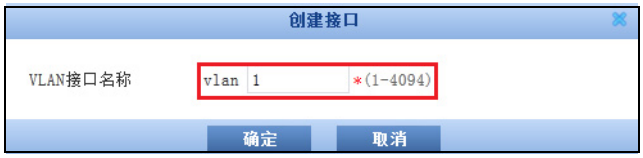
3. 点击**高级设置**，配置 NIC 模式。
4. 点击**确定**。
5. 选择**系统** > **虚拟系统** > **虚拟系统**。将接口分配给选定的虚拟系统并配置 IP 地址。更多信息参见 15 虚拟系统。
6. 点击 。

表 96 共享三层以太网接口命令

working-type layer3-shared-interface	设置接口为共享三层工作模式。
speed {10 | 100 | 1000 | auto} duplex {half | full | auto}	设置接口的链路速率和双工模式。
flow control {on | off}	启用或禁用接口的流量控制功能。

4.1.4.2 配置 VLAN 接口

1. 选择**网络** > **接口**。点击**新建**，选择 **VLAN**，创建 VLAN 接口。



2. 点击**确定**。
3. 点击 vlan1 对应的，为其分配未使用的二层接口。

4. 配置 IPv4 地址和 IPv6 地址。配置方式同以太网接口，详见 4.1.4.1.2 三层接口。
5. 在**高级设置**区域，如果不使用缺省的 MAC 地址，可以手动配置 MAC 地址。
6. 点击**确定**。
7. 点击。

表 97 VLAN 接口命令

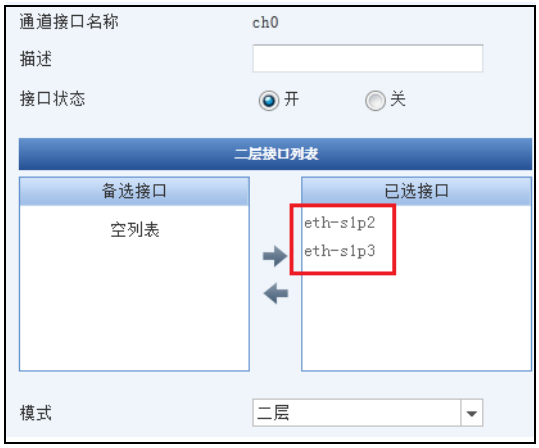
vlan *vlan_id*	创建 VLAN 或进入指定的 VLAN 配置模式。
unset vlan *vlan_id*	删除指定的 VLAN。
show interface vlan [*vlan_id* | **brief**]	显示 VLAN 信息。
shutdown	禁用接口。
unset shutdown	启用接口。
hold ethernet, channel, rint, veth	设置隶属于 VLAN 的二层接口。
unset hold ethernet, channel, rint, veth	删除隶属于 VLAN 的二层接口。
mtu {*mtu_value* | **default**}	设置三层或共享三层接口的 MTU。
default mac	获取 VLAN 接口的缺省 MAC 地址。
mac address *mac_address*	修改 VLAN 接口的 MAC 地址。

关于 IPv4 和 IPv6 的 CLI 配置，参见表 95 三层以太网接口命令。

4.1.4.3 配置以太网通道

1. 选择**网络** > **接口**。点击**新建**，选择 **Channel**，创建以太网通道。

2. 点击**确定**。
3. 点击以太网通道 ch0 所对应的，为其分配未使用的二层以太网接口。



4. 将以太网通道的工作模式设置为二层、三层或共享三层。见 4.1.4.1 配置以太网接口。
5. 点击**确定**。
6. 点击。

表 98 二层以太网通道命令

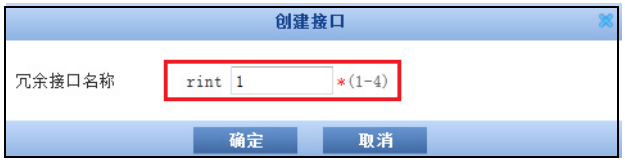
channel *channel_id*	创建以太网通道或者进入指定的以太网通道配置模式。
unset channel *channel_id*	删除指定的以太网通道。
show interface channel [*channel_id* | **brief**]	显示以太网通道信息。
shutdown	禁用接口。
unset shutdown	启用接口。
hold ethernet *interface_id*	设置隶属于以太网通道的二层以太网接口。
unset hold ethernet *interface_id*	删除隶属于以太网通道的二层以太网接口。
working-type layer2-interface	设置接口为二层工作模式。

表 99 共享三层以太网通道命令

hold ethernet *interface_id*	设置隶属于以太网通道的二层以太网接口。
unset hold ethernet *interface_id*	删除隶属于以太网通道的二层以太网接口。
working-type layer3-shared-interface	设置接口为共享三层工作模式。

4.1.4.4 配置冗余接口

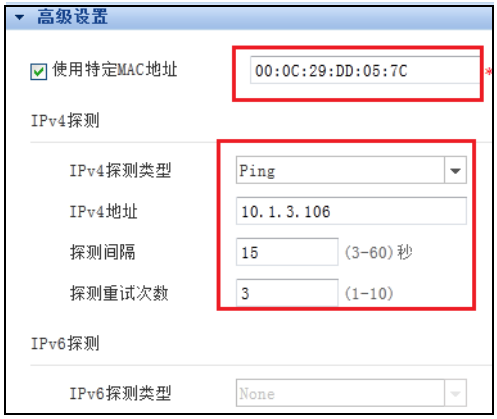
1. 选择**网络** > **接口**。点击**新建**，选择 **Redundant**，创建冗余接口。



2. 点击**确定**。
3. 点击冗余接口 rint1 所对应的，为其分配两个二层以太网接口（主和备用接口）。

4. 将冗余接口的工作模式设置为**二层**、**三层**或**共享三层**。然后再进行其他配置。详见 4.1.4.1 配置以太网接口。
   - 当模式设置为**二层**时，可设置等待时间，即冗余接口从故障恢复所花费的时间。

   - 当模式设置为**三层**时，在**高级设置**区域，可以修改 MAC 地址，并进行探测配置。在指定 IPv6 探测类型前，需要首先勾选**启用 IPv6**，启用冗余接口的 IPv6 功能。



5. 点击**确定**。
6. 点击。

表 100 二层冗余接口命令

rint *rint_id*	创建冗余接口或者进入指定的冗余接口配置模式。
unset rint *rint_id*	删除指定的冗余接口。
show interface rint [*rint_id* | **brief**]	显示冗余接口信息。
shutdown	禁用接口。
unset shutdown	启用接口。
hold ethernet primary *interface_id* **secondary** *interface_id*	设置冗余接口的主备以太网接口。
unset ethernet	删除冗余接口的主备接口。
switch	进行冗余接口的主备切换。
working-type layer2-interface	设置接口为二层工作模式。
wait-time *wait_time*	设置冗余接口的故障恢复等待时间。

表 101 三层冗余接口命令

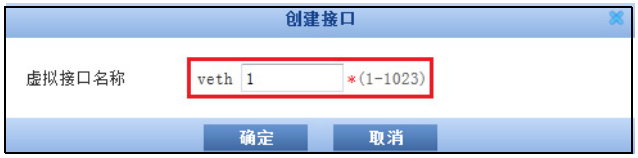
hold ethernet primary *interface_id* **secondary** *interface_id*	设置冗余接口的主备以太网接口。
unset ethernet	删除冗余接口的主备接口。
working-type layer3-interface	设置接口为三层工作模式。
mtu {*mtu_value* | **default**}	设置三层或共享三层接口的 MTU。
default mac	获取以太网接口、以太网通道、 VLAN 或冗余接口的缺省 MAC 地址。
mac address *mac_address*	修改以太网接口、以太网通道、 VLAN 或冗余接口的 MAC 地址。
monitor type	设置指定三层或共享三层冗余接口的 IPv4 探测方式。
unset monitor type	删除指定三层或共享三层冗余接口的 IPv4 探测方式。
monitor typev6	设置指定三层或共享三层冗余接口的 IPv6 探测方式。
unset monitor typev6	删除指定三层或共享三层冗余接口的 IPv6 探测方式。
wait-time *wait_time*	设置冗余接口的故障恢复等待时间。

表 102 共享三层冗余接口命令

hold ethernet primary *interface_id* **secondary** *interface_id*	设置冗余接口的主备以太网接口。
unset ethernet	删除冗余接口的主备接口。
working-type layer3-shared-interface	设置接口为共享三层工作模式。

4.1.4.5 配置虚拟接口

1. 选择**网络** > **接口**。点击**新建**，选择 **Virtual Interface**，创建虚拟接口。



2. 点击**确定**。
3. 点击 veth1 所对应的 。将虚拟接口的工作模式设置为：
   - **二层**，并指定其所属的 VLAN。
   - **三层**，并设置接口的 IP 地址和 IPv6 信息。详见 4.1.4.1.2 三层接口。

4. 点击**确定**。
5. 选择**系统**>**虚拟系统**>**虚拟网络**，将veth2划分到虚拟网络vnet1中，系统将自动显示虚拟接口连接的虚拟网络。更多信息参见 15 虚拟系统。
6. 点击 。

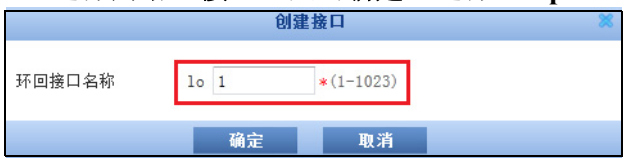
表 103 二层虚拟接口命令

veth *veth_id*	创建虚拟接口或进入指定的虚拟接口配置模式。
unset veth *veth_id*	删除指定的虚拟接口。
show interface veth [*veth_id* | **brief**]	显示虚拟接口信息。
shutdown	禁用接口。
unset shutdown	启用接口。
working-type layer2-interface	设置接口为二层工作模式。
port access vlan *vlan_id*	将二层接口划分到 VLAN 中。
unset port access vlan	删除二层接口所隶属的 VLAN。

关于虚拟接口的 CLI 配置，参见表 95 三层以太网接口命令。

4.1.4.6 配置环回接口

1. 选择**网络** > **接口**。点击**新建**，选择 **Loopback**，创建环回接口。



2. 点击**确定**。
3. 点击 lo1 所对应的，进行如下配置：

- 一个环回接口只能配置一个 IPv4 地址和一个 IPv6 地址。
- IPv4 地址格式为：[1-223].[0-255].[0-255].[0-255]，不可以为 127.0.0.0~127.255.255.255 或者 192.168.255.254。
- 环回接口不支持 IPv6 地址自动配置 （链路本地地址除外）。

4. 点击**确定**。
5. 点击。

表 104 环回接口命令

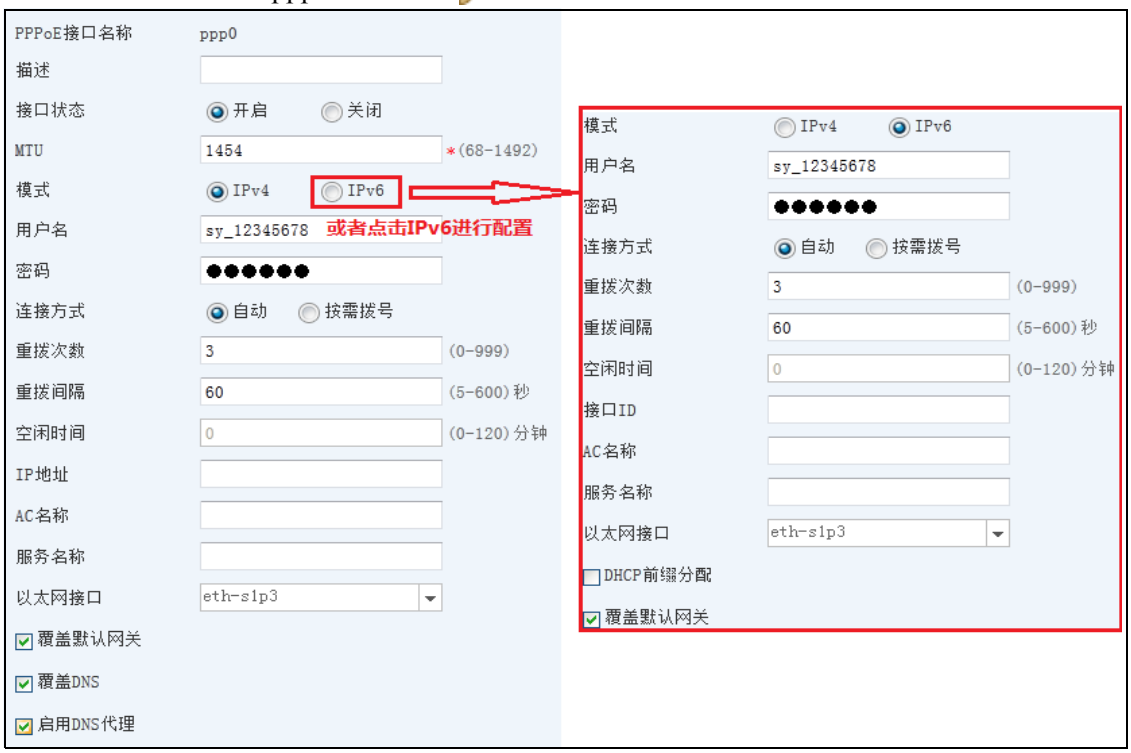
loopback *lo_id*	创建环回接口或者进入指定的环回接口配置模式。
unset loopback *lo_id*	删除指定的环回接口。
show interface loopback [*lo_id* | **brief**]	显示环回接口信息。
shutdown	禁用接口。
unset shutdown	启用接口。
mtu {*mtu_value* | **default**}	设置三层或共享三层接口的 MTU。

关于 IPv4 和 IPv6 的 CLI 配置，参见表 95 三层以太网接口命令。

4.1.4.7 配置 PPPoE 接口

1. 选择**网络** > **接口**。点击**新建**，选择 **PPPoE**，创建 PPPoE 接口。

2. 点击**确定**。
3. 点击 PPPoE 接口 ppp0 所对应的，进行如下配置：



PPPoE 接口的 IPv6 地址只能通过 DHCPv6 获取。

4. 点击**确定**。
5. 点击。

表 105 PPPoE 接口命令

pppoe *pppoe_id*	创建 PPPoE 接口或者进入指定的 PPPoE 接口配置模式。
unset pppoe *pppoe_id*	删除指定的 PPPoE 接口。
show interface pppoe [*pppoe_id* | **brief**]	显示 PPPoE 接口信息。
active {**on** | **off**}	启用或禁用 PPPoE 接口。
mtu {*mtu_value* | **default**}	设置三层或共享三层接口的 MTU。
mode {**ipv4** | **ipv6**}	设置指定 PPPoE 接口的工作模式。
username *user_name* **password** *passwd*	配置拨号用户。
unset user	删除拨号用户。
connection-type	配置拨号方式
connection-type ondemand idle	配置拨号闲置时间，在这个时间内如果没有数据传输，会自动断开拨号连接。
ip address *ipv4 netmask* [**secondary**]	为指定的三层或共享三层接口添加 IPv4 地址。
unset ip address [*ipv4*]	删除指定三层或共享三层接口的 IPv4 地址。
interface-id *if_id*	为指定的 PPPoE 接口配置接口标识。
unset interface-id	删除指定 PPPoE 接口的接口标识。
acname *ac_name*	设置 AC 名称。
unset acname	删除 AC 名称。
servicename *service_name*	设置服务名称。
unset servicename	删除服务名称。
hold {**ethernet** *interface_id* | **rint** *rint_id*}	设置隶属于 PPPoE 接口的二层以太网接口或二层冗余接口。
unset hold	删除隶属于 PPPoE 接口的二层接口。
overwrite-default-gateway	启用指定 PPPoE 接口的覆盖系统缺省网关功能。
unset overwrite-default-gateway	禁用指定 PPPoE 接口的覆盖系统缺省网关功能。
overwrite-dns	启用 IPv4 模式 PPPoE 接口的覆盖系统 DNS 功能。
unset overwrite-dns	禁用 IPv4 模式 PPPoE 接口的覆盖系统 DNS 功能。
enable-dns-proxy	启用为 IPv4 工作模式的 PPPoE 接口自动添加 DNS 代理的功能。
unset enable-dns-proxy	禁用为 IPv4 工作模式的 PPPoE 接口自动添加 DNS 代理的功能。
dhcp-prefix-delegate	启用指定 PPPoE 接口的自动触发 DHCPv6 客户端请求功能。
unset dhcp-prefix-delegate	禁用指定 PPPoE 接口的自动触发 DHCPv6 客户端请求功能。

表 106 PPPoE 接口属性

参数	说明
描述	PPPoE 接口的描述信息。 0 ～ 255 个字节的 UTF-8 字符，不包含 ?'\"<>&。
接口状态	PPPoE 接口状态。 • **开启**：表示该接口已连接。在此状态下，只能修改接口的描述信息。 • **关闭**：表示该接口已断开 （缺省状态）。在此状态下，可以配置接口全部信息。
MTU	数据的最大传输单元。
模式	PPPoE 接口的工作模式，包括 IPv4 （缺省状态）和 IPv6。
用户名	拨号用户的名称。
密码	拨号用户的密码。
连接方式	拨号类型。包括： • **自动** （缺省方式）：自动连接到 ISP。当连接断开时， NISG-IPS 将自动重连。 • **按需拨号**：根据访问需求进行拨号。
重拨次数	拨号连接最大尝试次数。 数值 0 表示没有重拨次数限制。
重拨间隔	拨号连接的时间间隔。
空闲时间	连接的的空闲时间。建立拨号连接后，如果在设定的空闲时间内无数据传输，系统将断开拨号连接。数值 0 表示不断开连接。 该属性仅在按需拨号方式时生效。
IP 地址	在 PPPoE 接口上配置的 IPv4 地址，用于 PPPoE 通信。 该属性仅在 IPv4 模式下生效。
接口 ID	64 位的手动配置的接口标识。当接口标识无法通过自动 PPPoE 协商获得时，需要进行手动配置。 该属性仅在 IPv6 模式下生效。
AC 名称	该名称通常是 ADSL Modem 的商标、型号或序列号，由 ISP 负责提供，一般不需配置。
服务名称	该名称通常是 ISP 的名称或 ISP 提供的服务名称，由 ISP 负责提供，一般不需要配置。
以太网接口	该接口用于 PPPoE 通信时接收或发送数据包。 此接口必须是二层以太网接口、冗余接口或 WLAN 接口。
覆盖默认网关	从 ISP 获取的网关地址将作为 NISG-IPS 的缺省网关。
覆盖 DNS	从 ISP 获取的 DNS 地址将作为 NISG-IPS 的缺省 DNS，并覆盖 NISG-IPS 的 DNS 主机模块配置的 DNS 服务器信息。该属性仅在 IPv4 模式下生效。
启用 DNS 代理	系统将根据从 ISP 获取的 DNS 信息自动添加 DNS 代理，该 DNS 代理信息对用户不可见。该属性仅在 IPv4 模式下生效。
DHCP 前缀分配	充当 DHCPv6 客户端的 PPPoE 接口将在 PPPoE 协商成功后自动向 DHCPv6 服务器请求分配前缀和其他配置参数。该属性仅在 IPv6 模式下生效。

4.1.4.8 配置隧道接口

在创建 IPSec VPN 隧道、 SSL VPN 和 GRE 隧道时，隧道接口自动被创建，用于建立 VPN 通信。当隧道被删除时，其关联的隧道接口也被删除。

1. 选择**网络** > **接口**。点击隧道接口所对应的 。
2. 配置 IPv4 地址。隧道接口不支持 IPv6 地址。
   - **静态 IP**：手动配置接口的 IPv4 地址和掩码长度。
   - **借用 IP**：使用其他三层接口的主 IP 地址。

3. 点击**确定**。
4. 点击 。

表 107 隧道接口命令

tunnel *tunnel_id*	进入指定的 VPN 隧道接口配置模式。
mtu {*mtu_value* | **default**}	设置三层或共享三层接口的 MTU。
unnumbered *l3_interface_name*	借用三层或共享三层接口 （PPPoE 接口除外） IP 地址。
unset unnumbered	删除借用其他三层或共享三层接口的 IP 地址。
show interface tunnel [*tunnel_id* | **brief**]	显示 VPN 隧道接口信息。

关于 IPv4 和 IPv6 的 CLI 配置，参见表 95 三层以太网接口命令。

表 108 隧道接口属性

配置信息	说明
类型	隧道接口的类型，分为 IPSec VPN、 SSL VPN 和 GRE 三种。
MTU	最大传输单元。取值范围为 68~1500 字节，缺省为 1500 字节。
获取 IP 地址方式	获取 IP 地址的方式包括静态 IP 和借用 IP。 • **静态 IP**：手动配置三层接口的静态 IP 地址。需要在 **IP 地址列表**中配置。 • **借用 IP**：借用其他三层接口的 IP 地址。可以借用 VLAN 接口、环回接口、三层或共享三层以太网接口、三层或共享三层以太网通道、三层或共享三层冗余接口以及三层虚拟接口的 IP 地址，参与路由交换。
引用	使用隧道接口的隧道和路由。 如果隧道接口正被路由所引用，那么与此接口关联的隧道将无法被删除。

4.2 工作模式

4.2.1 概述

NISG-IPS 支持两种工作模式：

- **在线模式**：具备 IPS 的全部功能，对网络流量进行过滤和控制。
- **旁路模式**：仅用作旁路 IPS 检测设备，对网络流量进行监听和分析。

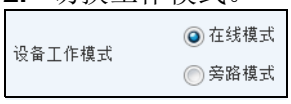
在线模式和旁路模式是两种互斥的工作模式，管理员可以根据自身需要选择任意一种工作模式。

表 109 切换工作模式的影响

模式切换	对系统的影响
在线切换到旁路	1. 连接中断，安全检查终止。 2. 管理接口和 IP 保持不变。 3. 其他所有以太网接口工作在二层模式，逻辑接口被删除。 4. 在线模式和旁路模式都具备的功能，将继承在线模式下的配置。
旁路切换到在线	1. IPS 检测终止。 2. 管理接口和 IP 保持不变。 3. 其他所有以太网接口工作在二层模式。 4. 在线模式和旁路模式都具备的功能，将继承旁路模式下的配置。 **注**：旁路模式下 IPS 自定义规则和应用的配置将被保留，下次切换回旁路模式时再生效。 5. 旁路模式下不具备的安全功能，将恢复出厂缺省配置。

4.2.2 基本配置步骤

1. 选择**网络 > 工作模式**。
2. 切换工作模式。



提示：切换工作模式时，当前模式下的安全配置将丢失，建议备份系统配置后再执行模式切换。

4.3 ARP

4.3.1 概述

地址解析协议 （Address Resolution Protocol， ARP）是一种将网络层 IP 地址解析为数据链路层 MAC 地址的协议。用来记录 IP 地址和 MAC 地址一一对应关系的表叫 ARP 表。NISG-IPS 的 ARP 表最多可存储 32768 条表项；表项的类型包括以下三种：

- 静态 ARP 表项：管理员手动创建和删除的 ARP 表项。

  创建静态 ARP 表项时需要输入目的 IP 地址和对应的目的 MAC 地址，以及表项所属的三层接口。

  因为攻击报文不能修改静态表项的 IP 地址和 MAC 地址的映射关系，所以配置静态 ARP 表项能够提高通信的安全性。

- 动态 ARP 表项：NISG-IPS 自动创建和删除的 ARP 表项。

  动态 ARP 表项的生存时间是由超时检测机制来控制的。当达到超时时间时，动态 ARP 表项会被自动删除。管理员可以为每个三层接口设置动态 ARP 表项的超时时间，取值范围为 3 ～ 30000 秒，缺省为 14400 秒。

- 代理 ARP 表项：管理员手动创建和删除的 ARP 表项。

  如果设置了对某 IP 地址的代理 ARP， NetEye 会用该代理 ARP 表项中三层接口的 MAC 地址应答该 IP 地址的 ARP 请求。

  当虚拟专用网 （VPN）的两端子网处于同一网段的情况下，需要手动添加代理 ARP 表项，实现两端子网的通信。

管理员只可以在 CLI 下配置 ARP 表项。在 WebUI 下，可以监控 ARP 表；更多信息，请参见 16.7 ARP。

4.3.2 基本配置步骤

表 110 ARP 命令

show arp [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id* **|** *ipv4*]	查看当前系统的 ARP 表项。
show arp static	查看静态 ARP 表项。
show arp dynamic	查看动态 ARP 表项。
show arp timeout	查看动态 ARP 表项的超时时间。
show arp proxy	查看代理 ARP 表项。
arp {**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*} *ipv4 mac_address*	创建静态 ARP 表项。

表 110 ARP 命令 (*续*)

arp proxy {**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*} *ipv4 mac_address*	创建代理 ARP 表项。
unset arp *ipv4*	删除指定 IPv4 地址的 ARP 表项。
unset arp static [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*]	删除静态 ARP 表项。
unset arp dynamic [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*]	删除动态 ARP 表项。
unset arp proxy [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*]	删除代理 ARP 表项。
arp {**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*} **timeout** {*timeout_value* **| default**}	编辑动态 ARP 表项的超时时间。

4.3.3 配置参数说明

表 111 ARP 表属性

配置信息	说明
IP 地址	即目的主机 IP 地址。该 IP 地址不能是环回地址、多播地址、指向子网的广播地址或受限制的广播地址。 添加静态 / 代理 ARP 条目时， IP 地址不可以是 0.0.0.0 和 255.255.255.255，也不可以是接口自身的 IP 地址。
MAC 地址	即与 IP 地址相对应的 MAC 地址。该 MAC 地址不能是广播或多播 MAC 地址。
类型	即 ARP 表项类型。 • **Static**：表示静态 ARP 表项。 • **Dynamic**：表示动态 ARP 表项。 • **Proxy**：表示代理 ARP 表项。
状态	即 ARP 表项的状态。包括四种： • **INCOMPLETE**：已发送 ARP 请求但还没有应答时的状态。 • **REACHABLE**：可用状态。 • **STALE**：可用，但生存时间过长，应再次查询学习。 • **FAILED**：不可用状态，该状态不可见。
生存时间	即动态 ARP 表项存活时间。
接口	即所属的三层接口。包括以太网接口、以太网通道、 VLAN 接口、虚拟接口、冗余接口和共享三层接口。

4.4 CAM

4.4.1 概述

内容可寻址存储器 （Content Addressable Memory，CAM）是一种系统内存结构，可以优化地址查询速度。 CAM 表是用于二层交换的地址表，提供 MAC 地址和二层接口的映射关系。 NISG-IPS 使用 CAM 表来查找转发数据帧的二层接口。当 NISG-IPS 接收到一个数据帧时，根据该数据帧的目的 MAC 地址查询 CAM 表，如果在该表中找到与 MAC 地址对应的 CAM 表项，则根据查询的结果从对应接口转发该数据帧；如果找不到对应的 CAM 表项，则在所属 VLAN 内广播。

NISG-IPS 的 CAM 表支持以下类型的表项且最多可存储 16384 条：

- 本地 CAM 表项：NISG-IPS 自身三层接口的 MAC 地址所对应的 CAM 表项。

  此类表项随三层接口创建和删除。
- 静态 CAM 表项：手动创建和删除的 CAM 表项。

  此类表项永不超时，只能手动删除。
- 动态 CAM 表项：NISG-IPS 通过动态学习创建的 CAM 表项。

  可以设置动态 CAM 表项超时时间。当表项达到超时时间，将被自动删除。
- 多播 CAM 表项：在 VLAN 内发送多播数据包时使用该类型。

管理员只可以在 CLI 下配置 CAM 表项。在 WebUI 下，可以监控 CAM 表；更多信息，请参见 16.8 CAM。

4.4.2 基本配置步骤

表 112 CAM 命令

show cam-table [vlan *vlan_id* | *mac_address*]	查看 CAM 表项。
show cam-table timeout	查看动态 CAM 表项的超时时间。
cam-table vlan *vlan_id* {**channel** *channel_id* | **ethernet** *interface_id* **| rint** *rint_id* **| veth** *veth_id*} *mac_address*	创建 CAM 表项。
unset cam-table *mac_address*	删除指定 MAC 地址的 CAM 表条目。
unset cam-table static vlan *vlan_id* [*mac_address*]	删除静态 CAM 表项。
unset cam-table dynamic [**vlan** *vlan_id*]	删除动态 CAM 表项。
cam-table timeout [**vlan** *vlan_id*] {*timeout_value* | **default**}	编辑动态 CAM 表的超时时间。

4.4.3 配置参数说明

表 113 CAM 表属性

配置信息	说明
目的地址	即数据包发往的 MAC 地址。该地址不能为 00:00:00:00:00:00 或 FF:FF:FF:FF:FF:FF。
地址类型	即 CAM 表项类型。 • **Local**：表示本地 CAM 表项。 • **Static**：表示静态 CAM 表项。 • **Dynamic**：表示动态 CAM 表项。 • **Multicast**：表示多播 CAM 表项。
三层接口信息	即表项所属 VLAN 接口或本地三层接口。
目的端口	当表项为动态或静态类型时，对应的二层接口；当表项为多播类型时，是一个二层接口表，表示多播数据包应从这些二层接口转发出去。
超时时间	即动态 CAM 表的超时时间，取值范围为 10 ～ 30000 秒，缺省为 300 秒。

4.5 STP

4.5.1 概述

生成树协议 （Spanning Tree Protocol， STP）有狭义和广义两层含义。狭义 STP 指 IEEE802.1D 中定义的标准 STP 协议，广义 STP 包括 IEEE802.1D 定义的 STP 协议和在其基础上衍生改进的生成树协议，如 RSTP 和 MSTP 等。

4.5.1.1 STP

STP 是由 IEEE802.1D 标准定义的一个二层交换网络管理协议，其目的是可以在布满网桥 （通常是交换机）的网络中形成以根网桥为树根其他网桥伸展如叶的树状拓扑结构。其主要作用是将拓扑中某些网桥的某些端口置于阻塞状态，避免桥接或交换的网络拓扑中产生环路，同时保障链路冗余。当一条链路发生故障时，被阻塞的端口将被启用，起到备份链路的作用。

NISG-IPS 实现了每 VLAN 生成树 (Per-VLAN Spanning Tree) 特性，即能够在二层交换网络中的每个 VLAN 上独立设置启用 STP 或 RSTP 协议，每个 VLAN 单独维护一个生成树。不仅可以保证每个 VLAN 内没有环路，而且能够有效实现二层网络的负载均衡。NISG-IPS 最多支持在 64 个 VLAN 上开启 STP 或 RSTP 实例。

STP 运行过程如下：

1. 确定根网桥
   根网桥是网桥 ID 最小的网桥。在一个二层网络中，只有一个根网桥。当网络拓扑稳定以后，只有根网桥能发送 BPDU （Bridge Protocol Data Unit，建立无环路树形拓朴结构所需的信息）报文，其他网桥只能对其进行接收和转发。
2. 确定根端口
   根端口是在非根网桥上存在的到达根网桥的路径开销最小的端口，一个非根桥设备上只有一个根端口。
3. 确定指定端口
   指定端口是一个网段的所有端口中到达根网桥的路径开销最小的端口，一个网段上只有一个指定端口。
4. 确定阻塞端口
   阻塞端口既不是根端口，也不是指定端口，只监听 BPDU 报文。

4.5.1.2 RSTP

快速生成树协议 （Rapid Spanning Tree Protocol， RSTP）由 IEEE802.1w 标准定义，是对 STP 协议的改进，并与 STP 协议完全兼容，主要实现了网络拓扑的快速收敛。启用 RSTP 协议的网桥会根据收到的 BPDU 版本号自动判断与之相连的网桥是支持 STP 协议还是支持 RSTP 协议。

缺省情况下， STP 协议的收敛时间为 50 秒，而 RSTP 协议的收敛时间最快可以达到 1 秒以内。

- 快速收敛

  RSTP 协议的快速收敛主要依赖于以下方面来实现：

  - 边缘端口 （Edge Port）：边缘端口是与服务器等终端设备直接相连的端口。边缘端口无需参与生成树计算，可以省略侦听和学习的状态，无时延地直接进入转发状态。
  - 链路类型：启用 RSTP 协议时，网桥 （交换机）根据端口的双工模式自动判断链路类型。如果端口工作在全双工模式下，则为点到点 （Point-to-Point Link）链路类型，端口可以快速地从阻塞状态进入转发状态，而无需等待转发延迟时间。

- 端口角色

  除了拥有和 STP 相同作用的根端口和指定端口外， RSTP 协议新增下列端口角色，可以加快端口状态的转换：

  - **替换端口 （Alternate Port）**：根端口的备份端口。
  - **备份端口 （Backup Port）**：个网段指定端口的备份端口。

- 端口状态

  RSTP 协议只有三种端口状态：丢弃、学习和转发。处于丢弃状态的端口实际上就是 STP 协议中禁用、阻塞和侦听三种状态的集合。

- 强制运行 RSTP

  可以提高数据转发效率。如果管理员确定和 NISG-IPS 相连的设备都运行 RSTP 协议，那么可以在 NISG-IPS 上启用强制运行 RSTP 的功能；如果与之直连的设备只支持 STP 协议，在 NISG-IPS 上强制运行 RSTP，将会导致互相不兼容的问题。

4.5.2 基本配置步骤

1. 选择**网络** > **STP**。
2. 双击 VLAN 接口条目，进行相关配置。

   - 当删除 VLAN 时，其所有生成树配置将一同被删除；当从 VLAN 中删除接口时，相应的端口配置也被删除，但不影响 VLAN 中其他端口的配置。
   - 管理员通过 CLI 可以配置 STP 定时器 （Hello， Max-age 以及 Forward-delay）。
3. 点击**确定**。
4. 点击。

表 114 STP 命令

show spanning-tree {brief | vlan *vlan_id*}	显示 STP 信息。
spanning-tree {enable per-vlan-stp | disable}	启用或禁用 NISG-IPS 设备的 STP 功能。
spanning-tree {enable {stp | rstp [protocol-migration]} | disable}	启用或禁用某个 VLAN 的 STP 功能。
spanning-tree default	重置 STP 配置信息，恢复缺省配置。
spanning-tree root {primary | secondary}	将某个 VLAN 设置为根网桥或备用根网桥。
unset spanning-tree root {primary | secondary}	取消设置根网桥或备用根网桥。
spanning-tree bridge-priority	设置网桥优先级。
spanning-tree interface port-priority	设置指定接口的端口优先级。
spanning-tree interface path-cost	设置指定接口的端口路径开销。

表 114 STP 命令 (*续*)

spanning-tree interface edge-port	设置某个接口为边缘端口。
unset spanning-tree interface edge-port	取消设置某个接口为边缘端口。
spanning-tree forward-delay	设置转发延迟时间。
spanning-tree hello-time	设置 Hello 时间。
spanning-tree max-age	设置 BPDU 报文最大生存时间。

4.5.3 配置参数说明

在 NISG-IPS 上， STP 功能只能在根系统下进行配置，在虚拟系统中可以查看 STP 配置。不支持 HA 同步。

表 115 STP 配置信息

配置信息	说明
STP	• **启用**：启用 NISG-IPS 的 STP 功能。 • **禁用**：禁用 NISG-IPS 的 STP 功能。当 STP 功能禁用时， NISG-IPS 支持对 STP 和 RSTP 的 BPDU 消息的透明传输，对 BPDU 不做任何处理直接转发。
协议	仅支持每 VLAN STP。
VLAN 列表	包含以下两个选项： • **接口 —** 包括所有 VLAN 接口。可以为 VLAN 接口启用 STP/RSTP。每个 VLAN 具有独立的 STP 配置。 • **协议 —** 包括 STP、 RSTP 或强制运行 RSTP。 当 VLAN 中有新的二层接口加入时， NISG-IPS 会自动检测该接口，并为其分配一套缺省参数配置。
STP/RSTP	• **启用**：启用某个 VLAN 的 STP 或 RSTP。 • **禁用**：禁用某个 VLAN 的 STP 或 RSTP。 当一个 VLAN 不包含任何二层接口时，能够开启 STP/RSTP，但不会进行生成树计算。
恢复默认设置	点击**重置**按钮，则当前 VLAN 恢复系统缺省的 STP 配置。
类型	网桥使用的生成树协议类型，管理员可以进行如下选择： • **STP—** 网桥只支持 STP 协议。 • **RSTP—** 与网桥相连的设备使用 STP 协议时，网桥自动使用 STP 协议与之兼容。 • **强制运行 RSTP—** 网桥不会兼容二层网络中其他 STP 设备，而强制运行 RSTP 协议。
根网桥	设置该 VLAN 所代表的虚拟网桥为其所在二层交换网络的根网桥。 一个二层网络中只能有一个根网桥。如果同时有多个网桥被配置成根网桥，则比较每个网桥的 MAC 地址，最小者为根网桥。根网桥优先级为 0。
备用根网桥	设置该 VLAN 所代表的虚拟网桥为其所在二层交换网络的备用根网桥。备用根网桥主要起到对根网桥的备份作用，可以在二层网络中设置多个备用根网桥。备用根网桥优先级为 4,096。
网桥优先级	设置 VLAN 网桥的优先级。 根网桥 （缺省设置）、备用根网桥和网桥优先级的设置只能选取其中一种。网桥优先级取值范围为 0 ～ 61,440，且必须为 4,096 的倍数。
端口优先级	设置 VLAN 中所包含各个端口的优先级。取值范围为 0 ～ 240，且必须为 16 的倍数。
端口路径开销	设置一个 VLAN 中所包含的各个端口的路径开销。缺省情况下，系统将根据端口链路速率自动判断路径开销。链路速率越高，路径开销值越小。 端口路径开销取值范围为 1 ～ 200,000,000。
边缘端口	设置工作在 Access 模式的二层以太网接口为边缘端口。边缘端口能够直接进入转发状态，加快收敛时间。 当管理员取消勾选**边缘端口**复选框或该边缘端口从网络中接收到 BPDU 消息时，该端口就会变成一个正常的生成树端口，参与生成树计算。

4.6 安全域

4.6.1 概述

安全域是接口的集合。创建安全域时，可以将接口划分到安全域中，以实现对这些接口所连接的网络进行统一的安全管理。不同安全域之间只有通过配置访问策略才能相互访问。 NISG-IPS 最多允许创建 30 个安全域。

4.6.2 基本配置步骤

1. 选择**网络** > **安全域**。点击**新建**。
2. 设置安全域类型。
   - 如果选择了**基于三层接口**，需为安全域分配三层接口。
   - 如果选择了**基于二层接口**，需为安全域分配 VLAN 接口内的二层接口。

3. 点击**确定**。
4. 点击 。

表 116 安全域命令

zone *zone_name*	创建安全域。
unset zone [*zone_name*]	删除安全域。
zone based-layer2	配置基于二层接口的安全域。
unset zone based-layer2	删除安全域中的二层接口。
zone based-layer3	配置基于三层或共享三层接口的安全域。
unset zone based-layer3	删除安全域中的三层或共享三层接口。
zone description	设置安全域的描述信息。
show zone [*zone_name*]	显示安全域的信息。

4.6.3 配置参数说明

表 117 安全域属性

配置信息	说明
名称	安全域的名称， 1~63 字节的 UTF-8 字符，不包含：?,'\"<>&# 和空格 名称不允许为 Any 和 mgt-interface。
类型	安全域类型。分为基于二层接口和基于三层接口 （缺省类型）。
接口	安全域包含的接口，一个接口只能划分到一个安全域中。
引用	引用安全域的策略列表。 被策略引用的安全域不能被删除。如需删除它们，应首先解除相应的引用关系。
描述	安全域的描述信息。 0 ～ 255 个字节的 UTF-8 字符，不包含：?'\''<>&。

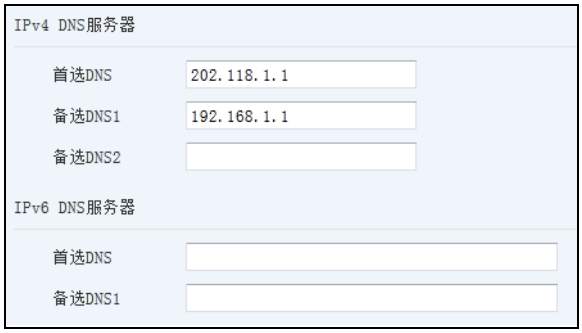
4.7 DNS 主机

4.7.1 概述

NISG-IPS 可作为 DNS 客户端从 DNS 服务器请求域名解析。管理员最多能够设置三个 IPv4 DNS 服务器和两个 IPv6 DNS 服务器 IP 地址，用以提供域名解析服务；如解析 NISG-IPS 系统升级服务器、 IPS 规则升级服务器、 LDAP 服务器等域名。

4.7.2 基本配置步骤

1. 选择**网络** > **DNS** > **主机**。
2. 配置 IPv4 和 IPv6 DNS 服务器。



3. 点击**确定**。
4. 点击。

表 118 DNS 主机命令

dns host	配置 NISG-IPS 域名服务器。
unset dns host	删除域名服务器配置。
show dns host	显示 DNS 服务器配置。

4.7.3 配置参数说明

表 119 DNS 主机属性

配置信息	说明
IPv4 DNS 服务器	IPv4 DNS 服务器的 IP 地址，包括首选 DNS、备选 DNS1 以及备选 DNS2。可以输入的 IP 地址范围为：[1-223].[0-255].[0-255].[0-255]，不可以为 127.0.0.0~127.255.255.255 或者 192.168.255.254。
IPv6 DNS 服务器	IPv6 DNS 服务器的 IP 地址，包括首选 DNS 和备选 DNS1。不可为 IPv6 DNS 服务器配置下列 IP 地址：环回地址 （::1）、多播地址 （FF00/8~FFFF/8）、未指定地址（::）、 ::FFFF:0:0/96。

4.8 DNS 代理

4.8.1 概述

NISG-IPS 的 DNS 代理具有以下优点：

- DNS 代理具有分隔 DNS 查询请求的功能。
- DNS 代理允许通过隧道接口发送 DNS 请求。
- 通过 NISG-IPS 上的本地缓存，可以提升 DNS 查询的速度。

DNS 代理分为非透明代理和透明代理服务， NISG-IPS 缺省不开启这两种服务。

- 非透明代理

  如果把 DNS 客户端的 DNS 服务器指向 NISG-IPS，那么对于 DNS 客户端来说，NISG-IPS 就相当于 DNS 服务器。

  当管理员配置 DNS 代理服务器或者添加本地静态缓存时， NISG-IPS 即开启非透明代理服务。更多信息，请参阅 4.8.3 配置参数说明和 4.9.3 配置参数说明。

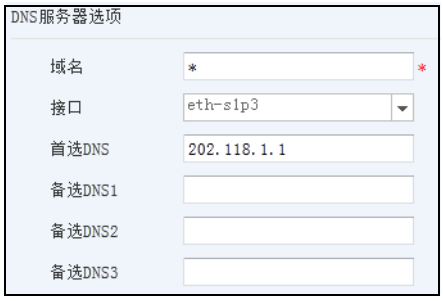
- 透明代理

  当 DNS 客户端将网关指向 NISG-IPS， DNS 服务器指向真正的 DNS 服务器的 IP 地址时， DNS 代理对用户完全透明。

  当管理员配置访问策略，并在策略中启用 DNS 代理时， NISG-IPS 即开启透明代理服务。更多信息，请参阅 10.1.1 访问策略。

4.8.2 基本配置步骤

1. 选择**网络** > **DNS** > **DNS 代理**。
2. 点击**新建**，配置域名、作为 DNS 代理的接口和 DNS 服务器地址。



   - NISG-IPS 最多支持 2048 个 DNS 代理条目。
   - 管理员可以在一个 DNS 代理条目中同时配置 IPv4 和 IPv6 DNS 服务器的 IP 地址。
   - 可为 DNS 服务器配置的的 IPv4 地址范围为：[1-223].[0-255].[0-255].[0-255]，不允许输入 127.0.0.0~127.255.255.255 或者 192.168.255.254。不可为 DNS 服务器配置下列 IPv6 地址：环回地址 （::1）、多播地址 （FF00/8~FFFF/8）、未指定地址（::）、 ::FFFF:0:0/96。
3. 点击**确定**。
4. 点击 。

表 120 DNS 代理命令

dns server-select	添加 DNS 代理。
unset dns server-select	删除 DNS 代理。
show dns server-select	显示 DNS 代理配置信息。

4.8.3 配置参数说明

表 121 DNS 代理配置信息

配置信息	说明
域名	需要使用 DNS 代理的域名。 可以输入合法的域名或输入 * （表示匹配所有的域名）。
接口	即转发域名解析请求的三层接口，环回接口除外。
首选 DNS	即首选 DNS 服务器的 IPv4 或 IPv6 地址。
备选 DNS1	即第一备选 DNS 服务器的 IPv4 或 IPv6 地址。
备选 DNS2	即第二备选 DNS 服务器的 IPv4 或 IPv6 地址。
备选 DNS3	即第三备选 DNS 服务器的 IPv4 或 IPv6 地址。

4.9 DNS 缓存

4.9.1 概述

NISG-IPS 支持两种缓存类型：

- 动态缓存：动态记录 IP 地址、相应的域名和生存时间。动态缓存表最多保存 1024 条条目。
- 静态缓存：配置静态缓存时，需要设置 IP 地址、相应的域名和入口接口信息。静态缓存表最多保存 2048 条条目。

当用户通过 NISG-IPS 使用 DNS 查询时：

1. 首先在入站智能 DNS 中查询。
2. 如果没有查询到相应的信息，则在静态缓存中查找记录。
3. 如果没有查询到，则继续查找动态缓存。
4. 如果仍然没有查询到相应的信息，则通过代理功能向其他 DNS 服务器转发请求包，直到查找成功并把此次查询结果记录在动态缓存中。

4.9.2 基本配置步骤

1. 选择**网络** > **DNS** > **静态缓存**。
2. 点击**启用**，启用该功能。如需禁用此功能，点击**禁用**。

3. 点击**新建**，配置域名和 IP 地址的对应关系以及入口接口。

4. 点击**确定**。
5. 点击。

提示：DNS 动态缓存功能缺省是启用的。管理员只可以在 CLI 下通过 **unset dns cache dynamic** [*domain_name*] 命令删除 DNS 动态缓存。

表 122 DNS 缓存命令

dns cache	添加静态 DNS 缓存。
dns cache-state {on | off}	启用或禁用 DNS 静态缓存。
unset dns cache dynamic	删除动态 DNS 缓存。
unset dns cache static	删除静态 DNS 缓存。
show dns cache	显示 DNS 缓存信息。
show dns cache-state	显示 DNS 静态缓存状态。

4.9.3 配置参数说明

表 123 DNS 静态缓存配置信息

配置信息	说明
域名	即静态缓存条目中的域名。
IP 地址	即静态缓存条目中与域名相对应的 IP 地址。可以在一个 DNS 静态缓存条目中同时配置 IPv4 和 IPv6 地址。 IPv4 地址格式为：[1-223].[0-255].[0-255].[0-255]，不能输入 127.0.0.0~127.255.255.255 或者 192.168.255.254。 一个域名可以同时对应最多 32 个 IP 地址。
接口	即收到域名解析请求的三层接口，环回接口除外。

4.10 入站智能 DNS

4.10.1 概述

当用户向受保护的网站发送 DNS 请求时， NISG-IPS 的入站智能 DNS 特性可以自动判断出用户 IP 地址所属的运营商，并在 DNS 应答中将对应运营商服务器的 IP 地址返回给用户，以便属于不同运营商的用户访问到所属运营商的网络服务器。如果多个服务器的 IP 地址属于同一个运营商，那么 NISG-IPS 会根据 IP 地址的权重分配数据包。因此，入站智能 DNS 功能不仅可以提高网络访问速度而且也可以实现负载均衡。比如，一个企业的网站在电信和联通都有带宽。当来自电信的用户访问企业网站的时候， NISG-IPS 可以根据 IP 地址自动判断用户所属的运行商，再将企业网站的电信地址返回给用户。当来自联通的用户访问网站时， NISG-IPS 将网站的联通地址返回给用户。

管理员可以根据实际需要，添加服务器域名和对应的 IP 地址及其权重的对应关系条目。可以为每个域名设置最多 32 个 IP 地址，且为每个 IP 地址设置相应的权重，以实现负载均衡。 NISG-IPS 支持 2048 个域名。

4.10.2 基本配置步骤

1. 选择**网络** > **入站智能 DNS**。
2. 点击**启用**，开启入站智能 DNS 功能。如需禁用此功能，点击**禁用**。
3. 点击**新建**，添加域名和IP地址及权重的对应关系。列表中也给出了IP地址所属的运营商，此运营商是 NISG-IPS 自动识别的。

提示：入站智能 DNS 的权重只对同一运营商的不同 IP 地址起作用。不同运营商 IP 地址的权重之间不会互相影响。

4. 点击**确定**。
5. 点击 。

4.10.3 配置参数说明

表 124 智能 DNS 参数

配置信息	说明
入站智能 DNS	• **启用**：启用智能 DNS 功能。 • **禁用**：禁用智能 DNS 功能。
域名	用户访问的域名。
IP 地址和权重列表	• **IP 地址**：域名对应的 IP 地址。每个域名最多对应 32 个 IP 地址。 • **权重**：每个地址可以分到的数据流量比例，取值范围为 1-255。

4.11 动态 DNS

4.11.1 概述

当 NISG-IPS 作为整个网络的出口设备且外网接口通过 ADSL 拨号线路连接到 Internet 时，外网接口的 IP 地址就会经常变动。所以不能在 Internet 上通过固定的 IP 地址登录到 NISG-IPS 上。 NISG-IPS 的动态域名解析功能 （即 DDNS）可以把动态变化的 IP 地址映射到一个固定的域名上。当管理员在 Internet 上访问 NISG-IPS 时，就可以直接通过此域名来访问。

4.11.2 基本配置步骤

1. 选择**网络** > **动态 DNS**。
2. 点击**启用**，启用 DDNS 功能。如禁用此功能，点击**禁用**。
3. 选择一个 PPPoE 接口。此接口应已在**网络** > **接口**页面配置完成。此 PPPoE 接口是出口接口，用于连接 PPPoE 服务器。
4. 输入在动态 DNS 服务商处申请的用户名和密码。

提示：需要预先在花生壳网站 （www.oray.com）上注册用户名和密码并设置域名。此域名与 ppp1 接口动态变化的 IP 地址绑定在一起。

5. 点击**确定**。
6. 点击 。

动态 DNS 命令

ddns daemon	启用或禁用动态 DNS 功能。
ddns account/unset ddns account	配置 / 取消配置动态 DNS 的账号。
ddns password/unset ddns password	配置 / 取消配置动态 DNS 账号的密码。
ddns interface/unset ddns interface	配置 / 取消配置接口的动态 DNS 功能。
ddns sp/unset ddns sp	配置 / 取消配置动态 DNS 的服务提供商。
show ddns	显示动态 DNS 的配置信息。
show ddns splist	显示动态 DNS 的服务提供商。

4.11.3 参数说明

Table 125 动态 DNS 参数

参数	说明
动态 DNS	• **启用**：用于启用动态 DNS 功能。 • **禁用**：用于禁用动态 DNS 功能。
服务提供商	NISG-IPS 只支持 Oray。
PPPoE	PPPoE 接口，其 IP 地址被映射到一个固定的域名。
用户名	在动态 DNS 服务商处登记的用户名。
密码	用户名的密码。

4.12 DHCP 服务器

4.12.1 概述

动态主机配置协议 （Dynamic Host Configuration Protocol， DHCP）用于动态地分配 IP 地址。 NISG-IPS 可以充当 DHCP 客户端、服务器和中继代理。

- **DHCP 服务器**：为任意安全域的任意接口上的主机 （DHCP 客户端）动态分配 IP 地址。
- **DHCP 中继代理**：在 DHCP 客户端和 DHCP 服务器之间转发 DHCP 信息。
- **DHCP 客户端**：从 DHCP 服务器处获得 IP 地址。参见 4.1.4.1.2 三层接口的步骤 4。

只有配置了合法 IP 地址的接口才能够进行 DHCP 服务器与 DHCP 中继代理的配置。

4.12.2 基本配置步骤

1. 选择**网络** > **DHCP** > **DHCP 服务器**。管理员可以通过点击**DHCP IP 地址绑定状态**进入监控页面，查看 DHCP IP 地址绑定状态信息。
2. 点击接口对应的 ，进行配置。
   - 点击**不设置**，禁用接口的 DHCP 服务。
   - 点击**中继**，将接口设置为 DHCP 中继代理并输入至少一个 DHCP 服务器 IP 地址。

     配置 DHCP 中继代理时，如果勾选**将客户端网关 IP 地址指向中继接口**，则 NISG-IPS 将把转发的 DHCP 应答报文中的网关字段强制修改为该 DHCP 中继接口的 IP 地址 （如果 DHCP 应答报文中没有网关字段，那么强制添加）。
   - 点击**服务器**，将接口设置为 DHCP 服务器并选择以下任一工作模式：
     - **自动**：NISG-IPS 自动检测网络上是否存在外部服务器。如果存在， NISG-IPS 上的 DHCP 服务器将停止工作，否则为网络中的 DHCP 客户端分配动态 IP 地址。
     - **启用**：NISG-IPS 上的 DHCP 服务器始终开启并工作。
     - **禁用**：NISG-IPS 上的 DHCP 服务器始终关闭，但是仍然保留已分配地址等信息。

同时需要选择**网络** > **DHCP** > **DHCP 作用域**，设置 IP 地址池等信息。参见 4.13 DHCP 作用域。

3. 点击**确定**。
4. 点击。

表 126 DHCP 服务器命令

dhcp interface none	取消指定接口的 DHCP 角色。
dhcp interface relay	设置指定接口为 DHCP 中继代理。
unset dhcp interface relay	取消指定接口的 DHCP 中继代理角色。
dhcp interface relay change-gateway	设置接口的 DHCP 中继代理是否更新网关。
dhcp interface server {auto | enable | disable}	设置指定接口的 DHCP 服务器模式。
unset dhcp interface all	删除所有接口的 DHCP 配置。
show dhcp interface [*interface_name*]	显示 DHCP 接口的配置信息。
show dhcp server ip-binding	显示 DHCP 服务器的 IP 地址绑定状态。

4.12.3 配置参数说明

表 127 DHCP 服务配置信息

属性	说明
接口	配置 DHCP 服务的接口。可以是三层或共享三层以太网接口、三层或共享三层以太网通道、三层或共享三层冗余接口、 VLAN 接口或虚拟接口。
DHCP 服务	即 NISG-IPS 提供的 DHCP 服务。 DHCP 的服务类型包括： • **不设置**：表示三层接口没有启用任何 DHCP 功能。 • **中继**：表示三层接口处于 DHCP 中继代理的功能状态。 • **服务器**：表示三层接口处于 DHCP 服务器的功能状态。 • **客户端**：表示三层接口处于 DHCP 客户端的功能状态。
服务器模式	即 NISG-IPS 中指定的三层接口作为 DHCP 服务器状态时的工作模式，包括： • **自动**：自动模式。 NISG-IPS 自动检测网络上是否存在外部服务器。如果存在，NISG-IPS 上的 DHCP 服务器将停止工作，否则为网络中的 DHCP 客户端分配动态 IP 地址。 • **启用**：启用模式。NISG-IPS 上的 DHCP 服务器始终开启并工作，NISG-IPS 不检测网络上是否存在外部服务器。 • **禁用**：禁用模式。 NISG-IPS 上的 DHCP 服务器始终关闭，但是仍然保留已分配地址等信息。
中继代理服务器	即 NISG-IPS 中指定的三层接口作为 DHCP 中继代理时，设置的代理服务器 IPv4 地址。地址格式为：[1-223].[0-255].[0-255].[0-255]，不能输入 127.0.0.0~127.255.255.255 或者 192.168.255.254。

4.13 DHCP 作用域

4.13.1 概述

当 NISG-IPS 的某个三层接口作为 DHCP 服务器时，作用域可以为服务器提供地址池。NISG-IPS 将地址池中的 IP 地址分配给 DHCP 客户端。 NISG-IPS 支持 256 个作用域。

4.13.2 基本配置步骤

1. 选择**网络** > **DHCP** > **DHCP 作用域**。
2. 点击**新建**，为 DHCP 服务器创建作用域。
   a. 输入作用域的名称。
   b. 在 IPv4 文本框中输入一个子网。

提示：在 **IPv4 地址**文本框中填写的子网以及 **IP 地址池列表**和**保留地址列表**中的 IP 地址应与作为 DHCP 服务器的三层接口的 IP 地址在同一网段。

---

   c. 输入与子网匹配的掩码。
   d. 在 **IP 地址池列表**中，点击**添加**，添加 IP 地址范围。此范围中的 IP 地址会被分配给 DHCP 客户端。
   e. 在**保留地址列表**中，点击**添加**，设置 IP 地址和 MAC 地址的绑定关系。此 IP 地址会被分配给指定 MAC 地址的客户端。

3. 为分配的 IP 地址配置租期。**无限制**表示无时间限制。

4. 配置高级设置。

5. 点击**确定**。
6. 点击。

表 128 DHCP 作用域命令

dhcp subnet	添加 DHCP 作用域。
unset dhcp subnet	删除 DHCP 作用域。
dhcp subnet domain	设置指定作用域的域名。
unset dhcp subnet domain	删除指定作用域的域名。
dhcp subnet dynamic	为指定的作用域添加地址池。
unset dhcp subnet dynamic	删除指定作用域的地址池。
dhcp subnet reserve	设置指定作用域的保留地址。
unset dhcp subnet reserve	删除指定作用域的特定保留地址。
dhcp subnet gateway, wins, dns, smtp, pop3, news, nis	设置指定作用域的特定服务的 IP 地址。
unset dhcp subnet gateway, wins, dns, smtp, pop3, news, nis	删除指定作用域的特定服务的 IP 地址。
dhcp subnet nistag	设置指定作用域的网络信息服务器的标签。
unset dhcp subnet nistag	删除指定作用域的网络信息服务器的标签。
dhcp subnet lease	设置指定作用域的租期。
show dhcp server subnet	显示 DHCP 作用域的配置信息。

4.13.3 配置参数说明

表 129 作用域配置信息

配置信息	说明
名称	作用域的名称。 1~63 字节的 UTF-8 字符，不包含：?,'\"<>&# 和空格。
网络地址	为作用域配置的子网及掩码长度。 地址类型为 IPv4 地址，格式为 [1-223].[0-225].[0-225].[0-225]，不能输入 127.0.0.0~127.255.255.255。
IP 地址池	包含一个或多个 IP 地址或地址范围。 DHCP 服务器将地址池中的 IP 地址分配给 DHCP 客户端。 IP 地址池列表中，最多支持 256 个 IP 地址。
保留 IP 地址	为指定的 DHCP 客户端保留的 IP 地址。 保留地址列表中，最多支持 256 个保留地址。
租期	即在作用域内分配的 IP 地址租期时间。 租期时间范围为 1 ～ 1440000 分钟，可以不限制租期时间。如果在 NISG-IPS 运行期间修改了租期时间，那么对于正在使用的租期将采用原有配置，直到相应客户端发送 DHCPREQUEST 报文请求更新租期后， NISG-IPS 自动更新租期时间。
高级设置	为 DHCP 客户端分配的其他网络配置参数，包括网关、域名、 DNS 服务器、 NEWS 服务器、 POP3 服务器、 SMTP 服务器、 WINS 服务器、 NetInfo 服务器以及 NetInfo 标签。 网关及上述服务器的 IP 地址格式为 [1-223].[0-255].[0-255].[0-255]，不能输入 127.0.0.0~127.255.255.255 或者 192.168.255.254。 NetInfo 标签名字为 0~255 字节的 UTF-8 字符，不包含：?'\"<>&。

4.14 DHCP Snooping

4.14.1 概述

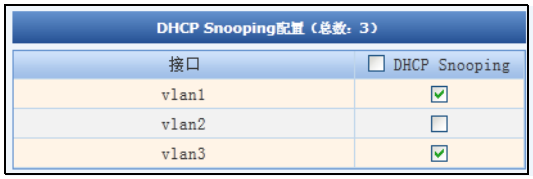
NISG-IPS 的DHCP Snooping特性可以监听同一VLAN中DHCP客户端和DHCP服务器之间的 DHCP 报文，生成以下信息的映射关系：

- DHCP 客户端的 MAC 地址以及获取到的 IP 地址
- 与客户端连接的 NISG-IPS 接口
- 接口所属的 VLAN

当 DHCP 客户端发送 DHCP Release 报文时， NISG-IPS 会删除此映射关系。

4.14.2 基本配置步骤

1. 选择**网络** > **DHCP** > **DHCP Snooping**。
2. 勾选 **DHCP Snooping** 复选框，启用所有 VLAN 接口的 DHCP Snooping 功能。勾选 VLAN 接口对应的复选框，启用此接口 DHCP Snooping 功能。如需禁用功能，取消勾选相应的复选框。



3. 点击**确定**。
4. 点击。

选择**监控** > **DHCP IP 地址绑定状态列表**，可以查看客户端的从 DHCP 服务器获取到的 IP 地址以及客户端的 MAC 地址等信息。

表 130 DHCP Snooping 命令

dhcp snooping	启用或禁用 DHCP Snooping。
show dhcp snooping	查看 DHCP Snooping 配置信息。

4.14.3 配置参数说明

表 131 DHCP Snooping 配置信息

配置信息	说明
DHCP Snooping	启用 / 禁用 NISG-IPS 上所有接口的 DHCP Snooping 功能。
接口	启用 / 禁用 VLAN 接口的 DHCP Snooping 功能。

4.15 DHCPv6

4.15.1 概述

DHCPv6 （IPv6 动态主机配置协议）用于 IPv6 寻址，为主机分配 IPv6 地址、 IPv6 前缀及其他网络配置参数。

- 有状态 DHCPv6 配置：指通过 DHCPv6 服务器分配 IPv6 地址和前缀。由于 DHCPv6 服务器保留已分配的地址和前缀信息，所以该过程称为有状态配置。
- 无状态 DHCPv6 配置：指设备通过无状态地址自动配置获取 IPv6 地址之后，再利用 DHCPv6 服务器获取除了地址以外的其他网络配置参数 （如 DNS 服务器、域名等）。在无状态 DHCPv6 配置过程中， DHCPv6 服务器不需要保存客户端的状态信息，因此称为无状态 DHCPv6 配置。

NISG-IPS 可以：

- 作为客户端，支持对 DHCPv6 前缀和其他网络配置参数的分配请求，暂不支持 DHCPv6 地址分配请求。
- 作为无状态 DHCPv6 服务器，为客户端分配 DNS 服务器地址、SNTP (Simple Network Time Protocol) 服务器地址和域名等网络配置参数。

下表列出可以作为 DHCPv6 客户端和无状态服务器的接口：

表 132 DHCPv6 接口

DHCPv6 客户端	无状态 DHCPv6 服务器
三层或共享三层以太网接口	三层或共享三层以太网接口
三层或共享三层以太网通道	三层或共享三层以太网通道
三层或共享三层冗余接口	三层或共享三层冗余接口
三层虚拟接口	三层虚拟接口
VLAN 接口	VLAN 接口
PPPoE 接口	

4.15.2 基本配置步骤

在为三层或共享三层接口配置 DHCPv6 之前，需要首先选择**网络** > **接口**，启用该接口的 IPv6 功能。

1. 选择**网络** >**IPv6**>**DHCPv6**。点击接口对应的 。
2. 在**类型**下拉框中选择 DHCPv6 类型：
   - **客户端**：将接口设置为 DHCPv6 客户端。
     - 点击**发送 DHCP 请求**按钮，作为DHCPv6客户端的接口会先后发送DHCP-PD和DHCP-inform 请求。
     - 在 **IPv6 地址列表**中，设置接口的 IPv6 地址。
     - 在**前缀分配列表**中，设置为其他三层接口所在的子网推送含有 64 位前缀的 RA 通告，同时为该接口配置基于推送前缀的 IPv6 地址。
     - 勾选**覆盖 DNS**，NISG-IPS 发送DHCP 请求时，会用获取到的DNS 覆盖NISG-IPS 中原有的 DNS 服务器信息。
     - 勾选**启用 DNS 代理**，系统将根据通过 DHCPv6 客户端接口获得的DNS 自动添加 DNS 代理。

- **服务器**：将接口设置为 DHCPv6 服务器。

- **不使用探测**：表示不使用 DHCPv6 探测功能。

3. 点击**确定**。
4. 点击 。

表 133 DHCPv6 命令

dhcpv6 type {client | none | server}	设置指定三层或共享三层接口的 DHCPv6 工作模式。
dhcpv6 ip	为指定的 DHCPv6 客户端接口配置 SLA 以及接口标识。
unset dhcpv6 ip	删除指定 DHCPv6 客户端接口的 SLA 以及接口标识。
dhcpv6 prefix-assignment	为指定的 DHCPv6 客户端接口配置前缀推送接口以及前缀推送接口的 SLA 和接口标识。
unset dhcpv6 prefix-assignment	删除指定 DHCPv6 客户端接口的前缀推送接口以及前缀推送接口的 SLA 和接口标识。
dhcpv6 overwrite-dns	为指定的 DHCPv6 客户端接口启用 DNS 覆盖功能。
unset dhcpv6 overwrite-dns	为指定的 DHCPv6 客户端接口禁用 DNS 覆盖功能。
dhcpv6 enable-dns-proxy	启用为 DHCPv6 客户端接口自动添加 DNS 代理的功能。
unset dhcpv6 enable-dns-proxy	禁用为 DHCPv6 客户端接口自动添加 DNS 代理的功能。
dhcpv6 client send-request	向 DHCPv6 服务器发送 DHCPv6 客户端请求。
show dhcpv6-client	显示 DHCPv6 客户端接口从 DHCPv6 服务器获取的配置信息。
show dhcpv6-client-config	显示 DHCPv6 客户端接口的配置信息。
dhcpv6 server-type {auto interface | manual}	通过手动方式或自动从 DHCPv6 客户端接口更新的方式配置无状态 DHCPv6 服务器信息。
dhcpv6 server {dns | dns2}	设置无状态 DHCPv6 服务器的 DNS 服务器信息。

表 133 DHCPv6 命令 (*续*)

unset dhcpv6 server {dns | dns2}	删除无状态 DHCPv6 服务器的 DNS 服务器配置信息。
dhcpv6 server domain_search_list	向无状态 DHCPv6 服务器的 Domain Search List （域名搜索列表）添加域名信息。
unset dhcpv6 server domain_search_list	删除无状态 DHCPv6 服务器的域名搜索列表中的指定域名信息。
dhcpv6 server {sntp | sntp2}	设置无状态 DHCPv6 服务器的 SNTP 服务器信息。
unset dhcpv6 server {sntp | sntp2}	删除无状态 DHCPv6 服务器的 SNTP 服务器信息。
show dhcpv6-server-config	显示无状态 DHCPv6 服务器接口的配置信息。

4.15.3 配置参数说明

表 134 DHCPv6 客户端属性

配置信息	说明
接口	DHCPv6 客户端接口。可以是三层或共享三层以太网接口、三层或共享三层以太网通道、三层或共享三层冗余接口、三层虚拟接口、 VLAN 接口以及 PPPoE 接口。
DUID	DHCPv6 设备的唯一标识符 （包括 DHCPv6 客户端、中继和服务器），用于 DHCPv6 设备之间的相互验证。该值是系统自动生成的。
类型	接口的 DHCPv6 工作模式，包括以下三种： • **不使用探测**：表示不使用 DHCPv6 探测功能。 • **客户端**：表示 DHCPv6 客户端模式。 • **服务器**：表示无状态 DHCPv6 服务器模式。
发送 DHCP 请求	点击该按钮，作为 DHCPv6 客户端的接口会先后发送 DHCP-PD 和 DHCP-inform 请求。
IPv6 地址列表	通过配置该列表，可以为工作模式为 DHCPv6 客户端的接口配置 IPv6 地址，配置项包括 SLA 以及接口 ID。 • **SLA**：表示对 DHCPv6 获得前缀的子网划分功能，取值范围为 0000 ～ FFFF。 SLA 与 DHCPv6 获得的前缀进行右对齐计算出 64 位前缀。 • **接口 ID**：包括手动和 EUI-64。当指定手动时，表示不使用 EUI-64 格式的接口标识；当指定 EUI-64 时，表示使用 EUI-64 格式的接口标识。 SLA 和接口 ID 结合 DHCP-PD 请求获得的前缀，共同组成一个前缀长度为 64 的 IPv6 地址。管理员最多可以添加 8 个条目。
前缀分配列表	通过配置该列表，可以为指定的三层接口所在的子网推送含有 64 位前缀的 RA 通告，同时为该接口配置基于推送前缀的 IPv6 地址。 配置项包括接口、 SLA 以及接口 ID。这里的接口指请求客户端之外的三层接口 （不包括环回接口、隧道接口和 PPPoE 接口）， SLA 和接口 ID 属性与 **IPv6 地址列表**中的属性相同。 对于每个接口，管理员最多可以添加 8 个条目。
覆盖 DNS	NISG-IPS 发送 DHCP 请求时，会用获取到的 DNS 覆盖 NISG-IPS 中原有的 DNS 服务器信息。
启用 DNS 代理	系统将根据通过 DHCPv6 客户端接口获得的 DNS 自动添加 DNS 代理。

表 135 无状态 DHCPv6 服务器属性

配置信息	说明
接口	无状态 DHCPv6 服务器接口，可以是三层或共享三层以太网接口、三层或共享三层以太网通道、三层或共享三层冗余接口、三层虚拟接口以及 VLAN 接口。
DUID	DHCPv6 设备的唯一标识符 （包括 DHCPv6 客户端、中继和服务器），用于 DHCPv6 设备之间的相互验证。该值是系统自动生成的。
类型	接口的 DHCPv6 工作模式，包括以下三种： • **不使用探测**：表示不使用 DHCPv6 探测功能。 • **客户端**：表示 DHCPv6 客户端模式。 • **服务器**：表示无状态 DHCPv6 服务器模式。
服务器信息	包括两种配置无状态 DHCPv6 服务器信息的方式。 • **从 DHCPv6 客户端接口更新**：表示通过指定 DHCPv6 客户端接口更新无状态 DHCPv6 信息。即服务器从指定 DHCPv6 客户端获取无状态信息作为自身的配置，并将这些配置信息分配给请求客户端。当指定 DHCPv6 客户端的无状态信息发生变化时，服务器需要同步更新自身的配置。 • **手动**：手动配置服务器无状态信息。当有客户端发起请求时，服务器将无状态 DHCPv6 信息分配给客户端。 **•DNS**：DNS 服务器的 IPv6 地址，包括 DNS1 和 DNS2。不可以是环回地址 （::1）、多播地址 （FF00/8~FFFF/8）、未指定地址 （::）和 ::FFFF:0:0/96。 **•域名搜索列表**：由最多 8 个域名组成。 **•SNTP 服务器**：SNTP 服务器的 IPv6 地址，包括 SNTP 服务器 1 和服务器 2。不可以是环回地址 （::1）、多播地址 （FF00/8~FFFF/8）、未指定地址 （::）和 ::FFFF:0:0/96。

4.16 邻居发现

4.16.1 概述

邻居发现 （Neighbor Discovery， ND）协议被节点 （主机和路由器）用来发现同一链路上的邻居。

- ND 报文类型

表 136 ND 报文类型

ND 消息名称	ICMPv6 类型值	作用
路由器请求 （RS）	133	当接口启用时，主机向路由器发送 RS 消息，请求立即产生 RA 消息，而不必等到下次预计的时间。
路由器通告 （RA）	134	路由器通告其自身的存在，并携带各种链路参数与互联网参数，例如前缀、当前跳数限值等。 RA 消息可以由路由器周期性发出，也可以因响应 RS 消息而发出。
邻居请求 （NS）	135	节点发出 NS 消息，以探测邻居的链路层地址，或者验证邻居仍然是可达的。此外也用于进行重复地址检测。
邻居通告 （NA）	136	对 NS 消息的响应。节点也可以发送非请求的 NA 消息，以通告链路层地址的改变。
重定向 （Redirect）	137	路由器用该消息通知源主机可以到达目的地的更优第一跳。

- ND 提供如下几种主要功能，用来解决网络中邻居节点之间通讯和互动的问题：
  - 路由器、前缀、参数发现
  - 下一跳判定
  - 地址解析与邻居不可达检测
  - 无状态地址自动配置与重复地址检测
  - 重定向

4.16.2 基本配置步骤

在接口配置 ND 之前，需要首先选择**网络** > **接口**，启用该接口的 IPv6 功能。

1. 选择**网络** >**IPv6**> **邻居发现配置**。
2. 点击接口对应的 。
3. 配置 ND 和 RA 信息。关于参数的相信信息，参见 4.16.3 配置参数说明。

4. 点击**确定**。
5. 点击 。

表 137 ND 命令

ipv6 nd dad detect	设置重复地址检测时发送邻居请求消息的次数。
ipv6 nd reachable-time	为指定的接口设置保持邻居可达状态的时间。
ipv6 nd retrans-timer	为指定的接口设置邻居请求消息的重传时间间隔。
ipv6 nd ra suppress	抑制指定的接口发送 RA 消息。
unset ipv6 nd ra suppress	允许指定接口发送 RA 消息。
ipv6 nd ra router-lifetime	设置 RA 消息中发布的路由器生存时间。
ipv6 nd ra interval	设置 RA 消息发布的时间间隔。
ipv6 nd ra hop-limit	设置 RA 消息中发布的跳数限制。

表 137 ND 命令 (*续*)

ipv6 nd ra managed-flag {on | off}	设置 RA 消息中的被管理地址配置标志位。
ipv6 nd ra other-flag {on | off}	设置设置 RA 消息中的其他配置标志位。
ipv6 nd ra retrans-timer {on | off}	设置 RA 消息中是否携带邻居请求消息的重传时间间隔。
ipv6 nd ra reachable-time {on | off}	设置 RA 消息中是否携带接口保持邻居可达状态的时间。
ipv6 nd ra link-address {on | off}	设置 RA 消息中是否携带接口的 MAC 地址。
ipv6 nd ra advlinkmtu {on | off}	设置 RA 消息中是否携带接口的 MTU。
ipv6 nd ra prefix	设置 RA 消息中的前缀信息及其相关的通告参数。
unset ipv6 nd ra prefix	删除 RA 消息中的前缀信息及其相关的通告参数。

4.16.3 配置参数说明

表 138 ND 配置属性

配置信息	说明
重复地址检测（DAD）重试次数	进行 DAD 检测时，发送 NS 消息的次数。取值范围为 0~600。
重传时间	进行 DAD 检测时，发送 NS 消息的间隔时间。取值范围为 1000~3600000 毫秒。 如果在设置的间隔时间内没有收到响应，则继续发送 NS 消息。当发送的次数达到所设置的 DAD 检测重试次数后，仍未收到响应，则认为待检测的地址可用。
基础可达时间	用于计算可达时间的基准值。可达时间即接口保持某个邻居可达状态的时间长度；在可达时间范围内，接口向该邻居转发流量。 取值范围为 1~3600000 毫秒。

表 139 RA 配置属性

配置信息	说明
抑制 RA 传输	抑制接口的 RA 通告，表示不允许在某个特定接口上进行 RA 通告。
路由器生存时间	RA 消息发布的路由器生存时间，即作为缺省路由器的时间。取值范围为 0~9000 秒。当该值为 0 时，表示 NISG-IPS 将不作为缺省路由器。 主机根据接收到的 RA 消息中的该值，就可以确定是否将发布该 RA 消息的设备作为默认路由器。
最大通告间隔	未请求的 RA 消息发布的最大时间间隔。取值范围为 4-1800 秒，该值必须小于或等于路由器生存时间的值。 配置 RA 消息发布的最大 / 最小时间间隔后，设备将在这两个时间间隔值之间随机选择一个值，作为周期性发布 RA 消息的时间间隔。
最小通告间隔	未请求的 RA 消息发布的最小时间间隔。取值范围为 3-1350 秒，该值必须小于或等于最大时间间隔值的 0.75 倍。
跳数限制	在 RA 报文中发布的跳数限制。取值范围为 0~255。
M 标志位	当启用该功能时，表示接收到 RA 消息的接口除了通过无状态地址自动配置外，还可以通过有状态地址配置获取 IPv6 地址。禁用该功能时，表示接收到 RA 消息的接口只可以通过无状态地址自动配置获取 IPv6 地址。

表 139 RA 配置属性 (*续*)

配置信息	说明
O 标志位	当启用该功能时，表示接收到 RA 消息的接口可以通过无状态 DHCPv6 配置获取 IPv6 地址以外的网络配置信息。禁用该功能时，表示接收到 RA 消息的接口不能通过无状态 DHCPv6 配置获取 IPv6 地址以外的网络配置信息。
重传时间	表示是否在 RA 报文中携带重传时间。如果启用该功能，则 RA 报文中将携带 ND 配置中所设置的重传时间的值。 设备发送 NS 消息后，如果未在指定的时间间隔内收到响应，则会重新发送 NS 消息。
可达时间	表示是否在 RA 报文中携带可达时间。如果启用该功能，则 RA 报文中将携带 ND 配置中所设置的可达时间的值。 当通过邻居可达性检测确认邻居可达后，在所设置的可达时间内，设备认为邻居可达；超过设置的时间后，如果需要向邻居发送报文，会重新确认邻居是否可达。
链路层地址	表示是否在 RA 报文中携带链路层地址。如果启用该功能，则 RA 报文中将携带通告接口的源链路层地址。
链路 MTU	表示是否在 RA 报文中携带 MTU。如果启用该功能，则 RA 报文中将携带通告接口自身的 MTU 值。
前缀列表	通过配置该列表，可以指定 RA 报文中通告的前缀的相关信息，配置项包括： • **IPv6 地址**：RA 通告前缀。 • **前缀长度**：通告前缀的长度。 • **首选生存时间**：通告前缀的首选时间。取值范围为 0-4294967295 秒。 • **有效生存时间**：通告前缀的有效时间。取值范围为 0-4294967295 秒。 • **不通告**：不在 RA 消息中通告该前缀。该功能缺省为禁用，表示在 RA 消息中通告该前缀。 • **非自动配置**：不用该前缀进行无状态地址自动配置。该功能缺省为禁用，表示该前缀可以用于无状态地址自动配置。 • **非在链**：该前缀非直连可达。从 NISG-IPS 收到 RA 报文的接口将根据 RA 报文中的 L 标志位判断其自身是否与 NISG-IPS 的 RA 通告接口处于同一链路。该功能缺省为禁用，表示该前缀是直连可达的。 管理员可以添加最多 32 条通告前缀，且各通告前缀不可以重叠。另外，添加的通告前缀不可以是本地链路前缀、全 0 前缀或者多播前缀。

4.17 网络配置范例

提示：范例里的 IP 地址只是用于举例说明。可以根据实际需要更改 IP 地址。

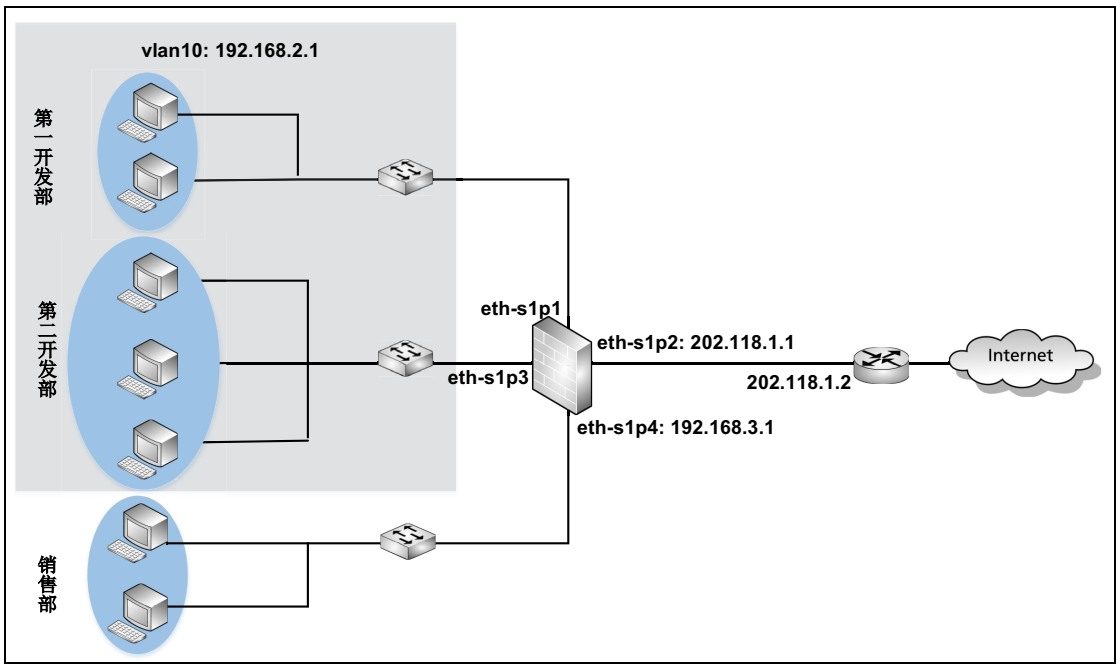
4.17.1 范例：配置以太网接口并划分 VLAN

某公司有两个开发部和一个销售部。

基本需求

- 为加强网络管理并提高安全性，第一开发部和第二开发部需划分到一个 VLAN 内。
- 为方便员工查找资料，允许开发部和销售部访问 Internet。
- 为防范内网员工，开发部和销售部不能互相访问。
- 为保证内网信息安全，不允许 Internet 用户访问公司内网。

组网拓扑



配置要点

- 配置以太网接口，设置以太网接口的工作模式和 IP 地址。
- 创建 VLAN 接口，将二层以太网接口划分给 VLAN 接口并为 VLAN 接口设置 IP 地址。
- 创建源地址转换规则，使内网员工可以通过 eth-s1p2 接口的公有 IP 地址访问 Internet。
- 创建访问策略，允许内网员工访问 Internet，不允许开发部和销售部互相访问，不允许外网用户访问内网。
- 创建路由，将下一跳 IP 地址设置为路由器的 IP 地址 202.118.1.2。

配置步骤

配置以太网接口

1. 选择**网络** > **接口**。
2. 在**接口列表中**分别点击接口所对应的，进行如下配置：
   - eth-s1p1：
     - 模式：二层
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.118.1.1/24
   - eth-s1p3：
     - 模式：二层
   - eth-s1p4：
     - 模式：三层
     - （静态） IP 地址：192.168.3.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer2-interface
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer2-interface
NetEye@root-system-if-eth-s1p3] exit
NetEye@root-system] interface ethernet s1p4
NetEye@root-system-if-eth-s1p4] working-type layer3-interface
NetEye@root-system-if-eth-s1p4] ip address 192.168.3.1 255.255.255.0
NetEye@root-system-if-eth-s1p4] end
NetEye@root> save config
```

创建 VLAN 接口

1. 选择**网络** > **接口**
2. 点击**新建** > **VLAN**，创建 vlan10。
3. 点击**确定**。
4. 点击 vlan10 所对应的，进行如下配置：
   - 二层接口列表 > 已选接口：eth-s1p1， eth-s1p3
   - （静态） IP 地址：192.168.2.1/24
5. 点击**确定**。
6. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vlan 10
NetEye@root-system-vlan10] hold ethernet s1p1,s1p3
NetEye@root-system-vlan10] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-vlan10] end
NetEye@root> save config
```

创建源地址转换规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建以下规则：
   - 序号：1
   - 名称：snat1
   - NAPT：勾选
   - 源 IP 地址列表 > IPv4 地址 / 掩码：192.168.2.0/24， 192.168.3.0/24
   - 转换后接口：eth-s1p2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 netmask 192.168.2.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] policy snat snat1 append before netmask
192.168.3.0 255.255.255.0
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy1：
     - 序号：1
     - 源安全域：任意
     - 源 IP：192.168.2.0/24， 192.168.3.0/24
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：允许
   - policy2：
     - 序号：2
     - 源安全域：任意
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：192.168.2.0/24， 192.168.3.0/24
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy1 any 192.168.2.0/24 any any any any permit enable 1
NetEye@root-system] policy access policy1 sourceip 192.168.3.0 netmask 255.255.255.0
NetEye@root-system] policy access policy2 any any any 192.168.2.0/24 any any deny enable 2
NetEye@root-system] policy access policy2 desip 192.168.3.0 netmask 255.255.255.0
NetEye@root-system] exit
NetEye@root> save config
```

创建路由

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，创建以下缺省路由：
   - 类型：IPv4 地址
   - 目的 IPv4 地址：0.0.0.0
   - 掩码长度：0
   - Metric：1
   - 出口接口：eth-s1p2
   - 网关：202.118.1.2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.1.2 1
NetEye@root-system] exit
NetEye@root> save config
```

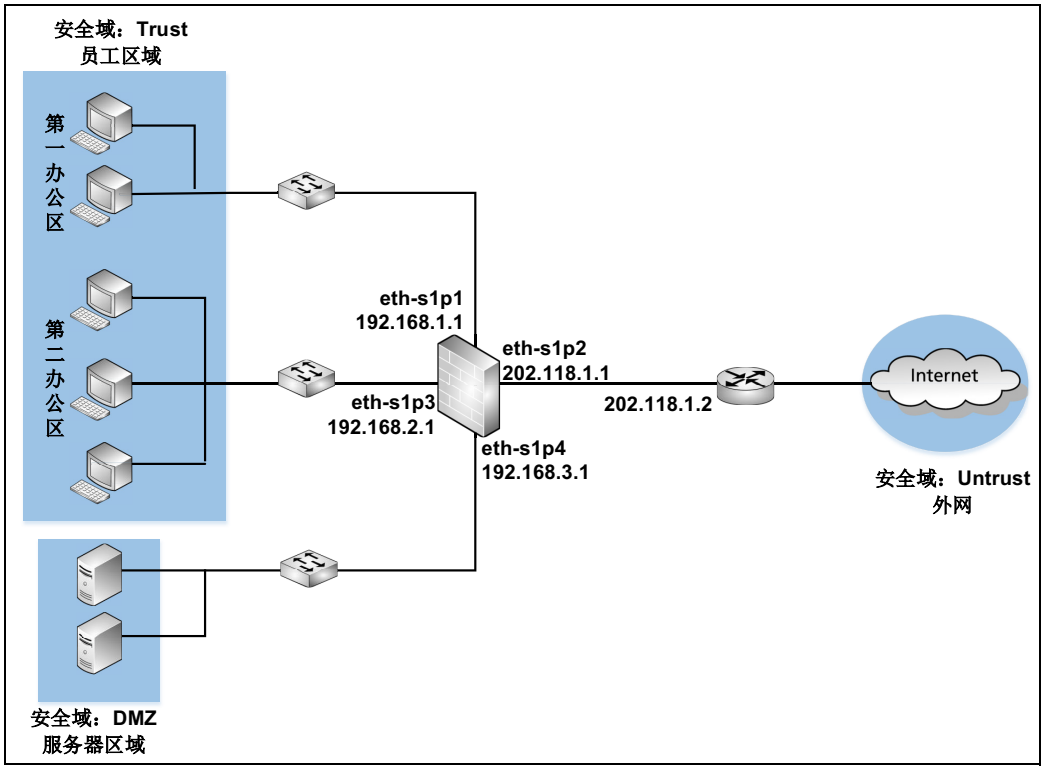
4.17.2 范例：划分安全域

某公司有两个办公区域和一个服务器区域。

基本需求

- 为制定统一的访问控制策略，将公司的两个办公区域划分到同一个安全域内；将服务器区域和外网各划分到不同的安全域。
- 允许内网员工访问服务器区域和 Internet。
- 允许服务器访问 Internet 进行自动更新，不允许服务器访问员工区域。
- 不允许 Internet 用户访问公司内网。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 创建安全域，将三层以太网接口划分到安全域中。
- 创建源地址转换规则，使内网可以通过 eth-s1p2 接口的公有 IP 地址访问 Internet。
- 创建访问策略，允许员工区域访问 Internet 和服务器区域，允许服务器访问 Internet，不允许服务器访问员工区域，不允许 Internet 用户访问内网。
- 创建路由，将下一跳 IP 地址设置为路由器的 IP 地址 202.118.1.2。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击接口所对应的，并配置接口为如下：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.118.1.1/24
   - eth-s1p3：
     - 模式：三层
     - （静态） IP 地址：192.168.2.1/24
   - eth-s1p4：
     - 模式：三层
     - （静态） IP 地址：192.168.3.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p3] exit
NetEye@root-system] interface ethernet s1p4
NetEye@root-system-if-eth-s1p4] working-type layer3-interface
NetEye@root-system-if-eth-s1p4] ip address 192.168.3.1 255.255.255.0
NetEye@root-system-if-eth-s1p4] end
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1， eth-s1p3
   - DMZ：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p4
   - Untrust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust
NetEye@root-system] zone Trust based-layer3 eth-s1p1,eth-s1p3
NetEye@root-system] zone DMZ
NetEye@root-system] zone DMZ based-layer3 eth-s1p4
NetEye@root-system] zone Untrust
NetEye@root-system] zone Untrust based-layer3 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

创建源地址转换规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建以下源地址转换规则：
   - 序号：1
   - 名称：snat1
   - NAPT：勾选
   - 源 IP 地址列表 > IPv4 地址 / 掩码：192.168.1.0/24， 192.168.2.0/24， 192.168.3.0/24
   - 转换后接口：eth-s1p2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] policy snat snat1 append before netmask
192.168.2.0 255.255.255.0
NetEye@root-system] policy snat snat1 append before netmask
192.168.3.0 255.255.255.0
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy11：
     - 序号：1
     - 源安全域：Trust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：允许
   - policy12：
     - 序号：2
     - 源安全域：Untrust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：拒绝
   - policy13：
     - 序号：3
     - 源安全域：DMZ
     - 源 IP：任意
     - 目的安全域：Untrust
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：允许
   - policy14：
     - 序号：4
     - 源安全域：DMZ
     - 源 IP：任意
     - 目的安全域：Trust
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy11 Trust any any any any any permit enable 1
NetEye@root-system] policy access policy12 Untrust any any any any any deny enable 2
NetEye@root-system] policy access policy13 DMZ any Untrust any any any permit enable 3
NetEye@root-system] policy access policy14 DMZ any Trust any any any deny enable 4
NetEye@root-system] exit
NetEye@root> save config
```

创建路由

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，创建以下路由：
   - 类型：IPv4 地址
   - 目的 IPv4 地址：0.0.0.0
   - 掩码长度：0
   - Metric：1
   - 出口接口：eth-s1p2
   - 网关：202.118.1.2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.1.2 1
NetEye@root-system] exit
NetEye@root> save config
```

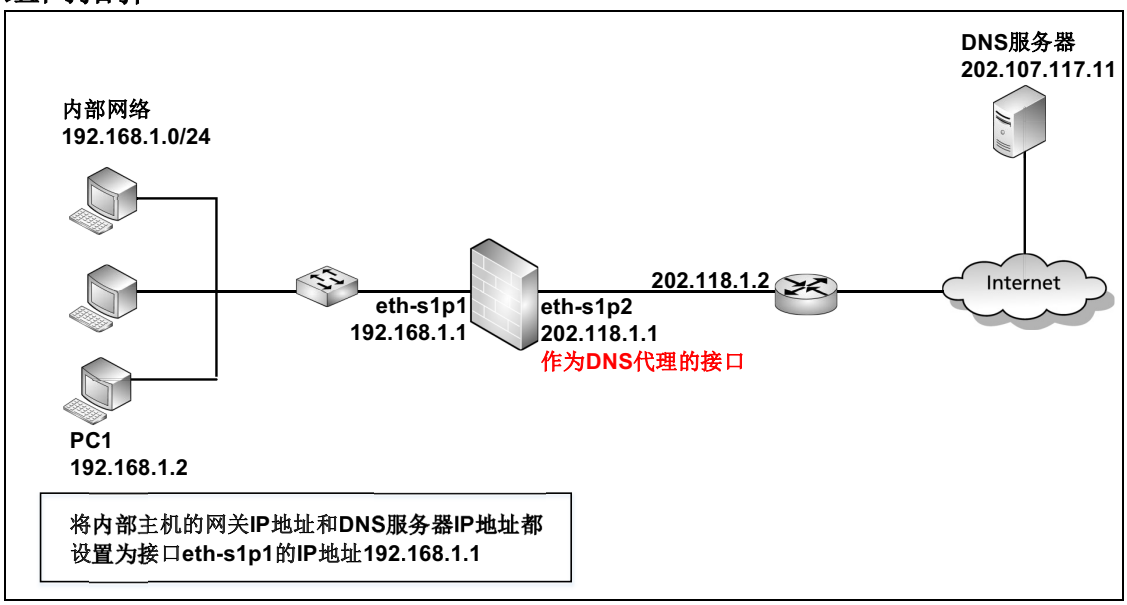
4.17.3 范例：NISG-IPS 作为 DNS 代理

某公司的内部网络通过 NISG-IPS 与 Internet 相连。

基本需求

为提升网络访问速度，公司要求内网员工使用 DNS 代理访问 Internet。

组网拓扑



配置要点

- 配置接口，设置接口的工作模式和 IP 地址。
- 配置DNS代理，将NISG-IPS的eth-s1p2接口设置为DNS代理并配置DNS服务器的IP地址。
- 创建源地址转换规则，使内网用户可以通过 eth-s1p2 接口的公有 IP 地址访问 Internet。
- 创建访问策略，允许内网用户访问 Internet，不允许外网用户访问内网用户。
- 创建路由，将下一跳 IP 地址设置为路由器的 IP 地址 202.118.1.2。
- 验证结果

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击接口所对应的，并配置接口为如下：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.118.1.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

配置 DNS 代理

1. 选择**网络** > **DNS** > **DNS 代理**。
2. 点击**新建**。
   - 域名：*

     设置要访问的域名， * 代表所有域名。
   - 接口：eth-s1p2

     选择要作为 DNS 代理的接口。如不指定具体的接口，可以选择 Any。
   - 首选 DNS：202.107.117.11

     设置 DNS 服务器。可根据需求设置备选服务器。
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dns server-select * output-interface eth-s1p2
primary 202.107.117.11
NetEye@root-system] exit
NetEye@root> save config
```

创建源地址转换规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建以下规则：
   - 序号：1
   - 名称：snat1
   - NAPT：勾选
   - 源 IP 地址列表 > IPv4 地址 / 掩码：192.168.1.0/24
   - 转换后接口：eth-s1p2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy1：
     - 序号：1
     - 源安全域：任意
     - 源 IP：192.168.1.0/24
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：允许
   - policy2：
     - 序号：2
     - 源安全域：任意
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：192.168.1.0/24
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy1 any 192.168.1.0/24 any any any any permit enable 1
NetEye@root-system] policy access policy2 any any any 192.168.1.0/24 any any deny enable 2
NetEye@root-system] exit
NetEye@root> save config
```

创建路由

1. 选择**网络 > 路由 > 缺省路由**。
2. 点击**新建**，创建以下缺省路由：
   - 类型：IPv4 地址
   - 目的 IPv4 地址：0.0.0.0
   - 掩码长度：0
   - Metric：1
   - 出口接口：eth-s1p2
   - 网关：202.118.1.2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.1.2 1
NetEye@root-system] exit
NetEye@root> save config
```

验证结果

在内网主机 PC1 上访问 www.baidu.com，可以访问成功。在 PC1 上抓取数据包，结果为如下：

	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	192.168.1.1	DNS	Standard query A www.baidu.com
2	0.023333	192.168.1.1	192.168.1.2	DNS	Standard query response CNAME www.a.shifen.com A 220.181.112.244 A 220.181.111.188
3	0.025374	192.168.1.2	220.181.112.244	TCP	1272 > http [SYN] Seq=0 Len=0 MSS=1460
4	0.127016	220.181.112.244	192.168.1.2	TCP	http > 1272 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440
5	0.127079	192.168.1.2	220.181.112.244	TCP	1272 > http [ACK] Seq=1 Ack=1 Win=64800 Len=0
6	0.127697	192.168.1.2	220.181.112.244	HTTP	GET / HTTP/1.1
7	0.129912	220.181.112.244	192.168.1.2	TCP	http > 1272 [ACK] Seq=1 Ack=327 Win=65209 Len=0

从上图可以看出， PC1 将 DNS 请求发送给作为 DNS 代理的 NISG-IPS， NISG-IPS 再将 DNS 应答返回给 PC1。同时在 NetEye 上也自动生成了 www.baidu.com 与对应 IP 地址的动态 DNS 缓存记录。选择**监控 > DNS 缓存**，可以查看 DNS 缓存。

在 PC1 上再次访问 www.baidu.com， NISG-IPS 会查询动态 DNS 缓存，将记录中对应的 IP 地址返回给 PC1。 NISG-IPS 不再向 DNS 服务器发送域名请求，提升了访问速度。抓包结果为如下：

	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	220.181.112.244	TLS	Application Data
2	0.086666	220.181.112.244	192.168.1.2	TCP	https > 1285 [ACK] Seq=0 Ack=603 Win=30464 Len=0
3	0.086711	220.181.112.244	192.168.1.2	TLS	Application Data
4	0.087220	220.181.112.244	192.168.1.2	TCP	[TCP segment of a reassembled PDU]
5	0.087249	220.181.112.244	192.168.1.2	TLS	Application Data

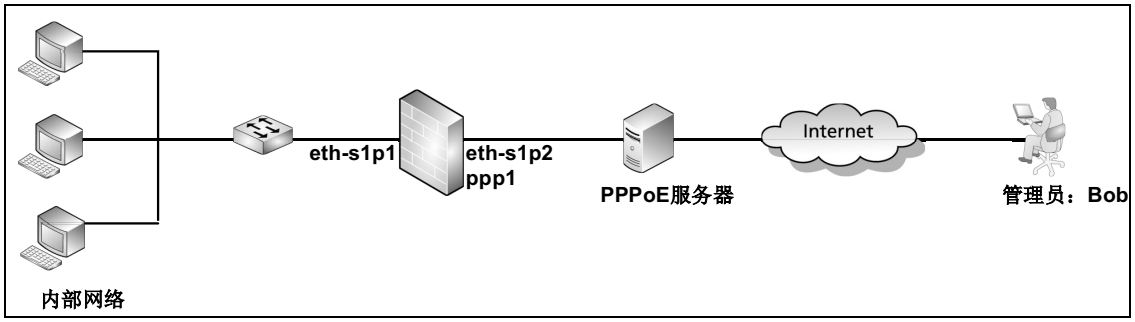
4.17.4 范例：配置动态 DNS

NISG-IPS 作为某公司网络的出口设备，通过 PPPoE 服务器与 Internet 相连。

基本需求

由于连接外网的 PPPoE 接口 ppp1 的公有 IP 地址是动态变化的，当公司网络管理员 Bob 在外网时，无法通过 ppp1 的 IP 地址登录到 NISG-IPS 上。因此，需要在 NISG-IPS 上配置动态 DNS 功能，将接口 ppp1 动态变化的 IP 地址映射到固定的域名上，以使 Bob 可以通过此域名访问 NISG-IPS。

组网拓扑



提示：需要预先在花生壳网站 （www.oray.com）上注册用户名和密码并设置域名。此域名与 ppp1 接口动态变化的 IP 地址绑定在一起。本范例使用的用户名是 example123456，对应的域名是 example123456.oicp.net。本范例只介绍如何在 NISG-IPS 上配置动态 DNS 功能，以使管理员可以在外网成功登录到 NISG-IPS 上，不介绍如何配置内部网络。

配置要点

- 创建 PPPoE 接口
- 配置动态 DNS
- 登录到 NISG-IPS

配置步骤

创建 PPPoE 接口

1. 选择**网络** > **接口**。点击**新建**，选择 **PPPoE**。创建 PPPoE 接口 ppp1。
2. 在**接口列表**中点击 ppp1 对应的，配置接口。
   - 模式：IPv4
   - 用户名：sy_12345678 （PPPoE 拨号用户的名称和密码）
   - 密码：123456
   - 以太网接口：eth-s1p2 （NISG-IPS 上的二层以太网接口）
   - 覆盖默认网关：勾选
   - 覆盖 DNS：勾选
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] ppp 1
NetEye@root-system-pppoe1] mode ipv4
NetEye@root-system-pppoe1] username sy_12345678 password 123456
NetEye@root-system-pppoe1] overwrite-default-gateway
NetEye@root-system-pppoe1] overwrite-dns
NetEye@root-system-pppoe1] hold ethernet eth-s1p2
NetEye@root-system-pppoe1] active on
NetEye@root-system-pppoe1] end
NetEye@root> save config
```

配置动态 DNS

1. 选择**网络** > **DDNS**。
2. 配置动态 DNS 功能。
   - DDNS：启用
   - 服务提供商：oray
   - PPPoE：ppp1 （要绑定的 PPPoE 接口）
   - 用户名：example123456 （已在 www.oray.com 上注册的用户名和密码）
   - 密码：12345678
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] ddns account example123456
NetEye@root-system] ddns password 123456789
NetEye@root-system] ddns interface ppp1
NetEye@root-system] ddns sp oray
NetEye@root-system] ddns daemon on
NetEye@root-system] exit
NetEye@root> save config
```

登录到 NISG-IPS

此时，管理员 Bob 在主机上打开浏览器，在地址栏输入 https://example123456.oicp.net，点击 **Enter** 键，便跳转到 NISG-IPS 的登录页面。

输入 NISG-IPS 的用户名和密码以及验证码，点击**登录**，跳转到 NISG-IPS 的 Home 页。之后 Bob 便可以对 NISG-IPS 进行配置。

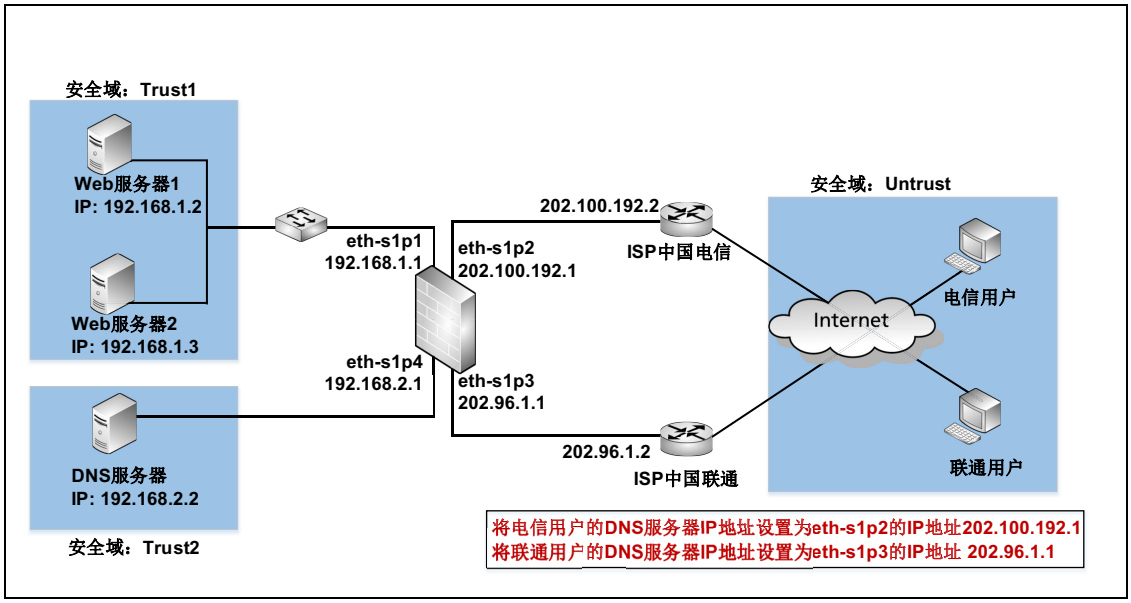
4.17.5 范例：配置入站智能 DNS

某公司的网站同时通过中国电信和中国联通带宽提供对外服务。网站的域名为 www.example.com，通过两台 Web 服务器提供服务。

基本需求

- Web服务器1利用电信的带宽提供对外服务，Web服务器2利用联通的带宽提供对外服务。
- 为提升网站访问速度，当电信用户和联通用户访问网站时，可以分别通过网站的电信 IP 地址和联通 IP 地址进行访问。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 配置入站智能 DNS，设置域名和 IP 地址的对应关系。
- 配置 DNS 代理，设置 DNS 服务器 IP 地址。
- 创建目的地址转换规则，为使外网用户可以访问内网服务器，需配置目的地址转换规则，将公有 IP 地址转换为 Web 服务器的私有 IP 地址。
- 创建安全域，将内网和外网划分到不同的安全域内。
- 创建访问策略，允许外网用户访问内网 Web 服务器。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击接口所对应的，并配置接口为如下：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.100.192.1/24
   - eth-s1p3：
     - 模式：三层
     - （静态） IP 地址：202.96.1.1/24
   - eth-s1p4：
     - 模式：三层
     - （静态） IP 地址：192.168.2.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.100.192.1 255.255.248.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 202.96.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p3] exit
NetEye@root-system] interface ethernet s1p4
NetEye@root-system-if-eth-s1p4] working-type layer3-interface
NetEye@root-system-if-eth-s1p4] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p4] end
NetEye@root> save config
```

配置入站智能 DNS

1. 选择**网络** > **DNS** > **入站智能 DNS**。
2. 启用入站智能 DNS 功能。
3. 点击**新建**，配置域名和IP地址以及权重的对应关系。列表中也给出了IP地址所属的运营商，此运营商是 NISG-IPS 自动识别的。
   - 域名：www.example.com
   - IP 地址：202.100.192.1 ； 权重：1
   - IP 地址：202.96.1.1 ； 权重：1

   提示：入站智能 DNS 的权重只对同一运营商的不同 IP 地址起作用。不同运营商 IP 地址的权重之间不会互相影响。
4. 点击**确定**。
5. 点击。

配置 DNS 代理

1. 选择**网络** > **DNS** >**DNS 代理**。
2. 点击**新建**，配置 DNS 服务器 IP 地址。
   - 域名：*
   - 接口：Any
   - 首选 DNS：192.168.2.2
3. 点击**确定**。
4. 点击。

提示：当用户通过 NISG-IPS 使用 DNS 查询时， NISG-IPS 首先在入站智能 DNS 中查询，如果查询失败， NISG-IPS 会通过代理功能将 DNS 请求发送给 DNS 服务器。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dns server-select * output-interface any primary
192.168.2.2
NetEye@root-system] exit
NetEye@root> save config
```

创建目的地址转换规则

1. 选择**网络 > 地址转换 > 目的地址转换**。
2. 点击**新建**，分别创建以下规则：
   - rule1：
     - 序号：1
     - 目的 IP：202.100.192.1
     - 目的端口 > TCP：80
     - 转换后 IP：192.168.1.2
     - 转换后端口 > TCP：80
   - rule2：
     - 序号：2
     - 目的 IP：202.96.1.1
     - 目的端口 > TCP：80
     - 转换后 IP：192.168.1.3
     - 转换后端口 > TCP：80

提示：为了方便用户访问，转换前端口一般设为知名端口如 80，此时建议开启攻击防御和 IPS 功能。

---

3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy dnat rule1 202.100.192.1 tcp 80
192.168.1.2 80 enable 1
NetEye@root-system] policy dnat rule2 202.96.1.1 tcp 80 192.168.1.3
80 enable 2
NetEye@root-system] exit
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust1：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - Untrust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2， eth-s1p3
   - Trust2：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p4
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust1
NetEye@root-system] zone Trust1 based-layer3 eth-s1p1
NetEye@root-system] zone Untrust
NetEye@root-system] zone Untrust based-layer3 eth-s1p2,eth-s1p3
NetEye@root-system] zone Trust2
NetEye@root-system] zone Trust2 based-layer3 eth-s1p4
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建以下访问策略：
   - 序号：1
   - 名称：policy1
   - 源安全域：Untrust
   - 源 IP：任意
   - 目的安全域：Trust1
   - 目的 IP/ 域名：192.168.1.2-192.168.1.3
   - 服务 > 自定义 > TCP：
     - 源端口：1-65535
     - 目的端口：80
   - 动作：允许
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy1 Untrust any Trust1
192.168.1.2-192.168.1.3 tcp 1-65535 80 any permit enable 1
NetEye@root-system] exit
NetEye@root> save config
```

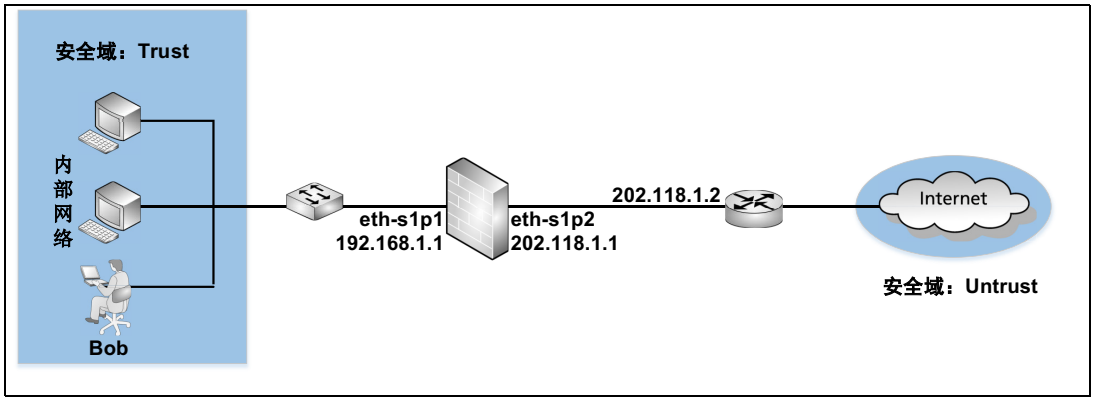
4.17.6 范例：NISG-IPS 作为 DHCP 服务器

某公司需要使用 NISG-IPS 给内网员工分配 IP 地址。

基本需求

- 将NISG-IPS设置为DHCP服务器并为内网员工分配地址段192.168.1.2-60中的IP地址。
- 名为 Bob 的员工必须使用 IP 地址 192.168.1.20，此员工的 MAC 地址为 44:37:E6:27:C5:D5。
- 为指定统一的访问控制策略，将内网和外网各划分到不同的安全域内。
- 内网员工可以通过 eth-s1p2 接口的公有 IP 地址访问 Internet。
- 为保护内网，不允许 Internet 用户访问内网。

组网拓扑



配置要点

- 配置接口，设置接口的工作模式和 IP 地址。
- 创建安全域，将三层以太网接口划分给安全域。
- 配置DHCP服务器模式并创建DHCP作用域，将NISG-IPS的eth-s1p1接口设置为DHCP服务器模式，通过创建 DHCP 作用域添加地址池等信息。
- 创建源地址转换规则，使内网用户可以通过eth-s1p2接口的公有IP地址访问Internet。
- 创建访问策略，允许内网用户访问 Internet，不允许外网用户访问内网用户。
- 创建路由，将下一跳 IP 地址设置为路由器的 IP 地址 202.118.1.2。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击接口所对应的，并配置接口为如下：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.118.1.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - Untrust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust
NetEye@root-system] zone Trust based-layer3 eth-s1p1
NetEye@root-system] zone Untrust
NetEye@root-system] zone Untrust based-layer3 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

配置 DHCP 服务器模式并创建 DHCP 作用域

1. 选择**网络 >DHCP>DHCP 服务器**。
2. 在 **DHCP 配置列表**中点击 eth-s1p1 所对应的，并进行以下配置：
   - 服务器：点击
   - 服务器模式：自动
3. 点击**确定**。
4. 选择**网络 >DHCP>DHCP 作用域**。
5. 点击**新建**，进行以下配置：
   - 名称：subnet1
   - IPv4 地址：192.168.1.0
   - 掩码长度：24
   - IP 地址池列表：192.168.1.2-192.168.1.60
   - 保留地址列表：192.168.1.20 （MAC 地址：44:37:E6:27:C5:D5）
   - 租期：无限制

提示：在 **IPv4 地址**文本框中填写的子网以及 **IP 地址池列表**中的 IP 地址应与 eth-s1p1 接口的 IP 地址在同一网段。

---

6. 点击**确定**。
7. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dhcp interface eth-s1p1 server auto
NetEye@root-system] dhcp subnet subnet1 192.168.1.0
NetEye@root-system] dhcp subnet subnet1 dynamic 192.168.1.2-
192.168.1.60
NetEye@root-system] dhcp subnet subnet1 reserve 192.168.1.20
44:37:E6:27:C5:D5
NetEye@root-system] dhcp subnet subnet1 lease unlimited
NetEye@root-system] exit
NetEye@root> save config
```

创建源地址转换规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建以下规则：
   - 序号：1
   - 名称：snat1
   - NAPT：勾选
   - 源 IP 地址列表 > IPv4 地址 / 掩码：192.168.1.0/24
   - 转换后接口：eth-s1p2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy11：
     - 序号：1
     - 源安全域：Trust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：允许
   - policy12：
     - 序号：2
     - 源安全域：Untrust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy11 Trust any any any any any permit enable 1
NetEye@root-system] policy access policy12 Untrust any any any any any deny enable 2
NetEye@root-system] exit
NetEye@root> save config
```

创建路由

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，创建以下缺省路由：
   - 类型：IPv4 地址
   - 目的 IPv4 地址：0.0.0.0
   - 掩码长度：0
   - Metric：1
   - 出口接口：eth-s1p2
   - 网关：202.118.1.2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.1.2 1
NetEye@root-system] exit
NetEye@root> save config
```

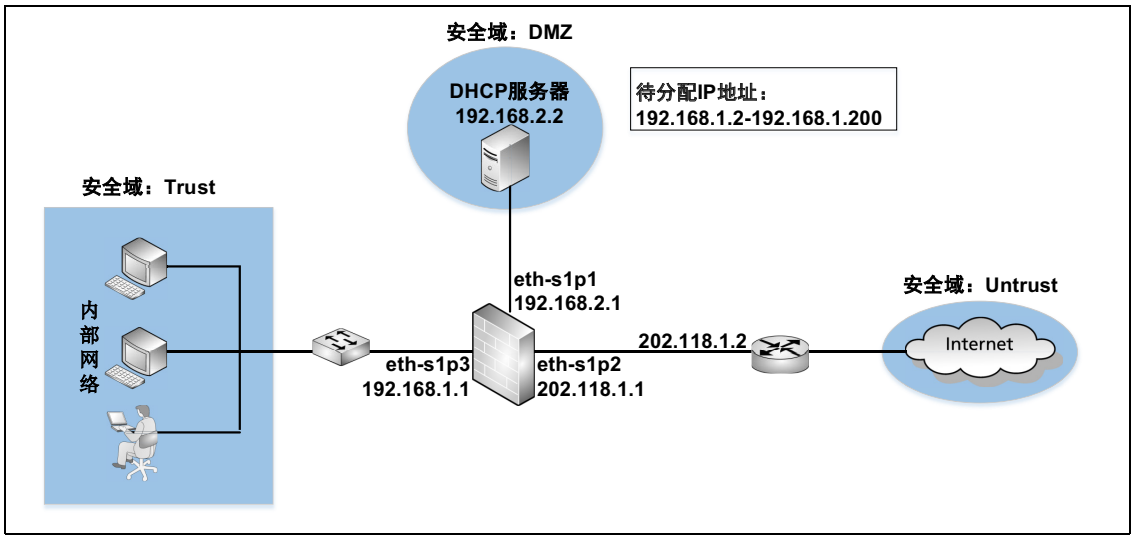
4.17.7 范例：NISG-IPS 作为 DHCP 中继代理

某公司要求内网员工通过 NISG-IPS 从 DHCP 服务器获取 IP 地址。

基本需求

- 将NISG-IPS设置为DHCP中继代理，NISG-IPS可以在内网DHCP客户端和DHCP服务器之间转发 DHCP 消息。
- 为制定统一的访问控制策略，将内网和外网划分到三个不同的安全域内。
- 内网员工可以通过 eth-s1p2 接口的公有 IP 地址访问 Internet。
- 为保护内网，不允许 Internet 用户访问内网。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 配置 DHCP 中继代理，将 NISG-IPS 的 eth-s1p3 接口设置为 DHCP 中继代理模式。
- 创建安全域，将三层接口划分给安全域。
- 创建访问策略，允许内网用户访问 Internet，不允许外网用户访问内网用户。
- 创建路由，将下一跳 IP 地址设置为路由器的 IP 地址 202.118.1.2。
- 创建源地址转换规则，使内网用户可以通过eth-s1p2接口的公有IP地址访问Internet。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击接口所对应的，并配置接口为如下：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.2.1/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.118.1.1/24
   - eth-s1p3：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

配置 DHCP 中继代理

1. 选择**网络** > **DHCP** > **DHCP 服务器**。
2. 在 **DHCP 配置列表**中点击 eth-s1p3 所对应的，进行以下配置：
   - 中继：点击
   - 中继代理服务器：192.168.2.2
   - 将客户端网关 IP 地址指向中继接口：勾选
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dhcp interface eth-s1p3 relay 192.168.2.2 primary
NetEye@root-system] dhcp interface eth-s1p3 relay change-gateway
enable
NetEye@root-system] exit
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust1：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p3
   - DMZ：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - Untrust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone DMZ
NetEye@root-system] zone DMZ based-layer3 eth-s1p1
NetEye@root-system] zone Trust
NetEye@root-system] zone Trust based-layer3 eth-s1p3
NetEye@root-system] zone Untrust
NetEye@root-system] zone Untrust based-layer3 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy11：
     - 序号：1
     - 源安全域：Trust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：允许
   - policy12：
     - 序号：2
     - 源安全域：Untrust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy11 Trust any any any any any permit enable 1
NetEye@root-system] policy access policy12 Untrust any any any any any deny enable 2
NetEye@root-system] exit
NetEye@root> save config
```

创建路由

1. 选择**网络 > 路由 > 缺省路由**。
2. 点击**新建**，创建以下路由：
   - 类型：IPv4 地址
   - 目的 IPv4 地址：0.0.0.0
   - 掩码长度：0
   - Metric：1
   - 出口接口：eth-s1p2
   - 网关：202.118.1.2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.1.2 1
NetEye@root-system] exit
NetEye@root> save config
```

创建源地址转换规则

1. 选择**网络 > 地址转换 > 源地址转换**。
2. 点击**新建**，创建以下源地址转换规则：
   - 序号：1
   - 名称：snat1
   - NAPT：勾选
   - 源 IP 地址列表 > IPv4 地址 / 掩码：192.168.1.0/24
   - 转换后接口：eth-s1p2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] exit
NetEye@root> save config
```

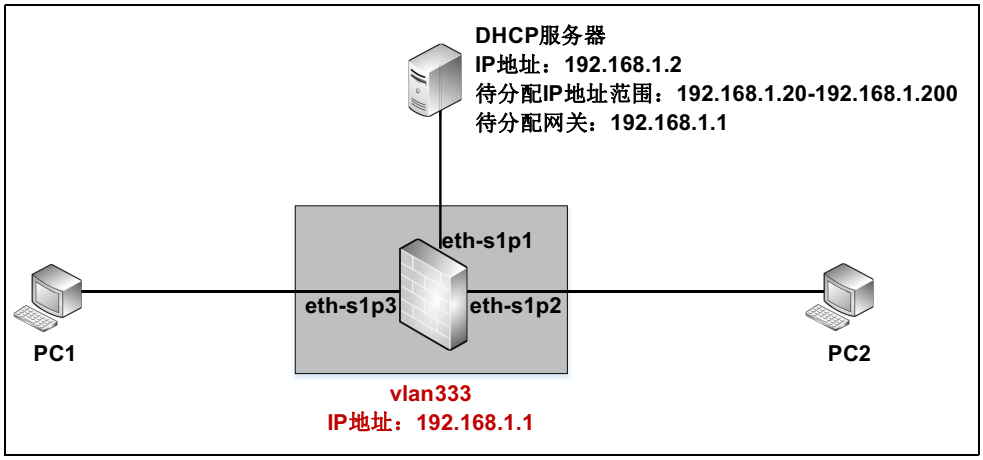
4.17.8 范例：应用 DHCP Snooping

本范例简要说明如何在实际场景中应用 DHCP Snooping 功能。用户 PC1 和 PC2 为 DHCP 客户端，通过 DHCP 从 DHCP 服务器处获取 IP 地址。

基本需求

为了保证 DHCP 客户端从合法的服务器处获取 IP 地址并防止用户随意指定 IP 地址，需启用 NISG-IPS 的 DHCP Snooping 功能，以监听 DHCP 客户端和 DHCP 服务器之间的报文并记录 IP 地址和 MAC 地址等信息的映射关系。

组网拓扑



配置要点

- 配置接口，将以太网接口的工作模式设置为二层。
- 创建 VLAN 接口，将三个二层以太网接口划分到 VLAN 内。
- 配置 DHCP Snooping，启用 DHCP Snooping 功能。
- 验证结果

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击 eth-s1p1、eth-s1p2 和 eth-s1p3 接口所对应的，并将接口的工作模式设置为二层。
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer2-interface
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer2-interface
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer2-interface
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

创建 VLAN 接口

1. 选择**网络** > **接口**。
2. 点击**新建** > **VLAN**，创建 vlan333。将 eth-s1p1，eth-s1p2 和 eth-s1p3 划分给 vlan333。将 vlan333 的 IP 地址设置为 192.168.1.1/24。
3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vlan 333
NetEye@root-system-vlan333] hold ethernet s1p1,s1p2,s1p3
NetEye@root-system-vlan333] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-vlan333] end
NetEye@root> save config
```

配置 DHCP Snooping

1. 选择**网络** > **DHCP > DHCP Snooping**。
2. 在 **DHCP Snooping 配置**列表中勾选 **DHCP Snooping** 复选框，启用此功能。
3. 点击**确定**。
4. 点击。

CLI

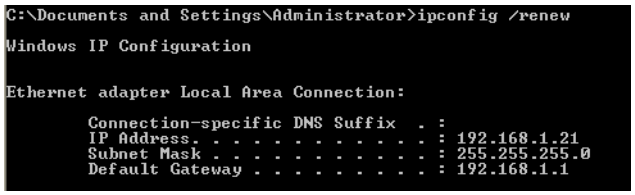
```
NetEye@root> configure mode
NetEye@root-system] dhcp snooping vlan333 on
NetEye@root-system] exit
NetEye@root> save config
```

验证结果

PC1 和 PC2 获取 IP 地址的方式为自动获取。分别在两台 PC 上执行 **ipconfig /renew** 命令，两台主机能够从 DHCP 服务器处正常获取 IP 地址和网关。

PC1：

PC2：

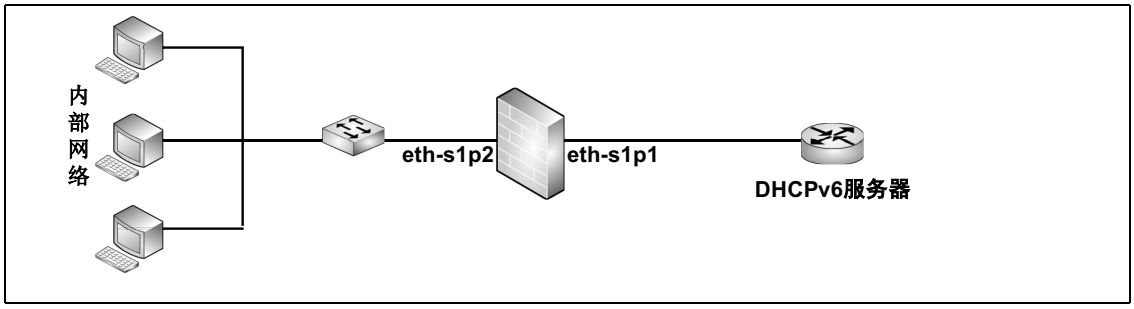


选择**监控** > **DHCP IP 地址绑定状态**。在**类型**下拉框中选择 **DHCP Snooping**，可以查看生成的映射关系条目。

4.17.9 范例：NISG-IPS 作为 DHCPv6 客户端

NISG-IPS 的 eth-s1p1 接口为 DHCPv6 客户端，连接 DHCPv6 服务器。 eth-s1p2 接口连接内网，使用 RA 将前缀信息告知内网主机，内网主机通过无状态地址自动配置获取 IPv6 地址。

组网拓扑



配置要点

- 配置接口，启用接口的 IPv6 功能并启用无状态自动配置。
- 配置 DHCPv6 客户端，将 eth-s1p1 接口设置为 DHCPv6 客户端。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击 eth-s1p1 和 eth-s1p2 所对应的，并进行如下配置：
   - 模式：三层
   - 启用 IPv6：勾选
   - 无状态自动配置：勾选
3. 点击**确定**。
4. 点击。

配置 DHCPv6 客户端

1. 选择**网络** > **IPv6**> **DHCPv6**。
2. 在 **DHCPv6 接口列表**中点击 eth-s1p1 所对应的，进行以下配置：
   - 类型：客户端
   - IPv6 地址列表：
     - SLA：23ed
     - 接口 ID：EUI-64
   - 前缀分配列表：
     - 接口：eth-s1p2
     - SLA：32ed
     - 接口 ID：EUI-64
3. 点击**确定**。
4. 在 **DHCPv6 接口列表**中点击 eth-s1p1 所对应的，并点击**发送 DHCP 请求**。
5. 点击。

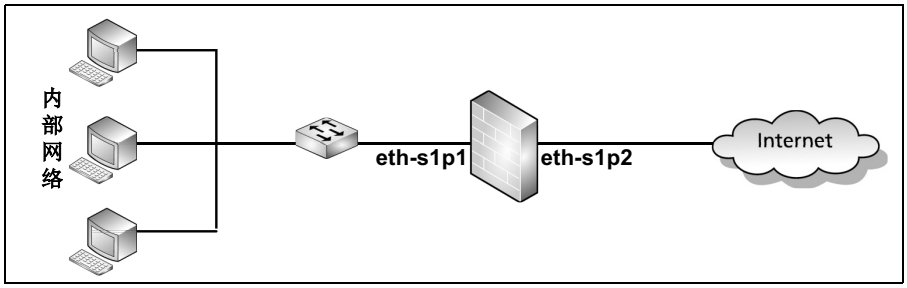
CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ipv6 enable
NetEye@root-system-if-eth-s1p2] ipv6 address autoconfig
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ipv6 enable
NetEye@root-system-if-eth-s1p1] ipv6 address autoconfig
NetEye@root-system-if-eth-s1p1] dhcpv6 type client
NetEye@root-system-if-eth-s1p1] dhcpv6 ip SLA 23ed eui-64
NetEye@root-system-if-eth-s1p1] dhcpv6 prefix-assignment interface
ethernet s1p2 SLA 32af eui-64
NetEye@root-system-if-eth-s1p1] dhcpv6 overwrite-dns
NetEye@root-system-if-eth-s1p1] dhcpv6 client send-request
NetEye@root-system-if-eth-s1p1] end
NetEye@root> save config
```

4.17.10 范例：配置无状态 DHCPv6 服务器

NISG-IPS 的 eth-s1p1 接口连接内网，并充当无状态 DHCPv6 服务器，其 IPv6 地址为 2001:1:1:2::1/64。

组网拓扑



配置要点

- 配置接口，启用接口的 IPv6 功能，并手动配置 IPv6 地址。
- 配置DHCPv6服务器，将eth-s1p1接口设置为无状态DHCPv6服务器，并配置要分配给内网主机的无状态 DHCPv6 信息。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中点击 eth-s1p1 所对应的，进行以下配置：
   - 模式：三层
   - 启用 IPv6：勾选
   - IP 地址列表：
     - IP 地址：2001:1:1:2::1
     - 前缀长度：64
     - 类型：手动
3. 点击**确定**。
4. 点击。

配置 DHCPv6 服务器

1. 选择**网络 >IPv6>DHCPv6**。
2. 在 **DHCPv6 接口列表**中点击 eth-s1p1 所对应的，进行以下配置：
   - 类型：服务器
   - 服务器信息：
     - 手动：点击
     - DNS1：2000::1
     - DNS2：2000::2
     - SNTP 服务器 1：2ffe::1
     - SNTP 服务器 2：2ffe::2
3. 点击**确定**。
4. 点击。

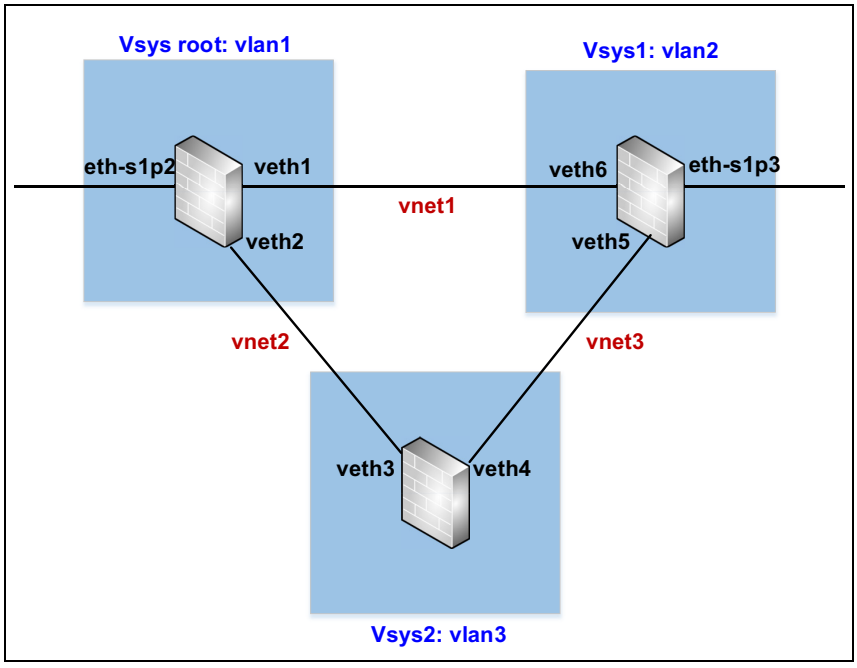
CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ipv6 enable
NetEye@root-system-if-eth-s1p1] ipv6 address 2001:1:1:2::1/64
NetEye@root-system-if-eth-s1p1] dhcpv6 type server
NetEye@root-system-if-eth-s1p1] dhcpv6 server dns 2000::1
NetEye@root-system-if-eth-s1p1] dhcpv6 server dns2 2000::2
NetEye@root-system-if-eth-s1p1] dhcpv6 server sntp 2ffe::1
NetEye@root-system-if-eth-s1p1] dhcpv6 server sntp2 2ffe::2
NetEye@root-system-if-eth-s1p1] end
NetEye@root> save config
```

4.17.11 范例：应用 STP

本范例是 STP 功能的简单应用，用于检测在链路冗余的网络拓扑中运行 STP 协议，是否有端口被阻塞；当主链路发生故障时，被阻塞的端口是否启用，恢复链路畅通。

组网拓扑



配置要点

管理员需要在 NISG-IPS 上搭建如下网络拓扑环境：

- 创建 VLAN 接口和虚拟接口，创建 vlan1、 vlan2 和 vlan3，创建虚拟接口 veth1 ～ veth6，将 eth-s1p2、 veth1 和 veth2 划入到 vlan1 中，将 veth3 和 veth4 划入到 vlan3 中，将 veth5、 veth6 和 eth-s1p3 划入到 vlan2 中。
- 创建虚拟系统，创建虚拟系统 Vsys1 和 Vsys2。将 vlan2 划入到 Vsys1 中，将 vlan3 划入到 Vsys2 中。
- 创建虚拟网络，创建虚拟网络 Vnet1、Vnet2 和 Vnet3。将 veth1 和 veth6 划入到 Vnet1 中用于连接 Vsys Root 和 Vsys1 ； 将 veth2 和 veth3 划入到 Vnet2 中用于连接 Vsys Root 和 Vsys2 ； 将 veth4 和 veth5 划入到 Vnet3 中用于连接 Vsys1 和 Vsys2。
- 配置 STP，在 vlan1、vlan2 和 vlan3 上分别开启 STP 功能，将 vlan1 设置为根网桥。修改 veth5 的端口路径开销为 10， veth6 的端口路径开销为 20，其他虚拟接口采用默认的端口路径开销 200,000,000。
- 查看结果

配置步骤

创建 VLAN 接口和虚拟接口

1. 选择**网络** > **接口**。
2. 点击**新建**，选择 **VLAN**，创建 VLAN 接口 vlan1。以同样的方式创建 vlan2 和 vlan3。
3. 点击**新建**，选择 **Virtual Interface**，创建虚拟接口 veth1。以同样的方式创建 veth2~veth6。
4. 在**接口列表**中点击 vlan1 所对应的，并将 eth-s1p2、 veth1 和 veth2 划分给 vlan1。
5. 点击**确定**。
6. 以同样的方式将 eth-s1p3、veth5 和 veth6 划入到 vlan2 中，将 veth3 和 veth4 划入到 vlan3 中。
7. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] vlan 2
NetEye@root-system-vlan2] vlan 3
NetEye@root-system-vlan3] veth 1
NetEye@root-system-veth1] veth 2
NetEye@root-system-veth2] veth 3
NetEye@root-system-veth3] veth 4
NetEye@root-system-veth4] veth 5
NetEye@root-system-veth5] veth 6
NetEye@root-system-veth6] exit
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] hold ethernet eth-s1p2
NetEye@root-system-vlan1] hold veth veth1,veth2
NetEye@root-system-vlan1] vlan 2
NetEye@root-system-vlan2] hold ethernet eth-s1p3
NetEye@root-system-vlan2] hold veth veth5,veth6
NetEye@root-system-vlan2] vlan 3
NetEye@root-system-vlan3] hold veth veth3,veth4
NetEye@root-system-vlan3] end
NetEye@root> save config
```

创建虚拟系统

1. 选择**系统 > 虚拟系统 > 虚拟系统**。
2. 点击**新建**，分别创建以下虚拟系统：
   - Vsys1：
     - 虚拟系统：1
     - 最大资源限制：20
     - 三层接口 > 已选接口：vlan2
   - Vsys2：
     - 虚拟系统：2
     - 最大资源限制：20
     - 三层接口 > 已选接口：vlan3
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vsys 1 resource-limit 20
NetEye@root-system-vsys1] hold vlan 2
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2 resource-limit 20
NetEye@root-system-vsys2] hold vlan 3
NetEye@root-system-vsys2] end
NetEye@root> save config
```

创建虚拟网络

1. 选择**系统 > 虚拟系统 > 虚拟网络**。
2. 点击**新建**，分别创建以下虚拟网络：
   - Vnet1：
     - 虚拟网络 ID：1
     - 链接虚拟接口列表：
       - 虚拟系统：root ； 接口：veth1
       - 虚拟系统：vsys1 ； 接口：veth6
   - Vnet2：
     - 虚拟网络 ID：2
     - 链接虚拟接口列表：
       - 虚拟系统：root ； 接口：veth2
       - 虚拟系统：vsys2 ； 接口：veth3
   - Vnet3：
     - 虚拟网络 ID：3
     - 链接虚拟接口列表：
       - 虚拟系统：root ； 接口：veth5
       - 虚拟系统：vsys2 ； 接口：veth4
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vnet 1
NetEye@root-system-vnet1] hold veth 1
NetEye@root-system-vnet1] hold veth 6
NetEye@root-system-vnet1] vnet 2
NetEye@root-system-vnet2] hold veth 2
NetEye@root-system-vnet2] hold veth 3
NetEye@root-system-vnet2] vnet 3
NetEye@root-system-vnet3] hold veth 4
NetEye@root-system-vnet3] hold veth 5
NetEye@root-system-vnet3] end
NetEye@root> save config
```

配置 STP

1. 选择**网络** >**STP**。
2. 在 **STP** 区域，点击**启用**。
3. 在 **VLAN 列表**中分别双击 VLAN 接口，进行如下配置：
   - vlan1：
     - STP/RSTP：启用
     - 根网桥：点击
   - vlan2：
     - STP/RSTP：启用
     - 端口配置列表：
       - 接口：veth5 ；端口路径开销：10
       - 接口：veth6 ；端口路径开销：20
   - vlan3：
     - STP/RSTP：启用
4. 点击**确定**两次。
5. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] spanning-tree enable per-vlan-stp
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] spanning-tree enable stp
NetEye@root-system-vlan1] spanning-tree root primary
NetEye@root-system-vlan1] vlan 2
NetEye@root-system-vlan2] spanning-tree enable stp
NetEye@root-system-vlan2] spanning-tree interface veth5 path-cost 10
NetEye@root-system-vlan2] spanning-tree interface veth6 path-cost 20
NetEye@root-system-vlan2] vlan 3
NetEye@root-system-vlan3] spanning-tree enable stp
NetEye@root-system-vlan3] end
NetEye@root> save config
```

查看结果

完成上述配置，可以通过 WebUI 或 CLI 查看 STP 的实时信息。选择**监控 >STP** 进入 STP 页面，或在 CLI 下执行 **show spanning-tree vlan** 命令。由于 vlan1 是根网桥， veth6 与 veth3 各自成为 vlan2 和 vlan3 的根端口； veth5 的路径开销低于 veth4 的路径开销，成为整个网段的指定端口； veth4 既不是根端口也不是指定端口，因此被阻塞，处于 Blocking 状态，其他接口处于 Forwarding 状态。

然后手动禁用 veth6 接口，查看被阻塞的 veth4 接口是否重新启用，网络是否恢复链路畅通。具体操作如下：

1. 选择**网络** > **接口**。
2. 在**接口列表**中点击 veth6 所对应的，进入**编辑**页面，点击**关**禁用 veth6 接口。
3. 点击**确定**。
4. 点击。

CLI

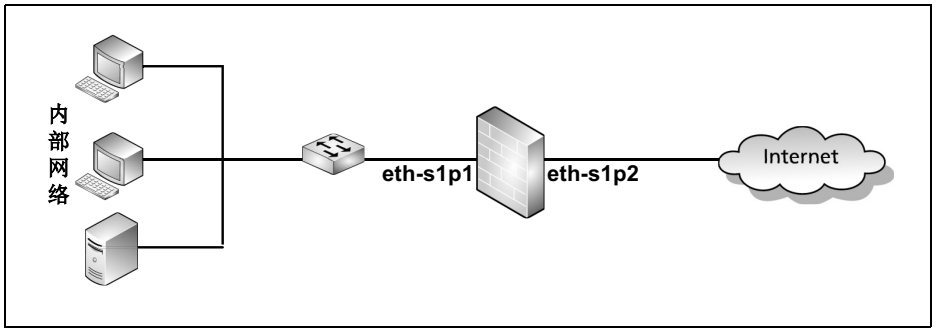
```
NetEye@root> configure mode
NetEye@root-system] veth 6
NetEye@root-system-veth6] shutdown
NetEye@root-system-veth6] end
NetEye@root> save config
```

完成上述配置，通过 WebUI 界面在 STP 页面上查看 STP 的实时信息，会发现 veth6 接口处于 Disable 状态，其他接口处于 Forwarding 状态。也可以通过 **show spanning-tree vlan** 命令可以在 CLI 界面下查看 STP 的实时信息。

4.17.12 范例：重复地址检测

NISG-IPS 的 eth-s1p1 接口连接内网，内网中有一台 Web 服务器，其 IP 地址为 2001:1:1:2::2/64。

组网拓扑



配置要点

- FW 设备在 eth-s1p1 接口上执行 DAD （重复地址检测），次数最多为 3 次。
- 接口 eth-s1p1 每隔 1,000 毫秒重新发送 ND 报文。
- 接口 eth-s1p2 维持 Web 服务器的邻居可达性状态时长约 10,000 毫秒。如果在该时间内没有收到 Web 服务器的可达性确认消息， eth-s1p2 将停止向其转发流量。
- 配置 eth-s1p1 接口的 IP 地址为 2001:1:1:2::2/64。稍后，接口的 IPv6 地址状态为 DUPLICATE。
- 配置接口 eth-s1p1 接口的 IP 地址为 2001:1:1:2::1/64（该地址不与内网中的任一主机重复）。稍后，接口的 IPv6 地址状态为 PREFERRED。

提示

在配置 ND 前，需要首先选择**网络 > 接口**，启用三层或三层共享接口的 IPv6 功能。

配置步骤

1. 选择**网络 >IPv6> 邻居发现配置**。
2. 在**邻居发现 / 路由器通告列表**中点击 eth-s1p1 所对应的，进行如下配置：
   - 重复地址检测 （DAD）重试次数：3
   - 重传时间：1000
   - 基础可达时间：10000
3. 点击**确定**。
4. 选择**网络 > 接口**。
5. 在**接口列表**中点击 eth-s1p1 所对应的。
6. 点击 **IP 地址列表**中的**添加**，进行如下配置：
   - IPv6 地址：2001:1:1:2::2
   - 前缀长度：64
   - 类型：手动
7. 点击**确定**。
8. 在**接口列表**中点击 eth-s1p1 所对应的。查看接口状态，为“ 重复 （DUP） ”。
9. IPv6 地址 2001:1:1:2::1 的配置和步骤 6 相同。
10. 点击**确定**。
11. 在**接口列表**中点击 eth-s1p1 所对应的。查看接口状态，为“ 首选 （PREFER） ”：
12. 点击**确定**。
13. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] ipv6 enable
NetEye@root-system-if-eth-s1p1] ipv6 nd dad detect 3
NetEye@root-system-if-eth-s1p1] ipv6 nd retrans-timer 1000
NetEye@root-system-if-eth-s1p1] ipv6 nd reachable-time 10000
NetEye@root-system-if-eth-s1p1] ipv6 address 2001:1:1:2::2/64
NetEye@root-system-if-eth-s1p1] ipv6 address 2001:1:1:2::1/64
NetEye@root-system-if-eth-s1p1] end
NetEye@root> save config
```

完成上述操作后，运行 **show interface ethernet s1p2** 命令。可以查看到如下信息：

- DAD已启用，重复检测次数为3次； ND报文的重新发送间隔为1,000毫秒；基础可达时间为 10,000 毫秒。

```
ND DAD is enabled, number of DAD attempts 3
ND retransmit time is 1000 milliseconds
ND base reachable time is 10000 milliseconds
```

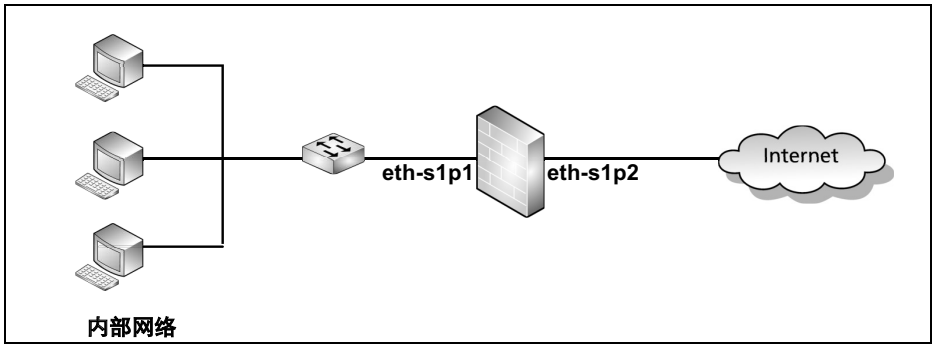
- IPv6地址2001:1:1:2::2处于DUP状态，表明已为网络中其他接口所使用； 2001:1:1:2::1 则处于 PREFER 状态，可以配置到 eth-s1p2 接口上。

```
Global unicast address(es):
  2001:1:1:2::2 , subnet is 2001:1:1:2::/64   [DUP]
  2001:1:1:2::1 , subnet is 2001:1:1:2::/64   [PREFER]
```

4.17.13 范例：配置路由器通告 （RA）

NISG-IPS 的 eth-s1p1 接口连接内网，其 IP 地址为 2001:1:1:2::1/64。

组网拓扑



配置要点

- 手动配置 eth-s1p1 接口的 IP 地址为 2001:1:1:2::1/64。
- 编辑 eth-s1p1 的 RA 相关属性：
  - 通告 （RA）参数：
    - 允许 eth-s1p1 向内网发布 RA 通告，内网主机不将 eth-s1p1 作为默认路由器。
    - RA 消息发布的时间间隔为 750~1000 秒。
    - 跳数限制为 64。
    - 内网主机只通过无状态地址自动配置获取 IPv6 地址，内网主机可以通过无状态 DHCPv6 配置获取其他网络配置信息。
    - RA 消息中不携带 eth-s1p1 的链路层地址和 MTU。
  - 前缀信息：
    - 通告前缀 2001:1:1:2::/64。
    - 内网主机可利用前缀进行无状态地址自动配置。
    - 不进行在链判定。

配置步骤

1. 选择**网络 >IPv6> 邻居发现配置**。
2. 在**邻居发现 / 路由器通告列表**中点击 eth-s1p1 所对应的，进入 eth-s1p1 的编辑页面，进行如下配置：
   - 路由器生存时间：0
   - 最大通告间隔：1000
   - 最小通告间隔：750
   - 跳数限制：64
   - 0 标志位：勾选
   - 链路层地址：取消勾选
   - 链路 MTU：取消勾选
3. 点击**前缀列表**中的**添加**，进行如下配置：
   - IPv6 地址：2001:1:1:2::
   - 前缀长度：64
4. 点击**确定**。
5. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] ipv6 enable
NetEye@root-system-if-eth-s1p1] unset ipv6 nd ra suppress
NetEye@root-system-if-eth-s1p1] ipv6 nd ra router-lifetime 0
NetEye@root-system-if-eth-s1p1] ipv6 nd ra interval 750 1000
NetEye@root-system-if-eth-s1p1] ipv6 nd ra hop-limit 64
NetEye@root-system-if-eth-s1p1] ipv6 nd ra managed-flag off
NetEye@root-system-if-eth-s1p1] ipv6 nd ra other-flag on
NetEye@root-system-if-eth-s1p1] ipv6 nd ra link-address off
NetEye@root-system-if-eth-s1p1] ipv6 nd ra advlinkmtu off
NetEye@root-system-if-eth-s1p1] ipv6 nd ra prefix 2001:1:1:2::/64
valid-lifetime default preferred-lifetime default no-adv off no-
autoconf
ig off off-link off
NetEye@root-system-if-eth-s1p1] exit
NetEye@root> save config
```

5 路由

本章介绍 NISG-IPS 的路由特性。

5.1 概述

NISG-IPS 提供静态路由（包括缺省路由和策略路由）、动态路由（包括 OSPF、 BGP 和 RIP）和多播路由特性。本节包括：

- 5.1.1 缺省路由
- 5.1.2 策略路由
- 5.1.3 动态路由
- 5.1.4 多播路由

当接收到新的单播数据包时， NISG-IPS 按如下顺序将其与路由进行匹配：

1. 如果找到匹配的直连路由， NISG-IPS 会直接将数据包转发。
2. 如果没有找到匹配的直连路由， NISG-IPS 会将数据包与所有已启用的策略路由进行匹配。关于策略路由的详细信息，请参见 5.1.2 策略路由。
3. 如果数据包没有匹配到任何策略路由，NISG-IPS 会将数据包的目的 IP 地址与缺省路由表中所有目的不为 0.0.0.0/0 的 IP 地址进行比较。
   a. 如果有多条与数据包的目的 IP 地址完全匹配的路由，数据包将选择子网掩码或前缀长度最大的路由 （即最长匹配原则）；
   b. 如果有多条子网掩码长度或前缀长度又相同的路由，数据包将选择管理距离最小的路由。
4. 如果数据包没有匹配到路由，NISG-IPS 会进行 ISP 智能选路。关于 ISP 智能选路的信息，参见 6 ISP 智能选路。
5. 如果 ISP 智能选路失败了，NISG-IPS 会使用目的为 0.0.0.0/0 的缺省路由将数据包转发出去。

5.1.1 缺省路由

缺省路由基于数据包的目的 IP 地址确定转发数据包的出口接口以及下一跳网关地址。

NISG-IPS 提供 IPv4 和 IPv6 路由。缺省情况下， NISG-IPS 提供一条缺省 IPv4 路由，其配置信息如下：

- 目的：0.0.0.0/0 （任意，目的不确定）
- 路由度量 （Metric）：1
- 下一跳网关地址：192.168.1.1

管理员可以：

- 创建、修改或删除缺省路由，包括目的确定和不确定的。

  如果目的不确定，可以将 IPv4 和 IPv6 路由的目的 IPv4 地址和 IPv6 地址分别设置为 “0.0.0.0/0” 和 “::/0”。

- 通过将路由的出口接口设置为 Null 接口来创建 Null 路由。

  如果数据包匹配到 Null 路由， NISG-IPS 会直接将其丢弃。因此 Null 接口可以用来防止路由环路。

5.1.1.1 负载均衡

管理员可以在一条缺省路由中设置多条负载均衡策略。负载均衡可以将通往相同目的网络的数据流量分配到多条链路上。NISG-IPS 只需要为会话的第一个数据包进行路由查询并根据权重将此会话分配给下一跳路由设备即可。数据包的下一跳信息会被记录在会话表中；当此会话后续的数据包达到 NISG-IPS 时，它会根据已记录的下一跳信息转发数据包。

在一条负载均衡策略中，管理员可以设置：

- 将数据包转发出去的 NISG-IPS 接口
- 下一跳路由设备的 IP 地址
- 下一跳路由设备得到的会话比例 （权重）
- 链路探测信息

如果 NISG-IPS 与某个下一跳路由设备之间的链路出现了故障，可以通过其它可用的链路转发数据包。当出现故障的链路恢复正常时，路由设备会重新获得其原有的权重。如果 NISG-IPS 检测出路由中所有通往下一跳路由设备的链路都出现故障，那么此条路由会被禁用。当其中任意一个链路恢复正常时，此条路由会再次被启用。

NISG-IPS 视以下情况为链路不通：

- 当 NISG-IPS 探测某一目的 IP 地址时，连续失败的次数达到了最大值，并且在探测周期内仍未得到回复。
- 出口接口被管理员手动设置为 “ 禁用 ” 或物理连接状态为 “ 断开 ”。

5.1.1.2 链路探测

NISG-IPS 周期性地向目的 IP 地址发送探测包，并根据对方的应答情况来判断链路的状况。如果 NISG-IPS 在指定的探测次数内得到应答，则认为链路正常。如果 NISG-IPS 连续失败的次数达到了最大值，并且在探测周期内仍未得到回复，则认为链路不通。

NISG-IPS 支持以下四种链路探测类型：

表 140 链路探测类型

探测类型	地址类型	发送的数据包	收到的回复
ARP Ping（ARP 探测）	IPv4	ARP 请求包	带有 MAC 地址的 ARP 应答
TCP Ping（TCP 探测）	IPv4 & IPv6	SYN 数据包	SYN/ACK 数据包
Ping（ICMP 探测）	IPv4 & IPv6	通过 Ping 命令或 Ping6 命令发送 ICMP Echo 数据包	Echo 回复包
NS Ping（NS 探测）	IPv6	邻居请求 (NS) 报文	邻居公告报文 (NA)

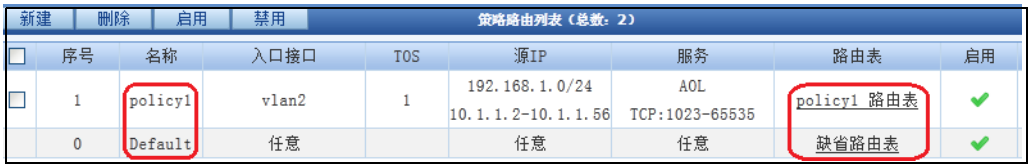
5.1.2 策略路由

策略路由基于以下参数 （前四个参数可以在策略路由策略中设置），确定用于转发数据包的出口接口和下一跳网关地址：

- 源 IP 地址
- TOS
- 服务
- 入口接口
- 目的 IP 地址

如需使用策略路由，管理员应先创建策略路由策略 （如 policy1）。在此策略中，可以定义匹配数据包的条件。然后配置此策略对应的路由表；此路由表用于转发匹配了策略的数据包；配置过程与 5.1.1 缺省路由中的配置相同。策略路由策略在创建后就处于启用的状态。当删除一条策略路由策略时，此策略的路由表也同时被删除。

NISG-IPS 提供一条名为 **Default** 的缺省策略路由策略。它允许任意数据包进入到缺省路由表中进行选路。此策略缺省为启用状态且不可配置，管理员可以配置缺省路由表中的路由。



5.1.3 动态路由

NISG-IPS 支持动态路由。动态路由是通过相互连接的路由器之间彼此交换信息，然后按照一定的算法计算得到最优路径，并且这些路由信息随着网络拓扑的变化动态地更新，随时获得最优的寻路效果。动态路由适用于具有一定规模的网络，但是配置比较复杂。

路由协议可以分为内部网关协议 （Interior Gateway Protocol， IGP）和外部网关协议（Exterior Gateway Protocol， EGP）两类。 IGP 是在一个自治系统内部使用的路由协议，规定数据包在自治系统内部的路由选择。 EGP 是在自治系统之间使用的路由协议，规定数据包在自治系统间的路由选择。

NISG-IPS 支持内部网关协议 OSPF 和 RIP，同时也支持外部网关协议 BGP。 NISG-IPS 只提供 CLI 方式配置动态路由。关于如何配置动态路由，参见*东软 NetEye 集成安全网关入侵防御系统 V4.2 命令参考手册*。

5.1.4 多播路由

NISG-IPS 提供静态和动态多播路由功能。本章只介绍静态多播路由。静态多播路由是由管理员手动设置的路由。动态多播路由是通过多播路由协议学到的路由，参见 7.1.1 DVMRP。

多播路由是多播数据包的路由过程。多播路由依赖于多播组 IP 地址。在 IPv4 中，多播组 IP 地址是范围从 224.0.0.0 到 239.255.255.255 的 D 类 IP 地址。通过多播路由， NISG-IPS 可以与其他路由设备交换多播组成员的信息，并以此作出多播转发决定。

多播路由根据以下参数确定转发数据包的出口接口 （转发接口）：

- 源 IP 地址
- 多播组 IP 地址
- 入口接口

如果多播数据包匹配以上多播路由参数，且数据包的 TTL 值大于管理员设置的 TTL 值，那么此数据包将会从出口接口转发出去；否则，数据包会被丢弃。

如果管理员不修改或删除静态多播路由，那么它们不会自动改变。

5.2 基本配置步骤

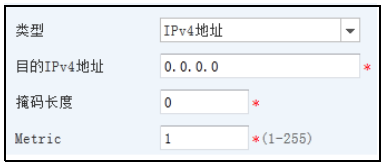
本节介绍如下基本配置步骤：

- 5.2.5 创建缺省路由
- 5.2.6 创建策略路由
- 5.2.7 创建静态多播路由

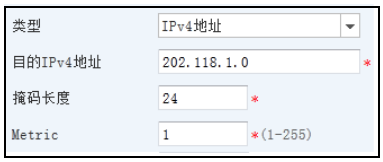
如需使用特定 IP 地址对象、 IP 地址对象组、服务对象和服务对象组，需要首先选择**系统 > 对象**创建它们。

5.2.5 创建缺省路由

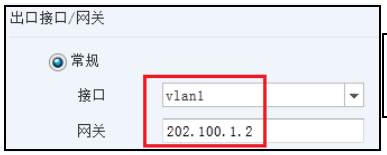
1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，设置目的地址和 Metric 值。
   - 目的地址不确定：

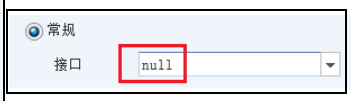


   - 目的地址确定：



3. 设置出口接口 / 网关。
   - 常规：只有一个出口接口和 / 或网关。可以将出口接口设置为 Null 来定义 Null 路由，匹配 Null 路由的数据包将被直接丢弃。





   - 负载均衡：有多个出口接口和 / 或网关。属于同一个会话的所有数据包都通过同一个接口路由出去。 NISG-IPS 根据权重将数据包从多个链路转发出去。如果 NISG-IPS 与某个下一跳路由设备之间的链路出现了故障，可通过其他可用的链路转发数据包。如果路由中通往所有的下一跳路由设备的链路都出现故障，那么此条路由会被禁用。当其中任一链路恢复正常时，此条路由会再次被启用。

4. 点击**确定**。
5. 点击 。

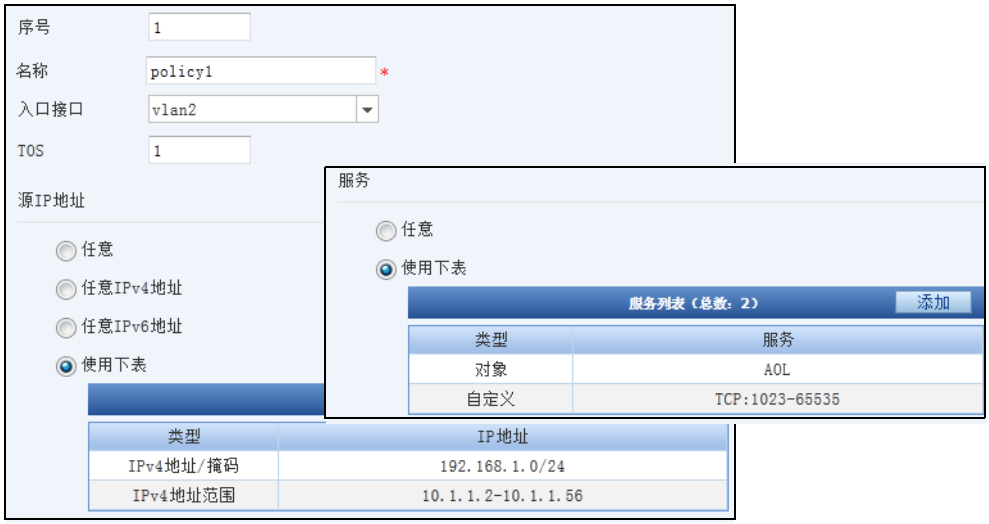
表 141 缺省路由命令

route	添加缺省路由。
route {**default** | *ipv4 netmask*} **load-balancing**	添加具有负载均衡功能的 IPv4 路由。
route {**default-v6** | *ipv6 prefix_length*} **load-balancing**	添加具有负载均衡功能的 IPv6 路由。
show route	显示缺省路由信息。
unset route	删除缺省路由。

5.2.6 创建策略路由

5.2.6.1 创建匹配入口数据包的策略

1. 选择**网络** > **路由** > **策略路由**。
2. 点击**新建**，设置接收数据包的接口以及数据包的 TOS、源 IP 地址和服务。



3. 点击**确定**。
4. 在下表中查看已创建的策略路由策略：

5. 点击 。

表 142 策略路由策略命令

policy route *policy_name* [**number** *pri*]	添加策略路由策略。
matching	为策略添加数据包匹配条件。
policy route *policy_name* {**enable** | **disable**}	启用或禁用策略。
show policy route [*policy_name*]	显示策略路由策略信息。

5.2.6.2 创建路由

在**策略路由列表**中，点击“**policy1 路由表**”，创建路由，用于转发匹配 policy1 的数据包。步骤与 5.2.5 创建缺省路由相同。

5.2.7 创建静态多播路由

必须配置多播策略以允许转发多播数据包。更多信息，参见第 10 章，策略。

5.2.7.1 启用 DVMRP 并选择 DVMRP 接口

1. 选择**网络** > **多播** >**DVMRP**。
2. 启用防火墙的 DVMRP（多播路由）功能，选择启用 DVMRP 的接口，以允许接口转发多播数据包。

其他 DVMRP 参数在静态多播路由中不起作用。

3. 点击**确定**。
4. 点击。

5.2.7.2 创建静态多播路由

1. 选择**网络** > **路由** > **多播路由**。
2. 点击**新建**，创建以下路由：

TTL 控制数据包是否能从 DVMRP 接口转发出去。只有当多播数据包的 TTL 值大于管理员设置的 TTL 值时，数据包才会从接口转发出去。在上图中， TTL 值是 1，如果数据包的 TTL 值大于等于 2，数据包可以被转发。

3. 点击**确定**。

4. 点击。

表 143 多播路由命令

dvmrp route	添加静态多播路由。
show dvmrp route	显示多播路由信息。
unset dvmrp route	删除静态多播路由。

5.3 配置参数说明

本节介绍配置路由时用到的参数：

5.3.1 缺省路由参数

表 144 缺省路由参数

参数	说明
类型	IP 地址的类型。 IPv4 地址或 IPv6 地址。
目的 IPv4 地址 / 目的 IPv6 地址	数据包要被发送到的目的主机或目的网络的地址。 缺省路由的目的 IPv4 和 IPv6 地址分别是 0.0.0.0 和 ::。
掩码长度 / 前缀长度	目的 IPv4 地址的掩码长度或目的 IPv6 地址的前缀长度。 缺省路由的掩码长度和前缀长度都为 0。 掩码长度的取值范围是 0 ～ 32 ；前缀长度的取值范围为 0 ～ 128。
Metric	指路由的优先级。取值范围为 1 ～ 255。 Metric 值越小，优先级越高。
出口接口 / 网关	用于为缺省路由设置一个出口接口、网关或两者均设置。 您可以配置常规的缺省路由，也可以配置带有负载均衡策略的缺省路由。
常规	用于配置不带负载均衡功能的缺省路由。 管理员至少需要设置以下一项： • **接口**：用于将数据包转发出去的三层接口。如果管理员选择 Null 接口，则不允许输入网关地址，数据包会被丢弃。 • **网关**：对端网络无法直达时的下一跳路由设备的 IP 地址。
负载均衡	用于配置具有负载均衡功能的缺省路由。 管理员可以为负载均衡策略配置以下参数： • **接口**：转发数据包的三层接口。 • **网关**：对端网络无法直达时的下一跳路由设备的 IP 地址。 • **权重**：下一跳路由设备所能分到的会话比例。权重越大，端口所获得的会话就越多。权重的取值范围为 1 ～ 255，缺省值为 1。 • **探测类型**：用于探测 IP 地址的方式，包括 ARP Ping、 Ping、 TCP Ping 和 NS Ping。也可以将探测类型设置为 None，即不进行探测。None 为缺省的探测类型。ARP Ping 只用于探测内网的 IPv4 地址； NS Ping 只用于探测 IPv6 地址。 • **探测 IPv4 地址 / 探测 IPv6 地址**：所探测的路由设备的 IPv4 或 IPv6 地址。 • **探测端口**：使用 TCP 探测时，所探测的路由设备的端口。端口的取值范围为 1 ～ 65535。 • **探测周期**：两次链路探测之间的时间间隔，取值范围为 1 ～ 30000 秒，缺省值为 3 秒。 • **探测重试次数**：NISG-IPS 探测 IP 地址时允许连续失败的最大次数。如果探测失败次数达到了此阈值，但是在探测周期内未得到回复，则认为链路不通。探测重试次数的取值范围为 1 ～ 999 次，缺省值为 3。 您最多可以为一条缺省路由配置 8 个负载均衡策略。

5.3.2 策略路由参数

表 145 策略路由参数

参数	说明
序号	表示策略路由策略的优先级。数值越小，优先级越高。如果在创建策略时未指定其序号，那么此策略的优先级将自动变成最小。
名称	名称为策略路由唯一标识。 长度 1 ～ 15 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #。
入口接口	用于接收数据包的三层接口。入口接口可以是任意一个可用的三层接口。
TOS	用于定义数据包中的交付服务 （吞吐量、延迟、可靠性及经济成本）。 TOS 的取值范围为 0 ～ 15： • 0 表示不要求任何服务。 • 1 表示要求最低的时延。 • 2 表示要求最高的吞吐量。 • 4 表示要求最高的可靠性。 • 8 表示要求最小的代价。
源 IP 地址	发送数据包的 IP 地址。源 IP 地址可以是以下任意类型： • **任意**：包括所有 IPv4 和 IPv6 地址。 • **任意 IPv4 地址**：包括所有 IPv4 地址。 • **任意 IPv6 地址**：包括所有 IPv6 地址。 • **使用下表**：包括 IP 地址对象，对象组， IPv4 地址， IPv4 地址段， IPv4 地址及掩码， IPv6 地址， IPv4 地址段， IPv4 地址及前缀。 您最多可以配置 32 个源 IP 地址条目。
服务	数据包使用的传输层服务。服务类型可以是以下任意一种： • **任意**：包括所有协议类型。 • **使用下表**：包括对象、对象组以及自定义协议。自定义协议包括 ICMP、 ICMPv6、TCP、 UDP 和 Other。当设置 ICMP 协议时，管理员可以选择以下任意类型：ECHO_and_ECHOREPLY， INFO_REQUEST_and_INFO_REPLY，TIMESTAMP_and_TIMESTAMPREPLY， ADDRESS_and_ADDRESSREPLY，ROUTER_ADVERTISEMENT， ROUTER_SOLICITATION， DEST_UNREACH，SOURCE_QUENCH， REDIRECT， TIME_EXCEEDED， PARAMETERPROB 和 Any （表示任意 ICMP 协议类型）。当设置 ICMPv6 协议时，管理员可以选择以下任意类型：DEST_UNREACH， PACKET_TOO_BIG， TIME_EXCEEDED，PARAMETERPROB， ECHO_and_ECHOREPLY 和 Any （表示任意 ICMPv6 协议类型）。 TCP 和 UDP 协议的目的端口号范围为 1 ～ 65535。其他协议号范围为 1 ～ 255。 您可以最多配置 32 个服务条目。
路由表	策略路由策略所对应的路由表。

5.3.3 静态多播路由参数

表 146 静态多播路由参数说明

参数	说明
源 IP 地址	发送多播数据包的 IP 地址。
多播组 IP 地址	目的多播组的 IP 地址。
入口接口	接收多播数据包的 DVMRP 接口。入口接口不可以与任何转发接口相同。
转发接口	将多播数据包转发出去的 DVMRP 接口。
TTL	控制数据包是否能从 DVMRP 接口转发出去。 TTL 相当于 DVMRP 的阈值，更多信息，参见 7.3.1 DVMRP 参数中的“ 阈值 ”。

5.4 路由范例

本节介绍如何在实际场景中配置路由功能，包括：

- 5.4.1 范例：创建基于负载均衡的静态路由
- 5.4.2 范例：创建策略路由
- 5.4.3 范例：应用静态多播路由

提示：范例里的 IP 地址只是用于举例说明。可以根据实际需要更改 IP 地址。

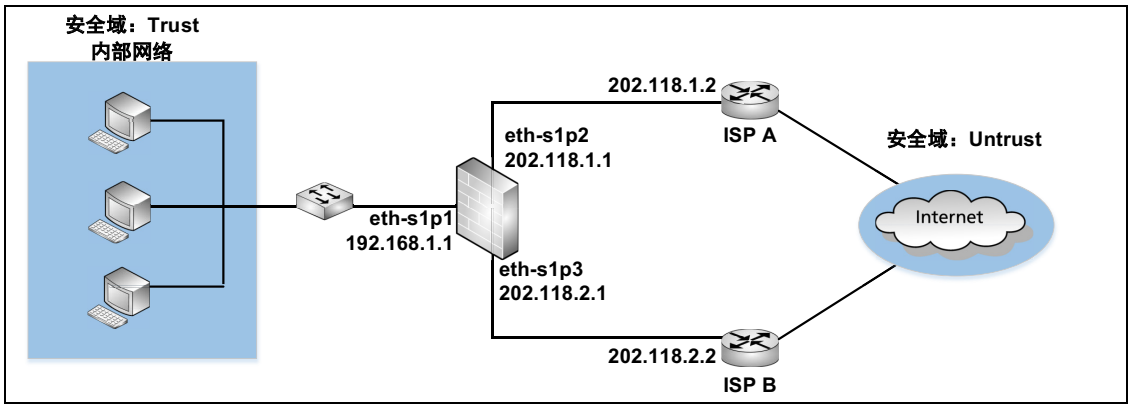
5.4.1 范例：创建基于负载均衡的静态路由

某公司的内部网络通过两家网络服务提供商（ISP）接入互联网。ISP A 的带宽和服务质量优于 ISP B。

基本需求

- ISP A 承担大部分从内网发往 Internet 的数据流量。
- 对通往两家 ISP 的链路进行探测，以保证在一条链路出现故障的情况下，流量仍然能够通过另一条链路转发。
- 允许内网访问 Internet。
- 为保证内网信息安全，不允许 Internet 用户访问公司内网。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 创建基于负载均衡的路由，将下一跳 IP 地址设置为 ISP A 和 ISP B 路由器的 IP 地址。
- 创建源地址转换规则，使内网员工可以通过 eth-s1p2 接口的公有 IP 地址访问 Internet。
- 创建安全域，允许不同安全域间的访问。
- 创建访问策略，允许内网员工访问 Internet，不允许 Internet 用户访问内网。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表中**分别点击接口所对应的，进行如下配置：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.118.1.1/24
   - eth-s1p3：
     - 模式：三层
     - （静态） IP 地址：202.118.2.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 202.118.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

创建基于负载均衡的路由

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，创建一条 IPv4 缺省路由。
   - 类型：IPv4 地址
   - 目的 IPv4 地址：0.0.0.0
   - 掩码长度：0
   - Metric：1
   - 出口接口 > 负载均衡：
     - 接口：eth-s1p2；网关：202.118.1.2；权重：7；探测类型：Ping；探测 IPv4 地址：202.118.1.2；探测周期：10；探测重试次数：5
     - 接口：eth-s1p3；网关：202.118.2.2；权重：3；探测类型：Ping；探测 IPv4 地址：202.118.2.2；探测周期：15；探测重试次数：5
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface
eth-s1p2 gateway 202.118.1.2 7 ip-track ping 192.168.1.20 10 5 1
NetEye@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface
eth-s1p3 gateway 202.118.2.2 3 ip-track ping 192.168.1.10 15 5 1
NetEye@root-system] exit
NetEye@root>save config
```

创建源地址转换规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建以下规则：
   - 序号：1
   - 名称：snat1
   - NAPT：勾选
   - 源 IP 地址列表 > IPv4 地址 / 掩码：192.168.2.0/24， 192.168.3.0/24
   - 转换后接口：eth-s1p2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] exit
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - Untrust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2， eth-s1p3
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust
NetEye@root-system] zone Trust based-layer3 eth-s1p1
NetEye@root-system] zone Untrust
NetEye@root-system] zone Untrust based-layer3 eth-s1p2,eth-s1p3
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy11：
     - 序号：1
     - 源安全域：Trust
     - 源 IP：192.168.1.0/24
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：允许
   - policy12：
     - 序号：2
     - 源安全域：Untrust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy11 Trust 192.168.1.0/24 any any any any permit enable 1
NetEye@root-system] policy access policy12 Untrust any any any any any deny enable 2
NetEye@root-system] exit
NetEye@root> save config
```

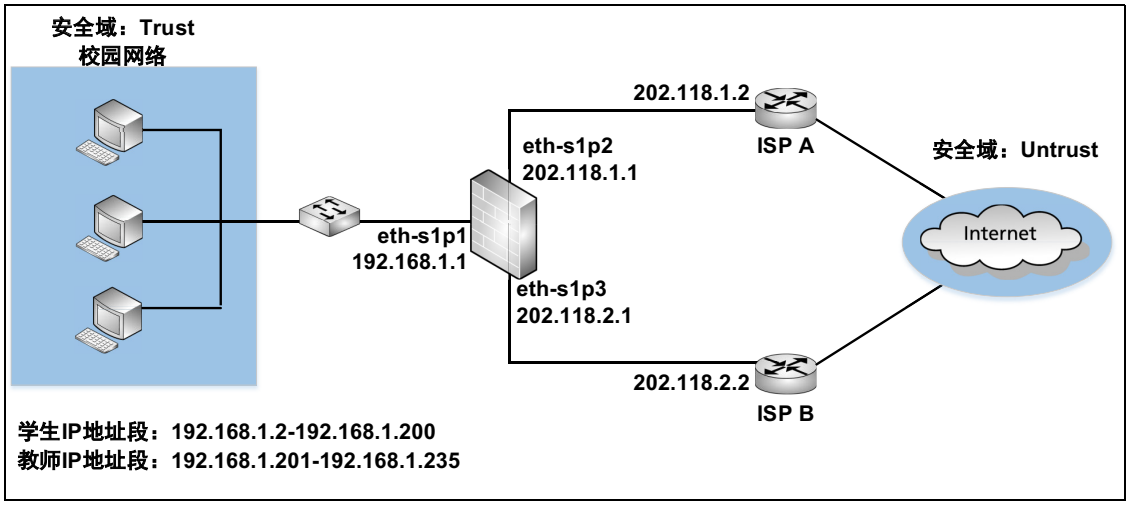
5.4.2 范例：创建策略路由

本范例介绍如何使用策略路由对某大学内网数据流进行分流控制。

基本需求

- 教师通过 ISP A 访问 Internet；学生通过 ISP B 访问 Internet。
- Internet 用户不允许访问内网。
- 为制定统一的访问控制策略，将内网和外网划分到不同的安全域。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 创建策略路由，控制来自不同源的数据流走向。
- 创建安全域，将三层以太网接口划分到安全域中。
- 创建访问策略，控制不同安全域间的访问。
- 创建源地址转换规则，允许内网访问 Internet。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表中**分别点击接口所对应的，进行如下配置：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.118.1.1/24
   - eth-s1p3：
     - 模式：三层
     - （静态） IP 地址：202.118.2.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 202.118.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

创建策略路由

1. 选择**网络** > **路由** > **策略路由**。
2. 点击**新建**，创建以下策略：
   - 序号：1
   - 名称：student
   - 入口接口：eth-s1p1
   - 源 IP 地址列表：192.168.1.2-192.168.1.200
3. 点击**确定**。
4. 在**策略路由列**表中点击 “**student 路由表** ”，点击**新建**，为匹配以上策略的数据流创建路由出口。
   - 类型：IPv4 地址
   - 目的 IPv4 地址：0.0.0.0
   - 掩码长度：0
   - Metric：1
   - 出口接口 > 常规：
     - 接口：eth-s1p3
     - 网关：202.118.2.2
5. 选择**网络** > **路由** > **策略路由**。
6. 点击**新建**，创建以下策略：
   - 序号：2
   - 名称：teacher
   - 入口接口：eth-s1p1
7. 源 IP 地址列表：192.168.1.201-192.168.1.235
8. 点击**确定**。
9. 在**策略路由列**表中点击 “**teacher 路由表** ”，点击**新建**，为匹配以上策略的数据流创建路由出口。
   - 类型：IPv4 地址
   - 目的 IPv4 地址：0.0.0.0
   - 掩码长度：0
   - Metric：2
   - 出口接口 > 常规：
     - 接口：eth-s1p2
     - 网关：202.118.1.2
10. 点击**确定**。
11. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy route student enable
NetEye@root-system-routepolicy-student] matching input-interface eth-s1p1
NetEye@root-system-routepolicy-student] matching sip 192.168.1.2 192.168.1.200
NetEye@root-system-routepolicy-student] matching protocol any
NetEye@root-system-routepolicy-student] route default interface eth-s1p3 gateway 202.118.2.2 1
NetEye@root-system-routepolicy-student] exit
NetEye@root-system] policy route teacher enable
NetEye@root-system-routepolicy-teacher] matching input-interface eth-s1p1
NetEye@root-system-routepolicy-teacher] matching sip 192.168.1.201 192.168.1.235
NetEye@root-system-routepolicy-teacher] matching protocol any
NetEye@root-system-routepolicy-teacher] route default interface eth-s1p2 gateway 202.118.1.2 2
NetEye@root-system-routepolicy-teacher] end
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - Untrust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2， eth-s1p3
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust
NetEye@root-system] zone Trust based-layer3 eth-s1p1
NetEye@root-system] zone Untrust
NetEye@root-system] zone Untrust based-layer3 eth-s1p2,eth-s1p3
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy11：
     - 序号：1
     - 源安全域：Trust
     - 源 IP：192.168.1.0/24
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：允许
   - policy12：
     - 序号：2
     - 源安全域：Untrust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy11 Trust 192.168.1.0/24 any any any any permit enable 1
NetEye@root-system] policy access policy12 Untrust any any any any any deny enable 2
NetEye@root-system] exit
NetEye@root> save config
```

创建源地址转换规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建以下源地址转换规则：
   - 序号：1
   - 名称：snat1
   - NAPT：勾选
   - 源 IP 地址列表 > IPv4 地址 / 掩码：192.168.1.0/24
   - 转换后接口：eth-s1p2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] exit
NetEye@root> save config
```

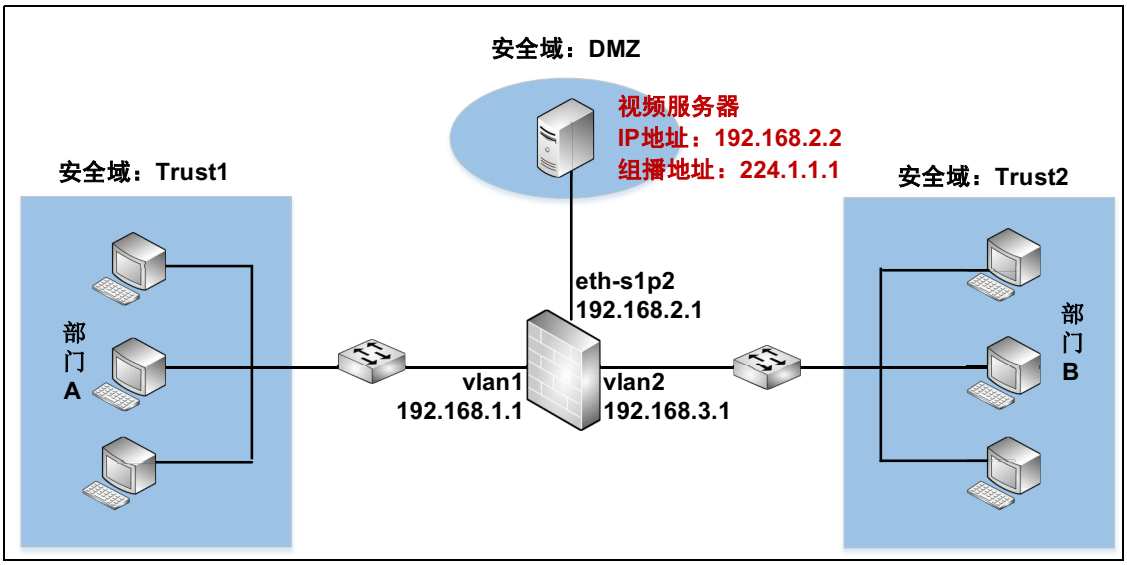
5.4.3 范例：应用静态多播路由

某公司的视频服务器使用多播组 IP 地址 224.1.1.1 向两个部门播放视频节目。多播数据包的 TTL 值为 5。

基本需求

- 允许部门 A 和 B 中的员工收看视频节目。
- 为制定统一的访问控制策略，将公司的两个部门和服务器各划分到不同的安全域中。
- 为加强网络管理并提高安全性，将两个部门划分到不同的 VLAN 内。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 创建 VLAN 接口，将二层以太网接口划分给 VLAN 接口并为 VLAN 接口设置 IP 地址。
- 配置 DVMRP，启用 NISG-IPS 的 DVMRP（多播路由）功能并选择启用 DVMRP 的接口。只有启用 DVMRP，多播路由才会生效。
- 创建静态多播路由，以使 vlan1 和 vlan2 中的主机能够观看视频服务器播放的节目。
- 创建安全域，将三层以太网接口划分到安全域中。
- 创建多播策略，允许不同接口间的多播数据转发。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击接口所对应的，并配置接口为如下：
   - eth-s1p1：
     - 模式：二层
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：192.168.2.1/24
   - eth-s1p3：
     - 模式：二层
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer2-interface
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer2-interface
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

创建 VLAN 接口

1. 选择**网络** > **接口**。
2. 点击**新建** >**VLAN**，创建 vlan1 和 vlan2。将 eth-s1p1 划分给 vlan1， eth-s1p3 划分给 vlan2。将 vlan1 的 IP 地址设置为 192.168.1.1/24，vlan2 的 IP 地址设置为 192.168.3.1/24。
3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] hold ethernet s1p1
NetEye@root-system-vlan1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-vlan1] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] hold ethernet s1p3
NetEye@root-system-vlan2] ip address 192.168.3.1 255.255.255.0
NetEye@root-system-vlan2] end
NetEye@root> save config
```

配置 DVMRP

1. 选择**网络** > **多播** >**DVMRP**，进行如下配置：
   - DVMRP：启用
   - 启用的 DVMRP 接口：
     - 接口：eth-s1p2， vlan1， vlan2

   其他参数在静态路由中不会生效。
2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dvmrp enable
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] dvmrp on
NetEye@root-system-vlan1] dvmrp metric 1
NetEye@root-system-vlan1] dvmrp threshold 1
NetEye@root-system-vlan1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] dvmrp on
NetEye@root-system-if-eth-s1p2] dvmrp metric 1
NetEye@root-system-if-eth-s1p2] dvmrp threshold 1
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] dvmrp on
NetEye@root-system-vlan2] dvmrp metric 1
NetEye@root-system-vlan2] dvmrp threshold 1
NetEye@root-system-vlan2] exit
NetEye@root-system] exit
NetEye@root> save config
```

创建静态多播路由

1. 点击**多播路由**超链接。
2. 点击**新建**，创建以下静态多播路由：
   - 源 IP 地址：200.200.20.2
   - 多播组 IP 地址：224.1.1.1
   - 入口接口：eth-s1p2
   - 转发接口 > 已选接口：vlan1， vlan2
   - TTL：2

   因为多播数据包的 TTL 值是 5，要使 NISG-IPS 转发多播数据包，需要将静态路由的 TTL 设置为小于 5 的值 （在本范例中，设置为 2）。
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dvmrp route 192.168.2.2 224.1.1.1 input eth-s1p2
forwarding vlan1,vlan2 threshold 2
NetEye@root-system] exit
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust1：
     - 安全域类型：基于三层接口
     - 已选接口：vlan1
   - DMZ：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2
   - Trust2：
     - 安全域类型：基于三层接口
     - 已选接口：vlan2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust1
NetEye@root-system] zone Trust1 based-layer3 vlan1
NetEye@root-system] zone Trust2
NetEye@root-system] zone Trust2 based-layer3 vlan2
NetEye@root-system] zone DMZ
NetEye@root-system] zone DMZ based-layer3 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

创建多播策略

1. 选择**防火墙** > **多播策略**。
2. 点击**新建**，创建一条名为 policy1 的多播策略，允许多播数据流转发。
   - 序号：1
   - 源安全域：DMZ
   - 源 IP：192.168.2.2
   - 多播组 IP：224.1.1.1
   - 允许的安全域：Trust1， Trust2， DMZ
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy multicast policy1 DMZ 192.168.2.2 224.1.1.1
Trust1,Trust2,DMZ enable 1
NetEye@root-system] end
NetEye@root> save config
```

6 ISP 智能选路

本章介绍 ISP 智能选路特性，包括：

6.1 概述

在多条 ISP （Internet Service Provider，互联网服务提供商）线路环境中，当用户访问网络时， NISG-IPS 的 ISP 智能选路特性可以根据用户的目的 IP 地址为用户选择一条最合适的 ISP 线路或多条带有负载均衡的线路。比如，用户访问电信网络则走电信线路，访问联通网络则走联通线路。因此可以充分利用出口链路资源，提高用户的访问速度。

6.1.1 ISP 智能选路策略

NISG-IPS 只有 1 条选路策略。在启用 ISP 智能选路策略后，管理员可以编辑此策略，但不能删除此策略或创建新的策略。

6.1.1.1 ISP 线路

管理员可以在选路策略中最多添加 8 条 ISP 线路。在每条线路中，设置运营商类型、出口接口、线路名称、下一跳网关以及此线路的带宽。NISG-IPS 支持的运行商包括中国电信、中国联通、中国移动、中国教育和科研网。管理员需要选择一条已添加的 ISP 线路作为出口。当选路失败时，使用此线路转发数据包。

6.1.1.1 ISP 智能选路规则

NISG-IPS 基于以下任一规则选择出最佳的线路：

- IP 地址库选路

  将数据包的目的 IP 地址与 IP 地址归属列表、地址库进行匹配，找出数据包的目的 IP 地址属于哪家运营商，然后使用此运营商的首选线路转发数据包。

  以下情况为选路失败：

  - 当数据包的目的 IP 地址既不在 IP 地址归属列表中又不在地址库中
  - 当 NISG-IPS 确定数据包目的 IP 地址的运营商后，发现 ISP 线路列表中没有这家运营商的 ISP 线路

- 基于可用带宽的负载均衡

  在所有 ISP 线路中，选择可用带宽最大的 ISP 线路转发数据包。如果存在多条 ISP 线路，它们的可用带宽相同且为最大，那么从中选择最大带宽值最高的 ISP 线路转发数据包； 如果存在多条 ISP 线路，它们的可用带宽相同且为最大，并且它们的最大带宽值也相同，那么从中随机地选择一条 ISP 线路转发数据包。

  当所有 ISP 线路的可用带宽都小于或等于 10Kbps 时，选路失败。

- 基于带宽利用率的负载均衡

  在所有 ISP 线路中，选择带宽利用率最小的 ISP 线路转发数据包。如果存在多条 ISP 线路，它们的带宽利用率相同且为最小，那么从中选择最大带宽值最高的 ISP 线路转发数据包； 如果存在多条 ISP 线路，它们的带宽利用率相同且为最小，并且最大带宽值也相同，那么从中随机地选择一条 ISP 线路转发数据包。

  当所有 ISP 线路的带宽利用率都大于或等于 99% 时，选路失败。

6.1.2 IP 地址归属

管理员可以建立 IP 地址与其所属运营商的对应关系，以便 NISG-IPS 基于 IP 地址库选路规则时进行智能选路。如果不确定 IP 地址的运营商，可以在 NISG-IPS 上查询此 IP 地址的运营商。

管理员也可以将 IP 地址与其运营商的对应关系记录到本地的文本文档（后缀为 .txt，每一行文字为一条 IP 地址归属信息条目），再将文本文档导入到 NISG-IPS 上。当记录 IP 地址与运营商的对应关系时，应遵循如下格式（这里的 IP 地址只是用于举例说明）：

- 运营商（不区分大小写）+ 空格 + IP 地址，如 China-Telecom 1.1.1.1
- 运营商 + 空格 + IP 地址范围，如 China-Unicom 1.1.1.2-1.1.1.3
- 运营商 + 空格 + IP 地址 / 掩码长度，如 China-Mobile 1.1.1.128/25
- 以上三种格式的混合形式，如 CERNET 1.1.2.128/25,1.1.2.1-1.1.2.126,1.1.2.127

对于每一种格式，如果有多个 IP 地址项，两个 IP 地址项中间应以逗号分隔。管理员也可以根据需要在每行后面补充描述信息，如 China-Telecom 1.1.1.1, 2.2.2.2 3.3.3.3-3.3.3.10 4.4.4.4-4.4.4.10 中国电信。

6.1.3 地址库及更新

地址库包含所有属于中国电信、中国联通、中国移动以及中国教育和科研网的 IP 地址，且每个 IP 地址只属于一个运营商。地址库用于 NISG-IPS 基于 IP 地址库选路规则时进行智能选路。

管理员可以对地址库进行更新。更新方式包括以下两种方式：

- 手动：通过手动上传本地文件完成地址库的更新。
- 自动：通过设置更新服务器地址和更新时间周期，可以使地址库自动进行更新。

6.2 基本配置步骤

本节介绍如何在 NISG-IPS 上配置 ISP 智能选路，包括：

6.2.1 设置 ISP 智能选路策略

1. 选择**网络** > **ISP 智能选路** > **策略**。
2. 点击**启用 ISP 智能选路**，启用 NISG-IPS 的智能选路功能。

3. 在 **ISP 线路列表**中，点击**添加**，添加一条 ISP 线路 （最多 8 条）。

4. 点击**确定**。在 **ISP 线路列表**中，**主**表示线路为首选线路。第一条添加的线路缺省为首选线路。当有多条线路时，管理员可以根据需要选择其他线路作为首选线路。
5. 在 **ISP 智能选路规则**下拉框中选择任一规则。

6. 选择一条 ISP 线路作为 ISP 智能选路失败时转发数据包的出口。
7. 点击**确定**。
8. 点击 。

6.2.2 设置 IP 地址归属

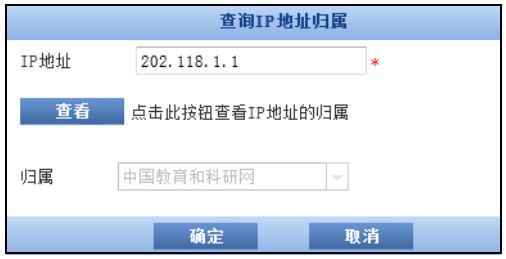
6.2.2.1 创建 IP 地址与运营商的对应关系

1. 选择**网络** > **ISP 智能选路** >**IP 地址归属**。
2. 点击**新建**，创建 IP 地址与所属运营商的对应关系。设置名称、IP 地址归属的运营商和描述信息。
3. 在 **IP 地址列表**中，点击**添加**，添加 IP 地址并点击**确定**。可以选择 IP 地址对象和对象组、 IPv4 地址、IPv4 地址范围、 IPv4 地址和掩码：

4. 点击**确定**。
5. 点击 。

6.2.2.2 查询 IP 地址的运营商

1. 选择**网络** > **ISP 智能选路** >**IP 地址归属**。
2. 点击**查询**。
3. 在 **IP 地址**文本框中输入要查询的 IP 地址。
4. 点击**查看**， IP 地址的运营商便会在**归属**处显示。

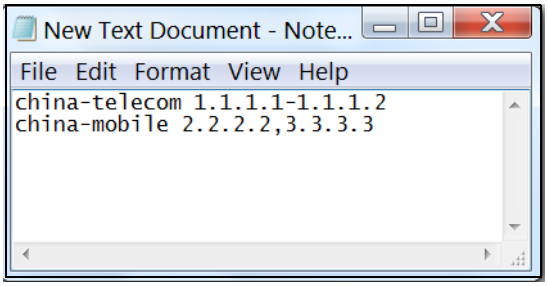


5. 点击**确定**。

6.2.2.3 导入 IP 地址与运营商的对应关系

管理员需要先将 IP 地址与运营商的对应关系记录到本地文本文档中 （后缀 .txt），再将文本文档导入到 NISG-IPS 上。文档中的文字必须是 UTF-8 字符。

假如已在本地文档中记录以下对应关系：



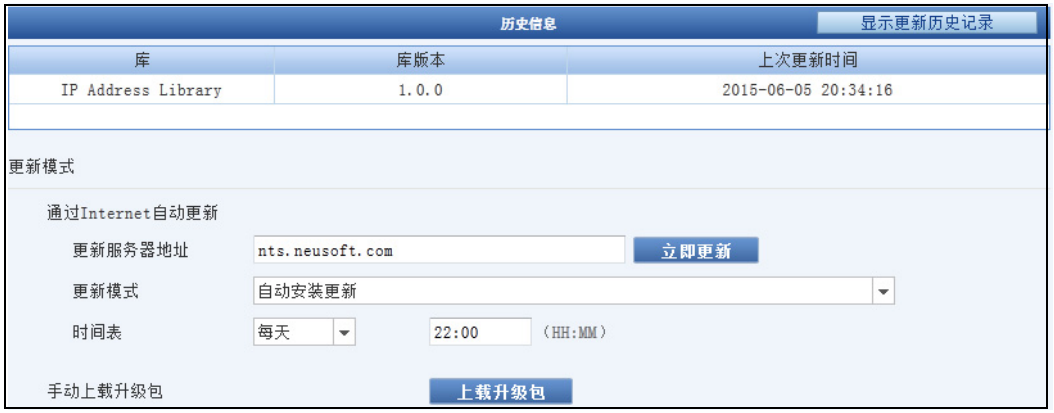
1. 选择**网络** > **ISP 智能选路** >**IP 地址归属**。
2. 点击**导入**。
3. 选择导入类型，**添加**是指将文本文档中的条目添加到现有 IP 地址归属列表中，**覆盖**是指覆盖现有 IP 地址归属列表。
4. 点击**浏览**，选择要导入的文本文档。

5. 点击**确定**。可以在 **IP 地址归属列表**中查看导入的条目。

6. 点击 。

6.2.3 设置地址库更新

1. 选择**网络** > **ISP 智能选路** > **更新**。
2. 在**历史信息**列表中，查看历史更新记录。



3. 设置地址库更新模式，可以通过 Internet 自动更新或手动更新两种方式进行更新。
   - 通过 Internet 自动更新：
     - 在**更新服务器地址**文本框中，输入服务器的地址。可以点击**立即更新**，立即更新地址库。
     - 在**更新模式**下拉框中选择**自动安装更新**或**从不检查更新**。
     - 设置更新的时间表，选择**每天**、**每周**、**每月**或**间隔**。选择**每天**时，需要设置每天更新的时间；选择**每周**时，需要设置每周某天更新的时间；选择**每月**时，需要设置每月某日的更新时间；选择**间隔时**，需要设置两次更新间隔的时间段。
   - 手动上载升级包：点击**上载升级包**，选择升级包的本地路径，点击**确定**。
4. 点击**确定**。
5. 点击。

6.3 配置参数说明

6.3.1 ISP 智能选路策略参数

表 147 ISP 智能选路策略参数

配置信息	说明
启用 ISP 智能选路	勾选此选项启用 ISP 智能选路功能，取消勾选禁用此功能。
ISP 智能选路规则	ISP 智能选路功能为数据包进行智能选路所采用的规则，包括以下： • IP 地址库选路 • 基于可用带宽的负载均衡 • 基于带宽利用率的负载均衡
当 ISP 智能选路失败时，选择出口	当选路规则选路失败时，使用所配置的出口转发数据包。 管理员可以选择任一已添加的 ISP 线路。
ISP 线路列表	此列表包含所有已添加的 ISP 线路。管理员添加 ISP 线路时，需要设置以下参数： • **类型**：ISP 线路的类型，包括中国电信、中国联通、中国移动、中国教育和科研网。 • **名称**：ISP 线路的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # • **接口**：三层接口 （环回接口、隧道接口以及虚拟接口除外）， ISP 线路上承载的流量通过该三层接口转发。 • **网关**：接口网关的 IP 地址。 • **带宽**：ISP 线路的最大带宽。取值范围为 1-999999，单位为 Kbps、 Mbps 或者 Gbps。 **主**表示线路为首选线路。

6.3.2 IP 地址归属参数

表 148 IP 地址归属参数

配置信息	说明
名称	IP 地址与运营商对应关系的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
归属	IP 地址列表中全部 IP 地址所属的运营商，包括中国电信、中国联通、中国移动以及中国教育和科研网。
描述	IP 地址与运营商对应关系的描述信息。长度 0-255 字节， UTF-8 字符。不能包含以下字符：？" ' \ < > &
IP 地址列表	此列表包含所有已添加的 IP 地址信息。管理员可以添加以下类型的 IP 地址： • IPv4 地址对象 • IPv4 地址对象组 • IPv4 地址 • IPv4 地址范围 • IPv4 地址 / 掩码 此列表最多支持 128 个 IP 地址条目。

6.3.3 地址库及更新参数

表 149 地址库及更新参数

配置信息	说明
历史信息	可以在此列表中查看地址库更新信息。
更新方式	包括以下两种方式： • **通过 Internet 自动更新**：通过设置更新服务器地址和更新时间周期，可以使地址库自动进行更新。缺省的服务器地址为 nts.neusoft.com/ip_address_library。更新模式包括：自动安装更新 （缺省）和从不检测更新。当更新模式为自动安装更新时，可以设置以下任一更新时间周期：每天更新、每周更新、每月更新或间隔若干小时对地址库进行更新。 • **手动**：通过手动上传本地升级包完成地址库的更新。

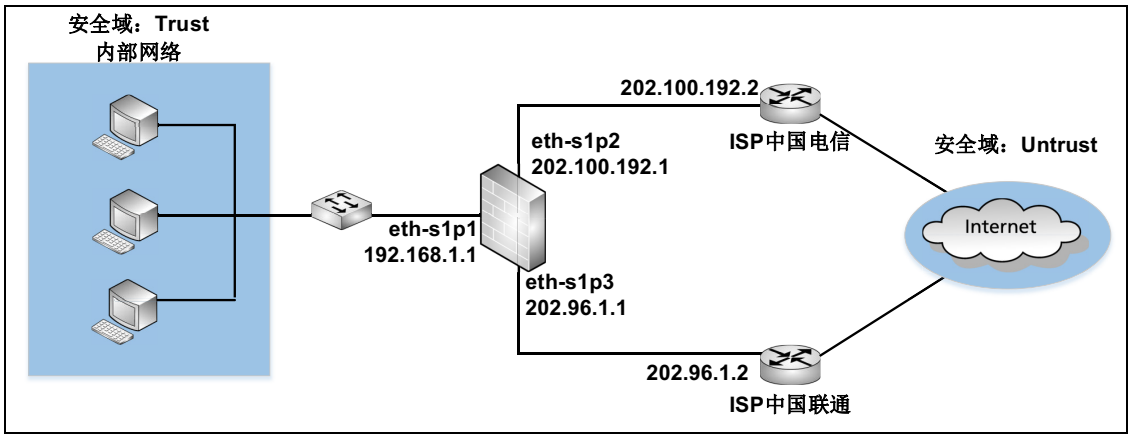
6.4 ISP 智能选路范例

某公司内部网络通过两个网络服务商 （ISP）中国电信和中国联通连接到互联网上。电信线路 100M，联通线路 100M。

基本需求

- 为提升网络访问速度，当内网员工的目的 IP 地址属于电信时，数据流走电信线路；当目的地址属于联通时，走联通线路。
- 为保证内网信息安全，不允许 Internet 用户访问公司内网。

组网拓扑



提示：这里的 IP 地址只是用于举例说明。可以根据实际需要更改 IP 地址。

配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 配置 ISP 智能选路策略，设置 ISP 智能选路规则并添加中国电信和中国联通两条出口线路。
- 创建安全域，将内网和外网划分到不同的安全域内。
- 创建源地址转换规则，使内网员工可以通过 eth-s1p2 的公有 IP 地址访问电信资源并通过 eth-s1p3 接口的公有 IP 地址访问联通资源。
- 创建访问策略，允许内网员工访问 Internet，不允许 Internet 用户访问内网。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表中**分别点击接口所对应的，进行如下配置：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.100.192.1/24
   - eth-s1p3：
     - 模式：三层
     - （静态） IP 地址：202.96.1.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.100.192.1 255.255.248.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 202.96.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

配置 ISP 智能选路策略

1. 选择**网络** > **ISP 智能选路** > **策略**，配置为如下：
   - ISP 智能选路功能：启用
   - ISP 智能选路的规则：IP 地址库选路
   - ISP 线路列表：
     - 类型：中国电信；名称：line1 ；接口：eth-s1p2 ；网关：202.100.192.2 ；带宽：100
     - 类型：中国电信；名称：line1 ；接口：eth-s1p2 ；网关：202.100.192.2 ；带宽：100
   - 当 ISP 智能选路失败时，选择作为出口：中国电信 _line1
2. 点击**确定**。
3. 点击 。

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - Untrust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2， eth-s1p3
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust
NetEye@root-system] zone Trust based-layer3 eth-s1p1
NetEye@root-system] zone Untrust
NetEye@root-system] zone Untrust based-layer3 eth-s1p2,eth-s1p3
NetEye@root-system] exit
NetEye@root> save config
```

创建源地址转换规则

5. 选择**网络 > 地址转换 > 源地址转换**。
6. 点击**新建**，分别创建以下规则：
   - rule1:
     - 序号：1
     - NAPT：勾选
     - 源 IP 地址列表 > IPv4 地址 / 掩码：192.168.1.0/24
     - 转换后接口：eth-s1p2
     - 入口接口：eth-s1p1
     - 出口接口：eth-s1p2
   - rule2:
     - 序号：2
     - NAPT：勾选
     - 源 IP 地址列表 > IPv4 地址 / 掩码：192.168.1.0/24
     - 转换后接口：eth-s1p3
     - 入口接口：eth-s1p1
     - 出口接口：eth-s1p3
7. 点击**确定**。
8. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat rule1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] policy snat rule1 matching input-interface eth-
s1p1
NetEye@root-system] policy snat rule1 matching output-interface eth-
s1p2
NetEye@root-system] policy snat rule2 netmask 192.168.1.0
255.255.255.0 interface eth-s1p3 napt enable
NetEye@root-system] policy snat rule2 matching input-interface eth-
s1p1
NetEye@root-system] policy snat rule2 matching output-interface eth-
s1p3
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy11：
     - 序号：1
     - 源安全域：Trust
     - 源 IP：192.168.1.0/24
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：允许
   - policy12：
     - 序号：2
     - 源安全域：Untrust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy11 Trust 192.168.1.0/24 any any any any permit enable 1
NetEye@root-system] policy access policy12 Untrust any any any any any deny enable 2
NetEye@root-system] exit
NetEye@root> save config
```

7 多播

本章介绍 NISG-IPS 的多播特性。

7.1 概述

NISG-IPS 支持 IPv4 多播。多播是将数据传送给一组主机的过程。这些主机由一个单独的目的 IP 地址 （多播组 IP 地址）来标识。

本节介绍 NISG-IPS 的 DVMRP （动态多播路由）和 IGMP Snooping 特性。

7.1.1 DVMRP

NISG-IPS 支持距离矢量多播路由协议 （Distance-Vector Multicast Routing Protocol，DVMRP）。 DVMRP 用于维护多播路由表、为每个多播源和目的主机组构建不同的多播树以及转发多播数据包。 DVMRP 可以侦听 IGMP、 DVMRP 和 PIM 报文。

启用 DVMRP 的 NISG-IPS 设备可与邻接的 DVMRP 路由设备互相交换路由信息，可以动态生成多播路由条目。如果动态学习到的多播路由条目未被使用且超出缓存时间，NISG-IPS 会自动将其删除，也可以从邻居路由更新中再次学习到。

DVMRP 支持协议无关多播 （Protocol Independent Multicast， PIM）邻居发现协议。NISG-IPS 可以与运行 PIM 协议的多播路由器建立邻居关系。在启用了 PIM 邻居发现功能的情况下，当收到某一 PIM 路由器发送的 PIMv1 Query 或 PIMv2 Hello 报文时，NISG-IPS 会与该路由器建立邻居关系，并且发送 DVMRP 路由交换报文。

7.1.2 IGMP Snooping

NISG-IPS 支持 IGMPv1 和 IGMPv2。通过使用 Internet 组管理协议 （Internet Group Management Protocol，IGMP），主机可以动态加入多播组，NISG-IPS 可以管理本地网络组成员信息。

为了有效抑制多播数据在链路层的扩散， NISG-IPS 提供 IGMP Snooping 功能。 IGMP Snooping 是运行在二层设备上的多播协议，用于管理和控制 VLAN 内的多播组。如果不启用 IGMP Snooping，当某一 VLAN 接收到多播数据包时，NISG-IPS 会将多播数据包转发给 VLAN 内的所有接口，因而会浪费大量的系统资源。

NISG-IPS 的 IGMP Snooping 功能主要包括：

- 监听 IGMP、 DVMRP 和 PIM 报文。
- 维护多播 CAM 表。

  多播 CAM 表是用于二层交换的地址表，为每个 VLAN 记录多播组 IP 地址、多播组 MAC 地址和 VLAN 内用于转发多播数据包的接口之间的对应关系。多播 CAM 表由动态和静态多播 CAM 表项组成。
- 根据多播 CAM 表在 VLAN 内转发多播数据包。

  NISG-IPS 只将多播数据包转发给处于启用状态的 CAM 表转发接口，而不转发给 VLAN 中的所有接口。
- 保持主机的 IGMP 协议版本和路由设备的 IGMP 协议版本的一致性。

7.1.2.1 动态多播 CAM 表项

动态多播 CAM 表项是 NISG-IPS 通过监听 IGMP 消息动态生成和删除的。在启用 IGMP Snooping 的 VLAN 中，当接收到主机发出的 IGMP 成员报告时， NISG-IPS 监听此报告。通过记录接收报告的二层接口、主机希望加入的多播组的 IP 地址以及对应的多播组 MAC 地址的映射关系， NISG-IPS 可以创建动态 CAM 表项。如果在 260 秒之内没有收到主机发送的成员报告或主机发送离开组消息时， NISG-IPS 将会自动删除此动态 CAM 表项。如果在 260 秒内收到报告， NISG-IPS 会刷新此表项。

7.1.2.2 静态多播 CAM 表项

静态多播 CAM 表项是管理员手动创建和修改的。在 VLAN 中启用 IGMP Snooping 后，VLAN 的静态多播 CAM 表项才会生效。

7.2 基本配置步骤

如需使用特定 IP 地址对象、 IP 地址对象组、服务对象和服务对象组，需要首先选择**系统 > 对象**创建它们。

7.2.1 配置动态多播路由

必须同时配置多播策略以允许转发多播数据包。更多信息，参见第 10 章，策略。

1. 选择**网络** > **多播** >**DVMRP**。
2. 启用防火墙的 DVMRP （多播路由）功能。
3. 点击**添加**，选择启用 DVMRP 的接口，以允许接口转发多播数据包，设置 DVMRP 接口的阈值和 Metric。
4. 可选设置：
   - **缓存有效时间**：动态学习到的多播路由在缓存中存在的时间长度。
   - **裁剪有效时间**：NISG-IPS 保持裁剪状态的时间长度。
   - **PIM 邻居发现**：NISG-IPS 能够监听 PIM 报文，与运行 PIM 协议的多播路由器建立邻居关系。

5. 点击**确定**。
6. 点击。 DVMRP 能够创建并删除动态多播路由。

表 150 DVMRP 命令

dvmrp {enable | disable}	启用或禁用 DVMRP。
dvmrp cache-lifetime *time*	设置 DVMRP 路由在多播缓存中的保存时间。
dvmrp prune-lifetime *time*	设置 NISG-IPS 保持裁剪状态的有效时间。
dvmrp metric {*metric_value* | **default**}	设置三层接口的 DVMRP 度量值。
dvmrp {on | off}	启用或禁用三层接口的 DVMRP 功能。
dvmrp pim {enable | disable}	启用或禁用 PIM 邻居发现功能。
dvmrp threshold {*threshold_value* | **default**}	设置三层接口的 TTL 阈值。
show dvmrp {interface | neighbor | timer}	显示 DVMRP 监控信息。
show dvmrp state	显示 DVMRP 配置信息。

7.2.2 应用 IGMP Snooping

必须启用 DVMRP 来启用多播路由功能并创建多播策略以允许转发多播数据包。更多信息，参见 7.2.1 配置动态多播路由和第 10 章，策略。

7.2.2.1 创建 VLAN 接口

1. 选择**网络** > **接口**。
2. 点击**新建**，创建包含二层接口的 VLAN 接口 （vlan1）。

7.2.2.2 为 VLAN 接口配置 IGMP Snooping 功能

1. 选择**网络** > **多播** >**IGMP Snooping**，点击 vlan1 对应的 。
2. 在**状态**区域点击**开**启用 IGMP Snooping 功能。
3. 点击任意接口选项，设置接口的 IGMP 版本和模式。

4. 点击**确定**。
5. 点击 。 NISG-IPS 可以通过监听 IGMP 报文创建并删除动态多播 CAM 表项。

7.2.2.3 创建静态多播 CAM 表项

1. 在**多播 CAM 表**列内点击 vlan1 对应的多播 CAM 表的超链接。点击**新建**创建如下静态多播 CAM 表项 (需要先启用 IGMP Snooping 功能)。

2. 点击**确定**。
3. 点击 。

表 151 IGMP Snooping 命令

igmp-snooping {**on** | **off**}	启用或禁用 IGMP Snooping 功能。
igmp-snooping interface-flags	设置 VLAN 中二层接口所连接的网络类型。
igmp-snooping version	设置 IGMP 版本。
multicast cam-table	添加静态多播 CAM 表项。
show igmp-snooping state [**vlan** *vlan_id*]	显示 IGMP Snooping 状态。
unset multicast cam-table	删除静态多播 CAM 表项。

7.3 配置参数说明

本节介绍配置多播功能时用到的参数：

7.3.1 DVMRP 参数

表 152 DVMRP 参数说明

参数	说明
DVMRP	用于在 NISG-IPS 设备上启用或禁用 DVMRP 功能。 DVMRP 缺省为禁用。
启用的 DVMRP 接口	启用 DVMRP 功能的三层接口 （除环回接口和隧道接口）。只有 DVMRP 接口才能参与多播信息的处理与转发。 • **接口**：三层接口名称。最多可以选择 32 个 DVMRP 接口。 • **阈值**：DVMRP 接口的阈值，用于控制数据包是否能从此接口转发出去。只适用于动态多播路由。 只有当多播数据包的 TTL 值大于接收数据包的 DVMRP 接口的阈值时，数据包才会从接口转发出去。阈值的取值范围为 1 ～ 255，缺省值是 1。 数据包的 TTL 值 （单位为跳数）是指数据包最多可以经过的路由设备数量。当数据包经过一个 DVMRP 路由设备，它的 TTL 值就会减 1。当 TTL 值为 0 时，数据包就会被丢弃。 • **Metric**：DVMRP 接口的路由度量值，用于多播路由交换和更新，只适用于动态多播路由。取值范围是 1 ～ 32，缺省值是 1。
缓存有效时间	动态学习到的多播路由在缓存中的存在时间，必须是 5 的整数倍。取值范围 60 ～ 7200 秒，缺省值是 300 秒。 对于未被使用的动态多播路由，超出该时间后，其信息将从 NISG-IPS 删除。
裁剪有效时间	NISG-IPS 保持裁剪状态的时间，必须是 5 的整数倍。取值范围是 120 ～ 7200 秒，缺省值是 7200 秒。 超过此时间， NISG-IPS 则恢复向下游路由器转发多播数据包。
PIM 邻居发现	如果启用， NISG-IPS 可以监听 PIM 消息并与运行 PIM 协议的多播路由器建立邻居关系。 此功能缺省为禁用。

7.3.2 IGMP Snooping 参数

所有 VLAN 都支持 IGMP Snooping。如果需要在 VLAN 内支持多播并使用 IGMP Snooping 功能，必须启用 IGMP Snooping ；否则，多播数据包将会被转发给 VLAN 内的所有接口。

表 153 IGMP Snooping 参数说明

参数	说明
VLAN	VLAN 接口名称。 管理员只可以为 VLAN 接口配置 IGMP Snooping 功能。IGMP Snooping 最多支持 1024 个 VLAN。
状态	用于在 VLAN 内启用或禁用 IGMP Snooping 功能： • **开**：启用 IGMP Snooping 功能。 • **关**：禁用 IGMP Snooping 功能。 IGMP 缺省为禁用。 启用 IGMP Snooping 后，该功能在 255 秒后生效。
二层接口	VLAN 内包含的二层接口。每个 VLAN 中最多可以包含 32 个接口。
IGMP 版本	VLAN 中二层接口支持的 IGMP 的版本，可以将其设置为： • **自动**：接口通过分析接收的报文动态地识别 IGMP 的版本。**自动**为缺省设置。 • **v1**：IGMP 版本 1。 NISG-IPS 不处理 IGMPv2 独有的报文，如离开组报文。 • **v2**：IGMP 版本 2。 NISG-IPS 既可以处理 IGMPv2 的报文也可以处理 IGMPv1 的报文。处于同一个网段的路由设备必须使用相同的 IGMP 版本。
IGMP 模式	与 VLAN 中二层接口连接的网络设备的类型，可以将其设置为： • **自动**：接口通过接收的报文动态地识别网络类型。**自动**为缺省设置。 • **多播路由器**：与接口相连的是多播路由器。 • **主机**：与接口相连的是主机。

7.3.3 静态多播 CAM 条目参数

表 154 多播 CAM 表参数说明

参数	说明
多播组 IP 地址	目的多播组的 IP 地址。
多播组 MAC 地址	目的多播组的 IP 地址所对应的 MAC 地址。系统根据 IP 地址自动计算 MAC 地址。
转发接口	VLAN 中用于转发多播数据包的接口。 必须为静态多播 CAM 条目设置至少一个转发口。如果某个出口接口是处于禁用的状态，那么不向此接口转发多播数据包。每个多播 CAM 条目最多支持 32 个转发接口。

7.4 多播范例

本节介绍如何在实际场景中配置多播功能，包括：

- 7.4.1 范例：动态 DVMRP 多播路由应用
- 7.4.2 范例：IGMP Snooping 和多播 CAM 表项应用

提示：范例里的 IP 地址只是用于举例说明。可以根据实际需要更改 IP 地址。

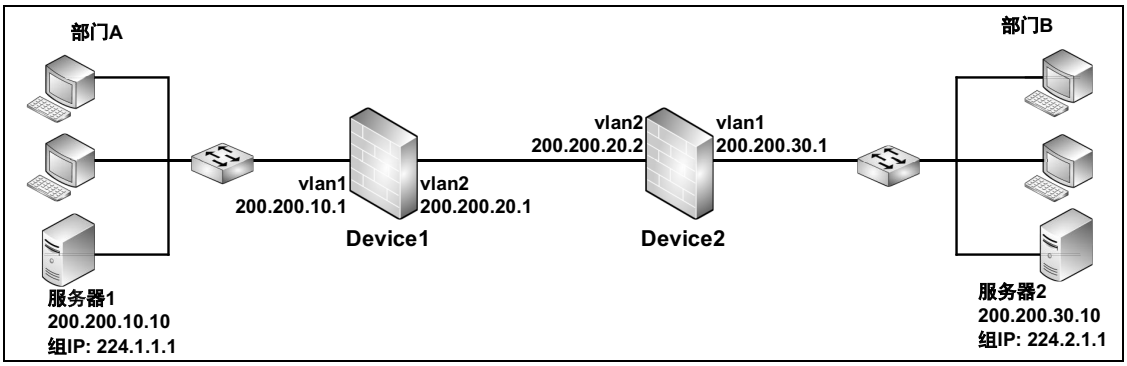
7.4.1 范例：动态 DVMRP 多播路由应用

某公司两个部门的视频服务器分别使用多播组 IP 地址 224.1.1.1 和 224.2.1.1 向两个部门播放视频节目。多播数据包的 TTL 值为 5。

基本需求

- 允许部门 A 和 B 中的员工收看视频节目。
- 为加强网络管理并提高安全性，将每个部门划分到 VLAN 内。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式。
- 创建VLAN接口，将二层以太网接口划分给VLAN接口并为VLAN接口设置IP地址。
- 配置 DVMRP，启用 DVMRP （多播路由）功能并选择启用 DVMRP 的接口。
- 创建多播策略，允许不同 VLAN 接口间的多播数据转发。

配置步骤

分别在 Device1 和 Device2 上进行如下配置：

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击 eth-s1p1 和 eth-s1p2 所对应的，将接口的模式设置为二层。
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer2-interface
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer2-interface
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

创建 VLAN 接口

1. 选择**网络** > **接口**。
2. 点击**新建** > **VLAN**，创建 vlan1 和 vlan2。将 eth-s1p1 划分给 vlan1， eth-s1p2 划分给 vlan2。将 Device1 上 vlan1 的 IP 地址设置为 200.200.10.1/24，vlan2 的 IP 地址设置为 200.200.20.1/24。将 Device2 上 vlan1 的 IP 地址设置为 200.200.30.1/24， vlan2 的 IP 地址设置为 200.200.20.2/24。
3. 点击。

CLI

Device1：

```
NetEye@root> configure mode
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] hold ethernet s1p1
NetEye@root-system-vlan1] ip address 200.200.10.1 255.255.255.0
NetEye@root-system-vlan1] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] hold ethernet s1p2
NetEye@root-system-vlan2] ip address 200.200.20.1 255.255.255.0
NetEye@root-system-vlan2] end
NetEye@root> save config
```

Device2：

```
NetEye@root> configure mode
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] hold ethernet s1p1
NetEye@root-system-vlan1] ip address 200.200.30.1 255.255.255.0
NetEye@root-system-vlan1] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] hold ethernet s1p2
NetEye@root-system-vlan2] ip address 200.200.20.2 255.255.255.0
NetEye@root-system-vlan2] end
NetEye@root> save config
```

配置 DVMRP

1. 选择**网络** > **多播** >**DVMRP**，进行如下配置：
   - DVMRP：启用
   - 启用的 DVMRP 接口 （选择转发多播数据包的接口 vlan1 和 vlan2）：
     - 接口：vlan1 ； 阈值：1 ； Metric：1
     - 接口：vlan2 ； 阈值：1 ； Metric：1
   - 缓存有效时间：7200
   - PIM 邻居发现：勾选
2. 点击**确定**。
3. 点击 。

如需监控动态多播路由或 DVMRP 邻居，选择**监控** > **路由**或**监控** > **多播** >**DVMRP 邻居**。更多信息，参见 16.17.1 DVMRP 邻居。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dvmrp enable
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] dvmrp on
NetEye@root-system-vlan1] dvmrp metric 1
NetEye@root-system-vlan1] dvmrp threshold 1
NetEye@root-system-vlan1] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] dvmrp on
NetEye@root-system-vlan2] dvmrp metric 1
NetEye@root-system-vlan2] dvmrp threshold 1
NetEye@root-system-vlan2] exit
NetEye@root-system] dvmrp cache-lifetime 7200
NetEye@root-system] dvmrp prune-lifetime 7200
NetEye@root-system] dvmrp pim enable
NetEye@root-system] exit
NetEye@root> save config
```

创建多播策略

1. 选择**防火墙** > **多播策略**。
2. 点击**新建**，分别在 Device1 和 Device2 上创建多播策略，允许多播数据流转发。
   - Device1 上：
     - 序号：1
     - 名称：policy1
     - 源安全域：Any
     - 源 IP：200.200.10.10
     - 多播组 IP：224.1.1.1
     - 允许的安全域：Any
   - Device2 上：
     - 序号：1
     - 名称：policy1
     - 源安全域：Any
     - 源 IP：200.200.30.10
     - 多播组 IP：224.2.1.1
     - 允许的安全域：Any
3. 点击**确定**。
4. 点击 。

CLI

Device1 上：

```
NetEye@root> configure mode override
NetEye@root-system] policy multicast policy1 any 200.200.10.10
224.1.1.1 any enable 1
NetEye@root-system] end
NetEye@root> save config
```

Device2 上：

```
NetEye@root> configure mode override
NetEye@root-system] policy multicast policy1 any 200.200.30.10
224.2.1.1 any enable 1
NetEye@root-system] end
NetEye@root> save config
```

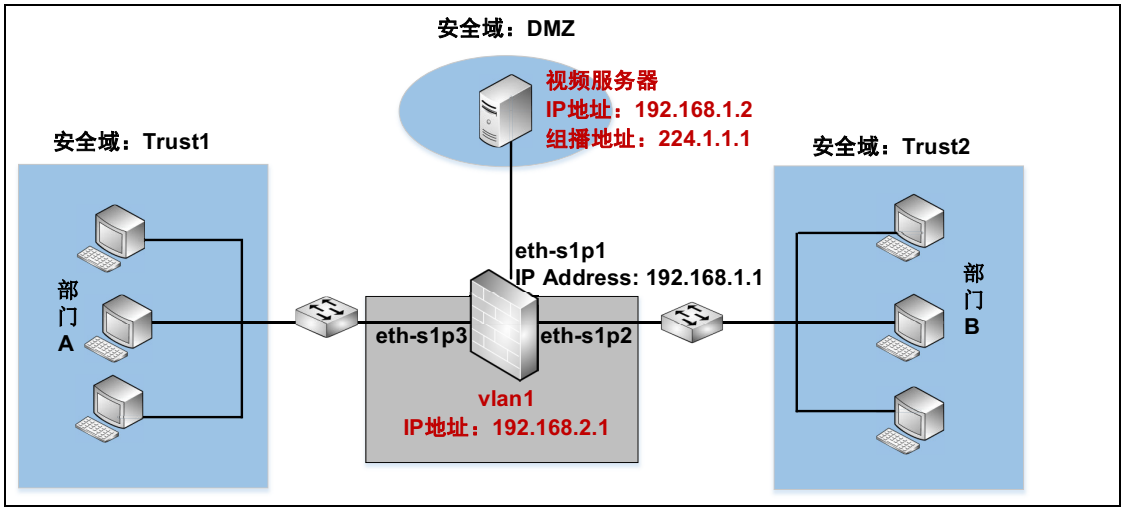
7.4.2 范例：IGMP Snooping 和多播 CAM 表项应用

某公司的视频服务器使用多播组 IP 地址 224.1.1.1 播放视频节目。多播数据包的 TTL 值为 5。

基本需求

- 允许部门 A 和 B 中的员工收看视频节目。
- 为制定统一的访问控制策略，将公司的两个部门和服务器各划分到不同的安全域。
- 为加强网络管理并提高安全性，将两个部门划分到一个 VLAN 内。
- 为了有效抑制多播数据在链路层的扩散，启用NISG-IPS的IGMP Snooping并创建静态 CAM 表项。之后安全域 Trust1 中的主机可以一直接收到多播数据包，而 Trust2 中的主机只有在点播视频节目后才能收到多播数据包。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 创建VLAN接口，将二层以太网接口划分给VLAN接口并为VLAN接口设置IP地址。
- 配置vlan1的IGMP Snooping属性，启用VLAN接口的IGMP Snooping功能并设置IGMP版本和模式。
- 创建静态多播 CAM 表项，设置一直可以接收到多播数据包的二层接口。
- 创建安全域，将三层以太网接口划分到安全域中。
- 创建多播策略，允许不同接口间的多播数据转发。
- 启用 DVMRP，启用动态多播路由功能。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击接口所对应的，并配置接口为如下：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
   - eth-s1p2：
     - 模式：二层
   - eth-s1p3：
     - 模式：二层
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer2-interface
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer2-interface
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

创建 VLAN 接口

1. 选择**网络** > **接口**。
2. 点击**新建**>**VLAN**，创建vlan1。将eth-s1p2和eth-s1p3接口划分给vlan1并将vlan1的IP地址设置为 192.168.2.1/24。
3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] hold ethernet s1p2,s1p3
NetEye@root-system-vlan1] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-vlan1] end
NetEye@root> save config
```

配置 vlan1 的 IGMP Snooping 属性

1. 选择**网络** > **多播** >**IGMP Snooping**，点击 vlan1 对应的，进行如下配置：
   - **状态：开** （启用 IGMP Snooping 功能）
   - 二层接口：eth-s1p2； IGMP 版本：v2； IGMP 模式：自动
   - 二层接口：eth-s1p3； IGMP 版本：v2； IGMP 模式：自动
2. 点击**确定**。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] igmp-snooping on
NetEye@root-system-vlan1] igmp-snooping version ethernet s1p2 v2
NetEye@root-system-vlan1] igmp-snooping version ethernet s1p3 v2
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet s1p2
auto
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet s1p3
auto
NetEye@root-system-vlan1] end
NetEye@root> save config
```

创建静态多播 CAM 表项

1. 选择**网络** > **多播** >**IGMP Snooping**。
2. 在**多播 CAM 表**列内点击 vlan1 对应的多播 CAM 表的超链接。
3. 点击**新建**，创建如下静态多播 CAM 表项：
   - 多播组 IP 地址：224.1.1.1
   - 转发接口 > 已选接口：eth-s1p3
4. 点击**确定**。
5. 点击  。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] multicast cam-table 224.1.1.1 eth-s1p3
NetEye@root-system-vlan1] end
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust1：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p3
   - DMZ：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - Trust2：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust1
NetEye@root-system] zone Trust1 based-layer2 vlan1 eth-s1p3
NetEye@root-system] zone Trust2
NetEye@root-system] zone Trust2 based-layer2 vlan1 eth-s1p2
NetEye@root-system] zone DMZ
NetEye@root-system] zone DMZ based-layer3 eth-s1p1
NetEye@root-system] exit
NetEye@root> save config
```

创建多播策略

1. 选择**防火墙** > **多播策略**。
2. 点击**新建**，创建一条名为 policy1 的多播策略，允许多播数据流转发。
   - 序号：1
   - 源安全域：DMZ
   - 源 IP：192.168.1.2
   - 多播组 IP：224.1.1.1
   - 允许的安全域：Trust1， Trust2， DMZ
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy multicast policy1 DMZ 192.168.1.2 224.1.1.1
Trust1,Trust2,DMZ enable 1
NetEye@root-system] end
NetEye@root> save config
```

启用 DVMRP

1. 选择**网络** > **多播** > **DVMRP**。
2. 启用 DVMRP （多播路由）并选择转发多播数据包的接口。
   - DVMRP：启用
   - **启用的 DVMRP 接口**列表 （选择转发多播数据包的接口 vlan1 和 vlan2）：
     - 接口：vlan1 ； 阈值：1 ； Metric：1
     - 接口：eth-s1p1 ； 阈值：1 ； Metric：1
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dvmrp enable
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] dvmrp on
NetEye@root-system-vlan1] dvmrp metric 1
NetEye@root-system-vlan1] dvmrp threshold 1
NetEye@root-system-vlan1] exit
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p2] dvmrp on
NetEye@root-system-if-eth-s1p2] dvmrp metric 1
NetEye@root-system-if-eth-s1p2] dvmrp threshold 1
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

8 地址转换

本章介绍 NISG-IPS 的网络地址转换 （Network Address Translation， NAT）特性。章节结构如下：

8.1 概述

网络地址转换可以使私有网络通过较少的公有 IP 地址获得 Internet 接入的能力，同时能够隐藏内网拓扑和真实 IP，可在一定程度上保护内网的安全性。

NISG-IPS 支持的三种地址转换类型：

表 155 地址转换类型

地址转换类型	用途和优点	方向	IP 映射类型	匹配条件
源地址转换（SNAT）	• 使内网用户可以访问外网资源 • 保护内网主机，节省地址空间	内网到外网 (私有 IP -> 公有 IP)	• 一对一 • 多对一 • 多对多	• 方向 （入 / 出口） • 目的 IP • 服务
目的地址转换（DNAT）	• 使公网用户可以访问内网服务器 • 保护内网服务器，提供负载均衡	外网到内网 (公有 IP -> 私有 IP)	• 一对一 • 一对多	• 方向 （入口） • 源 IP
地址映射（MIP）	• 同时实现 SNAT 和 DNAT，但不进行端口转换 • 满足用户特殊需求	双向 (私有 IP <-> 公有 IP)	• 一对一	• 方向 （入 / 出口） • 目的 IP • 服务

在 NISG-IPS 上， NAT 规则的匹配流程如下：

1. 将接收到的数据包与会话表进行匹配。
2. 如果不属于已有会话，与 NAT 规则进行匹配 （MIP 优先级高于 SNAT 和 DNAT）。
3. 根据匹配规则进行地址转换。来自相同会话的后续数据包都根据此规则进行转换。

8.1.1 源地址转换

源地址转换 （SNAT）将数据包的源 IP 地址进行转换，主要用于从被保护的内网访问外网的情况。要使内网用户可以访问 Internet，必须通过 SNAT 将内网用户的私有 IP 地址转换为公有 IP 地址。

根据映射的 IP 地址数量， SNAT 可分为一对一、多对一和多对多三种类型。为了使多个内网用户可以同时上网， SNAT 又支持 NAPT 功能，允许 SNAT 进行 IP 地址转换的同时，进行端口转换。

8.1.1.1 NAPT

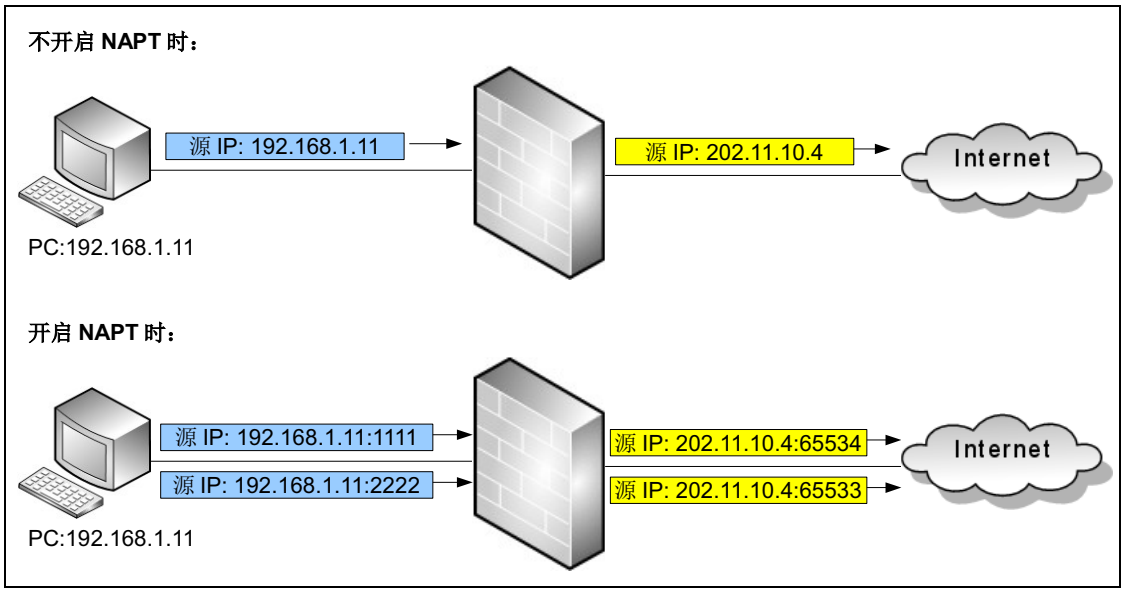
网络地址端口转换 （NAPT），指对网络地址进行转换的同时，对数据包的端口号也进行转换。对于每个转换后的 IP 地址，端口号从 65534 到 1024 降序分配，循环使用。

8.1.1.2 一对一 SNAT

NISG-IPS 可将单个源 IP 地址转换为单个 IP 地址或指定接口的 IP 地址。

- 不开启 NAPT 时， SNAT 不进行端口转换。转换后地址需要等当前会话释放资源（会话空闲时间超过指定的保留时间）后才能再分配给下一个匹配 SNAT 的请求数据包。
- 开启 NAPT 时，SNAT 进行端口转换。匹配 SNAT 的多个请求数据包都将进行源地址转换，同时将被降序分配端口号 （从 65534 到 1024 ，循环使用）。

图 9 一对一 SNAT

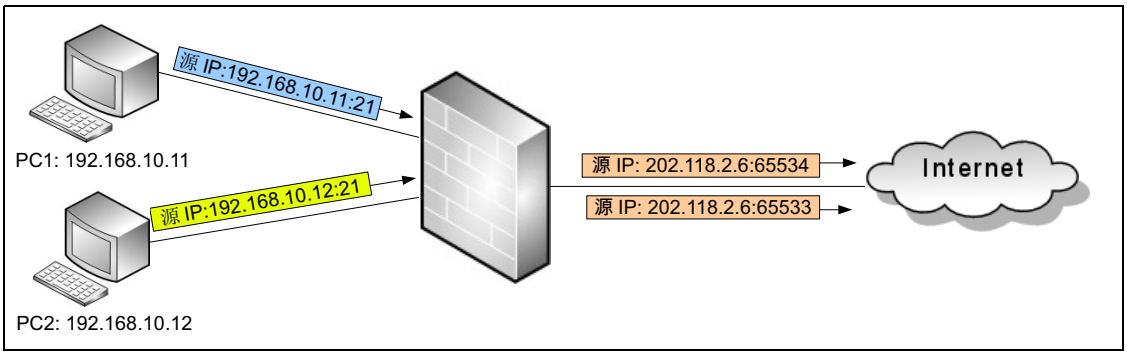


8.1.1.3 多对一 SNAT

NISG-IPS 可将多个源 IP 地址转换为单个 IP 地址或指定接口的 IP 地址，允许多个内网用户通过一个公网 IP 地址访问 Internet。内网用户数量不超过 65535 时，采用此种源地址转换方式。

此类 SNAT 需开启 NAPT，以实现多个源 IP 地址同时转换。

图 10 多对一源地址转换

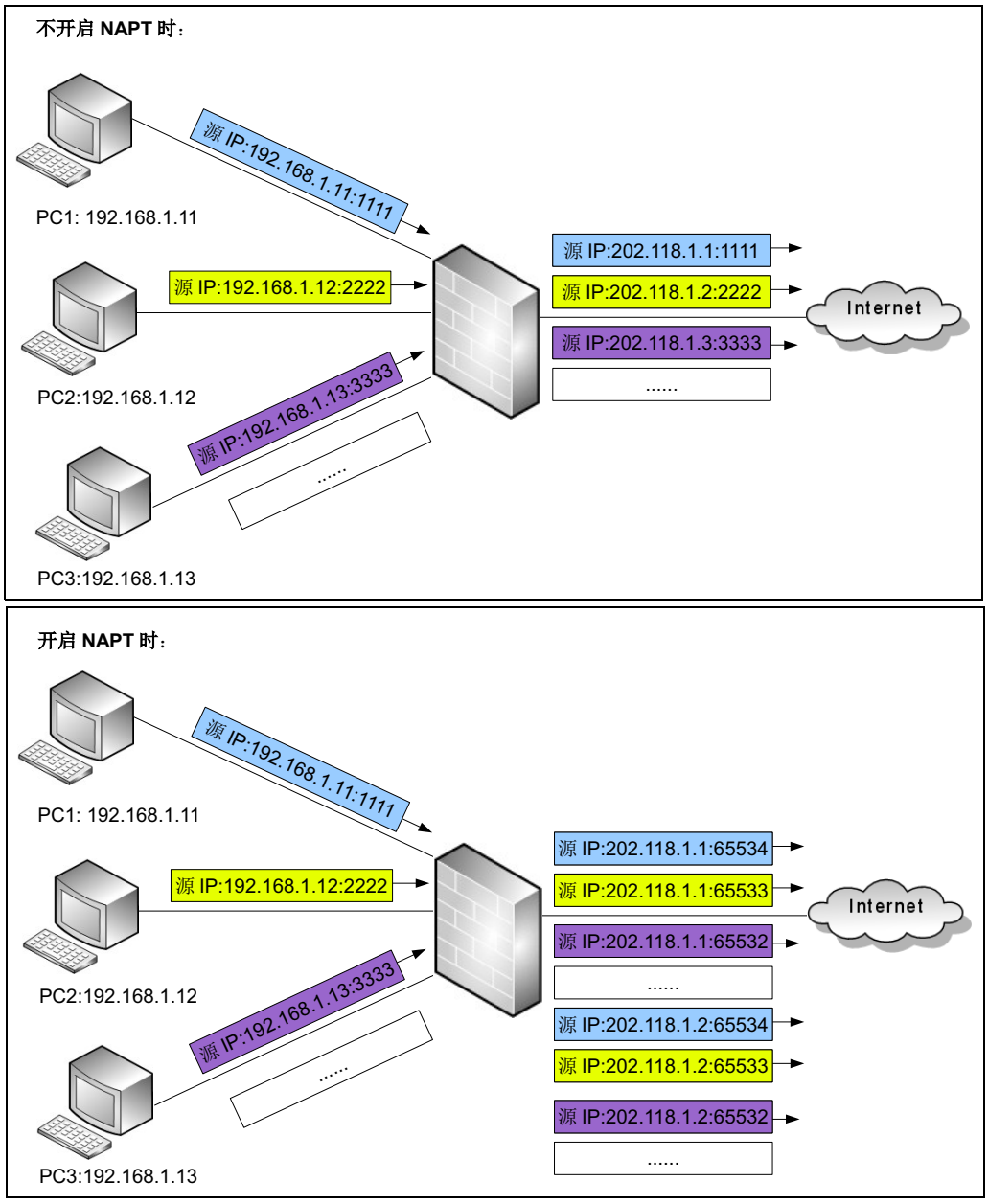


8.1.1.4 多对多 SNAT

NISG-IPS 可将多个源 IP 地址转换为多个 IP 地址，允许多个内网用户通过多个公网 IP 地址访问 Internet。有多个可用公网 IP 地址时，采用此种源地址转换方式。

- 不开启 NAPT 时，SNAT 不进行端口转换，转换后地址依次分配给匹配 SNAT 的请求数据包。
- 开启 NAPT 时， SNAT 进行端口转换。只有当第一个转换后 IP 地址的所有端口号（65534 到 1024 ）都被分配出去，系统才会分配第二个转换后 IP 地址。

图 11 多对多源地址转换



8.1.2 目的地址转换

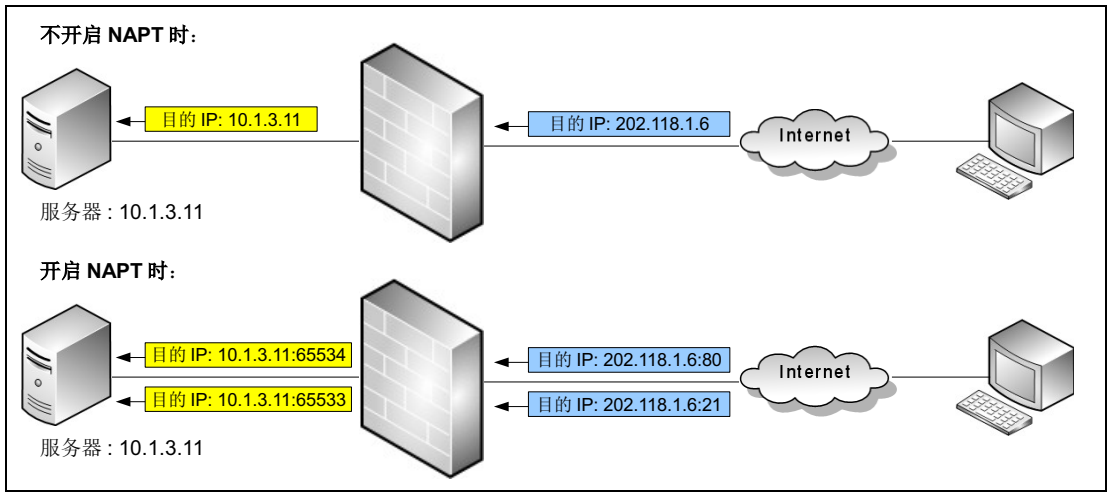
目的地址转换 （DNAT）将数据包的目的 IP 地址进行转换，主要用于从外网访问受保护内网服务器的情况。

根据转换的 IP 地址数量， DNAT 分为一对一和一对多两种类型。DNAT 支持负载均衡和链路探测，以保证内网服务器不间断提供服务。DNS 重写功能可使 DNAT 根据用户访问的域名来判断是否对数据包的目的 IP 地址进行转换。

8.1.2.1 一对一 DNAT

NISG-IPS 可将单个目的 IP 地址转换为单个 IP 地址，通常是将一台内网服务器的私有 IP 地址映射到一个公网 IP 地址上，适用于公网 IP 较多或内网仅部署一台服务器的情况。

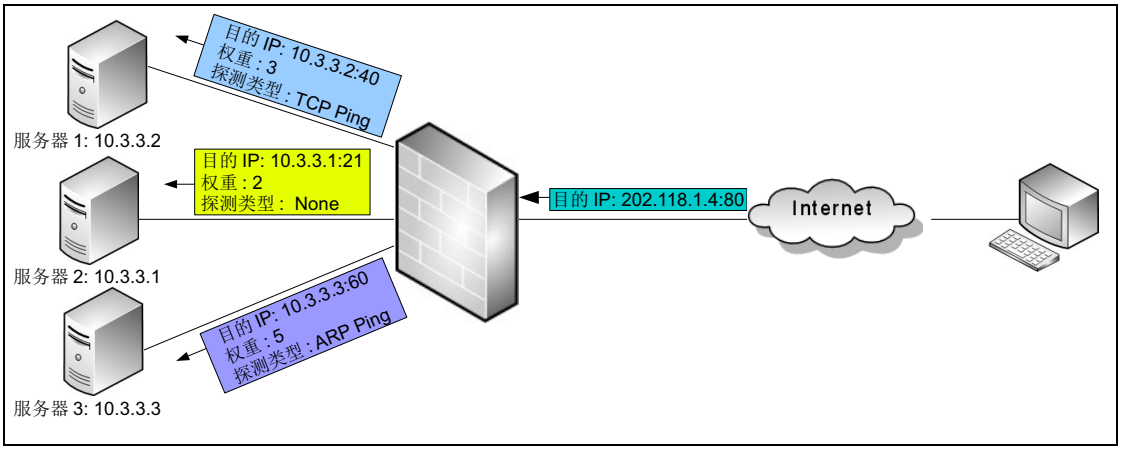
- 不开启 NAPT 时， DNAT 不进行端口转换。转换后地址需要等当前会话释放资源（会话超时）后才能再分配给下一个匹配 DNAT 的请求数据包。
- 开启 NAPT 时，DNAT 进行端口转换。匹配 DNAT 的多个请求数据包都将进行目的地址和端口号转换，端口号指定范围为 65534 到 1024 。



8.1.2.2 一对多 DNAT

NISG-IPS 可将一个目的 IP 地址转换为多个 IP 地址。采用一对多 DNAT，企业可以通过一个公网 IP 地址使多台内网服务器同时对外提供服务。

此类 DNAT 需开启 NAPT，以实现负载均衡。



8.1.2.3 负载均衡和链路探测

基于 DNAT 的负载均衡根据服务器的权重分配会话流量，避免单一服务器负载过重导致的服务不可用。

NISG-IPS 通过链路探测确定其与各服务器之间的链路是否畅通，避免链路故障导致的服务中断。如果与某服务器的链路不通，会话通过其他链路进行通信，同时该服务器的权重变为 0。链路恢复后，服务器权重恢复原值。

NISG-IPS 支持四种链路探测类型：ARP 探测、 TCP 探测、 ICMP 探测和 NS 探测。

关于链路探测类型的更多信息，请参见 5.1.1.2 链路探测。

8.1.2.4 域名转换 （DNS 重写）

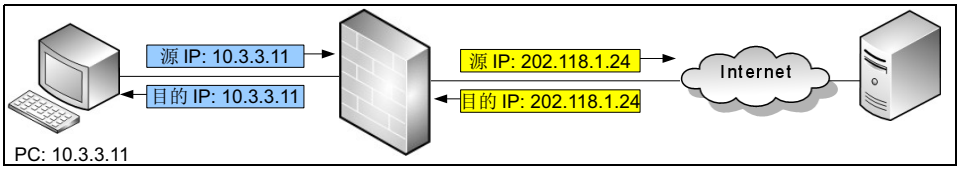
管理员可以在 DNAT 规则中设置要转换的目的 IP 地址对应的域名。设置域名后， NISG-IPS 在收到来自 DNS 服务器的数据包后，会将域名对应的数据包的目的 IP 地址与所有 DNAT 规则匹配。如果发现匹配规则， NISG-IPS 将把域名对应的外部 IP 地址转换为 DNAT 规则中指定的内部 IP 地址。

8.1.3 地址映射

地址映射 （Mapped IP， MIP）是指一个内网 IP 地址与一个公网 IP 地址一对一的映射，不涉及端口转换。地址映射具有双向性，通常用于既有源地址转换需求又有目的地址转换需求的情况。

8.1.3.1 一对一 MIP

MIP 映射通过设置主机 IP 和映射 IP，将主机 （通常为内网服务器）的私有 IP 和公有 IP 一对一映射，同时实现外网对内网主机的访问和内网主机对外网的访问。



8.1.3.2 域名转换 （DNS 重写）

可以在 MIP 规则中设置要转换的目的 IP 地址对应的域名。设置域名后， NISG-IPS 在收到来自 DNS 服务器的数据包后，会将域名对应的数据包的目的 IP 地址与所有 MIP 规则匹配。如果发现匹配规则， NISG-IPS 将把域名对应的外部 IP 地址转换为 MIP 规则中的内部 IP 地址。

8.2 基本配置步骤

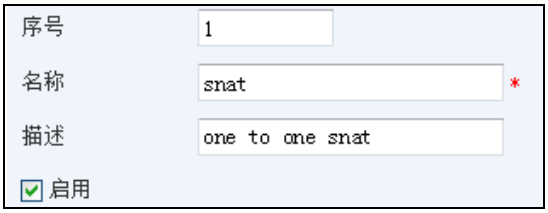
本节描述 NAT 的基本配置步骤：

8.2.1 创建 SNAT 规则

8.2.1.1 创建规则

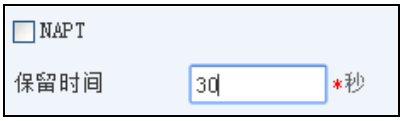
1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**创建新规则。

   设置规则名称、描述及序号 （优先级），启用或禁用规则。



8.2.1.2 一对一 SNAT （启用 / 禁用 NAPT）

1. 勾选 **NAPT**，或取消勾选 **NAPT** 并设置保留时间。



2. 添加源 IP 地址。

3. 添加转换后 IP 或指定转换后接口。

8.2.1.3 多对一 SNAT（启用 NAPT）

1. 勾选 **NAPT**。
2. 在**源 IP 地址列表**中添加多个 IP 地址。
3. 从**接口**下拉框中选择一个接口或者添加一个 IP 地址作为转换后 IP 地址。

8.2.1.4 多对多 SNAT（启用 / 禁用 NAPT）

1. 勾选 **NAPT**，或取消勾选 **NAPT** 并设置保留时间。
2. 在**源 IP 地址列表**中添加多个 IP 地址。
3. 在**转换后 IP 地址 / 接口**区域的列表中添加多个 IP 地址作为转换后 IP 地址。

8.2.1.5 高级设置

在**高级设置**区域，输入数据包匹配的条件。只有所有条件都匹配的数据包才会进行源地址转换。

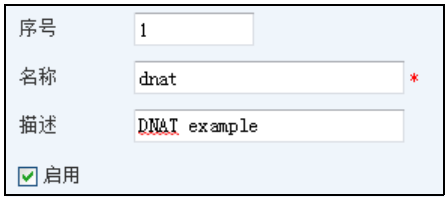
表 156 SNAT 规则命令

policy snat *policy_name*	添加 SNAT 规则。
policy snat *policy_name* append	添加源 / 转换后 IP 地址。
policy snat *policy_name* **description**	添加规则的描述。
policy snat *policy_name* **{enable | disable}**	启用或禁用规则。
policy snat *policy_name* **matching**	添加数据包匹配条件。
policy snat *policy_name* **number** *pri*	更改规则优先级。
show policy snat [*policy_name*]	显示规则信息。
unset policy snat [*policy_name*]	删除规则。
unset policy snat *policy_name* **matching**	删除数据包匹配条件。

8.2.2 创建 DNAT 规则

8.2.2.1 创建规则

1. 选择**网络** > **地址转换** > **目的地址转换**。
2. 点击**新建**创建规则。设置规则名称、描述及序号 （优先级），启用或禁用规则。

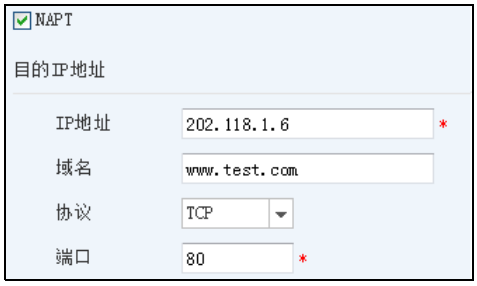


8.2.2.2 一对一 DNAT （不启用 NAPT）

1. 取消勾选 **NAPT**。
2. 输入目的 IP 地址 （和域名）和转换后 IP 地址。

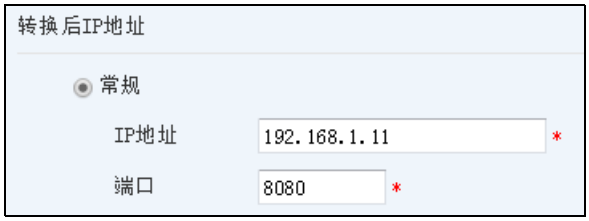
8.2.2.3 一对一 DNAT （启用 NAPT）

1. 勾选 **NAPT**。
2. 在**目的 IP 地址**区域，添加目的 IP 地址 （和域名），设置协议类型和端口号。



提示：为了方便用户访问，转换前端口一般设为知名端口如 80，此时建议开启攻击防御和 IPS 功能。

3. 在**转换后 IP 地址**区域，选择**常规**，输入 IP 地址和对应端口。



8.2.2.4 一对多 DNAT （启用 NAPT）

1. 勾选 **NAPT**。
2. 在**目的 IP 地址**区域，添加目的 IP 地址 （和域名），设置端口号和协议类型。
3. 在**转换后 IP 地址**区域，选择**负载均衡**，添加负载均衡策略 （IP 地址、端口、权重及探测方式）至列表。

8.2.2.5 高级设置

在**高级设置**区域，输入数据包匹配的条件。只有所有条件都匹配的数据包才会进行目的地址转换。

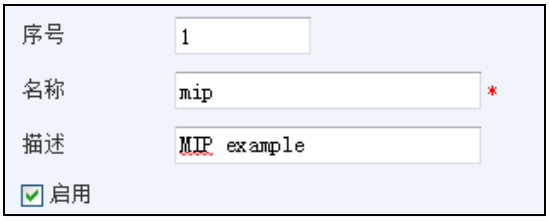
表 157 DNAT 规则命令

policy dnat *policy_name*	添加 DNAT 规则。
policy dnat *policy_name* **load-balancing**	添加负载均衡规则。
policy dnat *policy_name* **description**	添加规则描述。
policy dnat *policy_name* {**enable** | **disable**}	启用或禁用规则。
policy dnat *policy_name* **matching**	添加数据包匹配条件。
policy dnat *policy_name* **number** *pri*	更改规则优先级。
show policy dnat [*policy_name*]	显示规则信息。
unset policy dnat [*policy_name*]	删除规则。
unset policy dnat *policy_name* **matching**	删除数据包匹配条件。

8.2.3 创建 MIP 规则

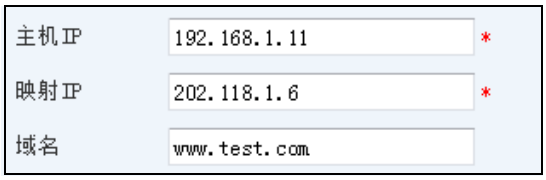
8.2.3.1 创建规则

1. 选择**网络** > **地址转换** > **地址映射**。
2. 点击**新建**创建规则。设置 MIP 规则名称、描述及序号（优先级），启用或禁用规则。



8.2.3.2 一对一映射

输入主机 IP 和对应的转换后 IP （和域名）。主机 IP 是内网主机的 IP 地址，映射 IP 是可用的公网 IP 地址。



8.2.3.3 高级设置

在**高级设置**区域，输入数据包匹配的条件。只有所有条件都匹配的数据包才会被转换。

表 158 MIP 规则命令

policy mip *policy_name*	添加 MIP 规则。
policy mip *policy_name* **description**	添加规则描述。
policy mip *policy_name* {**enable** | **disable**}	启用或禁用规则。
policy mip *policy_name* **matching**	添加数据包匹配条件。
policy mip *policy_name* **number** *pri*	更改规则优先级。
show policy mip [*policy_name*]	显示 MIP 规则信息。
unset policy mip [*policy_name*]	删除规则。
unset policy mip *policy_name* **matching**	删除数据包匹配条件。

8.3 配置参数说明

8.3.1 源地址转换规则参数

表 159 源地址转换规则配置信息

参数	说明
序号	源地址转换规则的优先级，取值范围为 1-80000。序号越小，优先级越高。
名称	源地址转换规则名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
描述	源地址转换规则描述信息。长度 0-255 个字节， UTF-8 字符。不能包含以下字符：？" ' \ < > &
启用	启用或禁用源地址转换规则。
NAPT	启用或禁用网络地址端口转换功能。（多对一 SNAT 必须启用 NAPT。） • 启用 NAPT， IP 地址和端口号都会进行转换。（转换后端口号不可以手动设置） • 不启用 NAPT，只对 IP 地址进行转换，端口号保持不变。
保留时间	指映射关系对应的所有会话都断开后，映射关系保持的时间。 取值范围为 30-99999999 秒。未启用 NAPT 时必须设置保留时间。
源 IP 地址	内网用户访问公网所使用的内网主机 IP 地址。 最多可以配置 32 个源 IP 地址条目。
转换后 IP 地址 / 接口	内网用户访问公网所使用的公网 IP 地址，可以是以下任一类型： • **接口**：勾选复选框，选择一个连接 Internet 的三层接口。 NISG-IPS 会将内网主机 IP 地址转换为此接口的 IP 地址。 • **IP 地址**：添加指定 IP 地址。 NISG-IPS 会将内网主机 IP 地址转换为指定 IP 地址。最多可以配置 8 个转换后 IP 地址条目。
高级设置	设置匹配 SNAT 规则的条件。匹配条件包括： • **方向**：包括 NISG-IPS 接收数据包的入口接口和转发数据包的出口接口。入口接口应该是连接内网的一个三层接口，出口接口应该是连接外网的一个三层接口。 • **目的 IP 地址**：内网用户要访问的公网 IP 地址。最多可以配置 32 个目的 IP 地址条目。 • **服务**：数据包使用的传输层服务，可以是对象、对象组以及自定义协议 (ICMP、ICMPv6、TCP、UDP 和 Other)。TCP 和 UDP 协议的目的端口号范围为 1-65535。其它协议号范围为 1-255。 管理员最多可以配置 32 个服务条目。

8.3.2 目的地址转换规则参数

表 160 目的地址转换规则配置信息

参数	说明
序号	目的地址转换规则的优先级。取值范围为 1-80000。数值越小，优先级越高。
名称	目的地址转换规则名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
描述	目的地址转换规则描述信息。长度 0-255 个字节， UTF-8 字符。不能包含以下字符：？" ' \ < > &
启用	启用或禁用目的地址转换规则。
NAPT	启用或禁用网络地址端口转换功能。（一对多 DNAT 必须启用 NAPT。） • 如果启用 NAPT，地址和端口号都会进行转换。（可以手动设置转换后端口号。） • 如果不启用 NAPT，只对地址进行转换，端口号保持不变。
目的 IP 地址	允许外网用户访问的内网服务器的公网 IP 地址。 管理员可以配置以下参数： • **IP 地址**：服务器的公网 IP 地址。 • **域名**：服务器对外公布的域名。域名长度为 2-255 字节。 • **协议**：数据包所使用的协议，有 TCP 和 UDP 两种。 • **端口**：进行端口转换之前的原始目的端口。 1-65535。 如果启用了网络地址端口转换，则必须设置协议和端口。
转换后 IP 地址	内网服务器对外公布的公网 IP 地址。可设置为以下任一类型： • **常规**：设置一个转换后 IP 地址及端口。适用于仅一台内网服务器提供服务的情况。 • **负载均衡**：设置多个转换后 IP 地址以及负载均衡策略。适用于多台内网服务器同时提供服务的情况。
负载均衡	管理员需设置以下负载均衡和链路探测参数： • **IP 地址**：要探测的内网服务器的私有 IP 地址。 • **目的端口**：服务器提供服务的真实端口，和私有 IP 地址对应。 • **权重**：服务器所能分到的会话比例。取值范围为 1-255。 • **探测类型**：IP 探测的方式，包括 ARP Ping、 TCP Ping、 (ICMP) Ping 和 NS Ping。 None 表示不进行探测。 只有探测 IP 地址设置为 IPv6 地址时，才可以选择 NS Ping。 • **探测端口**：使用 TCP Ping 时，所探测的服务器的端口。端口的取值范围为 1-65535。 探测端口可以是转换后目的端口，也可以是服务器上开放的其他端口。 • **探测周期**：两次链路探测之间的时间间隔，取值范围为 1-30000 秒。 • **探测重试次数**：NISG-IPS 探测 IP 地址时允许连续失败的最大次数。取值范围为 1-999 次。 如果探测失败次数达到了此阈值，但是在探测周期内未得到回复，则认为链路不通。 管理员最多可以为一条目的地址转换规则配置 8 条负载均衡策略。
高级设置	设置数据包匹配 DNAT 规则的条件。匹配条件包括： • **方向**：NISG-IPS 接收数据包的入口接口，必须是连接 Internet 的一个三层接口。 • **源 IP 地址**：访问内网服务器的用户所使用的公网 IP 地址。最多可以配置 32 个源 IP 地址条目。

8.3.3 地址映射规则参数

表 161 地址映射规则配置信息

参数	说明
序号	地址映射规则的优先级。取值范围为 1-80000。数值越小，优先级越高。
名称	地址映射规则名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
描述	地址映射规则的描述信息。长度 0-255 个字节，UTF-8 字符。不能包含以下字符：？" ' \ < > &
启用	启用或禁用地址映射规则。
主机 IP	内网主机的私有 IP 地址。
映射 IP	与内网主机的私有 IP 地址相对应的公网 IP 地址。
域名	与映射 IP 地址相对应的域名，长度为 2-255 字节。 当需要应用 DNS 重写时，管理员可以输入域名。
高级设置	设置匹配 MIP 规则的条件。匹配条件包括： • **方向**：入口接口应该设为连接内网的一个三层接口，出口接口应该设为连接外网的一个三层接口。 • **目的 IP 地址**：用户要访问的服务器的 IP 地址。 最多可以配置 32 个目的 IP 地址条目。 • **服务**：数据包使用的传输层服务，可以是对象、对象组以及自定义协议。自定义协议包括 ICMP、ICMPv6、TCP、UDP 和 Other。TCP 和 UDP 协议的目的端口号范围为 1-65535。其它协议号范围为 1-255。 管理员最多可以配置 32 个服务条目。

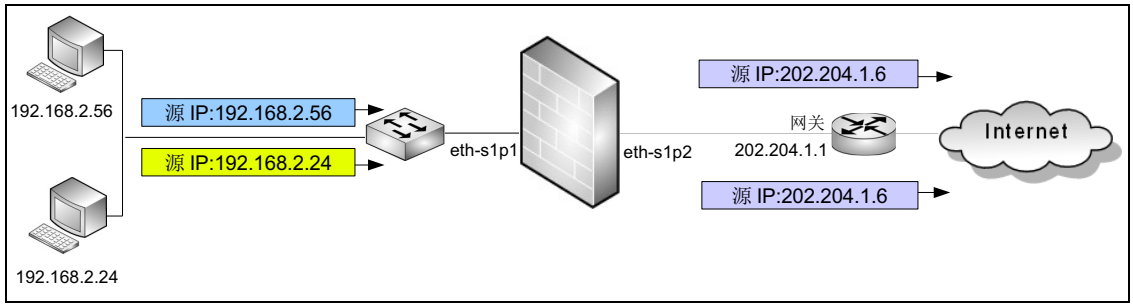
8.4 NAT 范例

8.4.1 范例：多对一 SNAT （启用 NAPT）

基本需求

- 内网用户可以访问 Internet 资源。
- 隐藏内部网络拓扑和主机真实 IP 地址。
- 公网 IP 地址资源有限，需要使多个内网用户可以使用相同公网 IP 访问外网。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置路由
- 配置访问策略
- 配置 SNAT 规则
- 开启 NAT 日志记录功能
- 验证 SNAT 结果

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 点击接口对应的，设置接口 IP 地址。
   - eth-s1p1：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.2.1/24
   - eth-s1p2：
     - 模式：三层
     - IP 地址：（静态 IP） 202.204.1.6/24
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.204.1.6 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

配置路由

1. 选择**网络 > 路由 > 缺省路由**。
2. 点击缺省路由条目对应的，修改网关地址为 202.204.1.1。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route default gateway 202.204.1.1 1
NetEye@root-system] exit
NetEye@root> save config
```

配置访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建一条访问策略，允许来自内网网段 192.168.2.0/24 的访问流量。
   - 名称：policy1
   - 源 IP 地址：192.168.2.0/24
   - 目的 IP 地址：任意
   - 服务：任意
   - 动作：允许
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access policy1 any 192.168.2.0/24 any any any any permit enable 1
NetEye@root-system] exit
NetEye@root> save config
```

配置 SNAT 规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建一条 SNAT 规则，使内网用户能够访问外网。
   - 名称：snat1
   - 启用：勾选
   - NAPT：勾选
   - 源 IP 地址：192.168.2.0/24
   - 转换后接口：eth-sp1p2
   - 入口接口：eth-s1p1
   - 出口接口：eth-s1p2
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy snat snat1 netmask 192.168.2.0 255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] policy snat snat1 matching input-interface eth-s1p1
NetEye@root-system] policy snat snat1 matching output-interface eth-s1p2
NetEye@root-system] policy snat snat1 matching dip any
```

```
NetEye@root-system] exit
NetEye@root> save config
```

开启 NAT 日志记录功能

1. 选择**系统 > 日志配置 > 报警配置**。
2. 点击缺省本地报警策略internal对应的图标，开启Informational级别、NAT类型的报警策略，为 NAT 事件生成本地报警日志。

提示：日志存储介质为硬盘时才可以生成本地报警日志。

---

3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] alert-config local-syslog internal level
Informational type NAT
NetEye@root-system] exit
NetEye@root> save config
```

验证 SNAT 结果

1. 在内网主机上访问外网服务器。
2. 选择**监控 > 地址转换**，查看当前的源地址转换会话条目。

提示：地址转换监控界面只显示当前活动的 NAT 会话条目，当某 NAT 会话断开连接或连接超时时，监控列表中将不再显示该 NAT 条目。

---

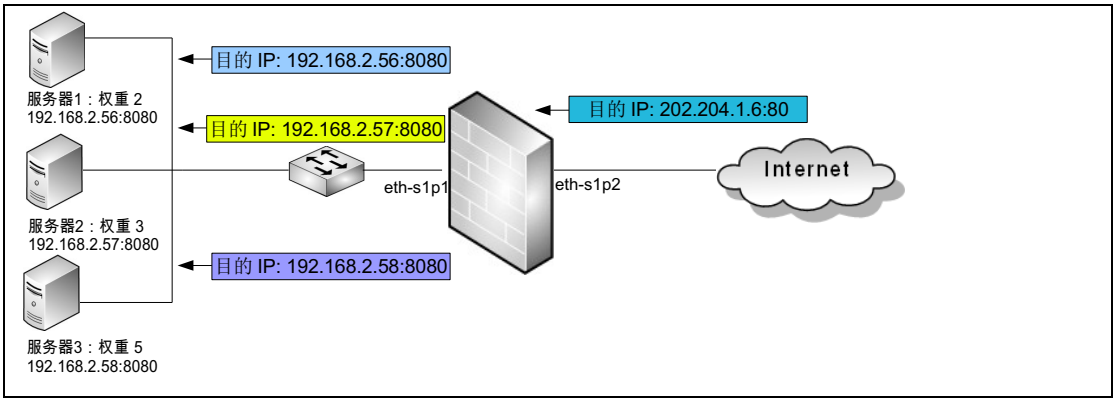
3. 选择**监控 > 报警 / 日志 > 系统日志**。
   a. 点击表头**类型**前面的图标，在弹出的对话框中选择 NAT 类型。
   b. 点击**是**，筛选出 NAT 日志信息。

8.4.2 范例：一对多 DNAT （启用 NAPT）

基本需求

- 允许公网用户访问内网服务器。
- 隐藏内部网络拓扑和服务器真实 IP 地址，降低内网服务器被直接攻击的可能性。
- 为服务器提供负载均衡功能，有效防止因服务器过载而导致服务失效的情况。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置访问策略
- 配置 DNAT 规则
- 开启 NAT 日志记录功能
- 验证 DNAT 结果

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 点击接口对应的，设置接口 IP 地址。
   - eth-s1p1：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.2.1/24
   - eth-s1p2：
     - 模式：三层
     - IP 地址：（静态 IP） 202.204.1.6/24
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.204.1.6 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

配置访问策略

1. 选择**防火墙 > 访问策略**。
2. 点击**新建**，创建一条访问策略，允许任意用户访问 192.168.2.0/24 网段的服务器。
   - 名称：policy1
   - 源 IP 地址：任意
   - 目的 IP 地址：192.168.2.0/24
   - 服务：服务 =TCP ； 源端口 =1-65535 ； 目的端口 =8080
   - 动作：允许
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access policy1 any any any 192.168.2.0/24 tcp 1-65535 8080 any permit enable 1
NetEye@root-system] exit
NetEye@root> save config
```

配置 DNAT 规则

1. 选择**网络** > **地址转换** > **目的地址转换**。
2. 点击**新建**，创建一条 DNAT 规则，使外网用户能够访问内网服务器。
   - 名称：dnat2
   - 启用：勾选
   - NAPT：勾选
   - 目的 IP 地址：
     - IP 地址：202.204.1.6
     - 协议 TCP
     - 端口：80
   - 转换后 IP 地址：（负载均衡）
     - IP 地址 =192.168.2.56； 端口 =8080； 权重 =2； 探测 =Ping:8080/3s/3
     - IP 地址 =192.168.2.57； 端口 =8080； 权重 =3； 探测 =Ping:8080/3s/3
     - IP 地址 =192.168.2.58； 端口 =8080； 权重 =5； 探测 =Ping:8080/3s/3
   - 入口接口：eth-s1p2
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy dnat dnat2 load-balancing 202.204.1.6 tcp 80 192.168.2.56 8080 2 ip-track tcpping port 8080 3 3 enable
NetEye@root-system] policy dnat dnat2 matching load-balancing 192.168.2.57 8080 3 ip-track tcpping port 8080 3 3
NetEye@root-system] policy dnat dnat2 matching load-balancing 192.168.2.58 8080 5 ip-track tcpping port 8080 3 3
NetEye@root-system] policy dnat dnat2 matching sip any
NetEye@root-system] policy dnat dnat2 matching input-interface eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

开启 NAT 日志记录功能

1. 选择**系统 > 日志配置 > 报警配置**。
2. 点击缺省本地报警策略internal对应的图标，开启Informational级别、NAT类型的报警策略，为 NAT 事件生成本地报警日志。

提示：日志存储介质为硬盘时才可以生成本地报警日志。

---

3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] alert-config local-syslog internal level
Informational type NAT
NetEye@root-system] exit
NetEye@root> save config
```

验证 DNAT 结果

1. 在外网主机上访问内网服务器。
2. 选择**监控 > 地址转换**，查看当前的源地址转换会话条目。

提示：地址转换监控界面只显示当前活动的 NAT 会话条目，当某 NAT 会话断开连接或连接超时时，监控列表中将不再显示该 NAT 条目。

---

3. 选择**监控 > 报警 / 日志 > 系统日志**。
   a. 点击表头**类型**前面的图标，在弹出的对话框中选择 NAT 类型。
   b. 点击**是**，筛选出 NAT 日志信息。

8.4.3 范例：MIP 映射

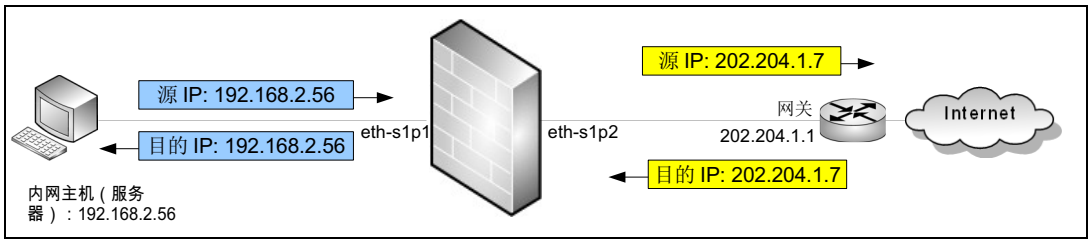
基本需求

- 允许内网主机作为服务器对外提供服务的同时可以访问公网资源。
- 隐藏内部网络拓扑和真实 IP 地址，保护内网安全，降低内网主机被直接攻击的可能性。

在本范例中：

1. 当内网主机访问外网时， NISG-IPS 将数据包的源 IP 地址 192.168.2.56 转换为 202.204.1.7。
2. 当外网主机访问内网主机服务时，NISG-IPS将数据包的目的IP地址202.204.1.7转换为192.168.2.56。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置路由
- 配置访问策略
- 配置 MIP 规则
- 开启 NAT 日志记录功能
- 验证 MIP 结果

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 点击接口对应的，设置接口 IP 地址。
   - eth-s1p1：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.2.1/24
   - eth-s1p2：
     - 模式：三层
     - IP 地址：（静态 IP） 202.204.1.6/24
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.204.1.6 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

配置路由

1. 选择**网络 > 路由 > 缺省路由**。
2. 点击缺省路由条目对应的，修改网关地址为 202.204.1.1。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route default gateway 202.204.1.1 1
NetEye@root-system] exit
NetEye@root> save config
```

配置访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建两条访问策略，允许内网主机被外网访问，同时允许其访问外网。
   - out：允许内网主机访问外网。
     - 源 IP 地址：192.168.2.56
     - 目的 IP 地址：任意
     - 服务：任意
     - 动作：允许
   - in：允许内网主机被外网访问。
     - 源 IP 地址：任意
     - 目的 IP 地址：192.168.2.56
     - 服务：服务 =TCP ； 源端口 =1-65535 ； 目的端口 =8080
     - 动作：允许
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access in any any any 192.168.2.56 tcp 1-65535 8080 any permit enable 1
NetEye@root-system] policy access out any 192.168.2.56 any any any any permit enable 2
NetEye@root-system] exit
NetEye@root> save config
```

配置 MIP 规则

1. 选择**网络** > **地址转换** > **地址映射**。
2. 点击**新建**，创建一条 MIP 规则：
   - 名称：mip1
   - 启用：勾选
   - 主机 IP：192.168.2.56
   - 映射 IP：202.204.1.7
   - 入口接口：eth-s1p1
   - 出口接口：eth-s1p2
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy mip mip1 192.168.2.56 202.204.1.7 enable
NetEye@root-system] policy mip mip1 matching input-interface eth-s1p1
NetEye@root-system] policy mip mip1 matching output-interface eth-s1p2
NetEye@root-system] policy mip mip1 matching dip any
NetEye@root-system] exit
NetEye@root> save config
```

开启 NAT 日志记录功能

1. 选择**系统 > 日志配置 > 报警配置**。
2. 点击缺省本地报警策略internal对应的图标，开启Informational级别、NAT类型的报警策略，为 NAT 事件生成本地报警日志。

提示：日志存储介质为硬盘时才可以生成本地报警日志。

3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] alert-config local-syslog internal level
Informational type NAT
NetEye@root-system] exit
NetEye@root> save config
```

验证 MIP 结果

1. 在内网主机上访问外网。
2. 选择**监控 > 地址转换**，查看当前的源地址转换会话条目。

提示：地址转换监控界面只显示当前活动的 NAT 会话条目，当某 NAT 会话断开连接或连接超时时，监控列表中将不再显示该 NAT 条目。

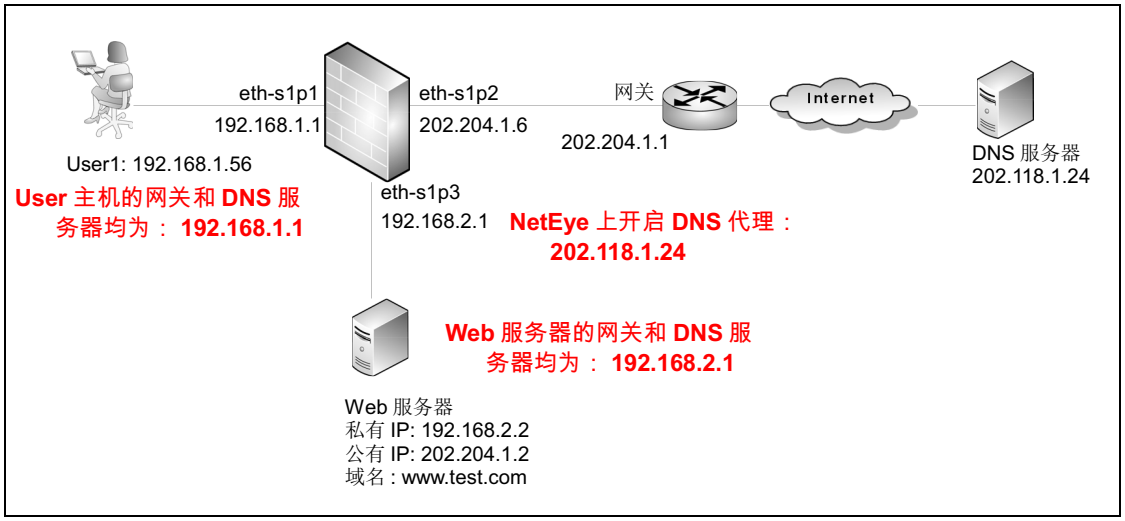
3. 选择**监控 > 报警 / 日志 > 系统日志**。
   a. 点击表头**类型**前面的图标，在弹出的对话框中选择 NAT 类型。
   b. 点击**是**，筛选出 NAT 日志信息。
4. 在外网主机上访问内网主机上的服务。
5. 选择**监控 > 地址转换**，查看当前的源地址转换会话条目。
6. 选择**监控 > 报警 / 日志 > 系统日志**。查看 NAT 日志信息。

8.4.4 范例：DNAT 和 DNS 代理

基本需求

- 使内网服务器在提供对外服务的同时允许内网用户通过其域名进行访问。（内网用户使用的 DNS 服务器在外网；内网主机和 Web 服务器处于不同的子网。）
- 隐藏内部网络拓扑和服务器真实 IP 地址，降低内网服务器被直接攻击的可能性。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置路由
- 配置访问策略
- 配置 DNS 代理
- 配置 DNAT 规则
- 开启 NAT 日志记录功能
- 验证 DNAT 结果

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 点击接口对应的，设置接口 IP 地址。
   - eth-s1p1：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - IP 地址：（静态 IP） 202.204.1.6/24
   - eth-s1p3：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.2.1/24
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.204.1.6 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet eth-s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

配置路由

1. 选择**网络 > 路由 > 缺省路由**。
2. 点击缺省路由条目对应的，修改网关地址为 202.204.1.1。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route default gateway 202.204.1.1 1
NetEye@root-system] exit
NetEye@root> save config
```

配置访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建一条访问策略，允许内网主机所在网段到内网服务器（192.168.2.2）的访问。
   - 名称：DNSproxy
   - 源 IP 地址：192.168.1.0/24
   - 目的 IP 地址：192.168.2.2
   - 服务：服务 =TCP ； 源端口 =1-65535 ； 目的端口 =8080
   - 动作：允许
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access DNSproxy any 192.168.1.0/24 any
192.168.2.2 tcp 1-65535 80 any permit enable
NetEye@root-system] exit
NetEye@root> save config
```

配置 DNS 代理

1. 选择**网络** > **DNS** > **DNS 代理**。
2. 点击**新建**，设置 DNS 代理。
   - 域名：www.test.com
   - 接口：Any
   - 首选 DNS：202.118.1.24
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] dns server-select www.test.com output-interface
any primary 202.118.1.24
NetEye@root-system] exit
NetEye@root> save config
```

配置 DNAT 规则

1. 选择**网络** > **地址转换** > **目的地址转换**。
2. 点击**新建**，创建 DNAT 规则。
   - 名称：dnat1
   - 启用：勾选
   - NAPT：勾选
   - 目的 IP 地址：
     - IP 地址：202.204.1.2
     - 协议：TCP
     - 端口：80
   - 转换后 IP 地址：IP 地址 =192.168.2.2 ； 端口 =8080
   - 入口接口：eth-s1p1
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy dnat dnat1 202.204.1.2 tcp 80 192.168.2.2 8080 enable
NetEye@root-system] policy dnat dnat1 matching input-interface eth-s1p1
NetEye@root-system] exit
NetEye@root> save config
```

开启 NAT 日志记录功能

1. 选择**系统** > **日志配置** > **报警配置**。
2. 点击缺省本地报警策略internal对应的 图标，开启Informational级别、NAT类型的报警策略，为 NAT 事件生成本地报警日志。

提示：日志存储介质为硬盘时才可以生成本地报警日志。

---

3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] alert-config local-syslog internal level Informational type NAT
NetEye@root-system] exit
NetEye@root> save config
```

验证 DNAT 结果

1. 在内网主机上访问内网服务器的域名。
2. 选择**监控 > 地址转换**，查看当前的源地址转换会话条目。

提示：地址转换监控界面只显示当前活动的 NAT 会话条目，当某 NAT 会话断开连接或连接超时时，监控列表中将不再显示该 NAT 条目。

---

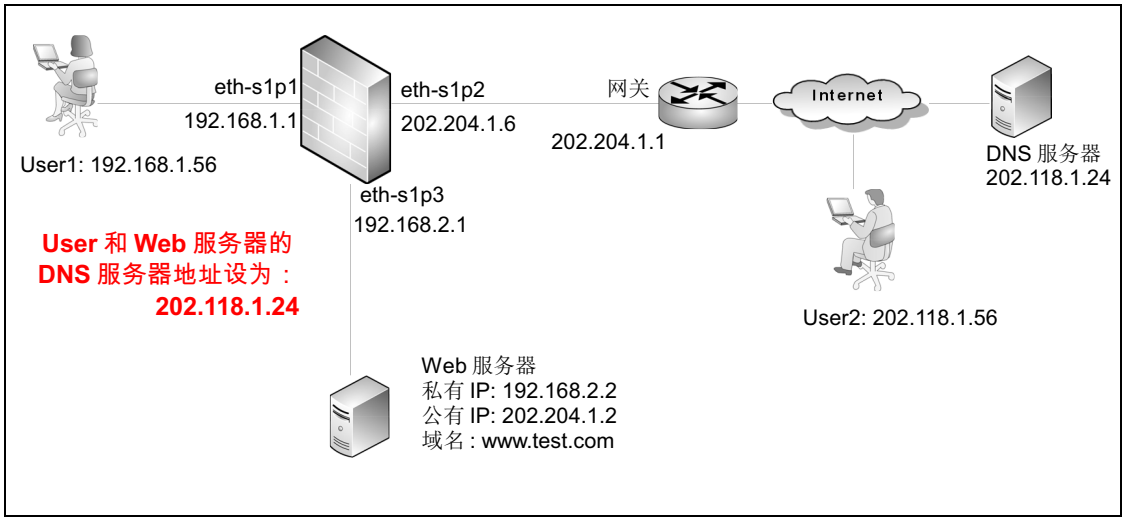
3. 选择**监控 > 报警 / 日志 > 系统日志**。
   a. 点击表头**类型**前面的 图标，在弹出的对话框中选择 NAT 类型。
   b. 点击**是**，筛选出 NAT 日志信息。

8.4.5 范例：SNAT， DNAT 和 DNS 重写

基本需求

- 使内网服务器同时允许内网用户和外网用户通过其域名进行访问 （用户使用的 DNS 服务器在外网）。
- 隐藏内部网络拓扑和服务器真实 IP 地址，降低内网服务器被直接攻击的可能性。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置路由
- 配置访问策略
- 配置 SNAT 规则
- 配置 DNAT 规则
- 开启 NAT 日志记录功能
- 验证 SNAT， DNAT 和 DNS 重写结果

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 点击接口对应的，设置接口 IP 地址。
   - eth-s1p1：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - IP 地址：（静态 IP） 202.204.1.6/24
   - eth-s1p3：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.2.1/24
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.204.1.6 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet eth-s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

配置路由

1. 选择**网络 > 路由 > 缺省路由**。
2. 点击缺省路由条目对应的，修改网关地址为 202.204.1.1。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route default gateway 202.204.1.1 1
NetEye@root-system] exit
NetEye@root> save config
```

配置访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建两条访问策略：
   - policy1：允许内网用户访问外网 （包括 DNS 服务器）；
   - policy2：允许任意地址到内网服务器 （192.168.2.2）的访问。
   - policy1：允许内网用户访问外网 （包括 DNS 服务器）。
     - 源 IP 地址：192.168.1.0/24
     - 目的 IP 地址：任意
     - 服务：任意
     - 动作：允许
   - policy2：允许任意地址到内网服务器 （192.168.2.2）的访问。
     - 源 IP 地址：任意
     - 目的 IP 地址：192.168.2.2
     - 服务：服务 =TCP ； 源端口 =1-65535 ； 目的端口 =8080
     - 动作：允许
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access policy1 any 192.168.1.0/24 any any
any any permit enable 1
NetEye@root-system] policy access policy2 any any any 192.168.2.2 tcp
1-65535 8080 any permit enable 1
NetEye@root-system] exit
NetEye@root> save config
```

配置 SNAT 规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建一条 SNAT 规则，使内网用户可以访问外网。
   - 名称：snat1
   - 启用：勾选
   - NAPT：勾选
   - 源 IP 地址：192.168.1.0/24
   - 转换后接口：eth-sp1p2

- 入口接口：eth-s1p1
- 出口接口：eth-s1p2

3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy snat snat1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] policy snat snat1 matching input-interface eth-
s1p1
NetEye@root-system] policy snat snat1 matching output-interface eth-
s1p2
NetEye@root-system] policy snat snat1 matching dip any
NetEye@root-system] exit
NetEye@root> save config
```

配置 DNAT 规则

1. 选择**网络** > **地址转换** > **目的地址转换**。
2. 点击**新建**创建两条 DNAT 规则：
   - dnat1：将用户访问的服务器域名转换为对应的内网 IP 地址。
   - dnat2：将用户访问的服务器公网 IP 转换为对应的内网 IP 地址。
   - dnat1：将用户访问的服务器域名转换为对应的内网 IP 地址。
     - 序号：1
     - 启用：勾选
     - NAPT：勾选
     - 目的 IP 地址：
       - IP 地址：202.204.1.2
       - 域名：www.test.com
       - 服务：TCP
       - 端口：80
     - 转换后 IP 地址：IP 地址 =192.168.2.2 ； 端口 =8080
     - 入口接口：eth-s1p2
   - dnat2：将用户访问的服务器公网 IP 转换为对应的内网 IP 地址。
     - 序号：2
     - 启用：勾选
     - NAPT：勾选
     - 目的 IP 地址：
       - IP 地址：202.204.1.2

- 服务：TCP
- 端口：80

- 转换后 IP 地址：IP 地址 =192.168.2.2 ； 端口 =8080
- 入口接口：eth-s1p1

3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy dnat dnat1 202.204.1.2 domain www.test.com tcp 80 192.168.2.2 8080 enable 1
NetEye@root-system] policy dnat dnat1 matching input-interface eth-s1p2
NetEye@root-system] policy dnat dnat2 202.204.1.2 tcp 80 192.168.2.2 8080 enable 2
NetEye@root-system] policy dnat dnat2 matching input-interface eth-s1p1
NetEye@root-system] exit
NetEye@root> save config
```

开启 NAT 日志记录功能

1. 选择**系统 > 日志配置 > 报警配置**。
2. 点击缺省本地报警策略internal对应的 图标，开启Informational级别、NAT类型的报警策略，为 NAT 事件生成本地报警日志。

提示：日志存储介质为硬盘时才可以生成本地报警日志。

---

3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] alert-config local-syslog internal level Informational type NAT
NetEye@root-system] exit
NetEye@root> save config
```

验证 SNAT， DNAT 和 DNS 重写结果

1. 在内网主机上访问内网服务器的域名。
2. 选择**监控 > 地址转换**，查看当前的源地址转换会话条目。

提示：地址转换监控界面只显示当前活动的 NAT 会话条目，当某 NAT 会话断开连接或连接超时时，监控列表中将不再显示该 NAT 条目。

---

3. 选择**监控 > 报警 / 日志 > 系统日志**。
   a. 点击表头**类型**前面的 图标，在弹出的对话框中选择 NAT 类型。
   b. 点击**是**，筛选出 NAT 日志信息。
4. 在外网主机上访问内网服务器的域名。
5. 选择**监控 > 地址转换**，查看当前的源地址转换会话条目。

- 选择**监控 > 报警 / 日志 > 系统日志**。查看 NAT 日志信息。

9 服务质量

本章介绍服务质量 （Quality of Service， QoS）的功能特性，包含以下内容：

9.1 概述

在运营商或企业用户的网络中，网络带宽资源非常宝贵， QoS 功能对日趋严重的带宽滥用、误用进行控制，限制 P2P、游戏等非法流量，使网络带宽资源被合理利用。

NISG-IPS 的 QoS 功能应用于流量比较大的环境，如运营商、大中型企业、教育系统等。

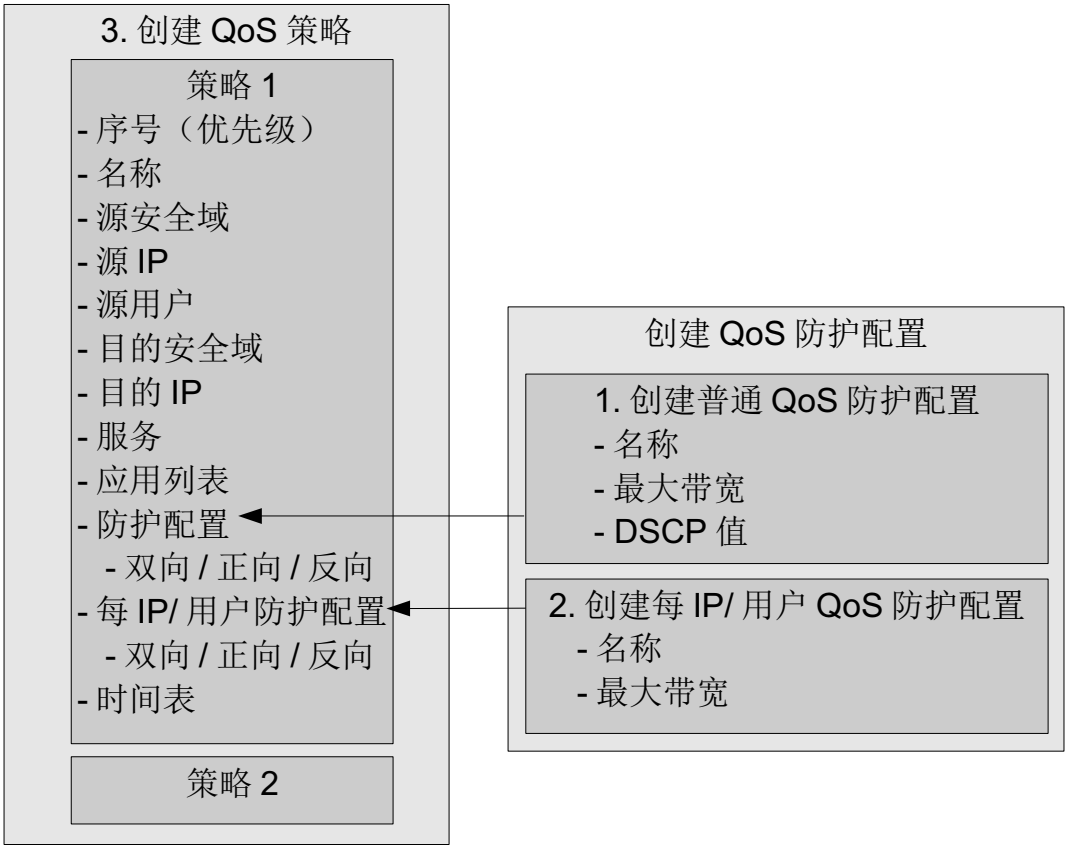
QoS 指网络带宽有限的情况下，为指定网络流量提供更优服务的一种能力。本节介绍 QoS 相关的一些基本概念：

- **策略序号**：QoS 策略的优先级。
- **匹配条件**包括：
  - 源安全域 /IP
  - 目的安全域 /IP
  - 源用户
  - 服务
  - 应用列表
- **普通 QoS 防护配置**：指定所有 IP/ 用户流量的最大带宽和 DSCP 值。
- **每 IP/ 用户 QoS 防护配置**：指定每 IP/ 用户流量可占用的最大带宽。
- **时间表**：QoS 策略的生效时间。

9.2 基本配置步骤

本节包含以下内容：

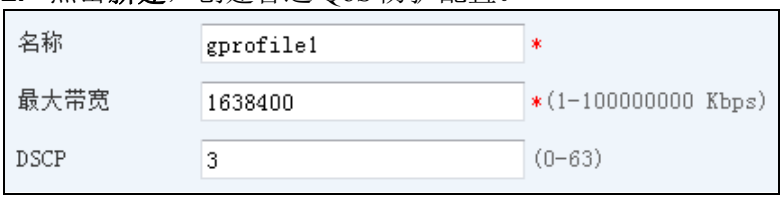
图 12 QoS 配置步骤



提示：QoS 只能通过 WebUI 进行配置。

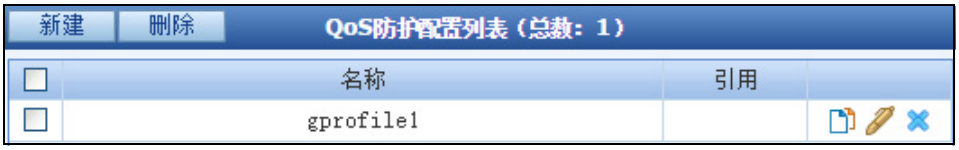
9.2.1 创建普通 QoS 防护配置

1. 选择 **IPS>QoS>QoS 防护配置**。
2. 点击**新建**，创建普通 QoS 防护配置。



提示：1M = 1 x 1024 x 8 Kbps

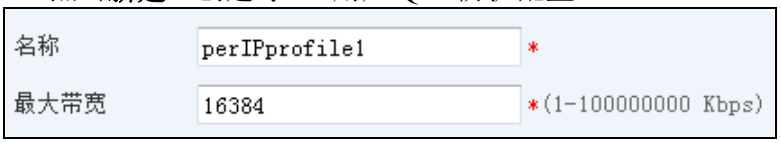
3. 点击**确定**。



4. 点击 克隆 QoS 防护配置。
5. 点击 查看引用该防护配置的策略。

9.2.2. 创建每 IP/ 用户 QoS 防护配置

1. 选择 **IPS>QoS> 每 IP/ 用户 QoS 防护配置**。
2. 点击**新建**，创建每 IP/ 用户 QoS 防护配置。

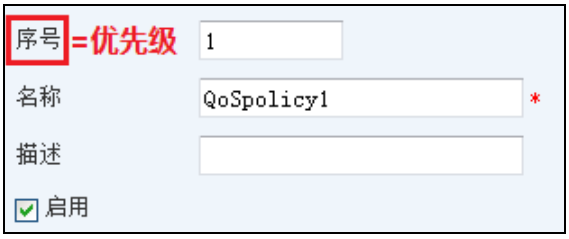


3. 点击**确定**。

4. 点击 克隆 QoS 防护配置。
5. 点击 查看引用该防护配置的策略。

9.2.3 创建 QoS 策略

1. 选择 **IPS>QoS>QoS 策略**。
2. 点击**新建**，创建 QoS 策略。
   a. 设置策略优先级、名称和启用状态：

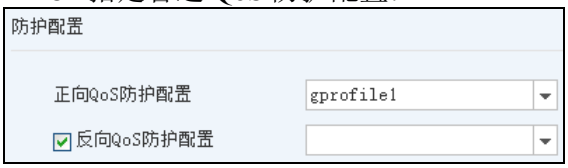


   b. 设置源安全域、源 IP 和源用户：

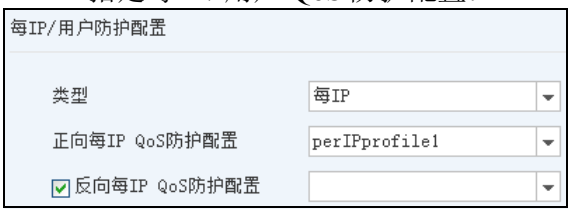
c. 设置目的安全域和目的 IP：

d. 设置服务和应用。关于如何添加应用到应用列表，请参见 12.2.1.2.3 创建应用控制防护配置 （2c）。

e. 指定普通 QoS 防护配置：



f. 指定每 IP/ 用户 QoS 防护配置：



g. 设置策略生效时间：

3. 点击**确定**。

- 点击移动策略位置以改变其优先级。
- 点击设置查找 QoS 策略的筛选条件。
- 点击策略名称链接编辑策略的描述信息：

- 点击对应的链接编辑以下参数信息：源 IP、源用户、目的 IP/ 域名、服务。

9.3 配置参数说明

本节介绍以下内容的配置参数：

9.3.1 QoS 策略

表 162 QoS 策略参数

参数	描述
序号	QoS 策略的优先级，序号越小，优先级越高。取值范围为 1-80000。
名称	QoS 策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
源安全域	QoS 策略要控制的数据包的发起安全域。
源 IP	每条 QoS 策略支持 4096 个源 IP 地址或地址段。
源用户	类型包括： • **任意**：包括已进行身份认证和未进行身份认证的所有用户。 • **任意认证用户**：包括已进行身份认证的所有用户。 • **使用下表**：可以选择包括未在 NISG-IPS 上创建的、外部认证服务器上的用户。 每条 QoS 策略支持 4096 个源用户。
目的安全域	QoS 策略要控制的数据包发往的安全域。
目的 IP/ 域名	每条 QoS 策略支持 4096 个目的 IP 地址、地址段或域名。
服务	QoS 策略要控制的数据包的源和目的端口。 管理员最多可添加 32 条服务 （4096 个端口号），协议列表内不允许出现重复的条目。
应用列表	QoS 策略要控制的数据包所属应用的类型。 管理员可通过选择应用名称或过滤条件添加应用。
时间表	QoS 策略的生效时间。管理员可以选择设置周期性或一次性时间表。 如果当前访问策略未设置时间表，并且其状态为启用，则表示它在任何时间内都生效。
启用	显示 QoS 策略是否启用。
描述	QoS 策略的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? " ' \<>&
（普通）防护配置	QoS 策略引用的普通 QoS 防护配置。 QoS 策略通过指定普通 QoS 防护配置定义整体流量的最大带宽和 DSCP 值。 QoS 策略中可以指定双向和单向两种 QoS 防护配置： • **双向 QoS 防护配置**：对双向的流量进行带宽控制。 • **正向 QoS 防护配置**：对从源到目的的流量进行带宽控制。仅当管理员勾选**反向 QoS 防护配置**时可见。 • **反向 QoS 防护配置**：对反向流量进行控制。 一个 QoS 防护配置可以被多条策略引用。
每 IP/ 用户防护配置	QoS 策略引用的每 IP/ 用户 QoS 防护配置。 QoS 策略通过指定每 IP/ 用户 QoS 防护配置定义每 IP 或每用户流量的最大带宽。 QoS 策略中可以为每 IP/ 用户 QoS 防护配置指定以下内容： • **防护配置类型**：包括**每 IP** 和**每用户**。 • **双向每 IP/ 用户 QoS 防护配置**：对双向的流量进行每 IP/ 用户带宽控制。 • **正向每 IP/ 用户 QoS 防护配置**：对从源到目的的流量进行每 IP/ 用户带宽控制。仅当管理员勾选**反向每 IP/ 用户 QoS 防护配置**时可见。 • **反向每 IP/ 用户 QoS 防护配置**：对反向流量进行每 IP/ 用户带宽控制。

9.3.2 QoS 防护配置

表 163 （普通） QoS 防护配置参数

参数	描述
名称	普通 QoS 防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\ < > & #
引用	点击 查看引用该普通 QoS 防护配置的 QoS 策略。 一个普通 QoS 防护配置可以被多个 QoS 策略引用，被引用的防护配置不能被删除。
最大带宽	最大可使用带宽。 指定服务占用的流量不能超过此限制。如果此阈值大于系统吞吐量， NISG-IPS 会尽最大努力转发流量。
DSCP	对流经 NISG-IPS 的数据包添加的标记，表示数据包在后续的网络设备上需要继续进行流量控制。关于差分服务代码点 （Differentiated Services Code Point， DSCP）的详细信息，请参见 RFC 2474。

9.3.3 每 IP/ 用户 QoS 防护配置

表 164 每 IP/ 用户 QoS 防护配置参数

参数	描述
名称	每 IP/ 用户 QoS 防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\ < > & #
引用	点击 查看引用当前每 IP/ 用户 QoS 防护配置的 QoS 策略。 一个每 IP/ 用户 QoS 防护配置可以被多个 QoS 策略引用，被引用的防护配置不能被删除。
最大带宽	每 IP 或用户可以使用的最大带宽。

9.4. QoS 范例

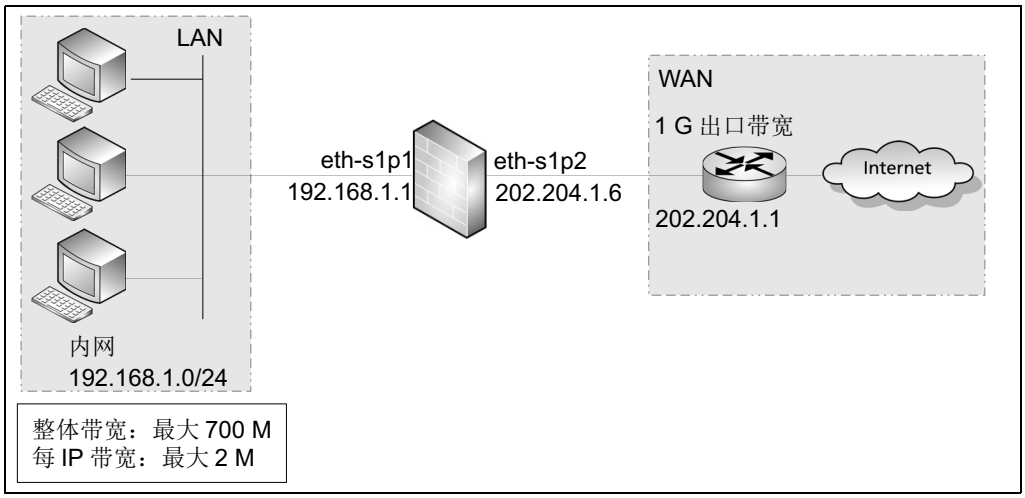
某企业网络出口总带宽为 1G （1024M），希望通过 NISG-IPS 的 QoS 功能限制带宽资源的使用，使带宽被合理地分配和使用。

基本需求

为了避免内网用户占用过多带宽，影响内网服务器对外提供服务器，需要进行以下限制：

- 内网员工的整体上网带宽在 700M 以内；
- 每位员工上网流量不超过 2M （每位员工分配一个 IP 地址）。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置安全域
- 配置路由
- 配置 SNAT 规则
- 配置访问策略
- 创建普通 QoS 防护配置
- 创建每 IP QoS 防护配置
- 创建 QoS 策略

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 点击接口对应的，设置接口 IP 地址。
   - eth-s1p1：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - IP 地址：（静态 IP） 202.204.1.6/24
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.204.1.6 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

配置安全域

1. 选择**网络 > 安全域**。
2. 点击**新建**，创建三层安全域 LAN 和 WAN，分别将三层接口 eth-s1p1 和 eth-s1p2 划入 LAN 和 WAN。
3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone LAN
NetEye@root-system] zone LAN based-layer3 eth-s1p1
NetEye@root-system] zone WAN
NetEye@root-system] zone WAN based-layer3 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

配置路由

1. 选择**网络 > 路由 > 缺省路由**。
2. 点击缺省路由条目对应的，修改网关为 202.204.1.1。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route default gateway 202.204.1.1 1
NetEye@root-system] exit
NetEye@root> save config
```

配置 SNAT 规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**，创建一条 SNAT 规则，允许内网用户访问外网。
   - 名称：snat1
   - 启用：勾选
   - NAPT：勾选
   - 源 IP 地址：192.168.1.0/24
   - 转换后接口：eth-s1p2
   - 入口接口：eth-s1p1
   - 出口接口：eth-s1p2
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy snat snat1 netmask 192.168.1.0
255.255.255.0 interface eth-s1p2 napt enable
NetEye@root-system] policy snat snat1 matching input-interface eth-
s1p1
NetEye@root-system] policy snat snat1 matching output-interface eth-
s1p2
NetEye@root-system] policy snat snat1 matching dip any
NetEye@root-system] exit
NetEye@root> save config
```

配置访问策略

1. 选择**防火墙 > 访问策略**。
2. 点击**新建**，创建一条访问策略，允许内网主机访问外网资源。
   - 名称：LANtoWAN
   - 源安全域：LAN
   - 源 IP 地址：192.168.1.0/24
   - 目的安全域：WAN
   - 目的 IP 地址：任意
   - 服务：任意
   - 动作：允许
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access LANtoWAN LAN 192.168.1.0/24 WAN any any any permit enable
NetEye@root-system] exit
NetEye@root> save config
```

创建普通 QoS 防护配置

1. 选择 **IPS** > **QoS** > **QoS 防护配置**。
2. 点击**新建**，创建 QoS 防护配置：
   - 名称：qosprofile1
   - 最大带宽：5734400 （=700M）
   - DSCP：3 （选填）

   提示：1M = 1 x 1024 x 8 Kbps
3. 点击**确定**。
4. 点击 。

创建每 IP QoS 防护配置

1. 选择 **IPS** > **QoS** > **每 IP/ 用户防护配置**。
2. 点击**新建**，创建每 IP QoS 防护配置：
   - 名称：peripprofile1
   - 最大带宽：16384 （=2M）
3. 点击**确定**。
4. 点击 。

创建 QoS 策略

1. 选择 **IPS** > **QoS** > **QoS 策略**。
2. 点击**新建**，创建 QoS 策略 policy1：
   - 序号：1
   - 名称：policy1
   - 启用：勾选
   - 源安全域：LAN
   - 源 IP 地址：任意
   - 目的安全域：WAN
   - 目的 IP 地址：任意
   - 防护配置：qosprofile1 （不勾选反向复选框）
   - 每 IP/ 用户防护配置：peripprofile1 （不勾选反向复选框）

   提示：不勾选**反向 QoS 防护配置**表示对进出流量进行限制。

3. 点击**确定**。
4. 点击 。

10 策略

策略用于对流经 NISG-IPS 的数据包实施访问控制。 NISG-IPS 访问控制的主要原则是：禁止未经许可的访问。本章内容包括：

10.1 概述

本节介绍 NISG-IPS 的策略特性，章节结构如下所示：

10.1.1 访问策略

访问策略对从特定源发往特定目的的数据包进行控制。

10.1.1.1 策略元素

访问策略的元素包括：

- 基本元素：序号 （优先级）、名称、描述、启用状态 （启用、禁用）、产生日志状态。
- 匹配条件：源安全域、源用户、源 IP、目的安全域、目的 IP、服务、时间表。
- 处理数据包的动作包括：允许和拒绝、引入 VPN 隧道、启用 DNS 透明代理。
- 其他：使用特定超时时间、策略命中计数。

10.1.1.2 访问策略包处理流程

当收到数据包时， NISG-IPS 将数据包中的会话信息与会话表进行匹配：

- 如果找到了一致的会话信息且数据包的会话状态与会话表中的状态相匹配， NISG-IPS 就转发数据包。
- 如果没找到，需要进一步将数据包与所有启用的访问策略进行匹配，并按照策略的优先级由高到低依次进行匹配。
  - 如果数据包匹配一条访问策略且策略的动作是**允许**，NISG-IPS 将数据包的会话信息保存在会话表中并转发数据包。（若策略需要身份认证，将根据用户的权限，决定当前会话请求是否被转发。）

    如果策略的动作是**拒绝**，则丢弃数据包。
  - 如果数据包没有匹配任何策略，则对该数据包应用缺省访问策略。

10.1.1.3 策略自学习

在 NISG-IPS 初始配置下时，将缺省访问策略设置为允许所有数据流通过。 NISG-IPS 可以通过策略自学习功能自动生成访问策略。管理员可以根据实际需求直接使用生成的策略或编辑策略。

10.1.2 多播策略

在 NISG-IPS 上，可以设置多播策略将来自于特定源 IP 的多播数据包转发和路由到指定的目的 IP 地址。 NISG-IPS 只转发匹配多播策略中所有条件的多播数据包。

10.1.3 会话策略

NISG-IPS 的会话策略特性通过限制会话的数量，可以防止会话表泛滥的发生。 NISG-IPS 提供三种类型的会话策略：

- 基于源 IP 地址的会话限制：用于限制来自每个 IP 地址的并发会话数。
- 基于目的 IP 地址的会话限制：用于限制发往每个 IP 地址的并发会话数目。
- 基于策略的会话限制：用于限制所有符合指定源和目的 IP 地址条件的并发会话总数。

当会话匹配了会话策略中规定的匹配条件后，且并发会话数目到达 NISG-IPS 允许的最大数目 （阈值）， NISG-IPS 将拒绝后续连接请求。

会话策略类型	匹配条件
基于源 IP 的会话限制	源 IP 地址、源和目的安全域、服务
基于目的 IP 的会话限制	目的 IP 地址、源和目的安全域、服务
基于策略的会话限制	源和目的 IP 地址、源和目的安全域、服务

10.1.4 IP-MAC 绑定

NISG-IPS 的 IP-MAC 地址绑定特性将主机的 IP 地址及其网卡的 MAC 地址绑定到一起，可以防止非法主机冒用合法主机的 IP 地址。

10.1.4.1 IP-MAC 地址绑定策略

管理员必须将源 IP 地址与 MAC 地址进行绑定，否则 NISG-IPS 不对数据包的源 IP 地址与 MAC 地址是否匹配进行检查。

10.1.4.2 IP-MAC 地址绑定策略自动探测

NISG-IPS 可以在内网三层接口上自动探测内网 IP 地址段，以生成地址段内 IP 地址与 MAC 地址的映射关系条目。支持的三层接口包括以太网接口、以太网通道、冗余接口、VLAN 接口、共享接口和管理接口 （mgt）。需要探测的 IP 地址段应与三层接口的 IP 地址在同一网段。管理员可以根据需求将生成的映射关系添加到 IP-MAC 地址绑定策略列表中。在探测过程中，可以跳转到其他页面进行配置，不会对探测结果产生影响。

10.1.4.3 IP-MAC 绑定策略包处理流程

当 NISG-IPS 接收到 IP 数据包时，将根据其源 IP 地址和源 MAC 地址查询所有已启用的 IP-MAC 地址绑定策略。匹配流程如下：

1. 如果找到与源IP地址匹配的IP-MAC地址绑定策略，NISG-IPS将继续检查数据包中的源 MAC 地址是否和策略中记录的 MAC 地址一致。
   - 如果两者一致，将继续对其进行访问策略检查，根据访问策略决定是否转发该数据包。关于访问策略匹配的信息，请参见 10.1.1.2 访问策略包处理流程。
   - 如果两者不一致，认为该数据包是非法的并拒绝其通过。
2. 如果未找到与源IP地址匹配的IP-MAC地址绑定策略，NISG-IPS继续将其源MAC地址与 IP-MAC 地址绑定策略进行匹配。
   - 如果找到匹配此 MAC 地址的 IP-MAC 地址绑定策略，将拒绝其通过。
   - 如果未找到匹配此MAC地址的IP-MAC地址绑定策略，则根据未匹配任何IP-MAC地址绑定策略的缺省动作对数据包进行处理
     - 如果动作为**允许**，则继续匹配访问策略，并根据对应访问策略的动作决定是否转发该数据包。
     - 如果动作为**拒绝**，则直接拒绝其通过。

10.1.4.4 关联 DHCP IP 地址绑定状态列表

管理员可以将 IP-MAC 绑定策略列表与 DHCP IP 地址绑定状态列表关联起来。关联后，NISG-IPS 首先查询 IP-MAC 绑定策略列表，然后查询 DHCP IP 地址绑定状态列表 （其匹配顺序与 IP -MAC 绑定策略列表的匹配顺序相同）。缺省情况下，关联 DHCP IP 地址绑定状态列表功能是禁用的。

10.1.5 缺省访问策略

缺省访问策略包括：

- 安全域间缺省访问策略：控制不同安全域之间的 IP 数据流。在 NISG-IPS 未被划分安全域前，所有数据流都被认为是域间数据流。
- 安全域内缺省访问策略：控制同一安全域内不同的 NISG-IPS 接口间的 IP 数据流。

缺省访问策略的动作可以设置为**允许**或**拒绝**。安全域间缺省访问策略的缺省动作为**拒绝**，安全域内缺省访问策略的缺省动作为**允许**。

缺省访问策略的优先级低于 NISG-IPS 中已存在的访问策略。

10.2 基本配置步骤

本节介绍 NISG-IPS 策略的基本配置步骤 , 包括：

如需在策略中使用安全域、用户和对象，需要先对其进行配置：

- 安全域：选择**网络** > **安全域**。
- 用户：选择**系统** > **认证** > **用户**。
- IP 地址对象或对象组：选择**系统** > **对象** > **IP 地址** > **IP 地址对象** /**IP 地址对象组**。

提示：IP-MAC 绑定策略可以同时包含 IPv4 地址和 IPv6 地址，而其他策略都不允许。

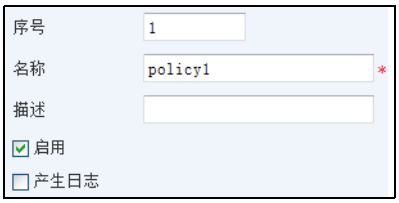
- 服务对象或对象组：选择**系统** > **对象** > **服务** > **服务对象** / **服务对象组**。

10.2.1 创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 如需使用 NISG-IPS 的策略自学习功能，设置一个自学习周期（单位为小时或天）并点击**开始**。

自学习结束后会自动生成访问策略。管理员可以根据实际需要编辑学到的策略。如需手动结束自学习过程，点击**停止**，系统自动生成学习到的策略。如需取消自学习，点击**取消**，系统不会生成策略。

3. 如需创建新的策略，点击**新建**。
4. 设置策略基本元素。



5. 指定数据包的源。

6. 设置数据包的目的地址和服务类型。

7. 设置访问策略的动作。

- 勾选 **VPN 隧道**复选框，选择 VPN 隧道或隧道组，匹配此策略的数据包会被引到相应的 VPN 隧道。
- 勾选**启用 DNS 透明代理**，启用 DNS 透明代理功能。
- 勾选**使用特定超时时间**，设置此条策略的 TCP 会话、UDP 和 ICMP 模拟会话的超时时间。管理员也可以选择**防火墙** > **缺省策略设置**，设置所有会话的缺省状态超时时间。

8. 设置策略的生效时间。

9. 点击**确定**。

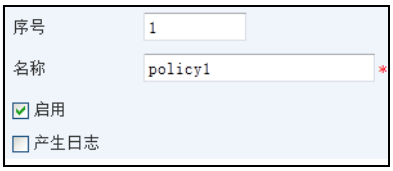
10. 点击。

表 165 访问策略命令

policy access *policy_name*	添加访问策略
policy access *policy_name* **description**	设置备注信息
policy access *policy_name* **log** {**on** | **off**}	启用或禁用日志功能
policy access *policy_name* **number** *pri*	修改策略优先级
policy access *policy_name* **protocol**	添加服务
policy access *policy_name* **schedule**	设置访问策略生效时间
policy access *policy_name* **sourceip**	添加源 IP 地址
policy access *policy_name* **desip**	添加目的 IP 地址
policy access *policy_name* **timeout**	设置会话超时时间
policy access *policy_name* **tunnel**	设置 VPN 隧道
policy access *policy_name* [**user** *user_list*]	添加源用户
unset policy access [*policy_name*]	删除访问策略
show policy access	查看访问策略的配置信息
timeout	设置会话缺省超时时间
timeout reset	设置会话缺省超时时间为缺省值

10.2.2 创建多播策略

1. 选择**防火墙** > **多播策略**。
2. 点击**新建**。
3. 设置策略的基本元素。



4. 设置数据包的源地址。

5. 设置数据包的目的多播组 IP 地址和允许的安全域。

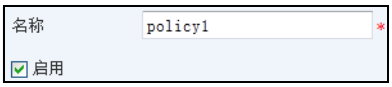
6. 点击**确定**。
7. 点击。

表 166 多播策略命令

policy multicast *policy_name*	添加多播策略
policy multicast *policy_name* **groupip**	添加多播组 IP 地址
policy multicast *policy_name* **log** {**on** | **off**}	启用或禁用日志功能
policy multicast *policy_name* **sourceip**	添加源 IP 地址
policy multicast *policy_name* **allowedzone**	添加目的安全域
policy multicast *policy_name* {enable | disable}	启用或禁用多播策略
policy multicast *policy_name* **number** *pri*	修改策略优先级
show policy multicast [*policy_name*]	查看多播策略的配置信息
unset policy multicast [*policy_name*]	删除多播策略

10.2.3 创建会话策略

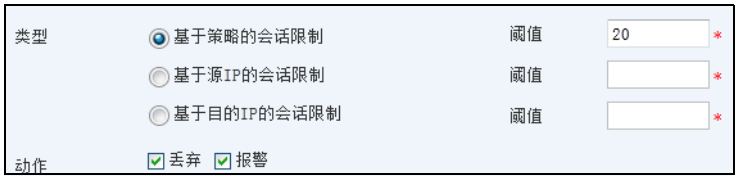
1. 选择**防火墙** > **会话策略**。
2. 点击**新建**。
3. 设置策略基本元素。



4. 设置数据包的源和目的地址。

5. 设置数据包的服务类型。

6. 设置会话策略的类型、允许的最大连接数及动作。



7. 点击**确定**。
8. 点击。

表 167 会话策略命令

policy session *policy_name*	添加会话策略
policy session *policy_name* **sourceip**	为会话策略添加源 IP 地址
policy session *policy_name* **desip**	为会话策略添加目的 IP 地址
policy session *policy_name* {**enable** | **disable**}	启用或禁用会话策略
policy session *policy_name* **protocol**	为会话策略追加服务
policy session *policy_name* type	为会话策略修改策略类型和阈值
show policy session [*policy_name*]	查看策略的配置信息
unset policy session [*policy_name*]	删除会话策略

10.2.4 配置 IP-MAC 绑定

IP-MAC 绑定配置包括：

10.2.4.1 创建 IP-MAC 绑定策略

1. 选择**防火墙** > **IP-MAC 绑定**。
2. 点击**新建**。
3. 设置策略名称。
4. 添加源 IP 地址。
5. 添加源 MAC 地址。

6. 点击**确定**。
7. 点击 。

提示：每个 IP-MAC 绑定策略只能包含一个 MAC 地址，但是可以包含多个 IP 地址或范围。

10.2.4.2 配置缺省动作

当数据包没有匹配到任何 IP-MAC 绑定策略时， NISG-IPS 将会根据 IP-MAC 绑定缺省动作对其进行处理。

1. 选择**防火墙** > **IP-MAC 绑定**。
2. 在**与下列 IP-MAC 绑定策略不匹配的连接**区域，设置**允许**或**拒绝**。

- 如果动作为**允许**，IP 和 MAC 地址都不匹配 IP-MAC 绑定策略的数据包将被允许通过。在关联 DHCP IP 地址绑定列表功能启用的情况下，只有 IP 和 MAC 地址都不匹配 IP-MAC 绑定策略和 DHCP IP 地址绑定策略的数据包才被允许通过。
- 如果动作为**拒绝**，IP 和 MAC 地址都不匹配 IP-MAC 绑定策略的数据包将被丢弃。在关联 DHCP IP 地址绑定列表功能启用的情况下，只有 IP 和 MAC 地址都匹配 IP-MAC 绑定策略和 DHCP IP 地址绑定策略的数据包才被允许通过。

注意：在 WebUI 上，将“**与下列 IP-MAC 绑定策略不匹配的连接**”的动作设置为**拒绝**前，必须配置一条 IP-MAC 绑定策略将管理主机的 IP 与 MAC 地址绑定且保证该策略成功启用。否则会因为缺省动作生效而导致网络连接失败。

3. 点击。

表 168 IP-MAC 绑定策略命令

policy ip-mac *policy_name*	添加 IP-MAC 绑定策略
policy default ip-mac {permit | deny}	修改缺省动作
unset policy ip-mac [*policy_name*]	删除 IP-MAC 绑定策略
show policy ip-mac	查看 IP-MAC 绑定策略配置信息
policy ip-mac dhcp-ip-mac {enable | disable}	启用或禁用关联 DHCP IP 地址绑定状态列表功能

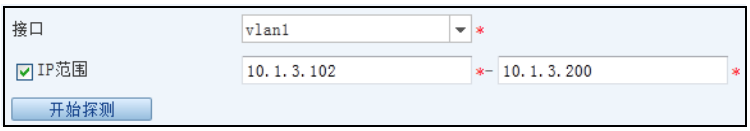
10.2.4.3 关联 DHCP IP 地址绑定状态列表

1. 选择**防火墙** > **IP-MAC 绑定**。
2. 点击**是**启用关联 DHCP IP 地址绑定状态列表功能。在查询完 IP-MAC 绑定策略列表后， NISG-IPS 将继续查询 DHCP IP 地址绑定状态列表。如需禁用此功能，点击**否**，NISG-IPS 将不会查询 DHCP IP 地址绑定状态列表。

3. 点击。

10.2.4.4 配置 IP-MAC 绑定策略自动探测

1. 选择**防火墙** > **IP-MAC 绑定**。
2. 点击**自动探测**。
3. 选择一个三层接口，在此接口上进行探测。
4. 勾选 **IP 范围**，设置 IP 地址范围； IP 地址范围必须与已选三层接口的 IP 地址在同一网段。也可以不勾选 **IP 范围**，此时 NISG-IPS 将探测所有与接口 IP 地址在同一网段的 IP 地址。
5. 点击**开始探测**。



6. 探测过程结束后或点击**停止探测**时，NISG-IPS 自动生成 IP-MAC 绑定策略。这些策略缺省是启用的。管理员可以根据实际需要选择生成的策略，点击**添加 IP-MAC 绑定策略**，将其添加到 IP-MAC 绑定策略列表中。

7. 点击**返回**，可以在 IP-MAC 绑定策略列表中看到添加的策略。点击 编辑相应的策略。

8. 点击 。

10.2.5 配置缺省访问策略

1. 选择**防火墙** > **缺省策略设置**。
2. 设置安全域间和安全域内缺省策略的动作。

3. 点击**确定**。
4. 点击 。

表 169 缺省策略设置命令

policy default inter-zone access {permit | deny}	设置域间缺省策略的动作
policy default intra-zone *zone_name* **{permit | deny}**	设置域内缺省策略的动作
show policy default	显示缺省策略的信息

10.3 配置参数说明

本节详细介绍了策略配置过程中的参数信息，包括：

10.3.1 访问策略参数

表 170 访问策略的配置信息

配置信息	说明
自学习周期	用于设置策略自学习的周期，单位为小时和天。设置之后点击**开始**，策略自学习过程开始；点击**停止**，停止学习；点击**取消**，取消学习。
序号	访问策略的优先级。取值范围为 1 ～ 80000 之间的整数。数值越小，优先级越高。 如果在创建策略时未指定其序号，那么此策略的序号将自动成为最大的。如果将已存在策略的序号指定给新建的策略，则已存在策略的序号将在原序号的基础上加 1。
名称	访问策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # 同一个虚拟系统内部的访问策略不允许配置相同的名称。
描述	访问策略的描述信息。长度 0 ～ 255 个字节。UTF-8 字符。不能包含以下字符：？" ' \ < > &
启用	用于启用或禁用访问策略。访问策略的状态缺省为启用。
产生日志	NISG-IPS 是否为匹配访问策略的数据包记录日志。此功能缺省为禁用。
源安全域	发送数据包的安全域。缺省为 **Any**，即所有安全域。
源 IP 地址	发送数据包的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 和 IPv6 地址。**任意**为缺省设置。 • 任意 IPv4 地址：包括所有 IPv4 地址。 • 任意 IPv6 地址：包括所有 IPv6 地址。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围、 IPv4 地址 / 掩码、IPv6 地址、 IPv6 地址范围和 IPv6 地址 / 前缀。 **IP 地址对象**为缺省设置。 管理员最多可以配置 4096 个源 IP 地址条目。源 IP 地址列表内的条目不允许出现完全相同的情况。
源用户	发送数据包的用户，可以是以下任一类型： • 任意：包括所有网络用户，包括已经通过身份认证和未通过身份认证的用户。**任意**为缺省设置。 • 任意认证用户：包括已经通过身份认证的所有网络用户。 • 使用下表：包括管理员选择的网络用户。管理员可以根据自身的需求选择是否包含未在 NISG-IPS 中配置的外部用户。 管理员最多可以选择 4096 个源用户。源用户列表内的条目不允许出现完全相同的情况。 关于用户的信息，请参见 3.16 网络用户。
目的安全域	数据包要到达的安全域。缺省为 **Any**，即所有安全域。

表 170 访问策略的配置信息 (*续*)

配置信息	说明
目的 IP 地址	数据包要到达的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 和 IPv6 地址。**任意**为缺省设置。 • 任意 IPv4 地址：包括所有 IPv4 地址。 • 任意 IPv6 地址：包括所有 IPv6 地址。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围、 IPv4 地址 / 掩码、 IPv6 地址、 IPv6 地址范围、 IPv6 地址 / 前缀和域名。 **IP 地址对象**为缺省设置。 域名的长度范围为 2 ～ 255 个字节。管理员最多可以设置 4096 个目的 IP 地址条目。目的 IP 地址列表内的条目不允许出现完全相同的情况。
服务	数据包使用的传输层服务，可以是以下任一类型： • 任意：包括所有协议类型。**任意**为缺省设置。 • 使用下表：包括服务对象、服务对象组以及自定义协议。**对象 AOL** 为缺省配置。 自定义协议包括 ICMP、 ICMPv6、 TCP、 UDP 和 Other。 TCP 和 UDP 协议的源和目的端口号范围为 1 ～ 65535。其它协议号范围为 1 ～ 255。 管理员最多可以配置 32 个服务条目 （共 4096 个端口号）。服务列表内的条目不允许出现完全相同的情况。
动作	描述 NISG-IPS 如何处理匹配访问策略的数据包： • 允许：转发数据包并更新其所属会话的状态。动作缺省为**允许**。 • 拒绝：丢弃数据包并取消其会话。
VPN 隧道	当访问策略的动作为**允许**时，可以选择启用或禁用 VPN 隧道功能。此功能缺省为禁用。启用后，可以将数据包引入到指定的 VPN 隧道或隧道组。
启用 DNS 透明代理	当访问策略的动作为**允许**时，可以启用或禁用透明代理功能。此功能缺省为禁用。 关于透明代理的信息，请参见 4.8 DNS 代理。
使用特定超时时间	当访问策略的动作为**允许**时，可以启用或禁用特定超时时间。此功能缺省为禁用。 启用后，可以为 TCP 会话状以及 ICMP 和 UDP 的模拟会话设置超时时间。超时时间范围为 1 ～ 99999999 秒。禁用该功能时， NISG-IPS 将采用系统提供的缺省状态超时时间设置。

时间表	用于启用或禁用访问策略的生效时间。此功能缺省为禁用。
	如果没有为启用的访问策略设置时间表，那么此条访问策略在任何时间都生效。
	• 循环：用于设置访问策略的循环生效时间。在循环生效时间范围内，访问策略在每周指定的具体时间生效。
	  • 每周：可以从周一至周日中选择。
	  • 时间列表：可以设置每天生效时间的起始时间和终止时间。格式为：HH:MM:SS ；可选范围：00:00:00 ～ 23:59:59。最多可以将 8 个时间条目添加到时间表内。时间范围允许重叠但不允许完全相同。
	• 单次：用于设置访问策略的单次生效时间。访问策略只在设置的时间段内生效，而不会在其他时间段重复生效。日期的格式为： YYYY-MM-DD ；可选择范围为 1970-01-01 ～ 2037-12-31。
	必须设置一个起始日期和时间以及终止日期和时间。

计数	表示访问策略被命中的次数，计数值随策略的命中次数增加而累加。当在设备重启、重置、恢复系统配置，或导入同名策略后，策略计数会清零；当策略被修改时，策略计数不会清零，可以手动进行清零。 策略计数可以当做筛选策略的条件。

10.3.2 多播策略参数

表 171 多播策略的配置信息

配置信息	说明
序号	表示多播策略的优先级。取值范围为 1 ～ 80000 之间的整数。数值越小，优先级越高。 如果在创建策略时未指定其序号，那么此策略的序号将自动成为最大的。如果将已存在策略的序号指定给新建的策略，则已存在策略的序号将在原序号的基础上加 1。
名称	多播策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & # 同一个虚拟系统内部的多播策略不允许配置相同的名称。
启用	用于启用或禁用多播策略。多播策略缺省为启用。
产生日志	NISG-IPS 是否为匹配多播策略的数据包记录日志。此功能缺省为禁用。
源安全域	NISG-IPS 接收多播数据包的入口安全域。缺省为 **Any**，即任意安全域。
源 IP 地址	发送多播数据包的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 多播地址。缺省为**任意**。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围和 IPv4 地址 / 掩码。缺省为 **IP 地址对象**。 管理员最多可以配置 4096 个源 IP 地址条目。源 IP 地址列表内的条目不允许出现完全相同的情况。
多播组 IP 地址	多播数据包的目的多播组的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 多播组地址。缺省为**任意**。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围和 IPv4 地址 / 掩码。缺省为 **IP 地址对象**。 管理员最多可以配置 4096 个多播组 IP 地址条目。多播组 IP 地址列表内的条目不允许出现完全相同的情况。
允许安全域	允许转发多播数据包的出口安全域。缺省为 **Any**，即所有安全域。

10.3.3 会话策略参数

表 172 会话策略的配置信息

配置信息	说明
名称	会话策略的名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # 同一个虚拟系统内部的会话策略不允许配置相同的名称。
启用	用于启用或禁用会话策略。会话策略缺省为启用。
源安全域	发送数据包的安全域。缺省为 **Any**，即所有安全域。
目的安全域	数据包要到达的安全域。缺省为 **Any**，即所有安全域。
源 IP 地址	发送数据包的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 和 IPv6 地址。**任意**为缺省设置。 • 任意 IPv4 地址：包括所有 IPv4 地址。 • 任意 IPv6 地址：包括所有 IPv6 地址。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围、 IPv4 地址 / 掩码、IPv6 地址、 IPv6 地址范围和 IPv6 地址 / 前缀。 **IP 地址对象**为缺省设置。管理员最多可以配置 4096 个源 IP 地址条目。源 IP 地址列表内的条目不允许出现完全相同的情况。
目的 IP 地址	数据包要到达的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 和 IPv6 地址。**任意**为缺省设置。 • 任意 IPv4 地址：包括所有 IPv4 地址。 • 任意 IPv6 地址：包括所有 IPv6 地址。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围、 IPv4 地址 / 掩码、IPv6 地址、 IPv6 地址范围和 IPv6 地址 / 前缀。 **IP 地址对象**为缺省设置。 管理员最多可以配置 4096 个目的 IP 地址条目。目的 IP 地址列表内的条目不允许出现完全相同的情况。
服务	数据包使用的传输层服务，可以是以下任一一种： • 任意：包括所有协议类型。**任意**为缺省设置。 • 使用下表：包括对象、对象组以及自定义协议。对象 AOL 为缺省设置。 自定义协议包括 ICMP、 ICMPv6、 TCP、 UDP 和 Other。 TCP 和 UDP 协议的目的端口号范围为 1 ～ 65535。其它协议号范围为 1 ～ 255。 管理员最多可以配置 32 个服务条目 （共 4096 个端口号）。服务列表内的条目不允许出现完全相同的情况。
类型	会话策略的类型： • 基于策略的会话限制 （缺省类型） • 基于源 IP 的会话限制 • 基于目的 IP 的会话限制
阈值	会话策略允许的最大并发会话数目。取值范围是 1 ～ 99999999。
动作	指 NISG-IPS 如何处理匹配到会话策略的数据包，包括： • 报警：发送报警事件。 • 丢弃：丢弃攻击数据包。 缺省为**报警 + 丢弃**。

10.3.4 IP-MAC 绑定策略参数

表 173 IP-MAC 绑定策略的配置信息

配置信息	说明
名称	IP-MAC 地址绑定策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & # 同一个虚拟系统内部的 IP-MAC 地址绑定策略不允许配置相同的名称。
启用	用于启用或禁用 IP-MAC 地址绑定策略。 IP-MAC 地址绑定策略缺省为启用。
绑定 IP 地址列表	用于设置发送数据包的源 IP 地址。 IP 地址可以是以下任一类型： • IP 地址对象 • 对象组 • IPv4 地址 • IPv4 地址范围 • IPv4 地址 / 掩码长度 • IPv6 地址 • IPv6 地址范围 • IPv6 地址 / 前缀长度 **IP 地址对象**为缺省设置。管理员最多可以添加 4096 个地址条目。 IP 地址列表内的条目不允许出现完全相同的情况。
MAC 地址	用于设置发送数据包的源 MAC 地址。 管理员只可以为每条 IP-MAC 地址绑定策略设置一个 MAC 地址。 **IP 地址绑定列表**中的每个 IPv4 和 IPv6 地址都与此 MAC 地址绑定。

表 174 IP-MAC 绑定策略自动探测

配置信息	说明
接口	启用策略自动探测的三层接口。
IP 范围	进行策略自动探测的 IP 地址范围。
开始探测	点击此按钮开始策略自动探测。
停止探测	点击此按钮停止策略自动探测。
探测结果	自动探测生成的 IP-MAC 绑定策略在此列表中显示。 如需将生成的策略添加到 **IP-MAC 绑定策略**列表中，选择策略，点击**添加 IP-MAC 绑定策略。**

10.4 策略范例

本节介绍如何在实际场景中配置策略，包括以下内容：

提示：范例里的 IP 地址只是用于举例说明。可以根据实际需要更改 IP 地址。

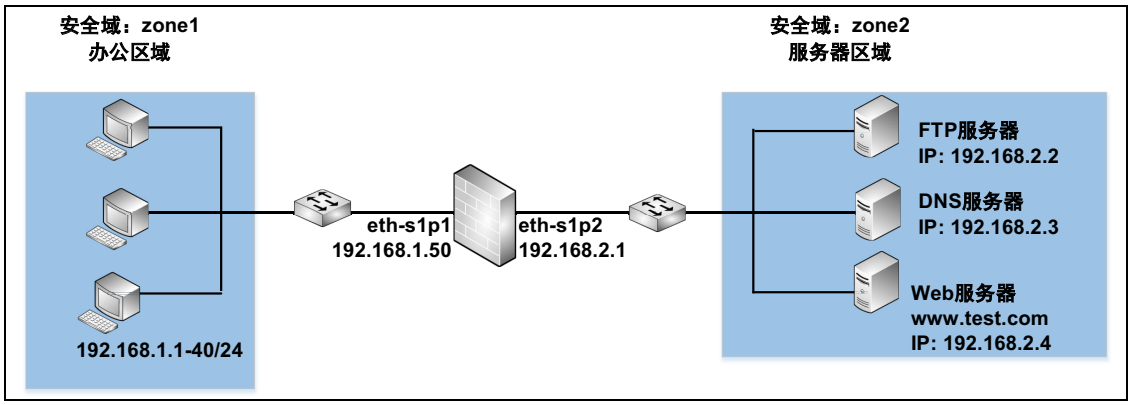
10.4.1 范例：创建访问策略

某公司的内网有一个办公区域和一个服务器区域。

基本需求

- 为制定统一的访问控制策略，将公司的办公区域和服务器区域划分到不同的安全域。
- 允许办公区域内 IP 地址范围在 192.168.1.1-192.168.1.20 中的员工访问服务器区域的 FTP 服务器，并对其访问情况进行记录。为避免 FTP 服务器的并发连接数过大，在已建立的 FTP 会话上，如果员工在 300 秒内未进行操作，会话能够超时断开。
- 允许办公区域内 IP 地址范围在 192.168.1.21-192.168.1.40 中的员工在工作时间 (08:30:00-17:30:00，周一至周五) 访问办公区域内的 Web 服务器。
- 不允许服务器区域访问办公区域。

组网拓扑



配置要点

- 配置以太网接口，设置以太网接口的工作模式和 IP 地址。
- 创建安全域，将三层以太网接口划分到安全域中。
- 创建访问策略，控制安全域间的数据访问。

配置步骤

配置以太网接口

1. 选择**网络** > **接口**。
2. 在**接口列表中**分别点击接口所对应的，进行如下配置：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.50/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：192.168.2.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.50 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - zone1：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - zone2：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone zone1
NetEye@root-system] zone zone1 based-layer3 eth-s1p1
NetEye@root-system] zone zone2
NetEye@root-system] zone zone2 based-layer3 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。点击**新建**分别创建以下访问策略：
   - policy1：
     - 序号：1
     - 产生日志：勾选
     - 源安全域：zone1
     - 源 IP：192.168.1.1-192.168.1.20
     - 目的安全域：zone2
     - 目的 IP/ 域名：192.168.2.2
     - 服务 > 自定义 > TCP ：
       - 源端口：1024-65535
       - 目的端口：21
     - 使用特定超时时间 > TCP_ESTED：300
     - 动作：允许
   - policy2：
     - 序号：2
     - 源安全域：zone1
     - 源 IP：192.168.1.21-192.168.1.40
     - 目的安全域：zone2
     - 目的 IP/ 域名：192.168.2.3-192.168.2.4
     - 服务 > 自定义 > TCP ：
       - 源端口：1024-65535
       - 目的端口：80
     - 服务 > 对象：DNS
     - 动作：拒绝
     - 时间 > 循环：
       - 每周：一，二，三，四，五
       - 时间列表：8:30:00-17:30:00
   - policy3：
     - 序号：3
     - 源安全域：zone2
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务 ：任意
     - 动作：拒绝
2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access policy1 zone1 192.168.1.1-192.168.1.20 zone2 any tcp 1024-65535 21 any permit enable 1
NetEye@root-system] policy access policy1 timeout tcp ested 300
NetEye@root-system] policy access policy1 log on
NetEye@root-system] policy access policy2 zone1 192.168.1.21-192.168.1.40 zone2 192.168.2.3,192.168.2.4 tcp 1-65535 80 any permit enable 2
NetEye@root-system] policy access policy2 protocol protocol-object dns
NetEye@root-system] policy access policy2 schedule start-week 1 end-week 5 08:30:00-17:30:00
NetEye@root-system] policy access policy3 zone2 any zone1 any any any deny enable 3
NetEye@root-system] exit
NetEye@root> save config
```

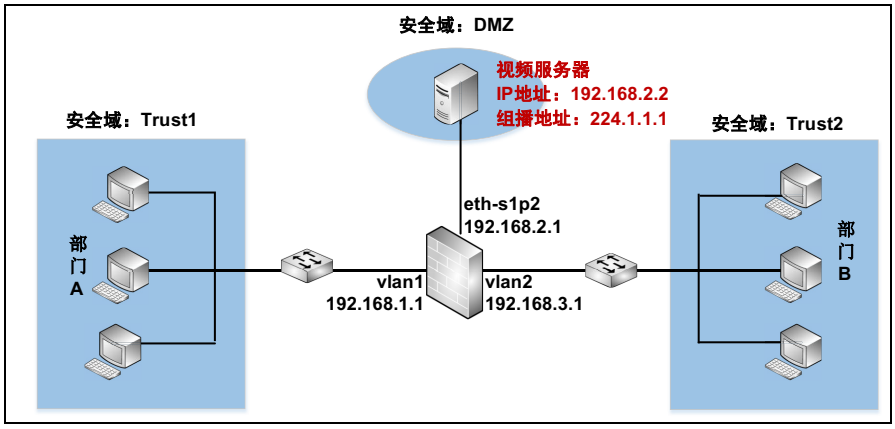
10.4.2 范例：安全域间多播策略的应用

某公司的视频服务器使用多播组 IP 地址 224.1.1.1 播放视频节目。多播数据包的 TTL 值为 5。

基本需求

- 部门 A 中的员工可以观看视频节目，部门 B 中的员工不可以观看视频节目。
- 为制定统一的访问控制策略，将两个部门和服务器划分到不同的安全域。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 创建 VLAN 接口，将二层以太网接口划分到 VLAN 接口中并设置 VLAN 接口的 IP 地址。
- 配置 DVMRP，启用 NISG-IPS 的 DVMRP（多播路由）功能并选择启用 DVMRP 功能的接口。
- 创建安全域，将三层以太网接口划分到安全域中。
- 创建多播策略，允许多播数据流在 DMZ 和 Trust1 之间转发。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击接口所对应的，并配置接口为如下：
   - eth-s1p1：
     - 模式：二层
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：192.168.2.1/24
   - eth-s1p3：
     - 模式：二层
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer2-interface
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer2-interface
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

创建 VLAN 接口

1. 选择**网络** > **接口**。
2. 点击**新建** >**VLAN**，创建 vlan1 和 vlan2。将 eth-s1p1 划分给 vlan1， eth-s1p3 划分给 vlan2。将 vlan1 的 IP 地址设置为 192.168.2.1/24， vlan2 的 IP 地址设置为 192.168.3.1/24。
3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] hold ethernet s1p1
NetEye@root-system-vlan1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-vlan1] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] hold ethernet s1p3
NetEye@root-system-vlan2] ip address 192.168.3.1 255.255.255.0
NetEye@root-system-vlan2] end
NetEye@root> save config
```

配置 DVMRP

1. 选择**网络** > **多播** >**DVMRP**，进行如下配置：
   - DVMRP：启用
   - **启用的 DVMRP 接口**列表：
     - 接口：eth-s1p2， vlan1， vlan2

   其他参数在静态路由中不会生效。
2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dvmrp enable
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] dvmrp on
NetEye@root-system-vlan1] dvmrp metric 1
NetEye@root-system-vlan1] dvmrp threshold 1
NetEye@root-system-vlan1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] dvmrp on
NetEye@root-system-if-eth-s1p2] dvmrp metric 1
NetEye@root-system-if-eth-s1p2] dvmrp threshold 1
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] dvmrp on
NetEye@root-system-vlan2] dvmrp metric 1
NetEye@root-system-vlan2] dvmrp threshold 1
NetEye@root-system-vlan2] exit
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust1：
     - 安全域类型：基于三层接口
     - 已选接口：vlan1
   - DMZ：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2
   - Trust2：
     - 安全域类型：基于三层接口
     - 已选接口：vlan2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust1
NetEye@root-system] zone Trust1 based-layer3 vlan1
NetEye@root-system] zone Trust2
NetEye@root-system] zone Trust2 based-layer3 vlan2
NetEye@root-system] zone DMZ
NetEye@root-system] zone DMZ based-layer3 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

创建多播策略

1. 选择**防火墙** > **多播策略**。
2. 点击**新建**，创建一条名为 policy1 的多播策略，允许多播数据流在安全域 DMZ 和 Trust 中转发。
   - 序号：1
   - 源安全域：DMZ
   - 源 IP：192.168.2.2
   - 多播组 IP：224.1.1.1
   - 允许的安全域：Trust1， DMZ
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy multicast policy1 DMZ 192.168.2.2 224.1.1.1
Trust1,DMZ enable 1
NetEye@root-system] end
NetEye@root> save config
```

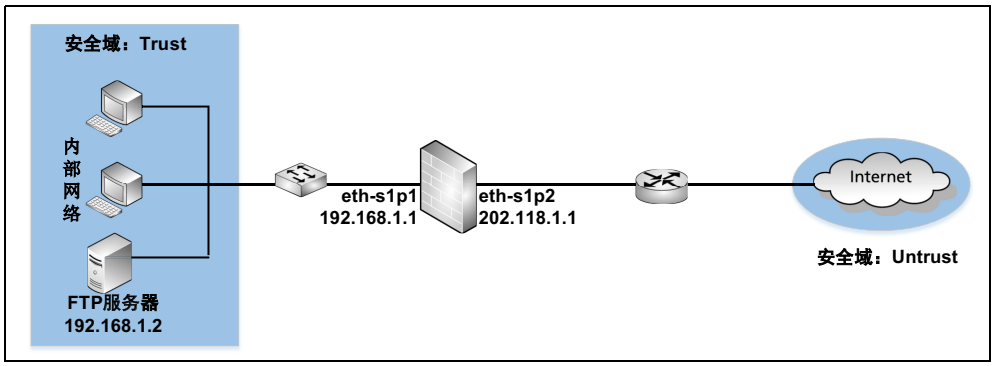
10.4.3 范例：创建基于目的 IP 地址的会话策略

某公司的内网络中部署了一台 FTP 服务器。

基本需求

- Internet 用户可以访问 FTP 服务器。
- 将 FTP 服务器的端口号改为 2121。
- 为防止FTP服务器受到外网的DoS攻击，当来自外网且目的地址为FTP服务器的IP地址的并发会话数到达 20 时，需使 NISG-IPS 拒绝后续数据包并发出报警信息。
- 为制定统一的访问控制策略，将公司内网和外网各划分到不同的安全域。

组网拓扑



配置要点

- 配置接口，设置以太网接口的工作模式和 IP 地址。
- 创建安全域，将三层以太网接口划分给安全域。
- 创建会话策略，以控制从外网发往 FTP 服务器的会话数。
- 创建目的地址转换规则，以使外网用户可以通过eth-s1p2的公有IP地址访问FTP服务器。
- 创建访问策略，只允许外网用户访问内网的 FTP 服务器。

配置步骤

配置接口

1. 选择**网络** > **接口**。
2. 在**接口列表**中分别点击接口所对应的，并配置接口为如下：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.1/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：202.118.1.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - Trust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - Untrust：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone Trust
NetEye@root-system] zone Trust based-layer3 eth-s1p1
NetEye@root-system] zone Untrust
NetEye@root-system] zone Untrust based-layer3 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

创建会话策略

1. 选择**防火墙** > **会话策略**。点击**新建**创建新的会话策略 policy1：
   - 序号：1
   - 源安全域：Untrust
   - 源 IP：任意
   - 目的安全域：Trust
   - 目的 IP/ 域名：202.118.1.1
   - 服务 > 自定义 > TCP：
     - 源端口：1-65535
     - 目的端口：21
   - 类型：基于目的 IP 的会话限制；阈值：20
2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy session policy1 Untrust Trust any
202.118.1.1 tcp 1-65535 21 20 type dstip enable drop alert
NetEye@root-system] end
NetEye@root> save config
```

创建目的地址转换规则

1. 选择**网络** > **地址转换** > **目的地址转换**。
2. 点击**新建**，创建以下规则：
   - 序号：1
   - 名称 rule1
   - 目的 IP：202.118.1.1
   - 目的端口 > TCP：21
   - 转换后 IP：192.168.1.2
   - 转换后端口 > TCP：2121

提示：为了方便用户访问，转换前端口一般设为知名端口如 21，此时建议开启攻击防御和 IPS 功能。

---

3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy dnat rule1 202.118.1.1 tcp 21 192.168.1.2 2121 enable
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy1：
     - 序号：1
     - 源安全域：Untrust
     - 源 IP：任意
     - 目的安全域：Trust
     - 目的 IP/ 域名：192.168.1.2
     - 服务 > 自定义 > TCP ：
       - 源端口：1-65535
     - 目的端口：2121
     - 动作：允许
   - policy2：
     - 序号：2
     - 源安全域：Untrust
     - 源 IP：任意
     - 目的安全域：任意
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy1 Untrust any Trust
192.168.1.2 tcp 1-65535 2121 permit enable 1
NetEye@root-system] policy access policy2 Untrust any any any any any
deny enable 2
NetEye@root-system] exit
NetEye@root> save config
```

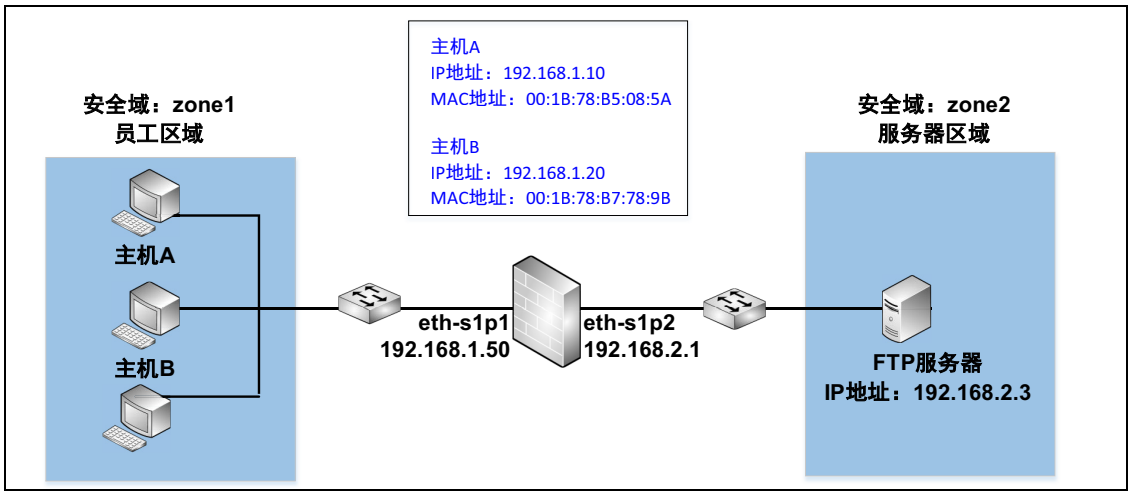
10.4.4 范例：创建 IP-MAC 绑定策略

某公司的内网有一个员工区域和一个服务器区域。

基本需求

- 只允许使用主机 A 和 B 的员工从 FTP 服务器下载内部资料。
- 为制定统一的访问控制策略，将员工区域和服务器区域各划分到不同的安全域中。
- 为了防止IP地址欺骗，将主机A和B的IP地址分别与其对应的MAC地址绑定。只有同时匹配绑定关系中的 IP 地址和 MAC 地址时，数据包才被允许通过。
- 当其他主机试图访问 FTP 服务器，而其 IP 和 MAC 地址不匹配任何 IP-MAC 绑定策略时，阻止此主机访问服务器。
- 不允许服务器访问员工区域。

组网拓扑



配置要点

- 配置以太网接口，设置以太网接口的工作模式和 IP 地址。
- 创建安全域，将三层以太网接口划分到安全域中。
- 创建 IP-MAC 绑定策略，将主机 A 和 B 的 IP 地址分别与其对应的 MAC 地址绑定。
- 创建访问策略，控制安全域间的数据访问。

配置步骤

配置以太网接口

1. 选择**网络** > **接口**。
2. 在**接口列表中**分别点击接口所对应的，进行如下配置：
   - eth-s1p1：
     - 模式：三层
     - （静态） IP 地址：192.168.1.50/24
   - eth-s1p2：
     - 模式：三层
     - （静态） IP 地址：192.168.2.1/24
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.50 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 192.168.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] end
NetEye@root> save config
```

创建安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**，分别创建以下安全域：
   - zone1：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p1
   - zone2：
     - 安全域类型：基于三层接口
     - 已选接口：eth-s1p2
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone zone1
NetEye@root-system] zone zone1 based-layer3 eth-s1p1
NetEye@root-system] zone zone2
NetEye@root-system] zone zone2 based-layer3 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

创建 IP-MAC 绑定策略

1. 选择**防火墙** > **IP-MAC 绑定**。
2. 点击**新建**，分别创建以下访问策略：
   - policy1：
     - 序号：1
     - 绑定 IP 地址列表：
       - 类型：IPv4 地址
       - IP 地址：192.168.1.10
     - MAC 地址：00:1b:78:b5:08:5a
   - policy2：
     - 序号：2
     - 绑定 IP 地址列表：
       - 类型：IPv4 地址
       - IP 地址：192.168.1.20
     - MAC 地址：00:1b:78:b7:78:9b
3. 点击**确定**。
4. 在**与下列 IP-MAC 绑定策略不匹配的连接**区域，点击**拒绝**。

警告

在将动作设置为**拒绝**前，必须配置一条 IP-MAC 绑定策略将管理主机的 IP 与 MAC 地址绑定且保证该策略成功启用。否则会因为缺省动作生效而导致网络连接失败。

5. 在**确认**对话框中点击**是**。
6. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy ip-mac policy1 192.168.1.10
00:1B:78:B5:08:5A enable
NetEye@root-system] policy ip-mac policy2 192.168.1.20
00:1B:78:B7:78:9B enable
NetEye@root-system] policy default ip-mac deny
NetEye@root-system] exit
NetEye@root> save config
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，分别创建以下访问策略：
   - policy1：
     - 序号：1
     - 源安全域：zone1
     - 源 IP：192.168.1.10， 192.168.1.20
     - 目的安全域：zone2
     - 目的 IP/ 域名：192.168.2.3
     - 服务 > 自定义 > TCP ：
       - 源端口：1024-65535
     - 目的端口：21
     - 动作：允许
   - policy2：
     - 序号：2
     - 源安全域：zone2
     - 源 IP：任意
     - 目的安全域：zone1
     - 目的 IP/ 域名：任意
     - 服务：任意
     - 动作：拒绝
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access policy1 zone1
192.168.1.10,192.168.1.20 zone2 192.168.2.3 tcp 1024-65535 21 any
permit enable 1
NetEye@root-system] policy access policy2 zone2 any zone1 any any any
deny enable 2
NetEye@root-system] exit
NetEye@root> save config
```

11 攻击防御

本章介绍安全域级的攻击检测和防御机制。

11.1 概述

网络攻击的目的包括获取机密数据、获取主机系统的相关信息、损坏目标系统等。

NISG-IPS 提供的攻击防御类型包括：

局域网保护	接口级	• ARP 过滤 （防主机欺骗） • ARP 网关保护 （防仿冒网关攻击）
	安全域级	ARP 攻击防御
防御来自外网的网络攻击	策略级	会话泛滥攻击防御 关于会话泛滥攻击的防御措施，请参见 10.1.3 会话策略。
	安全域级	• DoS 防御 • 探测防御 • TCP 逃避控制 • IP 选项校验 • ICMP 攻击防御

NISG-IPS 攻击防御的动作包括：

- **报警**：产生一个报警事件，通知管理员检测到攻击行为。
- **丢弃**：丢弃数据包。
- **丢弃并报警**：丢弃数据包，并且产生一个报警事件。

其中，报警事件内容包含如下信息：

- 攻击类型。
- 攻击数据包的源 IP 地址和源端口。
- 攻击数据包的目的 IP 地址和目的端口。
- 数据包所属的虚拟系统。
- 服务：此攻击数据包所属协议和端口号。
- 源安全域：接收此攻击数据包的安全域。
- 目的安全域：此攻击数据包将要发往的安全域。（只有在策略级报警事件中才记录目的安全域信息）
- 时间：此报警事件的产生时间。
- Vsys 信息：攻击数据包所属的虚拟系统。

在报警策略中选择相应的级别和类型后，可以通过以下报警方式查看到攻击防御的报警日志信息：

- E-mail 方式：产生的报警事件以邮件方式发送到指定的地址，用户可以通过邮件查看到报警消息；
- SNMP Trap 方式：用户可以通过网管平台查看报警消息；
- Syslog 方式：用户可以通过 Syslog 服务器查看到报警消息；
- Local Syslog 方式：用户可以直接通过 NISG-IPS 查看到报警消息。

攻击报文会占用大量的资源，影响受保护主机及其上下联设备的性能。这时需要通过抓包或查看报警信息来确定受到了何种攻击，并启用相应的防御措施。

11.2 基本配置步骤

配置攻击防御措施之前需要先选择安全域。这里的安全域是入口安全域，即可能会接收到攻击包的安全域。

大部分的防御措施中会要求设置阈值 （例如一个时间段内发送的数据包数量），用于判定是否为攻击行为。

11.2.1 配置 ARP 攻击防御和保护

1. 选择**防火墙 > 攻击防御 > ARP 攻击防御**。

2. 选择要开启 ARP 攻击防御的安全域，开启相关防御功能，设置相关阈值和动作。
3. 开启源MAC地址固定的ARP攻击防御后，还可以点击**配置保护 MAC**链接，添加不进行 ARP 攻击防御检测的 MAC 地址。

4. 选择**防火墙 > 攻击防御 > ARP 保护**。

5. 在 **ARP 保护规则列表**中，点击二层接口对应的图标，配置相应的保护模式。

提示：ARP 网关保护和 ARP 过滤保护功能需要在二层接口上配置。 ARP 网关保护需要在设备不与网关相连的接口上配置。

6. 点击**确定**。
7. 点击 。

提示：配置 ARP 防欺骗保护之前，建议先开启 IP-MAC 绑定功能，将需要保护的主机或网关 IP 地址同 MAC 地址绑定。

11.2.2 配置其他类型攻击防御

1. 选择**防火墙** > **攻击防御**。
2. 选择以下任意一种攻击防御类型：
   - DoS 攻击防御
   - 探测防御 （注意开启扫描会占用较多内存）
   - TCP 逃避控制
   - IP 选项校验
   - ICMP 攻击防御
3. 选择要开启攻击防御的安全域，开启相应的防御规则，指定阈值和防御动作。
4. 点击**确定**。
5. 点击 。

表 175 攻击防御相关命令

attack-defense *zone_name attack_name* **active** {**on** | **off**}	为指定安全域启用或禁用特定攻击类型的检测和防御。
attack-defense *zone_name* **spoofed-reset**	设置 TCP 逃避控制的伪造重置保护阈值。
attack-defense *zone_name* **small-pmtu parameter** *threshold_value*	设置 TCP 逃避控制的最小 MTU 值。
attack-defense *zone_name* **tcp-checksum** [**alert**]	启用或禁用对带有非法校验和的数据包的报警功能。
attack-defense tcp-sequence-track	设置 TCP 序列号检验功能。
customize-the-size-of-IP-datagrams-to-send active {**on** | **off**} **threshold** *threshold_ip_datagram*	启用或禁用自定义重组后发送数据包大小功能并设置阈值。
show customize-the-size-of-IP-datagrams-to-send	查看自定义重组后发送的数据包大小功能的设置。

表 175 攻击防御相关命令

attack-defense *zone_name attack_name* **threshold** *threshold_value*	为指定安全域设置指定攻击类型的检测阈值。
attack-defense *zone_name* **arp-anti-attack-source-mac exclude-mac** *mac_address_list*	设置源 MAC 地址固定的 ARP 报文攻击检测时受保护的 MAC 地址，即不进行检测的 MAC 地址。
arp-filter {**off** | **on** *interface_name* {**source** *ip_address_list* | **binding** *ip_address mac_address*}}	为指定的二层接口启用或禁用 ARP 网关保护和 ARP 过滤保护功能。
show attack-defense *zone_name* [*attack_defense_type_name*]	查看指定安全域上的攻击防御配置。
show arp-filter *[layer2_interface_name]*	查看指定二层接口上 ARP 过滤保护功能的配置。

11.3 配置参数说明

11.3.1 DoS 防御参数

DoS 攻击的攻击类型、方式及解决措施如表 176 所示。

表 176 DoS 攻击的类型、方式和解决措施

攻击类型	攻击方式	NISG-IPS 解决措施
会话泛滥	指攻击者向目标网络发送大量的连接请求，使该网络中防火墙的会话表被填满，导致该防火墙因无法继续创建会话而拒绝新的连接请求。	通过限制会话的数量，来遏制 Session Flood 的发生： • **基于源的会话限制**：限制来自相同源 IP 地址的并发会话数目。 • **基于目的的会话限制**：限制来自相同目的 IP 地址的并发会话数目。 • **基于策略的会话限制**：同时限制来自所有源 IP 地址和目的 IP 地址的并发会话数目。 关于会话策略的配置信息，请参见第 10 章，策略。
ICMP 泛滥	在短时间内向受害主机发送大量 ICMP Echo 请求包，耗尽主机资源。	限制每秒钟允许通过的 ICMP Echo 请求数据包个数。 **阈值**：1 - 1,000,000 pps。
TCP SYN 泛滥	在短时间内向受害主机发送带有虚假源 IP 地址的 TCP SYN 数据包，使受害主机系统中堆积大量的半连接，直至资源耗尽。	限制每秒钟允许通过的 TCP SYN 请求数据包数。 **阈值**：1 - 1,000,000 pps。
UDP 泛滥	在短时间内向受害主机发送大量 UDP 数据包，耗尽主机资源。	限制每秒钟允许通过的 UDP 数据包个数。 **阈值**：1 - 1,000,000 pps。
DNS 泛滥	在短时间内向受害主机发送大量 DNS 请求，耗尽主机资源。	限制每秒钟允许通过的来自某安全域的 （基于 UDP 的） DNS 查询请求数量。 **阈值**：1 - 1,000,000 pps。 同时启用 UDP 泛滥防御和 DNS 泛滥防御时： • 如果 DNS 泛滥的阈值大于 UDP 泛滥阈值，则以 UDP 泛滥的阈值和动作为准。 • 如果 DNS 泛滥阈值小于或等于 UDP 泛滥阈值，则以 DNS 泛滥的阈值和动作为准。

表 176 DoS 攻击的类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG-IPS 解决措施
TCP RST 扫描	向目标主机发送大量带有虚假源 IP 的 TCP RST 数据包，使该主机中正常的连接被恶意关闭，服务也因此被迫中断。	接收到 TCP RST 数据包时，会检查此数据包是否属于 NISG-IPS 中已存在的任何一个会话，如果不属于任何会话，将认定此数据包具有 TCP RST 扫描行为，并按照管理员设置的动作对其进行处理。
WinNuke	向使用 Windows 操作系统的主机的 139、138、137、113 或 53 端口发送 TCP URG 数据包，造成 NetBIOS 碎片重叠，并导致系统崩溃。	当 NISG-IPS 中存在目的端口为 139、138、137、113 或 53 的 TCP 会话时，如果接收到属于这个会话的 TCP URG 数据包，将认定此数据包具有 WinNuke 攻击的特征，并按照管理员设置的动作对其进行处理。
LAND	在短时间内向受害主机发送大量源、目的 IP 相同的 TCP SYN 数据包，使受害者系统中存在大量的无用连接，耗尽受害主机的资源，导致拒绝服务。	当接收到 TCP SYN 数据包时，会验证此数据包的源 IP 地址和目的 IP 地址是否相同。如果相同，会按照管理员设置的动作对其进行处理。
Smurf	伪造大量的源 IP 地址为受害主机 IP 且目的 IP 地址为广播地址的 ICMP Echo 请求包，使网络中的所有主机都不断地向受害主机发送应答数据包，导致受害主机被淹没乃至整个网络发生拥塞。	接收到 ICMP Echo 数据包时，会检查此数据包的目的 IP 地址是否为广播地址。如果是，将认定此数据包具有 Smurf 攻击行为，并按照管理员设置的动作对其进行处理。 IPv6 中不存在广播地址，所以 IPv6 中没有 Smurf 攻击。
Ping of Death	IP 数据包的最大长度为 65535 字节。攻击者通常会将过大的 IP 数据包分解成 IP 碎片发送给受害主机。受害主机接收到这些 IP 碎片包时会对其进行重组，当重组后的报文超过 65535 字节时，受害主机就会因系统崩溃而拒绝服务。	NISG-IPS 会对 IP 碎片数据包进行重组，如果重组后 IP 数据包的长度大于 65535，将认定这些 IP 碎片数据包具有 Ping of Death 攻击特征，并将这些数据包丢弃。
TearDrop	攻击者通过修改偏移字段，使 IP 碎片数据包发生重叠。当目的主机尝试重组这些 IP 碎片数据包时，就会引起系统崩溃，导致拒绝服务。	NISG-IPS 接收到 IP 碎片数据包后，会检查与这个 IP 碎片数据包相邻的 IP 碎片数据包，比较偏移值和数据的长度，来判断是否有数据重叠。 NISG-IPS 将会把含有重叠偏移的伪造 IP 碎片数据包丢弃，然后将剩余的 IP 碎片进行重组。
TCP SYN Cookie	通过 TCP 源探测 + 首包丢弃的方法防御 TCP SYN Flood 攻击的一种方式，对 IP 地址源只做一次验证，通过后就加入白名单，占用很少的系统资源。 同时，为了防止出现 SYN Flood 攻击时，有可能对所有的攻击报文都回复错误序列号的 SYN-ACK 报文，还可以通过增加黑名单降低系统资源占用率。	NISG-IPS 接收到 IP 发送的第一个 SYN 报文后，将其丢弃。收到同一 IP 发送的第二个 SYN 报文后，伪造一个带有错误序列号的 SYN+ACK 报文回应给 IP 源所在的客户端。 • 如果客户端回复了 RST 应答，则将这个源 IP 加入白名单； • 如果未收到客户端的 RST 应答，则针对同一 IP 后续发送的每个 SYN 报文都回复一个带有错误序列号的伪造 SYN+ACK 报文。 • 如果在发出 10 个伪造 SYN+ACK 报文后仍未收到客户端回应，则将这个源 IP 加入黑名单；否则将这个源 IP 加入白名单。 白名单和黑名单一共支持最多 2000 个 IPv4 地址，暂不支持 IPv6。

11.3.2 ARP 攻击防御

ARP 攻击防御主要防御 ARP 泛洪攻击， ARP 泛洪攻击的方式及解决措施如表 177 所示。

表 177 ARP 攻击防御的类型、方式和解决措施

攻击类型	攻击方式	NISG-IPS 解决措施
ARP 泛洪攻击	查找 ARP 表需要占用系统资源，所以网络设备一般会限制 ARP 表的大小。攻击者通常会利用这一点，通过伪造大量源 IP 地址变化的 ARP 报文，使设备的 ARP 表溢出，合法用户的 ARP 请求不能生成有效的 ARP 表项，导致正常通信中断。 另外，通过向设备发送大量目的 IP 地址不能解释的 IP 报文，使设备反复对目的 IP 地址进行解释，导致 CPU 负荷过重，也是 ARP 泛洪攻击的一种。	• **基于源 MAC 的 ARP 攻击检测**：如果在 5 秒内收到同一源 MAC 地址的 ARP 报文超过指定的阈值，则认为存在攻击，系统将丢弃 5 秒内收到的后续 ARP 报文。下一个 5 秒重新统计。 **阈值**：1 - 65535 （每 5 秒接收到的 ARP 报文数）。 网关或一些重要服务器可能会发送大量 ARP 报文，为了使这些 ARP 报文不被过滤掉，可以将这类设备的 MAC 地址配置成受保护 MAC。每安全域最多可设置 32 个受保护 MAC。 • **免费 ARP 报文限速**：免费 ARP 是指主机发送 ARP 报文查找自己的 IP 地址，一是确定在同一个子网内是否存在 IP 冲突，二是在主机硬件地址改变后发送免费 ARP 更新该主机在其他接收者设备缓存中的硬件地址。通过限定每秒允许接收到的最大免费 ARP 包数，丢弃超过阈值部分的免费 ARP 包，避免受到免费 ARP 攻击。 **阈值**：1 - 1000000 （每秒接收到的免费 ARP 报文数）。 • **ARP 报文源 MAC 一致性检查**：如果配置此功能，进行 ARP 学习前将对 ARP 报文进行检查。如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则认为是攻击报文，将其丢弃；否则，继续进行 ARP 学习。 • **ARP 主动确认**：设备收到一个 ARP 报文后，将进行主动确认。 若当前设备 ARP 表中没有与此 ARP 报文源 IP 地址对应的 ARP 表项，设备会首先验证该 ARP 报文的真实性。如果为真实报文，则根据此报文新建 ARP 表项；否则，忽略收到的 ARP 报文。 若当前设备 ARP 表中已有与报文源 IP 地址对应的 ARP 表项，但报文携带的源 MAC 地址和现有 ARP 表项中的 MAC 地址不相同，则需要判断该 ARP 表项的刷新时间是否超过 1 分钟。如果没有超过 1 分钟，则设备不会对 ARP 表项进行更新；如果超过 1 分钟，设备将启动当前 ARP 表项的正确性检查。如果 ARP 表项正确，则认为收到的 ARP 请求报文为攻击报文， ARP 表项不会更新；如果不正确，将启动 ARP 报文的真实性检查。如果 ARP 报文为真实报文，将根据报文更新 ARP 表项；如果不是真实报文，则忽略收到的 ARP 报文，ARP 表项不会更新。

11.3.3 ARP 保护参数

表 178 ARP 欺骗的类型、方式和解决措施

攻击类型	攻击方式	NISG-IPS 解决措施
ARP 欺骗	• **ARP 仿冒网关攻击**：攻击者仿冒网关向主机发送伪造的网关 ARP 报文，导致主机的 ARP 表记录错误的网关地址映射关系，从而使主机正常发送的数据不能被网关接收。 如果攻击源发送广播 ARP 报文或根据已掌握的局域网主机信息依次发送攻击报文，可能会导致整个局域网通信的中断。 • **ARP 仿冒用户攻击**：攻击者仿冒主机向网关或其他主机发送伪造的 ARP 报文，导致网关或其他主机的 ARP 表记录了错误的主机地址映射关系，从而使网关或其他主机正常发送的数据包不能被受害主机接收。 • **双向欺骗**：攻击者仿冒网关向主机发送伪造网关 ARP 报文，同时反过来再仿冒主机向网关发送伪造主机 ARP 报文，使网关和主机的数据包都先发往攻击者，攻击者篡改后再进行转发，从而实现中间人攻击。	• **网关保护**：端口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址是否和配置的被保护网关的 IP 地址相同。如果相同，则认为此报文非法，将其丢弃；否则，认为此报文合法，继续进行后续处理。 每个二层接口上最多可配置 32 个被保护网关的 IP 地址。 • **过滤保护**：端口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址和源 MAC 地址是否和允许的 IP 地址和 MAC 地址相同。如果相同，则认为此报文合法，继续进行后续处理；否则，则认为此报文非法，将其丢弃。 • **ARP 报文有效性检查**：所有接口收到 ARP 请求与应答报文时，将进行报文的合法性检查，如报文的 IP 或 MAC 地址是否为全 0 或全 1。如果认为该 ARP 报文合法，则进行转发；否则直接丢弃。

11.3.4 探测防御参数

探测攻击的攻击类型、方式及解决措施如表 179 所示。

表 179 探测防御的类型、方式和解决措施

攻击类型	攻击方式	NISG-IPS 解决措施
IP 地址扫描	将 ICMP Echo 请求包发送给多个主机，如果其中某个主机对 Echo 请求进行应答，那么说明这个主机是活动的，从而让攻击者知道有哪些主机是可以进一步入侵的。	当检测到同一源主机指定时间间隔 （阈值）内向其他目的主机发送 10 个以上的 ICMP Echo 请求包时，视为 IP 地址扫描攻击，并按照管理员设置的动作对其进行处理。 **阈值**：100 - 10000 毫秒 （必须是 100 的整数倍）
TCP SYN 端口扫描	向同一主机的不同端口发送 TCP SYN 数据包来扫描可用的服务。根据端口应答信息的不同，攻击者可以判断出哪些端口是开放的，从而确定进一步攻击目标主机的哪些服务。	检测到同一源主机在指定时间间隔 （阈值）内将 TCP SYN 数据包发送给同一目的主机的 16 个以上不同端口时，视为 TCP SYN 端口扫描攻击，并按照管理员设置的动作对其进行处理。 **阈值**：1 - 7200 秒
TCP FIN 扫描	将 TCP FIN 数据包发送给目标主机的某个端口，然后根据是否返回信息来判断这个端口是否开放 （若返回一个 RST 数据包，说明该端口是关闭的；若什么都不返回，说明该端口是开放的）。由于不同的操作系统对这种数据包的应答信息有所不同，所以攻击者还可以根据返回信息的差异，进一步判断出目标主机正在使用的操作系统类型。	如果接收到 TCP FIN 数据包，而且该数据包不属于当前任何一个连接，那么就认定这个数据包具有 TCP FIN 扫描攻击的特征并按照管理员设置的动作进行处理。
TCP XMAS 扫描	将同时设置了 FIN、 URG 和 PSH 标志位的 TCP 数据包发送给目标主机的某个端口，然后根据是否返回信息来判断这个端口是否是开放的 （若返回一个 RST 数据包，说明该端口被禁用；若什么都不返回，说明该端口启用）。由于不同的操作系统对这种异常包的应答信息有所不同，所以攻击者还可以根据返回信息的差异，进一步判断出目标主机正在使用的操作系统类型。	如果接收到同时设置了 FIN、 URG 和 PSH 标志位的 TCP 数据包，那么就认定这个数据包具有 TCP XMAS 扫描攻击的特征并按照管理员设置的动作进行处理。
TCP NULL 扫描	将未设置任何标志位的 TCP 数据包发送给目标主机的某个端口，然后根据是否返回信息来判断这个端口是否启用 （若返回一个 RST 数据包，说明该端口被禁用；若什么都不返回，说明该端口启用）。由于不同的操作系统对这种异常包的应答信息有所不同，所以攻击者还可以根据返回信息的差异，进一步判断出目标主机正在使用的操作系统类型。	如果接收到未设置任何标志位的 TCP 数据包，那么就认定这个数据包具有 TCP NULL 扫描攻击的特征并按照管理员设置的动作进行处理。

表 179 探测防御的类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG-IPS 解决措施
SYN&FIN 标志	因为 SYN 标志和 FIN 标志的用途截然相反，所以正常情况下， SYN 标志和 FIN 标志不能同时出现在一个 TCP 数据包中，同时设置了 SYN 和 FIN 标志位的 TCP 数据包是一个异常包。由于不同的操作系统对这种异常包的应答信息有所不同，攻击者可以根据返回信息的差异，判断出目标主机正在使用的操作系统类型。	如果 NISG-IPS 接收到同时设置了 SYN 和 FIN 标志位的 TCP 数据包，那么就认定这个数据包具有攻击的特征，并将其丢弃。
无 ACK 标志的 FIN 标志	正常情况下，设置了 FIN 标志位的 TCP 数据包也要同时设置 ACK 标志位，仅设置了 FIN 标志位而未设置 ACK 标志位的 TCP 数据包是一个异常包。攻击者将这种数据包发送给目标主机，然后根据返回信息的差异 （有的会直接丢弃该数据包，有的会返回一个 RST 数据包），判断目标主机正在使用哪种操作系统。	如果 NISG-IPS 接收到仅设置了 FIN 标志位而未设置 ACK 标志位的 TCP 数据包，那么就认定这个数据包具有攻击的特征，并将其丢弃。
非 SYN 标志	发起会话的第一个数据包是有 SYN 标记的数据包，如果没有，则视为异常数据包。攻击者有时会在未建立连接的情况下，向目标主机的某个端口发送这种异常数据包，并根据目标主机是否返回信息来判断这个端口是否是开放的（若返回一个 RST 数据包，说明该端口是关闭的；若什么都不返回，说明该端口是开放的）。	NISG-IPS 每接收到一个数据包，都会进行会话（即连接）的查找。如果该数据包属于已存在的会话， NISG-IPS 将更新这个会话，并转发该数据包；如果该数据包不属于已存在的会话， NISG-IPS 将会对其进行 SYN 标志检查。如果该数据包设置了 SYN 标志位， NISG-IPS 将建立新的会话，然后将其转发；如果该数据包未设置 SYN 标志位， NISG-IPS 就认定这个数据包具有攻击的特征，并将其丢弃。

11.3.5 TCP 逃避控制

TCP 逃避的攻击类型、方式及解决措施如表 180 所示。点击相关数值，可进行修改。

表 180 TCP 逃避的类型、方式和解决措施

攻击类型	攻击方式	NISG-IPS 解决措施
伪造 TCP 重置	TCP RST 数据包用于复位因某种原因引起的错误连接，接收到这种数据包的主机，会清空缓存中已经建立好的连接，如果要继续发送数据，就必须重新开始建立连接。攻击者经常利用这一点，向目标主机发送大量带有虚假源 IP 的 TCP RST 数据包，使该主机中正常的连接被恶意关闭，造成数据丢失和服务中断。	通过限制每个连接在规定的时间间隔内允许通过的最大 RST 数据包数量（即阈值），当达到阈值时，在规定的阻断时间内阻断后续的 RST 数据包，来防止虚假的 TCP RST 数据包对连接造成的破坏和系统资源的损耗。 • **阈值**：2 - 10,000。 • **时间间隔**：2 - 10,000 秒。 • **阻断间隔**：2 - 10,000 秒。
Small PMTU	路径 MTU（Path Maximum Transmission Unit， PMTU）表示因特网上任意一条路径的 MTU。主机可以利用 PMTU Discovery 功能，探测出与目标主机之间的最小 MTU 值，从而确定发送数据包的大小。主机一般根据自身的 MTU 值发出一个 IP 数据包，并且标记该数据包在传输过程中不可分片，当该数据包在传输过程中遇到某一数据链路段的 MTU 值小于该数据包，则该段的路由器会回应给主机一个 ICMP 目的不可达的响应报文，主机会根据这个报文中提供的数据来修改本身的 MTU 值。 Small PMTU 是一种带宽攻击方式，攻击者通过伪造 ICMP 应答包，欺骗受害主机将 MTU 设置成一个较小的值，使目标主机以小包的形式发送大量的数据，进而消耗目标主机的资源，以达到攻击的目的。	通过设置最小 MTU 值，与返回的 ICMP 目标不可达报文中的下一跳 MTU 值进行比较，如果前者大于后者，则丢弃此 ICMP 应答报文。 最小 MTU 值不宜过小，否则不能够起到防御攻击的作用；但是也不能过大，否则会导致合理的请求被丢弃。 • **最小 MTU**：68 - 512 字节。
TCP 控制位异常	TCP 控制位异常校验用于在 TCP 连接建立及关闭过程中检查数据包中的 SYN、 ACK、 FIN 位是否正确置位。TCP 连接的每一个环节数据包包头中的控制位都有着不同的状态，初始建立 TCP 连接时，客户端会向服务端发送带有 SYN 标志的数据包来请求连接，服务端接收到这个包以后会将同时带有 SYN 和 ACK 标志位的数据包回送给客户端，最后客户端发送 ACK 标志数据包确认，以此完成三次握手。结束连接时，会发送带有 FIN 的数据包用来结束一个 TCP 会话。	NISG-IPS 会在 TCP 连接的建立和关闭时，检查数据包包头中的控制位是否正确置位，如果控制位的置位有误，则阻断该连接，以防止恶意的攻击和对连接的破坏。

表 180 TCP 逃避的类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG-IPS 解决措施
TCP 数据重叠	当 TCP 数据包在网络中传输时，会由于传输的错误或者人为的修改，使 TCP 数据包中的数据产生重叠，主机接受到这种数据包将会导致系统崩溃。	NISG-IPS 可以对数据包中的数据进行校验，系统会自动去掉数据包中重叠的部分。
TCP 保护	TCP 协议本身的一些漏洞可能会被攻击者利用，存在安全隐患。	**校验 TCP 校验和**：探测带有非法校验和的数据包。如果数据包的校验和非法，那么将丢弃该数据包。 **校验 TCP 序列号**：探测不符合连接状态的数据包。将当前 TCP 数据包的序列号与 TCP 连接状态进行比对，如果数据包匹配 TCP 会话连接但是序列号错误，那么将丢弃该数据包。管理员可以配置对如下数据包进行序列号探测。 • **所有**：对所有数据包进行不符合连接状态探测，并记录序列校验对数据包采用的每个处理动作 （包括 ACK 号正确但序列号错误的非 RST 数据包）。 • **异常** ：对异常数据包进行不符合连接状态探测，并记录导致丢包和有攻击可能的重大事件 （包括无效的 ACK 号和无效的序列号）。 • **可疑** ：对可疑数据包进行不符合连接状态探测，并记录导致丢包的重大事件 （包括不同序列的 SYN 重传和不同窗口扩展的 SYN/SYN-ACK 重传）。

11.3.6 IP 选项校验参数

IP 选项校验的攻击类型、方式及解决措施如表 181 所示。

表 181 IP 选项校验的类型、方式和解决措施

攻击类型	攻击方式	NISG-IPS 解决措施
IP 记录路由选项	记录 IP 数据包在传输过程中经过的网络设备的 IP 地址。当目的主机接收到设置了记录路由选项的 IP 数据包后，可以获取其记录的路由信息。 攻击者可以利用记录路由选项的这种特性，对网络进行侦查。如果目标网络中的某台主机已被攻击者控制，那么攻击者向该主机发送设置了记录路由选项的 IP 数据包，就可以提取并利用该数据包所记录的路由信息，了解目标网络的拓扑及编址方案。	接收到设置了记录路由选项的 IP 数据包后，首先根据预先设置的动作（报警，丢弃，报警并丢弃）对其进行处理。如果 NISG-IPS 允许其通过，则再检验其选项格式是否正确。如果格式正确，NISG-IPS 需要把转发接口的 IP 地址记录在这个 IP 数据包的记录路由选项中，并将数据包转发；如果格式错误，会将数据包丢弃。
IP 时间戳选项	记录路由器处理数据包的时间，一般在调试网络时用于对路由器的行为进行跟踪。当某个目的主机接收到设置了 IP 时间戳选项的 IP 数据包后，就可以获取该数据包途经路由器的 IP 地址列表，及其在各个路由器之间的传输时间。 攻击者可以利用 IP 时间戳选项的这种特性，来对网络进行探测。如果目标网络中的某台主机已被攻击者控制，那么攻击者向该主机发送设置了 IP 时间戳选项的 IP 数据包，就可以提取并利用该数据包所记录的地址及时间信息，了解目标网络的拓扑及寻址方案。	接收到设置了 IP 时间戳选项的 IP 数据包后，首先根据预先设置的动作（报警，丢弃，报警并丢弃）对其进行处理。如果 NISG-IPS 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG-IPS 需要把时间记录在 IP 时间戳选项中，并将数据包转发；如果格式错误， NISG-IPS 会将数据包丢弃。
IP 宽松源路由选项	与 IP 严格源路由选项相似，但前者相对于后者对数据包在网络中选路的要求进行了放宽。设置了 IP 宽松源路由选项的数据包必须经过在选项中指定的所有路由器，并按指定的地址顺序前进，但允许数据包经过选项指定范围以外的路由器。 攻击者通常会利用 IP 宽松源路由选项的这种特性，使用所指定的路由来隐藏数据包的真实来源，从而非法获得一些受保护网络的访问权限。	接收到设置了 IP 宽松源路由选项的 IP 数据包后，则首先根据预先设置的动作（报警，丢弃，报警并丢弃）对其进行处理。如果 NISG-IPS 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG-IPS 使用转发出口的 IP 地址来替换选项中对应的 IP 地址，并将数据包转发；如果格式错误，NISG-IPS 会将数据包丢弃。
IP 严格源路由选项	使发送端可以预先确定数据包在网络中传输时的路由。这样，发送端根据需要就可以选择延时最小或吞吐量最大的路由，也可以选择更加安全或更加可靠的路由。 设置 IP 严格源路由选项的数据包在选路过程中必须经过其包头选项中指定的所有路由器，且不能经过未指定的路由器。若数据包经过未指定的路由器或到达终点时仍未经过某些指定的路由器，该数据包将会被丢弃。 攻击者通常会利用严格 IP 源路由选项的这种特性，使用所指定的路由来隐藏数据包的真实来源，从而非法获得一些受保护网络的访问权限。	接收到设置了 IP 严格源路由选项的 IP 数据包后，则首先根据预先设置的动作（报警，丢弃，报警并丢弃）对其进行处理。如果 NISG-IPS 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG-IPS 使用转发出口的 IP 地址来替换选项中对应的 IP 地址，并将数据包转发；如果格式错误，NISG-IPS 会将数据包丢弃。

表 181 IP 选项校验的类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG-IPS 解决措施
IP 跟踪路由选项	用于跟踪一个数据包从源到目的的选路路径。如果一个源主机向某个目的主机发送一个设置了 IP 跟踪路由选项的 ICMP Echo 请求数据包，则该请求包在到达目的主机前经过的每个路由器都会向源主机回应一个 ICMP TraceRoute 数据包。假设从源主机到目的主机共经过了 n （n 为正整数）个路由器，则源主机将接收到 n 个 ICMP TraceRoute 数据包和目的主机回应的 ICMP 应答数据包，从而达到跟踪路由的目的。 如果目的主机回应的 ICMP 应答包同样保留了 IP 跟踪路由选项，则目的主机还可以跟踪该应答包所经过的路由。 攻击者通常会利用 IP 跟踪路由选项的上述特性，来收集目标网络的拓扑和编址方案。	接收到设置了 IP 跟踪路由选项的 IP 数据包后，则首先根据预先设置的动作（报警，丢弃，报警并丢弃）对其进行处理。如果 NISG-IPS 允许其通过，则再检验其选项格式是否正确。如果格式正确，NISG-IPS 需要给这个选项数据包的源端发送一个 ICMP TraceRoute 消息，并将数据包转发；如果格式错误，NISG-IPS 会将数据包丢弃。
其他 IP 选项	除了以上介绍的几种 IP 选项攻击， NISG-IPS 还可以检测并防御携带其他 IP 选项的数据包。	接收到设置了其他 IP 选项的数据包后，首先根据预先设置的动作 （报警，丢弃，报警并丢弃）对其进行处理。如果 NISG-IPS 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG-IPS 会将其转发；如果格式错误，NISG-IPS 会将其丢弃。
IP 分片与重组	IP 碎片攻击是指攻击者利用数据包重组代码中的漏洞，向目标主机发送内容被恶意篡改的 IP 碎片数据包。当目标主机接收到这些数据包时，由于无法对其进行正确处理，而导致系统出现异常甚至崩溃。	如果 NISG-IPS 接收到 IP 碎片数据包，会首先检查其是否合法，对于合法的 IP 碎片数据包，NISG-IPS 会将其重组为一个完整的数据包；对于非法的 IP 碎片数据包， NISG-IPS 会将其丢弃，从而达到防御 IP 碎片攻击的目的。 NISG-IPS 允许自定义待发送 IP 报文的大小，取值范围为 30-1460 字节。

11.3.7 ICMP 防御参数

ICMP 攻击的攻击类型、方式及解决措施如表 182 所示。

表 182 ICMP 的攻击类型、方式和解决措施

攻击类型	攻击方式	NISG-IPS 解决措施
ICMP ISS Pinger	互联网安全扫描器（Internet Security Scanner， ISS），可以扫描主机信息及系统漏洞。	报警，丢弃，丢弃并报警
ICMP L3retriever Ping	利用 ICMP Echo 方式，发现网络上主机的状态。	报警，丢弃，丢弃并报警
ICMP Nemesis v1.1 Echo	通过 Nemesis v1.1 软件向网络中注入 ICMP 包。	报警，丢弃，丢弃并报警
ICMP Ping NMAP	网络映射器（Network Mapper， NMAP）扫描， NMAP 可以快速扫描大型网络及单个主机，发现网络上所运行的主机，获取主机的运行信息。	报警，丢弃，丢弃并报警
ICMP Icmpenum v1.1.1	用于扫描目标主机的 IP 地址。	报警，丢弃，丢弃并报警
ICMP Redirect Host	对主机重定向，可以修改主机的路由表，进而影响数据包的发送。	报警，丢弃，丢弃并报警
ICMP Redirect Net	对网络重定向。	报警，丢弃，丢弃并报警
ICMP Superscan Echo	利用 Superscan ICMP 请求回显来测试网络中主机的活动状态。	报警，丢弃，丢弃并报警
ICMP Traceroute IPOPTs	发送 ICMP 包并且对所经过的路径进行记录。	报警，丢弃，丢弃并报警
ICMP Webtrends Scanner	扫描网络中的主机及其运行状态。	报警，丢弃，丢弃并报警
ICMP Source Quench	一种流控制信息，攻击者可以利用其造成的低带宽来发动 DoS 攻击。	报警，丢弃，丢弃并报警
ICMP Broadscan Smurf Scanner	通过发送特定的 ICMP 来扫描网络中活动的主机。	报警，丢弃，丢弃并报警
ICMP Ping Speedera	使用 Speedera ping 占用主机资源。	报警，丢弃，丢弃并报警
ICMP TJPingPro1.1Build 2 Windows	可以获取网络中主机的路径。	报警，丢弃，丢弃并报警
ICMP Ping WhatsUp Gold Windows	可以获取网络中主机的用户名、 IP 地址等信息。	报警，丢弃，丢弃并报警
ICMP Ping CyberKit 2.2 Windows	可以检测网络连接及记录路由功能。	报警，丢弃，丢弃并报警
ICMP Ping Sniffer Pro/NetXRay Network Scan	通过发送 ping 来获取网络中活动的主机信息。	报警，丢弃，丢弃并报警

表 182 ICMP 的攻击类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG-IPS 解决措施
ICMP 目标不可达 - 访问被禁止	目标不可访问。	报警，丢弃，丢弃并报警
ICMP 目标不可达 - 访问目的主机被禁止	目标主机不可访问。	报警，丢弃，丢弃并报警
ICMP 目标不可达 - 访问目的网络被禁止	目标网络不可访问。	报警，丢弃，丢弃并报警
ICMP 数据孤岛带宽查询	用于收集连接的网络带宽。	报警，丢弃，丢弃并报警
ICMP 路径 MTU 拒绝服务攻击	ICMP 协议路径 MTU 拒绝服务，可以获取网络的 MTU，进而发动 DoS 攻击。	报警，丢弃，丢弃并报警

11.4 攻击防御范例

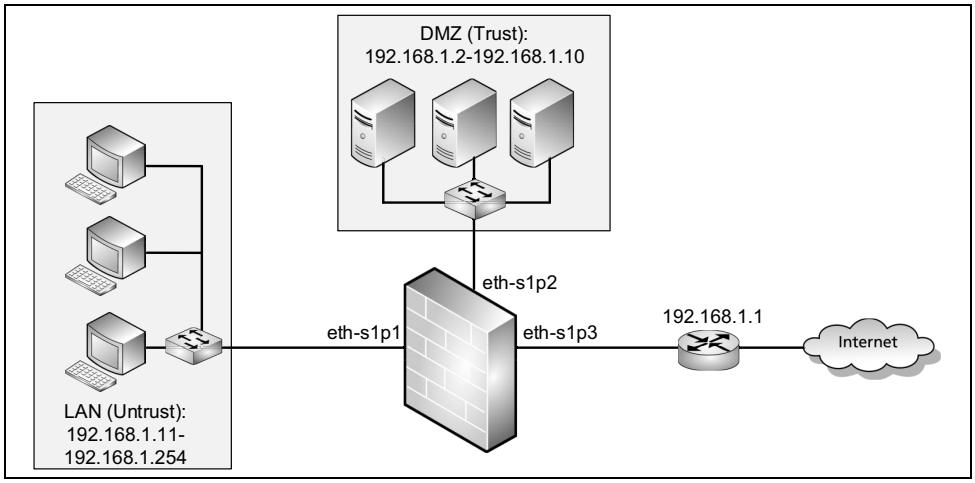
11.4.1 范例：ARP 攻击防御和保护

如下图所示， NISG-IPS 工作在透明模式。二层接口 eth-s1p1 和 eth-s1p2 分别划入二层安全域 LAN 和 DMZ，二层接口 eth-s1p3 连接出口路由器。

基本需求

- LAN 中的主机可以访问 DMZ 中的服务器。
- 在 LAN 上配置 ARP 攻击防御，防止 ARP 泛滥攻击和 ARP 欺骗攻击。
- 配置保护MAC，允许来自MAC地址为00:05:58:c2:06:32的主机的流量不进行ARP攻击防御检测。
- 在 eth-s1p1 上开启 ARP 网关保护，防止攻击者利用其它设备仿冒网关进行 ARP 攻击。

组网拓扑



配置要点

- 创建 VLAN 接口
- 创建二层安全域
- 配置访问策略
- 配置 ARP 攻击防御
- 配置 ARP 保护
- 开启攻击防御日志记录功能
- 验证结果

配置步骤

创建 VLAN 接口

1. 选择**网络 > 接口**。
2. 点击**新建**，创建 VLAN 接口 vlan1。
3. 点击vlan1对应的图标，将二层以太网接口eth-s1p1、eth-s1p2和eth-s1p3划入vlan1。
4. 点击**确定**。
5. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vlan 1
NetEye@root-system-valn1] hold ethernet eth-s1p1
NetEye@root-system-valn1] hold ethernet eth-s1p2
NetEye@root-system-valn1] hold ethernet eth-s1p3
NetEye@root-system-valn1] end
NetEye@root> save config
```

创建二层安全域

1. 选择**网络 > 安全域**。
2. 点击**新建**，创建二层安全域 LAN 和 DMZ，分别将 eth-s1p1 和 eth-s1p2 划入 LAN 和 DMZ。
3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone LAN
NetEye@root-system] zone LAN based-layer2 vlan 1 eth-s1p1
NetEye@root-system] zone DMZ
NetEye@root-system] zone DMZ based-layer2 vlan 1 eth-s1p2
NetEye@root-system] exit
NetEye@root> save config
```

配置访问策略

1. 选择**防火墙 > 访问策略**。
2. 点击**新建**，创建一条访问策略，允许 LAN 到 DMZ 的访问。
   - 序号：1
   - 名称：LANtoWAN
   - 源安全域：LAN

- 源 IP 地址：192.168.1.11-192.168.1.254
- 目的安全域：DMZ
- 目的 IP 地址：192.168.1.2-192.168.1.10
- 服务：任意
- 动作：允许

3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access LANtoDMZ LAN 192.168.1.11-
192.168.1.254 DMZ 192.168.1.2-192.168.1.10 any any permit enable
NetEye@root-system] exit
NetEye@root> save config
```

配置 ARP 攻击防御

1. 选择**防火墙** > **攻击防御** > **ARP 攻击防御**。
2. 在安全域下拉框中选择 **LAN**，在 LAN 上开启相关的 ARP 攻击防御功能。
   a. 开启相关防御功能，设置相关阈值和动作。
      - 基于源 MAC 的 ARP 攻击检测：启用；阈值 =50 包 /5 描述；动作 = 报警 + 丢弃
      - 免费 ARP 报文限速：启用；阈值 =100pps ；动作 = 报警 + 丢弃
      - ARP 报文源 MAC 一致性检查：启用；动作 = 报警 + 丢弃
      - ARP 主动确认：启用；动作 = 报警 + 丢弃
   b. 开启基于源 MAC 的 ARP 攻击检测后，点击**配置保护 MAC** 链接，添加不进行 ARP 攻击防御检测的主机 MAC 地址。
      - MAC 地址：00:05:58:C2:06:32
   c. 点击**确定**。
3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] attack-defense LAN arp-anti-attack-source-mac
active on alert drop
NetEye@root-system] attack-defense LAN arp-anti-attack-source-mac
threshold 50
NetEye@root-system] attack-defense LAN arp-anti-attack-source-mac
exclude-mac 00:05:58:c2:06:32
NetEye@root-system] attack-defense LAN arp-flood active on alert drop
NetEye@root-system] attack-defense LAN arp-flood threshold 100
```

```
NetEye@root-system] attack-defense LAN arp-anti-attack-valid-check
active on alert drop
NetEye@root-system] attack-defense LAN arp-anti-attack-active-ack
active on alert drop
NetEye@root-system] exit
NetEye@root> save config
```

配置 ARP 保护

1. 选择**防火墙 > 攻击防御 > ARP 保护**。
2. 在 **ARP 保护规则列表**中，点击二层接口 eth-s1p1 对应的图标，配置网关保护模式。
   - 二层接口：eth-s1p1
   - ARP 保护类型：网关保护
   - IP 地址：192.168.1.1

提示：ARP 网关保护和 ARP 过滤保护功能需要在二层接口上配置。 ARP 网关保护需要在设备上不与网关相连的接口上配置。

---

3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] arp-filter eth-s1p1 on source 192.168.1.1
NetEye@root-system] exit
NetEye@root> save config
```

开启攻击防御日志记录功能

1. 选择**系统 > 日志配置 > 报警配置**。
2. 点击缺省本地报警策略 internal 对应的图标，开启 Warning 级别、System 类型的报警策略，为攻击防御事件生成本地报警日志。

提示：日志存储介质为硬盘时才可以生成本地报警日志。

---

3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] alert-config local-syslog internal level Warning
type System
NetEye@root-system] exit
NetEye@root> save config
```

验证结果

1. 在 LAN（Untrust）安全域中的 PC 上用工具构造 ARP 报文，向 DMZ 中的服务器发送伪造报文。
2. 选择**监控 > 报警 / 日志 > 系统日志**，查看是否产生 ARP 攻击的报警日志。

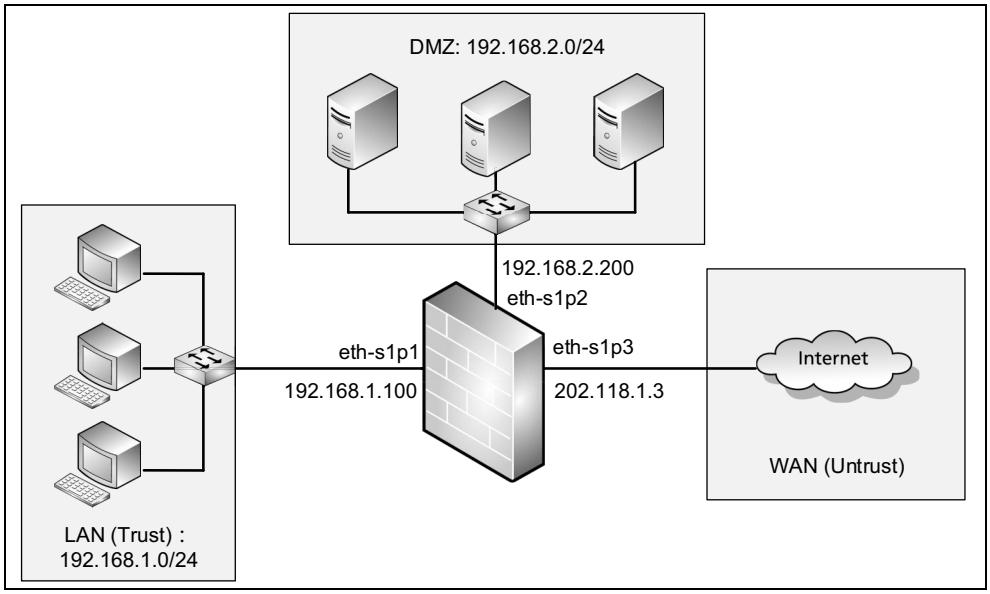
11.4.2 范例：DoS 攻击防御

基本需求

在允许内网主机访问外网、外网主机访问内网服务器的同时，保护内网主机和服务器免受 DoS 攻击的威胁。

- 根据保护对象不同，将内网划分为LAN 和 DMZ 安全域：LAN 中为内网客户端； DMZ 中为内网服务器。
- 外网接口 eth-s1p3 划入 WAN 安全域。
- 在入口安全域 WAN 上开启 ARP 类之外的攻击防御功能，防御来自外网的攻击流量。

组网拓扑



配置要点

- 配置接口 IP 地址
- 创建三层安全域
- 配置访问策略
- 配置 DoS 攻击防御
- 开启攻击防御日志记录功能
- 验证结果

配置步骤

配置接口 IP 地址

1. 选择**网络 > 接口**。
2. 点击接口对应的图标，配置接口 IP 地址。
   - eth-s1p1：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.1.100/24
   - eth-s1p2：
     - 模式：三层
     - IP 地址：（静态 IP） 192.168.2.200/24
   - eth-s1p3：
     - 模式：三层
     - IP 地址：（静态 IP） 202.118.1.3/24
3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.100 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 192.168.2.200 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet eth-s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 202.118.1.3 255.255.255.0
NetEye@root-system-if-eth-s1p3] end
NetEye@root> save config
```

创建三层安全域

1. 选择**网络 > 安全域**。
2. 点击**新建**，创建三层安全域 LAN、DMZ 和 WAN，分别将三层接口 eth-s1p1、eth-s1p2 和 eth-s1p3 划入 LAN、 DMZ 和 WAN。
3. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone LAN
NetEye@root-system] zone LAN based-layer3 eth-s1p1
NetEye@root-system] zone DMZ
NetEye@root-system] zone DMZ based-layer3 eth-s1p2
NetEye@root-system] zone WAN
NetEye@root-system] zone WAN based-layer3 eth-s1p3
NetEye@root-system] exit
NetEye@root> save config
```

配置访问策略

1. 选择**防火墙 > 访问策略**。
2. 点击**新建**，创建以下访问策略：
   - LANtoWAN：允许内网主机访问外网资源。
     - 源安全域：LAN
     - 源 IP 地址：192.168.1.0/24
     - 目的安全域：WAN
     - 目的 IP 地址：任意
     - 服务：任意
     - 动作：允许
   - WANtoDMZ：允许外网主机访问内网服务器。
     - 源安全域：WAN
     - 源 IP 地址：任意
     - 目的安全域：DMZ
     - 目的 IP 地址：192.168.2.0/24
     - 服务：服务 =TCP ； 源端口 =1-65535 ； 目的端口 =25、 110
     - 动作：允许
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access LANtoWAN LAN 192.168.1.0/24 WAN any
any any permit enable
NetEye@root-system] policy access WANtoDMZ WAN any DMZ 192.168.2.0/24
any any permit enable
NetEye@root-system] exit
NetEye@root> save config
```

配置 DoS 攻击防御

1. 选择**防火墙 > 攻击防御 > DoS 防御**。
2. 在安全域下拉框中选择 **WAN**，开启如下攻击防御规则：
   - ICMP 泛滥
   - TCP SYN 泛滥
   - UDP 泛滥
   - DNS 泛滥
   - WinNuke
   - LAND
   - Smurf
   - Ping of Death
   - Teardrop

   使用缺省阈值，设置处理动作为“**报警** + **丢弃**”。
3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root> configure mode
NetEye@root-system] attack-defense WAN icmp-flood active on drop alert
NetEye@root-system] attack-defense WAN icmp-flood threshold 10000
NetEye@root-system] attack-defense WAN tcp-syn-flood active on drop
alert
NetEye@root-system] attack-defense WAN tcp-syn-flood threshold 100000
NetEye@root-system] attack-defense WAN udp-flood active on drop alert
NetEye@root-system] attack-defense WAN udp-flood threshold 100000
NetEye@root-system] attack-defense WAN dns-flood active on drop alert
NetEye@root-system] attack-defense WAN dns-flood threshold 100000
NetEye@root-system] attack-defense WAN winnuke active on drop alert
NetEye@root-system] attack-defense WAN land active on alert drop
NetEye@root-system] attack-defense WAN smurf active on alert drop
NetEye@root-system] exit
NetEye@root> save config
```

提示：探测防御、 TCP 逃避控制、 IP 选项校验和 ICMP 攻击防御的配置步骤同 DoS 攻击防御类似。

开启攻击防御日志记录功能

1. 选择**系统 > 日志配置 > 报警配置**。
2. 点击缺省本地报警策略 internal 对应的图标，开启 Alert 级别和 Sytem 类型的报警策略，为攻击防御事件生成本地报警日志。

提示：日志存储介质为硬盘时才可以生成本地报警日志。

---

3. 点击**确定**。
4. 点击。

CLI

```
NetEye@root> configure mode
NetEye@root-system] alert-config local-syslog internal level Alert type System
NetEye@root-system] exit
NetEye@root> save config
```

验证结果

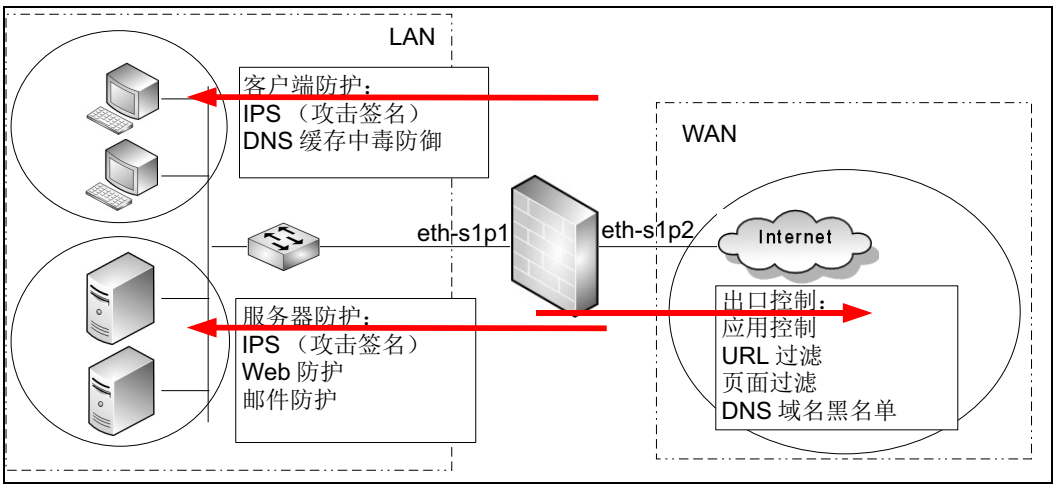
1. 在外网 PC 上构造发往 LAN 中主机或 DMZ 中服务器的攻击报文，发给 eth-s1p3 接口。
2. 选择**监控 > 报警 / 日志 > 系统日志**，查看是否产生 DoS 攻击事件的报警日志。

12 入侵防御系统

本章介绍入侵防御系统（Intrusion Prevention System， IPS）功能。

12.1 概述

图 13 IPS 典型应用场景



随着网络的发展，越来越多的攻击行为和恶意信息隐藏在应用层数据中。 NISG-IPS 的 IPS 功能针对应用层数据进行解析，并对其内容进行安全性检测和控制。

NISG-IPS 提供如下功能：

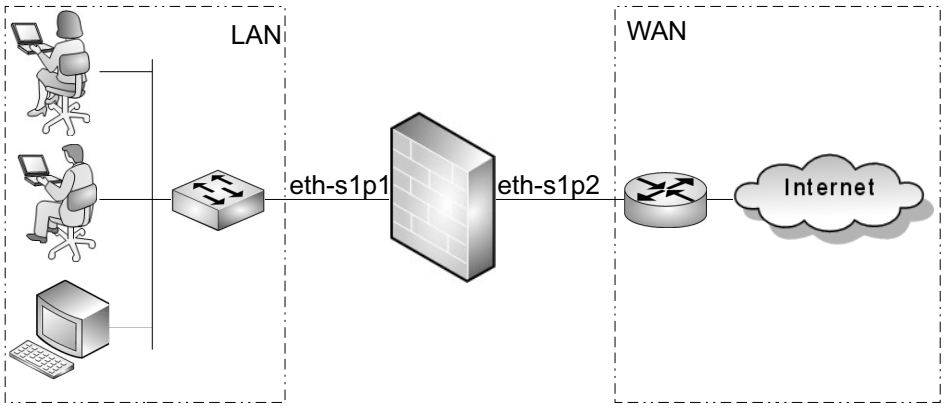
- 多样化的配置模式
  - 12.3.1 出口控制
  - 12.3.2 客户端防护
  - 12.3.3 服务器防护

  根据用户的实际应用场景，NISG-IPS 提供上述三种配置模式，每种配置模式允许用户定义所需的安全防护功能，如 IPS 等。
- 一体化的安全防护
  - 12.3.4 IPS
  - 12.3.5 SSL 检测
- 实时更新
  - 12.3.1.2.4 （应用知识库）更新
  - 12.3.1.3.4 （URL 分类）更新
  - 12.3.4.3 （攻击签名规则）更新

12.1.1 出口控制

出口控制用于在出口安全域上对用户流量进行安全过滤和检测，该配置模式一般用于内网用户访问 Internet 的场景。如下图所示，管理员可在出口安全域 WAN （包含与 Internet 相连的接口）上配置出口控制功能，对内网安全域中用户的上网行为进行控制。

图 14 IPS 出口控制典型应用



用户可为出口控制模式配置如下功能：

- **应用控制**：对用户的应用访问进行控制，可以设置允许或阻止用户访问某些应用。
- **URL 过滤**：对用户要访问的 URL 进行过滤控制。
- **DNS 域名黑名单**：对用户的 DNS 请求进行限制，阻断匹配黑名单的域名解析请求。
- **页面过滤**：阻断包含指定关键字且总分超过指定阈值的页面。

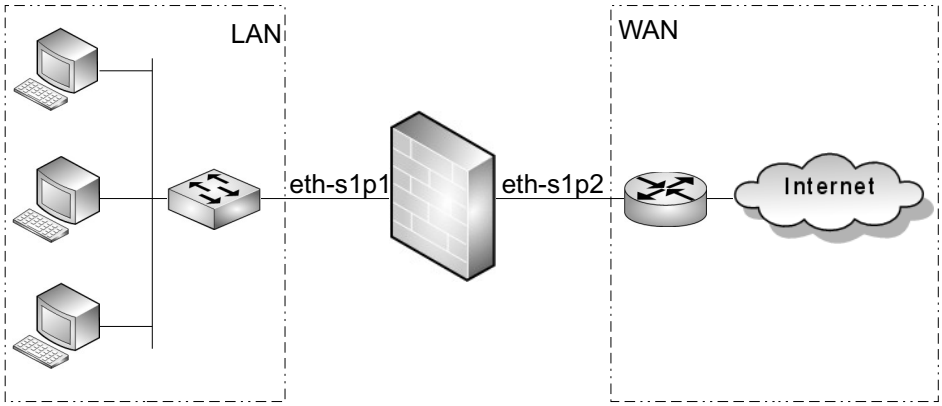
12.1.2 客户端防护

NISG-IPS 提供客户端防护功能，保护特定安全域中的客户端。

12.1.2.1 应用场景

在该配置模式中， NISG-IPS 可以检测客户端从服务器端下载文件和接收邮件的流量，阻断到指定客户端的非法流量。如下图所示，管理员可在安全域 LAN （包含与内网客户端相连的接口）上配置客户端防护以保护内网的客户端不受外网威胁。

图 15 IPS 客户端防护典型应用



12.1.2.2 安全功能

管理员可以为客户端防护配置如下安全功能：

12.1.2.2.1. IPS

入侵防御系统 （Intrusion Prevention System，IPS）能够识别应用层的恶意行为，通过阻断潜在的攻击保护用户的网络环境。 NISG-IPS 的 IPS 提供针对客户端流量和服务器流量的 IPS 检测，包括攻击签名检测和各应用层协议的协议限制。 NISG-IPS 提供实时的攻击签名规则升级功能。

12.1.2.2.2. SSL 检测

当前很多企业业务流量基于 SSL 加密来进行数据传输以提高安全性，但同时基于 SSL 的一些非法访问和攻击行为也使企业信息面临着泄漏等安全威胁。 NISG-IPS 支持 SSL 检测功能，能够对 SSL 加密流量进行 URL 过滤和 IPS 等深度检测，为企业信息提供一体化的安全保障。

下列步骤阐明 NISG-IPS 如何处理客户端与服务器之间的 SSL 流量：

1. NISG-IPS 对客户端发来的 SSL 加密流量进行解密。
2. NISG-IPS 对 SSL 流量进行深度检测，包括 URL 过滤、IPS 攻击签名检测、协议异常检测以及协议限制。
3. NISG-IPS 对检测后的流量进行加密，转发到服务器。

12.1.2.2.3. DNS 缓存中毒防御

当 DNS 服务器缓存区受到攻击时， NISG-IPS 可以防止客户端被重定向到非法网站，引起信息泄漏。管理员可以配置全局 DNS 缓存中毒防御，并在客户端防护策略中开启或关闭该功能。

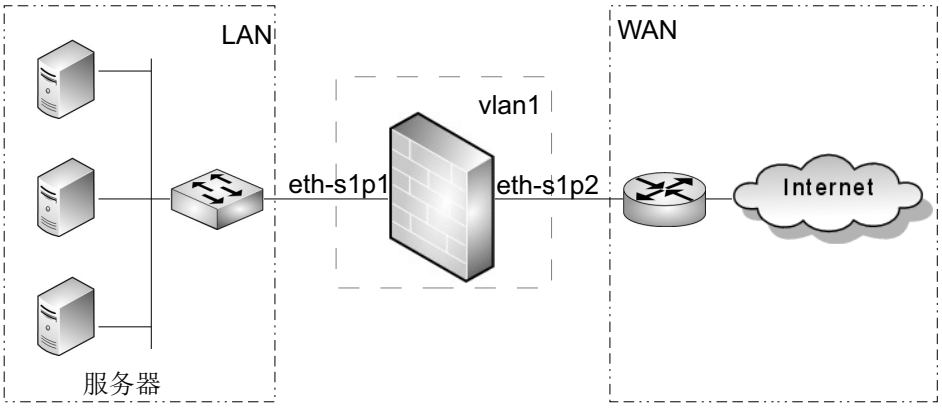
12.1.3 服务器防护

NISG-IPS 提供服务器防护功能，保护特定安全域中的服务器 （Web、邮件、 FTP、 DNS、 Telnet 和 Other 服务器）。

12.1.3.1 应用场景

在该配置模式中器， NISG-IPS 可以检测从客户端向服务器端上传文件和发送邮件的流量，阻断到服务器的非法流量。如下图所示，管理员可以在安全域 LAN （包含与内网服务器相连的接口）上配置服务器防护功能以保护内网中的服务器不受外网威胁。

图 16 IPS 服务器防护典型应用



12.1.3.2 安全功能

关于 IPS 和 SSL 检测，功能同客户端防护。

NISG-IPS 还支持如下服务器防护功能：

- Web 防护

  NISG-IPS 能够为 Web 服务器提供信息泄露检测和注入攻击防御。

- 邮件防护

  服务器的部分应答信息可能会泄露服务器的配置信息，从而可能被攻击者利用。NISG-IPS 信息泄漏功能可以将 SMTP、POP3 和 IMAP 服务器的响应信息替换为管理员设置的信息，有效地防止服务器信息外露。

12.2 基本配置步骤

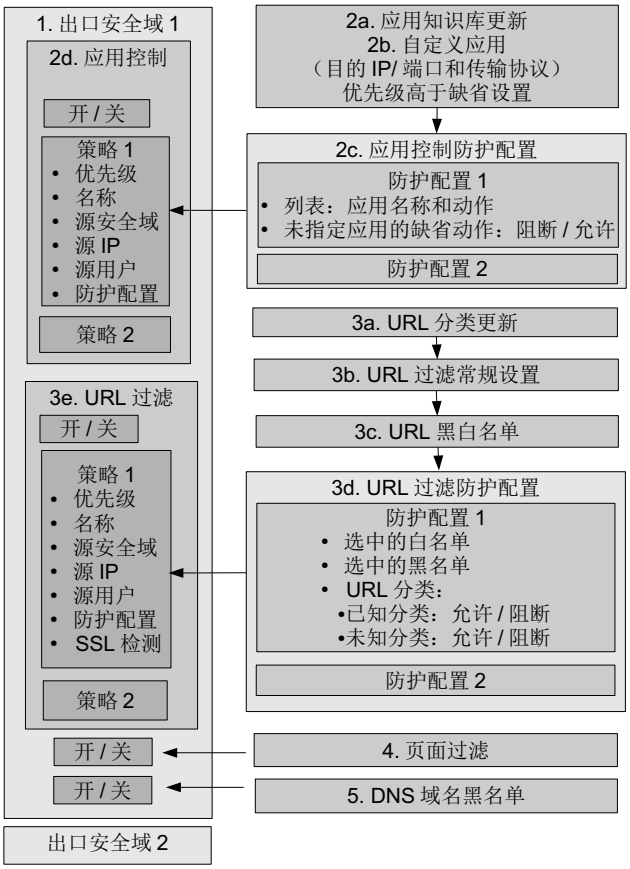
本节描述以下功能的基本配置步骤：

- 12.2.1 出口控制
- 12.2.2 客户端防护
- 12.2.3 服务器防护
- 12.2.4 SSL 检测
- 12.2.5 通知消息
- 12.2.6 概要信息页面

提示：IPS 只能通过 WebUI 进行配置，不支持 CLI。

12.2.1 出口控制

图 17 出口控制配置步骤



基本设置：

- 12.2.1.1 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

出口控制配置：

- 12.2.1.2 配置应用控制：
  - 12.2.1.2.1 更新应用知识库 （2a）
  - 12.2.1.2.2 添加自定义应用 （2b）
  - 12.2.1.2.3 创建应用控制防护配置 （2c）
  - 12.2.1.2.4 创建应用控制策略 （2d）
- 12.2.1.3 配置 URL 过滤：
  - 12.2.1.3.1 更新 URL 分类库 （3a）
  - 12.2.1.3.2 配置 URL 过滤常规设置 （3b）
  - 12.2.1.3.3 创建 URL 过滤防护配置：黑白名单 （3c）
  - 12.2.1.3.4 创建 URL 过滤防护配置 （3d）
  - 12.2.1.3.5 创建 URL 过滤策略 （3e）
- 12.2.1.4 配置页面过滤
- 12.2.1.5 配置 DNS 域名黑名单

12.2.1.1 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

出口控制用于控制出口安全域上的流量。根据需要创建安全域、访问策略、缺省路由和 NAT 规则。详细信息请参见 4.6 安全域，10.2.1 创建访问策略，5.1.1 缺省路由和 8.2.1 创建 SNAT 规则。

1. 选择**网络** > **安全域**，创建安全域（至少创建一个出口安全域）。下图中 LAN 是入口安全域， WAN 是出口安全域。

2. 选择**防火墙** > **访问策略**，创建访问策略允许内网到外网的访问。

3. 选择**网络** > **路由** > **缺省路由**，根据需要添加缺省路由。

4. 如果 NISG-IPS 工作在路由模式，选择**网络** > **地址转换** > **源地址转换**，添加如下源地址转换规则：

12.2.1.2 配置应用控制

12.2.1.2.1 更新应用知识库 （2a）

详细信息请参见 12.3.1.2.4 （应用知识库）更新。

1. 选择 **IPS**> **出口控制** > **应用控制** > **更新**。

2. 根据需要选择手动更新或从 Internet 更新。

12.2.1.2.2 添加自定义应用 （2b）

详细信息请参见 12.3.1.2.3 应用知识库和 12.3.1.2.2 自定义应用。

1. 选择 **IPS> 出口控制 > 应用控制 > 应用知识库**。
2. 根据分类、技术、风险等级和 / 或应用名称查找应用。当鼠标指向应用名称时，会出现该应用的描述信息。

3. 选择 **IPS> 出口控制 > 应用控制 > 自定义应用**。
4. 根据需要添加自定义应用，自定义条件主要包括 IP 地址、协议和端口。

提示：添加页面**应用**下拉框支持自动补齐。例如，如果您输入字母 G，下拉框将显示所有名称以 G 开头的应用供您选择。

12.2.1.2.3 创建应用控制防护配置 （2c）

详细信息请参见 12.3.1.2.1 （应用控制）防护配置。

1. 选择 **IPS> 出口控制 > 应用控制 > 防护配置**。
2. 点击**新建**创建防护配置。通过过滤条件或应用名称添加应用，**应用**下拉列表框输入支持自动补齐。

3. 点击**确定**，将应用添加到新建防护配置中。

应用条目的匹配流程如下：

a. 如果匹配到**应用列表**中的应用条目，则 NISG-IPS 将按照指定的动作对应用及其所属会话进行处理；
b. 如果未匹配到**应用列表**中的应用条目，则 NISG-IPS 根据指定的未知应用缺省处理动作进行处理。

提示：当 NISG-IPS 无法识别某项应用，即应用不在应用知识库中时，则应用及其所属会话将被放行。

---

4. 点击**确定**，查看新建防护配置。可点击 克隆已有防护配置。

12.2.1.2.4 创建应用控制策略 （2d）

详细信息请参见 12.3.1.1.1 应用控制策略。

1. 选择 **IPS**> **出口控制** > **策略**。
2. 选择出口安全域，开启应用控制功能。

3. 点击**应用控制**展开配置区域，点击**新建**，创建应用控制策略。

4. 点击**确定**。

12.2.1.3 配置 URL 过滤

12.2.1.3.1 更新 URL 分类库 （3a）

详细信息请参见 12.3.1.3.4 （URL 分类）更新。

1. 选择 **IPS> 出口控制 >URL 过滤 > 更新**。

2. 根据需要选择手动更新或从 Internet 更新。

12.2.1.3.2 配置 URL 过滤常规设置 （3b）

详细信息请参见 12.3.1.3.1 （URL 过滤）常规设置。

1. 选择 **IPS> 出口控制 >URL 过滤 > 常规设置**，设置 URL 过滤引擎失败时的动作。

2. 点击**确定**。
3. 根据需要查询 URL 分类。

12.2.1.3.3 创建 URL 过滤防护配置：黑白名单 （3c）

详细信息请参见 12.3.1.3.3 URL 黑白名单。

1. 选择 **IPS> 出口控制 >URL 过滤 > 黑白名单**。
2. 点击**新建**，创建 URL 白名单：

3. 点击**确定**。
4. 点击**新建**，创建 URL 黑名单。

5. 点击**确定**，查看新建防护配置。可点击 克隆已有黑白名单。

12.2.1.3.4 创建 URL 过滤防护配置 （3d）

详细信息请参见 12.3.1.3.2 （URL 过滤）防护配置。

1. 选择 **UT> 出口控制 >URL 过滤 > 防护配置**。
2. 点击**新建**，创建 URL 过滤防护配置。

URL 过滤匹配流程如下 （优先级从高到低）：

a. 如果匹配到白名单条目，则用户访问将被放行；

b. 如果匹配到黑名单条目，则用户访问将被阻断；

c. 如果匹配到 URL 分类，则 NISG-IPS 根据分类动作放行或阻断访问；

d. 如果未匹配到任何URL分类，则NISG-IPS根据未知URL分类缺省动作放行或阻断访问。

3. 点击**确定**，查看新建防护配置。可点击 克隆已有防护配置创建新的防护配置。

12.2.1.3.5 创建 URL 过滤策略 （3e）

详细信息请参见 12.3.1.1.2 URL 过滤策略。

1. 选择 **IPS> 出口控制** > **策略**。
2. 选择出口安全域，开启 URL 过滤功能。

3. 点击 **URL 过滤**展开配置区域，点击**新建**，创建 URL 过滤策略。

开启 HTTPS 检测时， NISG-IPS 能够对基于加密的 HTTP 协议的 URL 进行过滤检测。

4. 点击**确定**。

12.2.1.4 配置页面过滤

详细信息请参见 12.3.1.5 页面过滤。

1. 选择 **IPS> 出口控制 > 页面过滤**。
2. 配置页面过滤功能阻断含有指定关键字的 HTTP 响应页面。

3. 点击**确定**。
4. 选择 **IPS> 出口控制 > 策略**。
5. 选择出口安全域，开启页面过滤功能。

12.2.1.5 配置 DNS 域名黑名单

详细信息请参见 12.3.1.4 DNS 域名黑名单。

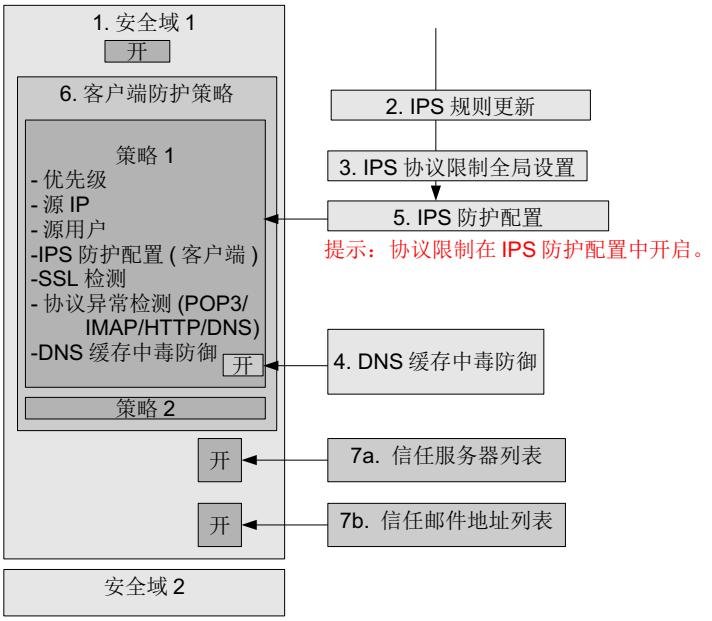
1. 选择 **IPS> 出口控制 >DNS 域名黑名单**。
2. 配置 DNS 域名黑名单。

3. 点击**确定**。
4. 选择 **IPS> 出口控制** > **策略**。
5. 选择出口安全域，开启 DNS 域名黑名单功能。

12.2.2 客户端防护

客户端配置步骤如下图所示：

图 18 客户端防护配置步骤



基本设置：

- 12.2.2.1 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

整体更新 （IPS 规则更新）：

- 12.2.2.2 更新 IPS 规则

常规设置：

- 12.2.2.3 配置 IPS SMTP/POP3/IMAP/DNS 协议限制 （客户端）
- 12.2.2.4 配置 DNS 缓存中毒防御

防护配置：

- 12.2.2.5 创建 IPS 防护配置

策略 / 信任服务器与邮件：

- 12.2.2.6 创建客户端防护策略
- 12.2.2.7 创建信任服务器 / 邮件列表

12.2.2.1 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

1. 选择**网络** > **安全域**，创建客户端防护安全域。详细信息请参见 4.6 安全域。

   提示：开启客户端防护的安全域应该包含与内网受保护客户端相连的接口。

2. 选择**防火墙** > **访问策略**，创建访问策略。详细信息请参见 10.2.1 创建访问策略。
3. 选择**网络** > **路由** > **缺省路由**，修改缺省路由。详细信息请参见 5.1.1 缺省路由。
4. 如果 NISG-IPS 工作在路由模式，选择**网络** > **地址转换** > **源地址转换**，添加源地址转换规则。详细信息请参见 8.2.1 创建 SNAT 规则。

12.2.2.2 更新 IPS 规则

- 12.2.2.2.1 更新攻击签名规则

12.2.2.2.1 更新攻击签名规则

更新攻击签名规则库。详细信息请参见 12.3.4.3 （攻击签名规则）更新。

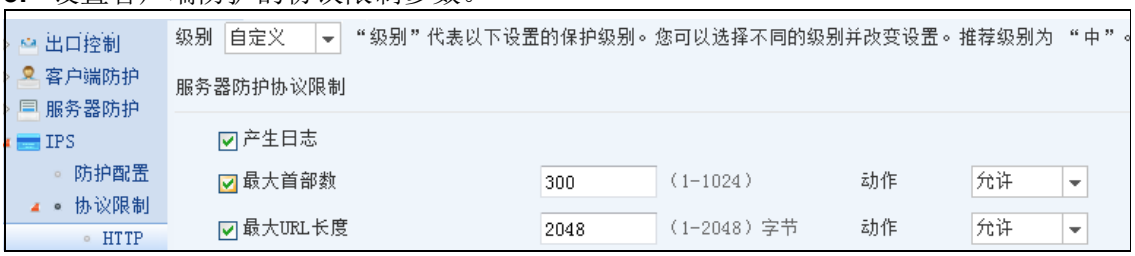
1. 选择 **IPS>IPS> 更新**。
2. 根据需要手动更新或从 Internet 更新。

12.2.2.3 配置 IPS SMTP/POP3/IMAP/DNS 协议限制 （客户端）

IPS 协议限制的基本内容如下：

- **类型**：HTTP、 SMTP、 POP3、 IMAP 和 DNS
- **级别**：低、中、高和自定义 （只有最后选中的级别生效。）
- **服务器端协议限制**：HTTP、 SMTP、 POP3、 IMAP 和 DNS
- **客户端协议限制**：SMTP、 POP3、 IMAP 和 DNS

1. 选择协议限制类型（客户端类型的 IPS 防护配置中可以选择 SMTP、POP3、IMAP 和 DNS）。例如选择 **IPS>IPS> 协议限制 >HTTP**。
2. 选择协议限制级别 （如选择**高**级别）。
3. 设置客户端防护的协议限制参数。

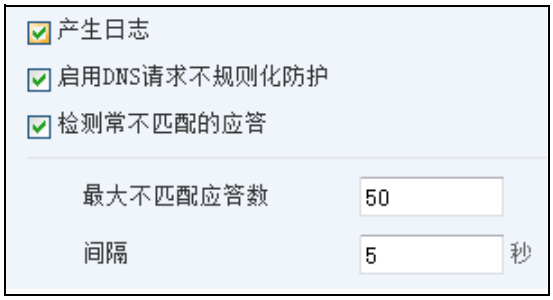


4. 点击**确定**。
5. 选择 **IPS>IPS> 防护配置**，在客户端 IPS 防护配置中启用协议限制。

12.2.2.4 配置 DNS 缓存中毒防御

设置 DNS 缓存中毒防御。详细信息请参见 12.3.2.4 DNS 缓存中毒防御。

1. 选择 **IPS> 客户端防护 >DNS 缓存中毒防御**。



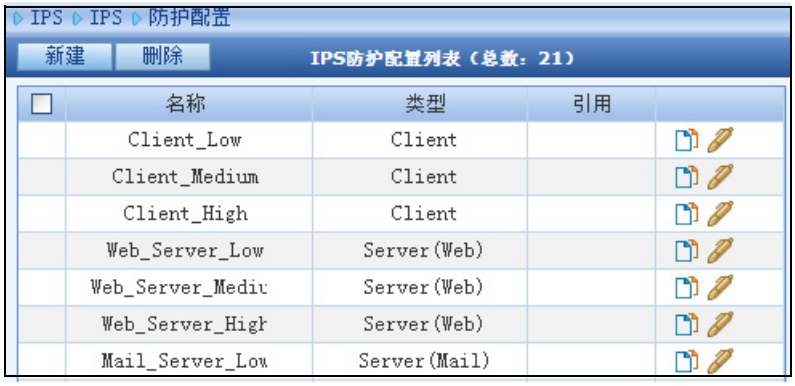
2. 点击**确定**。

12.2.2.5 创建 IPS 防护配置

- 12.2.2.5.1 查看缺省 IPS 防护配置 （概要）
- 12.2.2.5.2 创建 IPS 防护配置
- 12.2.2.5.3 启用 / 配置协议限制

12.2.2.5.1 查看缺省 IPS 防护配置 （概要）

1. 选择 **IPS>IPS> 防护配置。**
2. 查看缺省的 IPS 防护配置：



3. 点击缺省防护配置名称查看设置。

提示：将鼠标指向规则列表中的参数名称，会出现一个 ▼ 按钮，点击设置要显示的参数。

4. 下图表明了在客户端 / 服务器防护策略中如何选择 IPS 防护配置。

12.2.2.5.2 创建 IPS 防护配置

IPS 防护配置的基本配置内容如下：

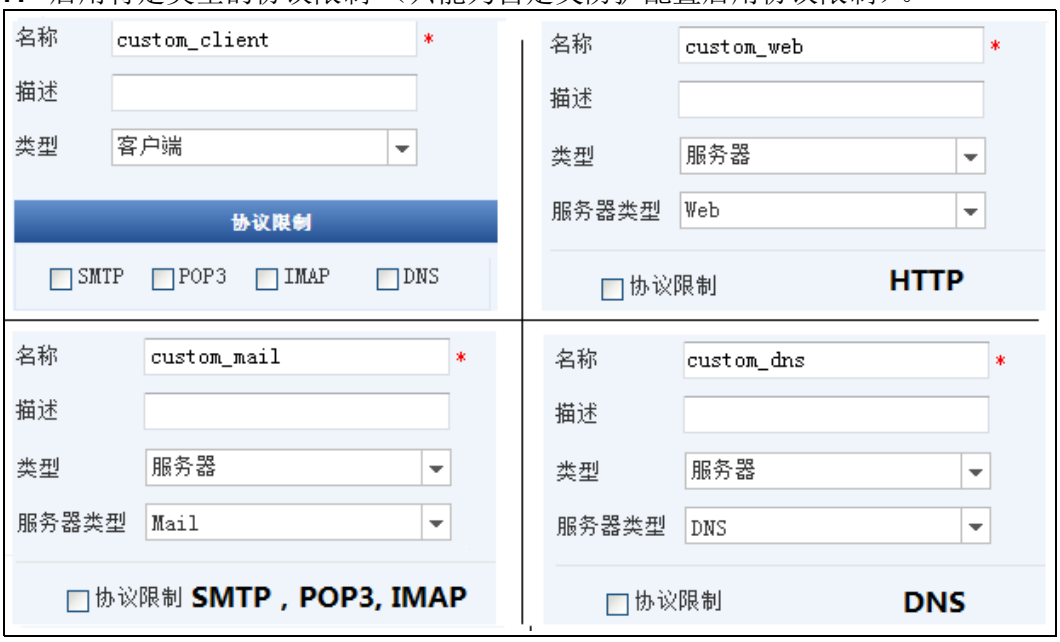
- **名称**：用于在客户端 / 服务器防护策略中选择防护配置
- **类型**：服务器 / 客户端
- **服务器类型**：Web/Mail/FTP/Telnet/DNS/ 其他
- **协议限制**：HTTP/SMTP/POP3/IMAP/DNS （只能在自定义防护配置中启用 / 禁用。）
- **攻击签名规则**：启用 / 禁用，允许 / 阻断

5. 点击 拷贝防护配置或点击**新建**创建新的防护配置。

6. 在攻击签名规则列表中，为防护配置指定要启用的规则和规则动作（允许 / 阻断）。

12.2.2.5.3 启用 / 配置协议限制

7. 启用特定类型的协议限制 （只能为自定义防护配置启用协议限制）。



12.2.2.6 创建客户端防护策略

创建客户端防护策略。详细信息请参见 12.3.2 客户端防护。

1. 选择 **IPS**> **客户端防护** > **策略**。
2. 选择入口安全域，为其开启客户端防护策略。

3. 点击**客户端防护策略列表**上方的**新建**按钮，创建客户端防护策略：

   a. 输入策略基本信息，设置受保护客户端的 IP 地址。

   开启 HTTPS 检测时，NISG-IPS 能够对客户端从 Web 服务器下载的 HTTPS 流量进行协议异常检测及 IPS 检测。具体配置，参见步骤 b 和步骤 d。

   b. 选择 IPS 检测级别并设置 IPS 防护配置。

c. 为 Mail 客户端流量设置最大受保护邮件大小，设置协议异常检测。

d. 为 HTTP/HTTPS 下载流量设置协议异常检测。

e. 为DNS客户端流量开启DNS缓存中毒防御功能，并设置协议异常检测处理动作。

4. 点击**确定**。

12.2.2.7 创建信任服务器 / 邮件列表

创建信任服务器列表。详细信息请参见 12.3.2.2 （客户端防护）信任服务器列表。

1. 选择 **IPS> 客户端防护 > 策略 > 信任服务器列表**。
2. 启用信任服务器列表，点击其后的空白区域展开列表。
3. 配置信任服务器列表。

创建信任邮件地址列表。详细信息请参见 12.3.2.3 （客户端防护）信任邮件地址列表。

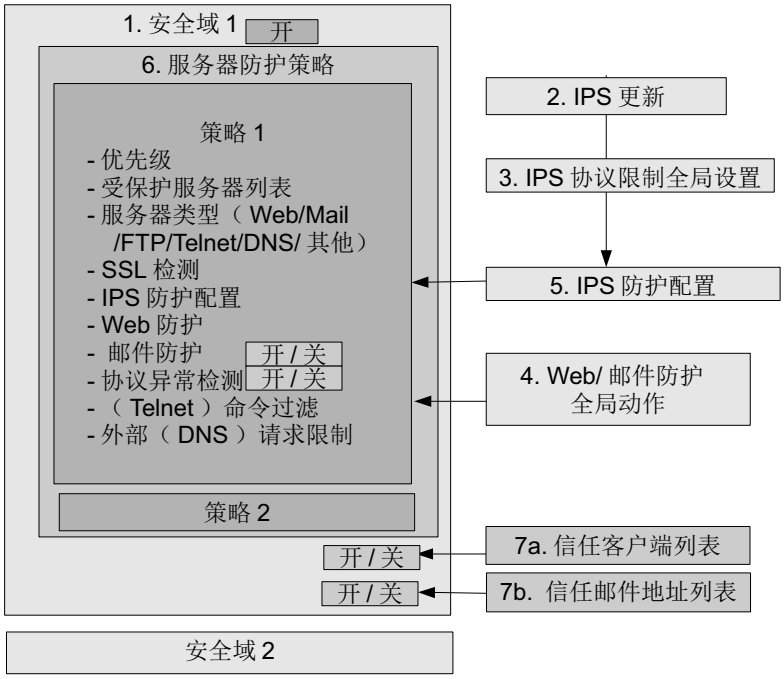
4. 选择 **IPS> 客户端防护 > 策略 > 信任邮件地址列表**。
5. 启用信任邮件地址列表。
6. 配置信任邮件地址列表。可以删除 / 编辑列表条目，方法同信任服务器列表。

对于匹配上述信任服务器和邮件列表的流量， NISG-IPS 将对其直接放行，不进行客户端防护检测。

12.2.3 服务器防护

服务器防护的配置步骤如下图所示：

图 19 服务器防护配置步骤



基本设置：

- 12.2.3.1 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

整体更新 （IPS 规则更新）：

- 12.2.3.2. 更新 IPS 规则

常规设置：

- 12.2.3.3. 配置 IPS 协议限制 （HTTP/SMTP/POP3/IMAP/DNS 服务器）
- 12.2.3.4 配置 Web/ 邮件防护

防护配置：

- 12.2.3.5 创建 IPS 防护配置

策略 / 信任客户端 / 邮件：

- 12.2.3.6 创建服务器防护策略
- 12.2.3.7 创建信任客户端 / 邮件列表

12.2.3.1 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

同客户端防护，参见 12.2.2.1 创建安全域 / 访问策略 / 缺省路由 /NAT 规则。

提示：开启服务器防护功能的安全域应该包含与内网服务器相连的接口。

12.2.3.2. 更新 IPS 规则

同客户端防护，参见 12.2.2.2 更新 IPS 规则。

12.2.3.3. 配置 IPS 协议限制 （HTTP/SMTP/POP3/IMAP/DNS 服务器）

关于客户端防护的协议限制配置，请参见 12.2.2.3 配置 IPS SMTP/POP3/IMAP/DNS 协议限制 （客户端）。

1. 选择协议限制类型（服务器类型的 IPS 防护配置中可以选择 HTTP、 SMTP、 POP3、 IMAP 和 DNS）。例如，选择 **IPS**>**IPS**> **协议限制** >**SMTP**。
2. 选择协议限制级别 （如选择**高**级别协议限制）。
3. 设置服务器防护的协议限制参数。
4. 点击**确定**。

   提示：最后选择的级别即生效级别。

5. 选择相应的服务器 IPS 防护配置，并在 IPS 防护配置中启用协议限制。

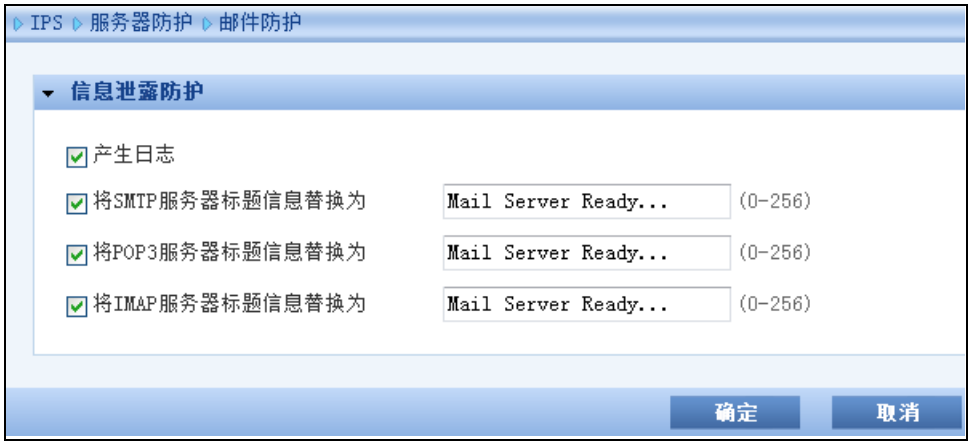
12.2.3.4 配置 Web/ 邮件防护

设置 Web 防护。详细信息请参见 12.3.3.4 Web 防护。

1. 选择 **IPS**> **服务器防护** >**Web 防护**。
2. 分别启用 / 禁用**信息泄露防护**的各项功能 （首部置换、隐藏错误信息及目录列表检测），整体启用 / 禁用记录日志功能。
3. 点击**注入攻击防御**，配置相关信息，包括跨站脚本攻击防御、 SQL 注入攻击防御、LDAP 注入攻击防御以及命令注入攻击防御。
4. 点击**确定**。

设置邮件防护。详细信息请参见 12.3.3.5 邮件防护。

5. 选择 **IPS**> **服务器防护** > **邮件防护**。
6. 启用 / 禁用邮件防护功能和记录日志功能。



7. 点击**确定**。

12.2.3.5 创建 IPS 防护配置

同客户端防护，详细信息请参见 12.2.2.5 创建 IPS 防护配置。

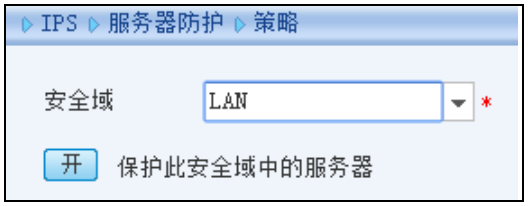
1. 服务器类型的防护配置如下所示：

2. 点击 按钮，查看缺省防护配置。
3. 点击 按钮，通过拷贝和编辑缺省防护配置创建新的防护配置。

12.2.3.6 创建服务器防护策略

详细信息请参见 12.3.3 服务器防护。

1. 选择 **IPS**> **服务器防护** > **策略**。
2. 选择入口安全域并为其开启服务器防护策略。



3. 点击**新建**创建 Web 服务器防护策略，并在策略中开启 Web 防护。

开启 HTTPS 检测时， NISG-IPS 能够对 Web 服务器的 HTTPS 流量进行如下检测：IPS、协议异常和 Web 防护。

4. 点击**确定**。

5. 点击**新建**创建邮件服务器防护策略，并在策略中开启邮件防护。

6. 点击**确定**。

7. 创建 FTP 服务器防护策略。

8. 点击**确定**。

9. 创建 Telnet 服务器防护策略。

10. 点击**确定**。

12.2.3.7 创建信任客户端 / 邮件列表

创建信任客户端列表，详细信息请参见 12.3.3.2 （服务器防护）信任客户端列表。

1. 选择 **IPS> 服务器防护 > 策略**。
2. 启用并配置信任客户端列表。

创建信任邮件地址列表。配置步骤同客户端防护，请参见 12.2.2.7 创建信任服务器 / 邮件列表。配置参数信息请参见 12.3.3.3 （服务器防护）信任邮件地址列表。

12.2.4 SSL 检测

NISG-IPS 能够对 HTTPS 流量进行 SSL 加解密和深度检测。管理员需要进行如下配置：

在下列策略中开启 SSL 检测功能：

- URL 过滤：参见 12.2.1.3.5 创建 URL 过滤策略 （3e）。
- 客户端防护：参见 12.2.2.6 创建客户端防护策略。
- 服务器防护：参见 12.2.3.6 创建服务器防护策略。

在上述策略中开启 SSL 检测后，管理员可以配置 SSL 检测证书策略，指定 SSL 检测所使用的证书。

1. 选择 **IPS** > **SSL 检测**，点击**新建**，创建 SSL 检测证书策略。

2. 管理员可以使用以下两种类型的证书进行 SSL 检测。
   - 使用系统默认证书。

   - 选择一个具有证书颁发功能的本地证书。

提示：要导入本地证书，点击**查看**页面底部的**导入本地证书**超链接进入**系统** > **证书** > **本地证书**页面。更多信息，请参见 3.28 证书。

这两种类型的证书都可以用于：

- **证书颁发**：作为 CA 证书颁发仿冒证书，适用于管理员无法获取服务器证书的情况。
- **解密**：直接用于解密来自客户端的 SSL 数据，适用于管理员拥有服务器证书的情况。

提示：在使用本地证书的证书颁发功能时，建议用户手动将防火墙的 SSL 证书导入到本地主机浏览器端。

3. 点击**删除**、**启用**或**禁用**来删除、启用或禁用 SSL 检测证书策略，点击和分别编辑和移动策略。通过移动策略，可以改变序号，进而改变策略的优先级。

	序号	名称	目的IP/域名	协议	目的端口	证书名称	用于	启用	
☐	1	sslcert1	Any	TCP	1-65535	Default System Certificate	证书颁发	✔	
☐	32	Default	Any	Any	1-65535	Default System Certificate	证书颁发	✔	

提示：缺省策略 “Default” 不可以删除或移动。

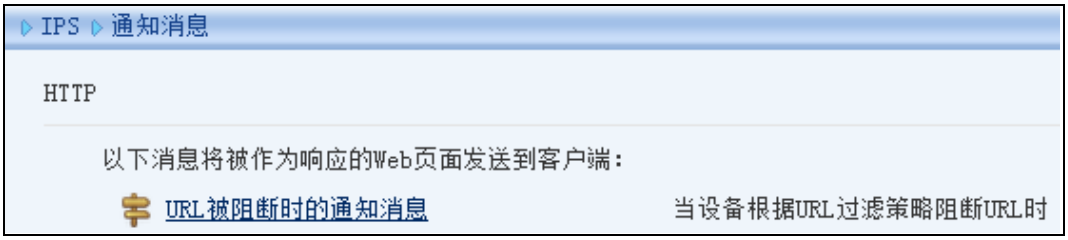
12.2.5 通知消息

通知消息分为两类：

- **系统预定义通知消息**：不可修改。用户只能在收到某些事件的通知消息时才会看到。
- **用户自定义通知消息**：可通过 WebUI 进行配置。

详细信息请参见 12.3.6 通知消息。

1. 选择 **IPS**> **通知消息**。



2. 点击链接编辑通知消息显示内容。

3. 点击**是**。

12.2.6 概要信息页面

概要信息页面给出了所有安全域的 IPS 信息。 IPS 策略应用域安全域。

1. 选择 **IPS**> **概要信息**查看所有安全域的 IPS 信息。

2. 点击本页面图标到相应的页面进行配置。

12.3 配置参数说明

本节列出以下 IPS 功能的配置参数：

12.3.1 出口控制

出口控制用于在出口安全域上对用户流量进行安全检查。本节包含以下内容：

12.3.1.1 出口控制策略

出口控制策略包括：

- **策略**：配置应用控制策略和 URL 过滤策略。
- **开关**：启用或禁用 DNS 域名黑名单和页面过滤功能。

12.3.1.1.1 应用控制策略

应用控制策略定义了哪些应用将进行安全检测，管理员可以在指定的安全域上开启或关闭应用控制功能。

表 183 应用控制策略参数

参数	说明
开 / 关	在指定的安全域上启用或禁用应用控制功能。
序号	应用控制策略的优先级，序号越小，优先级越高。取值范围为 1-80000。
名称	应用控制策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
源安全域	发起应用访问的内网用户所在的安全域。
源 IP	内网用户访问应用所使用的 IP 地址： • **任意** • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户自定义 IP 地址，最多支持 4096 个 IP 地址或 IP 地址段。 IPv4 和 IPv6 地址不可同时添加。
源用户	发起应用访问的内网用户： • **任意** • **任意认证用户** • **使用下表**：可以包括未在 NISG-IPS 上创建的、在外部认证服务器上认证的用户。 每条策略最多支持 4096 个源用户。
防护配置	显示应用控制策略所引用的防护配置名称。应用控制防护配置列出策略所限制的应用，并指明对应用执行的动作。
日志	对匹配访问控制策略的流量启用或禁用日志功能。
启用	启用或禁用应用控制策略。

提示：要查看应用控制的监控信息，选择**监控** > **报警 / 日志** > **应用控制报警**。

12.3.1.1.2 URL 过滤策略

NISG-IPS 提供出口安全域的 URL 过滤功能，对用户要访问的 URL 进行过滤控制。URL 过滤策略定义哪些 URL 允许访问、哪些 URL 禁止访问。管理员可以在指定的安全域上开启或关闭 URL 过滤功能。

表 184 URL 过滤策略参数

参数	说明
开 / 关	在指定的安全域上开启或关闭 URL 过滤功能。
序号	URL 过滤策略的优先级，序号越小，优先级越高。取值范围为 1-80000。
名称	URL 过滤策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\ < > & #
源安全域	发起 URL 访问的内网用户所在的安全域。
源 IP	内网用户访问 URL 所使用的 IP 地址： • **任意** • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户自定义 IP 地址，最多支持 4096 个 IP 地址或 IP 地址段。
源用户	发起 URL 访问的内网用户： • **任意** • **任意认证用户** • **使用下表**：可以选择包括未在 NISG-IPS 上创建的、在外部认证服务器上认证的用户。 每条策略最多支持 4096 个源用户。
防护配置	显示引用的防护配置名称。
日志	显示日志功能是否启用。对匹配 URL 过滤策略的流量启用或禁用日志功能。
开启 HTTPS 检测	启用或禁用对 HTTPS 流量的 SSL 检测功能。
启用	启用或禁用 URL 过滤策略。

提示：要查看 URL 过滤的监控信息，选择**监控** > **报警 / 日志** >**URL 过滤报警**。

12.3.1.2 应用控制

应用控制过滤出口应用流量。本节包含以下内容：

提示：要查看应用控制的监控信息，选择**监控** > **报警 / 日志** > **应用控制报警**。

12.3.1.2.1 （应用控制）防护配置

应用控制防护配置定义了 NISG-IPS 要进行控制的应用及每个应用的处理动作。所有虚拟系统最多支持 1024 个应用控制防护配置，每个防护配置最多支持 4096 个应用或应用分类。

表 185 应用控制防护配置参数

参数	说明
名称	应用控制防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？,"'\<>&#
引用	点击 查看引用防护配置的应用控制策略。 一个应用控制防护配置可以被多条策略引用，被应用控制策略引用的应用控制防护配置不能被删除。
描述	应用控制防护配置的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：？"′ \<>&
不在下表中的应用的缺省处理动作	包括**阻断**和**放行**。
应用列表	添加要控制的应用，最多添加 256 个条目。 • **序号**：应用规则的匹配顺序，序号越小，越先匹配。如果新建防护配置的序号已经存在，则新建防护配置将被插入已有防护配置的前面。 • **类型**：包括指定应用和指定应用的过滤条件。可通过指定应用过滤条件批量添加应用，也可以通过指定应用名称添加单个应用。 • **应用名称**：应用的名称或过滤条件。 • **动作**：对匹配到应用列表的应用的处理动作，包括**阻断**和**放行**。

12.3.1.2.2 自定义应用

NISG-IPS 允许管理员基于某些匹配条件自定义应用，以提高应用数据的转发速率。自定义应用通过指定目的 IP 地址、传输层协议和目的端口来进行特殊的应用控制，其优先级高于 NISG-IPS 的预定义应用。

表 186 自定义应用参数

参数	说明
应用	进行自定义匹配条件的应用，可以是应用知识库中的任意应用。
应用协议	应用使用的应用层协议，如 DNS 和 FTP。 一条自定义应用只能指定一个应用协议。
目的 IP	自定义应用数据包的目的 IP 地址（IPv4 或 IPv6）。
传输协议	自定义应用使用的传输层协议，包括 TCP 和 UDP。
目的端口	自定义应用数据包的目的端口号，取值范围为 1~65535。

12.3.1.2.3 应用知识库

应用知识库中列出了 NISG-IPS 能够识别的所有 RFC 标准应用，包括应用的名称、分类、子分类、所用技术以及风险等级。管理员可以查看所有应用或查询特定应用。

表 187 应用知识库参数

参数	说明
分类	应用知识库中预定义应用的分类，如交际类应用。 Any 表示任意分类。
子分类	预定义应用分类对应的子分类，如内容共享和认证服务。 Any 表示任意子分类。
技术	预定义应用使用的技术，如基于浏览器类、点对点类。 Any 表示任意技术。
风险	预定义应用的风险等级，由低到高分为 5 种级别，如  、  、  、  和  。 Any 表示任意级别。
清空过滤条件	重置过滤条件并清空查询结果。
查找	查找特定的应用。输入应用的名称，点击**查找**，则匹配该名称的特定应用将在下方列表显示。查找功能支持模糊匹配。
查找结果	显示匹配到过滤条件的应用。 将鼠标指向应用名称可以查看该应用的描述信息。

12.3.1.2.4 （应用知识库）更新

应用知识库规则支持手动和自动两种更新方式。规则升级包上载后立即生效，不需要重启。应用知识库更新不提供升级回退的功能。

应用知识库更新限制条件如下：

- License

  应用控制功能和应用知识库更新受 APPUP License 的限制。

- 虚拟系统

  NISG-IPS 只允许在根系统 （root）中进行应用知识库的更新操作，所有虚拟系统共享应用知识库更新后的结果。

表 188 应用知识库更新历史参数

参数	说明
规则库	应用知识库名称，固定为 Application-Control。
规则版本	应用知识库的最新版本。
引擎版本	应用知识库所对应的引擎版本。
上次更新时间	当前应用知识库上次更新时间。
显示 / 导出更新历史记录	点击查看或导出应用知识库的更新历史记录。 NISG-IPS 最多支持 50 条记录。

表 189 应用知识库更新模式参数

参数	说明
更新服务器地址	更新服务器的 URL 地址，可以为 IPv4/v6 地址或者域名。 缺省为 nts.neusoft.com/autoupdate。
更新模式	自动更新模式，包括**自动安装更新**和**从不检查更新**。
时间表	NISG-IPS 自动下载并安装升级包的定时更新时间。 • 当选择**每天**、**每周**或**每月**时，系统会在指定时间点后两个小时内随机开始升级。 • 当选择**间隔**时，系统将按照设定时间间隔进行规则更新。
立即更新	当更新服务器地址和更新内容配置成功后，点击**立即更新**， NISG-IPS 立即从指定的更新服务器上获取升级包并执行安装。
手动上载升级包	上传本地的应用知识库更新包。

12.3.1.3 URL 过滤

URL 过滤功能控制用户对 URL 的访问。本节包含以下内容：

提示：要查看 URL 过滤的监控信息，选择**监控** > **报警 / 日志** >**URL 过滤报警**。

12.3.1.3.1 （URL 过滤）常规设置

表 190 URL 过滤常规设置参数

参数	说明
当 URL 过滤引擎扫描失败时	当 URL 过滤引擎扫描失败时， NISG-IPS 将执行的动作，包括**允许**和**阻断**。
URL 分类查询	管理员可以输入要查询的 URL，点击**查找**按钮，查看 URL 分类。

12.3.1.3.2 （URL 过滤）防护配置

URL 过滤防护配置指定以下内容 （优先级从高到低）：

1. 一个白名单
2. 一个黑名单
3. URL 分类，包括：
   a. 指定 URL 分类的动作；
   b. 未知分类 URL 的缺省动作 （允许 / 阻断）。

所有虚拟系统最多可添加 1024 个 URL 过滤防护配置。

表 191 URL 过滤防护配置参数

参数	说明
名称	URL 过滤防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\ < > & #
引用	点击 查看引用 URL 过滤防护配置的策略。 一个 URL 过滤防护配置可以被多个 URL 过滤策略引用，且被引用的防护配置不能被删除。
描述	URL 过滤防护配置的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? "'\< > &
URL 白名单	勾选并选择 URL 白名单。如果匹配白名单，则允许用户访问。
URL 黑名单	勾选并选择 URL 黑名单。如果匹配黑名单，则拒绝用户访问。
URL 分类	开启 URL 分类过滤功能。 • **未知分类 URL 的缺省处理动作**：包括**允许**和**阻断**。 • **URL 分类列表**：NISG-IPS 对于已知分类的 URL，将根据用户指定动作允许或禁止对其访问；被禁用的 URL 分类， NISG-IPS 将直接放行。

12.3.1.3.3 URL 黑白名单

URL 白名单定义了用户可以访问的 URL， URL 黑名单则定义了用户不可以访问的 URL。 URL 黑白名单被 URL 过滤防护配置引用。当一个 URL 请求到达 NISG-IPS 时，首先进行白名单的匹配，再进行黑名单的匹配。如果黑白名单存在冲突，则以白名单为准优先处理。每个虚拟系统最多可添加 8 个 URL 黑名单和 8 个 URL 白名单。

表 192 URL 黑白名单参数

参数	说明
名称	URL 黑名单或者白名单的名称，不可重名。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
类型	URL 黑白名单对应的类型，包括黑名单和白名单。
条目数	URL 黑白名单包含的 URL 条目数。
引用	点击 查看引用 URL 黑白名单的防护配置。一个 URL 黑白名单可以被多个防护配置引用。
描述	URL 黑白名单的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? " ′ \<> &
URL 列表	向新建 URL 黑白名单中添加 URL 条目。 • **URL**：可以为 IP 地址或域名，支持通配符，取值范围为 2 ～ 255 字节。 • **描述**：长度 0~255 字节， UTF-8 字符。不能包含以下字符：？ " ' \ < > & • **启用**：启用 / 禁用 URL 条目。
导入	导入 URL 黑白名单，重名的黑白名单不允许导入。 导入文件的要求如下： • **文件类型**：文本文件。 • **文件格式**：每行一个 URL 地址。 • **文件扩展名**：.txt。

12.3.1.3.4 （URL 分类）更新

URL 分类支持手动和自动两种更新方式。规则升级包上载后立即生效，不需要重启。URL 分类更新不提供升级回退的功能。

URL 分类更新限制如下：

- License

  URL 分类更新受 UFOL License 的限制。

- 虚拟系统

  NISG-IPS 只允许在根系统 （root）中进行 URL 过滤规则更新操作，所有虚拟系统共享 URL 过滤规则更新后的结果。

表 193 URL 过滤规则更新历史参数

参数	说明
规则库	URL 过滤规则库名称，固定为 URL Filtering。
规则版本	URL 过滤规则库的最新版本。
引擎版本	URL 分类所对应的引擎版本。
上次更新时间	当前 URL 分类上次更新时间。
显示 / 导出更新历史记录	用于查看或导出 URL 分类的更新历史记录。 NISG-IPS 最多支持 50 条记录。

表 194 URL 过滤规则更新模式参数

参数	说明
更新服务器地址	URL 分类更新服务器的 URL 地址，可以为 IPv4/v6 地址或者域名。 缺省为 nts.neusoft.com/urlrule。
更新模式	自动更新模式，包括**自动安装更新**和**从不检查更新**。
时间表	NISG-IPS 自动下载并安装升级包的定时更新时间。 • 当选择**每天**、**每周**或**每月**时，系统会在指定时间点后两个小时内随机开始升级。 • 当选择**间隔**时，系统将按照设定时间间隔进行规则更新。
立即更新	当更新服务器地址和更新内容配置成功后，点击**立即更新**， NISG-IPS 立即从指定的更新服务器上获取升级包并执行安装。
手动上载升级包	上传本地的 URL 过滤规则更新包。

12.3.1.4 DNS 域名黑名单

IPS 在网络出口安全域上对用户的 DNS 请求进行限制，阻断匹配黑名单的域名解析请求。管理员需要在**出口控制 > 策略**页面中为安全域开启 DNS 域名黑名单功能，其相应配置才会生效。

表 195 DNS 域名黑名单参数

参数	说明
产生日志	启用 DNS 域名黑名单的日志功能。
域名黑名单	配置项包括： • **域名**：发往该域名的 DNS 请求将被丢弃。最多可添加 2048 个域名条目。 • **模糊匹配**：阻断域名部分匹配黑名单的 DNS 请求。 • **启用**：启用 / 禁用域名黑名单条目。

提示：要查看 DNS 域名黑名单的监控信息，选择**监控** > **报警 / 日志** >**IPS 报警**。

12.3.1.5 页面过滤

页面过滤应用于出口安全域，用于过滤包含管理员指定的关键字的 Web 页面。管理员需要在**出口控制 > 策略**页面中为安全域开启页面过滤功能，其相应配置才会生效。

表 196 页面过滤参数

参数	说明
分数阈值	当检测到的 Web 页面上关键字的分数总合超过分数阈值时， NISG-IPS 将按照管理员配置的动作进行处理。
当 Web 页面上的关键字总分超过分数阈值时	包括**允许**和**阻断**。
产生日志	启用页面过滤的日志功能。
关键字过滤	关键字过滤规则列表，最大条目数 4096。 • **关键字**：对 Web 页面内容进行过滤的字符串，允许输入 UTF-8 字符，不区分大小写，取值范围为 2 ～ 32 字节。 • **分值**：对 Web 页面内容进行关键字检测时，每检查到一次与关键字相符的字符串所加的分值。取值范围为 1 ～ 100。 • **描述**：关键字的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? " ' \ < > & • **启用**：启用关键字过滤规则。

提示：要查看页面过滤的监控信息，选择**监控** > **报警 / 日志** >**IPS 报警**。

12.3.2 客户端防护

本节包含以下内容：

12.3.2.1 （客户端防护）策略

NISG-IPS 根据数据包的源 IP 地址和源用户查找优先级最高 （序号最小）的客户端防护策略。如果匹配，则按照策略设置进行客户端防护 （IPS、协议异常检测和 DNS 缓存中毒防御）。

每安全域最多可添加 1024 条客户端防护策略。

表 197 客户端防护策略参数

参数	说明
开 / 关	为选择的安全域开启或关闭客户端防护。
序号	策略的优先级，序号越小，优先级越高，取值范围为 1-1024。
名称	策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<> &#
开启 SSL 检测	启用或禁用对 HTTPS 流量的 SSL 检测功能。
源 IP （客户端 IP 地址）	安全域内被保护客户端的 IP 地址。添加类型包括： • **任意** • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户自定义 IP 地址，最多支持 4096 个 IP 地址或 IP 地址段。针对同一条客户端防护策略不能同时添加 IPv4 地址和 IPv6 地址。
源用户	安全域内被保护的客户端： • **任意** • **任意认证用户** • **使用下表**：可以包括未在 NISG-IPS 上创建的、在外部认证服务器上认证的用户。 每条策略最多支持 4096 个源用户。
IPS	设置 IPS 检测级别，包括低、中、高和自定义。 IPS 检测内容包括攻击签名检测和协议限制。详细信息请参见 12.3.4 IPS。
受保护应用	受客户端防护策略保护的应用，包括： • **Mail （POP3 和 IMAP）** • **FTP （FTP 下载）** • **Web （HTTP/HTTPS 下载）** • **DNS （DNS 缓存中毒防御）**
日志	对于匹配客户端防护策略的流量，启用或禁用其日志功能。
启用	启用或禁用客户端防护策略。
最大受保护邮件	NISG-IPS 所能保护的 POP3 或 IMAP 邮件的最大值。

表 197 客户端防护策略参数 (*续*)

参数	说明
协议异常检测	用于检测不符合 RFC 规定的异常流量。 检测 POP3 和 IMAP 流量异常： • **检测应答格式异常** • **检测应答长度异常** • **检测 MIME 格式和长度异常** 检测 HTTP 下载流量中以下内容的格式和长度异常： • **HTTP 版本** • **原因短语** • **状态码** • **首部** 检测 DNS 流量： • **格式和长度异常**
DNS 缓存中毒防御	开启或关闭 DNS 缓存中毒防御功能。 详细信息请参见 12.3.2.4 DNS 缓存中毒防御。

12.3.2.2 （客户端防护）信任服务器列表

信任服务器列表定义了指定安全域内受 NISG-IPS 信任的服务器。信任服务器列表在客户端防护策略之前进行匹配。 NISG-IPS 根据数据包的源安全域、服务器 IP 地址或域名以及服务器类型与信任服务器列表进行匹配。如果匹配到信任服务器条目，则后续数据包不再与客户端防护策略进行匹配，直接放行。

管理员可以为每个安全域配置一个信任服务器列表，每个信任服务器列表最多包含 32 个信任服务器条目。

表 198 信任服务器列表参数

参数	说明
开 / 关	在指定的安全域内启用或禁用信任服务器列表功能。
名称	信任服务器策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
安全域	信任服务器所在的安全域。
IP 地址 / 域名 （服务器 IP 地址）	信任服务器的 IP 地址。添加类型包括： • **任意** • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户自定义 IP 地址或域名，最多支持 4096 个 IP 或 IP 地址段。
服务器类型	添加类型包括： • **任意** • **使用下表**：包括 Web 服务器、FTP 服务器、邮件服务器、DNS 服务器和其他类型服务器。

12.3.2.3 （客户端防护）信任邮件地址列表

信任邮件地址列表在客户端防护策略之后匹配。指定安全域内被保护的邮件客户端收到的所有邮件中，收件人或发件人在信任邮件地址列表中的邮件将不进行客户端防护检测。客户端防护中的信任邮件地址列表仅对 POP3 和 IMAP 流量进行检测。

每个安全域只能添加一个信任邮件地址列表，每个信任邮件地址列表最多可添加 128 条信任邮件地址。

表 199 信任邮件地址列表 （客户端保护）参数

参数	说明
开 / 关	在指定的安全域内启用或禁用信任邮件地址列表功能。
邮件地址	受信任的邮件地址或域名。允许配置 “(null)” 表示匿名发件人。

12.3.2.4 DNS 缓存中毒防御

DNS 缓存中毒防御功能用于防御客户端 DNS 缓存区中毒。管理员可以配置全局 DNS 缓存中毒防御功能，并在客户端防护策略中开启或关闭该功能。

表 200 DNS 缓存中毒防御参数

参数	说明
产生日志	启用 DNS 缓存中毒防御的日志功能。管理员另外需要在相应的客户端防护策略中开启日志和 DNS 缓存中毒防御功能，系统才能产生相应的日志。
启用 DNS 请求不规则化防护	改变 DNS 请求的 ID 号，使其不存在规律，防止攻击者利用 DNS 请求 ID 规律进行攻击。
检测常不匹配的应答	• **最大不匹配应答数**：在限定时间内，产生超过一定数量的错误应答，可被看做发生了攻击。 • **间隔**：设置检测不匹配应答的间隔时间。

提示：要查看 DNS 缓存中毒防御功能的监控信息，选择**监控** > **报警 / 日志** >**IPS 报警**。

12.3.3 服务器防护

12.3.3.1 （服务器防护）策略

NISG-IPS 根据服务器 IP 地址和服务器类型，查找与数据包匹配的服务器防护策略。如果匹配到策略，则按照匹配策略中规定的动作进行处理。如果没有匹配的策略，则不进行服务器防护。每个安全域最多配置 128 条服务器防护策略。

表 201 服务器防护策略参数

参数	说明
开 / 关	为指定安全域开启或关闭服务器防护功能。
序号	服务器防护策略的匹配优先级，序号越小，优先级越高。取值范围为 1-1024。
名称	服务器防护策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
服务器 IP	受保护服务器的 IP 地址或 IP 地址范围，最多可添加 4096 个 IP 地址或 IP 地址范围。 IPv4 和 IPv6 地址不可同时添加。
服务器类型	受保护服务器的类型，包括 Web、 Mail、 FTP、 Telnet、 DNS 和 Other。
开启 SSL 检测	启用或禁用对 HTTPS 流量的 SSL 检测功能。
IPS	启用或禁用 IPS 检测功能。设置 IPS 检测级别，包括低、中、高和自定义。为 Web、Mail、 FTP、 Telnet、 DNS 和 Other 类型服务器防护策略配置 IPS 检测级别。关于详细信息，请参见 12.3.4 IPS。
防护	为 Web 服务器防护策略启用 Web 防护或为邮件服务器防护策略启用邮件防护。 关于详细信息，请参见 12.3.3.4 Web 防护和 12.3.3.5 邮件防护。
启用	启用或禁用服务器防护策略。
日志	对匹配服务器防护策略的流量，启用其日志功能。

服务器防护策略为不同类型的服务器提供不同的防护功能：

表 202 服务器防护策略高级配置参数

类型	IPS	防护	针对特定服务器的配置
Web	是	**12.3.3.4 Web 防护**：全局配置，在策略中开启。	• **协议异常检测**：检测不符合 RFC 规定的 HTTP 上载流量。
Mail	是	**12.3.3.5 邮件防护**：全局配置，在策略中开启。	• **最大受保护邮件**：基于 SMTP 协议的邮件大小限制。 • **协议异常检测**：检测不符合 RFC 规定的 SMTP、 POP3、 IMAP 流量。

表 202 服务器防护策略高级配置参数 (*续*)

类型	IPS 防护	针对特定服务器的配置
FTP 上载	是	--
Telnet	是	• **命令过滤**：对来自 ANSI、 Xterm、 VT100 和 VT52 等终端的 Telnet 流量进行检测。启用该功能后， NISG-IPS 将字符重组成串，然后与管理员自定义命令进行匹配。 • **自定义命令阻断列表**：最多可以配置 512 个自定义命令。每个命令由字母、数字、下划线组成，取值范围为 1 ～ 64 字节。
DNS	是	• **外部请求限制**：如果启用该功能，来自列表中安全域的外部 DNS 请求将被丢弃。对于来自这些受限安全域的 DNS 请求中，如果想允许对特定域名或 IP 地址的 DNS 请求，可以启用**授权域**功能并添加允许请求的 IP 地址或域名。 • **协议异常检测**：检测不符合 RFC 规定的 DNS 流量。
其他	是 --	--

12.3.3.2 （服务器防护）信任客户端列表

管理员可以为指定的安全域配置信任客户端列表，定义哪些客户端受保护。信任客户端列表在服务器防护策略之前匹配。此安全域被保护的服务器中，所有源自信任客户端发起的流量都不进行服务器防护安全检测。

管理员可以为每个安全域配置一个信任客户端列表，最多包含 32 个信任客户端条目。

表 203 信任客户端列表参数

参数	说明
开 / 关	在指定的安全域内启用或禁用信任客户端列表。
名称	信任客户端策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?, "'\ < > & #
安全域	信任客户端所在的安全域。
IP 地址 （客户端 IP 地址）	信任客户端 IP 地址： • **任意** • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户指定 IP 地址。 列表中每个条目只能包含 1 个 IP 地址或 IP 地址段。
源用户	信任源用户： • **任意** （任意） • **任意认证用户** • **使用下表**：可以包含不在 NISG-IPS 上创建的、在外部认证服务器上认证的用户。 每个信任列客户端表最多支持 4096 个源用户。

12.3.3.3 （服务器防护）信任邮件地址列表

管理员可以为指定的安全域配置信任邮件地址列表。信任邮件地址列表在服务器防护策略之后进行匹配。此安全域被保护的邮件服务器中，收件人或发件人与信任邮件地址列表匹配的邮件都不进行服务器防护安全检测，如 IPS 的攻击签名检测。服务防护中的信任邮件地址列表仅对 SMTP 流量生效。

每个安全域只能添加一个信任邮件地址列表，每个信任邮件地址列表最多可添加 128 条信任邮件地址或域名。

表 204 （服务器防护）信任邮件地址列表参数

参数	说明
开 / 关	在指定的安全域内启用或禁用信任邮件地址。
邮件地址	信任发件人 / 收件人的邮件地址或域名。允许配置 “(null)” 表示匿名发件人。

12.3.3.4 Web 防护

Web 防护为系统全局配置，管理员可以在针对每安全域配置的每条服务器防护策略中开启或关闭 Web 防护。 Web 防护包括：

- 12.3.3.4.1 信息泄露防护
- 12.3.3.4.2 注入攻击防御

12.3.3.4.1 信息泄露防护

NISG-IPS 分别针对服务器端与客户端流量进行过滤，为 Web 服务器提供信息泄漏检测：

- **首部置换**：替换 HTTP 首部中包含的敏感信息（服务器名称或版本号等），以保护服务器。
- **隐藏错误信息**：隐藏 Web 服务器相关的错误信息，避免服务器内部信息泄露。
- **目录列表检测**：阻断 HTTP 传输中具有目录列表特征的信息，以防止信息泄漏或非法访问。该特性分为高、中、低三个级别：

表 205 目录列表检测级别

级别	检查内容	以下情况丢弃应答
低	只检查可疑的应答（包含以斜杠和反斜杠结尾的 URL）	• 被要求的目录出现在 HTML 页面的标题中； • HTML 页面有父目录的链接。
中	检查所有 HTTP 应答	检查条件与低级相同。
高	检查所有 HTTP 应答	HTTP 页面上有父目录的链接，且关键字为 “Parent Directory”。

表 206 信息泄露防护参数

参数	说明
产生日志	启用 / 禁用信息泄露防护的日志功能。 管理员另外需要在相应的服务器防护策略中开启日志和 Web 防护功能，系统才能产生相应的日志。
首部置换	管理员最多可以添加 32 个首部置换条目。 • **首部**：要检测的 HTTP 首部， 1-32 字节长度，不可以输入控制字符及以下特殊字符：( ) < > @ , ; : \ “ / [ ] ? = { } SP, HT。 • **首部值**：用来替换首部的值。支持正则表达式，长度为 1-32 字节。 • **动作**：当 NISG-IPS 检测到匹配的首部名和首部值时的替换动作，包括**删除**和**替换**。替换值 1-32 字节，不可以输入 CRLF、 SP、 HT。 • **启用**：启用 / 禁用首部置换条目。
隐藏错误信息	使用错误码代表 Web 服务器的错误消息，防止服务器信息泄露。
目录列表检测	• **严重级别**：包括高、中和低。 • **动作**：查找到与当前级别限制匹配的目录列表信息时的处理动作，包括**允许**和**阻断**。

12.3.3.4.2 注入攻击防御

NISG-IPS 可以防御以下几种注入攻击：

- **跨站脚本攻击**：指攻击者在具有信任关系的 Web 服务器和客户端之间，通过在 URL 中注入恶意的脚本，来获取包含用户的身份信息、资格证书的 Cookie 或者欺骗用户提供资格证书给攻击者。
- **LDAP 注入**：指攻击者在用户提交给 Web 应用的 HTTP 请求中，通过在 Form 和 URL 中注入非法的 LDAP 查询，来获取 LDAP 目录中存储的数据信息，导致用户信息泄露或者被添加、修改、甚至删除。
- **SQL 注入**：指攻击者以 URL 或 Form 输入形式变相地到数据库中执行 SQL 命令。如果攻击成功，可能导致信息泄露，改变数据库内容，甚至破坏数据库。
- **命令注入**：攻击者以 URL 或 Form 输入形式在 Web 服务器上执行系统命令。如果执行成功，攻击者可能以管理员的身份进入到 Web 服务器，造成巨大损失。

表 207 （Web 服务器）注入攻击防御参数

参数	说明
产生日志	启用日志。管理员另外需要在相应的服务器防护策略中开启日志和 Web 防护功能，系统才能产生相应的日志。
跨站脚本攻击防御	管理员最多可以添加 64 条脚本命令。 • **严重级别**：包括高、中和低三种。 • **脚本命令**：NISG-IPS 缺省进行跨站脚本攻击防御的命令和管理员自定义的脚本命令， 1-32 字节，允许输入字母、数字以及除了空格和问号以外的特殊字符。 • **阻断**：设置是否阻断指定命令。
LDAP 注入攻击防御	管理员最多可以添加 32 个识别名条目。 • **严重级别**：包括高、中和低三种。 • **识别名**：进行 LDAP 注入检测的关键字的名称，长度为 1 ～ 32 字节，允许输入字母、数字以及除了空格和问号以外的特殊字符。 • **阻断**：设置是否阻断指定命令。
SQL 注入攻击防御	管理员最多可以添加 256 条 SQL 命令。 • **严重级别**：包括高、中和低三种。 • **类型**：包括 Distinct SQL 命令和 Non-Distinct SQL 命令。 • **SQL 命令**：进行 SQL 注入检测的命令，长度为 1 ～ 120 字节，允许输入字母、数字以及除了空格和问号以外的特殊字符。 • **阻断**：设置是否阻断指定命令。
命令注入攻击防御	管理员最多可以添加 512 条 Shell 命令令。 • **严重级别**：包括高、中和低三种。 • **类型**：包括 Distinct Shell 命令和 Non-Distinct Shell 命令。 • **Shell 命令**：进行命令注入检测的命令，长度为 1 ～ 120 字节，允许输入字母、数字以及除了空格和问号以外的特殊字符。 • **阻断**：设置是否阻断指定命令。

12.3.3.5 邮件防护

管理员可以全局配置邮件防护功能，然后在服务器防护策略中开启或关闭信息泄露防护功能。

表 208 （邮件服务器）信息泄露防护参数

参数	说明
产生日志	管理员另外需要在相应的服务器防护策略中开启日志和邮件防护功能，系统才能产生相应的日志。
将 SMTP 服务器标题信息替换为	替换信息允许输入 UTF-8 所有字符，长度为 0 ～ 256 字节。
将 POP3 服务器标题信息替换为	替换信息允许输入 UTF-8 所有字符，长度为 0 ～ 256 字节。
将 IMAP 服务器标题信息替换为	替换信息允许输入 UTF-8 所有字符，长度为 0 ～ 256 字节。

12.3.4 IPS

IPS 定义攻击签名检测和协议限制，并且需要在客户端 / 服务器防护策略中指定。

提示：有关 IPS 的监控信息，选择**监控** > **报警 / 日志** >**IPS 报警**。

本节包含以下内容：

12.3.4.1 （IPS）防护配置

IPS 防护配置是攻击签名规则的集合。 NISG-IPS 基于攻击签名规则进行攻击检测，它能够根据签名特征识别出特定类型的攻击，并根据管理员设置的动作允许或阻断匹配签名特征的流量。

管理员可以根据需要配置不同的防护配置，并在 IPS 防护配置中开启或关闭协议限制功能。 IPS 防护配置可用于客户端防护策略和服务器防护策略。

NISG-IPS 提供 21 个缺省 IPS 防护配置。缺省的 IPS 防护配置只能查看，不能删除或编辑。管理员最多还可以添加 42 个自定义 IPS 防护配置，自定义 IPS 防护配置只能在根系统中创建。

表 209 IPS 防护配置参数

参数	说明
名称	IPS 防护配置的名称。 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
	缺省 IPS 防护配置分别以 _Low， _Medium 和 _High 命名，分别表示了低、中、高三个级别的 IPS 防护。 • **低：**仅防御严重级别为高的攻击。 • **中：**防御级别为高和中的攻击。 • **高：**防御所有攻击。
引用	点击 查看引用 IPS 防护配置的客户端或服务器防护策略。 一个 IPS 防护配置可以被多个客户端或服务器防护策略引用，被引用的防护配置不能被删除。
描述	IPS 防护配置的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? " '\ < > &
类型	IPS 防护配置的类型，包括客户端和服务器。 • 如果选择客户端类型，则只能配置目标为客户端或双向的攻击签名规则。 • 如果选择服务器类型，则只能配置目标为服务器或双向的攻击签名规则。
服务器类型	当 IPS 防护配置的类型为服务器时，可以进一步配置服务器的类型，包括 Web、Mail、 FTP、 Telnet、 DNS 和 Other。
协议限制	用于启用或禁用 IPS 防护配置的协议限制功能： • 针对客户端：开启或关闭 POP3、 IMAP、 SMTP 和 DNS 的协议限制功能。 • 针对服务器：开启或关闭 Web （HTTP）、 Mail （POP3、 IMAP、 SMTP）和 DNS 的协议限制功能。
攻击签名规则列表	为新建 IPS 防护配置设置攻击签名规则。
允许 / 阻断	设置攻击签名规则的动作，包括允许和阻断。 • 如果一条规则被启用且动作设为允许， NISG-IPS 将放行匹配该规则的流量。 • 如果一条规则被启用且动作设为阻断， NISG-IPS 将阻断匹配该规则的流量。
启用 / 禁用	启用和禁用攻击签名规则。

12.3.4.2 协议限制

协议限制为应用级协议的访问控制。协议本身的一些漏洞会被攻击者利用，具有潜在风险。NISG-IPS 分别为客户端防护和服务器防护提供了协议限制功能。管理员可以全局配置协议限制并在 IPS 防护配置中开启或关闭协议限制功能。

NISG-IPS 提供以下协议限制：

- 12.3.4.2.1 HTTP 协议限制
- 12.3.4.2.2 SMTP 协议限制
- 12.3.4.2.3 POP3 协议限制
- 12.3.4.2.4 IMAP 协议限制
- 12.3.4.2.5 DNS 协议限制

12.3.4.2.1 HTTP 协议限制

HTTP 协议限制功能只能在 Web 服务器类型的 IPS 防护配置中开启。

表 210 HTTP 协议限制参数

参数	说明
级别	协议限制级别，包括高、中、低和自定义四个级别。
产生日志	启用日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
最大首部数	• **取值**：1 ～ 1024。 • **动作**：当首部数超出限制时的处理动作，包括允许和阻断。
最大 URL 长度	• **取值**：1 ～ 2048 字节。 • **动作**：当长度超出限制时的处理动作，包括允许和阻断。
最大请求正文长度	• **取值**：1 ～ 65535 字节。 • **动作**：当长度超出限制时的处理动作，包括允许和阻断。
最大首部长度	• **取值**：1 ～ 2048 字节。 • **动作**：当长度超出限制时的处理动作，包括允许和阻断。
首部长度限制	• **首部名称**：最多添加 32 个首部。 • **最大长度**：1 ～ 2048 字节。该项设置的首部长度需要小于通用的最大首部长度值。 • **启用**：当首部长度超出限制时，阻断连接。
请求方式阻断列表	阻断特定请求方式（已选命令）的 HTTP 流量。
阻断非 ASCII 码首部	如果在首部中检测到非 ASCII 码字节，则阻断连接。
阻断 Form 字段的非 ASCII 码字符	如果在 Form 字段中检测到非 ASCII 码字符，则阻断连接。

12.3.4.2.2 SMTP 协议限制

表 211 服务器防护中的 SMTP 协议限制参数

参数	说明
级别	协议限制级别，包括高、中、低和自定义四个级别。
产生日志	启用日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
最大命令长度	• **取值**：1 ～ 1024 字节。 • **动作**：当长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大参数长度	• **取值**：1 ～ 512 字节。 • **动作**：当长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大 NOOP 命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。
最大命令数	• **取值**：1 ～ 256。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。
最大未知命令数	• **取值**：1 ～ 128 之间的整数。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。
阻断未知命令	阻断未知命令。管理员自定义命令不属于未知命令。
自定义 SMTP 命令列表	添加用户自定义命令，最大条目数 32。 命令中不允许包含空格与制表符，长度为 4 ～ 8 字节。
命令阻断列表	阻断已选 SMTP 命令。
转发时添加 Received 头字段	转发时添加 Received 头字段。
剥离带有多个 Content-Type 头字段的 MIME 字段	剥离带有多个 Content-Type 头字段的 MIME 字段。
剥离带有多个 Encoding 头字段的 MIME 字段	剥离带有多个 Encoding 头字段的 MIME 字段。
剥离带有未知 Encoding 头字段的 MIME 字段	剥离带有未知 Encoding 头字段的 MIME 字段。
剥离所有邮件附件	剥离所有邮件附件。
剥离所有分片邮件	剥离所有分片邮件。
阻断收件人没有域名的邮件	阻断收件人没有域名的邮件。

表 212 客户端防护中的 SMTP 协议限制参数

参数	说明
产生日志	启用 日志功能。管理员另外需要在相应的客户端防护策略中开启日志功能。
最大应答长度	• **取值**：1 ～ 2048 字节。 • **动作**：当长度超出限制时的处理动作，包括允许和阻断。

12.3.4.2.3 POP3 协议限制

表 213 服务器防护中的 POP3 协议限制参数

参数	说明
级别	协议限制级别，包括高、中、低和自定义四个级别。
产生日志	启用 POP3 协议限制的日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
最大命令长度	• **取值**：1 ～ 1024 字节。 • **动作**：当命令长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大参数长度	• **取值**：1 ～ 512 字节。 • **动作**：当参数长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大 NOOP 命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中 NOOP 命令次数超出限制时的处理动作，包括允许和阻断。
最大命令数	• **取值**：1 ～ 256。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。
最大未知命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中未知命令次数超出限制时的处理动作，包括允许和阻断。
阻断未知命令	阻断未知命令。管理员自定义命令不属于未知命令。
自定义 POP3 命令列表	添加用户自定义命令，最大条目数 32。 命令中不允许包含空格与制表符，长度为 4 ～ 8 字节。
命令阻断列表	阻断的已选 POP3 命令。

表 214 客户端中的 POP3 协议限制参数

参数	说明
产生日志	启用日志功能。管理员另外需要在相应的客户端防护策略中开启日志功能。
最大应答长度	• **取值**：1 ～ 2048 字节。 • **动作**：当应答长度超出限制时的处理动作，包括允许和阻断。

12.3.4.2.4 IMAP 协议限制

表 215 服务器防护中的 IMAP 协议限制参数

参数	说明
级别	协议限制级别，包括高、中、低和自定义四个级别。
产生日志	启用日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
最大命令长度	• **取值**：1 ～ 2048 字节。 • **动作**：当命令长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大参数长度	• **取值**：1 ～ 1024 字节。 • **动作**：当参数长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大 Tag 长度	• **取值**：1 ～ 512 字节。 • **动作**：当 Tag 长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大 NOOP 命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中 NOOP 命令次数超出限制时的处理动作，包括允许和阻断。
最大命令数	• **取值**：1 ～ 256。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。
最大未知命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中未知命令次数超出限制时的处理动作，包括允许和阻断。
阻断未知命令	阻断未知命令。管理员自定义命令不属于未知命令。
自定义 IMAP 命令列表	添加用户自定义命令，最大条目数 32。 命令中不允许包含空格与制表符，长度为 4 ～ 16 字节。
命令阻断列表	阻断已选 IMAP 命令。

表 216 客户端防护中的 IMAP 协议限制参数

参数	说明
产生日志	启用日志功能。管理员另外需要在相应的客户端防护策略中开启日志功能。
最大应答长度	• **取值**：1 ～ 4096 字节。 • **动作**：当应答长度超出限制时的处理动作，包括允许和阻断。

12.3.4.2.5 DNS 协议限制

表 217 服务器防护中的 DNS 协议限制参数

参数	说明
产生日志	启用日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
授权 IP 地址列表	添加允许 DNS 区域传输的授权 IP。来自列表中 IP 之外的 DNS 请求将被丢弃。最多添加 128 个 IP 地址条目。

表 218 客户端防护中的 DNS 协议限制参数

参数	说明
产生日志	启用 / 禁用日志功能。管理员另外需要在相应的客户端防护策略中开启日志功能。
UDP 资源记录数限制	限制资源记录数。启用该功能后，管理员可以为以下参数设置取值和动作： • **最大回答记录数** • **最大授权记录数** • **最大附加记录数**

12.3.4.3 （攻击签名规则）更新

NISG-IPS 通过手动和自动方式加载攻击签名规则升级包更新攻击签名规则。攻击签名规则升级包上载后立即生效，不需要重启系统。攻击签名规则更新不支持升级回退。

攻击签名规则更新功能限制如下：

- License

  攻击签名规则更新需要 IPSUP License 的许可。

- 虚拟系统

  NISG-IPS 只允许在根系统 （root）中进行攻击签名规则更新操作，所有虚拟系统共享攻击签名规则更新后的结果。

表 219 攻击签名规则库参数

参数	说明
规则库	攻击签名规则库名称，默认包括 HTTP、 DNS、 FTP、 IMAP、 ORACLE、 OTHERS、 POP3、 SIP、 SMTP、 TELNET、 TFTP 和 BACKDOOR。
规则版本	最新的攻击签名规则库版本。
引擎版本	攻击签名规则库所对应的引擎版本。
上次更新时间	当前攻击签名规则库上次更新时间。
显示 / 导出更新历史记录	用于查看或导出攻击签名规则库的更新历史记录。 NISG-IPS 最多支持 50 条记录。

表 220 攻击签名规则更新模式参数

参数	说明
更新服务器地址	执行自动更新的服务器的 URL 地址，可以为 IPv4/v6 地址或者域名。 缺省为 nts.neusoft.com/autoupdate。
更新模式 （自动）	攻击签名规则自动更新的模式，包括**自动安装更新**和**从不检测更新**。
时间表	NISG-IPS 自动下载并安装升级包的定时更新时间。 • 当选择**每天**、**每周**或**每月**时，系统会在指定时间点后两个小时内随机开始升级。 • 当选择**间隔**时，系统将按照设定时间间隔进行规则更新。
立即更新	当更新服务器地址和更新内容配置成功后，点击**立即更新**， NISG-IPS 立即从指定的更新服务器上获取升级包并执行安装。
手动上载升级包	上传本地的攻击签名规则更新包。

12.3.5 SSL 检测

用户可以配置 SSL 检测证书策略，指定 SSL 检测所使用的证书，证书策略参数如下所示。

表 221 SSL 检测证书策略参数

配置信息	说明
序号	SSL 检测证书策略的优先级。数值越小，优先级越高。取值范围为 1 ～ 31 之间的整数。系统默认存在一条序号为 32 的证书策略。
名称	SSL 检测证书策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
启用	用于启用或禁用 SSL 检测证书策略，证书策略的状态缺省为启用。
目的 IP 和端口列表	设置数据包要到达的目的 IP 地址、域名、端口号，及数据包使用的服务类型。策略列表最多可以添加 32 个条目。 • **IP 地址**：数据包要到达的 IP 地址。可以是以下任一类型： •**任意**：包括所有 IPv4 和 IPv6 地址。任意为缺省设置。 •**任意 IPv4 地址**：包括所有 IPv4 地址。 •**任意 IPv6 地址**：包括所有 IPv6 地址。 • **协议**：数据包使用的协议类型，包括任意、 TCP 和 UDP。 • **目的端口**：数据包发送到的目的端口号，取值范围为 1-65535。
SSL 检测证书	SSL 检测使用的证书，包括： • **系统默认证书**：与 Web 管理中 HTTPS 使用的证书相同， NISG-IPS 只有一个系统默认证书。 • **本地证书**：手动导入的本地证书。 **缺省项**：系统默认证书
用于	证书用途，系统默认证书和本地证书都支持证书颁发和解密功能。 • **证书颁发**：作为 CA 证书颁发仿冒证书，适用于管理员无法获取服务器证书的情况。 • **解密**：直接用于解密来自客户端的 SSL 数据，适用于管理员拥有服务器证书的情况。

12.3.6 通知消息

通知消息是服务器向客户端发出的回应信息，用于替换被 URL 过滤、协议限制或攻击签名检测功能阻断的内容。 NISG-IPS 的通知消息分为两种：

- **用户自定义通知消息:** 可通过 WebUI 进行配置。NISG-IPS 在 URL 被阻断时发送通知消息。
- **系统预定义通知消息：**系统预定义，不可编辑。

  系统通知消息主要指攻击签名检测通知消息。当检测到客户端访问的网站存在威胁时， NISG-IPS 将发送一个预定义通知消息给客户端。同时， NISG-IPS 将阻断连接，并将 Web 服务器的 URL 保存到缓存中，缓存超时时间为 600 秒。 URL 缓存的最大条目数为 100 条。到达最大条目数时，新的 URL 条目将替换时间最久的缓存条目。

12.3.7 概要信息

IPS 概要信息页面显示所有安全域的 IPS 信息。

表 222 IPS 概要信息页面参数

列名称	描述
安全域	配置 IPS 信息的安全域。
出口控制	在网络出口上控制出口流量，包括： • **应用控制**：控制用户访问 Internet 使用的应用。 • **URL 过滤**：过滤 URL 请求，阻断高危或可疑网站流量。 • **DNS 控制**：阻断到未授权 DNS 域名的请求。 • **页面过滤**：过滤网页内容。
防护	用于防护指定安全域内的客户端或服务器。

12.4. IPS 范例

本节给出三个 NISG-IPS 配置模式范例：

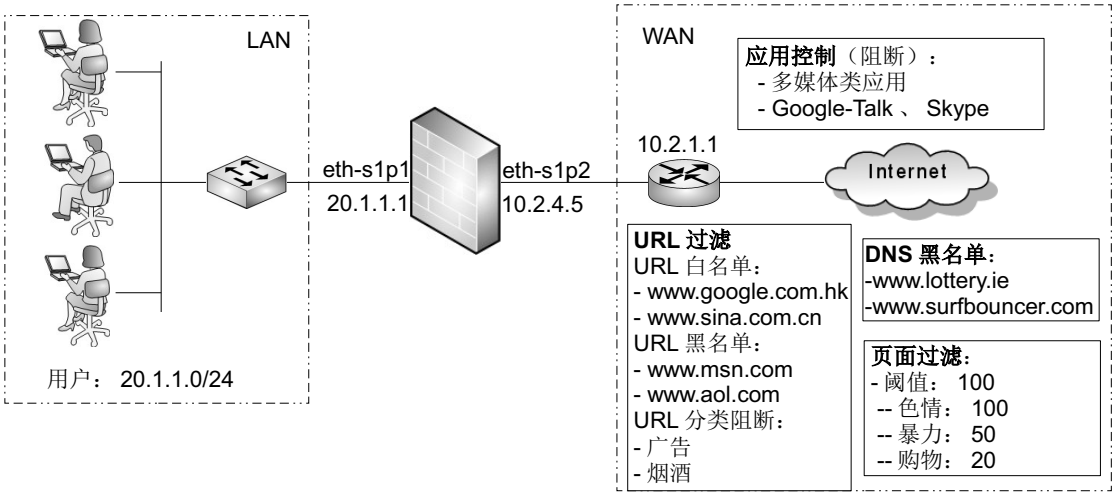
12.4.1. 范例 1：IPS 出口控制

基本需求

如下图所示，内网 LAN 中的用户通过 NISG-IPS 与 Internet 进行通讯，为了对用户的上网行为进行限制，管理员可以进行如下配置：

1. 配置应用控制，禁止用户访问某类应用及若干具体应用；
2. 配置 URL 过滤，对用户访问的网站进行控制：
   - URL 白名单：NISG-IPS 直接允许用户访问白名单所列的 URL，不进行 URL 过滤检测；
   - URL 黑名单：NISG-IPS 禁止用户访问黑名单上列出的 URL ；
   - URL 分类：NISG-IPS 禁止用户访问某种特定类型的 URL 内容，如广告、烟酒。
3. 配置 DNS 黑名单，NISG-IPS 将阻断用户向黑名单内所列域名或 IP 地址发出 DNS 请求；
4. 配置页面过滤，设置关键字、分值和阈值， NISG-IPS 阻断包含指定关键字且总分超过阈值的页面。

组网拓扑



配置要点

如果初次登录选择跳过初始化过程，配置 IPS 之前，需要先配置：

- 创建安全域 / 缺省路由 / 访问策略 /NAT 规则

IPS 配置步骤包括：

- 配置应用控制
  - 创建应用控制防护配置
  - 创建应用控制策略
  - 验证结果
- 配置 URL 过滤
  - 创建 URL 黑白名单
  - 创建 URL 过滤防护配置
  - 创建 URL 过滤策略
  - 验证结果
- 配置 DNS 域名黑名单
- 配置页面过滤

配置步骤

创建安全域 / 缺省路由 / 访问策略 /NAT 规则

1. 选择**网络** > **接口**，设置 eth-s1p2 和 eth-s1p1 为三层接口，并设置其 IP 地址分别为 10.2.4.5/21 和 20.1.1.1/24。
2. 选择**网络** > **安全域**，创建两个三层安全域 LAN 和 WAN，并将 eth-s1p1 划分给 LAN、eth-s1p2 划分给 WAN。
3. 选择**网络** > **路由** > **缺省路由**，修改缺省路由的网关为 10.2.1.1。
4. 选择**防火墙** > **访问策略**，创建访问策略，允许 LAN 中 20.1.1.0 网段到 WAN 的访问、拒绝 WAN 到 LAN 的访问：
   - 名称 =LANtoWAN，源安全运 =LAN，源 IP=20.1.1.0/24，目的安全域 =WAN，目的 IP/ 域名 = 任意，服务 = 任意，动作 = 允许；
   - 名称 =WANtoLAN，源安全运 =WAN，源 IP= 任意，目的安全域 =LAN，目的 IP/ 域名 = 任意，服务 = 任意，动作 = 拒绝。
5. 选择**网络** > **地址转换** > **源地址转换**，添加源地址转换规则，将源 IP 转换成 eth-s1p2 接口的 IP 地址：

   名称 =out，源 IP=20.1.1.0/24，转换后 IP/ 接口 =eth-s1p2。

配置应用控制

应用控制配置包括创建应用控制防护配置和策略。

创建应用控制防护配置

1. 选择 **IPS**> **出口控制** > **应用控制** > **防护配置**。
2. 点击**新建**，创建应用控制防护配置。
   - 名称 =Profile1
   - 不在下表中的应用的缺省处理动作 = 放行
   - 应用列表
     - 类型 = 过滤条件，动作 = 阻断，应用名称：分类 = 多媒体类应用，子分类 =Any，技术 =Any，风险等级 =Any ；
     - 类型 = 应用，动作 = 阻断，应用名称：Skype， Google=Talk。

   提示：通过名称添加应用到防护配置时，可以输入应用名称的首个或前两个字母，然后使用下拉框的自动补齐功能选择应用。
3. 点击**确定**。

创建应用控制策略

1. 选择 **IPS**> **出口控制** > **策略**。选择安全域 WAN，开启应用控制功能。
2. 展开**应用控制**区域，点击**新建**，创建应用控制策略 apppolicy1。

   序号 =1，名称 =apppolicy1，源安全域 =LAN，源 IP 地址 =20.1.1.0/24，防护配置 =Profile1。
3. 点击**确定**。启用该策略之后，20.1.1.0 网段的用户将不能使用 Google-Talk 和 Skype 应用，不能访问 Internet 多媒体类应用。

验证结果

1. 打开 Google-Talk 和 Skype 应用尝试登录，会发现登录失败。
2. 选择**监控** > **报警 / 日志** > **应用控制报警**，可以看到 Google-Talk、Skype 和多媒体类应用已被阻断。

配置 URL 过滤

URL 过滤配置包括创建 URL 黑白名单、 URL 过滤防护配置和 URL 过滤策略。

创建 URL 黑白名单

1. 选择 **IPS**> **出口控制** >**URL 过滤** > **黑白名单**。
2. 点击**新建**，创建 URL 白名单 Whitelist1，包括如下 URL：www.sina.com.cn 和 www.google.com.hk。
3. 点击**确定**。
4. 点击**新建**，创建黑名单 Blacklist1，包括如下 URL：www.msn.com 和 www.aol.com。
5. 点击**确定**。

创建 URL 过滤防护配置

1. 选择 **IPS**> **出口控制** >**URL 过滤** > **防护配置。**
2. 点击**新建**，创建 URL 过滤防护配置。
   - 名称 =URLProfile1
   - URL 白名单 =Whitelist1
   - URL 黑名单 =Blacklist1
   - URL 分类 = 启用
     - 分类 = 广告，启用 = 勾选，动作 = 阻断；
     - 分类 = 烟酒，启用 = 勾选，动作 = 阻断。
3. 点击**确定**。

创建 URL 过滤策略

1. 选择 **IPS**> **出口控制** > **策略**。选择安全域 WAN，开启 URL 过滤功能。
2. 展开 **URL 过滤**区域，点击**新建**，创建 URL 过滤策略 urlpolicy1。

   序号 =1，名称 =urlpolicy1，源安全域 =LAN，源 IP 地址 =20.1.1.0/24，防护配置 =URLProfile1。
3. 点击**确定**。启用该策略之后， 20.1.1.0 网段的用户可以访问白名单中的网址以及被允许的 URL 分类，但是不能访问黑名单中的网址和被阻断的 URL 分类 （广告和烟酒）。

验证结果

1. 内网用户可以成功访问 www.google.com.hk 和 www.sina.com.cn。
2. 内网用户访问 www.msn.com 和 www.aol.com 时提示 URL 被黑名单阻断：
3. 广告和弹出窗口类网页将被 URL 分类过滤功能阻断。
4. 选择**监控**>**报警/日志**>**URL过滤报警**，查看URL被黑白名单以及分类阻断或放行的日志信息。 URL 过滤支持模糊匹配。

配置 DNS 域名黑名单

1. 选择 **IPS**> **出口控制** >**DNS 域名黑名单**。
2. 配置 DNS 域名黑名单，阻断 www.lottery.ie 和 www.surfbouncer.com 的域名请求：
3. 点击**确定**。
4. 选择 **IPS**> **出口控制** > **策略**。
5. 选择安全域 WAN，开启 DNS 域名黑名单功能。内网用户将不能访问被域名黑名单阻断的网站。
6. 选择**监控**>**报警/日志**>**IPS报警**，可查看DNS黑名单阻断信息。对域名www.lottery.ie和www.surfbouncer.com 的 DNS 请求将被阻断。

配置页面过滤

1. 选择 **IPS> 出口控制** > **页面过滤**。
2. 配置页面过滤，阻断包含列表中关键字且总分超过阈值的页面。
   - 分数阈值 =100
   - 当 Web 页面上的关键字总分超过分数阈值时 = 阻断
   - 产生日志 = 启用
   - 关键字过滤
     - 关键字 = 色情，分值 =100，启用 = 勾选；
     - 关键字 = 暴力，分值 =50，启用 = 勾选；
     - 关键字 = 购物，分值 =20，启用 = 勾选。

   在上面的设置中，包含一个 “ 色情 ” 关键字的页面将被阻断，包含一个 “ 暴力 ” 关键字和 3 个 “ 购物 ” 关键字 (1*50+3*20=110) 的页面也将被阻断。
3. 点击**确定**。
4. 选择 **IPS> 出口控制** > **策略**。
5. 选择安全域 WAN，开启页面过滤功能。
6. 点击 。当内网用户访问的网页包含指定关键字且累计分数达到阈值时，页面将被阻断。
7. 选择**监控** > **报警 / 日志** >**IPS 报警**，可查看页面关键字过滤阻断信息，包含色情、购物和暴力关键字并超出规定分值的页面将被阻断访问。

提示：有时候用户访问不了白名单中的 URL，是因为其响应页面包含的过滤关键字总分数达到了阈值而被阻断。若出现此种情况，请检查两者配置是否冲突。

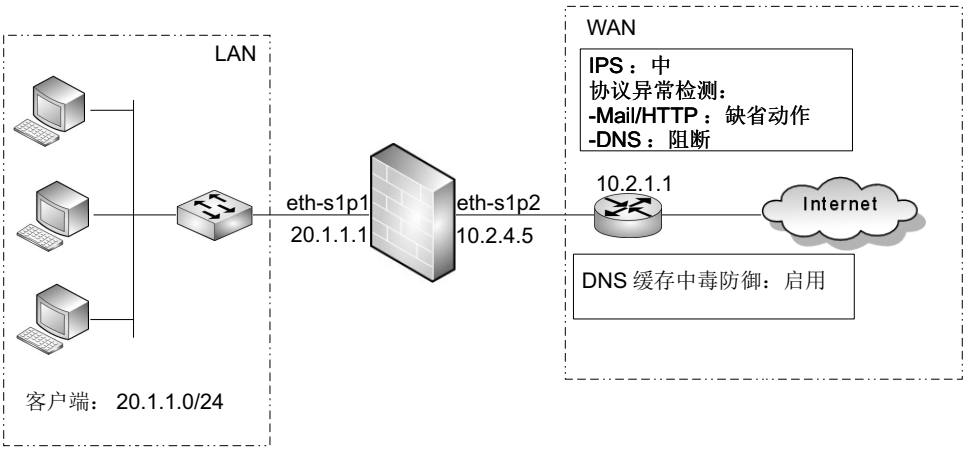
12.4.2. 范例 2：IPS 客户端防护

基本需求

如下图所示，某公司内网客户端通过 NISG-IPS 与 Internet 进行通讯，为了对客户端的安全进行防护，管理员可以进行如下配置：

8. 配置 IPS：
   - 开启中等级别的 IPS，进行攻击签名检测。对匹配攻击签名特征的流量， NISG-IPS 按照预定义动作进行放行或阻断；
   - 配置协议异常检测：
     - 对匹配 POP3/IMAP 和 HTTP 协议特征的异常流量，NISG-IPS 按照默认动作进行放行或阻断；
     - 对匹配 DNS 协议特征的异常流量，直接进行阻断。
9. 启用 DNS 缓存中毒防御：当 DNS 服务器缓存区受到攻击时，NISG-IPS 可以防止客户端被重定向到非法网站，引起信息泄漏。

组网拓扑



配置要点

如果初次登录选择路由模式：

- 修改访问策略
- 配置 DNS 缓存中毒防御功能
- 创建客户端防护策略

配置步骤

修改访问策略

1. 选择**防火墙** > **访问策略**。
2. 修改访问策略如下，允许客户端流量通过：

- 名称 =def_lw，源安全运 = 任意，源 IP=20.1.1.0/24，目的安全域 =WAN，目的 IP/ 域名 = 任意，服务 = 任意，动作 = 允许；
- 名称 =def_wl，源安全运 = 任意，源 IP= 任意，目的安全域 =LAN，目的 IP/ 域名 = 任意，服务 = 任意，动作 = 任意。

配置 DNS 缓存中毒防御功能

1. 选择 **IPS**> **客户端防护** >**DNS 缓存中毒防御**。配置 DNS 缓存中毒防御功能（使用默认配置即可）。
2. 点击**确定**。

创建客户端防护策略

1. 选择 **IPS**> **客户端防护** > **策略**。选择安全域 LAN，开启客户端防护功能。
2. 点击**新建**，进行如下基本配置：

   序号 =1，名称 =clientpolicy1，客户端 IP 地址 =20.1.1.0/24， IPS 检测级别 = 中。

提示：管理员可以选择 **IPS**>**IPS**> **防护配置**，点击缺省防护配置 Client_Medium 查看设置，还可以新建自定义防护配置并在策略中引用。

---

3. 在 **Mail** 应用防护区域，开启协议异常检测；对 POP3 和 IMAP 受保护的邮件最大值，使用系统默认设置 10 MB。
4. 在 **HTTP 下载**区域，开启协议异常检测，使用缺省设置。
5. 在 **DNS** 区域，开启 DNS 缓存中毒防御功能，并使用协议异常检测的缺省配置。
6. 点击**确定**。
7. 点击  。

验证结果

- 监控 IPS 功能
- 监控 DNS 缓存中毒防御功能

监控 IPS 功能

选择**监控** > **报警 / 日志** >**IPS 报警**，可查看 IPS 监控信息，包括 HTTP 协议异常检测报警日志、邮件 （SMTP & POP3）客户端防护和攻击检测报警日志、 DNS 协议异常检测报警日志。

监控 DNS 缓存中毒防御功能

1. 受保护客户端发出的DNS请求ID将被不规则化，以防止攻击者利用DNS请求的ID编号规律进行攻击。
2. 指定时间内探测到的 DNS 不匹配应答数超过限制值时， DNS 请求将被阻断，同时产生日志。
3. 选择**监控** > **报警 / 日志** >**IPS 报警**，可查看生成的 DNS 日志信息：

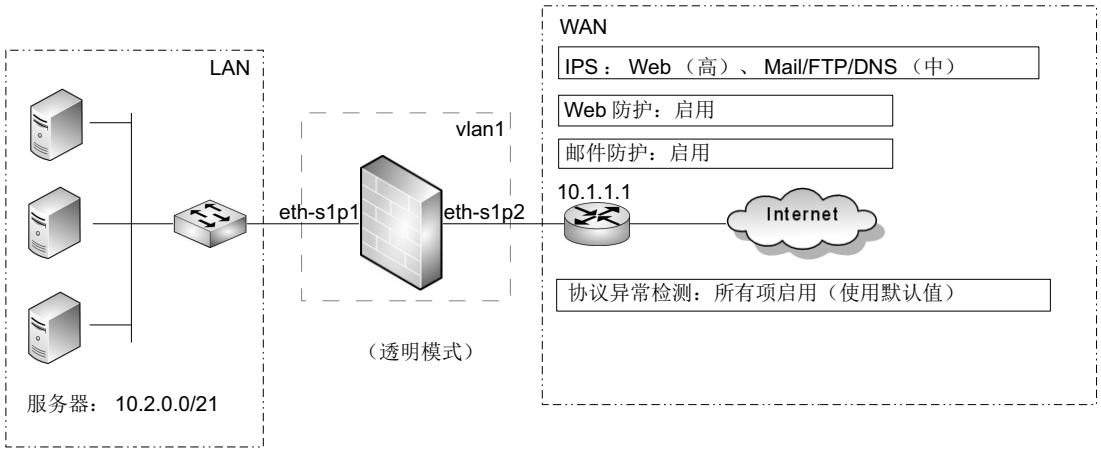
12.4.3. 范例 3：IPS 服务器防护

基本需求

如下图所示，某公司内部网络 LAN 中部署多台服务器向外网提供服务，为了对服务器的安全进行防护，管理员可以在 NISG-IPS 中配置相应的 Web、邮件、 FTP 和 DNS 服务器防护策略。

4. 配置 IPS：
   - 对 Web 服务器，开启高级别的 IPS 攻击签名检测；
   - 对邮件服务器、 FTP 服务器和 DNS 服务器，开启中等级别的 IPS 攻击签名检测；
5. 配置协议异常检测：对匹配 DNS、SMTP 和 HTTP 协议特征的异常流量，按照默认动作进行放行或阻断；
6. 启用 Web 防护：隐藏 Web 服务器信息，进行注入攻击防御；
7. 启用邮件防护：隐藏邮件服务器信息，防止信息泄漏。

组网拓扑



配置要点

假设管理员初次登录时选择了透明模式：

- 修改访问策略
- 创建服务器防护策略
  - Web 服务器防护策略
  - 邮件服务器防护策略
  - FTP 服务器防护策略
  - DNS 服务器防护策略
- 配置 Web 防护
- 配置邮件防护

配置步骤

修改访问策略

1. 选择**防火墙** > **访问策略**。
2. 修改访问策略如下：
   - 名称 =def_lw，源安全运 =LAN，源 IP= 任意，目的安全域 =WAN，目的 IP/ 域名 = 任意，服务 = 任意，动作 = 允许；
   - 名称 =def_wl，源安全运 =WAN，源 IP= 任意，目的安全域 =LAN，目的 IP/ 域名 =10.2.0.0/21，服务 = 任意，动作 = 允许。

创建服务器防护策略

1. 选择 **IPS**> **服务器防护** > **策略**。
2. 选择安全域 **LAN**，在 LAN 上开启服务器保护功能，创建以下策略：

Web 服务器防护策略

3. 点击**新建**，创建 Web 服务器防护策略：
   - 序号 =1
   - 名称 =webpolicy
   - IP 地址 =10.2.0.0/21
   - 服务器类型 =Web
   - 启用 Web 防护 = 勾选
   - 协议异常检测 = 勾选
   - 检测非标准端口 （非 80 端口）上的 HTTP 流量 = 勾选 / 允许
4. 点击**确定**。

邮件服务器防护策略

5. 点击**新建**，创建邮件服务器防护策略：
   - 序号 =2
   - 名称 =mailpolicy
   - IP 地址 =10.2.0.0/21
   - 服务器类型 =Mail
   - 启用邮件防护 = 勾选
   - 协议异常检测 = 勾选
     - 检测非标准端口 （非 25 端口）上的 SMTP 流量 = 勾选 / 阻断
     - 检测非标准端口 （非 110 端口）上的 POP3 流量 = 勾选 / 阻断
     - 检测非标准端口 （非 143 端口）上的 IMAP 流量 = 勾选 / 阻断
6. 点击**确定**。

FTP 服务器防护策略

7. 点击**新建**，创建 FTP 服务器防护策略：
   - 序号 =3
   - 名称 =ftppolicy
   - IP 地址 =10.2.0.0/21
   - 服务器类型 =FTP
   - IPS= 中
8. 点击**确定**。

DNS 服务器防护策略

9. 点击**新建**，创建 DNS 服务器防护策略：
   - 序号 =4
   - 名称 =dnspolicy
   - IP 地址 =10.2.0.0/21
   - 服务器类型 =DNS
   - IPS= 中
   - 外部请求限制 = 勾选，外部请求安全域 =LAN， WAN
   - 授权域 = 勾选，授权域名 =www.test.com
   - 协议异常检测 = 勾选
10. 点击**确定**。

配置 Web 防护

1. 选择 **IPS**> **服务器防护** >**Web 防护**。
2. 设置信息泄漏防护，使用系统默认设置即可。
3. 设置注入攻击防御。
   - 跨站脚本攻击防御 = 开启，安全级别 = 低，脚本命令 =.cookie，动作 = 阻断
   - LDAP 注入攻击防御 = 开启，安全级别 = 中，识别名 =c，动作 = 阻断
   - SQL 注入攻击防御 = 开启，安全级别 = 中，SQL 命令 =Has_dbaccess，动作 = 阻断
   - 命令注入攻击防御 = 开启，安全级别 = 中， Shell 命令 =access_log，动作 = 阻断
4. 点击**确定**。

配置邮件防护

1. 选择 **IPS**> **服务器防护** > **邮件防护**。
2. 启用邮件防护功能和记录日志功能，使用默认设置即可，则 SMTP、POP3 和 IMAP 服务器的标题信息将被替换为 Mail Server Ready...。
3. 点击**确定**。
4. 点击 。

验证结果

监控 IPS 功能

选择**监控** > **报警 / 日志** >**IPS 报警**，查看 IPS 监控信息。包括 HTTP 协议异常检测报警、邮件协议（SMTP&POP3）异常检测和服务器防护报警、FTP 服务器防护报警和 DNS 服务器防护报警信息。

13 虚拟专用网

虚拟专用网 （Virtual Private Network， VPN）功能利用公共网络建立虚拟专用网络，能够帮助远程用户、公司分支机构、商业伙伴等安全接入公司的内部网络，并保证数据的安全传输。本章介绍 NISG-IPS 的 VPN 功能：

13.1 概述

下表概要介绍 NISG-IPS 支持的 VPN 类型。

表 223 NISG-IPS 的 VPN 类型

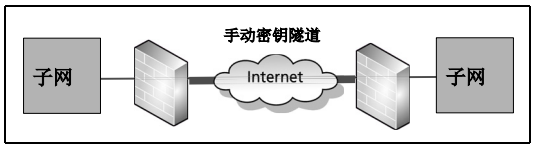
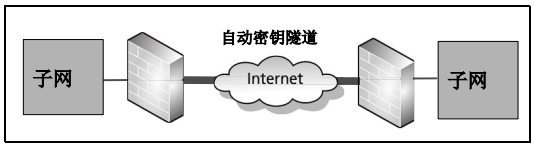
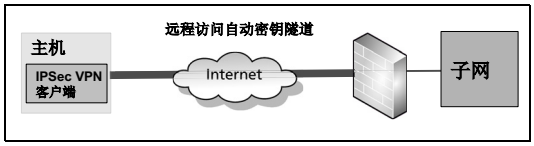
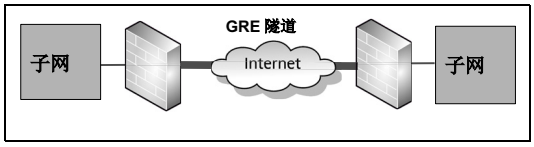
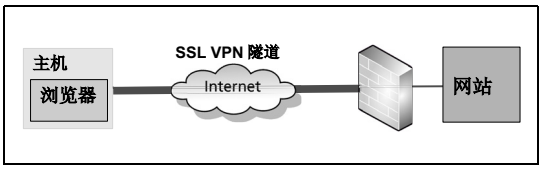
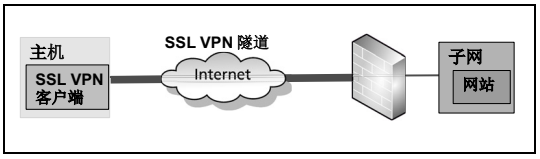
VPN 场景 （NISG-IPS= 网关设备）	描述
IPSec VPN	
	• **VPN 类型**：13.2.1 网段到网段手动密钥隧道 • **描述**：通过手动生成密钥建立隧道，仅支持网段到网段的 IPSec VPN。 • **适用场景**：一般用于小型或静态网络。 • **优点**：配置简单。 • **缺点**：难以管理和扩大规模，没有对端的身份验证。
	• **VPN 类型**：13.2.2 网段到网段自动密钥隧道 • **描述**：指两个网关设备之间通过自动生成密钥方式建立 IPSec VPN 隧道。隧道两端可以都是 NISG-IPS，也可以是 NISG-IPS 与其他支持标准 IPSec 协议的网关设备。 NISG-IPS 支持多 SA 功能，即一个网关设备可保护多个子网，可以对每条隧道从本端特定子网到对端特定子网之间的数据流进行精准的安全控制。 • **适用场景**：适合有 VPN 扩展需求的网络，多用于两个公司局域网之间通过 VPN 隧道互相通讯的场景。 • **优点**：使用方便、可扩展。 • **缺点**：配置复杂，需要更多的计算能力。
	• **VPN 类型**：13.2.3 远程访问自动密钥隧道 • **描述**：指远程用户 / 用户组与 VPN 网关之间建立 IPSec VPN 隧道，用户 / 用户组可以通过该隧道安全地访问受网关保护的内部子网。 • **适用场景**：一般用于移动办公人员 （远程用户）通过 VPN 隧道访问公司内网资源的场景。 • **优点**：可移动性、对用户进行认证。 • **缺点**：需要在远程主机上安装客户端软件。
GRE VPN	
	• **VPN 类型**：13.2.6 GRE 隧道 • **描述**：通过将一种协议的报文封装在另一种协议报文中，使被封装的报文能够在网络中传输。 • **适用场景**：其实现机制简单，通常用于对安全性要求不高的场景。 • **优点**：通用性好、技术简单、对隧道两端设备 CPU 消耗较少。 • **缺点**：无加密、无验证、安全性不高。

表 223 NISG-IPS 的 VPN 类型 (*续*)

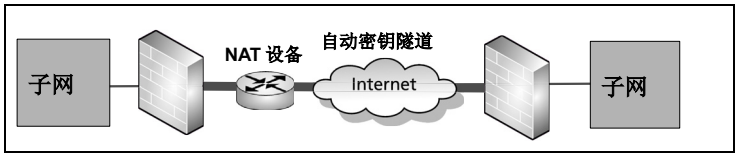
SSL VPN	
	• **VPN 类型**：13.2.8 SSL VPN Web 入口页面访问 • **描述**：为用户提供基于 HTTP/HTTPS 协议的 Web 应用服务，这种连接方式也称为 Web-Only 型 SSL VPN。 • **适用场景**：点到站点（Point-to-Site）的访问，适用于远程用户通过 Web 浏览器接入公司内网资源的场景，需要对用户的接入进行精细的访问控制。 • **优点**：配置最少，通过浏览器访问，无需安装客户端。 • **缺点**：仅限于 HTTP/HTTPS 网站的访问。
	• **VPN 类型**：13.2.9 SSL VPN 隧道 • **描述**：指 SSL VPN 客户端与 NISG-IPS 之间利用 SSL 建立隧道，客户端通过这条隧道与受保护的子网或网站进行安全通信。这种通信方式称为隧道型 SSL VPN。 • **适用场景**：点到站点（Point-to-Site）的访问，适用于远程用户通过隧道接入公司内网资源的场景，需要对用户的接入进行精细的访问控制。 • **优点**：既可访问子网，也可访问网站，并且可访问的网站类别不受限。 • **缺点**：需要在远程主机上安装客户端软件。

此外， NISG-IPS 支持如下 IPSec VPN 功能：

- 13.1.1 NAT 穿越
- 13.1.2 隧道组

13.1.1 NAT 穿越

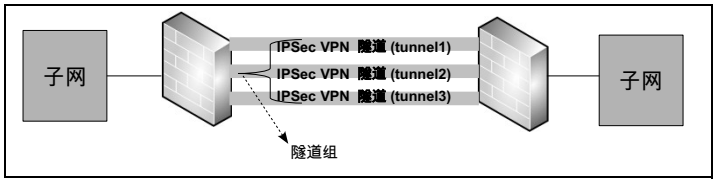
由于 IPSec VPN 与 NAT 互不兼容，如果在 VPN 隧道之间或远程用户与 VPN 隧道之间存在 NAT 设备，就会导致隧道通信失败，此时需要启用 NAT 穿越功能。 NAT 穿越只涉及 IPSec 自动密钥隧道， SSL VPN 的访问则不受 NAT 设备的限制。具体配置，参见 13.4.6 范例：NAT 穿越。



- 对于源地址转换 （SNAT），网关 A 可以主动发起隧道协商，而网关 B 因为 SNAT 规则的存在不能发起协商。
- 对于目的地址转换（DNAT），网关 A 和 B 都可以主动发起隧道协商。VPN 网关 A 发起的包不受 NAT 设备保护。
- 对于地址映射 （MIP），隧道任意一端都可以发起隧道协商，且 VPN 网关 A 发起的包是受保护的。

13.1.2 隧道组

隧道组是一组自动密钥隧道的集合，可以起到故障冗余的作用。一个隧道组中只有一个成员隧道处于工作状态，其余隧道处于备份状态。当处于工作状态的隧道发生故障时，将从其余可用的隧道中协商选出一个优先级最高的隧道继续工作。更多配置，参见 13.4.7 范例：IPSec VPN 隧道组。



13.2 基本配置步骤

本节描述了 NISG-IPS VPN 的基本配置步骤。

IPSec VPN

GRE VPN

SSL VPN

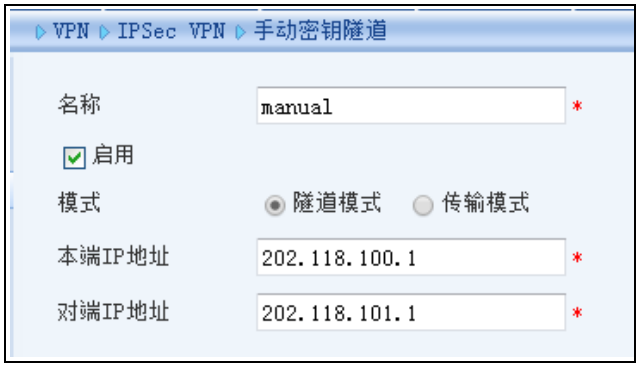
IP 地址池

13.2.1 网段到网段手动密钥隧道

管理员需要在两个网关设备上分别创建一条手动密钥隧道，下面以其中一个网关配置为例，另外的网关配置与此类似。

13.2.1.1 配置手动密钥隧道

1. 选择 **VPN** > **IPSec VPN** > **手动密钥隧道**。
2. 点击**新建**，创建一条手动密钥隧道。



- **名称：**隧道名称。长度 1-63 字节，UTF-8 字符，不能包含空格和以下字符：? , " ' \ < > & #。
- **模式：**包括隧道模式和传输模式。
  - **隧道模式 （默认）：**使用广泛，可以保护 VPN 网关后端的子网。
  - **传输模式 ：**使用较少，无法保护 VPN 网关后端的子网，只能保护 VPN 网关之间的数据传输。
- **本端 / 对端 IP 地址：**本端 / 对端网关设备出口接口的 IP 地址。

3. 配置 SA 参数 （认证和加密）。

提示：AH 和 ESP 都可以提供认证服务，但是 AH 提供的认证服务要强于 ESP。管理员可以根据实际安全需求，同时使用 AH 和 ESP，或选择其中一种。需要注意，两端设备的加密和认证算法必须相同， SPI 不能相同。

a. ESP：Encapsulating Security Payload （ESP）协议定义了加密算法和可选的认证机制，保证数据传输的机密性和完整性。
   - **加密算法 / 密钥：**用于对 IP 数据包进行加密的算法和对应的密钥。
   - **认证算法 / 密钥：**用于对 IP 数据包进行验证的算法和对应的密钥。
   - **本端 / 对端 SPI：**用于标识所建立的 SA 的本端和对端 SPI。必填项，为 8 位十六进制数，范围为 00000100-2FFFFFFF。

b. AH：Authentication Header （AH）协议定义了认证机制，只保证数据的源认证和完整性，不保障机密性。一般用于传输非机密性或不能加密的数据。
   - **认证算法 / 密钥：**参数解释同 ESP 认证算法 / 密钥。
   - **本端 / 对端 SPI：**参数解释同 ESP 本端 / 对端 SPI。

4. 点击**确定**。
5. 点击 。

13.2.1.2 隧道引流

选择**防火墙** > **访问策略**或者**网络** > **路由**，在策略或者路由中引用隧道，将匹配的数据包引入到隧道，这两种方式之间没有明显的差异。管理员需要在两端网关设备上分别进行隧道引流；可以在两端网关都使用路由或策略，也可以在一端网关使用路由引流，另外一端使用策略引流。

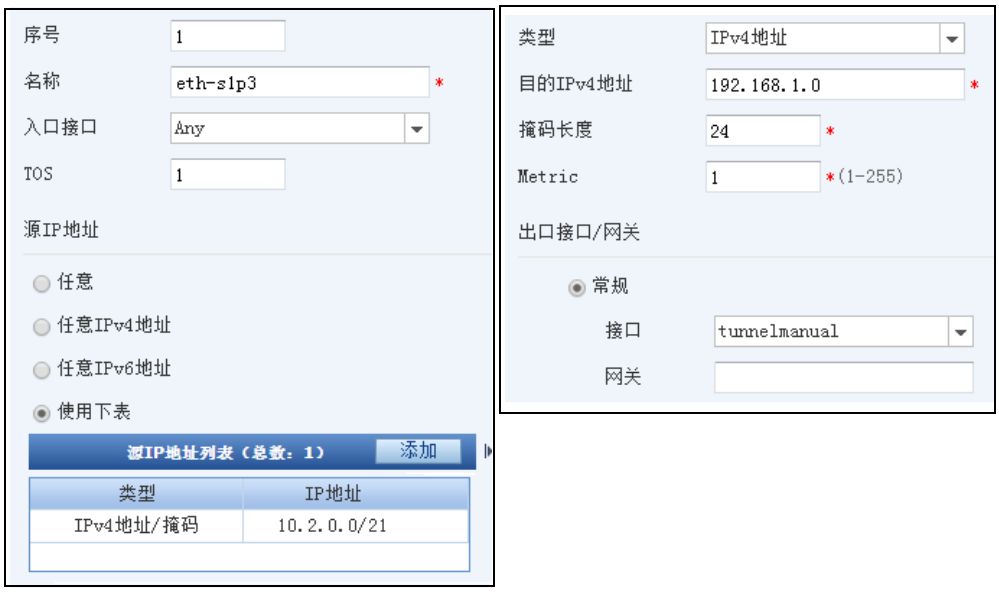
13.2.1.2.1 路由引流

管理员可以通过如下几种类型的路由，对数据进行引流：

- 选择**网络** > **路由** > **缺省路由**，新建静态路由引用隧道接口：

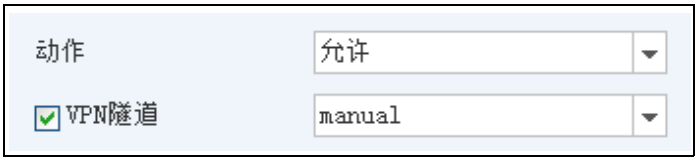
提示：在成功创建手动密钥隧道的同时，系统也将自动生成一个隧道接口tunnelmanual。选择**网络 > 接口**可以查看隧道接口。

- 选择**网络** > **路由** > **策略路由**，新建路由策略。在该策略路由的路由表中添加路由引用隧道接口。



13.2.1.2.2 访问策略引流

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建策略。
3. 点击策略对应的 ，引用 VPN 隧道，将本端子网向对端相应子网发起访问的数据流指向 VPN 隧道。
4. 引用隧道。



5. 点击**确定**。
6. 点击 。

13.2.1.3 预期结果

当一端主机向对端发起访问请求时，隧道将立即生效。选择**监控** > **IPSec VPN 隧道** > **手动密钥隧道**，查看隧道信息。

表 224 手动密钥隧道命令

show tunnel	显示指定的 VPN 隧道信息。
show tunnels manual	显示所有手动密钥隧道信息。
tunnel manual gateway	添加网关到网关的手动密钥隧道。
unset tunnel	删除 VPN 隧道。
unset tunnels manual	删除所有手动密钥隧道。

13.2.2 网段到网段自动密钥隧道

管理员需要在两个网关设备上分别创建一条自动密钥隧道，下面以其中一个网关配置为例，另外的网关配置与此类似。

13.2.2.1 配置自动密钥隧道

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条自动密钥隧道。

- **名称：**隧道名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
- **启用 NAT 穿越：**在隧道两端之间存在 NAT 设备的情况下，需要开启该功能，并设置发送 NAT Keepalive 数据报文的时间间隔。
- **对端类型：**隧道对端类型，包含静态 IP 地址、动态 IP 地址、拨号用户和拨号用户组。
- **永久：**当对端类型为静态 IP 地址时，可以将隧道设置为永久隧道，即隧道启用后立即主动发起协商，否则仅当有流量经过隧道时才发起协商。
- **出口：**自动密钥隧道的协商接口。
- **本端IP地址：**自动密钥隧道出口接口的IP地址，Any表示包括该接口上的所有IP地址。

- **认证方式：**对对端进行身份认证时采用的方式，包括：
  - **预共享密钥认证：**加密解密速度快，但安全性和可靠性不高。预共享密钥值需要用户事先互相协商达成一致，两端必须相同。
  - **证书认证：**加密解密速度慢，但是安全性和可靠性高，可防止信息否认。

3. 设置本端和对端受保护的子网。

- 如果对端类型为拨号用户或拨号用户组，则只能设置本端子网；
- 如果对端类型为静态 IP 地址或动态 IP 地址，则必须成对设置本端子网和对端子网。
- 如果两端设备之间存在 NAT 设备，则必须成对设置本端和对端子网。

4. 进行隧道高级设置 （可选，通常情况下使用默认值即可）。

a. 阶段 1：

- **自定义提议集：**IKE 交换第一阶段使用的提议集。
- **协商模式：**主模式和激进模式。

  •**主模式 （默认）：**通过六条消息完成 IEK 阶段一的信息交换，生成加密和认证密钥，并认证双方身份。

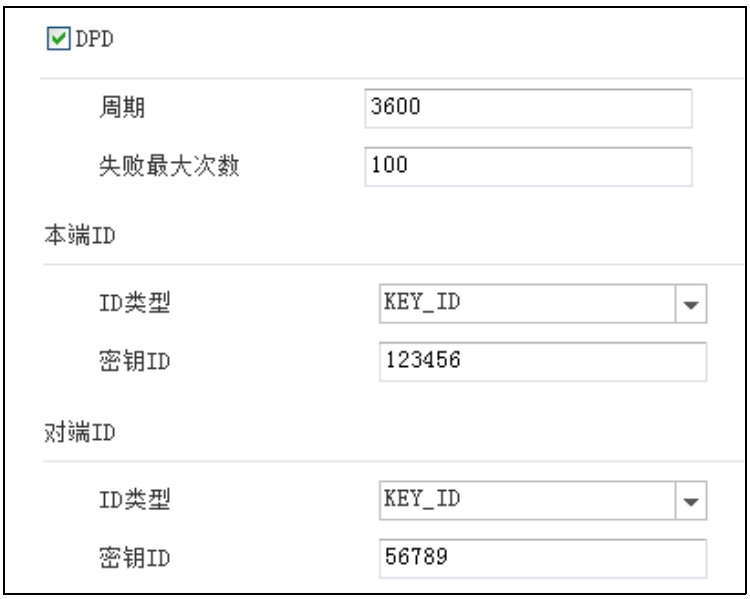
  ■**激进模式：**通过三条消息完成 IKE 阶段一的信息交换，减少了信息交换次数，但不能对双方的身份信息进行保护。
- **生存时间：**第一阶段协商生成的 IKE SA 的生存时间，超过设置的时间后，将重新生成 IKE SA。输入范围为 180-2147483647。

b. 阶段 2：

- **自定义提议集：**IKE 交换第二阶段使用的提议集。四个自定义提议集必须类型相同，如果第一个自定义提议集以 g2 开头，则其他三个也必须以 g2 开头。
- **抗重放攻击：**重放攻击防护。
- **工作模式：**传输模式和隧道模式。

  ■**隧道模式 （默认）：**使用广泛，可以保护 VPN 网关后端的子网。

  ■**传输模式：**使用较少，无法保护 VPN 网关后端的子网，只能保护 VPN 网关之间的数据传输。
- **生存时间：**第二阶段协商生成的 IPSec SA 的生存时间，超过生存时间后，将会重新生成 IPSec SA。输入范围为 180-2147483647。

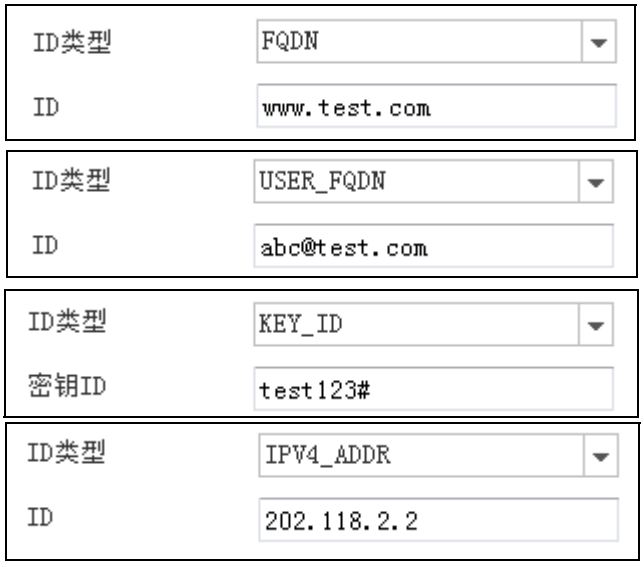


- **失效对等体检测 （DPD）：**通过发送 Keepalive 报文来探测对端的状态。发送周期范围为 1-3600 秒，重试次数范围为 2-32767。
- **本端和对端 ID：**在 IKE 协商过程中对本端和对端身份进行认证的标识，包括：
  - **IPV4_ADDR：**输入 IP 地址作为标识。
  - **FQDN：**输入完全合格域名作为标识。
  - **USER_FQDN：**输入邮件地址作为标识。

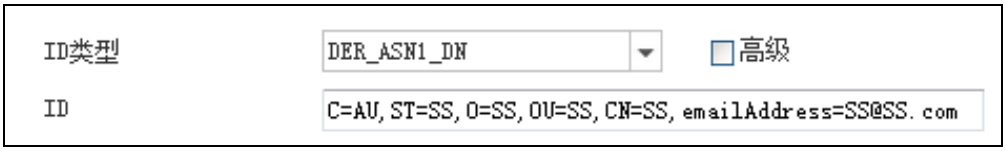
- **DER_ASN1_DN**：输入固定的格式作为标识（例如 C=country,ST=state,L=city,O=company,OU=department,CN=user, emailAddress=mail）。
- **KEY_ID**：输入字符串作为标识，长度 1-1023 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&。

如果 VPN 网关设备之间存在 NAT 设备：

- 使用预共享密钥认证时，ID 类型可设置为以下任意一种；



- 使用证书认证时，ID 类型需设置为 DER_ANS1_DN。ID 与本地证书主题相同，选择**系统 > 证书 > 本地证书**查看主题。



5. 点击**确定**。
6. 点击 。

13.2.2.2 预期结果

选择**防火墙 > 访问策略**或者**网络 > 路由**，在策略或者路由中引用隧道，将匹配的数据包引入到隧道。更多信息，参见 13.2.1.2 隧道引流。当一端主机向另一端发起访问请求时，一条自动密钥隧道将通过协商成功建立。选择**监控 > IPSec VPN 隧道 > 自动密钥隧道**，查看隧道信息。

表 225 自动密钥隧道命令

show tunnel	显示指定的 VPN 隧道信息。
show tunnels auto	显示所有自动密钥隧道信息。

表 225 自动密钥隧道命令 (*续*)

tunnel enable, disable	启用或禁用指定的 VPN 隧道。
tunnel nat-traversal auto enable, disable	启用或禁用自动密钥隧道的 NAT 穿越功能。
tunnel gateway certificate	添加证书认证方式的网关到网关自动密钥隧道。
tunnel gateway preshared-key	添加预共享密钥认证方式的网关到网关自动密钥隧道。
tunnel remote	设置自动密钥隧道对端的 IP 地址。
tunnel interface	设置自动密钥隧道本端出口和本端 IP 地址。
tunnel permanent on, off	设置自动密钥隧道类型为永久或普通。
tunnel certificate	设置自动密钥隧道的认证方式为证书认证，并设置证书。
tunnel preshared-key	设置自动密钥隧道的认证方式为预共享密钥认证，并设置预共享密钥。
tunnel local-subnet	设置自动密钥隧道本端子网。
unset tunnel local-subnet	删除自动密钥隧道的本端子网。
tunnel local-subnet remote-subnet	设置自动密钥隧道本端子网和对端子网。
unset tunnel local-subnet remote-subnet	删除自动密钥隧道的本端子网和对端子网。
tunnel ike phase1	设置自动密钥隧道协商的第一阶段属性。
tunnel ike phase1 default	设置自动密钥隧道协商的第一阶段属性为缺省值。
tunnel ike phase2	设置自动密钥隧道协商的第二阶段属性。
tunnel ike phase2 default	设置自动密钥隧道协商的第二阶段属性为缺省值。
tunnel ike lifetime	设置第一阶段或第二阶段 SA 的生存时间。
tunnel ike dpd	设置自动密钥隧道的 DPD 属性。
tunnel ike dpd disable	禁用自动密钥隧道的 DPD 功能。
tunnel ike	设置自动密钥隧道本端或对端的 IKE ID。
unset tunnel	删除 VPN 隧道。
unset tunnels auto	删除所有自动密钥隧道。

13.2.3 远程访问自动密钥隧道

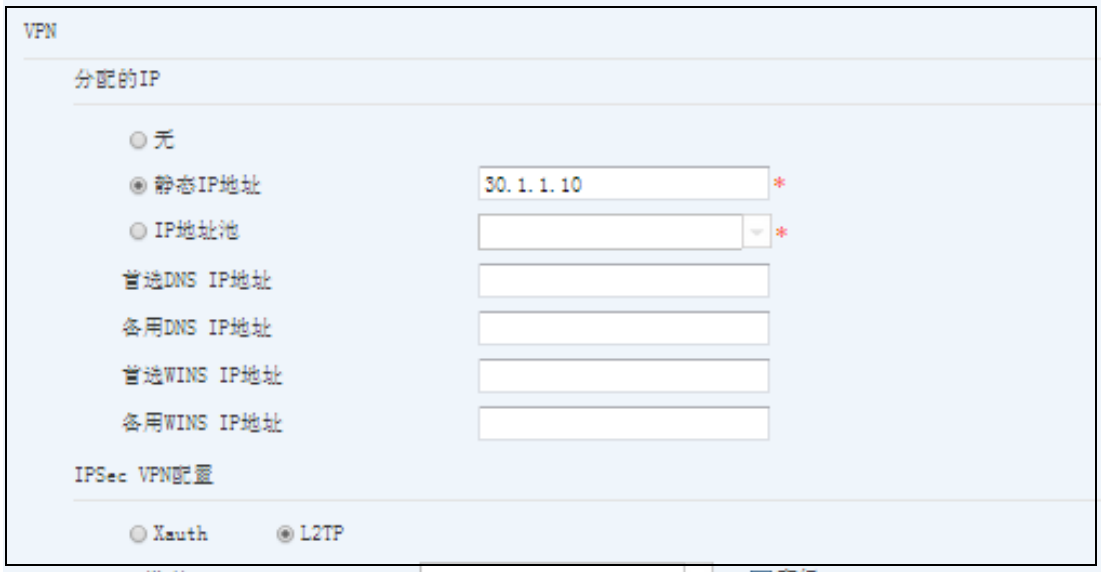
IPSec VPN 远程访问只能使用自动密钥隧道，不能使用手动密钥隧道。

13.2.3.1 创建 IPSec VPN 用户

1. 选择**系统 > 认证 > 网络用户**，创建类型为 IPSec VPN 的用户。

- **认证类型：**包括本地认证和外部认证。
- **使用特定超时时间：**设置 WebAuth 或 SSL VPN 用户的超时时间，范围是 0-3600 秒。该项设置不适用于 IPSec VPN 用户。
- **用户类型：**包括 WebAuth、 IPSec VPN 和 SSL VPN。多点登录即允许用户使用同一账号同时从不同地点登录。

2. 设置如何分配 IP 地址，设置认证 ID 类型。



a. 分配的 IP：

- **无**：不分配 IP 地址。该项只对 Xauth 用户有效，且其隧道模式需要为传输模式。
- **静态 IP 地址**：NISG-IPS 分配给远程用户的 IP 地址，可以是任意 IP 地址，不能与 NISG-IPS 上已有三层接口的 IP 地址重复。
- **IP 地址池**：NISG-IPS 将从已有地址池中分配一个 IP 地址给远程用户。
- **DNS/WINS IP 地址**：NISG-IPS 可为远程用户分配主备 DNS 服务器地址及主备 WINS 服务器地址。

b. IPSec VPN 配置类型：

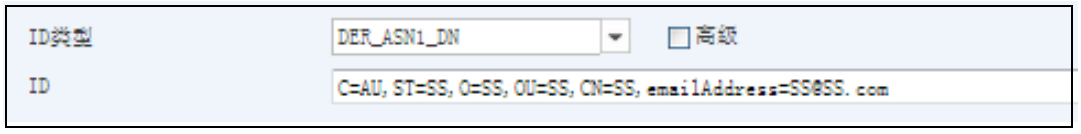
- **Xauth**：用户使用 Xauth 认证。
- **L2TP**：用户使用 L2TP 认证。

c. **ID 类型**：包括 IPV4_ADDR、 FQDN、 USER_FQDN、 DER_ASN1_DN 和 KEY_ID。

a.当 L2TP 远程用户与 NISG-IPS 之间存在 NAT 设备时：

■使用预共享密钥认证时，ID 类型需设置为 FQDN ；

- 使用证书认证时，ID 类型需设置为 DER_ANS1_DN。



b. 当Xauth远程用户与NISG-IPS之间存在NAT设备时，如果是预共享密钥认证，ID类型需设置为FQDN、USER_FQDN或KEY_ID；如果是证书认证，ID类型需设置为DER_ANS1_DN。

3. 点击**确定**。

4. 点击 。

表 226 IPSec VPN 用户命令

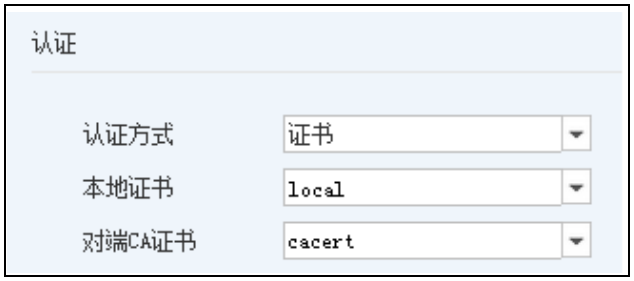
show user authuser	显示网络用户的相关信息。
user authuser enable, disable	启用或禁用网络用户。
user authuser authtype	添加网络用户，并设置本地或外部认证方式。
unset user authuser	删除网络用户。
user authuser timeout	设置络用户的超时时间。
user authuser ipsecvpn multipoint	设置 IPSec VPN 用户是否可以进行多点登录。
user authuser password	设置网络用户的口令。
user authuser assigned-ip	为网络用户分配 IP 地址、 DNS 地址和 WINS 地址。
user authuser ipsecvpn ike-id type	为 IPSec VPN 用户设置其 ID 类型。
unset user authuser ipsecvpn	删除网络用户的 IPSec VPN 角色。

13.2.3.2 创建自动密钥隧道

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条自动密钥隧道。具体参数配置可参见 13.2.2 网段到网段自动密钥隧道。

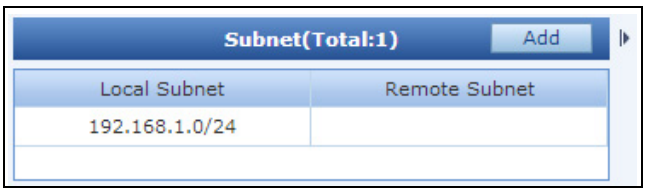
3. 设置认证方式（可任选一种）。
   - 若使用预共享密钥认证，需要输入已协商好的密钥。

   - 若使用证书认证，需要上载本地证书和对端的 CA 证书。



     - 选择**系统** > **证书** > **CA 证书**，点击**导入**，导入对端远程用户的 CA 证书。
     - 选择**系统** > **证书** > **本地证书**，点击**导入**，导入本地证书。

4. 设置本端受保护的子网。



   - 对于 Xauth 认证用户，该项必须设置。
   - 对于 L2TP 认证用户，该项不必设置。

5. 进行隧道高级设置 （可选）。
6. 点击**确定**。
7. 点击 。

表 227 自动密钥隧道命令

show tunnel	显示指定的 VPN 隧道信息。
show tunnels auto	显示所有自动密钥隧道信息。
tunnel dialup-user, dialup-group certificate	添加一条自动密钥隧道，对端为远程用户或用户组，认证方式为证书认证。
tunnel dialup-user, dialup-group preshared-key	添加一条自动密钥隧道，对端为远程用户或用户组，认证方式为预共享密钥认证。
tunnel enable, disable	启用或禁用指定的 VPN 隧道。
tunnel nat-traversal auto enable, disable	启用或禁用自动密钥隧道的 NAT 穿越功能。
tunnel remote user, group	设置自动密钥隧道对端的用户或用户组。
tunnel remote	设置自动密钥隧道对端的 IP 地址。
tunnel interface	设置自动密钥隧道本端出口和本端 IP 地址。
tunnel certificate	设置自动密钥隧道的认证方式为证书认证，并设置证书。
tunnel preshared-key	设置自动密钥隧道的认证方式为预共享密钥认证，并设置预共享密钥。
tunnel local-subnet	设置自动密钥隧道本端子网。
unset tunnel local-subnet	删除自动密钥隧道的本端子网。
tunnel local-subnet remote-subnet	设置自动密钥隧道本端子网和对端子网。
unset tunnel local-subnet remote-subnet	删除自动密钥隧道的本端子网和对端子网。

表 227 自动密钥隧道命令 (*续*)

tunnel ike phase1	设置自动密钥隧道协商的第一阶段属性。
tunnel ike phase1 default	设置自动密钥隧道协商的第一阶段属性为缺省值。
tunnel ike phase2	设置自动密钥隧道协商的第二阶段属性。
tunnel ike phase2 default	设置自动密钥隧道协商的第二阶段属性为缺省值。
tunnel ike lifetime	设置第一阶段或第二阶段 SA 的生存时间。
tunnel ike dpd	设置自动密钥隧道的 DPD 属性。
tunnel ike dpd disable	禁用自动密钥隧道的 DPD 功能。
tunnel ike	设置自动密钥隧道本端或对端的 IKE ID。
unset tunnel	删除 VPN 隧道。
unset tunnels auto	删除所有自动密钥隧道。

13.2.3.3 配置客户端

1. IPSec VPN远程用户需要安装NISG-IPS VPN客户端软件或使用Windows内置的客户端程序。
2. 进行客户端具体配置。若使用证书认证，需要将 NISG-IPS 的 CA 证书和本端的本地证书导入客户端。

13.2.3.4 预期结果

远程用户通过客户端进行拨号，连接到 NISG-IPS，一条自动密钥隧道随之成功建立。管理员可以选择**监控 > IPSec VPN 隧道 > 自动密钥隧道**，查看 VPN 隧道的监控信息。

13.2.4 隧道组

13.2.4.1 事先准备

以下介绍如何配置包含三条隧道的隧道组，管理员需要首先进行如下操作：

1. 选择**网络** > **接口**，选择三个三层接口，并配置 IP 地址；
2. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**，创建三条自动密钥隧道，它们的出口接口都指向上述三层接口。优先级最高的隧道在划分到隧道组中后，将处于工作状态。

13.2.4.2 配置隧道组

1. 选择 **VPN** > **IPSec VPN** > **隧道组**。
2. 点击**新建**，创建隧道组，并添加要包含的隧道。

   - 隧道组中只能包含网段到网段的自动密钥隧道，一个隧道组最多包含 16 条隧道。
   - 一条隧道只能从属于一个隧道组。
   - 隧道组中包含的隧道的优先级为 0-255 之间的整数，数值越大，优先级越高。
3. 点击**确定**。
4. 点击 。

表 228 自动密钥隧道组命令

show tunnelgroup	查看指定的隧道组配置信息。
show tunnelgroups	查看所有的隧道组配置信息。
tunnelgroup	添加隧道组。
unset tunnelgroup	删除指定的隧道组。
tunnelgroup tunnel priority	向指定的隧道组中添加隧道成员。
unset tunnelgroup	删除指定的隧道组。
unset tunnelgroup tunnel	删除指定隧道组中的隧道成员。
unset tunnelgroups	删除所有的隧道组。

13.2.4.3 预期结果

然后选择**防火墙 > 访问策略**或者**网络 > 路由**，在策略或者路由中引用隧道组，将匹配的数据包引入到隧道组。两端可以通过处于工作状态的隧道进行通信。管理员可以选择**监控 > IPSec VPN 隧道 > 隧道组**，查看隧道组信息；或者选择**监控 > IPSec VPN 隧道 > 自动密钥隧道**，查看成员隧道信息。

13.2.5 IPSec VPN 用户组

IPSec VPN 用户组是 IPSec VPN 用户的集合，可以包括本地和外部创建的用户，用户组可以通过自动密钥隧道对受 NISG-IPS 保护的子网进行远程访问。

1. 选择 **VPN > IPSec VPN > 用户组**。
2. 点击**新建**，创建一个用户组。

- **包含外部用户**：用户组包含的外部用户，包括 Xauth 认证用户和 L2TP 认证用户。
- **用户列表**：用户组包含的 IPSec VPN 用户，一个用户只能为一个用户组所包含。

3. 点击**确定**。
4. 点击 。

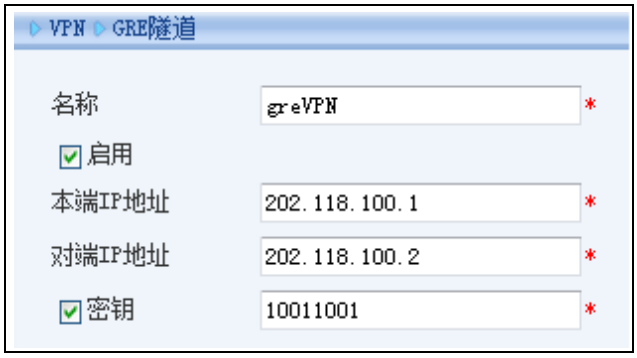
表 229 IPSec VPN 用户组命令

group	添加 IPSec VPN 用户组。
unset group	删除 IPSec VPN 用户组。
group external	设置指定的 IPSec 用户组是否包含外部 IPSec VPN 用户。
group user	添加 IPSec VPN 用户到用户组中。
unset group user	从用户组中删除 IPSec VPN 用户。
show vpn group	显示 IPSec VPN 用户组的配置信息。

13.2.6 GRE 隧道

13.2.6.1 配置 GRE 隧道

1. 选择 **VPN** > **GRE 隧道**。
2. 点击**新建**，创建一条隧道。



   - **隧道名称**：GRE 隧道名称。长度 1-63 字节，UTF-8 字符。
   - **本端和对端 IP 地址**：本端和对端 NISG-IPS 设备所使用出口接口的 IP 地址。
   - **密钥** （可选）：GRE 隧道的标识，范围为 0-4294967295。
3. 点击**确定**。
4. 点击 。

13.2.6.2 预期结果

选择**防火墙** > **访问策略**或者**网络** > **路由**，在策略或者路由中引用隧道，将匹配的数据包引入到隧道。更多信息，参见 13.2.1.2 隧道引流。当一端主机向另一端发起访问请求时，一条 GRE VPN 隧道将成功建立。管理员可以选择**监控** > **GRE 隧道**，查看 GRE 隧道信息。

表 230 GRE 隧道命令

show tunnel	显示指定的 GRE 隧道信息。
show tunnels gre	显示所有 GRE 隧道信息。
tunnel enable, disable	启用或禁用指定的 GRE 隧道。
tunnel gre	添加 GRE 隧道。
unset tunnel	删除指定的 GRE 隧道。
unset tunnels gre	删除所有 GRE 隧道。

13.2.7 SSL VPN 用户组

为了方便管理，将一组类型相同，具有相同应用或服务访问需求的用户划分为一个 SSL VPN 用户组，每个用户组由一个组名来标识。管理员需要指定 SSL VPN 用户组进行 SSL VPN 连接。

1. 选择 **VPN > SSL VPN > 用户组**。
2. 点击**新建**，创建一个用户组。

- **用户列表**：用户组包含的 SSL VPN 用户，一个用户只能为一个用户组所包含。
- **包含外部用户**：用户组是否包含外部 SSL VPN 用户。

3. 点击**确定**。
4. 点击 。

提示：管理员可以修改正被 SSL VPN 服务使用的 SSL VPN 用户组，但不能删除。

表 231 SSL VPN 用户组命令

group	添加 SSL VPN 用户组。
unset group	删除 SSL VPN 用户组。
group external	设置指定的 SSL VPN 用户组是否包含外部 SSL VPN 用户。
group user	将 SSL VPN 用户添加到用户组中。
unset group user	从用户组中删除 SSL VPN 用户。
show sslvpn group	显示 SSL VPN 用户组的配置信息。

13.2.8 SSL VPN Web 入口页面访问

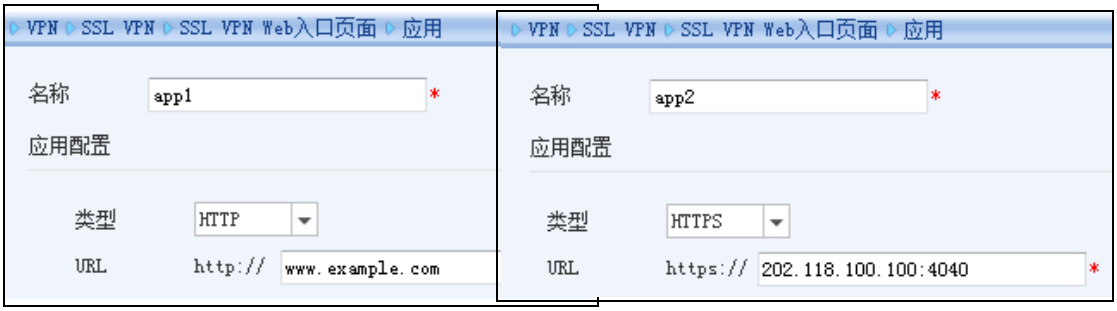
13.2.8.1 事先准备

在配置 SSL VPN 的 Web 入口页面前，管理员可能需要首先进行如下操作：

- 选择**系统** > **证书**，导入 CA 证书和 SSL 本地证书；
- 选择**系统** > **认证** > **网络用户**，创建 SSL VPN 用户；
- 选择 **VPN** > **SSL VPN** > **用户组**，创建 SSL VPN 用户组，包含 SSL VPN 用户。

13.2.8.2 配置应用

1. 选择 **VPN** > **SSL VPN** > **SSL VPN Web 入口页面** > **应用**。
2. 点击**新建**，添加新的应用。



   - **类型**：SSL VPN 应用的类型，包括 HTTP 和 HTTPS。
   - **URL**：SSL VPN 应用的地址，包括域名和 IP 地址。
3. 点击**确定**。

提示：被 SSL VPN 页面模板引用的 SSL VPN 应用不能被删除。

表 232 SSL VPN 应用命令

application	添加 SSL VPN 应用。
unset application	删除 SSL VPN 应用。
application type	设置 SSL VPN 应用的类型。
application url	设置 SSL VPN 应用的地址。
show sslvpn application	显示 SSL VPN 应用的配置信息。

13.2.8.3 配置页面模板

1. 选择 **VPN > SSL VPN > SSL VPN Web 入口页面 > 页面模板**。
2. 点击**新建**，创建新的页面模板。

- **入口页面设置：**设置在入口页面上方显示的标题、主题颜色、 Logo 以及页面语言，包括英文和简体中文。

  导入 Logo 图片时，要求为 jpg、gif、png 或 bmp 格式，图片规格为 15 x 80 像素。文件大小不能超过 150 KB。选择 Logo 图片后可以在预览区域查看实际显示效果。上传长度为 0 的空文件时， Logo 显示为空白。
- **应用设置：**包括应用类型、名称和 URL 地址；还可以设置分割线，用于在入口页面上分开两种应用。
- **允许自定义应用：**管理员可以在入口页面自定义更多的应用。

提示：一个应用可被多个页面模板同时引用。被服务引用的模板不可删除，但可修改。

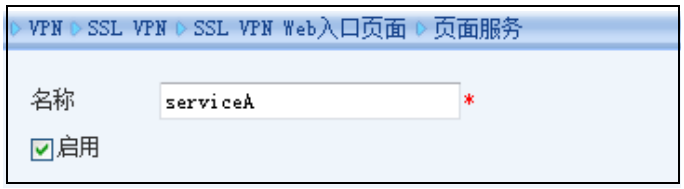
3. 点击**确定**。

表 233 SSL VPN 页面模板命令

portal-template	添加 SSL VPN 页面模板。
unset portal-template	删除 SSL VPN 页面模板。
portal-template applist	将指定应用添加到 SSL VPN 页面模板的应用列表中。
unset portal-template applist	从 SSL VPN 页面模板的应用列表中删除应用。
portal-template applist tag	将分割线添加到 SSL VPN 页面模板的应用列表中。
portal-template applist tag clear	从 SSL VPN 页面模板的应用列表中清除全部分割线。
portal-template customapp	设置是否允许用户在入口页面添加指定协议的自定义应用。
portal-template language	设置 SSL VPN 页面模板的语言，包括简体中文和英文。
portal-template themecolor	设置 SSL VPN 页面模板的主题颜色。
portal-template title	设置 SSL VPN 页面模板的标题名称。
unset portal-template title	删除 SSL VPN 页面模板的标题名称。
show sslvpn portal-template	显示 SSL VPN 页面模板的配置信息。

13.2.8.4 配置页面服务

1. 选择 **VPN** > **SSL VPN** > **SSL VPN Web 入口页面** > **页面服务**。
2. 点击**新建**，创建新的页面服务。



3. 设置服务绑定。

- **服务绑定：**定义了 SSL VPN 对外提供服务的接口、 IP 地址和端口号。每个 SSL VPN 服务最多可以绑定 4 个 IP 地址和端口对。

- **接口：**提供 SSL VPN 服务的三层接口，环回接口、隧道接口和虚拟接口除外。
- **IP 地址：**三层接口的 IP 地址， Any 表示该接口上的所有 IP 地址。
- **端口：**提供 SSL VPN 服务的端口号。

4. 进行服务配置。

- **用户组列表：**服务包含的 SSL VPN 用户组，列表中的用户组成员可以访问该服务。
- **入口页面：**用户访问 SSL VPN 服务后能够看到的 Web 页面。
- **会话超时：**用户访问 SSL VPN 服务后不进行任何操作后自动登出时的时间，范围为 0-60000 秒。当超时时间设置为 0 时，除非用户关闭浏览器，否则登录后永不超时。
- **登录失败上限：**连续登录失败最大次数，超过上限该登录 IP 将被锁定。取值范围为 0-10 的整数，0 表示没有登录失败上限。
- **登录时需要验证码：**用户访问 SSL VPN 服务时需要在入口页面输入验证码。
- **验证用户证书：**勾选该选项表示启用对客户端和服务器端证书的双向认证，否则只进行服务器端证书的单向认证。
- **保存用户配置：**将用户自定义应用保存在系统上。但当 SSL VPN 服务所使用的页面模板不允许用户自定义应用时，此选项失去作用。
- **允许用户修改密码：**允许用户修改 SSL VPN 入口页面的密码，新密码将在用户下次登录通过验证时生效。

5. 进行 SSL 配置。

- **SSL 证书：**SSL VPN 服务端的证书，只能选择本地证书类型。
- **支持的 SSL 版本：**包括三个版本。当三个选项全不勾选时，用户将无法访问 SSL VPN 服务。
- **算法等级：**加密算法强度，包括高、中、低。级别越高，安全性越高。

6. 设置用户使用的操作系统以及浏览器必须满足的安全性要求 （使用默认设置即可）。

7. 设置允许访问 SSL VPN 服务的地址和安全域。

- 管理员可以设置单个 IP 地址或 IP 地址段。
- IP 地址和入口安全域共同组成一个访问条目，系统最多支持 32 个条目。
- 入口安全域为 Any，表示允许意安全域的访问。

8. 配置用户组访问授权。用户可以向**用户组访问授权列表**添加访问条目，以允许或拒绝用户组访问特定的应用。用户也可以对不在上述列表中的用户组和应用指定一个缺省处理动作。

9. 点击**确定**。
10. 点击 。

表 234 SSL VPN 页面服务命令

portal-service	添加 SSL VPN 服务。
unset portal-service	删除 SSL VPN 服务。
portal-service allow	添加 SSL VPN 服务的允许访问条目。
unset portal-service allow	删除 SSL VPN 服务的允许访问条目。
portal-service client-security	设置 SSL VPN 服务对客户端安全性的要求。
portal-service client-security level	设置 SSL VPN 服务对客户端安全等级的要求。
portal-service certificate	设置 SSL VPN 服务的 SSL 证书。
portal-service config group	添加被 SSL VPN 服务引用的用户组。
unset portal-service config group	删除 SSL VPN 服务的用户组。
portal-service config logonfailtimes	设置 SSL VPN 服务的用户登录失败上限。
portal-service config logon-verify-code enable, disable	设置用户登录到 SSL VPN 服务时是否需要输入验证码。
portal-service config portal-template	设置 SSL VPN 服务的入口页面模板。
portal-service config save-user-config enable, disable	设置用户登录 SSL VPN 服务时是否保存用户的自定义设置。
portal-service config timeout	设置 SSL VPN 服务的用户会话超时时间。
portal-service config user-change-password enable, disable	设置用户登录到 SSL VPN 服务后是否允许其修改登录密码。

表 234 SSL VPN 页面服务命令 (*续*)

portal-service config verify-client-certificate enable, disable	设置用户登录到 SSL VPN 服务时是否验证用户 SSL 证书。
portal-service port	添加 SSL VPN 服务的 IP 地址和端口号。
unset portal-service port	删除 SSL VPN 服务的 IP 地址和端口号。
portal-service privilege default-user-privilege permit, forbid	设置 SSL VPN 服务的用户默认访问权限。
portal-service privilege group application	向 SSL VPN 服务的用户组访问授权表中添加一条用户组访问条目。
unset portal-service privilege group application	从 SSL VPN 服务的用户组访问授权表中删除一条用户组访问条目。
portal-service ssl cipher-level	设置 SSL VPN 服务的加密算法等级。
portal-service ssl ssl-version	设置 SSL VPN 服务支持的 SSL 版本。
show sslvpn portal-service	显示 SSL VPN 服务的配置信息。

13.2.8.5 预期结果

- 用户从客户端打开浏览器 , 输入 https://IP address:port, 进入 SSL VPN Web 入口页面；输入用户名和密码及 NetEye 的验证码，即可登录入口页面，点击页面上的超链接可以访问相应的应用。
- 管理员可登录NISG-IPS，选择**监控>在线用户>SSL VPN用户**，可以查看SSL VPN用户和隧道的相关信息。

13.2.9 SSL VPN 隧道

13.2.9.1 事先准备

在配置 SSL VPN 隧道前，管理员可能需要首先进行如下操作：

- 选择 **VPN** > **IP 地址池**，创建 IP 地址池；
- 选择**系统** > **认证** > **网络用户**，创建 SSL VPN 用户，并为用户分配地址池中的 IP 地址；

> **提示：**也可以为用户分配静态 IP 地址，但地址掩码必须是 255.255.255.252，例如 1.1.1.1 和 1.1.1.5。

- 选择 **VPN** > **SSL VPN** > **用户组**，创建 SSL VPN 用户组，包含 SSL VPN 用户。

13.2.9.2 配置 SSL VPN 隧道

1. 选择 **VPN** > **SSL VPN** > **SSL VPN 隧道** > **隧道**。
2. 点击**新建**，创建隧道。

- **用户组：**允许通过此 SSL VPN 隧道访问授权子网的用户组。
- **出口接口：**该 SSL VPN 隧道对外提供访问的接口。
- **本地 IP 地址：**出口接口的 IP 地址。当指定为 Any 时，表示包含该接口上的所有 IP 地址。
- **授权子网列表：**列出允许用户通过此 SSL VPN 隧道进行访问的网络。

3. 点击**确定**。
4. 点击 。

表 235 SSL VPN 隧道命令

tunnel enable, disable	启用或禁用 SSL VPN 隧道。
tunnel interface enable, disable	创建一条 SSL VPN 隧道。
unset tunnel	删除指定的 SSL VPN 隧道。
tunnel interface	设置隧道的出口接口和本端 IP 地址。
tunnel group	设置 SSL VPN 隧道绑定的 SSL VPN 用户组。
unset tunnel group	删除 SSL VPN 隧道绑定的 SSL VPN 用户组。
tunnel allowed-subnet	设置 SSL VPN 隧道的授权访问子网。
unset tunnel allowed-subnet	删除 SSL VPN 隧道的授权访问子网。
show sslvpn-tunnel configure	显示 SSL VPN 隧道的配置信息。

13.2.9.3 预期结果

用户可以启动 SSL VPN 客户端软件，连接到 SSL VPN 网关，并成功建立起一条 SSL VPN 隧道。通过该隧道，用户可进一步访问受保护的内部子网。选择**监控 > 在线用户 > SSL VPN 用户**，可以查看 SSL VPN 用户相关的隧道信息。

有关 SSL VPN 客户端安装和配置的详细信息，请参见*东软 NetEye SSL VPN Android 客户端用户使用指南*和*东软 NetEye SSL VPN Windows 客户端用户使用指南*。

13.2.10 IP 地址池

IP 地址池被用来为 IPSec VPN 用户和 SSL VPN 用户分配 IP 地址。

1. 选择 **VPN > IP 地址池**。
2. 点击**新建**，创建一个 IP 地址池。

- IP 地址池中的地址不能与已有地址池中的地址重复或重叠。
- 正在引用中的 IP 地址池不能删除。要删除该地址池，首先解除引用关系。

3. 点击**确定**。
4. 点击 。

表 236 IP 地址池命令

ippool	添加 IP 地址池或向已存在的 IP 地址池中添加 IP 地址。
unset ippool	删除 IP 地址池。
show vpn ippool	显示 IP 地址池的配置信息。

13.3 配置参数说明

本节介绍了 IPSec VPN 和 SSL VPN 的相关参数。

13.3.1 IPSec VPN 相关参数

在 IPSec VPN 隧道的配置过程中，会涉及到如下参数配置：

13.3.1.1 IPSec VPN 用户组参数

表 237 IPSec VPN 用户组参数

配置信息	说明
组名称	IPSec VPN 用户组名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
包含的用户	组内包含的在 NISG-IPS 上创建的 IPSec VPN 用户。
引用隧道	与 IPSec VPN 用户组关联的隧道。
包含外部用户	表示该用户组是否包含外部 Xauth 或 L2TP 用户。

13.3.1.2 自动密钥隧道参数

表 238 自动密钥隧道参数

参数	描述
名称	自动密钥隧道名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # 不能与现有的手动密钥隧道、隧道组、 GRE 隧道和 SSL VPN 隧道重名。
启用	启用或禁用自动密钥隧道。
启用 NAT 穿越	当隧道两端中间存在 NAT 设备时，需要启用 NAT 穿越功能。并且在 **Keepalive 间隔**文本框中输入发送 NAT Keepalive 数据报文的时间间隔。
对端类型	自动密钥隧道对端类型，包含： • **静态 IP 地址**：对端的 IP 地址或域名 • **动态 IP 地址**：表示对端 IP 地址通过 DHCP 服务器或 PPPoE 服务器获取 • **拨号用户**：对端的拨号用户名 • **拨号用户组**：对端的拨号用户组名称
永久隧道	当对端类型为静态 IP 地址时，可以将隧道设置为永久隧道，在被启用后立即主动发起协商，直到协商成功为止。而非永久隧道仅当有流量经过隧道时才发起协商。
出口	自动密钥隧道的协商接口。
本端 IP 地址	自动密钥隧道协商口的 IP 地址。 IP 选择 Any 时，表示包括该接口上的所有 IP 地址。
认证方式	在 IKE 协商过程中对对端进行身份认证时采用的认证方式，包括： • **预共享密钥认证**：加密解密速度快，但安全性和可靠性不高。 • **证书认证**：加密解密速度慢，但是安全性和可靠性高，可防止信息否认。
密钥	使用预共享密钥作为认证方式时，需要输入的用户事先互相协商好的密钥值。长度 1-127 字节， UTF-8 字符。不能包含？和空格。 本端和对端的密钥必须相同。
本地证书	使用证书作为认证方式时，用于验证本端身份的证书。
对端 CA 证书	使用证书作为认证方式时，用于验证对端身份的 CA 证书。 CA 证书选择 any 时，表示包括 NISG-IPS 上的所有 CA 证书。

表 238 自动密钥隧道参数 (*续*)

参数	描述
本端 / 对端子网	受 VPN 网关保护的本端或对端子网。不支持多播地址 224.0.0.0-255.255.255.255，不能以 0 开头， NISG-IPS 最多支持 32 个本端或对端子网。 要创建多 SA 的 VPN 自动密钥隧道，用户需要配置多个本端和对端子网，两者必须成对添加。
高级设置	
在阶段 1 中，通讯双方协商 IKE SA。	
自定义提议集	第一阶段使用的提议集包括： • g1-3des-md5, g1-3des-sha1, g1-aes128-md5, g1-aes128-sha1。 • g2-3des-sha1, g2-3des-md5, g2-aes128-sha1, g2-aes128-md5, g2-aes192-md5, g2-aes192-sha1, g2-aes256-md5, g2-aes256-sha1。 • g5-3des-md5, g5-3des-sha1, g5-aes256-md5, g5-aes256-sha1。 可以选择一到四个提议集，每个提议集都提示了在阶段 1 中使用的算法： • **g1/g2/g5**：使用 DH 组 （一种非对称加密算法）用于密钥交换，对应的密钥长度分别是 768、 1024 和 1536 比特。 • **aes/3des**：使用的对称加密算法。 • **sha1/md5**：使用的 Hash 函数。
模式	指定自动密钥隧道使用的隧道模式，包括： • **主模式 （默认）**：通过六条消息完成 IEK 阶段一的信息交换，生成加密和认证密钥，并认证双方身份。 • **激进模式**：通过三条消息完成 IKE 阶段一的信息交换，减少了信息交换次数，但不能对双方的身份信息进行保护。
生存时间	第一阶段协商生成的 IKE SA 的生存时间，超过设置的时间后，将重新生成 IKE SA。输入范围为 180-2147483647，单位为秒。
在阶段 2 中，通讯双方协商 IPSec SA。当用户使用国密办加密卡时，系统将显示 SCB2 提议集信息。	
自定义提议集	第二阶段使用的提议集包括： • nopfs-esp-3des-md5, nopfs-esp-3des-sha1, nopfs-esp-aes128-md5, nopfs-esp-aes128-sha1, nopfs-esp-scb2-sha1, nopfs-esp-scb2-md5。 • g1-esp-3des-sha1, g1-esp-aes128-md5, g1-esp-scb2-sha1, g1-esp-scb2-md5。 • g5-esp-3des-md5, g5-esp-3des-sha1, g5-esp-aes128-md5, g5-esp-aes128-sha1, g5-esp-scb2-sha1, g5-esp-scb2-md5。 • g2-ah-md5, g2-ah-sha1。 • g2-esp-aes128-md5, g2-esp-aes128-sha1, g2-esp-3des-md5, g2-esp-3des-sha1, g2-esp-aes192-md5, g2-esp-aes192-sha1, g2-esp-aes256-md5, g2-esp-aes256-sha1, g2-esp-scb2-sha1, g2-esp-scb2-md5。 • g2-ah-md5-esp-3des, g2-ah-sha1-esp-3des, g2-ah-md5-esp-aes128, g2-ah-sha1-esp-aes128, g2-ah-sha1-esp-scb2, g2-ah-md5-esp-scb2。 • 四个自定义提议集必须类型相同，如果第一个自定义提议集以 g2 开头，则其他三个也必须以 g2 开头。每个提议集都提示了在阶段 2 中使用的算法： • nopfs：未启用完美向前保护 （PFS）。 • g1/g2/g5：使用 DH 组 （一种非对称加密算法）用于密钥交换，对应的密钥长度分别是 768、 1024 和 1536 比特。 • ah/esp：使用的封装协议。 • aes/3des/scb2：使用的对称加密算法。 • sha1/md5：使用的散列函数。

表 238 自动密钥隧道参数 (*续*)

参数	描述
抗重放攻击	重放攻击防护，默认为启用。 通过检测每个 ISAKMP 报文是否重复来抵御发送重复报文的攻击，以保护 IKE 协商过程。
模式	指定自动密钥隧道使用的隧道模式，包括： • **隧道模式（默认）**：通常应用在两个安全网关之间的通讯。 • **传输模式**：通常应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯 。
生存时间	第二阶段协商生成的 IPSec SA 的生存时间，超过生存时间后，将会重新生成 IPSec SA。输入范围为 180-2147483647，单位为秒。
DPD	即隧道两端的 VPN 网关通过发送 Keepalive 报文来探测对端的状态。 • **周期**：发送 Keepalive 报文间隔时间，范围为 1-3600 秒。 • **失败最大次数**：DPD 的重试次数，范围为 2-32767。
本端 ID	配置在 IKE 协商过程中对本端身份进行认证的认证标识。 本端 ID 类型包括： • **IPV4_ADDR**：输入 IP 地址作为本端标识。 • **FQDN**：输入完全合格域名作为本端标识， • **USER_FQDN**：输入邮件地址作为本端标识。 • **DER_ASN1_DN**： •输入固定格式的基本信息 （例如 C=country,ST=state,L=city,O=company,OU=department,CN=user, emailAddress=mail） •或者勾选**高级**复选框，输入相关参数，其中国家代码使用 2 个字母表示，省份、城市、公司、部门和公共名长度 1-127 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & 使用证书认证时，标识类型只能选择 DER_ASN1_DN。 • **KEY_ID**：输入字符串作为本端标识，长度 1-1023 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > &
对端 ID	配置在 IKE 协商过程中对对端身份进行认证的认证标识。 输入要求和本端标识相同。
VPN 类型	指示对端类型，包括网关到网关和远程用户。
引用	指示该隧道是否被策略引用。
启用 / 禁用	用于启用或禁用自动密钥隧道。

13.3.1.3 手动密钥隧道参数

表 239 手动密钥隧道配置信息

参数	描述
名称	手动密钥隧道名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
	不能与现有的自动密钥隧道、隧道组、 GRE 隧道和 SSL VPN 隧道重名。
启用	手动隧道的状态，启用或禁用。
模式	手动密钥隧道的模式，包括隧道模式 （默认）和传输模式。
本端 / 对端 IP 地址	创建手动密钥隧道时，本端或对端 NISG-IPS 设备所使用接口的 IP 地址。
ESP：当用户使用国密办加密卡时，系统将显示 SCB2 加密算法和密钥。	
加密算法	对 IP 数据包进行加密的算法，包括 AES-128、 AES-192、 AES-256、 3DES、 SCB2 和无。数字表示密钥的长度，密钥越长，被保护的数据包越安全，但用于解析密钥的时间也越长。
加密密钥	ESP 加密的密钥。不同的加密算法对应的加密密钥长度也不同： • **AES-128**：密钥为 32 位十六进制数 • **AES-192**：密钥为 48 位十六进制数 • **AES-256**：密钥为 64 位十六进制数 • **3DES**：密钥为 48 位十六进制数 • **SCB2**：密钥为 32 位十六进制数
认证算法	对 IP 数据包进行认证的算法，包括 HMAC-MD5 和 HMAC-SHA1。
认证密钥	ESP 认证的密钥。不同的认证算法对应的认证密钥长度也不同： • **HMAC-MD5**：密钥为 32 位十六进制数 • **HMAC-SHA1**：密钥为 40 位十六进制数
本端 / 对端 SPI	用于标识所建立的 SA 的本端 / 对端 SPI，必填项，为 8 位十六进制数，范围为 00000100-2FFFFFFF。本端和对端的 SPI 不能相同。
AH	
认证算法	对 IP 数据包进行认证的算法，包括 HMAC-MD5 和 HMAC-SHA1。
认证密钥	AH 认证的密钥。不同的认证算法对应的认证密钥长度也不同： • **HMAC-MD5**：密钥为 32 位十六进制数 • **HMAC-SHA1**：密钥为 40 位十六进制数
本端 / 对端 SPI	用于标识所建立的 SA 的本端 / 对端 SPI，必填项，为 8 位十六进制数，范围为 00000100-2FFFFFFF。本端和对端的 SPI 不能相同。

13.3.1.4 隧道组参数

表 240 隧道组参数

参数	说明
组名称	隧道组名称，长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。 不能与自动密钥隧道、手动密钥隧道、 GRE 隧道以及 SSL VPN 隧道重名。
隧道名称	隧道组中包含的网关到网关自动密钥隧道隧道，最多可包含 16 条。 一条隧道只能从属于一个隧道组。一旦这条隧道被划分到一个隧道组中，则该隧道不允许被独立引用。
优先级	隧道组中包含的隧道的优先级。为 0-255 之间的整数，数值越大，优先级越高。
隧道状态	隧道组包含的隧道的状态，包括 usable 和 unusable。
引用	当前的隧道组是否用作 VPN 隧道被路由或访问策略引用。
启用	启用或禁用隧道组。

13.3.1.5 常规设置

NISG-IPS 支持国密办硬件加密卡，通过国密办自主研发的 SCB2 加密算法对 IPSec VPN 隧道进行加密。加密卡（有时也叫加速卡）既可加强安全性，又能够提升性能。用户可以在当前页面或选择**监控 > IPSec VPN 隧道 > 加速卡统计**，查看加密卡的状态。

表 241 常规设置参数

参数	说明
名称	加密卡名称，如 SCB2。
启用	加密卡的状态：启用或禁用。用户插入加密卡后，其状态即为启用状态，用户不可手动禁用加密卡。

13.3.2 GRE 隧道参数

表 242 GRE 隧道参数

参数	说明
名称	GRE 隧道名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # GRE 隧道不能与现有的 IPSec VPN 隧道、隧道组和 SSL VPN 隧道重名。
启用	启用或禁用 GRE 隧道。
本端 / 对端 IP 地址	创建 GRE 隧道时，本端或对端 NISG-IPS 设备所使用出口接口的 IP 地址。
密钥	GRE 隧道的标识，取值范围为 0-4294967295。

13.3.3 SSL VPN 相关参数

在 SSL VPN 的配置过程中，会涉及到如下参数的配置：

- 13.3.3.1 SSL VPN 用户组参数

SSL VPN Web 入口页面参数包括：

- 13.3.3.2 SSL VPN Web 入口页面的应用参数
- 13.3.3.3 SSL VPN Web 入口页面的页面模板参数
- 13.3.3.4 SSL VPN Web 入口页面的页面服务参数

SSL VPN 隧道配置包括：

- 13.3.3.5 SSL VPN 隧道参数

13.3.3.1 SSL VPN 用户组参数

SSL VPN 用户必须被用户组包含才能使用 SSL VPN 服务。

表 243 SSL VPN 用户组参数

参数	说明
名称	SSL VPN 用户组名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
包含的用户	用户组包含的 SSL VPN 用户，一个 SSL VPN 用户只能被一个 SSL VPN 用户组包含。
被服务引用	引用 SSL VPN 用户组的 SSL VPN 服务。
引用隧道	引用 SSL VPN 用户组的 SSL VPN 隧道。
包含外部用户	用户组是否包含外部 SSL VPN 用户。 外部用户包括在 NISG-IPS 上创建，而密码保存在外部服务器上的用户，以及在外部服务器上创建，用户名和密码都保存在外部服务器上的用户。

13.3.3.2 SSL VPN Web 入口页面的应用参数

表 244 应用参数

参数	说明
名称	SSL VPN 应用名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
类型	SSL VPN 应用的类型，包括 HTTP 和 HTTPS。
URL	SSL VPN 应用的地址。

13.3.3.3 SSL VPN Web 入口页面的页面模板参数

表 245 页面模板参数

参数	说明
名称	SSL VPN 页面模板名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
入口页面设置	• **标题：**显示在入口页面左上方的文字，长度 1-90 字节， UTF-8 字符。可以为空。 • **主题色：**入口页面显示的主题颜色。可以点击色块后进行选择，也可以在文本框中直接输入颜色编码。颜色编码的取值范围为 #000000-#FFFFFF。 • **Logo：**显示在入口页面左上角和登录页面登录框上方的图片。 **语言：**入口页面的显示语言，包括英文和简体中文。
应用设置	• **类型：**入口页面所允许设置的应用类型，包括 HTTP 和 HTTPS。 • **应用：**要添加至入口页面中的应用名称。 • **URL：**应用的 URL 地址。 • **分割线：**用于在入口页面上分开两种应用。 一个 SSL VPN 页面模板中最多可以添加 32 个应用或分割线。
允许自定义应用	设置用户是否可以在入口页面自定义应用。

13.3.3.4 SSL VPN Web 入口页面的页面服务参数

表 246 页面服务参数

参数	说明
名称	SSL VPN 服务名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
启用	启用或禁用 SSL VPN 服务。
服务绑定	定义了 SSL VPN 对外提供服务的接口、 IP 地址和端口号，一个 SSL VPN 服务可以在 NISG-IPS 的多个 IP 地址和接口上提供服务。 • **接口：**提供 SSL VPN 服务的三层接口， Loopback 接口、隧道接口和虚拟接口除外。 • **IP 地址：**所选的三层接口的 IP 地址， Any 表示该接口上的所有 IP 地址。 • **端口：**提供 SSL VPN 服务的端口。

表 246 页面服务参数 (*续*)

参数	说明
服务配置	• **用户组列表：**列表中的用户组成员可以登录 SSL VPN 服务。 • **入口页面：**用户登录 SSL VPN 服务后能够看到的页面。 • **会话超时：**用户登录 SSL VPN 服务后不进行任何操作后自动登出时的时间，范围为 0-60000 秒。 0 表示永不超时，但用户关闭浏览器后会自动登出。 • **登录失败上限：**最大登录失败次数。上限为 0-10 的整数， 0 表示没有登录失败上限。达到失败次数上限后，该登录 IP 地址会被系统锁定。具体的锁定时间为第一次 5 分钟，第二次 1 小时，第三次 24 小时。 • **登录时需要验证码：**用户登录 SSL VPN 服务时需要在入口页面输入验证码。 • **验证用户证书：**勾选该选项表示启用客户端和服务器端的双向认证，否则只进行客户端对服务器的单向认证。当服务启用后，该选项不能修改。 • **保存用户配置：**将用户自定义应用保存在系统上。但当 SSL VPN 服务所选择的页面模板不允许用户自定义应用时，此选项失去作用。 • **允许用户修改密码：**允许用户修改 SSL VPN 入口页面的密码，新密码将在用户下次登录通过验证时生效。如果 SSL VPN 用户同时也是 WebAuth 或 IPSec VPN 用户，则 WebAuth 和 IPSec VPN 密码也会同时变化。
SSL 配置	• **SSL 证书：**SSL VPN 服务端的证书，只能选择本地证书类型，不能为空。 • **支持的 SSL 版本：**包括 SSL v2.0、 SSL v3.0 和 TLS v1.0。当三个选项全不勾选时，系统无法建立 SSL VPN 连接。 • **算法等级：**SSL 加密算法强度，包括高、中、低。级别越高，其安全性越高。
客户端安全要求	定义登录到 SSL VPN 服务的用户使用的操作系统以及浏览器必须满足的安全性要求。 • **开启客户端安全要求：**要求客户端浏览器安装安全性插件，并选择安全强度。包括高、中、低和自定义。 • **浏览器版本：**客户端需使用要求的浏览器类型和版本。只有 IE7+/Firefox10+/ Chrome22+ 版本的浏览器能够显示 Web 入口页面的内容。 • **操作系统版本：**客户端需使用要求的系统版本。系统版本必须是 Windows XP/Linux 3.0+。 • **安装防病毒软件：**要求客户端操作系统中安装防病毒软件。 • **开启 Windows 防火墙：**要求客户端操作系统中开启 Windows 防火墙。 • **退出时清除浏览器缓存：**用户登出系统时清除浏览器缓存。只有访问当前服务产生的缓存文件会被清除。 • **退出时清除浏览器 Cookie：**用户登出系统时清除浏览器 cookie。只有访问当前服务产生的 cookie 会被清除。 • **退出时清除浏览器历史记录：**用户登出系统时清除浏览器访问历史记录。只有访问当前服务产生的历史记录会被清除。 • **退出时清除浏览器自动表单记录：**用户登出系统时清除自动表单记录。只有访问当前服务产生的自动表单记录会被清除。 • **退出时清除操作系统临时文件：**用户登出系统时清除系统临时文件。只有访问当前服务产生的系统临时文件会被清除。
被允许的访问	可以访问 SSL VPN 服务的地址列表，由 IP 地址段或单个 IP 地址组成。 起始 IP 地址 （必填）、终止 IP 地址和安全域共同组成一个允许访问条目。安全域 “Any” 表示允许来自任意安全域的访问。 访问允许列表最多可以包含 32 个条目。
用户组访问授权	• **用户组：**授权允许或拒绝访问特定应用的 SSL VPN 用户组。 • **应用：**SSL VPN 服务所使用的页面模板中包含的应用。 • **动作：**表示允许或拒绝用户组访问应用。 • **用户默认权限：**当用户组和应用的组合不在**用户组访问授权列表**中时，按照默认动作（允许和拒绝）进行处理。 访问授权列表最多可以包含 65535 个条目。

13.3.3.5 SSL VPN 隧道参数

表 247 SSL VPN 隧道参数

参数	描述
名称	SSL VPN 隧道名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # SSL VPN 隧道名称不能与已经存在的 IPSec VPN 隧道和 GRE 隧道名称相同。
用户组	允许通过此 SSL VPN 隧道访问授权子网的用户组。
出口接口	SSL VPN 隧道的接口，通过该接口，用户组能够访问授权的子网。
本地 IP 地址	出口接口的 IP 地址。当指定为 Any 时，表示包含该接口上的所有 IP 地址。
授权子网	用户可以通过此 SSL VPN 隧道进行访问的网络。
启用	启用或禁用 SSL VPN 隧道。

13.3.4 IP 地址池相关参数

IP 地址池被用来为 IPSec VPN 用户和 SSL VPN 用户分配 IP 地址。

表 248 IP 地址池参数

名称	说明
名称	IP 地址池的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
IP 地址范围	IP 地址范围，也可以是单个 IP 地址。
引用	表示 IP 地址池是否被 IPSec VPN 或 SSL VPN 用户所引用。

13.4 VPN 范例

本节分步骤详细介绍了 VPN 范例的配置：

IPSec VPN

- 13.4.1 范例：网段到网段的手动密钥隧道
- 13.4.2 范例：基于路由的网段到网段自动密钥隧道 (单 SA)
- 13.4.3 范例：基于策略的网段到网段自动密钥隧道 （多 SA）
- 13.4.4 范例：网段到网段自动密钥隧道 （PPPoE 拨号接入）
- 13.4.5 范例：远程访问 IPSec VPN
- 13.4.6 范例：NAT 穿越
- 13.4.7 范例：IPSec VPN 隧道组

GRE VPN

- 13.4.8 范例：GRE 隧道

SSL VPN

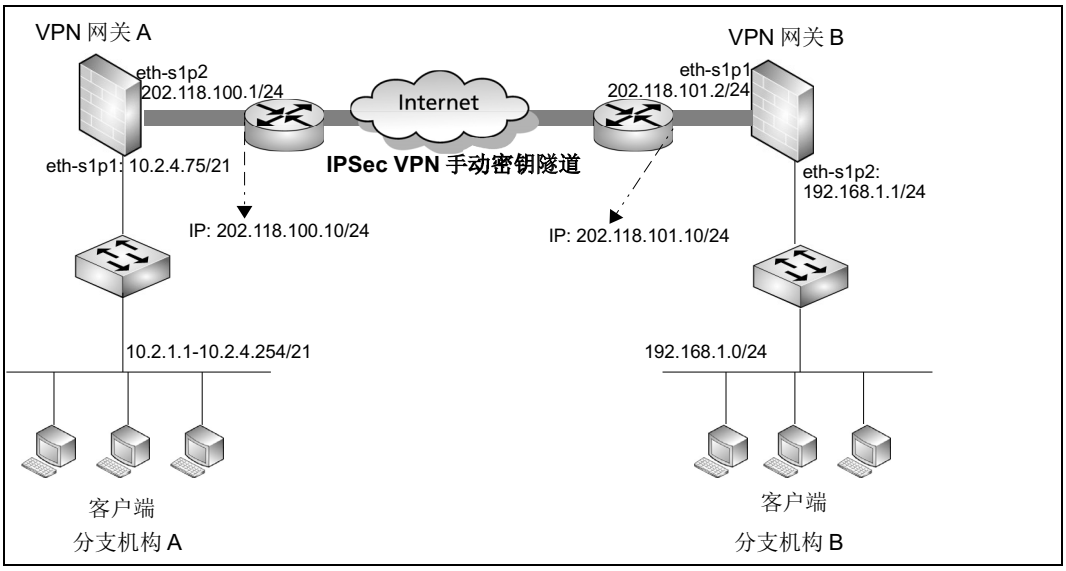
- 13.4.9 范例：SSL VPN 入口页面
- 13.4.10 范例：SSL VPN 隧道
- 13.4.11 范例：HA 自动同步 （SSL VPN 隧道)

13.4.1 范例：网段到网段的手动密钥隧道

基本需求

某公司的两个分支机构之间要通过 Internet 进行安全通信，在它们的出口处各部署一个 VPN 网关设备。这两个分支机构规模较小，网络拓扑比较稳定，未来很长一段时间内没有 VPN 扩展的需求。为了快速便捷地配置 VPN，管理员可在 VPN 网关 A 和网关 B 之间建立一条手动密钥隧道，对两个分支机构间的通信数据进行加密，以保障通信安全。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置访问策略
- 创建手动密钥隧道
- 配置路由

配置步骤

配置接口 IP 地址

VPN 网关 A：

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p1：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=10.2.4.75/21。
   - eth-s1p2：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=202.118.100.1/24。
2. 点击**确定**。

VPN 网关 B:

用同样的方法为 VPN 网关 B 配置 IP 地址。

- eth-s1p1：开，三层， MTU=1500，静态 IP， IP 地址列表主 IP=202.118.101.2/24。
- eth-s1p2：开，三层， MTU=1500, 静态 IP， IP 地址列表主 IP=192.168.1.1/24。

CLI

VPN 网关 A:

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 10.2.4.75 255.255.248.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.100.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
```

VPN 网关 B:

除了 IP 地址，其他的命令与 VPN 网关 A 一致。

```
NetEye@root-system-if-eth-s1p1] ip address 202.118.101.2 255.255.255.0
NetEye@root-system-if-eth-s1p2] ip address 192.168.1.1 255.255.255.0
```

配置访问策略

VPN 网关 A:

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建两条访问策略，允许本端和对端子网之间的互相访问。
   - 序号 =1，名称 =atob，源安全域 = 任意，源 IP=10.2.1.1-10.2.4.254，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许；
   - 序号 =2，名称 =btoa1，源安全域 = 任意，源 IP=192.168.1.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.2.1.1-10.2.4.254，服务 = 任意，动作 = 允许。
3. 点击**确定**。

VPN 网关 B:

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建两条访问策略。
   - 序号 =1，名称 =btoa，源安全域 = 任意，源 IP=192.168.1.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.2.1.1-10.2.4.254，服务 = 任意，动作 = 允许；
   - 序号 =2，名称 =atob1，源安全域 = 任意，源 IP=10.2.1.1-10.2.4.254，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许。
3. 点击**确定**。

CLI

VPN 网关 A:

```
NetEye@root-system] policy access atob any 10.2.1.1-10.2.4.254 any
192.168.1.0/24 any any permit enable
NetEye@root-system] policy access btoa1 any 192.168.1.0/24 any
10.2.1.1-10.2.4.254 any any permit enable
```

VPN 网关 B:

```
NetEye@root-system] policy access btoa any 192.168.1.0/24 any
10.2.1.1-10.2.4.254 any any permit enable
NetEye@root-system] policy access atob1 any 10.2.1.1-10.2.4.254 any
192.168.1.0/24 any any permit enable
```

创建手动密钥隧道

VPN 网关 A：

1. 选择 **VPN** > **IPSec VPN** > **手动密钥隧道**。
2. 点击**新建**，进行如下配置：
   - 名称 =atob，本端 IP 地址 =202.118.100.1，对端 IP 地址 =202.118.101.2
   - ESP= 勾选
     - 加密算法 =AES-128
     - 加密密钥 =6c6a79b4357c6c6a6c6a79b4357c6c6a
     - 认证算法 =HMAC-MD5
     - 认证密钥 =7c6a79b4357c6c6a6c6a79b4357c6c6a
     - 本端 SPI=10011001
     - 对端 SPI=1eeeffff

提示：ESP 和 AH 必须至少配置一项；本端和对端的加密算法和认证算法必须相同，本端和对端的 SPI 值正好相反。

---

3. 点击**确定**。

VPN 网关 B:

1. 选择 **VPN** > **IPSec VPN > 手动密钥隧道**。
2. 点击**新建**，进行如下配置：
   - 名称 =btoa，本端 IP 地址 =202.118.101.2，对端 IP 地址 =202.118.100.1
   - ESP= 勾选
     - 加密算法 =AES-128
     - 加密密钥 =6c6a79b4357c6c6a6c6a79b4357c6c6a
     - 认证算法 =HMAC-MD5
     - 认证密钥 =7c6a79b4357c6c6a6c6a79b4357c6c6a
     - 本端 SPI=1eeeffff
     - 对端 SPI=10011001
3. 点击**确定**。

提示：在成功创建手动密钥隧道的同时，两个网关上将各自生成一个隧道接口 tunnelatob 和 tunnelbtoa。选择**网络 > 接口**可以查看隧道接口。

CLI

VPN 网关 A：

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel atob manual gateway remote-ip
202.118.101.2 local-ip 202.118.100.1 esp 10011001 1eeeffff auth
hmac-md5 key 7c6a79b4357c6c6a6c6a79b4357c6c6a encrypt aes128 key
6c6a79b4357c6c6a6c6a79b4357c6c6a mode tunnel enable
NetEye@root-system-vpn] exit
```

VPN 网关 B：

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel btoa manual gateway remote-ip
202.118.100.1 local-ip 202.118.101.2 esp 1eeeffff 10011001 auth
hmac-md5 key 7c6a79b4357c6c6a6c6a79b4357c6c6a encrypt aes128 key
6c6a79b4357c6c6a6c6a79b4357c6c6a mode tunnel enable
NetEye@root-system-vpn] exit
```

配置路由

管理员需要进行如下配置：

- 创建路由允许访问任意网络；
- 通过路由对 VPN 隧道进行引流。

VPN 网关 A：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，创建两条路由。

- 目的 IPv4 地址 =0.0.0.0，掩码长度 =0，Metric=1，出口接口 =eth-s1p2，网关 =202.118.100.10；
- 目的 IPv4 地址 =192.168.1.0，掩码长度 =24，Metric=1，出口接口 =tunnelatob。

3. 点击**确定**。
4. 点击 。

VPN 网关 B：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，创建两条路由。
   - 目的 IPv4 地址 =0.0.0.0，掩码长度 =0，Metric=1，出口接口 =eth-s1p1，网关 =202.118.101.10；
   - 目的 IPv4 地址 =10.2.0.0，掩码长度 =21，Metric=1，出口接口 =tunnelbtoa。
3. 点击**确定**。
4. 点击 。

CLI

VPN 网关 A：

```
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.100.10
NISG-IPS@root-system] route 192.168.1.0 255.255.255.0 interface
tunnelatob
NetEye@root-system] end
NetEye@root> save config
```

VPN 网关 A：

```
NetEye@root-system] route default interface eth-s1p1 gateway
202.118.101.10
NISG-IPS@root-system] route 10.2.0.0 255.255.248.0 interface
tunnelbtoa
NetEye@root-system] end
NetEye@root> save config
```

验证结果

VPN 网关 A/B:

选择**监控** > **IPSec VPN 隧道 > 手动密钥隧道**，进入手动密钥隧道监控页面，查看 VPN 隧道的监控信息。

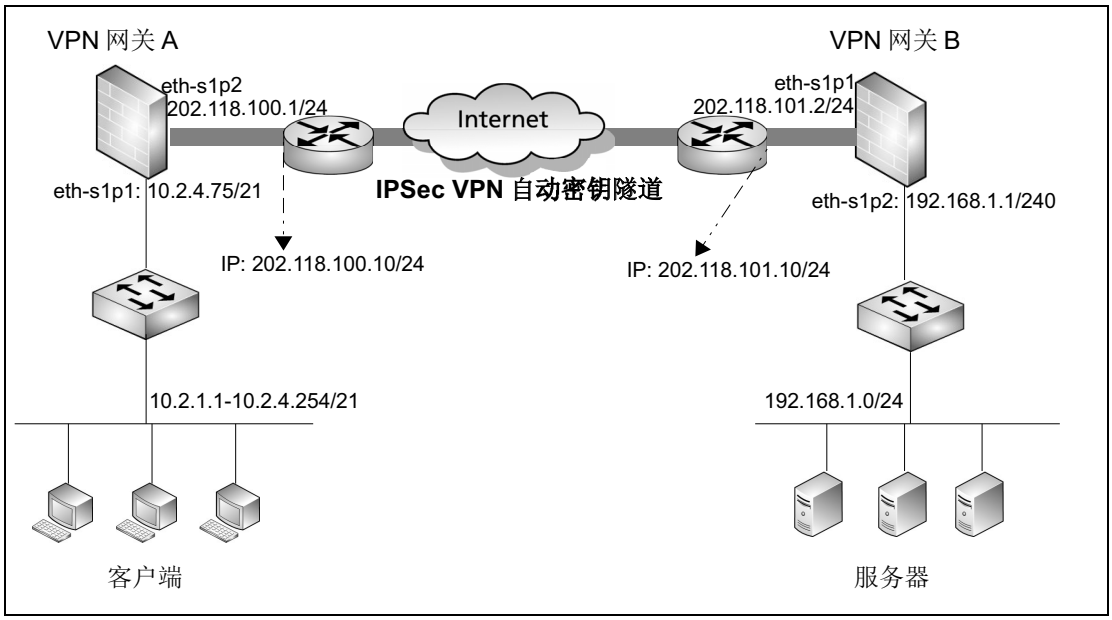
13.4.2 范例：基于路由的网段到网段自动密钥隧道 (单 SA)

基本需求

在 VPN 网关 A 和 B 之间建立一条使用证书认证方式的自动密钥隧道，当位于 VPN 网关 A 内部的客户端主机发起对 VPN 网关 B 内部的服务器的访问时， NISG-IPS 通过路由将数据流引入 VPN 隧道，从而保证了通信安全。自动密钥隧道具有如下特点：

- 具有 VPN 扩展性，易维护易管理；
- 需要对端身份认证 （证书或与共享密钥），提高安全性；
- 通过自动密钥生成隧道，相对手动密钥隧道配置过程较为复杂，但比其安全，实际应用也更广泛。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置访问策略
- 导入证书
- 创建自动密钥隧道
- 配置路由

配置步骤

配置接口 IP 地址

VPN 网关 A：

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p1：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=10.2.4.75/21。
   - eth-s1p2：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=202.118.100.1/24。
2. 点击**确定**。

VPN 网关 B：

用同样的方法为 VPN 网关 B 配置 IP 地址。

- eth-s1p1：开，三层， MTU=1500，静态 IP， IP 地址列表主 IP=202.118.101.2/24。
- eth-s1p2：开，三层， MTU=1500, 静态 IP， IP 地址列表主 IP=192.168.1.1/24。

CLI

VPN 网关 A:

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 10.2.4.75 255.255.248.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.100.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
```

VPN 网关 B:

除了 IP 地址，其他的命令与 VPN 网关 A 一致。

```
NetEye@root-system-if-eth-s1p1] ip address 202.118.101.2 255.255.255.0
NetEye@root-system-if-eth-s1p2] ip address 192.168.1.1 255.255.255.0
```

配置访问策略

VPN 网关 A:

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建一条名称为 atob 的访问策略，允许本端客户端主机访问对端服务器。

   名称 =atob，源安全域 = 任意，源 IP=10.2.1.1-10.2.4.254，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许。
3. 点击**确定**。

VPN 网关 B:

以同样方式创建一条名称为 atob1 的访问策略，允许对端客户端主机访问本端服务器。

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建一条访问策略。

   名称 =atob1，源安全域 = 任意，源 IP=10.2.1.1-10.2.4.254，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许。
3. 点击**确定**。

CLI

VPN 网关 A:

```
NetEye@root-system] policy access atob any 10.2.1.1-10.2.4.254 any
192.168.1.0/24 any any permit enable
```

VPN 网关 B:

```
NetEye@root-system] policy access atob1 any 10.2.1.1-10.2.4.254 any
192.168.1.0/24 any any permit enable
```

导入证书

两个 VPN 网关设备需要导入各自的本地证书和彼此的 CA 证书 （可以相同）。

- 如果无可用的 CA 和本地证书，可以向证书颁发机构 （CA）申请证书。更多信息，参见 3.30.2 范例：使用本地 CA 中心颁发证书 和 3.30.3 范例：通过第三方 CA 中心自动注册证书 。
- 如果已存在可用的 CA 和本地证书，请按照以下步骤导入证书。

VPN 网关 A:

1. 选择**系统** > **证书** > **CA 证书**。
2. 点击**导入**，从本地路径导入名称为 ca 的 CA 证书。
3. 点击**确定**。
4. 选择**系统** > **证书** > **本地证书**。
5. 点击**导入**，从本地路径导入名称为 local1 的本地证书。
6. 点击**确定**。

VPN 网关 B:

以同样的方法为 VPN 网关 B 导入 CA 证书 （名称为 ca）和本地证书 （名称为 local2）。

CLI

管理员可以使用 SecureCRT 等 SSH 连接工具通过 X/Zmodem 方式上传证书。

VPN 网关 A:

```
NetEye@root-system] import certificate ca from x/zmodem ca
NetEye@root-system] import certificate local from x/zmodem local1
```

VPN 网关 B:

```
NetEye@root-system] import certificate ca from x/zmodem ca
```

```
NetEye@root-system] import certificate local from x/zmodem local2
```

创建自动密钥隧道

VPN 网关 A：

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条自动密钥隧道，使用证书认证。
   - 名称 =atob ；
   - 对端：类型 = 静态 IP 地址， IP 地址 / 域名 =202.118.101.2 ；
   - 出口：出口 =eth-s1p2，本端 IP 地址 =202.118.100.1 ；
   - 认证：认证方式 = 证书，本地证书 =local1，对端 CA 证书 =ca。
3. 点击**高级设置**，设置本端和对端 ID， ID 值为本端和对端本地证书的主题信息。
   - 本端 ID：

     ID 类型 =DER_ANS1_DN,
     ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com。
   - 对端 ID：

     ID 类型 =DER_ANS1_DN,
     ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com。
4. 点击**确定**。

VPN 网关 B：

对 VPN 网关 B 进行同样的配置，除下列内容外：

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条自动密钥隧道，使用证书认证。
   - 名称 =btoa ；
   - 对端：类型 = 静态 IP 地址， IP 地址 / 域名 ==202.118.100.1 ；
   - 出口：出口 =eth-s1p1，本端 IP 地址 =202.118.101.2 ；
   - 认证：认证方式 = 证书，本地证书 =local2，对端 CA 证书 =ca。
3. 点击**高级设置**，配置 VPN 网关 B 的本端和对端 ID 如下：
   - 本端 ID：

     ID 类型 =DER_ANS1_DN,
     ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com。
   - 对端 ID：

     ID 类型 =DER_ANS1_DN,
     ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com。
4. 点击**确定**。

CLI

VPN 网关 A：

```
NetEye@root-system-vpn] tunnel atob gateway 202.118.101.2 interface
eth-s1p2 202.118.100.1 certificate local1 ca enable
NetEye@root-system-vpn] tunnel atob ike local-id asn1-dn
C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
NetEye@root-system-vpn] tunnel atob ike peer-id asn1-dn
C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
NetEye@root-system-vpn] exit
```

VPN 网关 B：

```
NetEye@root-system-vpn] tunnel btoa gateway 202.118.100.1 interface
eth-s1p1 202.118.101.2 certificate local2 ca enable
NetEye@root-system-vpn] tunnel btoa ike local-id asn1-dn
C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
NetEye@root-system-vpn] tunnel btoa ike peer-id asn1-dn
C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
NetEye@root-system-vpn] exit
```

配置路由

管理员需要进行如下配置：

- 创建路由允许访问任意网络；
- 通过路由对 VPN 隧道进行引流。

VPN 网关 A：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，进行如下配置：
   - 目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =eth-s1p2，网关 =202.118.100.10 ；
   - 目的 IPv4 地址 =192.168.1.0，掩码长度 =24， Metric=1，出口接口 =tunnelatob。

   提示：创建隧道时将自动生成一个隧道接口 tunnelatob。
3. 点击**确定**。
4. 点击 。

VPN 网关 B：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，创建路由。
   - 目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =eth-s1p1，网关 =202.118.101.10 ；
   - 目的 IPv4 地址 =10.2.0.0，掩码长度 =21， Metric=1，出口接口 =tunnelbtoa。
3. 点击**确定**。
4. 点击 。

CLI

VPN 网关 A：

```
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.100.10
NISG-IPS@root-system] route 192.168.1.0 255.255.255.0 interface
tunnelatob
NetEye@root-system] end
NetEye@root> save config
```

VPN 网关 B：

```
NetEye@root-system] route default interface eth-s1p1 gateway
202.118.101.10
NISG-IPS@root-system] route 10.2.0.0 255.255.248.0 interface
tunnelbtoa
NetEye@root-system] end
NetEye@root> save config
```

验证结果

当网关 A 后端子网中的客户端向网关 B 后端的服务器发访问请求时，一条自动密钥隧道将通过协商成功建立。

VPN 网关 A 和 B：

1. 选择**监控** > **IPSec VPN 隧道** > **自动密钥隧道**。
2. 查看已建立的隧道信息，点击  ，查看隧道详细配置。

13.4.3 范例：基于策略的网段到网段自动密钥隧道 （多 SA）

基本需求

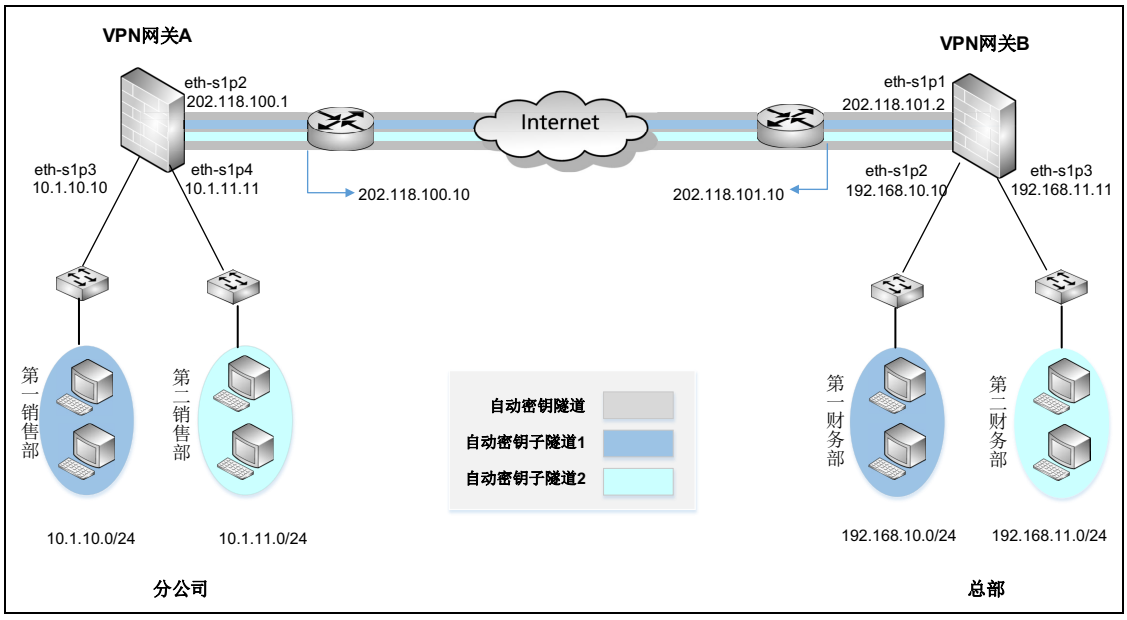
多 SA 功能与多子网关联。通过创建一条支持多 SA 的自动密钥隧道，可以对本端特定子网到对端相应子网之间的数据流进行精准的安全控制。多 SA 功能一般适用于两端 VPN 网关后端有多个子网的情形。

本范例中，在 VPN 网关 A 和 B 之间建立一条多 SA 自动密钥隧道，将各子网与该隧道绑定，使用访问策略对隧道进行引流。

- 当分公司的第一销售部与总部第一财务部需要互相通讯时，将它们所在的子网关联到该隧道，自动生成一个子隧道 1。当第一销售部发起访问时，数据包流量将通过该密钥隧道的子隧道 1 转发出去。
- 同理，将第二销售部与第二财务部所在的子网与该隧道关联，自动生成子隧道 2。当第二销售部发起访问时，数据包流量将通过该隧道的子隧道 2 转发出去。
- 第一销售部与第二财务部之间，第二销售部与第一财务部之间禁止互相通讯。

提示：用户在**监控**页面将只能查看到一条自动密钥隧道，子隧道信息不显示。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置路由
- 创建自动密钥隧道
- 配置访问策略

配置步骤

配置接口 IP 地址

VPN 网关 A:

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p2：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=202.118.100.1/24。
   - eth-s1p3：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=10.1.10.10/24。
   - eth-s1p4：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=10.1.11.11/24。
2. 点击**确定**。

VPN 网关 B:

用同样的方法为 VPN 网关 B 配置 IP 地址。

- eth-s1p1：开，三层， MTU=1500，静态 IP， IP 地址列表主 IP=202.118.101.2/24。
- eth-s1p2：开，三层， MTU=1500，静态 IP，IP 地址列表主 IP=192.168.10.10/24。
- eth-s1p3：开，三层， MTU=1500，静态 IP， IP 地址列表主 IP=192.168.11.11/24。

CLI

VPN 网关 A:

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.100.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 10.1.10.10 255.255.255.0
NetEye@root-system-if-eth-s1p3] exit
NetEye@root-system] interface ethernet s1p4
NetEye@root-system-if-eth-s1p4] working-type layer3-interface
NetEye@root-system-if-eth-s1p4] ip address 10.1.11.11 255.255.255.0
NetEye@root-system-if-eth-s1p4] exit
```

VPN 网关 B:

除了 IP 地址，其他的命令与 VPN 网关 A 一致。

```
NetEye@root-system-if-eth-s1p1] ip address 202.118.101.2 255.255.255.0
NetEye@root-system-if-eth-s1p2] ip address 192.168.10.10 255.255.255.0
NetEye@root-system-if-eth-s1p3] ip address 192.168.11.11 255.255.255.0
```

配置路由

VPN 网关 A：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，添加一条路由。管理员也可以修改系统已存在的缺省路由 （出口接口和网关）。

   目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =eth-s1p2，网关 =202.118.100.10
3. 点击**确定**。

VPN 网关 B：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，添加一条路由。管理员也可以修改系统已存在的缺省路由 （出口接口和网关）。

   目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =eth-s1p1，网关 =202.118.101.10。
3. 点击**确定**。

CLI

VPN 网关 A:

```
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.100.10
NetEye@root-system] exit
```

VPN 网关 B:

```
NetEye@root-system] route default interface eth-s1p1 gateway
202.118.101.10
NetEye@root-system] exit
```

创建自动密钥隧道

VPN 网关 A：

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条新的隧道，使用预共享密钥认证。
   - 名称 =atob ；
   - 对端：类型 = 静态 IP 地址， IP 地址 / 域名 =202.118.101.2 ；
   - 出口：出口 =eth-s1p2，本端 IP 地址 =202.118.100.1 ；
   - 认证：认证方式 = 预共享密钥，密钥 =123456。
3. 设置本端和对端子网。
   - 本端子网 =10.1.10.0/24，对端子网 =192.168.10.0/24 ；
   - 本端子网 =10.1.11.0/24，对端子网 =192.168.11.0/24。
4. 点击**确定**。

VPN 网关 B：

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道。**
2. 点击**新建**，创建一条新的隧道，使用预共享密钥认证。
   - 名称 =btoa ；
   - 对端：类型 = 静态 IP 地址， IP 地址 / 域名 =202.118.100.1 ；
   - 出口：出口 =eth-s1p1，本端 IP 地址 =202.118.101.2 ；
   - 认证：认证方式 = 预共享密钥，密钥 =123456。
3. 设置本端和对端子网。
   - 本端子网 =192.168.10.0/24，对端子网 =10.1.10.0/24 ；
   - 本端子网 =192.168.11.0/24，对端子网 =10.1.11.0/24。
4. 点击**确定**。

CLI

VPN 网关 A：

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel atob gateway 202.118.101.2 interface
eth-s1p2 202.118.100.1 preshared-key 123456 enable
NetEye@root-system-vpn] tunnel atob local-subnet 10.1.10.0
255.255.255.0 remote-subnet 192.168.10.0 255.255.255.0
NetEye@root-system-vpn] tunnel atob local-subnet 10.1.11.0
255.255.255.0 remote-subnet 192.168.11.0 255.255.255.0
NetEye@root-system-vpn] exit
```

VPN 网关 B：

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel btoa gateway 202.118.100.1 interface
eth-s1p1 202.118.101.2 preshared-key 123456 enable
NetEye@root-system-vpn] tunnel btoa local-subnet 192.168.10.0
255.255.255.0 remote-subnet 10.1.10.0 255.255.255.0
NetEye@root-system-vpn] tunnel btoa local-subnet 192.168.11.0
255.255.255.0 remote-subnet 10.1.11.0 255.255.255.0
NetEye@root-system-vpn] exit
```

提示：用户也可以通过证书进行认证。更多信息，参见 导入证书 。

配置访问策略

用户需要进行如下配置：

- 创建访问策略以允许本端和对端特定子网之间的双向访问；
- 通过访问策略对 VPN 隧道进行引流。

VPN 网关 A：

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建四条访问策略。
   a. 策略atob1允许从10.1.10.0/24到192.168.10.0/24的数据流访问，策略atob2则允许从10.1.11.0/24 到 192.168.11.0/24 的数据流访问。
      - 名称 =atob1，源安全域 = 任意，源 IP=10.1.10.0/24，目的安全域 = 任意，目的 IP/域名 =192.168.10.0/24，服务 = 任意，动作 = 允许；
      - 名称 =atob2，源安全域 = 任意，源 IP=10.1.11.0/24，目的安全域 = 任意，目的 IP/域名 =192.168.11.0/24，服务 = 任意，动作 = 允许。
   b. 再配置两条策略，允许反向访问。
      - 名称 =btoa1，源安全域 = 任意，源 IP=192.168.10.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.1.10.0/24，服务 = 任意，动作 = 允许；
      - 名称 =btoa2，源安全域 = 任意，源 IP=192.168.11.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.1.11.0/24，服务 = 任意，动作 = 允许。
3. 点击atob1和atob2对应的 ，分别引用VPN隧道atob，将本端两个子网向对端相应子网发起访问的数据流指向 VPN 隧道。
4. 点击**确定**。
5. 点击 。

VPN 网关 B：

以同样方式创建四条访问策略，并通过 btoa_1 和 btoa_2 对隧道 btoa 进行引流。

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建四条访问策略。

- 名称 =btoa_1，源安全域 = 任意，源 IP=192.168.10.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.1.10.0/24，服务 = 任意，动作 = 允许；
- 名称 =btoa_2，源安全域 = 任意，源 IP=192.168.11.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.1.11.0/24，服务 = 任意，动作 = 允许；
- 名称 =atob_1，源安全域 = 任意，源 IP=10.1.10.0/24，目的安全域 = 任意，目的 IP/ 域名 =192.168.10.0/24，服务 = 任意，动作 = 允许；
- 名称 =atob_2，源安全域 = 任意，源 IP=10.1.11.0/24，目的安全域 = 任意，目的 IP/ 域名 =192.168.11.0/24，服务 = 任意，动作 = 允许。

3. 点击 btoa_1 和 btoa_2 对应的 ，分别引用 VPN 隧道 btoa，将本端两个子网向对端相应子网发起访问的数据流指向 VPN 隧道。
4. 点击**确定**。
5. 点击 。

CLI

VPN 网关 A:

```
NetEye@root-system] policy access atob1 any 10.1.10.0/24 any
192.168.10.0/24 any any permit enable
NetEye@root-system] policy access atob1 tunnel atob
NetEye@root-system] policy access atob2 any 10.1.11.0/24 any
192.168.11.0/24 any any permit enable
NetEye@root-system] policy access atob2 tunnel atob
NetEye@root-system] policy access btoa1 any 192.168.10.0/24 any
10.1.10.0/24 any any permit enable
NetEye@root-system] policy access btoa2 any 192.168.11.0/24 any
10.1.11.0/24 any any permit enable
NetEye@root-system] end
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system] policy access btoa_1 any 192.168.10.0/24 any
10.1.10.0/24 any any permit enable
NetEye@root-system] policy access btoa_1 tunnel btoa
NetEye@root-system] policy access btoa_2 any 192.168.11.0/24 any
10.1.11.0/24 any any permit enable
NetEye@root-system] policy access btoa_2 tunnel btoa
NetEye@root-system] policy access atob_1 any 10.1.10.0/24 any
192.168.10.0/24 any any permit enable
NetEye@root-system] policy access atob_2 any 10.1.11.0/24 any
192.168.11.0/24 any any permit enable
NetEye@root-system] end
NetEye@root> save config
```

验证结果

可以在两端 VPN 网关上查看 VPN 隧道，隧道已成功建立，并能够有效隔离不同子网间的访问。

- 查看隧道
- 监控访问

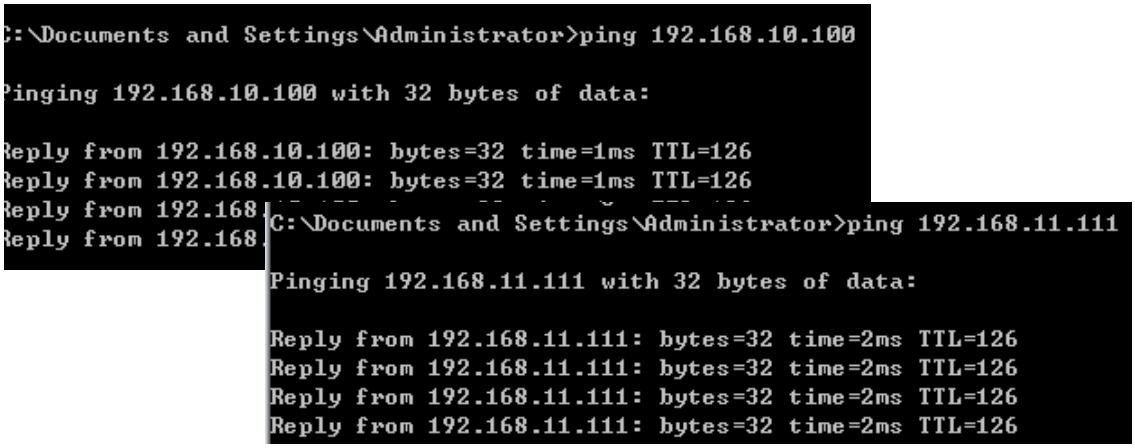
查看隧道

VPN 网关 A 和 B：

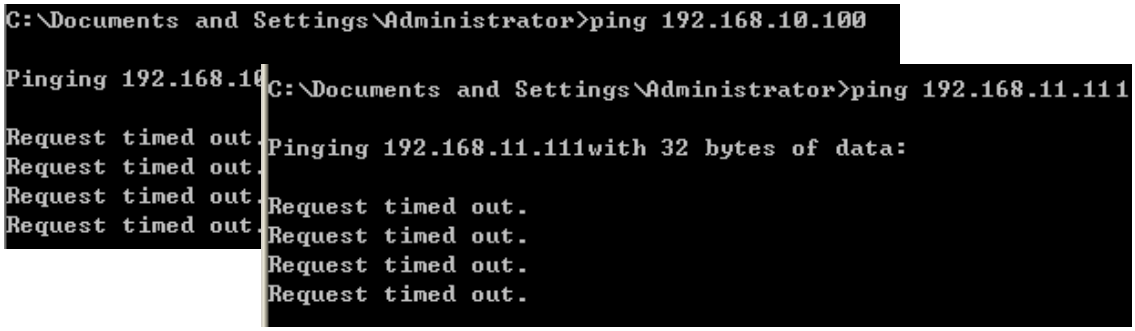
1. 选择**监控 >IPSec VPN 隧道 > 自动密钥隧道**，查看已建立的隧道。
2. 点击 ，查看隧道详细配置。

监控访问

第一销售部任意主机能够访问第一财务部，第二销售部任意主机能够访问第二财务部，结果如下：



第二销售部无法访问第一财务部，第一销售部无法访问第二财务部，结果如下：



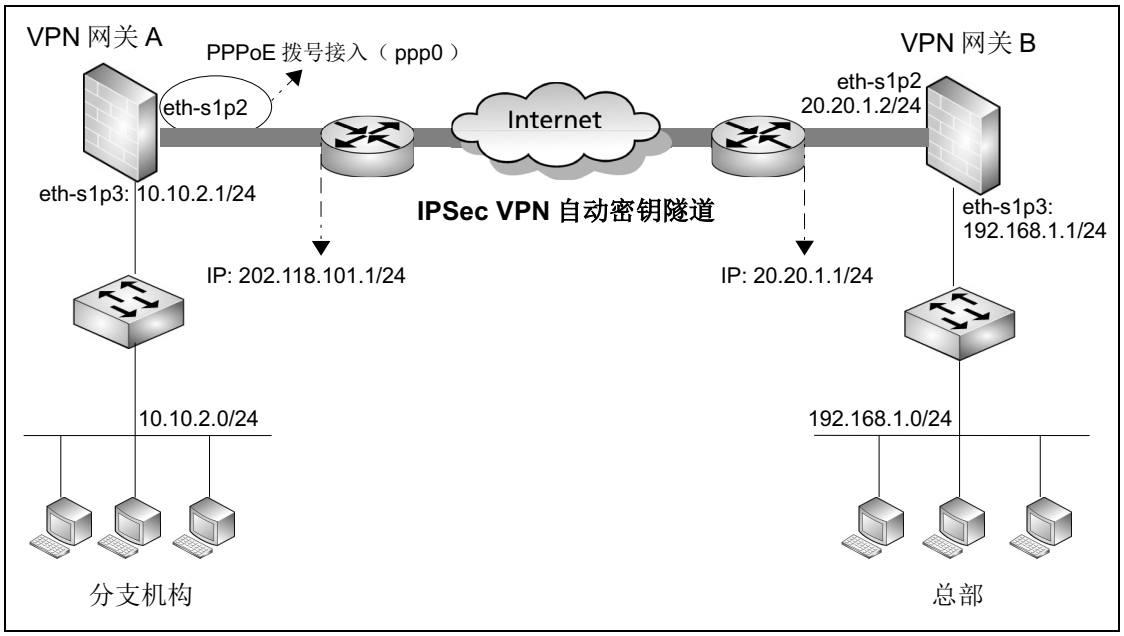
上述结果显示，多 SA 的 VPN 功能能够实现不同部门的访问控制隔离，保证各自通讯数据的安全。

13.4.4 范例：网段到网段自动密钥隧道 （PPPoE 拨号接入）

基本需求

某公司的总部与分支机构处于不同城市，分支机构通过 PPPoE 拨号方式接入 Internet。当分支机构与总部之间互相进行通讯时，需要在两端 VPN 网关上建立一条自动密钥隧道以保证双方通讯数据安全。其中，分支机构使用动态 IP 地址，总部则使用静态 IP 地址来进行隧道协商。双方都通过访问策略对隧道进行引流。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置 PPPoE 连接
- 配置路由
- 创建自动密钥隧道
- 配置访问策略

配置步骤

配置接口 IP 地址

VPN 网关 A:

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p3：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=10.10.2.1/24。
2. 点击**确定**。

VPN 网关 B:

用同样的方法为 VPN 网关 B 配置 IP 地址。

- eth-s1p2：开，三层， MTU=1500，静态 IP，IP 地址列表主 IP=20.20.1.2/24。
- eth-s1p3：开，三层， MTU=1500，静态 IP， IP 地址列表主 IP=192.168.1.1/24。

CLI

VPN 网关 A:

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] ip address 10.10.2.1 255.255.255.0
NetEye@root-system-if-eth-s1p3] exit
```

VPN 网关 B:

除了 IP 地址，其他的命令与 VPN 网关 A 一致。

```
NetEye@root-system-if-eth-s1p2] ip address 20.20.1.2 255.255.255.0
NetEye@root-system-if-eth-s1p3] ip address 192.168.1.1 255.255.255.0
```

配置 PPPoE 连接

VPN 网关 A:

1. 选择**网络** > **接口**。
2. 点击**新建**，并选择 **PPPoE**，输入数字 0，创建 PPPoE 接口 ppp0。
3. 点击**确定**。
4. 点击 PPPoE 接口对应的 ，进行如下配置。
   - 配置 PPPoE 接口时，需要首先保证接口状态为关闭。完成其他所有配置后，将接口状态置为开启，从而进行拨号连接。
   - 输入从 ISP 获取的用户名（user123）和密码（neteye），用于 PPPoE 服务器认证。
   - 将 eth-s1p2 接口划入 ppp0 接口，该 PPPoE 接口将作为 PPPoE 客户端拨号接入 Internet。
   - 其他选项使用默认设置。
5. 点击**确定**。

当路由配置完毕后，PPPoE 服务器将为 PPPoE 接口分配一个公网 IP 地址 202.118.101.2，客户端主机通过该 IP 地址即可访问 Internet。选择**网络** > **接口**，可查看该 IP 地址信息。

CLI

VPN 网关 A:

```
NetEye@root-system] pppoe 0
NetEye@root-system-pppoe0] hold ethernet eth-s1p2
NetEye@root-system-pppoe0] username user123 password neteye
NetEye@root-system-pppoe0] active on
NetEye@root-system-pppoe0] exit
```

配置路由

VPN 网关 A:

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，添加一条路由。管理员也可以修改系统已存在的缺省路由 （出口接口和网关）。

   目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =ppp0，网关 =202.118.101.1.
3. 点击**确定**。

VPN 网关 B:

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，添加一条路由。管理员也可以修改系统已存在的缺省路由 （出口接口和网关）。

   目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =eth-s1p2，网关 =20.20.1.1.
3. 点击**确定**。

CLI

VPN 网关 A:

```
NetEye@root-system] route default interface ppp0 gateway 202.118.101.1
```

VPN 网关 B:

```
NetEye@root-system] route default interface eth-s1p2 gateway 20.20.1.1
```

创建自动密钥隧道

VPN 网关 A:

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条新的隧道，使用预共享密钥认证。
   - 名称 =atob ；
   - 对端：类型 = 静态 IP 地址， IP 地址 / 域名 =20.20.1.2 ；
   - 出口：出口 =ppp0，本端 IP 地址 =Any ；

- 认证：认证方式 = 预共享密钥，密钥 =neteye。

3. 设置本端 （10.10.20.0/24）和对端 （192.168.1.0/24）子网。
4. 点击**确定**。

VPN 网关 B：

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道。**
2. 点击**新建**，创建一条新的隧道，使用预共享密钥认证。
   - 名称 =btoa ；
   - 对端：类型 = 动态 IP 地址；
   - 出口：出口 =eth-s1p2，本端 IP 地址 =20.20.1.2 ；
   - 认证：认证方式 = 预共享密钥，密钥 =neteye。
3. 设置 （192.168.1.0/24）本端和对端 （10.10.20.0/24）子网。
4. 点击**确定**。

CLI

VPN 网关 A：

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel atob gateway 20.20.1.2 interface ppp0
any preshared-key neteye local-subnet 10.10.2.0 255.255.255.0
remote-subnet 192.168.1.0 255.255.255.0 enable
NetEye@root-system-vpn] exit
```

VPN 网关 B:

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel btoa gateway any interface eth-s1p2
20.20.1.2 preshared-key neteye local-subnet 192.168.1.0
255.255.255.0 remote-subnet 10.10.2.0 255.255.255.0 enable
NetEye@root-system-vpn] exit
```

配置访问策略

VPN 网关 A:

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建两条访问策略，允许本端和对端子网之间的访问。
   - 名称 =atob，源安全域 = 任意，源 IP=10.10.2.0/24，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许；
   - 名称 =btoa1，源安全域 = 任意，源 IP=192.168.1.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.10.2.0/24，服务 = 任意，动作 = 允许。
3. 点击策略 atob 对应的 ，引用 VPN 隧道 atob，将本端流向对端子网的数据流指向 VPN 隧道。
4. 点击**确定**。

VPN 网关 B:

以同样方式创建两条访问策略，并通过策略 btoa 对隧道 btoa 进行引流。

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建两条访问策略，允许本端和对端子网之间的访问。
   - 名称 =btoa，源安全域 = 任意，源 IP=192.168.1.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.10.2.0/24，服务 = 任意，动作 = 允许；
   - 名称 =atob1，源安全域 = 任意，源 IP=10.10.2.0/24，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许。
3. 点击策略 atob 对应的 ，引用 VPN 隧道 atob，将本端流向对端子网的数据流指向 VPN 隧道。

点击**确定**。

CLI

VPN 网关 A:

```
NetEye@root-system] policy access atob any 10.10.2.0/24 any
192.168.1.0/24 any any permit enable
NetEye@root-system] policy access atob tunnel atob
NetEye@root-system] policy access btoa1 any 192.168.1.0/24 any
10.10.2.0/24 any any permit enable
```

VPN 网关 B:

```
NetEye@root-system] policy access btoa any 192.168.1.0/24 any
10.10.2.0/24 any any permit enable
NetEye@root-system] policy access btoa tunnel btoa
NetEye@root-system] policy access atob1 any 10.10.2.0/24 any
192.168.1.0/24 any any permit enable
```

验证结果

由于 VPN 网关 A 的出口地址为动态 IP，对端无法识别。因此只能是 VPN 网关 A 后端的客户端首先向对端发起访问请求，从而使网关 A 能够主动发起 VPN 隧道协商。在隧道成功建立后，网关 A 和 B 后端的客户端可以通过加密数据传输进行通讯。管理员可以查看如下隧道信息。

VPN 网关 A 和 B:

1. 选择**监控 >IPSec VPN 隧道 > 自动密钥隧道**。
2. 查看已建立的隧道。点击  ，查看隧道详细配置。

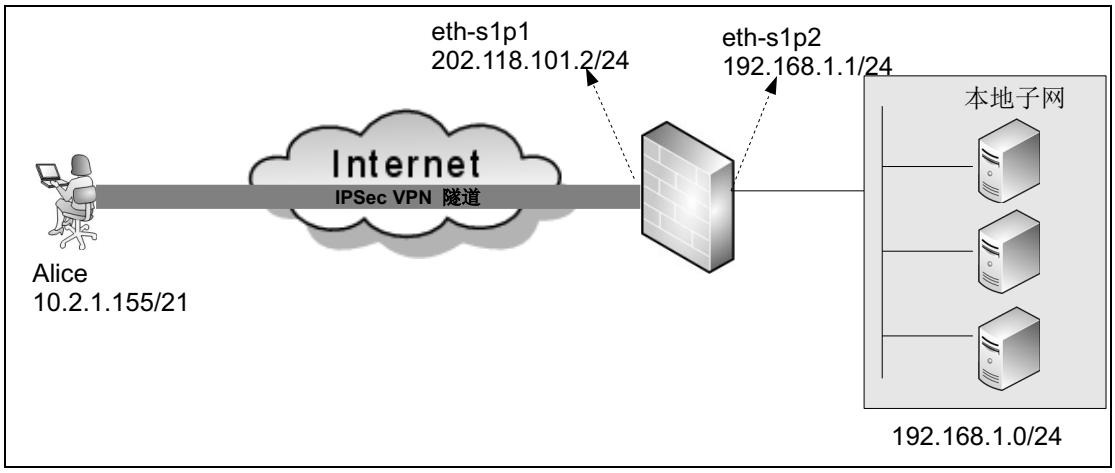
13.4.5 范例：远程访问 IPSec VPN

基本需求

远程访问 IPSec VPN 主要用于移动办公人员 （远程用户）访问企业的内网资源。在本范例中，远程用户 Alice 使用 Windows 操作系统，通过 Internet 拨号进入公司内网，访问 VPN 网关后的服务器子网 192.168.1.0/24。远程访问 IPSec VPN 具有如下特点：

- 远程访问用户无固定 IP 地址；
- 远程用户必须使用账号登录；
- 对远程用户进行认证 （预共享密钥或者证书认证）；
- 需要在客户端主机上进行相关配置；
- 使用 Xauth 或者 L2TP 拨号建立 VPN 连接。

组网拓扑



配置要点

- 配置接口 IP 地址
- 创建 IPSec VPN 用户
- 创建自动密钥隧道
  - 使用预共享密钥认证
  - 使用证书认证
- 配置访问策略
- 配置远程 VPN 客户端
  - Windows 内置客户端配置
  - NISG-IPS VPN 客户端软件安装和配置
  - TheGreenBow IPSec VPN 客户端配置
- 拨号连接

配置步骤

配置接口 IP 地址

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p1：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=202.118.101.2/24。
   - eth-s1p2：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=192.168.1.1/24。
2. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 202.118.101.2 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
```

创建 IPSec VPN 用户

1. 选择**系统** > **认证** > **网络用户**。
2. 点击**新建**，创建 IPSec VPN 用户：
   名称 =Alice，用户类型 =IPSec VPN，密码 / 确认密码 =alice123，分配的 IP= 静态 IP 地址 =30.1.1.10， IPSec VPN 配置 =L2TP。

提示：为远程用户分配静态 IP 地址或者 IP 地址池时，为避免 IP 冲突，不建议使用 VPN 网关后的子网 IP。

---

3. 设置认证方式。

提示：如果客户端与 VPN 网关之间存在 NAT 设备，则 ID 类型不能设置为 IPV4_ADDR。在此种场景下，当 VPN 的认证方式为预共享密钥认证时， IPSec VPN 用户的 ID 类型需设置为 FQDN （Xauth 用户还可以设置 USER_FQDN 或 KEY_ID）；当 VPN 的认证方式为证书认证时， ID 类型需设置为 DER_ANS1_DN。

   - 对于预共享密钥认证，对 ID 类型进行如下设置：
     ID 类型 =IPV4_ADDR， ID=10.2.1.155
   - 对于证书认证，则 ID 类型需要进行如下设置：
     ID 类型 =DER_ASN1_DN，
     ID=C=cn,ST=liaoning,O=test,OU=nsd,CN=Alice,emailAddress=Alice@test.com

---

提示：ID 与本地证书的主题信息相同。选择**系统 > 证书 > 本地证书**，查看主题信息。

---

4. 点击**确定**。

CLI

- 预共享密钥认证

```
NetEye@root-system] user authuser Alice authtype local password
alice123 enable
NetEye@root-system] user authuser Alice ipsecvpn ike-id ipv4-address
10.2.1.155 type l2tp
NetEye@root-system] user authuser Alice assigned-ip 30.1.1.10
NetEye@root-system] exit
```

- 证书认证

```
NISG-IPS@root-system] user authuser Alice ipsecvpn ike-id asn1-dn
C=cn,ST=liaoning,O=test,OU=nsd,CN=Alice,emailAddress=Alice@test.com
type l2tp
```

创建自动密钥隧道

- 使用预共享密钥认证
- 使用证书认证

使用预共享密钥认证

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，进行如下配置：
   - 名称 =ctog ；
   - 对端：类型 = 拨号用户，用户 =Alice ；
   - 出口：出口 =eth-s1p1，本端 IP 地址 =202.118.101.2 ；
   - 认证：认证方式 = 预共享密钥，密钥 =test123。
3. 如果是 Xauth 用户，还需要设置本端子网 (（192.168.1.0/24）。
4. 点击**确定**。

CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel ctog dialup-user user Alice interface
eth-s1p1 202.118.101.2 preshared-key test123 enable
NetEye@root-system-vpn] tunnel ctog local-subnet 192.168.1.0
255.255.255.0
NetEye@root-system-vpn] exit
```

使用证书认证

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条自动密钥隧道，具体配置请参见 使用预共享密钥认证 。设置认证方式为证书认证。
   - 认证
     - 认证方式 = 证书
     - 本地证书 =local
     - 对端 CA 证书 =ca
   - 高级设置 （可选）
     - ID 类型 =DER_ASN1_DN
     - ID=C=cn,ST=liaoning,O=test,OU=nsd,CN=alice,emailAddress=Alice@test.com
3. 点击**确定**。

CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel ctog dialup-user user Alice interface
eth-s1p1 202.118.101.2 certificate local ca enable
NetEye@root-system-vpn] tunnel ctog ike local-id asn1-dn
C=cn,ST=liaoning,O=test,OU=nsd,CN=alice,emailAddress=Alice@test.com
NetEye@root-system-vpn] exit
```

配置访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建访问策略，允许远程用户访问 VPN 网关后端的服务器子网。

   名称 =ctog，源安全域 = 任意，源 IP=30.1.1.10，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许。

   提示：这里的源 IP 地址非远程用户的真实 IP 地址，而是 NISG-IPS 分配给远程用户用来访问本地子网的一个虚拟的 IP 地址。

3. 点击**确定**。
4. 点击  。

CLI

```
NetEye@root-system] policy access ctog any 30.1.1.10 any 192.168.1.0/
24 any any permit enable
NetEye@root-system] exit
NetEye@root> save config
```

配置远程 VPN 客户端

IPSec VPN 远程访问用户可以使用 Windows 内置客户端连接到 VPN 网关，也可以安装 VPN 客户端软件进行访问。

- Windows 内置客户端配置
- NISG-IPS VPN 客户端软件安装和配置
- TheGreenBow IPSec VPN 客户端配置

Windows 内置客户端配置

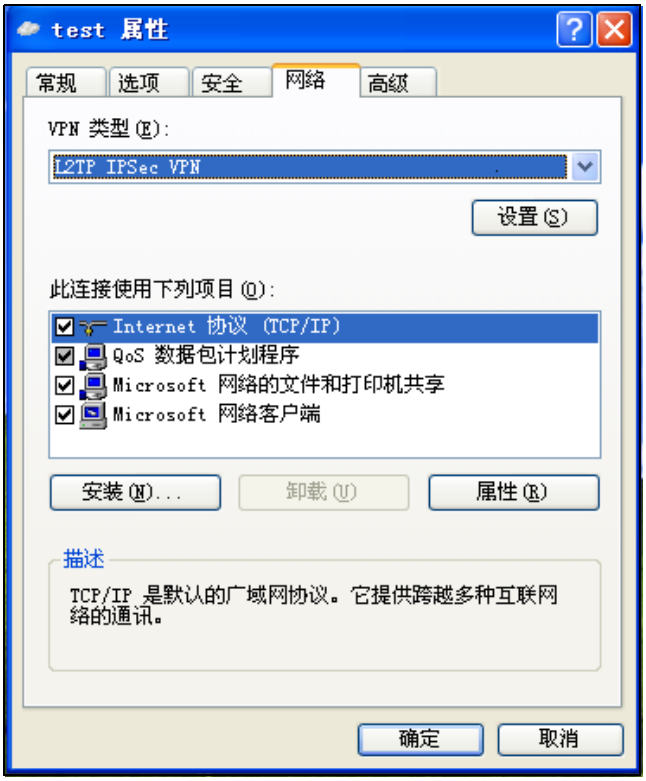
1. 选择**开始** > **所有程序** > **附件** > **通讯** > **网络连接**。
2. 在**网络任务**里选择**创建一个新的连接**，出现如下对话框。

3. 点击**下一步**。
4. 选择**连接到我的工作场所的网络**，点击**下一步**。
5. 选择**虚拟专用网络连接**，点击**下一步**。
6. 输入公司名，点击**下一步**。
7. 选择**不拔初始连接**，点击**下一步**。
8. 输入隧道的出口接口地址 202.118.101.2，点击**下一步**。

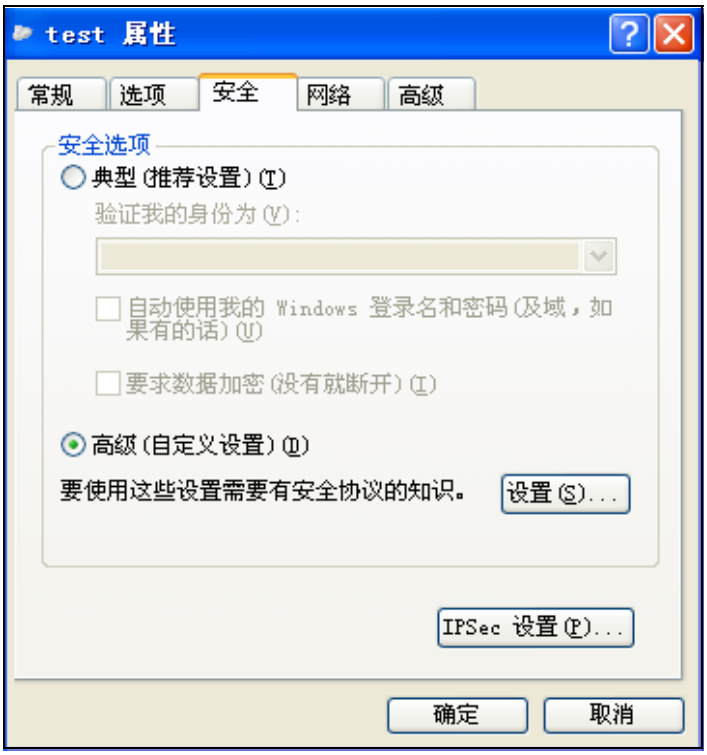
9. 点击**完成**，完成创建连接。

10. 在弹出的连接对话框上，点击**属性**。

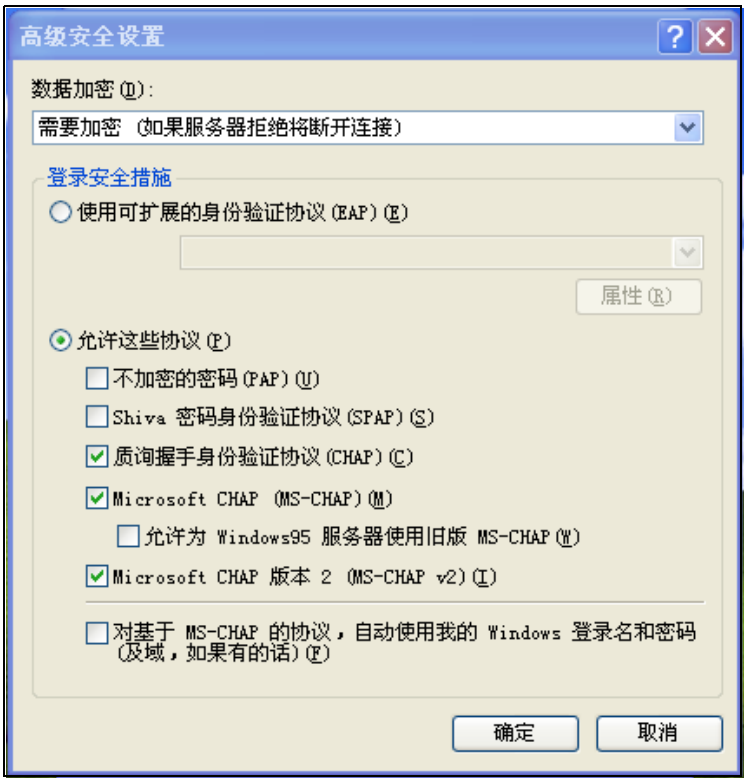
11. 选择**网络**，在 **VPN 类型**下拉框中选择 **L2TP IPSec VPN**，点击**确定**，返回连接窗口。



12. 点击**属性**，选择**安全**，进行安全设置。



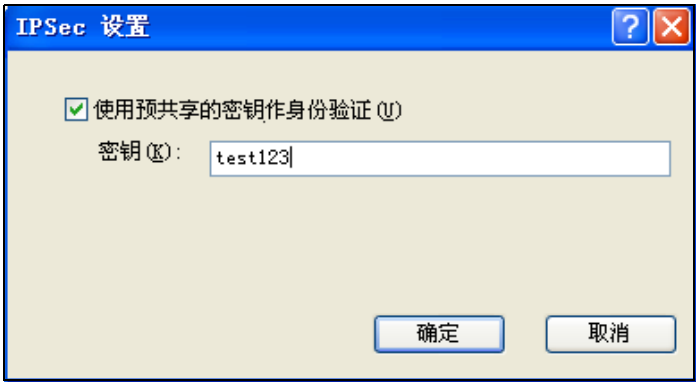
13. 选择**高级 （自定义设置）**，点击**设置。**



14. 在**允许这些协议**下，勾选**质询握手身份验证协议 (CHAP)**，点击**确定**。

15. 配置预共享密钥认证或者证书认证。

- 设置预共享密钥认证：点击 **IPSec 设置 ...**，勾选**使用预共享的密钥作身份认证**，设置预共享密钥为 test123，点击**确定**。

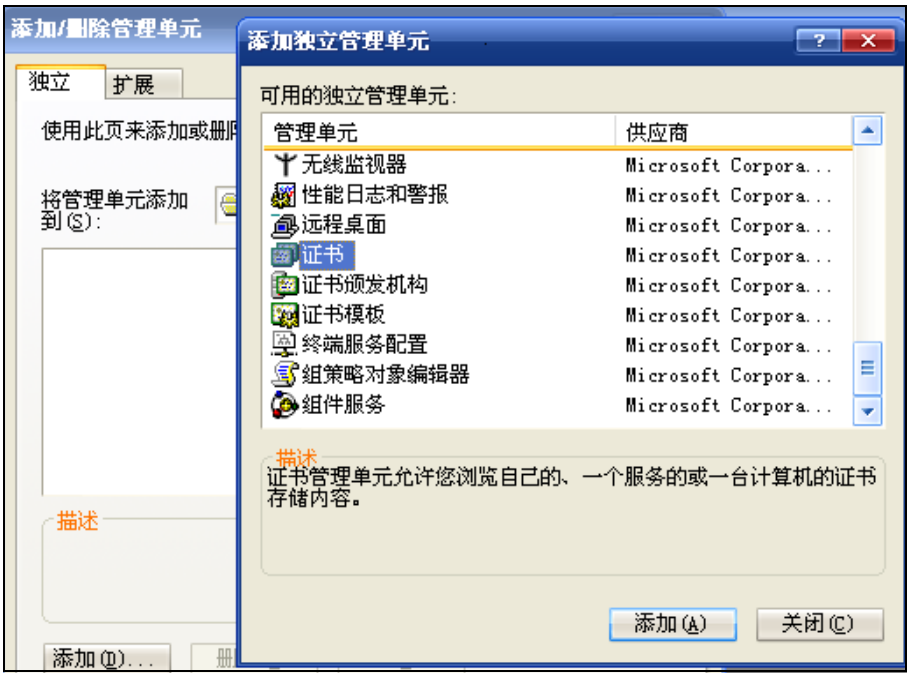


提示：当使用证书认证时，需要取消勾选**使用预共享的密钥作身份验证**。

- 设置证书认证 （导入证书）：

  a.点击**开始** > **运行**，输入 **mmc** 命令。

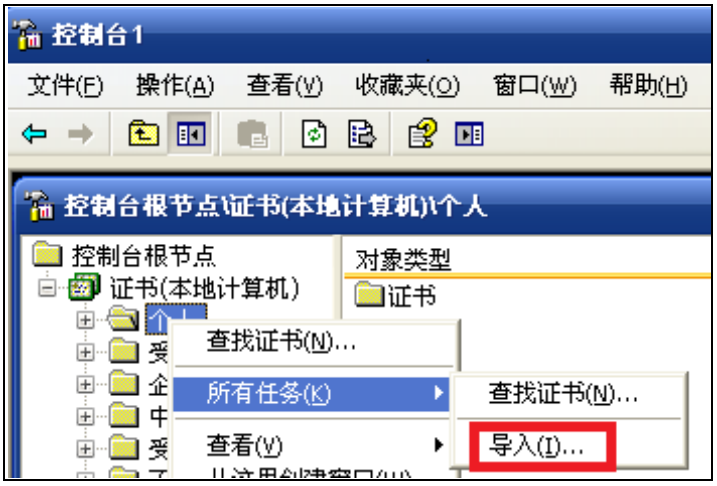
  b.选择**文件** > **添加 / 删除管理单元**。在**独立**页面中点击**添加**，选择**证书**，点击**添加**。



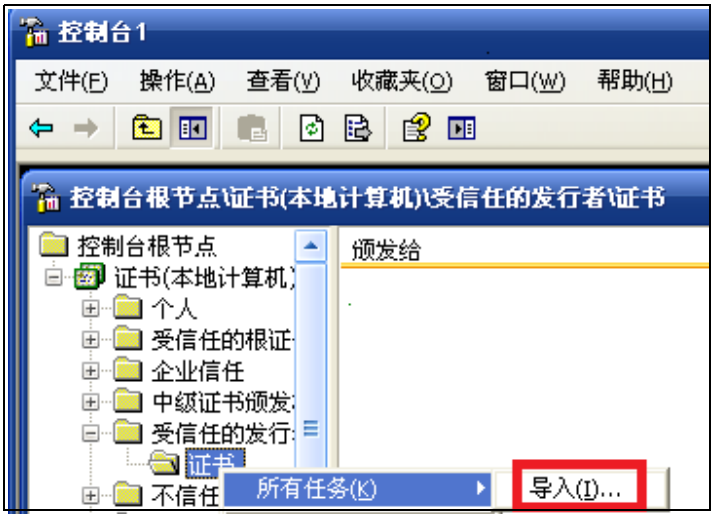
  c.选择**计算机账户** > **本地计算机** （运行这个控制台的计算机），添加证书完成。

  d.在控制台根节点下，展开证书节点，导入个人证书和 CA 证书。

■导入个人证书：



■导入 CA 证书：

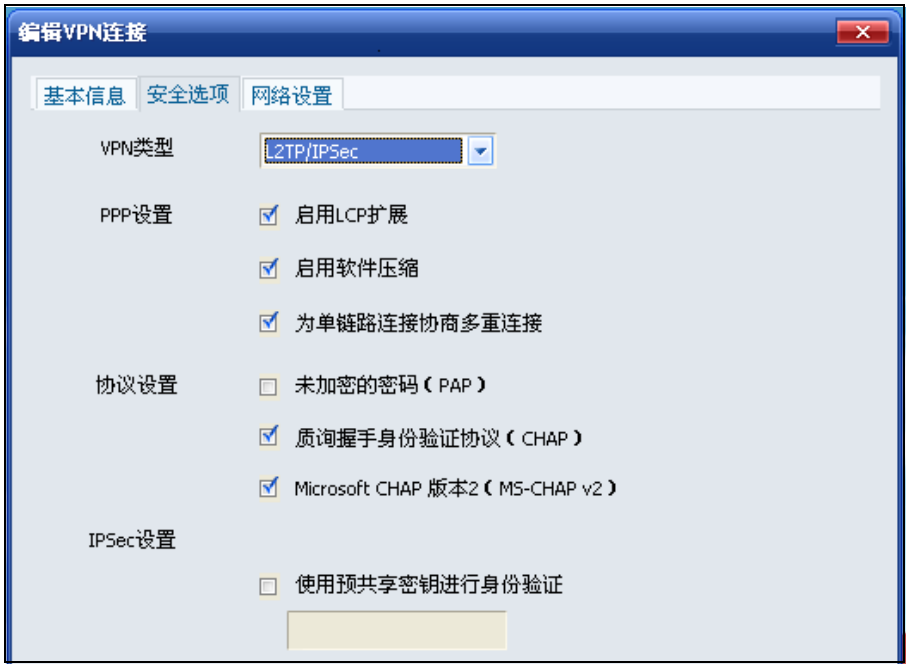


16. 点击**确定**。

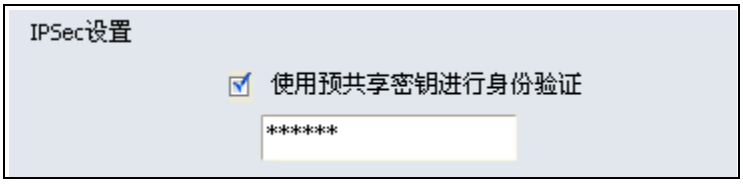
NISG-IPS VPN 客户端软件安装和配置

1. 在 Windows 操作系统下安装 IPSec VPN 客户端软件。
2. 点击**创建**，在弹出的**新建 VPN 连接**窗口中创建 VPN 连接。

3. 点击**安全选项**选项卡，设置安全选项信息。



- 如果使用预共享密钥认证，请勾选使用**预共享密钥进行身份验证**复选框。



- 如果使用证书认证，则需要取消勾选**使用预共享密钥进行身份验证**复选框。在**证书**选项卡中导入 CA 和本地证书。

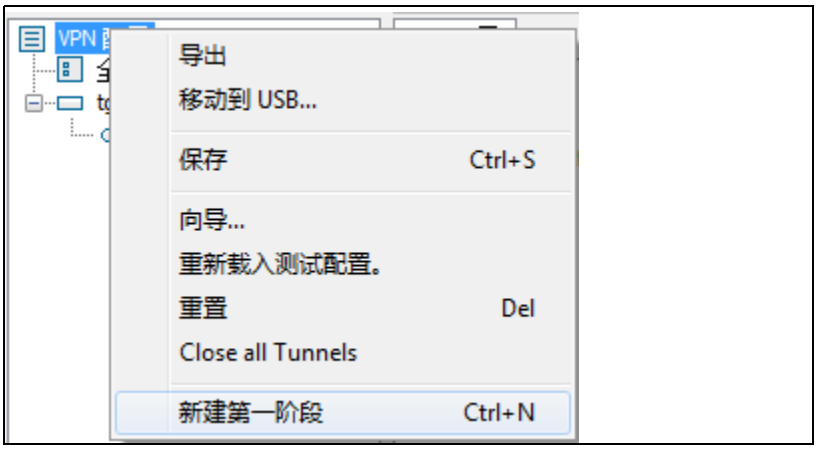
有关 VPN 客户端安装和配置的详细信息，请参见*东软 NetEye VPN 客户端用户使用指南*。

TheGreenBow IPSec VPN 客户端配置

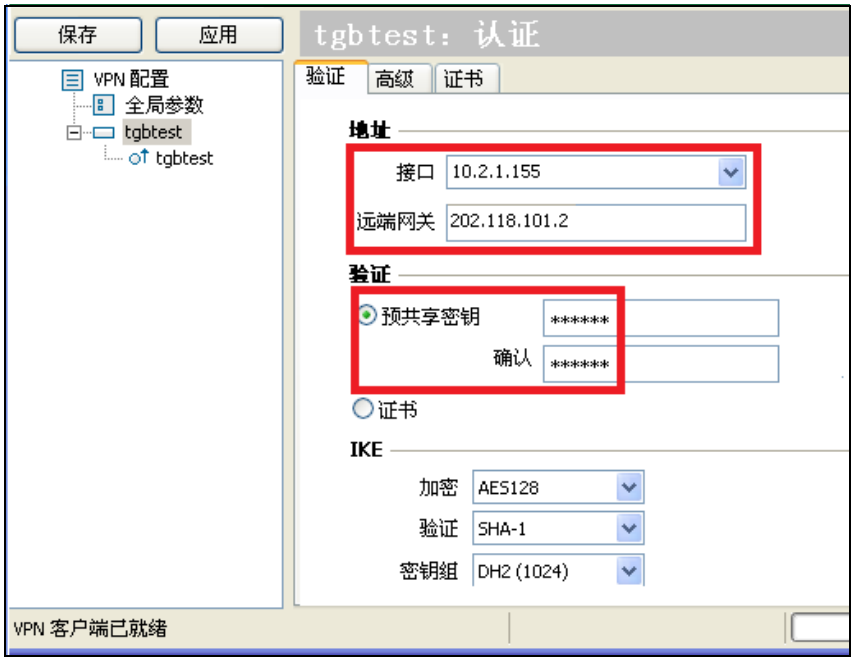
Xauth 认证用户可以安装和配置 TheGreenBow IPSec VPN 客户端软件连接到 IPSec VPN 网关。配置如下：

第一阶段：

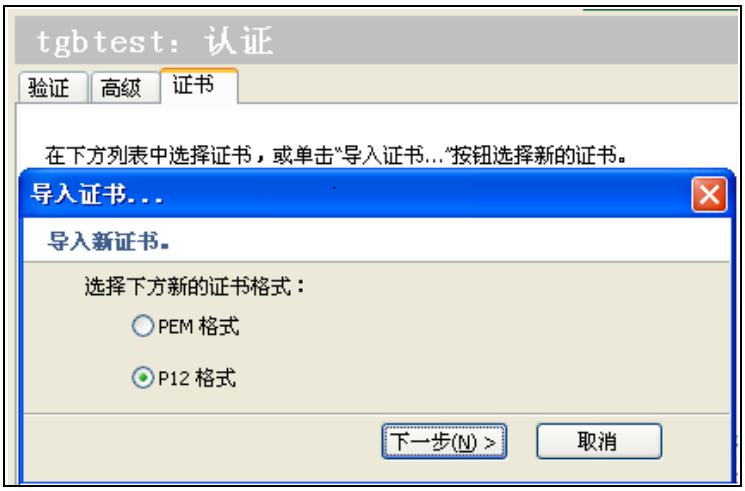
1. 打开客户端软件，右键点击 **VPN 配置**，选择**新建第一阶段**。



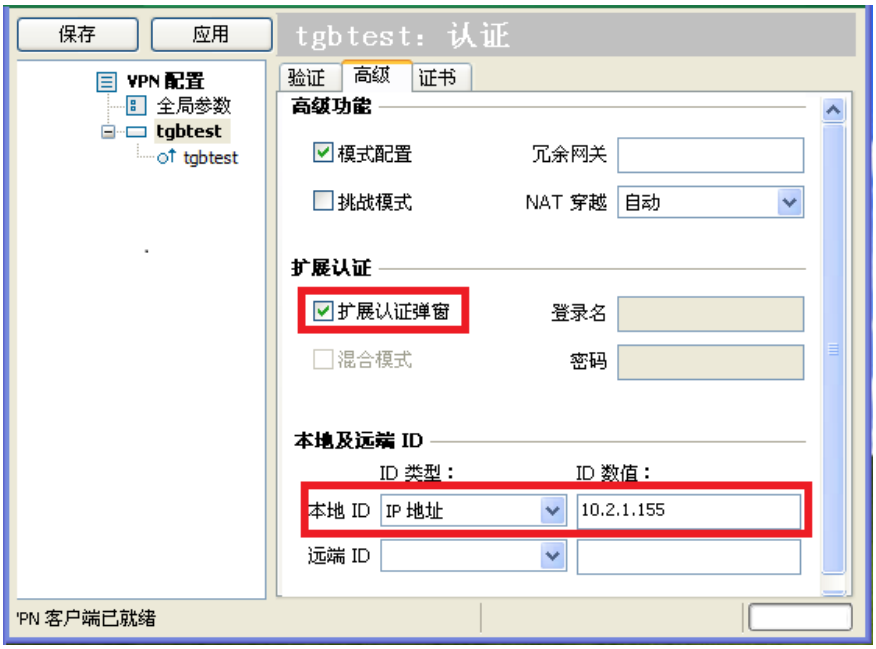
2. 进入**验证**页面，进行如下配置：
   - 如果使用预共享密钥认证，输入密钥。



- 如果使用证书认证，则点击**证书**按钮，进入**证书**页面，导入 CA 和本地证书（选择 **P12 格式**导入本地证书，选择 **PEM 格式**导入 CA 证书）。

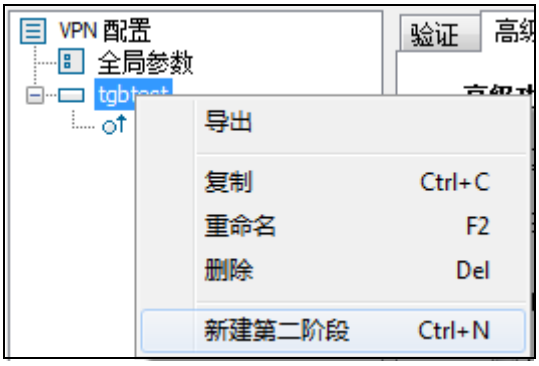


3. 进入**高级**页面，进行如下配置：

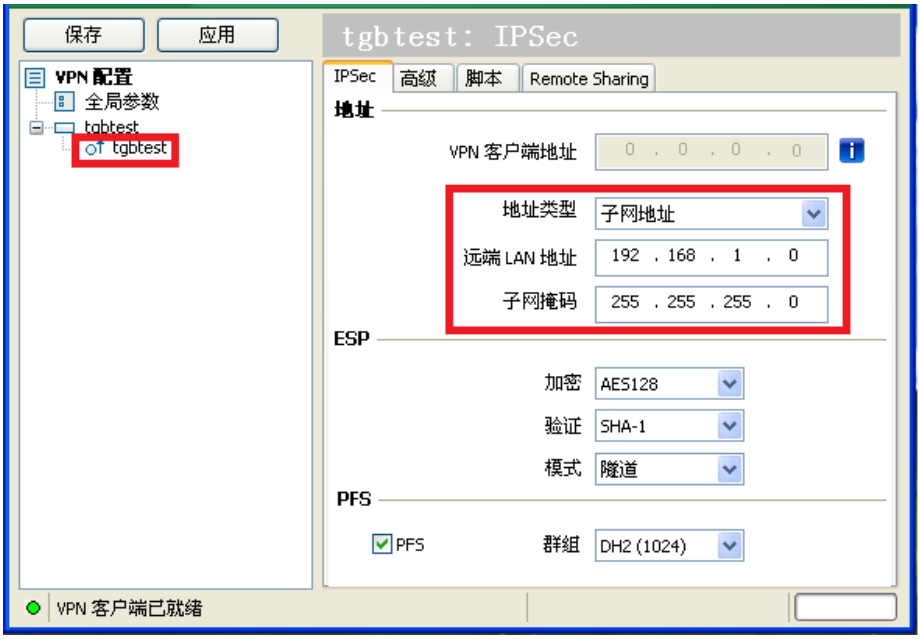


第二阶段：

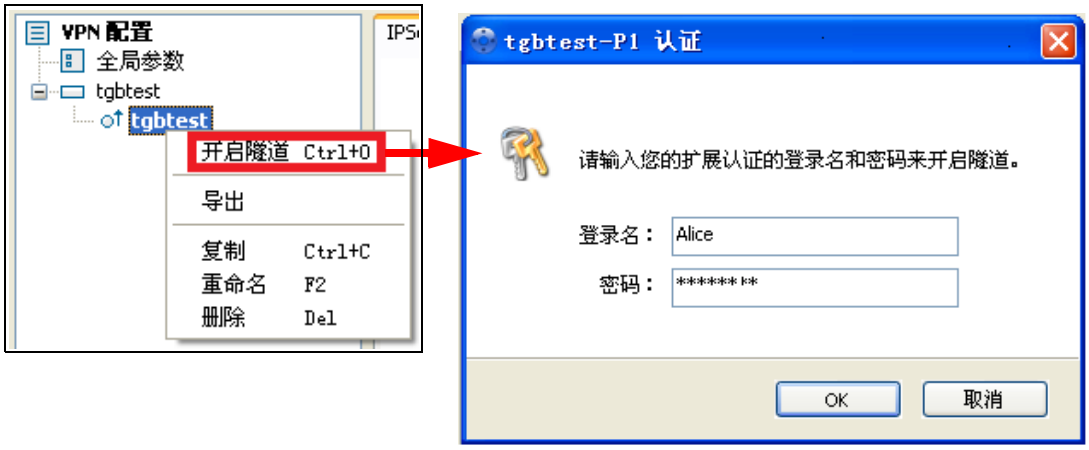
4. 选择**新建第二阶段**。



5. 进入 **IPSec** 页面，进行如下配置：



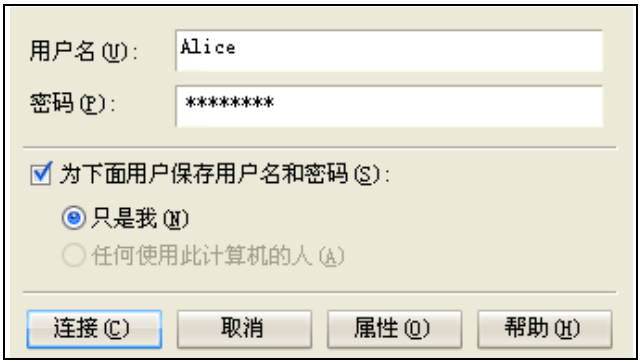
6. 点击**开启隧道**，在弹出的登录页面中输入用户名和密码进行 VPN 连接。



拨号连接

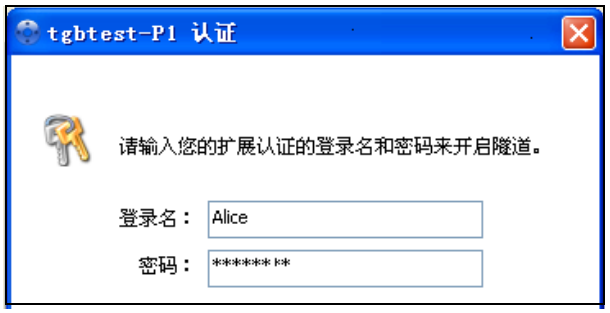
- Windows 内置客户端登录：

  输入用户名 Alice 及其对应的密码 alice123，点击**连接**，登录到 VPN 网关。



- 东软 NISG-IPS VPN 客户端软件登录。选中 VPN 连接，点击**连接**。

- Xauth 用户通过 TheGreenBow 客户端软件登录。



验证结果

选择**监控** > **IPSec VPN 隧道 > 自动密钥隧道**，进入 **自动密钥隧道**页面，查看 L2TP 用户和 Xauth 用户拨号连接 VPN 隧道的监控信息。

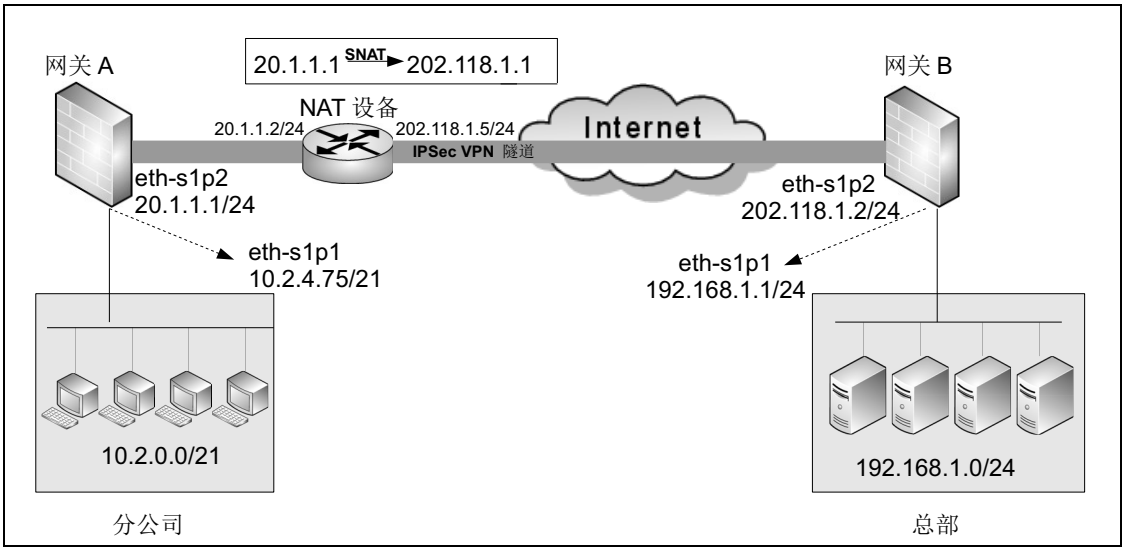
13.4.6 范例：NAT 穿越

基本需求

IPSec VPN 与 NAT 不兼容，在实施网段到网段 IPSec VPN 时，如果在 VPN 隧道之间存在 NAT 设备就会导致隧道通信失败，此时需要启用 NAT 穿越。

在本范例中，分公司需要远程访问总部的内网服务器资源。为了保证数据在互联网上安全传输，在分公司和总部之间建立了一条 IPSec VPN 隧道。另外，分公司的出口连接着一台 NAT 设备，通过 SNAT 规则将分公司的出口 IP 转换为公网 IP 地址，以隐藏分公司的真实 IP 地址。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置路由
- 创建自动密钥隧道
- 创建访问策略

提示：本范例场景中，事先已在 NAT 设备上配置了一条 SNAT 规则 （20.1.1.1 > 202.118.1.1），将分公司的出口 IP 转换为与 NAT 设备出口 IP 同一网段的地址。当存在 DNAT 或 MIP 规则的情况下， VPN 隧道两端的配置与 SNAT 环境下的配置相同。

配置步骤

配置接口 IP 地址

网关 A：

1. 选择**网络** > **接口**，配置接口：
   - eth-s1p1：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表，主 =10.2.4.75/21。
   - eth-s1p2：接口状态=开,模式=三层, MTU=1500，获取IP地址方式=静态IP，IP地址列表，主 =20.1.1.1/24。
2. 点击**确定**。

网关 B：

1. 选择**网络** > **接口**，配置接口：
   - eth-s1p1：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表，主 =192.168.1.1/24。
   - eth-s1p2：接口状态=开,模式=三层, MTU=1500，获取IP地址方式=静态IP，IP地址列表，主 =202.118.1.2/24。
2. 点击**确定**。

CLI

网关 A：

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 10.2.4.75 255.255.248.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 20.1.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
```

网关 B:

除了 IP 地址，其他命令与网关 A 的命令相同。

```
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.2 255.255.255.0
```

配置路由

网关 A：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，添加一条缺省路由。

   目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1, 出口接口 =eth-s1p2, 网关 =20.1.1.2。

3. 点击**确定**。

网关 B：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，添加一条缺省路由。

   目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =eth-s1p2，网关 =202.118.1.5。
3. 点击**确定**。

CLI

网关 A：

```
NetEye@root-system] route default interface eth-s1p2 gateway 20.1.1.2
```

网关 B：

```
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.1.5
```

创建自动密钥隧道

网关 A：

1. 选择**网络** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条隧道。
   - 名称 =atb ；
   - 对端：类型 = 静态 IP 地址，IP 地址 / 域名 =202.118.1.2 ；
   - 出口：出口 =eth-s1p2，本端 IP 地址 =20.1.1.1 ；
   - 认证：认证方式 = 预共享密钥，密钥 =123456。
3. 设置本端和对端子网。本端子网 =10.2.0.0/21，对端子网 =192.168.1.0/24。
4. 点击**高级设置**，配置本端和对端 ID。
   - 本端 ID 类型 =KEY_ID，密钥 ID=test ；
   - 对端 ID 类型 =KEY_ID，密钥 ID=test。

提示：当设置 ID 类型为 IPV4_ADDR 时，最好将本端密钥 ID 设置为 SNAT 转换后 IP，在本范例中为 202.118.1.1。

---

5. 点击**确定**。

CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel atb gateway 202.118.1.2 interface eth-
s1p2 20.1.1.1 preshared-key 123456 local-subnet 10.2.0.0
255.255.248.0 remote-subnet 192.168.1.0 255.255.255.0 enable
NetEye@root-system-vpn] tunnel atb ike local-id key-id test
NetEye@root-system-vpn] tunnel atb ike peer-id key-id test
NetEye@root-system-vpn] exit
```

VPN 网关 B：

方案 A：设置对端类型为**静态 IP 地址**，该 IP 地址为 SNAT 转换后 IP。

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条新的隧道。
   - 名称 =bta ；
   - 对端：类型 = 静态 IP 地址，IP 地址 / 域名 =202.118.1.1 ；
   - 出口：出口 =eth-s1p2，本端 IP 地址 =202.118.1.2 ；
   - 认证：认证方式 = 预共享密钥，密钥 =123456。
3. 设置本端和对端子网。本端子网 =192.168.1.0/24, 对端子网 =10.2.0.0/21。
4. **高级配置**区域：本端 ID 类型 =KEY_ID=test, 对端 ID 类型 =KEY_ID=test。
5. 点击**确定**。

CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel bta gateway 202.118.1.1 interface eth-s1p2 202.118.1.2 preshared-key 123456 local-subnet 192.168.1.0 255.255.255.0 remote-subnet 10.2.0.0 255.255.248.0 enable
NetEye@root-system-vpn] tunnel bta ike local-id key-id test
NetEye@root-system-vpn] tunnel bta ike peer-id key-id test
NetEye@root-system-vpn] exit
```

方案 B：设置对端类型为**动态 IP 地址**。

名称 =bta,

对端类型 = 动态 IP 地址，出口 =eth-s1p2, 本端 IP 地址 =202.118.1.2，认证方式 = 预共享密钥，密钥 =123456, 本端子网 =192.168.1.0/24, 对端子网 =10.2.0.0/21。

- 名称 =bta，对端：类型 = 动态 IP 地址；
- 出口：出口 =eth-s1p2，本端 IP 地址 =202.118.1.2 ；
- 认证：认证方式 = 预共享密钥，密钥 =123456 ；
- 本端子网 =192.168.1.0/24, 对端子网 =10.2.0.0/21。

提示：当设置对端类型为动态 IP 时，不需要在**高级配置**区域设置本端和对端 ID。

CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel bta gateway any interface eth-s1p2 202.118.1.2 preshared-key 123456 local-subnet 192.168.1.0 255.255.255.0 remote-subnet 10.2.0.0 255.255.248.0 enable
NetEye@root-system-vpn] exit
```

创建访问策略

VPN 网关 A:

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**, 创建一条访问策略 atb，允许数据流从子网 10.2.0.0/21 访问 192.168.1.0/24。

   名称 =atb，源安全域 = 任意，源 IP=10.2.0.0/21，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许。
3. 点击 atb 对应的，引用 VPN 隧道 atb，将本端子网向对端相应子网发起访问的数据流指向 VPN 隧道。
4. 点击**确定**。
5. 点击 。

VPN 网关 B:

以同样方式创建一条访问策略 bta，允许对端子网访问本端，并对隧道 bta 进行引流。

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**, 创建一条访问策略 bta，允许数据流从子网 10.2.0.0/21 访问 192.168.1.0/24。

   名称 =bta，源安全域 = 任意，源 IP=10.2.0.0/21，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许。
3. 点击 bta 对应的，引用 VPN 隧道 bta，将本端子网向对端相应子网发起访问的数据流指向 VPN 隧道。
4. 点击**确定**。
5. 点击 。

CLI

VPN 网关 A:

```
NetEye@root-system] policy access atb any 10.2.0.0/21 any 192.168.1.0/
24 any any permit enable
NetEye@root-system] policy access atb tunnel atb
NetEye@root-system] exit
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system] policy access bta any 10.2.0.0/21 any 192.168.1.0/
24 any any permit enable
NetEye@root-system] policy access bta tunnel bta
NetEye@root-system] exit
NetEye@root> save config
```

验证结果

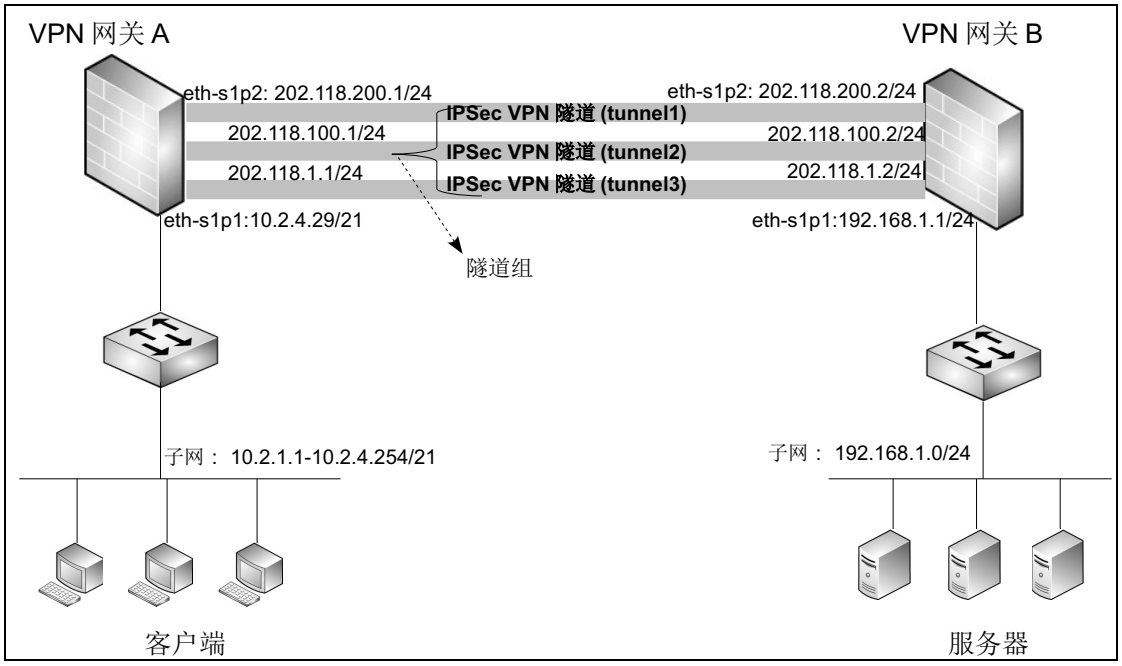
选择**监控** > **IPSec VPN 隧道** > **自动密钥隧道**，查看自动密钥隧道信息。

13.4.7 范例：IPSec VPN 隧道组

基本需求

隧道组是一组自动密钥隧道的集合，可以起到故障冗余的作用。为了防止正在工作的隧道断开而影响 VPN 网关 A 和 B 之间的通信，需要建立包含多条隧道的隧道组。当正在工作的隧道发生故障，则选择当前优先级最高的一条可用隧道作为通信的隧道，从而保证 VPN 业务的连续性。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置访问策略
- 创建自动密钥隧道
- 创建自动密钥隧道组
- 创建路由

配置步骤

配置接口 IP 地址

VPN 网关 A：

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p1：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=10.2.4.29/21。
   - eth-s1p2：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=202.118.200.1/24，从属 IP=202.118.100.1/24，202.118.1.1/24。

提示：为 eth-s1p2 接口配置三个 IP 地址，其中一个是主 IP ，其余两个是从属 IP。后续将创建三条自动密钥隧道，它们的出口接口都指向 eth-s1p2，但分别对应三个不同的 IP 地址。只有拥有主 IP 地址的隧道在划分到隧道组中后，将处于工作状态。

---

2. 点击**确定**。

VPN 网关 B：

用同样的方法为 VPN 网关 B 配置 IP 地址。

- eth-s1p1：开，三层， MTU=1500，静态 IP， IP 地址列表主 IP=192.168.1.1/24。
- eth-s1p2：开，三层，MTU=1500，静态 IP，IP 地址列表主 IP=202.118.200.2/24。从属 IP=202.118.100.2/24，202.118.1.2/24。

CLI

VPN 网关 A:

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 10.2.4.29 255.255.248.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.200.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] ip address 202.118.100.1 255.255.255.0
secondary
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.1 255.255.255.0
secondary
NetEye@root-system-if-eth-s1p2] exit
```

VPN 网关 B:

除了 IP 地址，其他的命令与 VPN 网关 A 一致。

```
NetEye@root-system-if-eth-s1p1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] ip address 202.118.200.2 255.255.255.0
NetEye@root-system-if-eth-s1p2] ip address 202.118.100.2 255.255.255.0
secondary
NetEye@root-system-if-eth-s1p2] ip address 202.118.1.2 255.255.255.0
secondary
```

配置访问策略

VPN 网关 A:

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建一条访问策略，允许本端客户端主机访问对端服务器。

   名称 =atob，源安全域 = 任意，源 IP=10.2.1.1-10.2.4.254，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许。
3. 点击**确定**。

VPN 网关 B:

1. 选择**防火墙** > **访问策略**。
2. 点击**新建** , 创建一条访问策略 atb，允许对端客户端主机访问本端服务器。

   名称 =atob1，源安全域 = 任意，源 IP=10.2.1.1-10.2.4.254，目的安全域 = 任意，目的 IP/ 域名 =192.168.1.0/24，服务 = 任意，动作 = 允许。
3. 点击**确定**。

CLI

VPN 网关 A:

```
NetEye@root-system] policy access atob any 10.2.1.1-10.2.4.254 any
192.168.1.0/24 any any permit enable
NetEye@root-system] exit
```

VPN 网关 B:

```
NetEye@root-system] policy access atob1 any 10.2.1.1-10.2.4.254 any
192.168.1.0/24 any any permit enable
NetEye@root-system] exit
```

创建自动密钥隧道

VPN 网关 A

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条自动密钥隧道 tunnel1。
   - 名称 =tunnel1 ；
   - 对端：类型 = 静态 IP 地址，IP 地址 / 域名 =202.118.200.2 ；
   - 出口：出口 =eth-s1p2，本端 IP 地址 =202.118.200.1 ；
   - 认证：认证方式 = 预共享密钥，密钥 =123456。
3. 点击**确定**。
4. 以同样的方式创建自动密钥隧道 tunnel2 和 tunnel3。

VPN 网关 B:

1. 选择 **VPN** > **IPSec VPN** > **自动密钥隧道**。
2. 点击**新建**，创建一条自动密钥隧道 tunnel1。
   - 名称 =tunnel1 ；

- 对端：类型 = 静态 IP 地址，IP 地址 / 域名 =202.118.200.1 ；
- 出口：出口 =eth-s1p2，本端 IP 地址 =202.118.200.2 ；
- 认证：认证方式 = 预共享密钥，密钥 =123456。

3. 点击**确定**。
4. 以同样的方式创建自动密钥隧道 tunnel2 和 tunnel3。

CLI

VPN 网关 A：

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel tunnel1 gateway 202.118.200.2 interface
eth-s1p2 202.118.200.1 preshared-key 123456 enable
NetEye@root-system-vpn] tunnel tunnel2 gateway 202.118.100.2 interface
eth-s1p2 202.118.100.1 preshared-key 123456 enable
NetEye@root-system-vpn] tunnel tunnel3 gateway 202.118.1.2 interface
eth-s1p2 202.118.1.1 preshared-key 123456 enable
```

VPN 网关 B:

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel tunnel1 gateway 202.118.200.1 interface
eth-s1p2 202.118.200.2 preshared-key 123456 enable
NetEye@root-system-vpn] tunnel tunnel2 gateway 202.118.100.1 interface
eth-s1p2 202.118.100.2 preshared-key 123456 enable
NetEye@root-system-vpn] tunnel tunnel3 gateway 202.118.1.1 interface
eth-s1p2 202.118.1.2 preshared-key 123456 enable
```

创建自动密钥隧道组

VPN 网关 A 和 B:

1. 选择 **VPN** > **IPSec VPN** > **隧道组**。
2. 点击**新建**，在两个网关上各创建一个 IPSec VPN 隧道组，将隧道 tunnel1、 tunnel2、tunnel3 包含进来，并设置不同的优先级。
   - 隧道名称 =tunnel1，优先级 =100 ；
   - 隧道名称 =tunnel2，优先级 =80 ；
   - 隧道名称 =tunnel3，优先级 =60。
3. 点击**确定**。

CLI

```
NetEye@root-system-vpn] tunnelgroup group enable
NetEye@root-system-vpn] tunnelgroup group tunnel tunnel1 priority 100
NetEye@root-system-vpn] tunnelgroup group tunne2 tunnel1 priority 80
NetEye@root-system-vpn] tunnelgroup group tunne3 tunnel1 priority 60
NetEye@root-system-vpn] tunnelgroup group enable
NetEye@root-system-vpn] exit
```

创建路由

VPN 网关 A：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，添加一条静态路由，将此路由的出口接口指定为隧道组接口。
   目的 IPv4 地址 =192.168.1.0，掩码长度 =24， Metric=1, 出口接口 =tunnelgroup

   提示：创建隧道组时将自动生成一个隧道组接口 tunnelgroup。
3. 点击**确定**。

VPN 网关 B：

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，添加一条静态路由，将此路由的出口接口指定为隧道组接口。
   目的 IPv4 地址 =10.2.0.0，掩码长度 =21， Metric=1, 出口接口 =tunnelgroup
3. 点击**确定**。
4. 点击 。

CLI

VPN 网关 A：

```
NetEye@root-system] e 192.168.1.0 255.255.255.0 interface tunnelgroup
NetEye@root-system] exit
NetEye@root> save config
```

VPN 网关 B：

```
NetEye@root-system] e 10.2.0.0 255.255.248.0 interface tunnelgroup
NetEye@root-system] exit
NetEye@root> save config
```

验证结果

当隧道协商成功后，网关 A 后端子网中的客户端主机能够成功访问网关 B 后端的服务器子网。

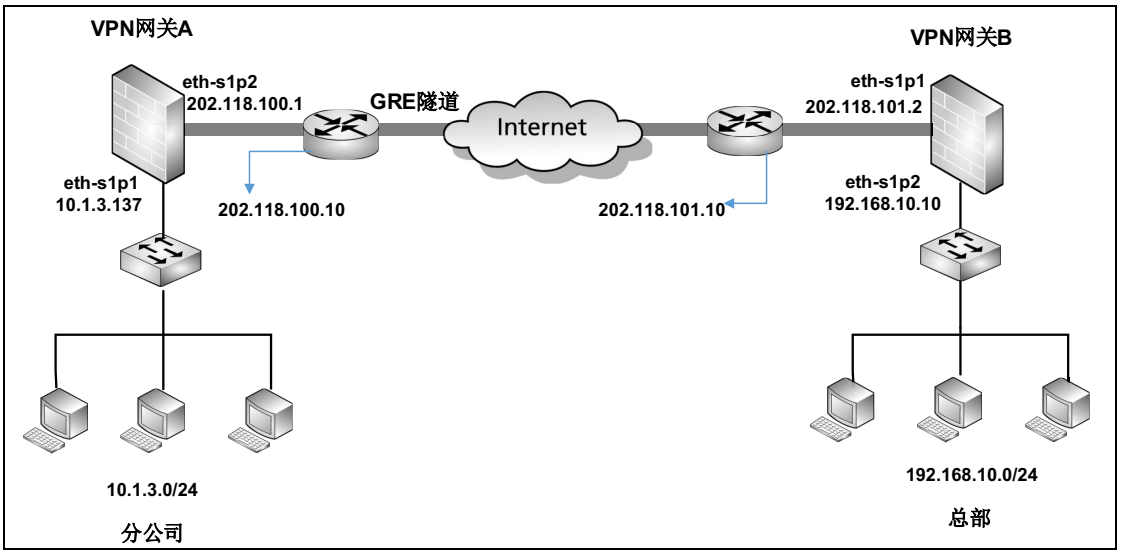
- 选择**监控** > **IPSec VPN 隧道** > **隧道组**，查看两端设备隧道组中的隧道，皆为可用状态。
- 或者选择**监控** > **IPSec VPN 隧道** > **自动密钥隧道**，查看到数据流量通过 tunnel1 进行转发。
- 当 tunnel1 发生故障时，NISG-IPS 会根据优先级选择 tunnel2 来接替 tunnel1 继续工作。

13.4.8 范例：GRE 隧道

基本需求

某分公司要从其私有网络穿越 Internet 与总部进行通讯，并需要对公网隐藏其内部私有 IP 地址，但对数据传输的安全性没有太多要求，此时可以在两边网关设备上创建一条 GRE 隧道，实现数据传输。 GRE VPN 部署简单、通用性好，并且对隧道两端网关设备的 CPU 消耗较少。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置路由
- 创建 GRE 隧道
- 配置访问策略

配置步骤

配置接口 IP 地址

VPN 网关 A：

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p1：接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=10.1.3.137/24。
   - eth-s1p2：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=202.118.100.1/24。
2. 点击**确定**。

VPN 网关 B:

用同样的方法为 VPN 网关 B 配置 IP 地址。

- eth-s1p1：开，三层， MTU=1500，静态 IP， IP 地址列表主 IP=202.118.101.2/24。
- eth-s1p2：开，三层， MTU=1500，静态 IP， IP 地址列表主 IP=192.168.10.10/24。

CLI

VPN 网关 A:

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 10.1.3.137 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 202.118.100.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
```

VPN 网关 B:

除了 IP 地址，其他的命令与 VPN 网关 A 一致。

```
NetEye@root-system-if-eth-s1p1] ip address 202.118.101.2 255.255.255.0
NetEye@root-system-if-eth-s1p2] ip address 192.168.10.10 255.255.255.0
```

配置路由

VPN 网关 A:

1. 选择**网络** > **路由** > **缺省路由**，添加一条缺省路由。
2. 点击**新建**，添加一条路由。管理员也可以修改系统已存在的缺省路由 （出口接口和网关）。

   目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =eth-s1p2，网关 =202.118.100.10。
3. 点击**确定**。

VPN 网关 B:

1. 选择**网络** > **路由** > **缺省路由**，添加一条缺省路由。
2. 点击**新建**，添加一条路由。管理员也可以修改系统已存在的缺省路由 （出口接口和网关）。

   目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =eth-s1p1，网关 =202.118.101.10。
3. 点击**确定**。

CLI

VPN 网关 A:

```
NetEye@root-system] route default interface eth-s1p2 gateway
202.118.100.10
```

```
NetEye@root-system] exit
```

VPN 网关 B:

```
NetEye@root-system] route default interface eth-s1p1 gateway
202.118.101.10
NetEye@root-system] exit
```

创建 GRE 隧道

VPN 网关 A:

1. 选择 **VPN** > **GRE 隧道**。
2. 点击**新建**，创建 GER 隧道。

   名称 =atob_gre，本地 IP 地址 =202.118.100.1，对端 IP 地址 =202.118.101.2，密钥 =10011001。
3. 点击**确定**。

VPN 网关 B:

1. 选择 **VPN** > **GRE 隧道**。
2. 点击**新建**，创建 GER 隧道。

   名称 =btoa_gre，本地 IP 地址 =202.118.101.2，对端 IP 地址 =202.118.100.1，密钥 =10011001

   提示：本端和对端密钥值必须相同。
3. 点击**确定**。

CLI

VPN 网关 A:

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel atob_gre gre remote-ip 202.118.101.2
local-ip 202.118.100.1 key 10011001 enable
NetEye@root-system-vpn] exit
```

VPN 网关 B:

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel btoa_gre gre remote-ip 202.118.100.1
local-ip 202.118.101.2 key 10011001 enable
NetEye@root-system-vpn] exit
```

配置访问策略

VPN 网关 A:

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建两条访问策略。

- 策略 atob 允许数据流从本端子网访问对端子网。

  名称 =atob，源安全域 = 任意，源 IP=10.1.3.0/24，目的安全域 = 任意，目的 IP/ 域名 =192.168.10.0/24，服务 = 任意，动作 = 允许。

- 策略 btoa 则允许数据流从对端子网访问本端子网。

  名称 =btoa，源安全域 = 任意，源 IP=192.168.10.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.1.3.0/24，服务 = 任意，动作 = 允许。

3. 点击 atob 对应的 ，引用 VPN 隧道 atob_gre，将本端子网向对端相应子网发起访问的数据流指向 VPN 隧道。
4. 点击**确定**。
5. 点击 。

VPN 网关 B:

以同样方式创建两条访问策略 btoa_1 和 atob_1，并通过 btoa_1 进行隧道引流。

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建两条访问策略。
   - 策略 btoa_1 允许数据流从本端子网访问对端子网。

     名称 =btoa_1，源安全域 = 任意，源 IP=192.168.10.0/24，目的安全域 = 任意，目的 IP/ 域名 =10.1.3.0/24，服务 = 任意，动作 = 允许。

   - 策略 atob_1 则允许数据流从对端子网访问本端子网。

     名称 =atob_1，源安全域 = 任意，源 IP=10.1.3.0/24，目的安全域 = 任意，目的 IP/ 域名 =192.168.10.0/24，服务 = 任意，动作 = 允许。
3. 点击 btoa_1 对应的 ，引用 VPN 隧道 btoa_gre，将本端子网向对端相应子网发起访问的数据流指向 VPN 隧道。
4. 点击**确定**。

点击 。

CLI

VPN 网关 A:

```
NetEye@root-system] policy access atob any 10.1.3.0/24 any
192.168.10.0/24 any any permit enable
NetEye@root-system] policy access atob tunnel atob_gre
NetEye@root-system] policy access btoa any 192.168.10.0/24 any
10.1.3.0/24 any any permit enable
NetEye@root-system] exit
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system] policy access btoa_1 any 192.168.10.0/24 any
10.1.3.0/24 any any permit enable
NetEye@root-system] policy access btoa_1 tunnel btoa_gre
```

```
NetEye@root-system] policy access atob_1 any 10.1.3.0/24 any
192.168.10.0/24 any any permit enable
NetEye@root-system] exit
NetEye@root> save config
```

验证结果

选择**监控 > GRE 隧道**，查看已建立的 GRE 隧道。

13.4.9 范例：SSL VPN 入口页面

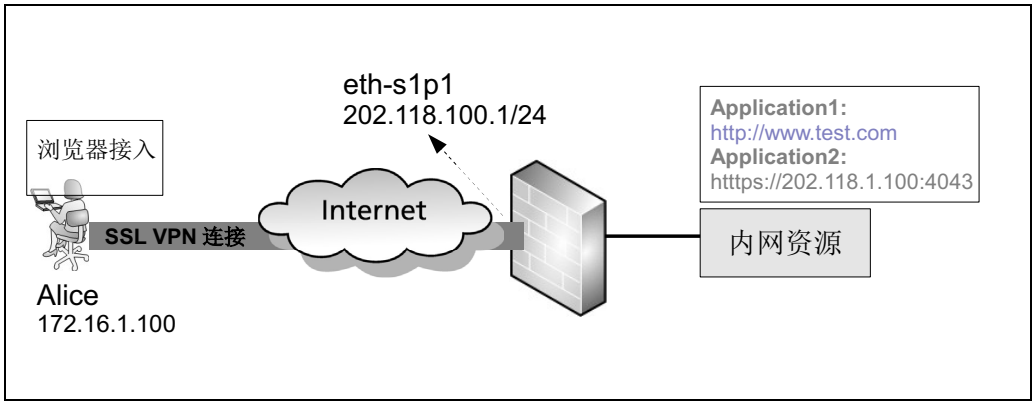
基本需求

非办公区域远程用户 Alice 通过 Web-Only 型的 SSL VPN 隧道，登录 Web 入口页面，可以访问受 VPN 网关保护的内网 Web 服务器资源。

SSL VPN 具有如下特点：

- 配置简单，可轻松实现远程访问；
- 远程用户通过浏览器访问，无需安装客户端软件；
- 限于访问 HTTP/HTTPS 网站；
- 客户端通过证书对 SSL VPN 服务器进行认证，用户通过用户名和密码进行身份认证，保证合法访问。

组网拓扑



配置要点

- 配置接口 IP 地址
- 配置访问策略
- 导入 CA/ 本地证书
- 创建 SSL VPN 用户
- 创建 SSL VPN 用户组
- 创建 SSL VPN 应用
- 创建 SSL VPN 页面模板
- 创建 SSL VPN 页面服务

配置步骤

配置接口 IP 地址

1. 选择**网络** > **接口**，配置接口。

   eth-s1p1：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=202.118.100.1/24。

2. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 202.118.100.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
```

配置访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建一条访问策略，允许用户访问 HTTP 和 HTTPS 服务。

   名称 =ctog，源安全域 = 任意，源 IP=172.16.1.100，目的安全域 = 任意，目的 IP/ 域名 = 任意，服务 =HTTP/HTTPS，动作 = 允许。

3. 点击**确定**。

CLI

```
NetEye@root-system] policy access ctog any 172.16.1.100 any any
protocol-object HTTP any permit enable
NetEye@root-system] policy access ctog protocol protocol-object HTTPS
```

导入 CA/ 本地证书

1. 选择**系统** > **证书** > **CA 证书** 。
2. 点击**导入**，从本地导入 NISG-IPS 的 CA 证书，名称为 ca。
3. 选择**系统** > **证书** > **本地证书**。
4. 点击**导入**，从本地导入 NISG-IPS 的本地证书，名称为 local1。
5. 点击**确定**。

CLI

```
NetEye@root-system] import certificate ca from x/zmodem ca
NetEye@root-system] import certificate local from x/zmodem local1
```

创建 SSL VPN 用户

1. 选择**系统** > **认证** > **网络用户**。
2. 点击**新建**，创建一个新的用户。

   名称 =Alice，用户类型 =SSL VPN，密码 / 确认密码 =test12。
3. 点击**确定**。

CLI

```
NetEye@root-system] user authuser Alice authtype local password test12
enable
NetEye@root-system] user authuser Alice sslvpn
```

创建 SSL VPN 用户组

SSL VPN 为用户组提供 SSL VPN 服务。如果某个用户要访问 SSL VPN 服务，需要首先将其划分到 SSL VPN 用户组中。

1. 选择 **VPN** > **SSL VPN** > **用户组**。
2. 点击**新建**，创建一个新的用户组 group1 并为其分配用户 Alice。
3. 点击**确定**。

CLI

```
NetEye@root-system] sslvpn
NetEye@root-system-sslvpn] group group1
NetEye@root-system-sslvpn] group group1 user Alice
NetEye@root-system-sslvpn] group group1 external no
```

创建 SSL VPN 应用

1. 选择 **VPN** > **SSL VPN** > **SSL VPN Web 入口页面** > **应用**。
2. 点击**新建**，添加新的应用。
   - 名称 =Application1，类型 =HTTP， URL=www.test.com ；
   - 名称 =Application2，类型 =HTTPS， URL=202.118.1.100:4043。
3. 点击**确定**。

CLI

```
NetEye@root-system-sslvpn] application Application1 type http url
www.test.com
NetEye@root-system-sslvpn] application Application2 type https url
202.118.1.100:4043
```

创建 SSL VPN 页面模板

1. 选择 **VPN** > **SSL VPN** > **SSL VPN Web 入口页面** > **页面模板**。
2. 点击**新建**，创建一个新的页面模板。

名称 =temp1，标题 =Welcome，主题色 =#FFCC99，语言 = 简体中文，应用列表 =Application1+Application2，允许自定义应用 =HTTP+HTTPS。

3. 点击**确定**。

CLI

```
NetEye@root-system-sslvpn] portal-template temp1
NetEye@root-system-sslvpn] portal-template temp1 applist Application1
NetEye@root-system-sslvpn] portal-template temp1 applist Application2
NetEye@root-system-sslvpn] portal-template temp1 title Welcome
NetEye@root-system-sslvpn] portal-template temp1 language Chinese
NetEye@root-system-sslvpn] portal-template temp1 themecolor #FFCC99
NetEye@root-system-sslvpn] portal-template temp1 customapp HTTP enable
NetEye@root-system-sslvpn] portal-template temp1 customapp HTTPS
enable
```

创建 SSL VPN 页面服务

1. 选择 **VPN** > **SSL VPN** > **SSL VPN Web 入口页面** > **页面服务**。
2. 点击**新建**，创建新的页面服务。
   - 服务绑定

     名称 =service1，接口 =eth-s1p1， IP 地址 =202.118.100.1，端口 =10443
   - 服务配置

     用户组 =group1，入口页面 =temp1
   - SSL 配置

     SSL 证书 =local1
   - 客户端安全要求

     使用默认设置
   - 被允许的访问

     IP 地址 =172.16.1.100
   - 用户组访问授权
     - 用户组 =group1，应用 =Application1，动作 = 允许；
     - 用户组 =group1，应用 =Application2，动作 = 允许。
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root-system-sslvpn] portal-service service1 interface eth-s1p1
ip 202.118.100.1 port 10443 portal-template temp1 certificate local1
group1
NetEye@root-system-sslvpn] portal-service service1 allow zone any
172.16.1.100
```

```
NetEye@root-system-sslvpn] portal-service service1 privilege group
group1 application Application1 permit
NetEye@root-system-sslvpn] portal-service service1 privilege group
group1 application Application2 permit
NetEye@root-system-sslvpn] portal-service service1 privilege default-
group-privilege permit
NetEye@root-system-sslvpn]portal-service service1 enable
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

验证结果

- 查看客户端
- 查看 VPN 网关

查看客户端

1. 打开浏览器 , 输入 https://202.118.100.1:10443, 登录到 SSL VPN Web 入口页面。输入用户名 Alice, 密码 test12 及验证码。
2. 点击应用对应的超链接，可对内网相应网站进行访问。管理员可以点击**添加**，添加更多的自定义应用。

查看 VPN 网关

选择**监控 > 在线用户 > SSL VPN 用户**，查看 SSL VPN 用户相关信息。

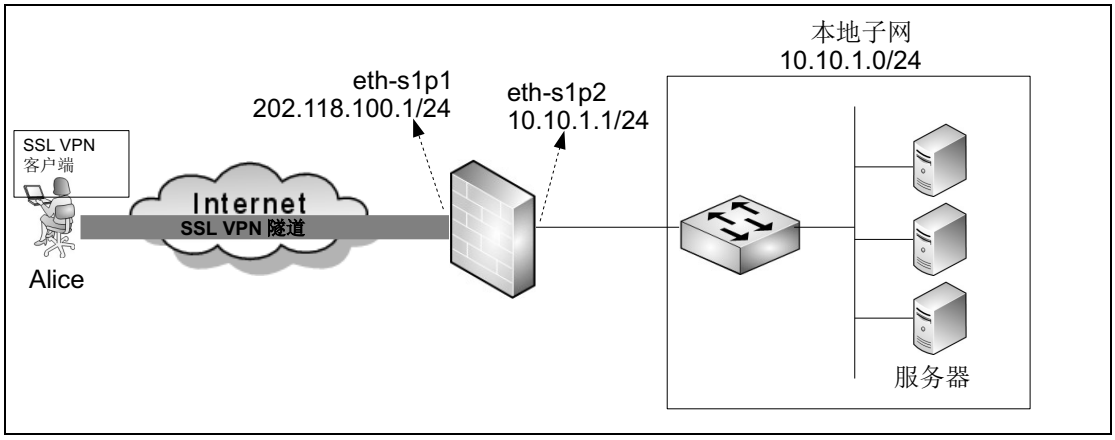
13.4.10 范例：SSL VPN 隧道

基本需求

在本范例中，远程用户 Alice 使用 SSL VPN 隧道访问受 VPN 网关保护的子网服务器资源。隧道型 SSL VPN 具有如下特点：

- 配置简单，可轻松实现远程访问；
- VPN 可扩展性强；
- 无需通过浏览器访问，但是需要安装 SSL VPN 客户端；
- 与 Web-Only 型的 SSL VPN 相比，隧道型 SSL VPN 可访问多样性的内网资源，应用类别不受限制；
- 客户端通过证书对 SSL VPN 服务器进行认证，用户通过用户名和密码进行身份认证，保证合法访问。

组网拓扑



配置要点

NISG-IPS 配置

- 配置接口 IP 地址
- 创建 IP 地址池
- 创建访问策略
- 创建 SSL VPN 用户
- 创建 SSL VPN 用户组
- 创建 SSL VPN 隧道

远程用户客户端配置

- 添加 SSL VPN 连接
- 连接到 SSL VPN 服务器

配置步骤

配置接口 IP 地址

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p1：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=202.118.100.1/24。
   - eth-s1p2：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表主 IP=10.10.1.1/24。
2. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 202.118.100.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 10.10.1.1 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
```

创建 IP 地址池

1. 选择 **VPN** > **IP 地址池**。
2. 点击**新建**，创建地址池。系统将从该地址池中为远程用户分配一个 IP 地址，进行 SSL VPN 连接。

   名称 =pool1，起始 IP 地址 =192.168.1.2，终止 IP 地址 =192.168.1.100。

   提示：IP 地址池包含的 IP 不能与 VPN 网关后的子网 IP 重合。
3. 点击**确定**。

CLI

```
NetEye@root-system] ippool pool1 192.168.1.2-192.168.1.100
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建一条访问策略，允许远程用户访问内网服务器。其中，源 IP 为 IP 地址池中的地址。

   名称 =ctog，源安全域 = 任意，源 IP=192.168.1.2-192.168.1.100，目的安全域 = 任意，目的 IP/ 域名 =10.10.1.0/24，服务 = 任意，动作 = 允许。

3. 点击**确定**。

CLI

```
NetEye@root-system] policy access ctog any 192.168.1.2-192.168.1.100
any 10.10.1.0/24 any any permit enable
```

创建 SSL VPN 用户

1. 选择**系统** > **认证** > **网络用户**。
2. 点击**新建**，创建一个新的用户。

   名称 =Alice，用户类型 =SSL VPN，密码 / 确认密码 =test12， IP 地址池 =pool1。
3. 点击**确定**。

CLI

```
NetEye@root-system] user authuser Alice authtype local password test12
enable
NetEye@root-system] user authuser Alice sslvpn
NetEye@root-system] user authuser Alice assigned-ip pool1
```

创建 SSL VPN 用户组

1. 选择 **VPN** > **SSL VPN** > **用户组**。
2. 点击**新建**，创建一个新的用户组 group1 并为其分配用户 Alice。
3. 点击**确定**。

CLI

```
NetEye@root-system] sslvpn
NetEye@root-system-sslvpn] group group1
NetEye@root-system-sslvpn] group group1 user Alice
NetEye@root-system-sslvpn] group group1 external no
```

创建 SSL VPN 隧道

1. 选择 **VPN** > **SSL VPN** > **SSL VPN 隧道** > **隧道**。
2. 点击**新建**，创建一条新的 SSL VPN 隧道。

   名称 =tunnel1，用户组 =group1，出口接口 =eth-s1p1，本地 IP 地址 =202.118.100.1，授权子网列表 =10.10.1.0/24。
3. 点击**确定**。
4. 点击 。

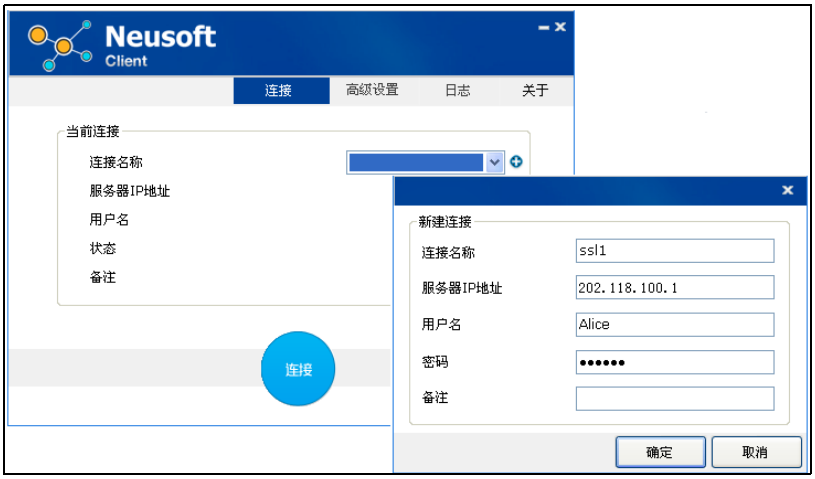
CLI

```
NetEye@root-system-sslvpn] tunnel tunnel1 interface eth-s1p1
202.118.100.1 group group1 allowed-subnet 10.10.1.0 255.255.255.0
enable
```

```
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

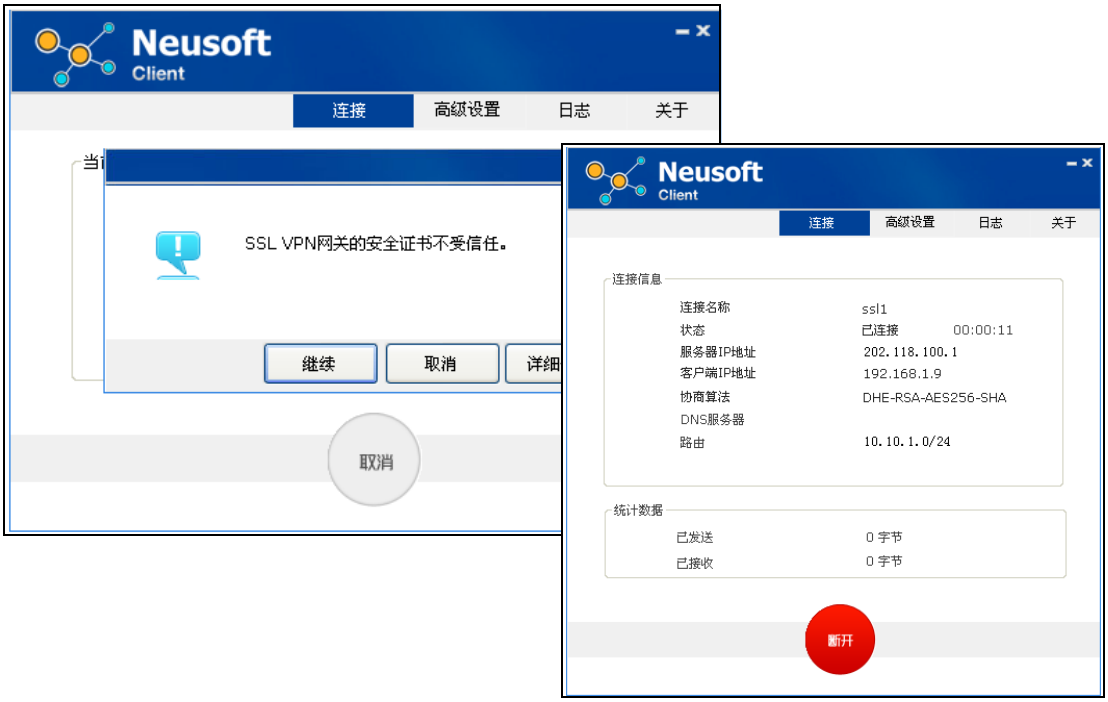
添加 SSL VPN 连接

在客户端安装 SSL VPN 客户端软件。关于 SSL VPN 客户端软件具体的安装步骤，请参见*东软 NetEye SSL VPN Windows 客户端用户使用指南*。添加一条 SSL VPN 连接，配置如下：



连接到 SSL VPN 服务器

点击**连接**和**继续**， Alice 会成功连接到 SSL VPN 服务器。



验证结果

登录 NISG-IPS，选择**监控** > **在线用户** > **SSL VPN 用户**，查看 Alice 的在线信息。 Alice 可以进一步访问 NISG-IPS 后端的服务器。

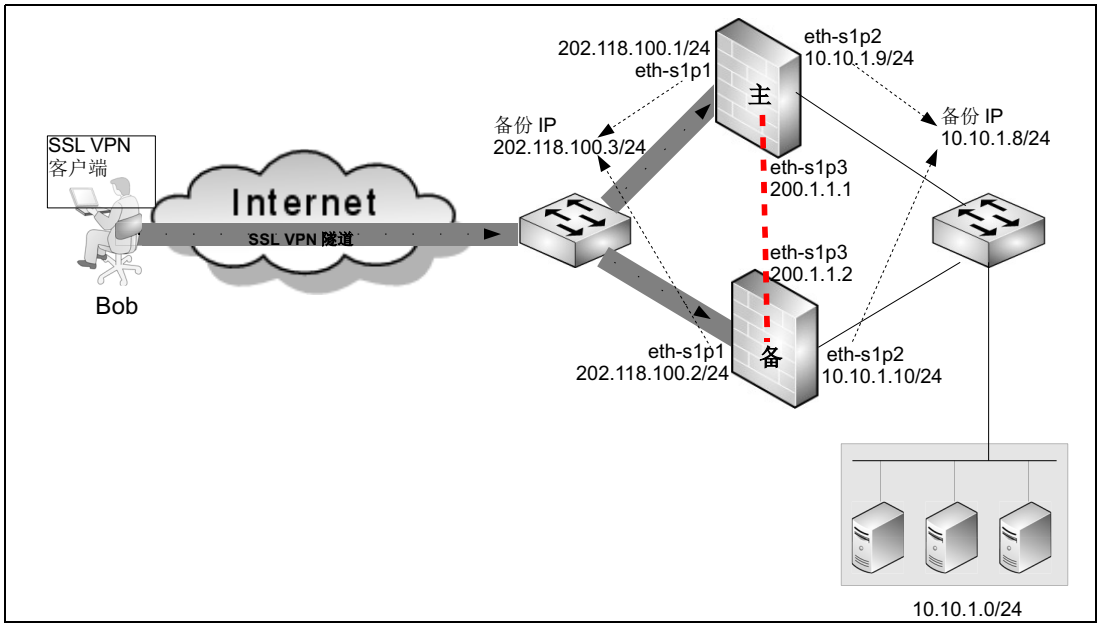
13.4.11 范例：HA 自动同步 （SSL VPN 隧道)

基本需求

在高可用性环境中，两台相同配置的设备组成一个组。其中一台设备作为主设备提供网络服务；另一台设备则作为备份设备。高可用性的冗余机制，可以避免由于单点故障而导致网络中断。

该范例描述了如何在隧道型 SSL VPN 环境中应用高可用性 , 主设备使用备份 IP 地址 202.118.100.3 提供 SSL VPN 隧道服务。当发生故障时，备份设备会接管它的工作，并自动同步其配置和运行信息，以保证业务的连续性。

组网拓扑



配置要点

- 主备设备的基本配置：
  - 配置接口 IP 地址
  - 配置虚拟路由器探测组
  - 配置虚拟路由器
  - 配置集群
- 主设备的 SSL VPN 配置：
  - 创建 IP 地址池
  - 创建访问策略
  - 创建 SSL VPN 用户
  - 创建 SSL VPN 用户组
  - 创建 SSL VPN 隧道

- 客户端配置：
  - 安装 SSL VPN 客户端
  - 创建客户端连接

配置步骤

配置接口 IP 地址

主设备：

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p1：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP（主） =202.118.100.1/24。
   - eth-s1p2：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP（主） =10.10.1.9/24。
   - eth-s1p3: 接口状态 = 开，模式 = 二层。
2. 点击**确定**。

提示：以太网接口 eth-s1p3 作为二层接口，其 IP 地址只能在集群中设置。有关设置 eth-s1p3 的 IP 地址的详细信息，请参见 配置集群 。

备份设备：

1. 选择**网络** > **接口**，配置接口。
   - eth-s1p1：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP（主） =202.118.100.2/24。
   - eth-s1p2：接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP（主） =10.10.1.10/24。
   - eth-s1p3：接口状态 = 开，模式 = 二层。
2. 点击**确定**。

CLI

主设备：

```
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 202.118.100.1 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 10.10.1.9 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet eth-s1p3
NetEye@root-system-if-eth-s1p3] working-type layer2-interface
NetEye@root-system-if-eth-s1p3] exit
```

备份设备：

```
NetEye@root-system] interface ethernet eth-s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] ip address 202.118.100.2 255.255.255.0
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet eth-s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] ip address 10.10.1.10 255.255.255.0
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet eth-s1p3
NetEye@root-system-if-eth-s1p3] working-type layer2-interface
NetEye@root-system-if-eth-s1p3] exit
```

配置虚拟路由器探测组

主设备：

1. 选择**系统** > **高可用性** > **虚拟路由器探测组**。
2. 点击**新建**，进行如下配置：

   组 ID=1，优先级 =120， IP 探测类型 =Ping，接口 =Any， IP=10.10.1.1，权重 =30。

   提示：要探测的 IP 地址 10.10.1.1 为目的网络中的设备。

3. 点击**确定**。

备份设备：

与主设备配置方法相同（优先级除外）。

1. 选择**系统** > **高可用性** > **虚拟路由器探测组**。
2. 点击**新建**，进行如下配置：

   组 ID=1，优先级 =100， IP 探测类型 =Ping，接口 =Any， IP=10.10.1.1，权重 =30。
3. 点击**确定**。

CLI

主设备：

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] priority 120
NetEye@root-system-dg1] interval 1
NetEye@root-system-dg1] ip-track type ping interface any ip 10.10.1.1
interval 3 threshold 3 weight 30
NetEye@root-system-dg1] exit
```

备份设备：

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] priority 100
NetEye@root-system-dg1] interval 1
NetEye@root-system-dg1] ip-track type ping interface any ip 10.10.1.1
interval 3 threshold 3 weight 30
NetEye@root-system-dg1] exit
```

配置虚拟路由器

主设备：

1. 选择**系统** > **高可用性** > **虚拟路由器**。
2. 点击**新建**，创建 ID 号分别为 1 和 2 的虚拟路由器并分配到虚拟路由器探测组中。
   - VRID=1，接口 =eth-s1p1，组名 =1，权重 =30，启用该虚拟路由器 = 勾选，备份 IP 地址 =202.118.100.3，掩码长度 =24 ；
   - VRID=2，接口 =eth-s1p2，组名 =1，权重 =30，启用该虚拟路由器 = 勾选，备份 IP 地址 =10.10.1.8，掩码长度 =24。
3. 点击**确定**。

备份设备：

与主设备配置方法相同。

CLI

主设备：

```
NetEye@root-system] virtual er 1
NetEye@root-system-vr1] election interface eth-s1p1
NetEye@root-system-vr1] backup ip address 202.118.100.3 mask
255.255.255.0
NetEye@root-system-vr1] virtual-er enable
NetEye@root-system-vr1] exit
NetEye@root-system] virtual er 2
NetEye@root-system-vr2] election interface eth-s1p2
NetEye@root-system-vr2] backup ip address 10.10.1.8 mask 255.255.255.0
NetEye@root-system-vr2] virtual-er enable
NetEye@root-system-vr2] exit
NetEye@root-system] detection group 1
NetEye@root-system-dg1] hold virtual-er 1 weight 30
NetEye@root-system-dg1] hold virtual-er 2 weight 30
NetEye@root-system-dg1] exit
```

备份设备：

备份设备的 CLI 配置与主设备相同。

配置集群

当在主备两台设备分别配置集群并且启用自动同步功能之后，两台设备上的配置信息和运行信息都会自动同步到对端。

主设备：

1. 选择**系统** > **高可用性** > **集群**，配置集群。
   - 基本信息

     接口 =eth-s1p3，本端 IP 地址 =200.1.1.1，掩码长度 =24，对端 IP 地址 =200.1.1.2，集群 ID=1
   - 同步

     自动同步配置信息 = 开启

     自动同步运行信息 = 开启

     自动同步系统时间 = 开启

     当设备启动时 = 勾选

     将此时间设置应用到两端设备 = 勾选
2. 点击**确定**。

CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth-s1p3
NetEye@root-system-cluster] local ip address 200.1.1.1 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 200.1.1.2
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] time syn enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] time benchmark on
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] exit
```

备份设备：

1. 选择**系统** > **高可用性** > **集群**，配置集群。
   - 基本信息

     接口 =eth-s1p3，本端 IP 地址 =200.1.1.2，掩码长度 =24，对端 IP 地址 =200.1.1.1，集群 ID=1
   - 同步

     自动同步配置信息 = 开启

     自动同步运行信息 = 开启

     自动同步系统时间 = 开启

当设备启动时 = 勾选

2. 点击**确定**。

CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth-s1p3
NetEye@root-system-cluster] local ip address 200.1.1.2 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 200.1.1.1
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] time syn enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] exit
```

提示：以下设置只需要在主设备上进行，因为开启集群功能后，主设备上的实时配置将自动同步到备份设备。

创建 IP 地址池

1. 选择 **VPN** > **IP 地址池**。
2. 点击**新建**，创建一个地址池。 NISG-IPS 将从地址池中为用户分配地址进行 SSL VPN 连接。

   名称 =ippool1，起始 IP 地址 =30.1.1.1，终止 IP 地址 =30.1.1.100。

   提示：IP 地址池包含的 IP 不能与 VPN 网关后的子网 IP 重合。

3. 点击**确定**。

CLI

```
NetEye@root-system] ippool ippool1 30.1.1.1-30.1.1.100
```

创建访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**，创建一条访问策略，允许远程用户使用 IP 地址池中的地址访问目的网络。

   名称 =policy1，源安全域 = 任意，源 IP=30.1.1.1-30.1.1.100，目的安全域 = 任意，目的 IP/ 域名 =10.10.1.0/24，服务 = 任意，动作 = 允许。

3. 点击**确定**。

CLI

```
NetEye@root-system] policy access policy1 any 30.1.1.1-30.1.1.100 any
10.10.1.0/24 any any permit enable
```

创建 SSL VPN 用户

1. 选择**系统** > **认证** > **网络用户**。
2. 点击**新建**，创建一个 SSL VPN 用户。

   名称 =Bob，用户类型 =SSL VPN，密码 / 确认密码 =123456， IP 地址池 =ippool1，首选 DNS IP 地址 =10.1.3.121，首选 WINS IP 地址 =10.1.3.119。
3. 点击**确定**。

CLI

```
NetEye@root-system] user authuser Bob authtype local password 123456
enable
NetEye@root-system] user authuser Bob sslvpn
NetEye@root-system] user authuser Bob assigned-ip ippool1 dns1
10.1.3.121 wins1 10.1.3.119
```

创建 SSL VPN 用户组

1. 选择 **VPN** > **SSL VPN** > **用户组**。
2. 点击**新建**，创建一个名称为 group1 用户组，并将用户 Bob 划分到该组中。
3. 点击**确定**。

CLI

```
NetEye@root-system] sslvpn
NetEye@root-system-sslvpn] group group1
NetEye@root-system-sslvpn] group group1 user Bob
```

创建 SSL VPN 隧道

1. 选择 **VPN** > **SSL VPN** > **SSL VPN 隧道** > **隧道**。
2. 点击**新建**，创建一条新的隧道。

   名称 =ssltunnel1，用户组 =group1，出口接口 =eth-s1p1，本地 IP 地址 =202.118.100.3，授权子网列表 =10.10.1.0/24。
3. 点击**确定**。
4. 点击 。

CLI

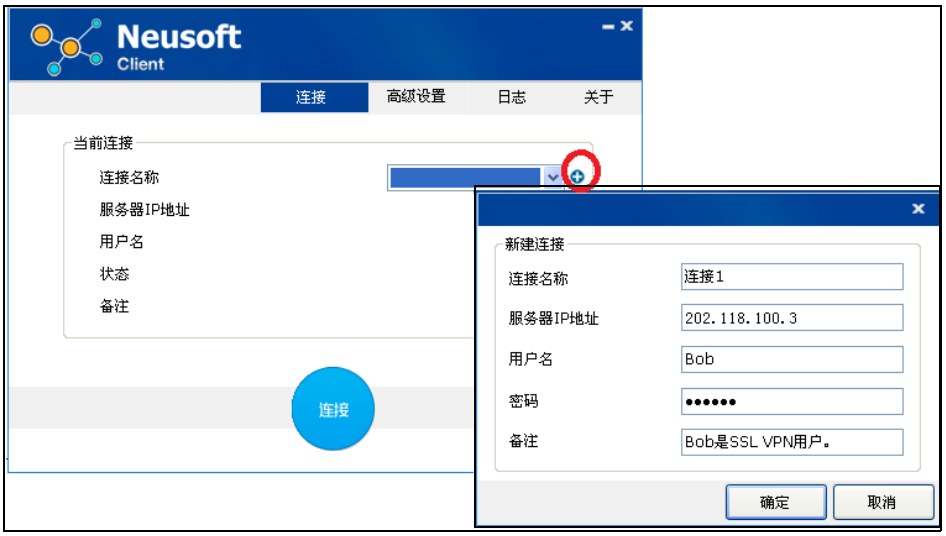
```
NetEye@root-system-sslvpn] tunnel ssltunnel1 interface eth-s1p1
202.118.100.3 enable
NetEye@root-system-sslvpn] tunnel ssltunnel1 group group1
NetEye@root-system-sslvpn] tunnel ssltunnel1 allowed-subnet 10.10.1.0
255.255.255.0
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

安装 SSL VPN 客户端

在客户端安装 SSL VPN 客户端软件。有关 SSL VPN 客户端软件使用的详细信息，请参见*东软 NetEye SSL VPN Windows 客户端用户使用指南*和*东软 NetEye SSL VPN Android 客户端用户使用指南*。

创建客户端连接

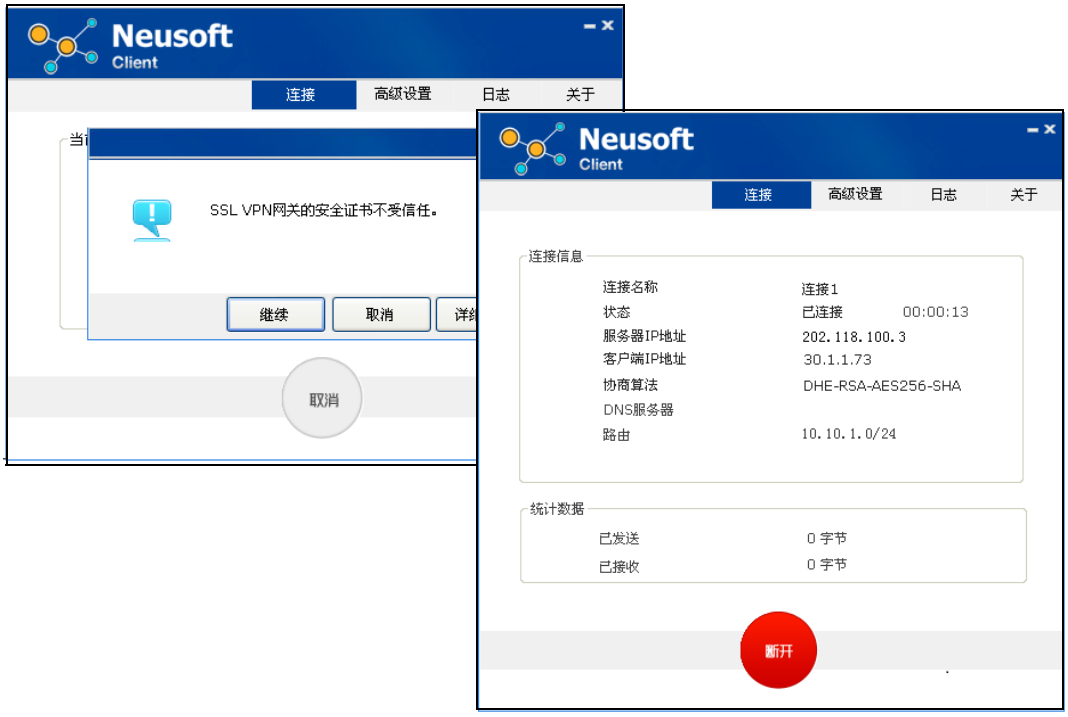
1. 添加一条 SSL VPN 连接，进行如下配置：



2. 点击**高级设置**选项卡，勾选**自动重连**复选框，保证当发生故障切换时， SSL VPN 可以立即重新连接。

验证结果

点击**连接**和**继续**。 SSL VPN 用户 Bob 可以成功连接 NISG-IPS，通过使用分配到的地址 30.1.1.73，可以对内网资源进行访问。当主设备发生故障时，备份设备会立即接替其工作，从而使 Bob 的访问不受任何影响。



14 高可用性

NISG-IPS 提供高可用性 （High Availability， HA）功能用于防止设备单点故障导致的网络中断。

本章主要介绍以下内容：

14.1 概述

本节介绍以下内容：

14.1.1 三层高可用性

14.1.1.1 虚拟路由器冗余协议

NISG-IPS 通过虚拟路由器冗余协议 (Virtual Router Redundancy Protocol, VRRP) 实现高可用性功能。该协议能够提高路由的可靠性，使流量绕开已经发生故障的设备。 NISG-IPS 支持 VRRPv2 版本。

14.1.1.2 VRRP 路由器和虚拟路由器

VRRP 路由器是运行 VRRP 协议的真实路由器。虚拟路由器包含两个或两个以上的 VRRP 路由器，代表多个 VRRP 路由器实现高可用性。一台 VRRP 路由器可被多台虚拟路由器引用。在高可用性组网中，需要将主机的缺省网关设置为虚拟路由器的 IP 地址（在 NISG-IPS 中称为备份 IP 地址），而不是具体的某个 VRRP 路由器的 IP 地址。

各 VRRP 路由器在虚拟路由器中处于不同状态。 VRRP 路由器有如下三种状态：

- Initialize：表示 VRRP 路由器处于未启用状态，或者处于初始状态，未参与选举。
- Master：表示该设备为主设备，拥有备份 IP 地址，并且负责转发数据包。
- Backup：处于 Backup 状态时，设备为备份设备，不转发数据包，仅负责监听主设备状态，主设备故障时，接替主设备工作。

提示：当 VRRP 路由器未配置任何选举接口或备份 IP 时，它将一直处于 Backup 状态。

14.1.1.3 主设备的选举

每个 VRRP 路由器都有一个优先级 （1-255），优先级最高的将成为主设备。主设备选举遵循以下规则：

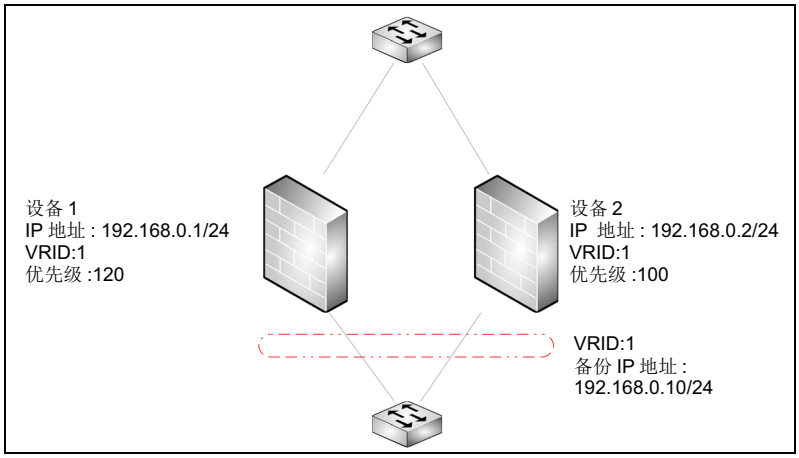
- 拥有备份 IP 地址的 VRRP 路由器将成为主设备，该设备拥有最高优先级 255。
- 如果同一虚拟路由器中的VRRP路由器的优先级相同，选举接口IP地址较大的设备将成为主设备。
- 当开启抢占模式时，备份设备如果优先级大于主设备，则将成为主设备。

14.1.1.4 部署模式

NISG-IPS 可部署在主备模式和主主模式下。

典型主备模式部署如图 20 所示。

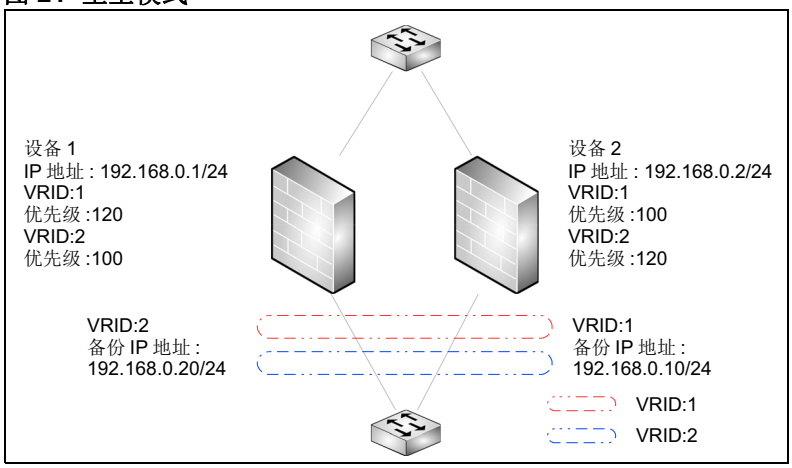
图 20 主备模式



根据优先级，设备 1 为主设备，设备 2 为备份设备。内部网络中主机的网关都需要指向虚拟路由器 1 的备份 IP 地址。

典型主备模式部署如图 21 所示。

图 21 主主模式



在虚拟路由器 1 中，设备 1 为主设备，设备 2 为备份设备。在虚拟路由器 2 中，设备 1 为备份设备，设备 2 为主设备。您需要将内网的部分主机的网关设置为虚拟路由器 1 的备份 IP 地址，将剩余部分的主机的网关设置为虚拟路由器 2 的备份 IP 地址。此时，两台设备都转发流量并且互为备份设备。

14.1.2 二层高可用性

14.1.2.1 原理概述

NISG-IPS 能够部署在两台路由器之间提供二层高可用性。在此种情况下， NISG-IPS 只支持主备模式部署，两端路由器需运行 OSPF 协议。当 NISG-IPS 完成主备选举后，备份设备会阻断路由器通过本设备的邻居建立过程。

14.1.2.2 设备的状态

设备在二层高可用性中有如下四种状态：

- Initialize：表示 VRRP 路由器处于未启用状态，或者处于初始状态，未参与选举。
- Negotiate：表示虚拟路由器正处于主备协商阶段。
- Master：表示该设备为主设备，拥有备份 IP 地址，并且负责转发数据包。
- Backup：处于 Backup 状态时，设备为备份设备，不转发数据包，仅负责监听主设备状态，主设备故障时，接替主设备工作。

14.1.2.3 主设备的选举

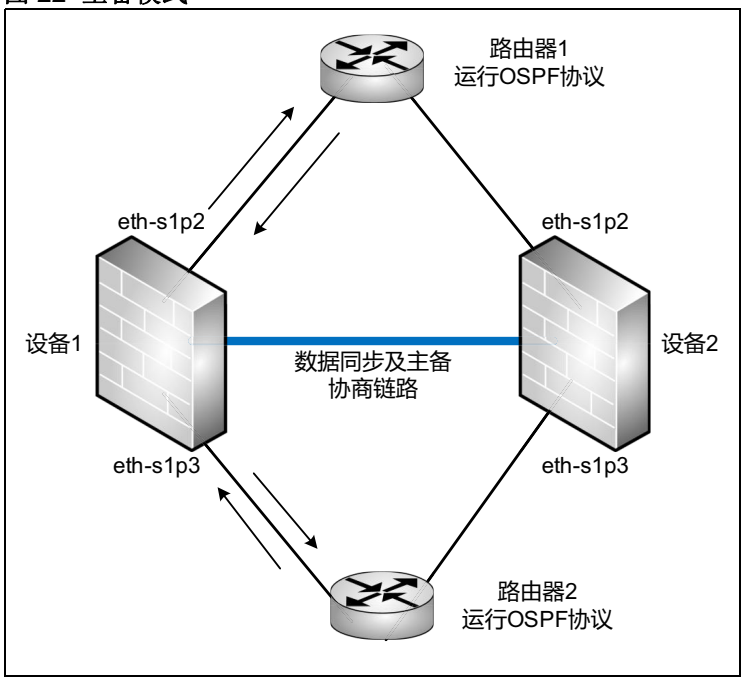
主设备的选举遵循以下原则：

1. 比较 VLAN 中启用的二层接口数量，数量多的为主设备。
2. 如果启用的二层接口数量相同，优先级高的为主设备。
3. 如果优先级相同，则比较 VLAN 的 IP 地址的大小， VLAN IP 地址大的为主设备。

14.1.2.4 部署模式

部署在二层时，仅支持主备模式部署，典型部署场景如图 22 所示。

图 22 主备模式



设备 1 和设备 2 中的 eth-s1p2 同时连接路由器 1，eth-s1p3 同时连接在路由器 2 上。每台设备的 eth-s1p2 和 eth-s1p3 都为二层物理接口并且处于同一 VLAN 之中。设备 1 和设备 2 通过数据同步链路进行协商，选举出主设备（设备 1）和备份设备（设备 2）。主设备允许路由器 1 和路由器 2 建立邻居关系。备份设备阻断路由器 1 和路由器 2 的 OSPF 报文，使其不能建立邻居关系。因此，在主备选举成功后，只有一条链路可转发数据。

14.1.3 NISG-IPS 的增强功能

增强功能仅在 NISG-IPS 部署在三层 HA 模式时可用。

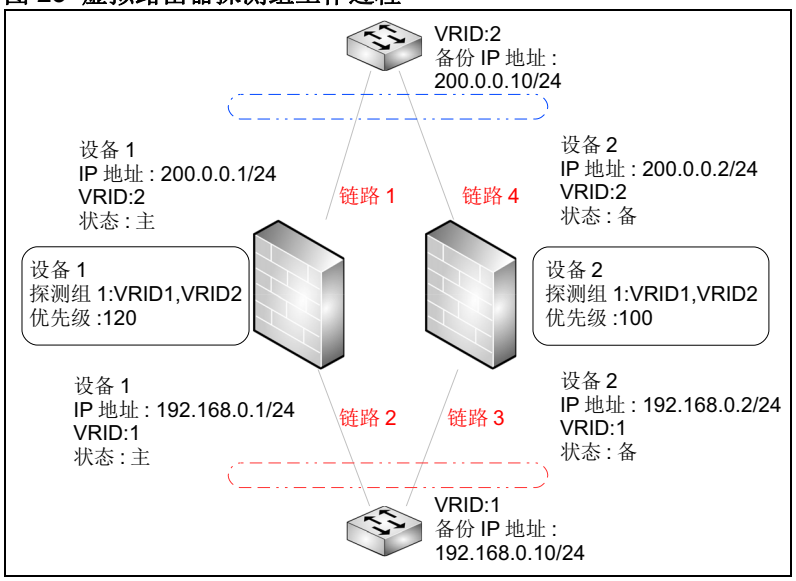
14.1.3.1 IP 探测

VRRP 协议无法感知链路故障， NISG-IPS 可以用 IP 探测来监控链路状态。您可以为每条链路配置不同的权重。如果探测失败次数达到阈值，则认为链路出现故障，系统会在 VRRP 路由器的优先级中减去相应的权重。优先级的变化可引起主设备的重新选举。此时的主备切换可避免因链路故障引起的网络中断。

14.1.3.2 虚拟路由器探测组

当有多个虚拟路由器关联同一组 VRRP 路由器时，需要确保在所有的虚拟路由器中主设备都为同一台 VRRP 路由器。如果主设备不为同一 VRRP 路由器，则会出现流量不通，连接故障的情况。图 23 中的例子将解释为什么您需要配置虚拟路由器探测组。

图 23 虚拟路由器探测组工作过程



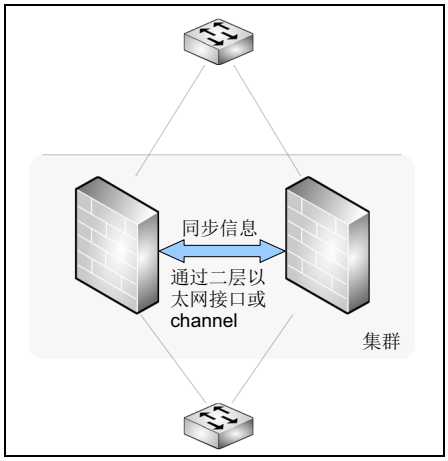
在上图的场景中，设备 1 在虚拟路由器 1 和虚拟路由器 2 中都为主设备。因此，数据包经过链路 1 和链路 2。当设备上连接链路 1 的接口因某种原因故障时，设备 1 在虚拟路由器 2 中的优先级会降低，系统进行主备切换。切换后，设备 2 成为虚拟路由器 2 的主设备。传入流量和传出流量不走同一设备，导致网络异常。

因此，需要使虚拟路由器的主设备都在同一 VRRP 路由器上，并且同时进行主备切换。NISG-IPS 提供虚拟路由器探测组实现此功能。您可在不同设备上为探测组配置不同的优先级，并为虚拟路由器配置权重。权重将影响探测组的优先级，如果虚拟路由器发生主备切换，则会在设备上 （上图设备 1）配置的探测组优先级中减去相应权重，这时如果减去权重后的优先级小于另一设备上 （上图设备 2）配置的优先级，则探测组中将触发主备切换，使所有虚拟路由器的主设备都切换到另一 VRRP 路由器上。

这样数据流量就会全部通过链路 3 和链路 4，流经设备 2。

14.1.4 集群

集群由两台 NISG-IPS 设备组成，两台设备之间进行配置信息和运行信息的同步。在发生故障切换时，新的主设备就已经获取原主设备的全部信息，可以保证业务不间断运行。



系统通过二层以太网接口或者二层以太网通道接口在两设备间同步信息。二层以太网通道口可增加同步的带宽，如果用户需要同步运行信息，因同步数据量较大，推荐使用二层以太网通道口同步。

在二层部署时，管理员必须创建集群，系统通过集群的同步接口同步数据及互发主备选举必须的协商包。系统通过 VLAN 接口做为数据转发接口，两台 NISG-IPS 设备各自的 VLAN 中至少包含两个二层以太网接口，两个二层接口分别与不同的路由器相连。

同步的信息包括：

- **系统时间**
- **系统配置。**有些配置信息不可同步，管理员需要进行手动配置。这些配置信息包括：
  - 主机名
  - 系统语言
  - 接口的配置 （Tunnel 接口除外）
  - Vsys 的配置

    当两台 NISG-IPS 设备分别存在名字相同的 Vsys 时，可以对 Vsys 内的配置信息和运行信息进行同步。
  - 虚拟网络的配置
  - STP 的配置
  - 管理用户的登录、退出、配置锁
  - 虚拟路由器的优先级、 IP 探测、选举接口和认证
  - 虚拟路由器探测组的优先级和 IP 探测
  - 集群配置
  - License 的相关操作
  - 标题信息 （Banner）的设置
  - 重启、关闭、恢复出厂设置的操作

- 技术支持
- 系统的备份和恢复
- 系统升级的配置和操作
- 日志的复制和删除
- 设置存储介质
- 显示的相关操作
- 导出的相关操作
- 查询的相关操作
- NTP 手动校时
- ISP 智能选路相关配置信息
- 动态路由相关配置信息

- **运行信息。**发生故障切换时，备份设备将接管主设备的所有工作，包括运行信息。

NISG-IPS 默认同步下列运行信息：

- UDP 会话 （53 端口除外）
- TCP 会话 （80 和 8080 端口除外）
- IPSec SAs
- NAT 资源
- ARP 表
- DHCP 地址分配信息
- WebAuth 用户认证状态
- VPN 用户连接状态
- VPN IP 地址池分配

14.2 基础配置步骤

本节描述了以下功能的基本配置：

14.2.1 配置虚拟路由器

配置过程中涉及的参数信息，请参见 14.3.1 虚拟路由器。

设备 1

1. 选择**系统** > **高可用性** > **虚拟路由器**。
2. 点击**新建**，配置选举接口和其他参数。
   - 选择二层模式部署。

   - 选择三层模式部署。

3. （可选）在三层接口上配置 IP 探测，探测链路的可达性。

- 添加两条针对相同接口和相同 IP 地址的探测条目，后一个条目会覆盖前一个。
- 最多能够配置 64 个 IP 探测条目。

4. 点击**确定**，点击。

设备 2

与设备 1 中配置方式相同，优先级请不要与设备 1 配置相同值。

表 249 配置虚拟路由器命令

virtual router *vr_id*	添加虚拟路由器或进入到虚拟路由器配置模式。
unset virtual router *vr_id*	删除当前指定的虚拟路由器。
election interface *interface_name*	设置虚拟路由器的选举接口。
unset election interface *interface_name*	删除虚拟路由器的选举接口。
priority *pri*	设置 VRRP 路由器在虚拟路由器中的优先级。
interval *interval_value*	设置主路由器向备份路由器发送报文的通告周期。
preempt {enable | disable}	启用或禁用抢占模式。
auth {enable password *auth_key* **| disable}**	启用或禁用同一虚拟路由器内 VRRP 路由器成员间的认证。
virtual-router {enable | disable}	启用或禁用虚拟路由器。
backup ip address *ipv4* **mask** *netmask*	添加虚拟路由器的备份 IP 地址。
unset backup ip address *ipv4*	删除虚拟路由器的备份 IP 地址。
ip-track	设置虚拟路由器的 IP 探测。
unset ip-track	删除虚拟路由器的 IP 探测。
show virtual-router {all | *vr_id***}**	显示虚拟路由器的配置信息。
vlan-linkage {enable | disable}	在选择二层时，启用或禁用接口联动功能。

14.2.2 配置虚拟路由器探测组

配置过程中涉及的参数信息，请参见 14.3.2 虚拟路由器探测组。

设备 1

1. 选择**系统 > 高可用性 > 虚拟路由器探测组**。
2. 点击新建，配置组 ID、优先级、通告周期和抢占模式。

提示：当您创建虚拟路由器探测组时，原虚拟路由器所配置的优先级、通告周期和抢占模式将被探测组配置的值所取代。原虚拟路由器中配置的 IP 探测也将失效，如有需要，需在探测组中重新配置 IP 探测。
虚拟路由器退出探测组后，该虚拟路由器的优先级、通告周期和抢占模式将恢复到原有的配置。

3. 添加虚拟路由器，并为其配置权重。

提示：系统需已有虚拟路由器，才可创建有效的虚拟路由器探测组。
探测权重应大于两个虚拟路由器的优先级的差值，否则无法触发切换。

4. (可选) 在三层接口上配置 IP 探测，探测链路的可达性。

5. 点击**确定**，点击。

设备 2

1. 选择**系统 > 高可用性 > 虚拟路由器探测组**。
2. 点击新建，配置组 ID、优先级、通告周期和抢占模式。

3. 添加虚拟路由器和权重。

4. （可选）在三层接口上配置 IP 探测，探测链路的可达性。

5. 点击**确定**，点击 。

表 250 配置虚拟路由器探测组命令

detection group *group_id*	创建探测组或进入到探测组配置模式。
unset detection group *group_id*	删除指定的探测组。
hold virtual-router weight	设置探测组成员。
unset hold virtual-router *vr_id*	从探测组中删除指定的虚拟路由器成员。
priority *pri*	设置探测组的优先级。
interval *interval_value*	设置探测组的通告周期。
preempt {enable | disable}	启用或禁用探测组的抢占模式。
ip-track	设置虚拟路由器的 IP 探测。
unset ip-track	删除探测组的 IP 探测。
show detection-group {all | *group_id*}	显示探测组的配置信息。

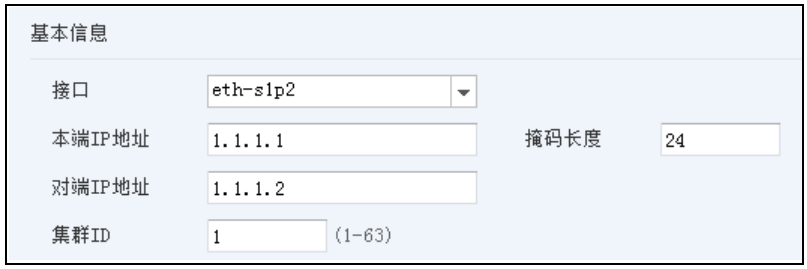
14.2.3 配置集群

配置过程中涉及的参数信息，请参见 14.3.3 集群。

使用 NISG-IPS 设备进行集群同步时，请确保设备的型号和软件版本相同。

设备 1

1. 选择**系统 > 高可用性 > 集群**。
2. 配置集群 ID、本端和对端 IP 地址、用于同步的二层以太网接口或以太网通道。



- 建议使用二层以太网接口同步配置信息，二层以太网通道同步运行信息。
- 本端和对端 IP 地址格式为 [1-223].[0-255].[0-255].[0-255]，不可以是 127.0.0.0-127.255.255.255 或 192.168.255.254。

3. 配置同步、加密和认证。

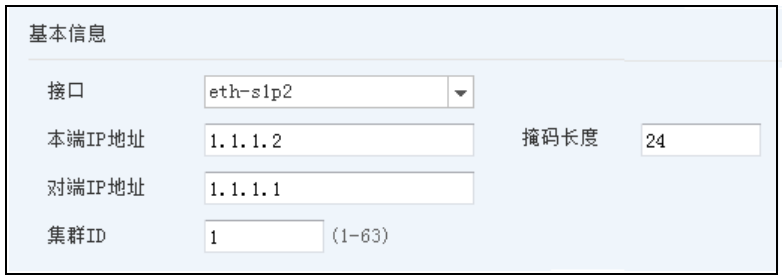
- **查看本地和对端设备信息的差异**：启用自动同步配置功能前，可以查看两台集群设备的配置差异。
- **立即同步**：在执行自动配置同步前，推荐先进行手动立即同步。手动同步能够同步所有配置信息，并覆盖现有配置。自动同步能够同步手动同步之后修改的配置信息，为增量同步，不覆盖原有配置信息。

- **将此时间设置应用到两端设备**：同一个集群内，只有一台设备可以设置为时间同步基准。
- **加密**：如果设备 1 和设备 2 通过交换设备相连，推荐开启加密功能。

4. 点击**确定**，点击。

设备 2

1. 选择**系统 > 高可用性 > 集群**。
2. 配置 IP 地址等内容。



3. 配置其余内容，除不勾选**将此时间设置应用到两端设备**选项外，与设备 1 一致。
4. 点击**确定**，点击。

表 251 配置集群命令

clusterid *cluster_id*	设置集群标识，将 NISG-IPS 设备加入到指定的集群中。
unset clusterid	将 NISG-IPS 设备从集群中删除。
local interface *interface_name*	设置集群设备本端的同步接口。
unset local interface	删除集群设备的本端同步接口。
local ip address *ipv4* **mask** *netmask*	设置集群设备本端同步接口的 IP 地址。
peer ip address *ipv4*	设置集群设备对端同步接口的 IP 地址。
config check	检验集群内设备配置信息的一致性。
config sync	手动同步配置信息到对端设备。
config sync auto {enable | disable}	启用或禁用自动同步配置信息功能。
rti sync {enable | disable}	启用或禁用自动同步运行信息功能。
rti session default	设置同步默认的会话信息。
rti session {tcp | udp | other}	添加要进行同步的自定义会话信息。
unset rti session {tcp | udp | other}	删除要进行同步的自定义会话信息。
time sync {enable | disable}	启用或禁用自动同步系统时间功能。
time boot {on | off}	设置当 NISG-IPS 启动时，是否立即同步系统时间。
time daily {*time_sync* **| off}**	设置每日同步系统时间。
time benchmark {on | off}	设置当前 NISG-IPS 为系统时间同步基准。
time modified {on | off}	设置 NISG-IPS 系统时间更改时，是否立即同步系统时间。
encrypt {enable password *enc_key* **| disable}**	启用或禁用同一集群内设备间的同步信息加密功能。
auth {enable | disable}	启用或禁用集群内设备间的认证。
show cluster	显示集群配置信息。

14.3 配置参数说明

本节介绍以下配置参数信息：

14.3.1 虚拟路由器

管理员可以在根系统和 Vsys 中配置虚拟路由器。

表 252 虚拟路由器的配置信息

配置信息	说明
VRID	虚拟路由器的唯一标识，取值范围是 1 ～ 255 的整数。 管理员也可以点击**自动生成 VRID** 按钮，由系统自动生成一个唯一的 VRID 值。 当部署二层 HA 时， VRID 为 241 ～ 255。 当部署三层 HA 时， VRID 为 1 ～ 240。
模式	选择系统部署模式，可选择二层或者三层。
描述	虚拟路由器的描述信息，为 0 ～ 255 字节 UTF-8 字符，不包含：?'\"<>&。
接口	指转发流量的接口，包括三层和三层共享以太网接口、三层和三层共享以太网通道、 VLAN 接口。其中，三层共享接口应用在 Vsys 中。
组名	指虚拟路由器所属的探测组的 ID，仅在部署在三层时使用。
优先级	虚拟路由器的优先级，取值范围是 1 ～ 254 的整数。
通告周期	指虚拟路由器中的主设备发送报文的时间间隔。同一虚拟路由器中的 VRRP 路由器，其通告周期必须相同。 通告周期取值范围为 1 ～ 60，单位秒。
抢占模式	指拥有较高优先级的备份设备是否抢占当前低优先级的主设备而成为新的主设备。IP 地址所有者永远处于抢占模式。 当部署在二层模式时，必须为启用状态，不可配置。
认证	指对虚拟路由器内成员之间 VRRP 报文和通讯数据采用简单的明文方式的认证。 认证信息为 1-8 字节 UTF-8 字符，不包含问号和空格。 两台成员设备之间需要配置相同的认证信息。 仅在部署在三层时可用。
启用该虚拟路由器	当前 NISG-IPS 设备是否参与虚拟路由器的选举过程，勾选表示参与。
备份 IP 地址	指虚拟路由器所备份的 IP 地址，可以是一个或多个。一个虚拟路由器最多支持 255 个备份 IP 地址。 正被 VPN 隧道引用的备份 IP 地址及其对应的虚拟路由器不可以被删除。 仅在部署在三层时可用。

表 252 虚拟路由器的配置信息 (*续*)

配置信息	说明
IP 探测	探测某个 IP 地址是否可达。管理员需指定以下配置选项： • **类型**：探测探测，包括： •**ARP Ping**：向处于同一个局域网的主机发送 ARP 请求。 •**Ping**：向目的 IP 地址发送 ICMP 回送 （Echo）请求，并监听 ICMP 应答 （Reply）报文。 •**TCP Ping**：使用 TCP 协议探测 IP 地址。 • **接口**：指定用哪个接口发送探测报文进行 IP 探测。管理员可以选择： •**Any**：表示通过查询路由决定探测所使用的接口。 • **指定接口**：任何三层或三层共享以太网接口、三层或三层共享以太网通道、 VLAN 接口。 •**IP 地址**：要探测的目的 IP 地址，即探测此 IP 地址是否可达。 • **探测端口**：使用 TCP Ping 方式需要指明探测端口，取值范围为 1 ～ 65535。 • **探测周期**：指定每隔多久发一个探测报文。取值范围为 1 ～ 30000 秒。 • **探测重试次数**：指定连续重试的次数。超过该值就认为发生了故障。取值范围为 1 ～ 999。 • **权重**：当 IP 探测失败后，虚拟路由器的优先级将减去该权重。取值范围为 1 ～ 254 之间的整数。 仅在部署在三层时可用。
状态	指 NISG-IPS 设备在虚拟路由器中的状态。 当部署二层高可用性时，分为四种：Initialize、 Negotiate、 Master、 Backup。 当部署三层高可用性时，分为三种：Initialize、 Master、 Backup。
启动接口联动	仅在部署在二层时可见。 当开启此功能，当 VLAN 中有一个接口故障，其余接口将自动关闭。

14.3.2 虚拟路由器探测组

管理员可以在根系统和 Vsys 中配置虚拟路由器探测组。该功能仅当系统部署在三层时使用。

表 253 虚拟路由器探测组的配置信息

配置信息	说明
组 ID	标识虚拟路由器探测组。取值范围是 1 ～ 255 的整数。
描述	虚拟路由器探测组的描述信息，为 0 ～ 255 个字节的 UTF-8 字符。不包含：?'\"<>&。
优先级	探测组的优先级。取值范围是 1 ～ 254 的整数。
通告周期	虚拟路由器探测组发送报文的时间间隔。取值范围为 1 ～ 60 秒。
抢占模式	表示高优先级的探测组是否抢占低优先级的探测组。
成员	指该探测组中所包含的虚拟路由器，一个虚拟路由器只能加入一个探测组。
权重	当 IP 探测失败后，探测组的优先级将减去该虚拟路由器权重。取值范围是 1 ～ 254 的整数。

表 253 虚拟路由器探测组的配置信息 (*续*)

配置信息	说明
IP 探测	探测某个 IP 地址是否可达。管理员需指定以下配置选项： • **类型**：探测探测，包括： **•ARP Ping**：向处于同一个局域网的主机发送 ARP 请求。 **•Ping**：向目的 IP 地址发送 ICMP 回送 （Echo）请求，并监听 ICMP 应答 （Reply）报文。 **•TCP Ping**：使用 TCP 协议探测 IP 地址。 • **接口**：指定用哪个接口发送探测报文进行 IP 探测。管理员可以选择： **•Any—** 表示通过查询路由决定探测所使用的接口。 • **指定接口 —** 任何三层或三层共享以太网接口、三层或三层共享以太网通道、VLAN 接口。 **•IP 地址**：要探测的目的 IP 地址，即探测此 IP 地址是否可达。 • **探测端口**：使用 TCP Ping 方式需要指明探测端口，取值范围为 1 ～ 65535。 • **探测周期**：指定每隔多久发一个探测报文。取值范围为 1 ～ 30000 秒。 • **探测重试次数**：指定连续重试的次数。超过该值就认为发生了故障。取值范围为 1 ～ 999。 • **权重**：当 IP 探测失败后，虚拟路由器的优先级将减去该权重。取值范围为 1 ～ 254 之间的整数。
状态	探测组内虚拟路由器成员的状态，包括三种：Initialize、 Master、 Backup。

14.3.3 集群

管理员只能在根系统中配置集群。

表 254 集群的配置信息

配置信息	说明
接口	HA 接口，即同步数据使用的接口。当部署二层 HA 时，该接口也通过主备协商包。可以是任何一个未被使用的二层以太网接口和二层以太网通道。
本端 IP 地址	本端同步接口的 IP 地址及相应的掩码长度。
对端 IP 地址	对端同步接口的 IP 地址。
集群 ID	标识所属的集群。 ID 范围：1 ～ 63。 集群成员必须具有相同的集群 ID。
配置同步	手动或自动同步配置信息，使集群内各成员配置保持一致。 在执行配置同步前，管理员可以点击**查看本地和对端设备信息的差异**按钮，查看两端配置信息的差异。
运行信息同步	自动同步运行信息，使集群内各成员运行信息保持一致。开启后，可以勾选**自定义会话信息**复选框，对要同步的会话信息进行自定义设置。
系统时间同步	同步系统时间，使集群内所有成员的时间保持一致。
加密	对集群中的同步数据进行加密。两端设备都需要配置相同的加密密码。 密码为 1-255 字节的 UTF-8 字符，不包含问号和空格。
认证	验证集群中本端和对端设备的身份。两端设备都需要配置相同的认证密码。 密码为 1-255 字节的 UTF-8 字符，不包含问号和空格。

14.4HA 范例

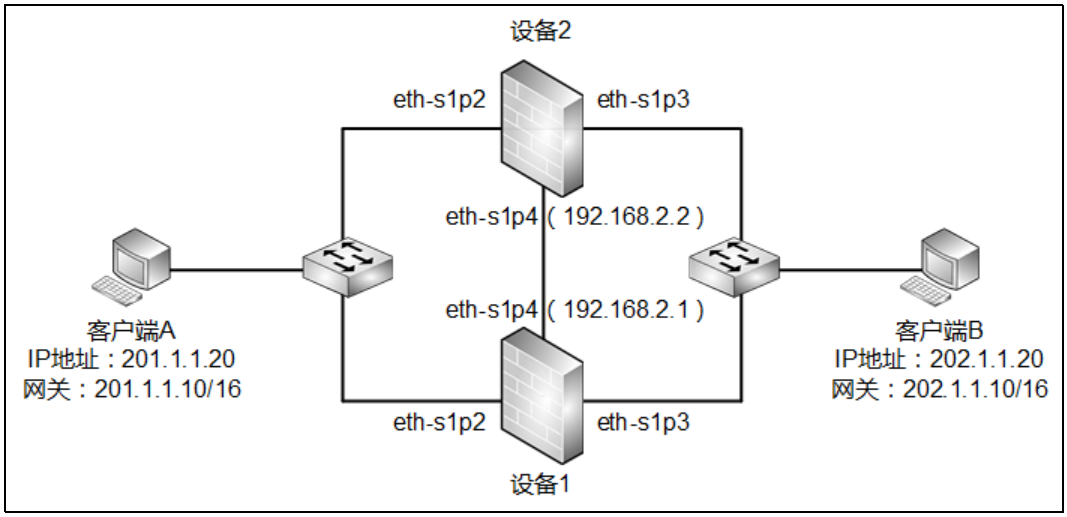
14.4.1 范例：三层主备模式部署

基本需求

某公司网络出口处部署 NISG-IPS 设备，因出口处位置关键，如设备故障，直接影响公司内部全部员工的工作，造成经济损失，威胁网络安全。

- 公司决定以主备形式部署 NISG-IPS 设备。
- 使用 IP 探测功能，防止外部不被公司控制的网络环境中断，给公司带来影响。
- 通过虚拟路由器组防止单个虚拟路由器主备切换导致网络中断。

组网拓扑



本文以 201.1.0.0/16 网段做为内网， 202.1.0.0/16 网段做为外网举例。

配置要点

- 配置访问策略。
- 配置虚拟路由器。
- 配置虚拟路由器探测组，其中包括虚拟路由器探测组的权重， IP 探测等信息。
- 配置集群。

配置步骤

配置访问策略

设备 1

1. 选择**防火墙** > **访问策略**，点击**新建**。

   名称 =access1，源安全域 = 任意，源 IP=201.1.0.0/16，目的安全域 = 任意，目的 IP/域名 =202.1.0.0/16，服务 = 任意，动作 = 允许。

2. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access access1 any 201.1.0.0/16 any
202.1.0.0/16 any any permit enable
NetEye@root-system] exit
```

配置虚拟路由器

设备 1

1. 选择**系统** > **高可用性** > **虚拟路由器**。
2. 点击**新建**，进行如下配置。

提示：如果配置虚拟路由器探测组，单个虚拟路由器的优先级、通告周期和抢占模式的设置将被虚拟路由器探测组取代。

   VRID=1，接口 =eth-s1p2，优先级 =100，通告周期 =1，抢占模式 = 启用， VR= 启用，备份 IP=201.1.1.10/16。

3. 点击**确定**。
4. 点击**新建**，进行如下配置。

   VRID=2，接口 =eth-s1p3，优先级 =100，通告周期 =1，抢占模式 = 启用， VR= 启用，备份 IP=202.1.1.10/16。

5. 点击**确定**。

设备 2

6. 创建新的 VR。VRID=1，接口 =eth-s1p2，优先级 =100，通告周期 =1，抢占模式 = 启用， VR= 启用，备份 IP=201.1.1.10/16。
7. 创建新的 VR。VRID=2，接口 =eth-s1p3，优先级 =100，通告周期 =1，抢占模式 = 启用， VR= 启用，备份 IP=202.1.1.10/16。

CLI

设备 1

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] backup ip address 201.1.1.10 mask 255.255.0.0
NetEye@root-system-vr1] election interface eth-s1p2
```

```
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] exit
NetEye@root-system] virtual router 2
NetEye@root-system-vr2] backup ip address 202.1.1.10 mask 255.255.0.0
NetEye@root-system-vr2] election interface eth-s1p3
NetEye@root-system-vr2] virtual-router enable
NetEye@root-system-vr2] exit
```

设备 2

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] backup ip address 201.1.1.10 mask 255.255.0.0
NetEye@root-system-vr1] election interface eth-s1p2
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] exit
NetEye@root-system] virtual router 2
NetEye@root-system-vr2] backup ip address 202.1.1.10 mask 255.255.0.0
NetEye@root-system-vr2] election interface eth-s1p3
NetEye@root-system-vr2] virtual-router enable
NetEye@root-system-vr2] exit
```

配置虚拟路由器探测组

设备 1

1. 选择**系统** > **高可用性** > **虚拟路由器探测组**。
2. 点击**新建**，进行如下配置。

提示：在两个设备上建立的虚拟路由器探测组优先级的差值需小于虚拟路由器的权重值。如本举例中在设备 1 上的优先级为 120，在设备 2 上的优先级为 110，两值差为 10，小于为虚拟路由器设置的权重值 20。如果这个值大于或等于权重值，如某虚拟路由器故障，虚拟路由器探测组优先级变化后，不能触发重新选举，导致网络故障。

- 组 ID=1，优先级 =120，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID1（权重 =20） +VRID2 （权重 =20）；
- IP 探测类型 =Ping，接口 =Any，IP 地址 =202.1.1.20，通告周期 =3，探测重试次数 =3，权重 =20。

3. 点击**确定**。

设备 2

4. 创建新的 VRDG。组 ID=1，优先级 =110，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID1 （权重 =20） +VRID2 （权重 =20）。 IP 探测配置与设备 1 相同。

CLI

设备 1

```
NetEye@root-system] detection group 1

NetEye@root-system-dg1] hold virtual-router 1 weight 20

NetEye@root-system-dg1] hold virtual-router 2 weight 20

NetEye@root-system-dg1] priority 120
```

```
NetEye@root-system-dg1] ip-track type ping interface any ip 202.1.1.20
interval 3 threshold 3 weight 20
NetEye@root-system-dg1] exit
```

设备 2

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] hold virtual-router 1 weight 20
NetEye@root-system-dg1] hold virtual-router 2 weight 20
NetEye@root-system-dg1] priority 110
NetEye@root-system-dg1] ip-track type ping interface any ip 202.1.1.20
interval 3 threshold 3 weight 20
NetEye@root-system-dg1] exit
```

配置集群

设备 1

1. 选择**系统** > **高可用性** > **集群**，设置集群。

   接口 =eth-s1p4，本端 IP=192.168.2.1/24，对端 IP=192.168.2.2，集群 ID=1。

提示：HA 同步接口使用二层以太网接口或以太网通道。当同步需要同步运行信息时，由于数据量较大，建议使用以太网通道，以太网通道不仅可以增大带宽，还可以提高接口可靠性。

---

2. （可选）点击**查看本地和对端设备信息的差异**，查看两端配置是否有差异。如果有差异，点击**立即同步**，设备 1 的配置信息将同步到设备 2，保持配置一致。
3. 点击**自动同步配置信息**对应的**开启**按钮，设备 1 上的实时配置变化将被同步到设备 2。当设备 2 也启用了该项功能，则任意一端的配置变化将导致两台设备彼此之间进行自动同步。
4. 点击**自动同步运行信息**对应的**开启**按钮，则设备 1 上的默认运行信息将被同步到设备 2 上。当设备 2 也开启了该项功能时，两端设备将互相同步默认运行信息。
5. 勾选**自定义会话信息**，可以通过指定协议类型和对应端口来自定义所要同步的会话。
6. 点击**自动同步系统时间**所对应的开启按钮。
7. 勾选**当设备启动时**，并勾选**将此时间设置应用到两端设备**。当设备 1 启动时，其系统时间将自动同步到设备 2。
8. 点击确定，点击 。

设备 2

9. 创建集群。接口 =eth-s1p4，本端 IP=192.168.2.2/24，对端 IP=192.168.2.1，集群 ID=1。
10. 配置同步，开启**自动同步配置信息 / 运行信息 / 系统时间**。勾选**自定义会话信息**，并与设备 1 配置相同的会话信息。

CLI

设备 1

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth-s1p4
NetEye@root-system-cluster] local ip address 192.168.2.1 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 192.168.2.2
NetEye@root-system-cluster] config check
NetEye@root-system-cluster] config sync
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] rti session tcp 21-221
NetEye@root-system-cluster] rti session udp 33-333
NetEye@root-system-cluster] rti session other 6-60
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] time benchmark on
NetEye@root-system-cluster] end
NetEye@root> save config
```

设备 2

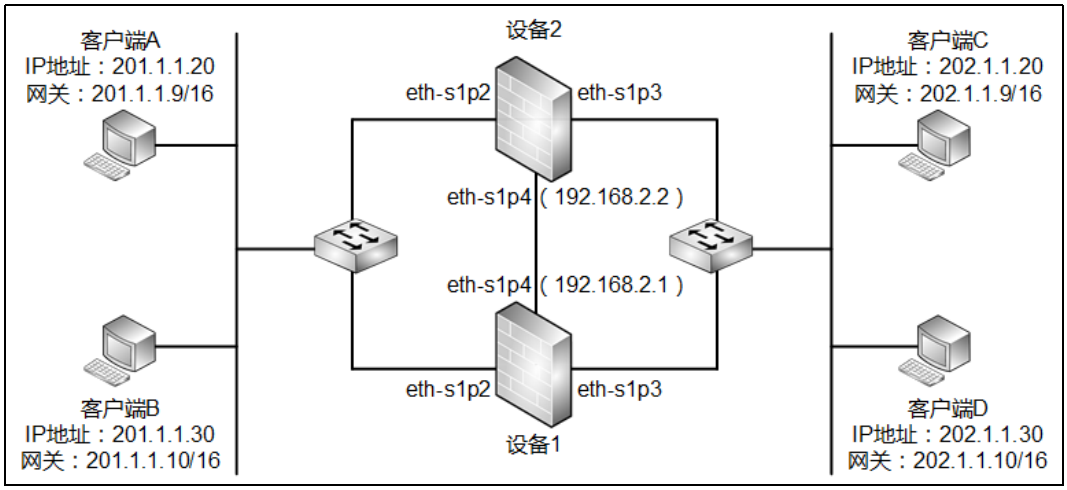
```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth-s1p4
NetEye@root-system-cluster] local ip address 192.168.2.2 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 192.168.2.1
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] rti session tcp 21-221
NetEye@root-system-cluster] rti session udp 33-333
NetEye@root-system-cluster] rti session other 6-60
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] end
NetEye@root> save config
```

14.4.2 范例：三层主主模式部署

基本需求

某公司网络出口处部署 NISG-IPS 设备，因出口处位置关键，如设备故障，直接影响公司内部全部员工的工作，需进行高可用性部署，公司决定以主主形式部署 NISG-IPS 设备，确保出口网络不中断。并通过虚拟路由器组防止单个虚拟路由器主备切换导致网络中断。

组网拓扑



配置要点

- 配置访问策略。
- 配置虚拟路由器。
- 配置虚拟路由器探测组。
- 配置集群。

配置步骤

配置访问策略

设备 1

1. 选择**防火墙** > **访问策略**，点击**新建**。

   名称 =access1，源安全域 = 任意，源 IP=201.1.0.0/16，目的安全域 = 任意，目的 IP/域名 =202.1.0.0/16，服务 = 任意，动作 = 允许。

2. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access access1 any 201.1.0.0/16 any
202.1.0.0/16 any any permit enable
NetEye@root-system] exit
```

配置虚拟路由器

设备 1

1. 选择**系统** > **高可用性** > **虚拟路由器**。
2. 点击**新建**，进行如下配置。

提示：如果配置虚拟路由器探测组，单个虚拟路由器的优先级、通告周期和抢占模式的设置将被虚拟路由器探测组取代。

VRID=1，接口 =eth-s1p2，优先级 =100，通告周期 =1，抢占模式 = 启用， VR= 启用，备份 IP=201.1.1.9/16。

3. 点击**确定**。
4. 根据上述方式配置如下虚拟路由器：
   - 创建新的虚拟路由器。 VRID=2，接口 =eth-s1p2，优先级 =100，通告周期 =1，抢占模式 = 启用， VR= 启用，备份 IP=201.1.1.10/16。
   - 创建新的虚拟路由器。 VRID=3，接口 =eth-s1p3，优先级 =100，通告周期 =1，抢占模式 = 启用， VR= 启用，备份 IP=202.1.1.9/16。
   - 创建新的虚拟路由器。 VRID=4，接口 =eth-s1p3，优先级 =100，通告周期 =1，抢占模式 = 启用， VR= 启用，备份 IP=202.1.1.10/16。

设备 2

配置与设备 1 完全相同。

CLI

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] backup ip address 201.1.1.9 mask 255.255.0.0
NetEye@root-system-vr1] election interface eth-s1p2
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] exit
NetEye@root-system] virtual router 2
NetEye@root-system-vr2] backup ip address 201.1.1.10 mask 255.255.0.0
NetEye@root-system-vr2] election interface eth-s1p2
NetEye@root-system-vr2] virtual-router enable
NetEye@root-system-vr2] exit
NetEye@root-system] virtual router 3
NetEye@root-system-vr3] backup ip address 202.1.1.9 mask 255.255.0.0
NetEye@root-system-vr3] election interface eth-s1p3
NetEye@root-system-vr3] virtual-router enable
NetEye@root-system-vr3] exit
NetEye@root-system] virtual router 4
NetEye@root-system-vr4] backup ip address 202.1.1.10 mask 255.255.0.0
NetEye@root-system-vr4] election interface eth-s1p3
NetEye@root-system-vr4] virtual-router enable
NetEye@root-system-vr4] exit
```

设备 2

配置与设备 1 完全相同。

配置虚拟路由器探测组

设备 1

1. 选择**系统** > **高可用性** > **虚拟路由器探测组**。
2. 点击**新建**，配置虚拟路由器探测组 1。

提示：在两个设备上建立的虚拟路由器探测组优先级的差值需小于虚拟路由器的权重值。

组 ID=1，优先级 =100，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID1 （权重 =10） +VRID3 （权重 =10）。

3. 点击**确定**。
4. 再次点击**新建**，配置虚拟路由器探测组 2。

组 ID=2，优先级 =95，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID2 （权重 =10） +VRID4 （权重 =10）。

5. 点击**确定**。

设备 2

1. 选择**系统** > **高可用性** > **虚拟路由器探测组**。
2. 点击**新建**，配置虚拟路由器探测组 1。

组 ID=1，优先级 =95，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID1 （权重 =10） +VRID3 （权重 =10）。

3. 点击**确定**。
4. 再次点击**新建**，配置虚拟路由器探测组 2。

组 ID=2，优先级 =100，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID2 （权重 =10） +VRID4 （权重 =10）。

5. 点击**确定**。

CLI

设备 1

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] hold virtual-router 1 weight 10
NetEye@root-system-dg1] hold virtual-router 3 weight 10
NetEye@root-system-dg1] priority 100
NetEye@root-system-dg1] exit
NetEye@root-system] detection group 2
NetEye@root-system-dg2] hold virtual-router 2 weight 10
NetEye@root-system-dg2] hold virtual-router 4 weight 10
NetEye@root-system-dg2] priority 95
NetEye@root-system-dg2] exit
```

设备 2

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] hold virtual-router 1 weight 10
NetEye@root-system-dg1] hold virtual-router 3 weight 10
NetEye@root-system-dg1] priority 95
NetEye@root-system-dg1] exit
NetEye@root-system] detection group 2
NetEye@root-system-dg2] hold virtual-router 2 weight 10
NetEye@root-system-dg2] hold virtual-router 4 weight 10
NetEye@root-system-dg2] priority 100
NetEye@root-system-dg2] exit
```

配置集群

设备 1

1. 选择**系统** > **高可用性** > **集群**，设置集群。

   接口 =eth-s1p4，本端 IP=192.168.2.1/24，对端 IP=192.168.2.2，集群 ID=1。

提示：HA 同步接口使用二层以太网接口或以太网通道。当同步需要同步运行信息时，由于数据量较大，建议使用以太网通道，以太网通道不仅可以增大带宽，还可以提高接口可靠性。

---

2. （可选）点击**查看本地和对端设备信息的差异**，查看两端配置是否有差异。如果有差异，点击**立即同步**，设备 1 的配置信息将同步到设备 2，保持配置一致。
3. 点击**自动同步配置信息**对应的**开启**按钮，设备1上的实时配置变化将被同步到设备2。当设备 2 也启用了该项功能，则任意一端的配置变化将导致两台设备彼此之间进行自动同步。
4. 点击**自动同步运行信息**对应的**开启**按钮，则设备 1 上的默认运行信息将被同步到设备 2 上。当设备 2 也开启了该项功能时，两端设备将互相同步默认运行信息。
5. 勾选**自定义会话信息**，可以通过指定协议类型和对应端口来自定义所要同步的会话。
6. 点击**自动同步系统时间**所对应的开启按钮。
7. 勾选**当设备启动时**，并勾选**将此时间设置应用到两端设备**。当设备 1 启动时，其系统时间将自动同步到设备 2。
8. 点击确定，点击 。

设备 2

9. 创建集群。接口 =eth-s1p4，本端 IP=192.168.2.2/24，对端 IP=192.168.2.1，集群 ID=1。
10. 配置同步，开启**自动同步配置信息 / 运行信息 / 系统时间**。勾选**自定义会话信息**，并与设备 1 配置相同的会话信息。

CLI

设备 1

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth-s1p4
NetEye@root-system-cluster] local ip address 192.168.2.1 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 192.168.2.2
NetEye@root-system-cluster] config check
NetEye@root-system-cluster] config sync
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] rti session tcp 21-221
NetEye@root-system-cluster] rti session udp 33-333
NetEye@root-system-cluster] rti session other 6-60
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] time benchmark on
NetEye@root-system-cluster] end
NetEye@root> save config
```

设备 2

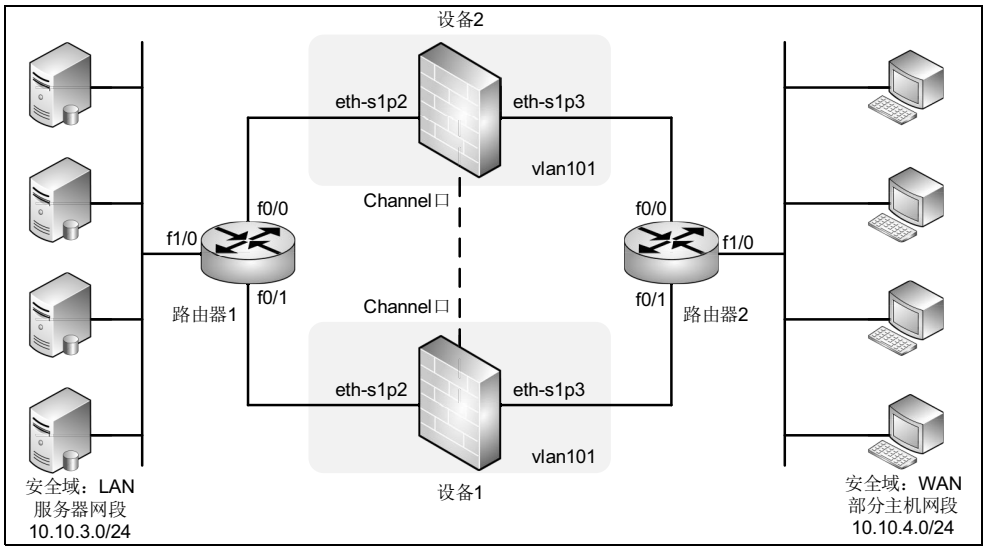
```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth-s1p4
NetEye@root-system-cluster] local ip address 192.168.2.2 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 192.168.2.1
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] rti session tcp 21-221
NetEye@root-system-cluster] rti session udp 33-333
NetEye@root-system-cluster] rti session other 6-60
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] end
NetEye@root> save config
```

14.4.3 范例：二层主备模式部署

基本需求

某公司要对数据中心进行安全保护，且由于数据中心十分重要，不允许出现服务长时间中断的情况。公司原网络拓扑中为两条链路连接的两台路由器，为不改变原有拓扑和编址规划，公司决定在通过二层方式部署 NISG-IPS 设备，对内部数据中心服务器进行保护，并且采取高可用性组网，保证网络服务的连贯性。

组网拓扑



配置要点

- 配置路由器
- 配置接口
- 配置安全域
- 配置策略
- 配置虚拟路由器
- 配置集群

配置步骤

配置路由器

需确保两台与 NISG-IPS 设备连接的路由器都在运行 OSPF 协议，具体配置步骤，请参照路由器的产品文档，本文以思科路由器为例进行说明。

路由器 1

```
Router> enable
Router# config terminal
Router(config)# interface fastEthernet 0/0
```

```
Router(config-if)# ip address 10.10.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface fastEthernet 0/1
Router(config-if)# ip address 10.10.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface fastEthernet 1/0
Router(config-if)# ip address 10.10.3.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router ospf 100
Router(config-router)# network 10.10.1.0 0.0.0.255 area 0
Router(config-router)# network 10.10.2.0 0.0.0.255 area 0
Router(config-router)# network 10.10.3.0 0.0.0.255 area 0
Router(config-router)# end
Router# write
```

路由器 2

```
Router> enable
Router# config terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# ip address 10.10.1.2 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface fastEthernet 0/1
Router(config-if)# ip address 10.10.2.2 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface fastEthernet 1/0
Router(config-if)# ip address 10.10.4.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router ospf 200
Router(config-router)# network 10.10.1.0 0.0.0.255 area 0
Router(config-router)# network 10.10.2.0 0.0.0.255 area 0
Router(config-router)# network 10.10.4.0 0.0.0.255 area 0
Router(config-router)# end
Router# write
```

配置接口

设备 1

1. 选择**网络 > 接口**。
2. 点击**新建**，在下拉框中选择 **VLAN**。
3. 在弹出的对话框中输入编号 101，点击**确定**。
4. 点击 vlan101 对应的 图标，将二层接口 （eth-s1p2 和 eth-s1p3）划入到 vlan101 中。
5. 点击**确定**。
6. 点击**新建**，在下拉框中选择 **Channel**。
7. 在弹出的对话框中输入编号 1，点击**确定**。
8. 点击新建的 ch1 对应的 图标，将二层接口 （eth-s1p4 和 eth-s1p5）划入到 ch1。
9. 点击**确定**。

设备 2

配置方式同设备 1，参数如下：

- 创建 vlan101，将 eth-s1p2 和 eth-s1p3 划入 vlan101。
- 创建 Channel 1，将 eth-s1p4 和 eth-s1p5 划入 Channel 1 中。

CLI

设备 1

```
NetEye@root> configure mode override
NetEye@root-system] vlan 101
NetEye@root-system-vlan101] hold ethernet s1p2
NetEye@root-system-vlan101] hold ethernet s1p3
NetEye@root-system-vlan101] exit
NetEye@root-system] channel 1
NetEye@root-system-if-ch1] hold ethernet s1p4
NetEye@root-system-if-ch1] hold ethernet s1p5
NetEye@root-system-if-ch1] end
NetEye@root> save config
```

设备 2

```
NetEye@root> configure mode override
NetEye@root-system] vlan 101
NetEye@root-system-vlan101] hold ethernet s1p2
NetEye@root-system-vlan101] hold ethernet s1p3
NetEye@root-system-vlan101] exit
NetEye@root-system] channel 1
NetEye@root-system-if-ch1] hold ethernet s1p4
```

```
NetEye@root-system-if-ch1] hold ethernet s1p5
NetEye@root-system-if-ch1] end
NetEye@root> save config
```

配置安全域

设备 1

1. 选择**网络 > 安全域**。
2. 新建安全域 lan 和 wan，并分配接口。
   - 名称 =wan，类型 = 基于二层接口 （vlan101），接口 =eth-s1p3 ；
   - 名称 =lan，类型 = 基于二层接口 （vlan101），接口 =eth-s1p2。

设备 2

配置与设备 1 相同。

CLI

设备 1

```
NetEye@root> configure mode override
NetEye@root-system] zone wan
NetEye@root-system] zone wan based-layer2 vlan 101 eth-s1p3
NetEye@root-system] zone lan
NetEye@root-system] zone lan based-layer2 vlan 101 eth-s1p2
NetEye@root-system] end
NetEye@root> save config
```

设备 2

配置与设备 1 相同。

配置策略

设备 1

1. 选择**防火墙 > 访问策略**。
2. 新建策略：

   名称 =allow，源安全域 =wan，源 IP=10.10.4.0/24，目的安全域 = 任意，目的 IP/域名 =10.10.3.0/24，服务 = 任意，动作 = 允许。
3. 因 OSPF 协议运行中需要有多播包通过 NISG-IPS 设备，所以需配置多播策略。

   选择**防火墙 > 多播策略**。
4. 新建策略：

   名称 =allow，源安全域 =Any，源 IP= 任意，多播组 IP=224.0.0.5， 224.0.0.6/24，允许的安全域 =Any。

设备 2

配置与设备 1 相同。

CLI

设备 1

```
NetEye@root> configure mode override
NetEye@root-system] policy access allow wan 10.10.4.0/24 lan
10.10.3.0/24 any any permit enable
NetEye@root-system] policy multicast allow any any 224.0.0.5,224.0.0.6
any enable
NetEye@root-system] end
NetEye@root> save config
```

设备 2

配置与设备 1 相同。

配置虚拟路由器

设备 1

1. 选择**系统 > 高可用性 > 虚拟路由器**。
2. 点击**新建**，进行如下配置：

   VRID=241，接口 =vlan101，优先级 =100，通告周期 =1，抢占模式 = 启用， VR= 启用，接口联动 = 启用。
3. 点击**确定**。

设备 2

1. 选择**系统 > 高可用性 > 虚拟路由器**。
2. 点击**新建**，进行如下配置。

   VRID=241，接口 =vlan101，优先级 =95，通告周期 =1，抢占模式 = 启用， VR= 启用，接口联动 = 启用。
3. 点击**确定**。

CLI

设备 1

```
NetEye@root> configure mode override
NetEye@root-system] virtual router 241
NetEye@root-system-vr241] election interface vlan101
NetEye@root-system-vr241] virtual-router enable
NetEye@root-system-vr241] vlan_linkage enable
NetEye@root-system-vr241] priority 100
NetEye@root-system-vr241] end
NetEye@root> save config
```

设备 2

```
NetEye@root> configure mode override
NetEye@root-system] virtual router 241
NetEye@root-system-vr241] election interface vlan101
NetEye@root-system-vr241] virtual-router enable
NetEye@root-system-vr241] vlan_linkage enable
NetEye@root-system-vr241] priority 95
NetEye@root-system-vr241] end
NetEye@root> save config
```

配置集群

设备 1

1. 选择**系统** > **高可用性** > **集群**，设置集群。

   接口 =ch1，本端 IP=192.168.2.1/24，对端 IP=192.168.2.2，集群 ID=1。

提示：HA 同步接口使用二层以太网接口或以太网通道。当同步需要同步运行信息时，由于数据量较大，建议使用以太网通道，以太网通道不仅可以增大带宽，还可以提高接口可靠性。

---

2. （可选）点击**查看本地和对端设备信息的差异**，查看两端配置是否有差异。如果有差异，点击**立即同步**，设备 1 的配置信息将同步到设备 2，保持配置一致。
3. 点击**自动同步配置信息**对应的**开启**按钮，设备1上的实时配置变化将被同步到设备2。当设备 2 也启用了该项功能，则任意一端的配置变化将导致两台设备彼此之间进行自动同步。
4. 点击**自动同步运行信息**对应的**开启**按钮，则设备 1 上的默认运行信息将被同步到设备 2 上。当设备 2 也开启了该项功能时，两端设备将互相同步默认运行信息。
5. 勾选**自定义会话信息**，可以通过指定协议类型和对应端口来自定义所要同步的会话。
6. 点击**自动同步系统时间**所对应的开启按钮。
7. 勾选**当设备启动时**，并勾选**将此时间设置应用到两端设备**。当设备 1 启动时，其系统时间将自动同步到设备 2。
8. 点击确定，点击 。

设备 2

9. 创建集群。接口 =ch1，本端 IP=192.168.2.2/24，对端 IP=192.168.2.1，集群 ID=1。
10. 配置同步，开启**自动同步配置信息 / 运行信息 / 系统时间**。勾选**自定义会话信息**，并与设备 1 配置相同的会话信息。

CLI

设备 1

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface ch1
NetEye@root-system-cluster] local ip address 192.168.2.1 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 192.168.2.2
NetEye@root-system-cluster] config check
NetEye@root-system-cluster] config sync
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] rti session tcp 21-221
NetEye@root-system-cluster] rti session udp 33-333
NetEye@root-system-cluster] rti session other 6-60
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] time benchmark on
NetEye@root-system-cluster] end
NetEye@root> save config
```

设备 2

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface ch1
NetEye@root-system-cluster] local ip address 192.168.2.2 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 192.168.2.1
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] rti session tcp 21-221
NetEye@root-system-cluster] rti session udp 33-333
NetEye@root-system-cluster] rti session other 6-60
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] end
NetEye@root> save config
```

15 虚拟系统

NISG-IPS 支持虚拟系统 （即虚拟防火墙）功能。

15.1 概述

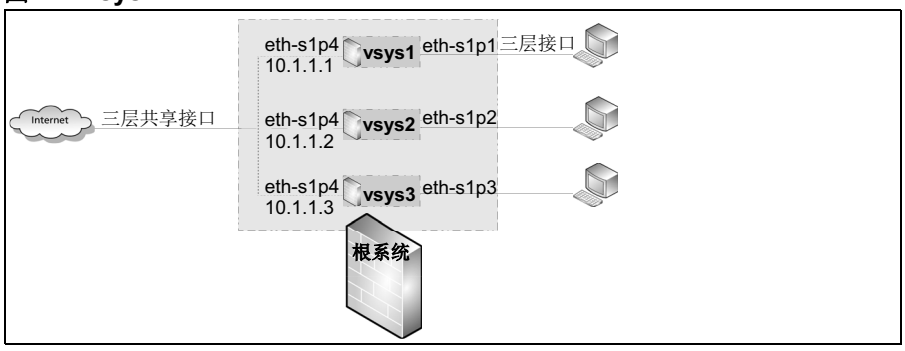
NISG-IPS 初始是一个单独的系统，我们将它称为根系统。一个 NISG-IPS 系统可以被逻辑地划分成多个虚拟系统 (Virtual System， Vsys)，每个虚拟系统拥有自己的管理员、审计员、策略、用户认证数据库等。虚拟系统最大数目由 License 决定。 NISG-IPS 还支持虚拟网络 （Virtual Network），通过虚拟接口连接多个虚拟系统。

本节包含以下内容：

15.1.1 虚拟系统 （Vsys）

下图演示了 Vsys 的基本用途。

图 24 Vsys



有以下需求时使用虚拟系统：

- 独立的管理员

  Vsys 管理员由根系统管理员创建和管理。Vsys 管理员不能改变虚拟系统的网络拓扑，也没有修改接口工作模式的权限。关于 Vsys 管理员的详细信息，请参见 3.15 管理用户。

- 独立的安全配置

  每个虚拟系统可以有自己的攻击防御、策略、IPS 和其他安全配置，IPS 功能包括 IPS、 URL 过滤和应用控制。

- 最大资源限制

  NISG-IPS 的会话资源和规则资源 （包括 ARP 和 CAM 表）对于所有 Vsys 来说是共享的，规则资源指策略、路由、 NAT 规则和防护配置等。会话资源和规则资源将按照实际需要，由系统动态地分配给每个 Vsys，从而保证资源需求尽可能地得到满足。

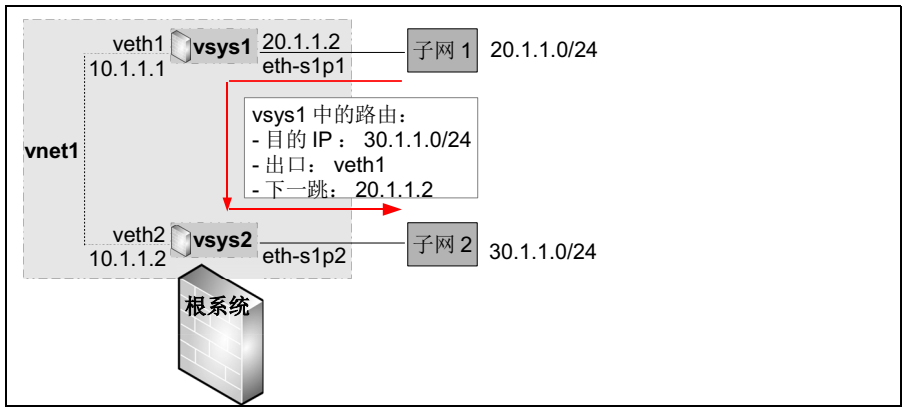
- 独立的管理 IP/ 接口

  管理 IP 是虚拟系统的一个三层接口 IP， Vsys 管理员可以通过管理 IP 来远程管理 NISG-IPS 虚拟系统。该管理 IP 可以与根系统或其他 Vsys 的管理 IP 相同 （三层共享接口充当管理接口的情况除外）。

15.1.2 虚拟网络 （Vnet）

下图演示了虚拟网络的基本用途。

图 25 Vnet



- 虚拟接口
  - 二层虚拟接口可以划分到 VLAN 接口中，这些 VLAN 接口再划分到虚拟系统中。
  - 三层虚拟接口可以直接划分到虚拟系统中。
  - 一个虚拟接口只能被划分给一个虚拟系统。
- 虚拟网络

  通过虚拟接口相连的多个虚拟系统组成一个虚拟网络 （Virtual Network）。从一个虚拟接口上发出的数据包，会被该虚拟网络的其他虚拟接口收到。

15.2 应用场景

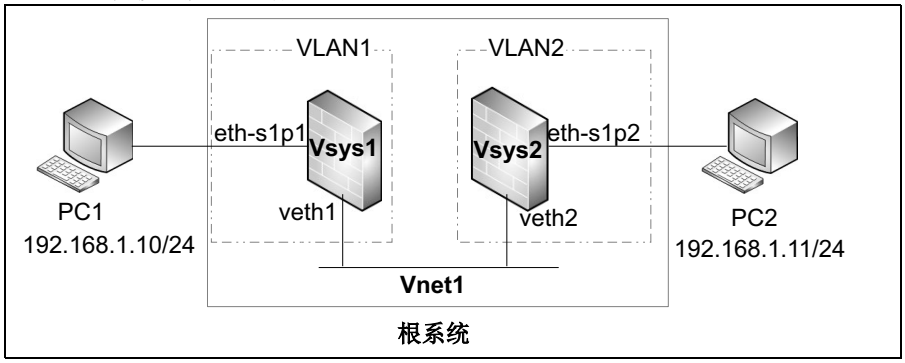
虚拟系统同根系统一样支持三种工作模式：

- 1. 透明模式
- 2. 路由模式
- 3. 混合模式

1. 透明模式

透明模式主要用于数据流的二层转发。

图 26 透明模式典型拓扑



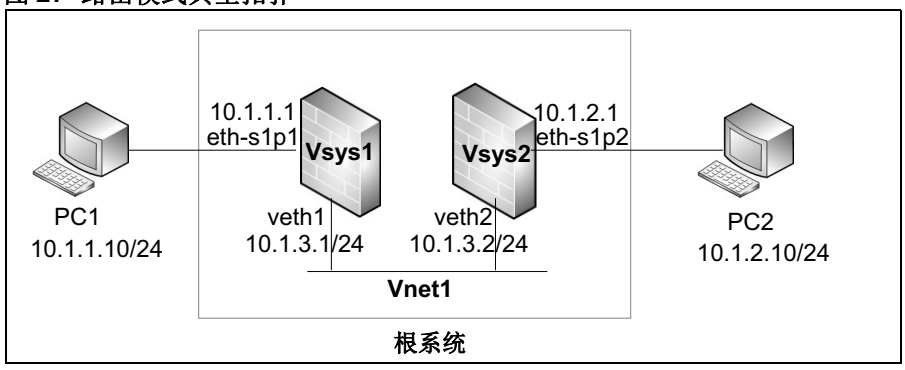
此范例的配置步骤包括：

1. 将 eth-s1p1 和 veth1 划入 VLAN1。
2. 将 VLAN1 划入 Vsys1。
3. 将 eth-s1p2 和 veth2 划入 VLAN2。
4. 将 VLAN2 划入 Vsys2。
5. 创建虚拟系统 Vnet1。
6. 将 veth1 和 Vsys1 划入 Vnet1。
7. 将 veth2 和 Vsys2 也划入 Vnet1。
8. 在 Vsys1 和 Vsys2 中分别配置访问策略，允许 PC 之间通讯。

2. 路由模式

路由模式是指虚拟设备可以让工作在不同网段之间的主机以三层路由的方式进行通信。虚拟设备处于路由工作模式时，各接口所连接的网络必须处于不同的网段，需要为虚拟设备的接口设置 IP 地址。

图 27 路由模式典型拓扑



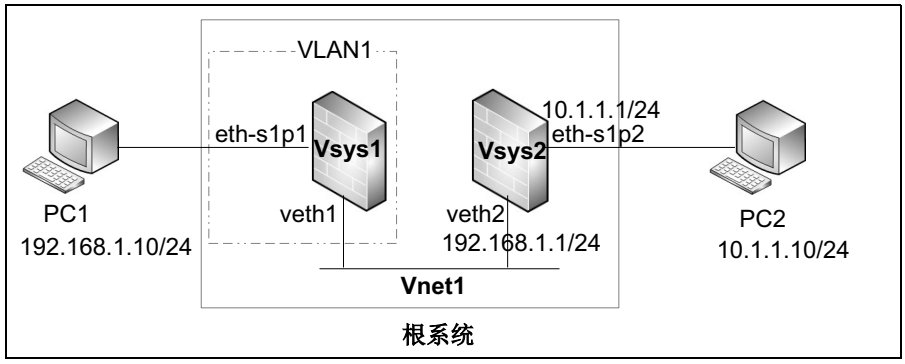
此范例的配置步骤包括：

1. 将 eth-s1p1 和 eth-s1p2 设置为三层工作模式，创建三层虚拟接口 veth1 和 veth2。
2. 创建虚拟系统 Vsys1，将 eth-s1p1 和 veth1 划入 Vsys1。
3. 创建虚拟系统 Vsys2，将 eth-s1p2 和 veth2 划入 Vsys2。
4. 在 Vsys1 中，配置 eth-s1p1 的 IP 地址为 10.1.1.1，配置 veth1 的 IP 地址为 10.1.3.1。
5. 在 Vsys2 中，配置 eth-s1p2 的 IP 地址为 10.1.2.1，配置 veth2 的 IP 地址为 10.1.3.2。
6. 创建虚拟网络 Vnet1，将 Vsys1 和 veth1 划入 Vnet1，将 Vsys2 和 veth2 也划入 Vnet1。
7. 在 Vsys1 和 Vsys2 中分别配置访问策略，允许 PC 之间通讯。
8. 在Vsys1上配置一条到PC2的静态路由，下一跳为10.1.3.2；在Vsys2上配置一条到PC1的静态路由，下一跳为 10.1.3.1。
9. 设置 PC1 的网关为 10.1.1.1，设置 PC2 的网关为 10.1.2.1。

3. 混合模式

混合模式能够同时实现数据流的二层转发和三层路由功能。

图 28 混合模式典型拓扑



此范例的配置步骤包括：

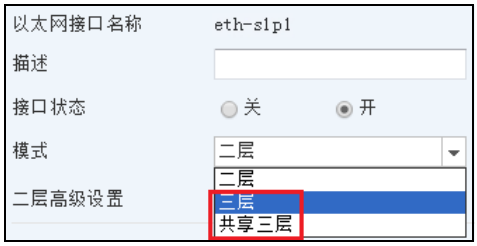
1. 将 eth-s1p1 和 veth1 划入 VLAN1，再将 VLAN1 划入 Vsys1。
2. 将 eth-s1p2 设置为三层接口，创建三层虚拟接口 veth2，然后将 eth-s1p2 和 veth2 划入 Vsys2。
3. 在 Vsys2 中，配置 eth-s1p2 的 IP 地址为 10.1.1.1/24，配置 veth2 的 IP 地址为 192.168.1.1/24。
4. 创建虚拟网络 Vnet1，将 Vsys1 和 veth1 划入 Vnet1，将 Vsys2 和 veth2 也划入 Vnet1。
5. 在 Vsys1 和 Vsys2 中分别配置访问策略，允许 PC 之间通讯。
6. 设置 PC1 的网关为 192.168.1.1，设置 PC2 的网关为 10.1.1.1。

15.3 基本配置步骤

本节介绍虚拟系统的基本配置流程：

15.3.1 创建三层接口

1. 选择**网络** > **接口**。
2. 点击将已有的二层接口设置为三层或三层共享接口，或点击**新建**创建新的三层或三层共享接口。



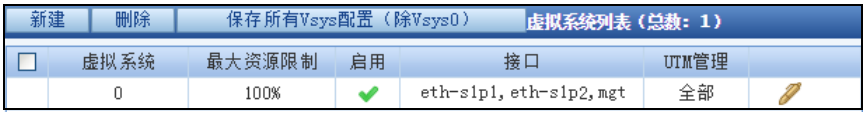
- 如果三层接口被划分到虚拟系统中：
  - 接口的MAC地址、MTU值以及IP地址等信息只能在虚拟系统中进行设置，在根系统下无法查看。
  - 三层接口所绑定的二层接口在虚拟系统下将无法修改，而只能在根系统下修改。
- 如果一个三层共享接口被划分到不同的虚拟系统，其 IP 地址不能相同，但可以是同一网段的 IP 地址。

表 255 接口命令

interface ethernet	进入以太网接口配置模式。
working-type layer3-shared-interface	设置接口为三层共享工作模式。
channel	进入以太网通道配置模式。
hold ethernet	添加二层接口到以太网通道。

15.3.2 创建虚拟系统 （资源限制 / 接口 / 管理 IP/IPS）

1. 选择**系统** > **虚拟系统** > **虚拟系统**。



系统默认存在一个编号为 0 的虚拟系统，即根系统。默认情况下，根系统是启用状态，最大资源限制是 100%（表示根系统最多可占用 100% 的系统资源），包含所有三层接口， IPS 功能全部开启。

2. 创建虚拟系统，指定名称、最大资源、三层接口、管理 IP 地址和内容检测功能。

3. 点击**确定**。

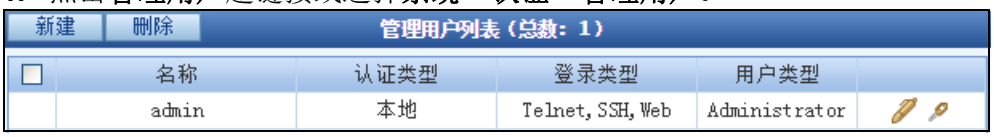
表 256 虚拟系统命令

show vsys [*vsys_id* | **root**]	查看虚拟系统信息。
vsys *vsys_id* **resource-limit** *num*	创建虚拟系统。
unset vsys [*vsys_id*]	删除指定虚拟系统或所有虚拟系统。
vsys *vsys_id* **enable**	启用指定的虚拟系统。
vsys *vsys_id* **disable**	禁用指定的虚拟系统。
hold	添加以太网接口、以太网通道、 VLAN 接口、荣誉接口、虚拟接口和 PPPoE 接口到指定虚拟系统。
unset hold	将以太网接口、以太网通道、 VLAN 接口、荣誉接口、虚拟接口和 PPPoE 接口从指定虚拟系统中删除。
vsys *vsys_id* **resource-limit** *num*	修改虚拟系统资源限制。
manage-ip-address	为指定虚拟系统设置管理 IPv4 地址。
manage-ipv6-address	为指定虚拟系统设置管理 IPv6 地址。
save all-vsys-config	保存除根系统外的所有虚拟系统的配置信息。
switch vsys *vsys_name*	切换虚拟系统。

15.3.3 创建虚拟系统管理员

根系统管理员可以创建虚拟系统并管理虚拟系统资源。

1. 点击**管理用户**超链接或选择**系统** > **认证** > **管理用户**。



2. 将虚拟系统划分给已有的根系统管理员或虚拟系统管理员，或为虚拟系统创建新的虚拟系统管理员。

提示：一个根系统管理员可以管理多个虚拟系统。

3. 点击**确定**。

表 257 虚拟系统管理员命令

user administrator *user_name* **vsys-administrator vsys**	为指定虚拟系统创建虚拟系统管理员。
unset user administrator *user_name*	删除虚拟系统管理员。
user administrator *user_name* **allowed-vsys** *vsys_name*	为根系统管理员或虚拟系统管理员添加虚拟系统管理权限。
unset user administrator *user_name* **allowed-vsys** *vsys_name*	删除根系统管理员或虚拟系统管理员的虚拟系统管理权限。
show user administrator [*user_name*]	显示当前虚拟系统的所有管理员信息。
show line	显示当前虚拟系统的所有在线管理员信息。

15.3.4 登录 / 切换虚拟系统

以下步骤包括：

1. 通过管理 IP 登录虚拟系统
2. 通过 CLI 登录虚拟系统
3. 通过 WebUI 切换虚拟系统

通过管理 IP 登录虚拟系统：

1. 打开浏览器，输入 https://vsys 管理 IP，进入虚拟系统登录页面：

2. 输入用户名和密码登录虚拟系统：

通过 CLI 登录虚拟系统：

上面两个操作步骤没有对应的命令，但是如果虚拟系统已经划分给根系统管理员管理，根系统管理员可以通过命令行控制台进行以下操作达到相同目的：

a. 退出根系统。

b. 输入虚拟系统名称，按 Enter 键。

c. 输入用户名和密码登录虚拟系统。

```
NetEye@root> exit


Vsys Name:vsys1
Neusoft NetEye (NetEye) (tty1)


Username:vsys1admin
Password:
NetEye@vsys1> _
```

通过 WebUI 切换虚拟系统：

1. 要切换虚拟系统：

   - 在根系统下选择**虚拟系统 > 虚拟系统**，点**虚拟系统**查看页面底端的**切换虚拟系统**链接。

   - 在虚拟系统下选择**虚拟系统 > 虚拟系统**。

2. 点击对应的按钮，切换到相应的虚拟系统下。

提示：根系统管理员可以在根系统和授权虚拟系统之间进行切换。虚拟系统管理员只能在授权虚拟系统之间进行切换。

表 258 虚拟系统切换命令

switch vsys *vsys_name*	切换虚拟系统。

15.3.5 管理虚拟系统

以下是管理虚拟系统最常见的步骤。

1. 选择**网络** > **接口**，并设置虚拟系统间通讯用的接口 IP 地址：

2. 选择**网络** > **安全域**，创建安全域。

3. 选择**防火墙** > **访问策略**，创建访问策略允许虚拟系统间的访问。

4. 自定义虚拟系统中的功能。更多信息请参见 15.4.3 虚拟系统中可配置的功能。
   - 只能在根系统下进行的配置：
     - IPS 防护配置。
     - IPS 攻击签名、 URL 过滤规则和应用知识库升级。
   - 每 Vsys 配置：
     - URL 过滤和应用控制的防护配置。
     - 所有虚拟系统共享升级后规则库。
   - 虚拟系统中不提供缺省的 IPS 策略。

表 259 安全域和访问策略命令

zone *zone_name*	创建安全域。
zone based-layer3	配置基于三层或三层共享接口的安全域。
policy access	添加访问策略。

15.3.6 创建虚拟网络

1. 切换到根系统，选择工作模式后进行以下配置。关于工作模式的更多信息请参见 15.2 应用场景。（虚拟网络只能在根系统下配置。）
2. 选择**网络** > **接口**，创建三层接口：

3. 选择**系统** > **虚拟系统** > **虚拟系统**，为虚拟系统划分虚拟接口：

4. 选择**系统** > **虚拟系统** > **虚拟网络**，创建虚拟网络，为虚拟网络划分虚拟接口和虚拟系统。

5. 登录虚拟系统创建访问策略，允许虚拟系统间通讯。参见 10.2.1 创建访问策略。
6. 对于工作在路由模式的虚拟系统，还需要创建缺省路由。

表 260 虚拟网络命令

vnet *vnet_id*	创建虚拟网络。
unset vnet *vnet_id*	删除虚拟网络。
hold veth *veth_id*	划分虚拟接口到虚拟网络。
unhold veth *veth_id*	从虚拟网络中删除虚拟接口。
description [*string*]	为虚拟网络添加描述信息或修改、删除虚拟网络描述信息。
show vnet [*vnet_id* | **brief**]	查看虚拟网络信息。

15.4 配置参数说明

本节介绍以下内容的相关参数：

15.4.1 虚拟系统

表 261 虚拟系统参数

参数	说明
虚拟系统	虚拟系统标识。虚拟系统名称由 vsys+ 虚拟系统标识组成。虚拟系统标识的取值范围为 1 ～ 255。
最大资源限制	根系统管理员划分给虚拟系统的最大资源百分比。取值范围为 1 ～ 100。
启用	虚拟系统是否处于启用状态。✔ 表示启用，✘ 表示禁用。
接口	根系统管理员划分给虚拟系统的三层或三层共享接口，包括三层或三层共享以太网接口、三层虚拟接口、 VLAN 接口、三层或三层共享以太网通道、三层或三层共享冗余接口以及 PPPoE 接口。
IPS 管理	根系统管理员为虚拟系统划分的 IPS 功能。可划分的 IPS 功能包括 IPS、URL 过滤和应用控制。
描述	长度 0~255 字节， UTF-8 字符。不能包含以下字符：？ " ’ \ < > &
启用虚拟系统	启用或禁用虚拟系统。
管理 IP 地址	选择一个三层接口作为虚拟系统的管理口，同时设置一个 IPv4 或 IPv6 地址作为管理 IP 地址。
保存所有 Vsys 配置 （除 Vsys0）	保存除 root 外的所有 Vsys 配置。
管理用户	用于跳转到管理用户页面，为虚拟系统创建或指定管理用户。
切换虚拟系统	用于跳转到切换虚拟系统页面，进行虚拟系统切换。

15.4.2 虚拟网络

表 262 虚拟网络参数

参数	说明
ID	虚拟网络标识。取值范围为 1 ～ 255 之间的整数。
虚拟系统	虚拟网络连接的虚拟系统。
接口	虚拟系统接入虚拟网络使用的虚拟接口。
描述	长度 0~255 字节， UTF-8 字符 （除？ " ’ \ < > &）。
链接虚拟接口列表	添加虚拟接口，将对应的虚拟系统接入虚拟网络。

15.4.3 虚拟系统中可配置的功能

虚拟系统下可配置的功能包括：

- **主页**
- **系统 > 概述 > 访问设置**
- **系统 > 维护 > 备份 / 恢复 / 集中管理**
- **系统 > 认证 / 证书 / 对象**
- **系统 > 高可用性 > 虚拟路由器 / 虚拟路由器探测组**
- **系统 > 虚拟系统**：只能切换虚拟系统。
- **系统 > 服务配置 > 访问设置**（root 管理用户登录设置除外）**/ 标题信息**
- **系统 > 日志配置**
- **网络 > 接口 / 安全域**：仅能添加 Loopback 接口、编辑已添加的以太网接口。
- **网络 > DNS**
- **网络 > DHCP**
- **网络 > 路由 / 地址转换 / 多播 /IPv6**
- **防火墙**：包括策略和攻击防御。
- **IPS> 概要信息**
- **IPS> 出口控制 > 策略**
- **IPS> 出口控制 > 应用控制**
- **IPS> 出口控制 >URL 过滤 > 常规设置**：仅能查询 URL 分类。
- **IPS> 出口控制 >URL 过滤 > 防护配置 / 黑白名单**
- **IPS> 出口控制 >DNS 域名黑名单 / 页面过滤**
- **IPS> 客户端防护 / 服务器防护**
- **IPS> 通知消息**
- **IPS>QoS**
- **VPN**：包括 IPSec VPN 、 GRE VPN 和 SSL VPN。
- **监控**：仅提供当前所在系统的监控信息。

15.5 Vsys 范例

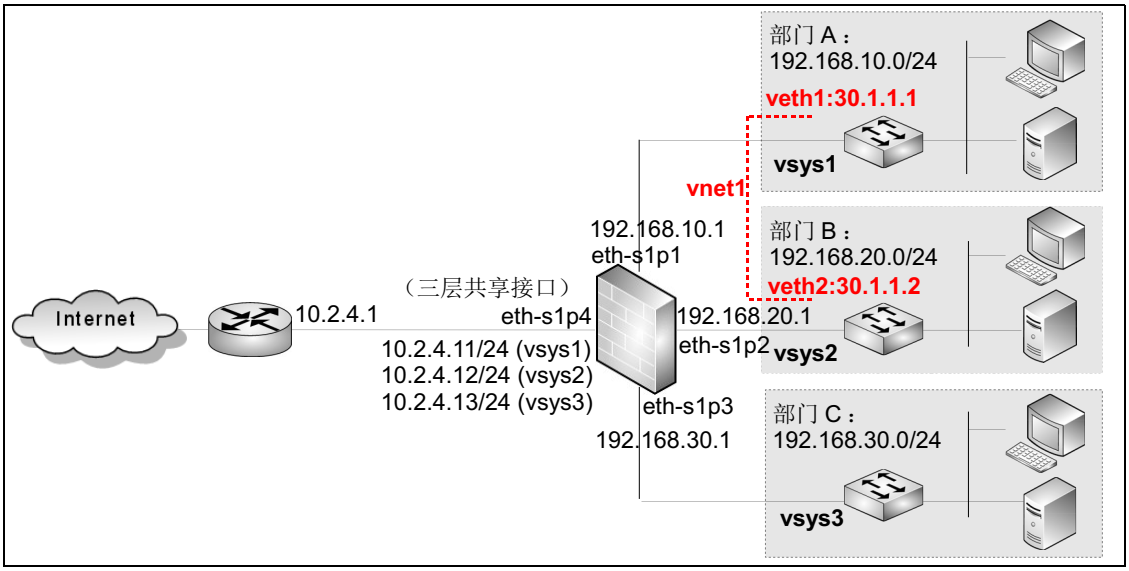
15.5.1 范例：基于三层共享接口的多 Vsys 应用

基本需求

某企业有三个部门：A、B、C。它们处于不同的网段且需要有不同的安全配置，而且整个企业只有一个网络出口接入互联网。

- 为了让这三个部门有各自不同的安全配置，可为每个部门分别创建一个虚拟系统。
- 为了让三个部门可以同时访问互联网，需要将外网出口作为共享接口分配给这三个虚拟系统共用。
- 为了让部门 A 和 B 能够相互通讯，可以在他们之间创建一个虚拟网络，将这两个部门所在的虚拟系统连在一起。

组网拓扑



配置要点

- 创建三层接口
- 创建虚拟系统，划分接口，设置管理 IP
- 为 admin 添加 Vsys 1-3 的管理权限
- 配置虚拟系统
- 创建虚拟接口

- 将虚拟接口划入虚拟系统
- 创建虚拟网络
- 设置 Vsys 的虚拟接口 IP、静态路由和访问策略
- 创建虚拟系统管理员

配置步骤

创建三层接口

1. 选择**网络** > **接口**，将 eth-s1p1、eth-s1p2、eth-s1p3 设置为三层接口，将 eth-s1p4 设置为三层共享接口。
2. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-interface
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] working-type layer3-interface
NetEye@root-system-if-eth-s1p2] exit
NetEye@root-system] interface ethernet s1p3
NetEye@root-system-if-eth-s1p3] working-type layer3-interface
NetEye@root-system-if-eth-s1p3] exit
NetEye@root-system] interface ethernet s1p4
NetEye@root-system-if-eth-s1p4] working-type layer3-shared-interface
NetEye@root-system-if-eth-s1p4] exit
NetEye@vsys1-system] end
NetEye@vsys1> save config
```

创建虚拟系统，划分接口，设置管理 IP

1. 选择**系统** > **虚拟系统** > **虚拟系统**，创建虚拟系统 vsys1、 vsys2、 vsys3。
   - vsys1：最大资源限制 =50%；三层接口 =eth-s1p1、eth-s1p4；开启所有 IPS 管理功能；管理 IP 地址 =eth-s1p1 （192.168.10.1/24）
   - vsys2：最大资源限制 =50%；三层接口 =eth-s1p2、eth-s1p4；开启所有 IPS 管理功能；管理 IP 地址 =eth-s1p2 （192.168.20.1/24）
   - vsys3：最大资源限制 =50%；三层接口 =eth-s1p3、eth-s1p4；开启所有 IPS 管理功能；管理 IP 地址 =eth-s1p3 （192.168.30.1/24）
2. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vsys 1 resource-limit 50
NetEye@root-system-vsys1] hold ethernet s1p1
NetEye@root-system-vsys1] hold ethernet s1p4
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2 resource-limit 50
NetEye@root-system-vsys2] hold ethernets1p2
NetEye@root-system-vsys2] hold ethernet s1p4
NetEye@root-system-vsys2] exit
NetEye@root-system] vsys 3 resource-limit 50
NetEye@root-system-vsys3] hold ethernet s1p3
NetEye@root-system-vsys3] hold ethernet s1p4
NetEye@root-system-vsys3] exit
NetEye@root-system] vsys 1
NetEye@root-system-vsys1] manage-ip-address 192.168.10.1 255.255.255.0
ethernet s1p1
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2
NetEye@root-system-vsys2] manage-ip-address 192.168.20.1 255.255.255.0
ethernet s1p2
NetEye@root-system-vsys2] exit
NetEye@root-system] vsys 3
NetEye@root-system-vsys3] manage-ip-address 192.168.30.1 255.255.255.0
ethernet s1p3
NetEye@root-system-vsys4] end
NetEye@root> save config
```

为 admin 添加 Vsys 1-3 的管理权限

1. 选择**系统** > **认证** > **管理用户**，点击 admin 对应的按钮，为根系统管理员 admin 添加 vsys1、 vsys2 和 vsys3 的管理权限。
2. 点击**确定**。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] user administrator admin allowed-vsys vsys1
NetEye@root-system] user administrator admin allowed-vsys vsys2
NetEye@root-system] user administrator admin allowed-vsys vsys3
NetEye@root-system] end
NetEye@root> save config
```

配置虚拟系统

1. 选择**系统** > **虚拟系统** > **虚拟系统**，点击页面底端的**切换虚拟系统**链接。
2. 点击虚拟系统 vsys1 对应的按钮，进入虚拟系统 vsys1。
   a. 选择**网络**>**接口**，进入**接口**页面，设置eth-s1p1的IP地址设置为192.168.10.1/24，设置 eth-s1p4 的 IP 地址为 10.2.4.11/24。
   b. 选择**网络** > **路由** > **缺省路由**，添加一条缺省路由，网关指向 ISP 路由器 10.2.4.1，出口接口为 eth-s1p4。
   c. 选择**防火墙** > **访问策略**，进入**访问策略**页面，添加一条允许 192.168.10.0/24 网段到任意目的地址的访问策略。
3. 切换到 vsys2，并进行以下操作：
   a. 选择**网络**>**接口**，进入接口页面，设置eth-s1p2的IP地址设置为192.168.20.1/24，设置 eth-s1p4 的 IP 地址为 10.2.4.12/24。
   b. 选择**网络** > **路由** > **缺省路由**，添加一条缺省路由，网关指向 ISP 路由器 10.2.4.1，出口接口为 eth-s1p4。
   c. 选择**防火墙** > **访问策略**，进入访问策略页面，添加一条允许 192.168.20.0/24 网段到任意目的地址的访问策略。
4. 切换到 vsys3，并进行以下操作：
   a. 选择**网络**>**接口**，进入接口页面，设置eth-s1p3的IP地址设置为192.168.30.1/24，设置 eth-s1p4 的 IP 地址为 10.2.4.13/24。
   b. 选择**防火墙** > **访问策略**，进入访问策略页面，添加一条允许 192.168.30.0/24 网段到任意目的地址的访问策略。
5. 点击。

CLI

```
NetEye@root> switch vsys vsys1
NetEye@vsys1> configure mode override
NetEye@vsys1-system] interface ethernet s1p1
NetEye@vsys1-system-if-eth-s1p1] ip address 192.168.10.1 255.255.255.0
NetEye@vsys1-system-if-eth-s1p1] exit
NetEye@vsys1-system] interface ethernet s1p4
NetEye@vsys1-system-if-eth-s1p4] ip address 10.2.4.11 255.255.255.0
NetEye@vsys1-system-if-eth-s1p4] exit
NetEye@vsys1-system] route default interface s1p4 gateway 10.2.4.1
NetEye@vsys1-system] policy access vsys1out any 192.168.10.0/24 any
any any any permit enable
NetEye@vsys1-system] end
NetEye@vsys1> save config
NetEye@vsys1> switch vsys vsys2
NetEye@vsys2> configure mode override
```

```
NetEye@vsys2-system] interface ethernet s1p2
NetEye@vsys2-system-if-eth-s1p2] ip address 192.168.20.1 255.255.255.0
NetEye@vsys2-system-if-eth-s1p2] exit
NetEye@vsys2-system] interface ethernet s1p4
NetEye@vsys2-system-if-eth-s1p4] ip address 10.2.4.12 255.255.255.0
NetEye@vsys2-system-if-eth-s1p4] exit
NetEye@vsys1-system] route default interface s1p4 gateway 10.2.4.1
NetEye@vsys2-system] policy access vsys2out any 192.168.20.0/24 any
any any any permit enable
NetEye@vsys2-system] end
NetEye@vsys2> save config
NetEye@vsys2> switch vsys vsys3
NetEye@vsys3> configure mode override
NetEye@vsys3-system] interface ethernet s1p3
NetEye@vsys3-system-if-eth-s1p3] ip address 192.168.30.1 255.255.255.0
NetEye@vsys3-system-if-eth-s1p3] exit
NetEye@vsys3-system] interface ethernet s1p4
NetEye@vsys3-system-if-eth-s1p4] ip address 10.2.4.13 255.255.255.0
NetEye@vsys3-system-if-eth-s1p4] exit
NetEye@vsys1-system] route default interface s1p4 gateway 10.2.4.1
NetEye@vsys3-system] policy access vsys3out any 192.168.30.0/24 any
any any any permit enable
NetEye@vsys3-system] end
NetEye@vsys3> save config
```

创建虚拟接口

1. 选择**系统** > **虚拟系统** > **虚拟系统**，点击 Vsys 0 对应的图标切换到根系统。
2. 选择**网络** > **接口**，创建三层虚拟接口 veth1 和 veth2。
3. 点击。

CLI

```
NetEye@vsys4> switch vsys root
NetEye@root> configure mode override
NetEye@root-system] veth 1
NetEye@root-system-veth1] working-type layer3-interface
NetEye@root-system-veth1] exit
NetEye@root-system] veth 2
NetEye@root-system-veth2] working-type layer3-interface
NetEye@root-system-veth2] end
NetEye@root> save config
```

将虚拟接口划入虚拟系统

1. 选择**系统**>**虚拟系统**>**虚拟系统**，将虚拟接口 veth1 和 veth2 分别划入 vsys1 和 vsys2。
2. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vsys 1
NetEye@root-system-vsys1] hold veth 1
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2
NetEye@root-system-vsys2] hold veth 2
NetEye@root-system-vsys2] end
NetEye@root> save config
```

创建虚拟网络

1. 选择**系统**>**虚拟系统**>**虚拟网络**，创建虚拟网络 vnet1，将 vsys1 和 veth1 划入 vnet1，将 vsys2 和 veth2 也划入 vnet1。
2. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vnet 1
NetEye@root-system-vnet1] hold veth 1
NetEye@root-system-vnet1] hold veth 2
NetEye@root-system-vnet1] end
NetEye@root> save config
```

设置 Vsys 的虚拟接口 IP、静态路由和访问策略

1. 选择**系统**>**虚拟系统**>**虚拟系统**，点击页面底端的**切换虚拟系统**链接，点击 Vsys 1 对应的图标，进入虚拟系统 vsys1。
2. 选择**网络**>**接口**，设置 veth1 的 IP 地址为 30.1.1.1/24。
3. 点击**确定**。
4. 选择**网络**>**路由**>**缺省路由**，添加到 192.168.20.0/24 网段的静态路由，出口接口为 veth1，下一跳网关为 30.1.1.2。
5. 选择**防火墙**>**访问策略**，添加一条访问策略 vsys2to1，允许 192.168.20.0/24 到 192.168.10.0/24 的访问。

6. 切换到 vsys2，并进行以下配置：
   a. 选择**网络** > **接口**，设置 veth2 的 IP 地址为 30.1.1.2/24。
   b. 选择**网络** > **路由** > **缺省路由**，添加到 192.168.10.0/24 网段的静态路由，出口接口为 veth2，下一跳网关为 30.1.1.1。
   c. 选择**防火墙** > **访问策略**，添加一条访问策略，允许 192.168.10.0/24 到 192.168.20.0/24 的访问。
7. 点击  。

CLI

```
NetEye@root> switch vsys vsys1
NetEye@vsys1> configure mode override
NetEye@vsys1-system] veth 1
NetEye@vsys1-system-veth1] ip address 30.1.1.1 255.255.255.0
NetEye@vsys1-system-veth1] exit
NetEye@vsys1-system] route 192.168.20.0 255.255.255.0 interface veth1
gateway 30.1.1.2
NetEye@vsys1-system] policy access vsys2to1 any 192.168.20.0 any
192.168.10.0 any any permit enable
NetEye@vsys1-system] end
NetEye@vsys1> save config
NetEye@vsys1> switch vsys vsys2
NetEye@vsys2> configure mode override
NetEye@vsys2-system] veth 2
NetEye@vsys2-system-veth2] ip address 30.1.1.2 255.255.255.0
NetEye@vsys2-system-veth2] exit
NetEye@vsys2-system] route 192.168.10.0 255.255.255.0 interface veth2
gateway 30.1.1.1
NetEye@vsys2-system] policy access vsys1to2 any 192.168.10.0 any
192.168.20.0 any any permit enable
NetEye@vsys2-system] end
NetEye@vsys2> save config
```

创建虚拟系统管理员

1. 选择**系统** > **虚拟系统** > **虚拟系统**，点击 Vsys 0 对应的 图标切换到根系统。
2. 选择**系统** > **认证** > **管理用户**，为 vsys1 添加 Vsys 管理员 vsys1ad，密码为 test_123。
3. 点击**确定**。
4. 分别为 vsys2、 vsys3 添加 Vsys 管理员 vsys2ad、 vsys3ad，密码均为 test_123。
5. 点击 。
6. 以 Vsys 管理员身份登录虚拟系统进行管理，登录方式同根系统管理员登录根系统。

CLI

```
NetEye@vsys2> switch vsys root
NetEye@root> configure mode override
NetEye@root-system] user administrator vsys1ad vsys-administrator
vsys vsys1 authtype local password simple
Password(6-128): <test_123>
Repeat Password(6-128): <test_123>
NetEye@root-system] user administrator vsys1ad logintype
web,ssh,telnet
NetEye@root-system] user administrator vsys2ad vsys-administrator
vsys vsys2 authtype local password simple
Password(6-128): <test_123>
Repeat Password(6-128): <test_123>
NetEye@root-system] user administrator vsys2ad logintype
web,ssh,telnet
NetEye@root-system] user administrator vsys3ad vsys-administrator
vsys vsys3 authtype local password simple
Password(6-128): <test_123>
Repeat Password(6-128): <test_123>
NetEye@root-system] user administrator vsys3ad logintype
web,ssh,telnet
NetEye@root-system] end
NetEye@root> save config
```

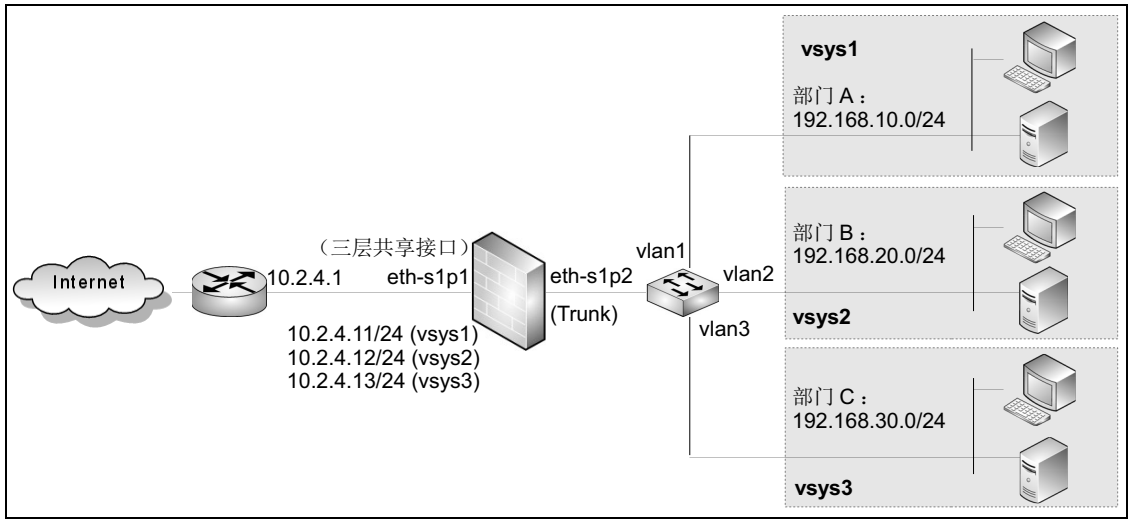
15.5.2 范例：基于 Trunk 接口的多 Vsys 应用

基本需求

如下图所示，某公司有三个部门 A、 B、 C。这三个部门分属于不同的 IP 网段，但它们有不同的安全配置和服务需求，而整个公司只有一个网络出口连接互联网，且只有一个网络入口连接内网交换机。

- 为了让这三个部门网络可以有自己的安全配置，可以为每个部门单独创建一个虚拟系统。
- 为了让这三个部门的员工都可以访问互联网，可以将出口接口作为共享接口分配给这三个虚拟系统共用，同时将入口接口设为 Trunk 模式。

组网拓扑



配置要点

- 创建三层接口
- 创建虚拟系统
- 为 admin 添加 Vsys 管理权限
- 为 Vsys 设置接口 IP 和访问策略

提示：关于如何创建 Vsys 管理员和设置虚拟系统管理 IP 地址，请参见 15.5.1 范例：基于三层共享接口的多 Vsys 应用。

配置步骤

创建三层接口

1. 选择**网络** > **接口**，设置 eth-s1p1 接口为三层共享接口。
2. 点击**确定**。
3. 创建 VLAN 接口 vlan1、vlan2 和 vlan3，设置 eth-s1p2 接口为二层接口 Trunk 模式，将 vlan1、 vlan2 和 vlan3 划入 eth-s1p2。
4. 在内网三层交换机上设置相应的 Trunk 口和 VLAN，并将三层交换机设置为内网网关。
5. 点击**确定**。
6. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet s1p1
NetEye@root-system-if-eth-s1p1] working-type layer3-shared-interface
NetEye@root-system-if-eth-s1p1] exit
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] exit
NetEye@root-system] vlan 3
NetEye@root-system-vlan3] exit
NetEye@root-system] interface ethernet s1p2
NetEye@root-system-if-eth-s1p2] port mode trunk
NetEye@root-system-if-eth-s1p2] port trunk allowed vlan 1,2,3
NetEye@root-system] end
NetEye@root> save config
```

创建虚拟系统

1. 选择**系统 > 虚拟系统 > 虚拟系统**，点击**新建**，创建虚拟系统 vsys1、vsys2 和 vsys3，将 eth-s1p1 和 vlan1 划入 vsys1、 eth-s1p1 和 vlan2 划入 vsys2、 eth-s1p1 和 vlan3 划入 vsys3。
2. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vsys 1 resource-limit 50
NetEye@root-system-vsys1] hold ethernet s1p1
NetEye@root-system-vsys1] hold vlan 1
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2 resource-limit 50
NetEye@root-system-vsys2] hold ethernet s1p1
NetEye@root-system-vsys2] hold vlan 2
NetEye@root-system-vsys2] exit
NetEye@root-system] vsys 3 resource-limit 50
NetEye@root-system-vsys3] hold ethernet s1p1
NetEye@root-system-vsys3] hold vlan 3
NetEye@root-system] end
NetEye@root> save config
```

为 admin 添加 Vsys 管理权限

1. 点击**虚拟系统**页面底端的**管理用户**超链接，跳转到**管理用户**页面，点击 admin 对应的按钮，进入编辑页面，为 admin 添加管理 vsys1、 vsys2 和 vsys3 的权限。
2. 点击**确定**。
3. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] user administrator admin allowed-vsys vsys1
NetEye@root-system] user administrator admin allowed-vsys vsys2
NetEye@root-system] user administrator admin allowed-vsys vsys3
NetEye@root-system] end
NetEye@root> save config
```

为 Vsys 设置接口 IP 和访问策略

1. 选择**系统 > 虚拟系统 > 虚拟系统**，点击页面底端的**切换虚拟系统**超链接。
2. 点击虚拟系统 1 对应的按钮，切换到虚拟系统 vsys1。
3. 选择**网络 > 接口**，设置 eth-s1p1 的 IP 地址为 10.2.4.11/24，设置 vlan1 的 IP 地址为 192.168.10.1/24。
4. 选择**网络**>**路由**>**缺省路由**，添加一条缺省路由，网关指向ISP路由器10.2.4.1，出口接口为 eth-s1p4。
5. 选择**防火墙** > **访问策略**，添加一条允许 192.168.10.0/24 网段到任意目的地址的访问策略 vsys1out。
6. 切换到 vsys2，并进行以下配置：
   a. 选择**网络 > 接口**，设置 eth-s1p1 的 IP 地址为 10.2.4.12/24，设置 vlan2 的 IP 地址为 192.168.20.1/24。
   b. 选择**网络** > **路由** > **缺省路由**，添加一条缺省路由，网关指向 ISP 路由器 10.2.4.1，出口接口为 eth-s1p1。
   c. 选择**防火墙**>**访问策略**，添加一条允许 192.168.20.0/24 网段到任意目的地址的访问策略 vsys2out。
7. 切换到 vsys3，并进行以下配置：
   a. 选择**网络 > 接口**，设置 eth-s1p1 的 IP 地址为 10.2.4.13/24，设置 vlan3 的 IP 地址为 192.168.30.1/24。
   b. 选择**网络** > **路由** > **缺省路由**，添加一条缺省路由，网关指向 ISP 路由器 10.2.4.1，出口接口为 eth-s1p1。
   c. 选择**防火墙**>**访问策略**，添加一条允许 192.168.30.0/24 网段到任意目的地址的访问策略 vsys3out。
8. 点击。

CLI

```
NetEye@root> switch vsys vsys1
NetEye@vsys1> configure mode override
NetEye@vsys1-system] interface ethernet s1p1
NetEye@vsys1-system-if-eth-s1p1] ip address 10.2.4.11 255.255.255.0
NetEye@vsys1-system-if-eth-s1p1] exit
NetEye@vsys1-system] vlan 1
NetEye@vsys1-system-vlan1] ip address 192.168.10.1 255.255.255.0
NetEye@vsys1-system-vlan1] exit
NetEye@vsys1-system] route default interface s1p1 gateway 10.2.4.1
NetEye@vsys1-system] policy access vsys1out any 192.168.10.0 any any
any any permit enable
NetEye@vsys1-system] end
NetEye@vsys1> save config
NetEye@vsys1> switch vsys vsys2
```

```
NetEye@vsys2> configure mode override
NetEye@vsys2-system] interface ethernet s1p1
NetEye@vsys2-system-if-eth-s1p1] ip address 10.2.4.12 255.255.255.0
NetEye@vsys2-system-if-eth-s1p1] exit
NetEye@vsys2-system] vlan 2
NetEye@vsys2-system-vlan2] ip address 192.168.20.1 255.255.255.0
NetEye@vsys2-system-vlan2] exit
NetEye@vsys1-system] route default interface s1p1 gateway 10.2.4.1
NetEye@vsys2-system] policy access vsys2out any 192.168.20.0 any any
any any permit enable
NetEye@vsys2-system] end
NetEye@vsys2> save config
NetEye@vsys2> switch vsys vsys3
NetEye@vsys3> configure mode override
NetEye@vsys3-system] interface ethernet s1p1
NetEye@vsys3-system-if-eth-s1p1] ip address 10.2.4.13 255.255.255.0
NetEye@vsys3-system-if-eth-s1p1] exit
NetEye@vsys3-system] vlan 3
NetEye@vsys3-system-vlan3] ip address 192.168.30.1 255.255.255.0
NetEye@vsys3-system-vlan3] exit
NetEye@vsys1-system] route default interface s1p1 gateway 10.2.4.1
NetEye@vsys3-system] policy access vsys3out any 192.168.30.0 any any
any any permit enable
NetEye@vsys3-system] end
NetEye@vsys3> save config
```

16 监控

NISG-IPS 的监控功能对系统信息进行全面的监控，使管理员能够更好地维护系统性能和安全。本章结构如下：

16.1 拓扑

拓扑监控显示安全域、三层接口以及二层接口间的网络拓扑关系。

选择**监控** > **拓扑**。

表 263 拓扑参数

参数	说明
安全域	三层接口所属的安全域。
三层接口	安全域包含的接口。 三层安全域包含的是三层接口，二层安全域对应的是 VLAN 接口。
IP 地址	接口对应的 IP 地址。 IPv4 地址仅显示主 IP 地址， IPv6 地址则显示所有 IP 地址。 三层安全域对应的是三层接口的 IP 地址。二层安全域对应的是 VLAN 接口的 IP 地址。
二层接口	三层接口包含的二层接口。
链路状态	对应二层接口或三层接口的链路状态。 • **绿色图标 —** 接口已连接。 • **红色图标 —** 连接已断开。
虚拟系统	安全域所属的虚拟系统。

16.2 流量统计

NISG-IPS 的流量统计监控使管理员能够及时发现系统瓶颈或隐患，全面考察系统的稳定性和可靠性。流量统计监控以下内容：

16.2.1 接口流量

选择**监控** > **流量统计数据** > **接口流量**。

表 264 接口流量参数

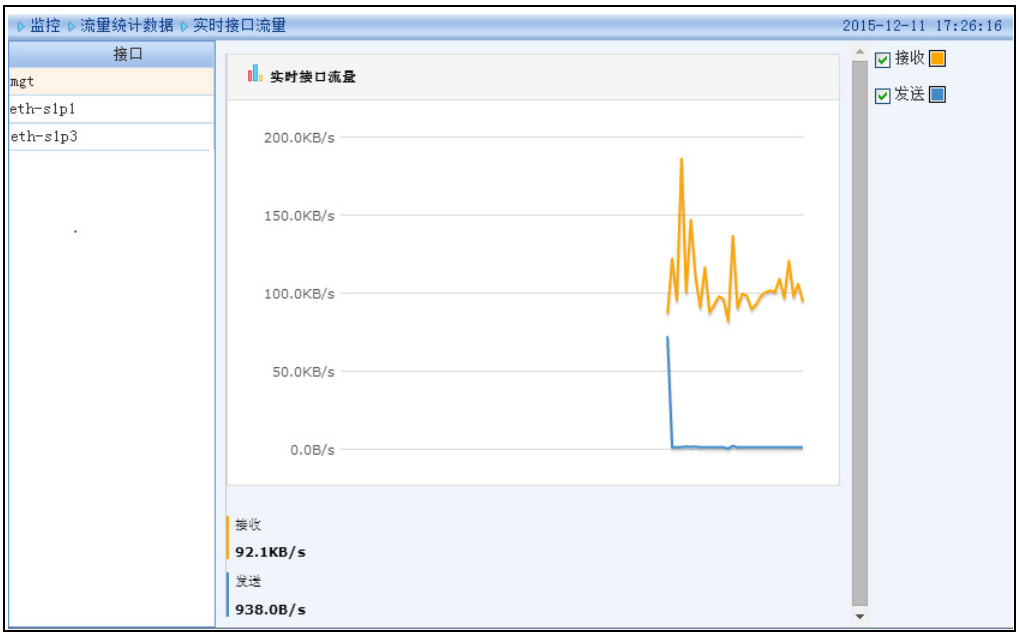
参数	说明
接口	接口名称。
链路状态	接口的连接状态。 • **绿色图标 —** 接口已连接。 • **红色图标 —** 连接已断开。
状态	接口的启禁用状态。
接收数据包数	接口接收的数据包数。
接收字节数	接口接收的字节数。
接收丢弃 / 错误 / 单播 / 非单播包数	接口接收的数据包中丢失 / 错误 / 单播 / 非单播包数。
发送数据包数	接口转发的数据包数。
发送字节数	接口转发的字节数。
发送丢弃 / 错误 / 单播 / 非单播包数	接口转发的数据包中丢失 / 错误 / 单播 / 非单播包数。

16.2.2 实时接口流量

NISG-IPS 提供以太网接口的实时流量统计信息，并以折线图的形式直观地显示出来。

选择**监控** > **流量统计数据** > **实时接口流量**，点击接口查看接口实时流量信息。

- 可通过折线图右上方的复选框设置要显示的内容，包括接收流量和发送流量。
- 鼠标指向折线图时，可以查看到具体时间点的接收和发送速率。
- 在折线图底部，可以查看到接口接收和发送的总体流量值。



提示：纵坐标轴表示接口流量大小，单位为 B/s、 KB/s、 MB/s 或 GB/s，可根据实际流量的大小进行自适应调节：如缺省情况下为字节 （B/s），当达到 1024 字节时则变为 KB/s，以此类推。

16.2.3 应用排名

选择**监控** > **流量统计数据** > **应用排名**，进入**应用排名**页面查看应用排名实时信息。管理员还可以设置应用显示条数、刷新方法 （手动和自动）及刷新时间间隔。

16.2.4 URL 排名

选择**监控** > **流量统计数据** > **URL 排名**，进入 **URL 排名**页面查看 URL 排名实时信息。管理员还可以设置 URL 显示条数、刷新方法 （手动和自动）及刷新时间间隔。

16.2.5 用户排名

选择**监控** > **流量统计数据** > **用户排名**，进入**用户排名**页面查看用户排名实时信息。管理员还可以设置用户显示条数、刷新方法 （手动和自动）及刷新时间间隔。

16.2.6 IP 地址排名

选择**监控** > **流量统计数据** > **IP 地址排名**，进入 **IP 地址排名**页面查看 IP 地址排名实时信息。管理员还可以设置 IP 地址显示条数、刷新方法 （手动和自动）及刷新时间间隔。

16.3 虚拟系统

显示所有虚拟系统的信息。关于虚拟系统的详细信息，请参见第 15 章，虚拟系统。

选择**监控** > **虚拟系统**。

表 265 虚拟系统参数

参数	说明
虚拟系统名称	虚拟系统的名称。
三层接口	虚拟系统包含的三层接口。
管理员	虚拟系统的管理员。
状态	虚拟系统的启禁用状态。
最大资源限制	虚拟系统分配到的资源百分比。
会话利用率	虚拟系统可以使用的会话表资源百分比。
策略利用率	虚拟系统可以使用的策略资源百分比。
NAT 利用率	虚拟系统可以使用的 NAT 资源百分比。
描述	虚拟系统的描述信息。

16.4 STP

NISG-IPS 提供 STP 生成树协议的监控功能，实时显示各个 VLAN 和实例中二层接口的工作状态。关于 STP 的详细信息，请参见 4.5 STP。

选择**监控** > **STP**。要查看 STP 监控信息，要先启用 STP。

表 266 STP 参数

参数	说明
VLAN	启用 STP 的 VLAN。
协议	VLAN 上开启的协议类型，包括 STP 和 RSTP。
二层接口	VLAN 包含的二层接口，包括二层以太网接口、二层 Channel 接口、二层冗余接口和二层虚拟接口。
状态	VLAN 中二层接口的工作状态，包括禁用、阻塞、侦听、学习、转发和丢弃。

16.5 路由

NISG-IPS 的路由监控功能使管理员能够了解缺省路由、策略路由及多播路由的实时信息。关于路由的详细信息，请参见第 5 章，路由。

选择**监控** > **路由**或点击**默认路由表**超链接进入**缺省路由**页面。

表 267 缺省路由参数

参数	说明
类型	路由类型，包括直连路由 （Connected）和静态路由 （Static）。
目的 IP 地址	数据包经过 NISG-IPS 发往的目的主机或目的网络 IPv4 或 IPv6 地址。
路由信息	路由过程的详细信息。

选择**监控** > **路由**或点击**策略路由**超链接进入**策略路由**页面。

表 268 策略路由策略参数

参数	说明
名称	策略路由策略名称。
目的 IP 地址	数据包经过 NISG-IPS 发往的目的主机或目的网络 IPv4 或 IPv6 地址。
路由信息	路由过程的详细信息。

选择**监控** > **路由**或点击**多播路由**超链接进入**多播路由**页面。

表 269 多播路由参数

参数	说明
源 IP 地址	多播数据包的源 IP 地址。
多播组 IP	目的多播组的 IP 地址。
入口接口	NISG-IPS 接收多播数据包的三层接口。
转发接口	NISG-IPS 转发多播数据包的三层接口。
TTL	多播数据包在被丢弃前能经过路由设备的最大数目。

16.6 NAT

NISG-IPS 的地址转换监控功能，管理员可以对实时地址转换信息进行监控。关于地址转换的详细信息，请参见第 8 章，地址转换。

选择**监控** > **NAT**。

表 270 地址转换参数

参数	说明
源地址	数据包初始源 IP 地址及转换后源 IP 地址 （括号内）。
目的地址	数据包初始目的 IP 地址及转换后目的 IP 地址 （括号内）。

16.7 ARP

NISG-IPS 提供对 ARP 表和代理 ARP 表的实时监控。关于更多信息，请参见 4.7 DNS 主机。

16.7.1 ARP 表

选择**监控** > **ARP** > **ARP 表**。点击**刷新**手动刷新 ARP 表信息。点击 进行关键字筛选。

表 271 ARP 表参数

参数	说明
IP 地址	目的主机 IP 地址。该 IP 地址不能是环回地址、多播地址、指向子网的广播地址或受限制的广播地址。
MAC 地址	与 IP 地址相对应的 MAC 地址。该 MAC 地址不能是广播或多播 MAC 地址。
类型	ARP 表项类型，包括静态、动态及代理三种。
状态	ARP 表项状态： • INCOMPLETE：已发送 ARP 请求但还没有应答。 • REACHABLE：可用。 • STALE：可用，但生存时间过长，应再次查询学习。 • FAILED：不可用，该状态不可见。
生存时间 （秒）	动态 ARP 表项存活时间。
接口	表项所属的三层接口。接口包括除隧道接口、 PPPoE 接口和环回接口以外三层接口。

16.7.2 代理 ARP 表

选择**监控** > **ARP** > 代理 **ARP 表**。点击**刷新**，手动刷新代理 ARP 表信息。点击 进行关键字筛选。

表 272 代理 ARP 表参数

参数	说明
IP 地址	目的主机 IP 地址。
MAC 地址	与 IP 地址对应的 MAC 地址。
接口	表项所属三层接口。接口包括除隧道接口、 PPPoE 接口和环回接口以外三层接口。

16.8 CAM

NISG-IPS 提供对 CAM 表的监控功能，显示概要信息和地址表实时信息。关于 CAM 的详细信息，请参见 4.4 CAM。

选择**监控** > **CAM**。点击**刷新**，手动刷新地址表信息。点击 进行关键字筛选。

表 273 统计信息参数

参数	说明
动态地址个数	CAM 表中当前动态表项的个数。
静态地址 （用户自定义）个数	CAM 表中当前静态表项的个数。
系统自身绑定地址个数	CAM 表中当前系统自身型的表项的个数。
多播地址个数	CAM 表中当前多播表项的个数。
MAC 地址数最大数	CAM 表中可以包含的最多 MAC 地址个数。
MAC 地址总数	CAM 表中当前 MAC 地址的合计个数。

表 274 地址表参数

参数	说明
目的地址	数据包的目的 MAC 地址。
地址类型	CAM 表项类型，包括 dynamic、 static、 local 和 multicast。
三层接口信息	表项所属 VLAN。
目的端口	接收数据包的目的端口。
超时时间 （秒）	动态 CAM 表项的超时时间，单位为秒。取值范围为 10-30000 秒，缺省为 300 秒。

16.9 DHCP IP 地址绑定状态

显示 NISG-IPS 中开启 DHCP 服务器功能的接口与其分配的 IP 地址的信息。关于 DHCP 的详细信息，请参见 4.12 DHCP 服务器。

选择**监控** > **DHCP IP 地址绑定状态**，查看 DHCP IP 地址绑定状态。可通过选择**类型**和**子网**对显示结果进行筛选。

表 275 DHCP IP 地址绑定状态参数

参数	说明
类型	所查看的 DHCP 类型。
子网	提供 IP 地址的作用域名称。
接口	与客户端连接的 NISG-IPS 接口。
IP 地址	DHCP 服务器分配给 DHCP 客户端的 IP 地址。
MAC 地址	与相应 IP 地址绑定的 DHCP 客户端的 MAC 地址。
DHCP 服务器	DHCP 服务器的 IP 地址。
结束时间	DHCP 客户端租用 IP 地址的结束时间。
租期 （分钟）	在作用域内分配的 IP 地址租期时间。

16.10 DHCPv6 客户端

NISG-IPS 提供对 DHCPv6 客户端的实时监控。关于 DHCPv6 的详细信息，请参见 4.15 DHCPv6。

选择**监控** > **DHCPv6 客户端**。

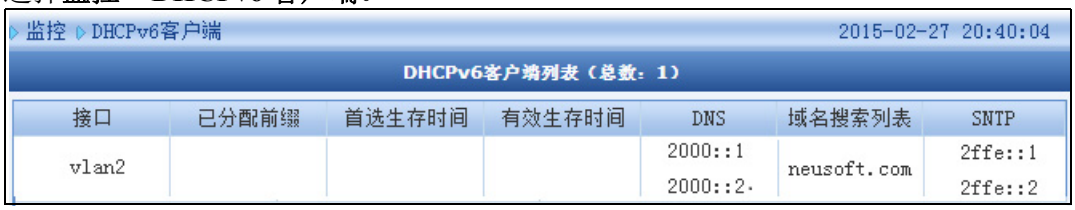


表 276 DHCPv6 客户端参数

参数	说明
接口	NISG-IPS 上开启 DHCP 客户端功能的接口。
已分配前缀	客户端获取到的前缀。
首选生存时间	获取到的前缀的首选生存期，单位为秒。
有效生存时间	获取到的前缀的有效生存期，单位为秒。
DNS	客户端获取到的 DNS 服务器地址。
域名搜索列表	客户端获取到的域名搜索列表。
SNTP	客户端获取的的 SNTP 服务器地址，用于同步客户端的系统时间。

16.11 DNS 缓存

NISG-IPS 提供对 DNS 动态缓存进行实时监控。关于 DNS 缓存的详细信息，请参见 4.9 DNS 缓存。

选择**监控** > **DNS 缓存**。

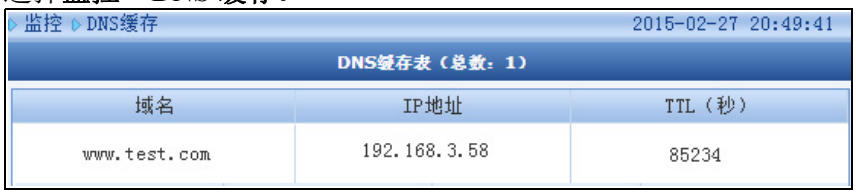


表 277 DNS 动态缓存参数

参数	说明
域名	动态缓存域名。
IP 地址	动态缓存条目中与域名对应的 IPv4 或 IPv6 地址。
TTL （秒）	动态缓存的生存时间。

16.12 高可用性

NISG-IPS 提供对虚拟路由器、虚拟路由器探测组及集群进行实时监控。关于高可用性的更多信息，请参见第 14 章，高可用性。

16.12.1 虚拟路由器

显示虚拟路由器及 IP 探测状态实时信息。

选择**监控** > **高可用性** > **虚拟路由器**。从 **VRID** 下拉框选择虚拟路由器标识号查看信息。

表 278 虚拟路由器参数

参数	说明
探测项	NISG-IPS 探测的项目，包括： • 选举接口：即本地和对端 NISG-IPS 之间通信的接口。 • 备用 IP：即本地和对端 NISG-IPS 的备用 IP 地址。 • 状态：即本地 NISG-IPS 和对端 NISG-IPS 的工作状态，即主和备。 • 运行时间：两次探测行为的时间间隔。 • 组 ID：虚拟路由器探测组 ID。
本地	本地 NISG-IPS 探测项目信息。
远程	远端 NISG-IPS 探测项目信息。

表 279 IP 探测状态参数

参数	说明
类型	IP 探测类型，包括 ARP Ping、 Ping 和 TCP Ping。
接口	IP 探测的当前设备上的某个三层接口。
IP 地址	NISG-IPS 通过指定接口要探测的目的 IP 地址。
端口	IP 探测类型为 TCP Ping 时需要的探测端口。
状态	表示探测的 IP 地址是否可达。 • ✔ — 探测地址可达。 • ✘ — 探测地址不可达。

16.12.2 虚拟路由器探测组

显示虚拟路由器探测组及 IP 探测状态实时信息。

选择**监控** > **高可用性** > **虚拟路由器探测组**。从**组 ID** 下拉框中选择虚拟路由器探测组查看监控信息。

表 280 虚拟路由器探测组

参数	说明
探测项	虚拟路由器探测组成员。
本地	本地 NISG-IPS 探测项目信息。
远程	对端 NISG-IPS 探测项目信息。

表 281 IP 探测状态参数

参数	说明
类型	IP 探测类型，包括 ARP Ping、 Ping 和 TCP Ping。
接口	IP 探测的当前设备上的某个三层接口。
IP 地址	NISG-IPS 通过指定接口要探测的目的 IP 地址。
端口	IP 探测类型为 TCP Ping 时需要的探测端口。
状态	表示探测的 IP 地址是否可达。 • ✔ — 探测地址可达。 • ✘ — 探测地址不可达。

16.12.3 集群

选择**监控** > **高可用性** > **集群**。

表 282 集群参数

参数	说明
探测项	NISG-IPS 探测的项目，包括： • 接口：集群内用于传递同步数据的网络接口。 • IP 地址：同步接口的 IP 地址。 • 集群状态：集群内成员的工作状态。 • 配置同步：配置信息同步的启用状态。 • 运行信息同步：运行信息同步的启用状态。 • 系统时间同步：系统时间同步的启用状态。
本地	本地 NISG-IPS 探测项目信息。
远程	对端 NISG-IPS 探测项目信息。

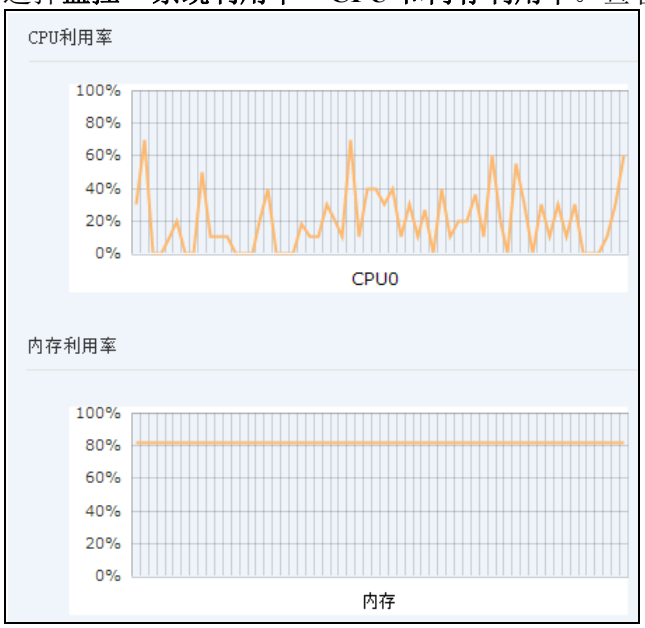
16.13 系统利用率

本节介绍 NISG-IPS 的系统资源利用率监控功能，管理员可以对 CPU 和内存及进程利用情况实时进行监控。

16.13.1 CPU 和内存利用率

CPU 和内存利用率显示当前系统的 CPU 和内存使用情况。

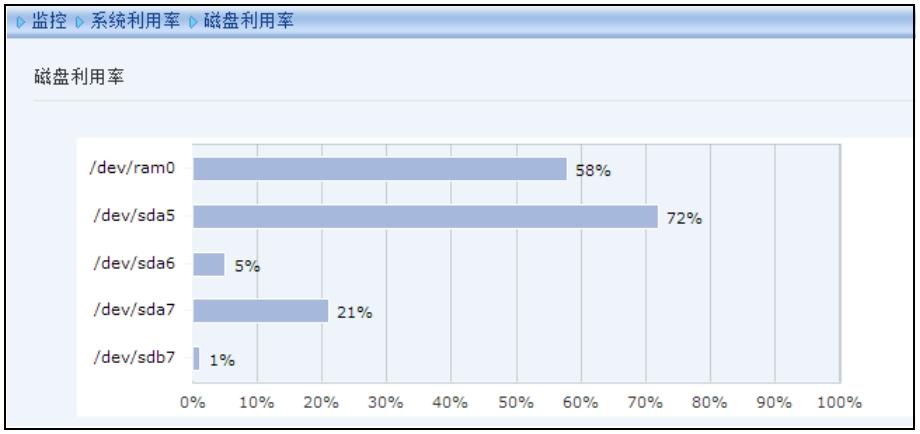
选择**监控** > **系统利用率** > **CPU 和内存利用率**。查看 CPU 和内存使用情况。



16.13.2 磁盘利用率

磁盘利用率监控显示当前系统磁盘的使用情况和日志存储空间的利用率。

选择**监控** > **系统利用率** > **磁盘利用率**，进入**磁盘利用率**页面查看磁盘和日志存储空间利用率。



16.13.3 进程

NISG-IPS 提供进程监控功能，管理员可以通过监视和控制进程来管理 CPU 和内存资源。

选择**监控** > **系统利用率** > **进程**。

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STATE	START	TIME	COMMAND
root	1	0.0	0.0	4076	620	?	Ss	Dec10	0:01	init [3]
root	2	0.0	0.0	0	0	?	S	Dec10	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	Dec10	0:00	[migration/0]
root	4	0.0	0.0	0	0	?	S	Dec10	0:00	[ksoftirqd/0]
root	5	0.0	0.0	0	0	?	S	Dec10	0:00	[watchdog/0]
root	6	0.0	0.0	0	0	?	S	Dec10	0:00	[migration/1]
root	7	0.0	0.0	0	0	?	S	Dec10	0:00	[ksoftirqd/1]
root	8	0.0	0.0	0	0	?	S	Dec10	0:00	[watchdog/1]
root	9	0.0	0.0	0	0	?	S	Dec10	0:02	[migration/2]
root	10	0.0	0.0	0	0	?	S	Dec10	0:00	[ksoftirqd/2]

表 283 进程参数

参数	说明
USER	发起或执行进行的用户。
PID	被内核使用的识别系统进行的唯一标识。
%CPU	活动进程占用 CPU 的百分比。
%MEM	活动进程占用内存的百分比。
VSZ	进程占用虚拟内存的大小，单位为 KB。
RSS	进程占用内存的大小，单位为 KB。
TTY	当前进程的控制终端设备类型。
STATE	进程的状态。
START	进程的启动时间。
TIME	进程目前的执行时间。
COMMAND	进程对应的命令。

16.14 在线用户

NISG-IPS 提供在线网络用户监控功能，管理员可以查询在线 WebAuth 用户和 SSL VPN 用户的实时信息。关于网络用户的更多信息，请参见 3.16 网络用户。

16.14.1 WebAuth 用户

选择**监控** > **在线用户** > **WebAuth 用户**。点击**刷新**，手动刷新在线 WebAuth 用户实时信息。勾选某个 WebAuth 用户对应的复选框，点击**离线**强制某个在线 WebAuth 用户下线。点击 进行关键字筛选。

表 284 WebAuth 用户参数

参数	说明
用户	在线的 WebAuth 用户。
IP 地址	在线 WebAuth 用户的登录 IP 地址。
在线时间 （秒）	WebAuth 用户的在线时长，单位为秒。
实时流量 （KB/ 秒）	在线 WebAuth 用户产生的实时流量。
流量 （KB）	在线 WebAuth 用户产生的总流量。
空闲时间 （秒）	在线 WebAuth 用户在空闲时间内不产生流量，则断开该网络连接，单位为秒。

16.14.2 SSL VPN 用户

选择**监控** > **在线用户** > **SSL VPN 用户**。点击**刷新**，手动刷新在线用户实时信息。勾选某个用户对应的复选框，点击**离线**，强制某个在线用户下线。点击 进行关键字筛选。

表 285 SSL VPN 用户参数

参数	说明
用户	在线的 SSL VPN 用户。
用户组	在线 SSL VPN 用户所属的用户组。
登录类型	在线 SSL VPN 用户的登录类型。 NISG-IPS 支持通过隧道和 Web-portal 登录。
隧道 / 入口页面	在线 SSL VPN 用户使用的隧道或入口页面。
IP 地址	SSL VPN 用户登录使用的 IP 地址。
在线时间 （秒）	SSL VPN 用户的在线时长，单位为秒。
发送 （字节）	在线 SSL VPN 用户发送的字节数。
接收 （字节）	在线 SSL VPN 用户接收到的字节数。
空闲时间 （秒）	在线 SSL VPN 用户在空闲时间内不产生网络流量，则断开该网络连接，单位为秒。

16.15 IPSec VPN 隧道

管理员可以对自动密钥隧道、手动密钥隧道、加速卡统计信息、软加密统计信息及隧道组进行监控。关于 IPSec VPN 隧道的详细信息，请参见第 13 章，虚拟专用网。

16.15.1 自动密钥隧道

选择**监控** > **IPSec VPN 隧道** > **自动密钥隧道**，在**隧道类型**下拉框中选择**全部**、**静态 IP 地址**、**动态 IP 地址**、**拨号用户或拨号用户组**，查看自动密钥隧道信息。当选择**拨号用户组**时，还可以选择要查看的用户组。点击，查看自动密钥隧道信息。

表 286 自动密钥隧道参数

参数	说明
名称	自动密钥隧道名称。
状态	自动密钥隧道状态。 • 开启：VPN 隧道可以转发数据包。 • 关闭：VPN 隧道不能转发数据包。 • 协商：VPN 隧道处于协商状态。
对端类型	自动密钥隧道对端类型，包括静态 IP 地址、动态 IP 地址，拨号用户和拨号用户组。
对端	自动密钥隧道对端标识信息。
隧道添加时间	自动密钥隧道的添加时间。
接收数据包数	自动密钥隧道接收的数据包个数。
发送数据包数	自动密钥隧道发送的数据包个数。

16.15.2 手动密钥隧道

选择**监控** > **IPSec VPN 隧道** > **手动密钥隧道**。点击，查看手动密钥隧道信息。

表 287 手动密钥隧道参数

参数	说明
名称	手动密钥隧道名称。
状态	手动密钥隧道的启禁用状态。
对端	手动密钥隧道的对端 IP 地址。
隧道创建时间	手动密钥隧道的添加时间。
接收数据包数	手动密钥隧道接收的数据包个数。
发送数据包数	手动密钥隧道发送的数据包个数。

16.15.3 加速卡统计

选择**监控** > **IPSec VPN 隧道** > **加速卡统计**。

表 288 加速卡统计信息

参数	说明
名称	加速卡的名称。
状态	加速卡的启禁用状态。
加密数据包数	加速卡加密的数据包数。
加密字节数	加速卡加密的字节数。
解密数据包数	加速卡解密的数据包数。
解密字节数	加速卡解密的字节数。
错误数	发送或接收加密数据包时，被检测到的错误包次数。

16.15.4 软加密统计

选择**监控** > **IPSec VPN 隧道** > **软加密统计**。

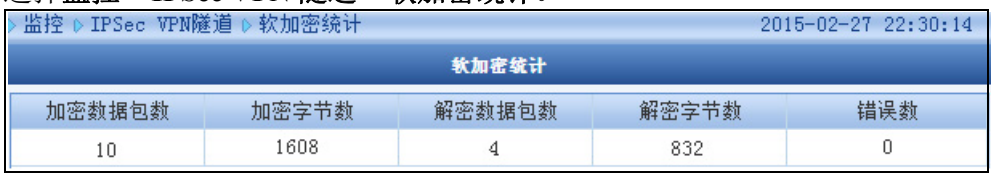


表 289 软加密统计信息

参数	说明
加密数据包数	软加密数据包的个数。
加密字节数	软加密字节数。
解密数据包数	软加密解密的数据包个数。
解密字节数	软加密解密的字节数。
错误数	发送或接收软加密数据包时，被检测到的错误包次数。

16.15.5 隧道组

选择**监控 > IPSec VPN 隧道 > 隧道组**。

表 290 隧道组参数

参数	说明
隧道组 ID	隧道组唯一标识。
启用	隧道组的使用状态： • ✗ — 隧道组未启用。 • ✓ — 隧道组已启用。
VPN 隧道	与当前隧道组关联的 IPSec VPN 隧道。
优先级	隧道组中 IPSec VPN 隧道的优先级。
VPN 隧道状态	隧道组中 IPSec VPN 隧道的当前状态。

16.16 GRE 隧道

NISG-IPS 中提供 GRE 隧道监控的相关数据，数据包括隧道状态、对端 IP 地址、隧道创建时间、接收和发送的数据包个数等信息。具体 GRE 隧道相关内容请参见 13.2.6 GRE 隧道。

选择**监控 > GRE 隧道**。

表 291 GRE 隧道参数

参数	说明
名称	GRE 隧道的名称
状态	GRE 隧道的状态，包括
对端	GRE 隧道对端的 IP 地址。
隧道创建时间	GRE 隧道的创建时间，为日期加时刻表达方式。
接收数据包数	GRE 隧道接收到数据包的数量。
发送数据包数	GRE 隧道发送的数据包的数量。

16.17 多播

NISG-IPS 中提供对 DVMRP 邻居及 IGMP Snooping 的实时信息进行监控。关于多播的详细信息，请参见 5.1.4 多播路由和 7.1.2 IGMP Snooping。

16.17.1 DVMRP 邻居

选择**监控** > **多播** > **DVMRP 邻居**。

表 292 DVMRP 邻居信息

参数	说明
IP 地址	DVMRP 邻居的 IP 地址。
超时时间	DVMRP 邻居的超时值，单位为秒。
生成 ID	DVMRP 邻居的多播路由标识。
版本	DVMRP 协议的版本。
索引	DVMRP 的邻居编号。

16.17.2 IGMP Snooping 状态

选择**监控** > **多播** > **IGMP Snooping 状态**。

表 293 IGMP Snooping 状态信息

参数	说明
VLAN	接收多播数据包的接口信息。
状态	VLAN 中 IGMP Snooping 状态，包括开启和关闭。
二层接口	VLAN 包含的二层接口。
IGMP 版本	IGMP 的版本号有三种，分别是 v1、 v2 和自动。缺省版本为自动。
IGMP 模式	和 NISG-IPS 直接连接的网络的类型： • 多播路由器：与 NISG-IPS 相连的是多播路由器。多播数据包向该类型的接口发送。 • 主机：该类型的接口相连的是主机。 • 自动协商：接口通过接收的数据包动态地识别网络类型。 默认类型是自动协商。
多播 CAM 表	VLAN 对应的多播 CAM 表。

16.18 报警 / 日志

管理员可以对系统日志、 URL 过滤报警、 IPS 及应用控制报警进行实时监控。

16.18.1 系统日志

选择**监控** > **报警 / 日志** > **系统日志**。点击**刷新**获取最新的系统日志信息。点击 进行关键字筛选。

表 294 系统日志参数

参数	说明
日期时间	系统日志产生的日期和时间。
级别	系统日志的安全等级，包括 Emergency、 Alert、 Critical、 Error、 Waring、 Notice、 Informational 和 Debugging。
类型	产生系统日志的模块类型，包括 Manage、 Session、 NAT、 FW、 VPN、 IPS、 URL Filtering 和 Application Control。
用户	触发日志产生的用户。
重复次数	系统日志的重复次数。 NISG-IPS 对重复产生的日志进行合并标明日志产生的次数。
日志信息	系统日志主体部分，描述事件具体信息。

16.18.2 URL 过滤报警

选择**监控** > **报警 / 日志** > **URL 过滤报警**。点击**刷新**获取最新的 URL 过滤报警信息。点击 进行关键字筛选。

表 295 URL 过滤报警参数

参数	说明
日期时间	日志产生的日期和时间。
源 IP	HTTP 请求的源 IP 地址。
URL	HTTP 请求的 URL 信息。
分类	HTTP 请求的分类信息。
信息	HTTP 请求被隔离的详细信息。
动作	对 HTTP 请求的处理所执行的动作，包括放行和阻断。

16.18.3 IPS 报警

选择**监控** > **报警 / 日志** > **IPS 报警**。点击**刷新**获取最新的 IPS 报警信息。点击 进行关键字筛选。

表 296 IPS 报警参数

参数	说明
日期时间	日志产生的日期和时间。
配置防护文件	攻击匹配的攻击签名规则所引用的防护配置。
源 IP	发起攻击的源 IP 地址。
源端口	发起攻击的源端口。
目的 IP	攻击目标的目的 IP 地址。
目的端口	攻击目标的目的端口。
名称	攻击匹配的攻击签名规则集名称。
类别	攻击匹配的攻击签名规则类别。
严重级别	匹配攻击签名规则的攻击的严重程度，包括 High （Critical）、 Medium （Error）、 Low （Warning）和 Info （Notification）。
服务	匹配攻击签名规则的攻击使用的服务。
规则 ID	攻击匹配的攻击签名规则标识。
信息	IPS 报警的详细信息。
动作	对攻击行为的处理所执行的动作，包括放行、阻断和拒绝。

16.18.4 应用控制报警

选择**监控** > **报警 / 日志** > **应用控制报警**。点击**刷新**获取最新的应用控制报警信息。点击 进行关键字筛选。

表 297 应用控制报警参数

参数	说明
日期时间	日志产生的日期和时间。
配置防护文件	应用请求匹配的应用控制策略所引用的防护配置。
源 IP	应用请求的源 IP 地址。
源端口	应用请求的源端口。
目的 IP	应用请求的目的 IP 地址。
目的端口	应用请求的目的端口。
协议类型	应用使用的协议类型，如 DNS、 HTTP、 SMTP、 POP3、 IMAP 和 FTP。
应用	匹配应用控制策略的应用名称。
分类	应用所属分类，包括交际类、商务类、多媒体类、网络构建类、通用互联网类。
子分类	应用所属子分类，包括 IP 协议、网络共享等。
风险等级	应用对系统的潜在风险等级。
动作	对该应用请求的处理所执行的动作，包括放行和阻断。

17 报表

本章介绍 NISG-IPS 的报表特性。章节结构如下：

17.1 概述

报表是基于 WebUI 的一种应用，统计 NISG-IPS 记录的实时数据，最终以图表 （线图、条形图、圆饼图和表格）的形式展现给用户。

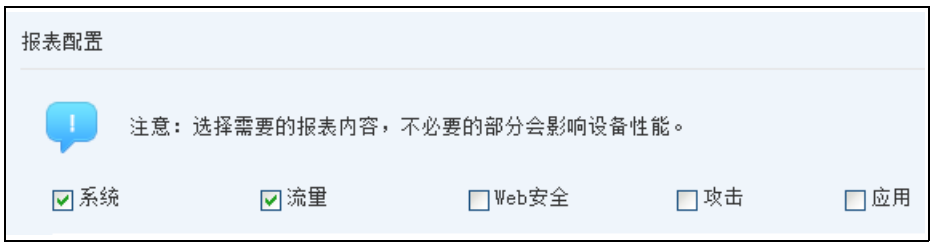
报表可记录以下类别相关的数据：系统、流量、 Web 安全、攻击、应用和用户。管理员可以制定具体的报表生成计划，使 NISG-IPS 按照计划在规定的时间自动地生成报表，并可以通过 SMTP 服务器将生成的报表以邮件方式发送给特定用户。

17.2 基本配置步骤

本节介绍报表相关的基本配置步骤：

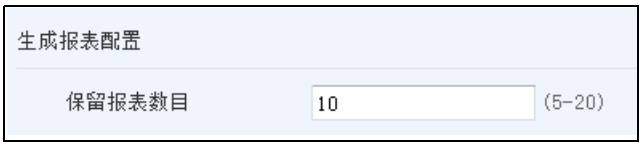
17.2.1 配置常规设置

1. 选择**监控 > 报表 > 常规设置**。
2. 选择报表要记录的数据类型。



3. 设置 SMTP 服务器及发件人信息。

4. 设置保留报表数目。



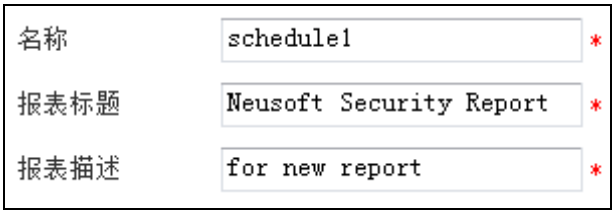
5. 使用默认 Logo 或者点击**导入**上传 Logo，导入后的 Logo 将在**预览**区域显示。

6. 点击**确定**。
7. 点击 。

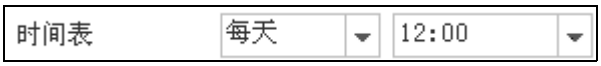
17.2.2 创建报表生成计划

每个虚拟系统最多支持 10 个报表计划。

1. 选择**监控 > 报表 > 计划**。
2. 点击**新建**，设置报表基本信息。

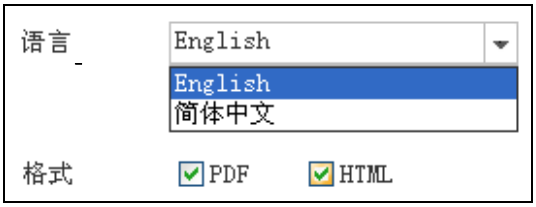


3. 设置报表生成时间表，可以设置每天、每周、每月生成。

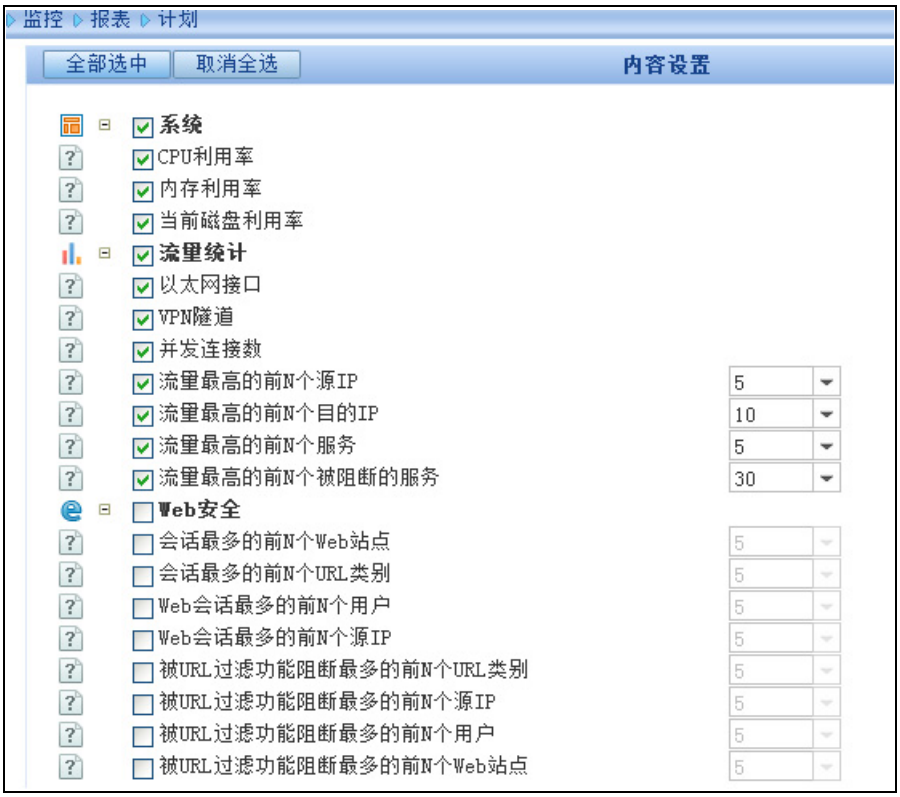


4. 添加报表收件人。

5. 设置报表显示语言及格式。



6. 设置报表要记录的具体内容。



提示：在**内容设置**区域选择记录的内容所属的类别在**常规设置 > 报表配置**区域也要选择，否则对应内容将不会在报表中显示。

7. 设置要记录的用户统计信息。

需要首先在**常规设置** > **报表配置**区域勾选**流量**。如需额外为每类用户显示前 3 个用户的前 5 个应用信息，点击，在弹出的窗口中，勾选**显示前 3 个用户应用统计**复选框。

8. 选择特定用户或 IP 地址要记录的内容。
   a. 点击**特定用户**对应的，在弹出的**用户列表**区域点击**添加**，设定用户或 IP 地址（最多 5 个）。
   b. 勾选要记录的内容所对应的复选框。

提示：只可以选择 NISG-IPS 上已存在的网络用户。

9. 点击**确定**。
10. 点击 。
11. 查看报表示例图。
    - 点击 图标，查看相应的报表统计信息的示例图。
    - 点击页面底部的**查看报表样例**按钮查看报表样例，也可以将此报表样例保存到本地。
12. NISG-IPS 提供一个报表计划预览日历，管理员可以在列表中查看已创建的计划，也可以在日历中查看到不同类型的报表计划：D代表每天计划，W代表每周计划，M代表每月计划。

17.2.3 管理报表结果

1. 选择**监控** > **报表** > **结果**。
2. 删除报表结果或下载报表结果至本地。

3. 查看报表结果。

所有报表结果按照生成时间倒序显示在**报表结果列表**中。关于报表结果的详细信息，请参见 17.3.4 全局内容参数和 17.3.5 特定用户内容参数。


Neusoft Security Report

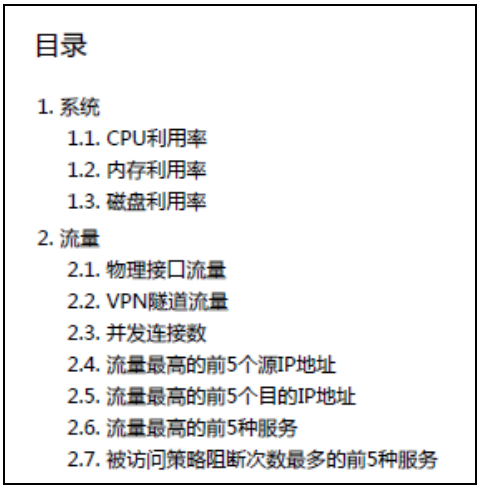
报表生成设备: Neusoft(序列号: 000C29FB8FF0)

报表生成时间: 2012-08-18 02:00:01

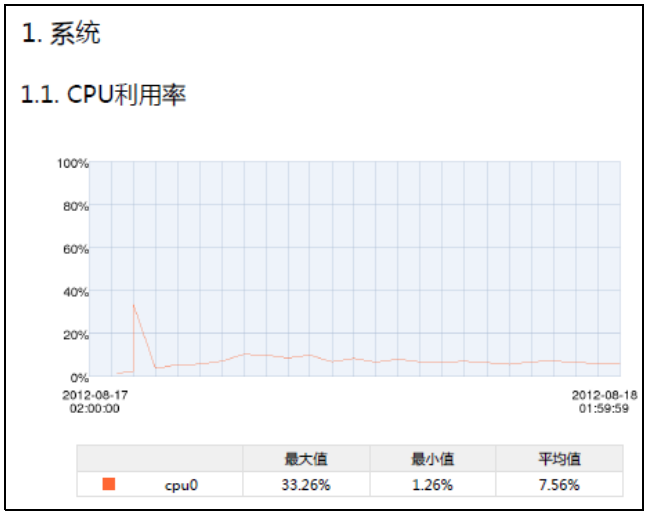
报表计划时间: 2012-08-17 02:00:00~2012-08-18 01:59:59

报表描述: Report

Neusoft


目录

1. 系统
   1.1. CPU利用率
   1.2. 内存利用率
   1.3. 磁盘利用率
2. 流量
   2.1. 物理接口流量
   2.2. VPN隧道流量
   2.3. 并发连接数
   2.4. 流量最高的前5个源IP地址
   2.5. 流量最高的前5个目的IP地址
   2.6. 流量最高的前5种服务
   2.7. 被访问策略阻断次数最多的前5种服务


1. 系统

1.1. CPU利用率

100%
80%
60%
40%
20%
0%
2012-08-17 02:00:00
2012-08-18 01:59:59

	最大值	最小值	平均值
cpu0	33.26%	1.26%	7.56%

4. 如果管理员设置了 SMTP 服务器信息，NISG-IPS 可以将生成的报表以邮件方式发送给指定用户。

17.3 配置参数说明

本节介绍报表的配置参数，包括：

- 17.3.1 常规设置
- 17.3.2 报表计划参数
- 17.3.3 报表结果参数
- 17.3.4 全局内容参数
- 17.3.5 特定用户内容参数

17.3.1 常规设置

表 298 常规设置配置信息

参数	说明
报表配置	报表可以记录以下类别相关的数据：系统、流量、 Web 安全、攻击及应用。
地址	SMTP 服务器地址，域名或 IP 地址。 SMTP 服务器用于将生成的报表通过邮件发送给用户。
端口	SMTP 服务器端口号， 1-65535。
安全连接	用于启用或禁用 SSL 加密，缺省为禁用。如果启用安全连接，服务器端口号需设置为 465。
发送人	发件人邮件地址， 5-255 字节。
身份认证	用于启用或禁用发送人身份认证，缺省为禁用。 如果 SMTP 服务器要求身份认证，则必须启用身份认证并配置发件人用户名和密码： • **用户名：**长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。 • **密码：1**-255 个字节， UTF-8 字符。不能包含空格和问号。
主题	邮件主题。长度 0-64 字节， UTF-8 字符。不能包含以下字符：？' \ 。
保留报表数目	设置可保留的报表数目， 5-20 条，缺省为 10 条。
Logo 配置	报表封皮使用的 Logo。 • **使用默认：**默认使用系统自带的 Logo。 • **导入：**从本地导入 JPG 格式的图片。上传的图片必须小于 100 K，分辨率至少为 96 dpi。如果导入多个图片，系统仅保留最后一个。

17.3.2 报表计划参数

表 299 报表计划配置信息

参数	说明
名称	长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。 同一虚拟系统内的报表名称须唯一。
报表标题	长度 1-63 个字节， UTF-8 字符。
报表描述	长度 0-255 个字节， UTF-8 字符。不能包含以下字符：？" ' \ < > & 。
时间表	用于设置报表生成时间，缺省的时间表为每天 01:00 生成报表。 • 如选择每周生成，缺省为每周一 01:00。 • 如选择每月生成，缺省为每月 1 日 01:00。
收件人列表	列出报表收件人邮件地址。报表生成后， NISG-IPS 会自动将生成的报表发送给收件人。 管理员最多可以添加 32 个收件人地址。
语言	报表显示语言，英文或简体中文，缺省为英文。

表 299 报表计划配置信息 (*续*)

参数	说明
格式	报表输出格式， PDF 或 HTML 或两种格式都选。
内容设置	设置在报表中要显示的内容。 用户可以选择与以下主题相关的内容：系统、流量统计、 Web 安全、攻击、应用以及用户。 所有内容选项在缺省情况下都是禁用的。关于每个选项的信息，请参见 17.3.4 全局内容参数和 17.3.5 特定用户内容参数。

17.3.3 报表结果参数

表 300 报表结果配置信息

参数	说明
时间	报表生成的时间。
名称	报表生成计划中配置的报表名称。
状态	显示报表是否生成成功。 状态包括：成功、失败、正在生成中。
信息	显示以下两种报表生成信息： • 报表生成失败。 • 连接 SMTP 邮件服务器失败。 “-” 表示报表已成功生成或正在生成中。
报告文件	为管理员提供下载报表的链接。

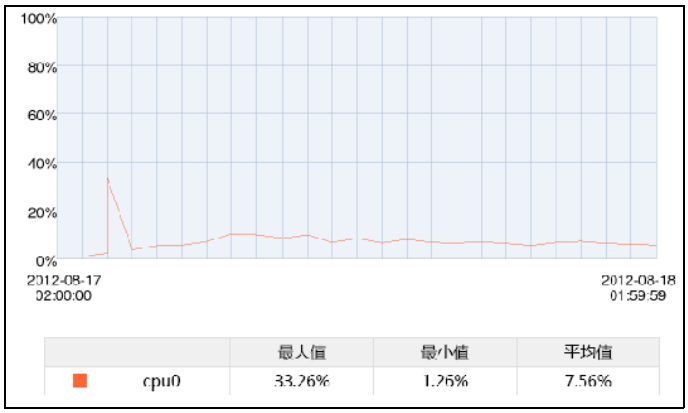
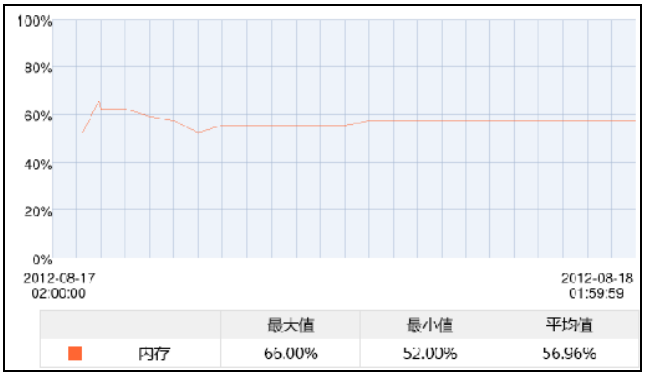
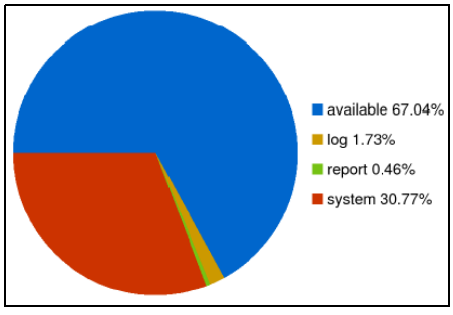
17.3.4 全局内容参数

本节介绍报表中显示的具体内容并给出报表示例。管理员可以选择与以下主题相关的内容：

- 17.3.4.1 系统
- 17.3.4.2 流量统计
- 17.3.4.3 Web 安全
- 17.3.4.4 攻击
- 17.3.4.5 应用
- 17.3.4.6 用户

17.3.4.1 系统

表 301 系统信息

类型	描述
CPU 利用率	NISG-IPS 每 5 分钟统计一次 CPU 利用率并显示平均值。如果系统有多个内核或多个 CPU，那么每个内核或 CPU 会单独显示。  线图中纵坐标为 CPU 利用率百分比。图中绘制图的点为 5 分钟内的均值。
内存利用率	NISG-IPS 每 5 分钟统计一次系统内存利用率并显示平均值。  线图中纵坐标为内存利用率百分比。图中绘制图的点为 5 分钟内的均值。
当前磁盘利用率	NISG-IPS 统计生成报表时的磁盘使用情况。 

17.3.4.2 流量统计

表 302 流量信息

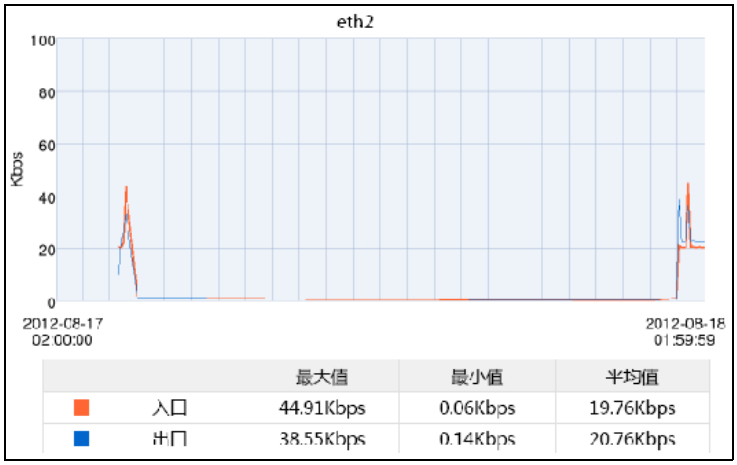
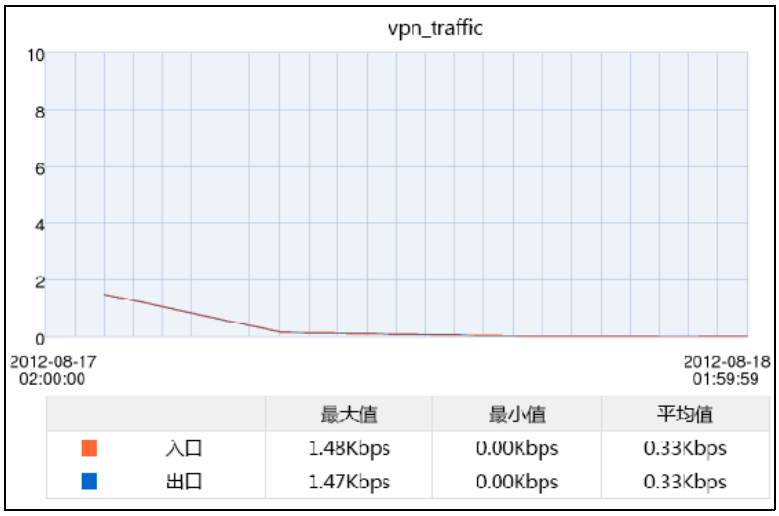
类型	描述
以太网接口	NISG-IPS 每 5 分钟统计一次入口和出口以太网接口的流量信息。  线图中绘制图的点为 5 分钟内的均值。
VPN 隧道	NISG-IPS 每五分钟统计一次 VPN 隧道入口和出口接口的流量信息。报表中只显示自动密钥隧道配置中前 10 个已经启用的网段到网段隧道的信息。  线图中绘制图的点为 5 分钟内的均值。

表 302 流量信息 (*续*)

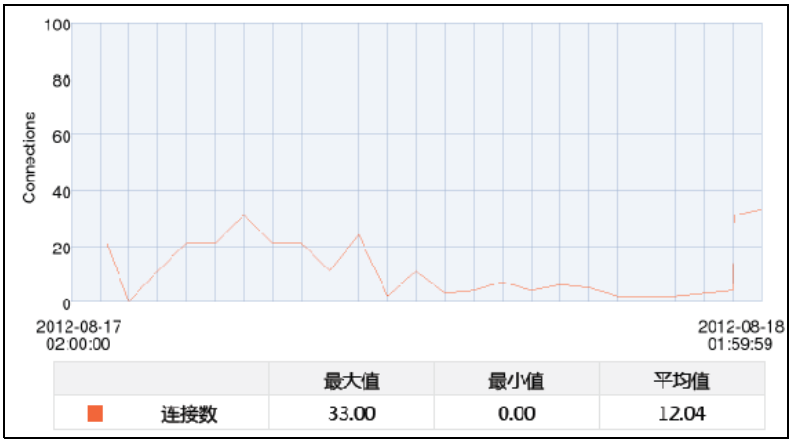
类型	描述
并发连接数	NISG-IPS 每 5 分钟统计一次并发连接总数。  线图中绘制图的点为 5 分钟内的总值。
流量最高的前 N 个源 IP	NISG-IPS 统计流量最高的前 N 个源 IP 地址的信息。 序列 | 源IP地址 | 流量(KB) | 百分比 1 | 192.168.111.2 | 1902 | 8.34% 2 | 192.168.111.3 | 1706 | 7.48% 3 | 192.168.111.4 | 1560 | 6.84% 4 | 192.168.111.5 | 1329 | 5.83% 5 | 192.168.111.6 | 1290 | 5.66% 说明： • 流量 （KB）：来自某一特定源 IP 地址的总流量。 • 百分比：来自某一特定源 IP 地址的总流量占系统总流量的比例。
流量最高的前 N 个目的 IP	NISG-IPS 统计流量最高的前 N 个目的 IP 地址的信息。 序列 | 目地IP地址 | 流量(KB) | 百分比 1 | 192.168.101.2 | 1902 | 8.34% 2 | 192.168.101.3 | 1706 | 7.48% 3 | 192.168.101.4 | 1560 | 6.84% 4 | 192.168.101.5 | 1329 | 5.83% 5 | 192.168.101.6 | 1290 | 5.66% 说明： • 流量 （KB）：发往某一特定目的 IP 地址的总流量。 • 百分比：发往某一特定目的 IP 地址的总流量占系统总流量的比例。

表 302 流量信息 (*续*)

类型	描述
流量最高的前 N 个服务	NISG-IPS 统计流量最高的前 N 种服务的信息。 序列 | 端口 | 服务名称 | 流量(KB) | 百分比 1 | UDP:12 | UDP_ANY | 1840 | 8.07% 2 | TCP:13 | TCP_ANY | 1577 | 6.91% 3 | UDP:14 | UDP_ANY | 1376 | 6.03% 4 | TCP:15 | TCP_ANY | 1157 | 5.07% 5 | UDP:16 | UDP_ANY | 1104 | 4.84% 说明： • 端口：目的端口号。如果无端口则显示协议号，如 Other：44。 • 服务名称：使用特定目的端口的服务对象的名称。 • 流量 （KB）：发往某一特定目的端口的总流量。 • 百分比：发往某一特定目的端口的总流量占系统总流量的比例。
流量最高的前 N 个被阻断的服务	NISG-IPS 统计被访问策略阻断次数最多的前 N 个服务。 序列 | 端口 | 服务 | 阻断次数 | 百分比 1 | OTHER:1231 | | 23 | 10.95% 2 | OTHER:1232 | | 19 | 9.05% 3 | OTHER:1235 | | 16 | 7.62% 4 | OTHER:1240 | | 12 | 5.71% 5 | OTHER:1247 | | 11 | 5.24% 说明： • 阻断次数：某一特定目的端口被访问策略阻断的总次数。 • 百分比：某一特定目的端口被访问策略阻断的总次数占所有端口被访问策略阻断的总次数的比例。

17.3.4.3 Web 安全

表 303 Web 安全信息

类型	描述
会话最多的前 N 个 Web 站点	被访问次数最多的前 N 个网站的信息。 序列 / 域名 / 会话数 / 百分比 1 / www.baidu.com_1 / 23 / 11.56% 2 / www.baidu.com_2 / 19 / 9.55% 3 / www.baidu.com_3 / 16 / 8.04% 4 / www.baidu.com_4 / 13 / 6.53% 5 / www.baidu.com_5 / 12 / 6.03% 说明： • 会话数：某一特定网站被访问的总次数。 • 百分比：某一特定网站被访问的总次数占所有网站被访问的总次数的比例。
会话最多的前 N 个 URL 类别	被访问次数最多的前 N 种 URL 类别的信息。 序列 / URL分类 / 会话数 / 百分比 1 / 烟酒 / 39 / 8.57% 2 / 匿名技术 / 33 / 7.25% 3 / 艺术 / 31 / 6.81% 4 / 商业 / 27 / 5.93% 5 / 运输 / 26 / 5.71%
Web 会话最多的前 N 个用户	访问 Web 次数最多的前 N 名用户的信息。 序列 / 用户名 / 会话数 / 百分比 1 / test1 / 45 / 22.61% 2 / test2 / 41 / 20.60% 3 / test3 / 33 / 16.58% 4 / test4 / 30 / 15.08% 5 / user*default / 26 / 13.07% 说明： 百分比：某一特定用户访问 Web 的总次数占所有用户访问 Web 的总次数的比例。
Web 会话最多的前 N 源 IP	访问 Web 次数最多的前 N 个源 IP 地址的信息。 序列 / 源IP地址 / 会话数 / 百分比 1 / 192.168.60.2 / 31 / 15.58% 2 / 192.168.60.3 / 27 / 13.57% 3 / 192.168.60.4 / 23 / 11.56% 4 / 192.168.60.5 / 19 / 9.55% 5 / 192.168.60.6 / 18 / 9.05% 说明： 百分比：某一特定源 IP 地址访问 Web 的总次数占所有 Web 访问总次数的比例。

表 303 Web 安全信息 (*续*)

类型	描述
被 URL 过滤功能阻断最多的前 N 个 URL 类别	被 URL 过滤功能阻断次数最多的前 N 个 URL 类别的信息。 序列 | URL分类 | 阻断的URL过滤 | 百分比 1 | 烟酒 | 39 | 8.57% 2 | 匿名技术 | 33 | 7.25% 3 | 艺术 | 31 | 6.81% 4 | 商业 | 27 | 5.93% 5 | 运输 | 26 | 5.71% 说明： • 阻断的 URL 过滤：某一特定 URL 类别被 URL 过滤功能阻断的总次数。 • 百分比：某一特定 URL 类别被 URL 过滤功能阻断的总次数占所有被 URL 过滤功能阻断的 URL 类别的总次数的比例。
被 URL 过滤功能阻断最多的前 N 个源 IP	被 URL 过滤功能阻断次数最多的前 N 个源 IP 地址的信息。 序列 | 源IP地址 | 阻断的URL过滤 | 百分比 2 | 192.168.60.3 | 52 | 11.43% 3 | 192.168.60.4 | 50 | 10.99% 4 | 192.168.60.5 | 46 | 10.11% 5 | 192.168.60.6 | 45 | 9.89%
被 URL 过滤功能阻断最多的前 N 个用户	被 URL 过滤功能阻断次数最多的前 N 个用户的信息。 序列 | 用户名 | 阻断的URL过滤 | 百分比 1 | test1 | 90 | 19.78% 2 | test2 | 84 | 18.46% 3 | test3 | 76 | 16.70% 4 | test4 | 71 | 15.60% 5 | user*default | 68 | 14.95%
被 URL 过滤功能阻断最多的前 N 个 Web 站点	被 URL 过滤功能阻断次数最多的前 N 个 Web 站点的信息。 序列 | 域名 | 阻断的URL过滤 | 百分比 1 | www.baidu.com_6 | 12 | 18.18% 2 | www.baidu.com_12 | 8 | 12.12% 3 | www.baidu.com_18 | 7 | 10.61% 4 | www.baidu.com_30 | 3 | 4.55% 5 | www.baidu.com_24 | 3 | 4.55%

17.3.4.4 攻击

表 304 攻击信息

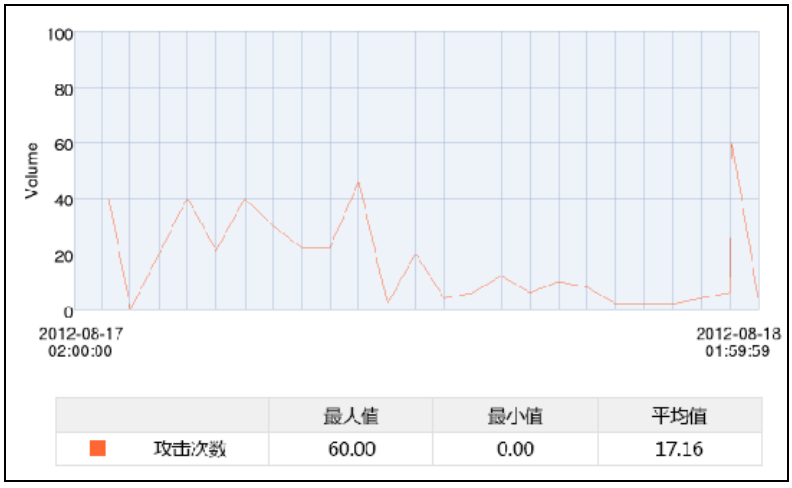
类型	描述
攻击事件统计	NISG-IPS 每 5 分钟统计一次攻击发生的总数。  线图中纵坐标为攻击发生的总次数。图中绘制图的点为 5 分钟内的总次数。
检测到攻击次数最多的前 N 个攻击者	被检测到攻击次数最多的前 N 个攻击者的信息。 序列 | 攻击者 | 检测到的攻击数量 | 百分比 1 | 10.168.1.2 | 31 | 8.40% 2 | 192.169.3.2 | 29 | 7.86% 3 | 10.168.1.3 | 27 | 7.32% 4 | 192.169.2.3 | 24 | 6.50% 5 | 10.168.1.4 | 22 | 5.96% 说明： • 攻击者：攻击者的 IP 地址。 • 检测到的攻击数量：某一特定攻击者发起攻击的总次数。 • 百分比：某一特定攻击者发起攻击的总次数占检测到攻击总次数的比例。
检测到攻击次数最多的前 N 个主机	被攻击次数最多的前 N 个主机的信息。 序列 | 受攻击主机 | 检测到的攻击数量 | 百分比 1 | 10.2.1.2 | 31 | 8.40% 2 | 192.169.2.2 | 29 | 7.86% 3 | 10.2.1.3 | 27 | 7.32% 4 | 192.169.3.3 | 24 | 6.50% 5 | 10.2.1.4 | 22 | 5.96%

表 304 攻击信息 (*续*)

类型	描述
检测到攻击次数最多的前 N 个服务	被攻击次数最多的前 N 个服务的信息。 序列 | 端口 | 服务 | 检测到的攻击数量 | 百分比 1 | TCP:280 | TCP_ANY | 23 | 8.42% 2 | OTHER:1231 | | 23 | 8.42% 3 | OTHER:1232 | | 19 | 6.96% 4 | UDP:281 | UDP_ANY | 18 | 6.59% 5 | OTHER:1235 | | 15 | 5.49% 说明： • 端口：目的端口号。如果无端口则显示协议号，如 Other：44。 • 服务：使用特定目的端口的服务对象的名称。
被 IPS 检测到次数最多的前 N 个攻击者	被 IPS 检测出发起攻击次数最多的前 N 个攻击者的信息。 序列 | 攻击者 | 检测到的攻击数量 | 百分比 1 | 10.168.1.2 | 31 | 8.40% 2 | 192.169.3.2 | 29 | 7.86% 3 | 10.168.1.3 | 27 | 7.32% 4 | 192.169.2.3 | 24 | 6.50% 5 | 10.168.1.4 | 22 | 5.96% 说明： • 检测到的攻击数量：IPS 检测出的某一特定攻击者发起攻击的总次数。 • 百分比：IPS 检测出的某一特定攻击者发起攻击的总次数占 IPS 检测到攻击总次数的比例。
被 IPS 检测到次数最多的前 N 个被攻击的主机	被 IPS 检测到被攻击次数最多的前 N 个主机的信息。 序列 | 受攻击主机 | 检测到的攻击数量 | 百分比 1 | 192.169.2.2 | 29 | 16.29% 2 | 192.169.3.3 | 24 | 13.48% 3 | 192.169.2.4 | 21 | 11.80% 4 | 192.169.3.5 | 17 | 9.55% 5 | 192.169.2.6 | 16 | 8.99%
被 IPS 检测到次数最多的前 N 个服务	被 IPS 检测到被攻击次数最多的前 N 个服务的信息。 序列 | 端口 | 服务 | 检测到的攻击数量 | 百分比 1 | TCP:280 | TCP_ANY | 23 | 28.05% 2 | UDP:281 | UDP_ANY | 18 | 21.95% 3 | TCP:285 | TCP_ANY | 10 | 12.20% 4 | UDP:286 | UDP_ANY | 9 | 10.98% 5 | TCP:290 | TCP_ANY | 5 | 6.10%

表 304 攻击信息 (*续*)

类型	描述
被 IPS 检测到次数最多的前 N 个攻击类型	被 IPS 检测出发起攻击次数最多的前 N 个攻击类型的信息。 序列 | 攻击类型 | 检测到的攻击数量 | 百分比 1 | 未知 | 104 | 58.43% 2 | 输入验证错误 | 44 | 24.72% 3 | 跨站脚本(CSS/XSS) | 30 | 16.85%
被 IPS 检测到次数最多的前 N 个客户端	客户端保护中 IPS 检测到被攻击次数最多的前 N 个客户端的信息。 序列 | 客户端IP | 检测到的攻击数量 | 百分比 1 | 192.169.2.2 | 29 | 30.85% 2 | 192.169.2.4 | 21 | 22.34% 3 | 192.169.2.6 | 16 | 17.02% 4 | 192.169.2.10 | 14 | 14.89% 5 | 192.169.2.8 | 14 | 14.89% 说明： • 检测到的攻击数量：客户端保护中 IPS 检测出的某一特定主机被攻击的总次数。 • 百分比：客户端保护中 IPS 检测出的某一特定主机被攻击的总次数占客户端保护中 IPS 检测出攻击的总次数的比例。
被 IPS 检测到次数最多的前 N 个服务器	服务器保护中 IPS 检测到被攻击次数最多的前 N 个服务器的信息。 序列 | 服务器IP/域名 | 检测到的攻击数量 | 百分比 1 | 192.169.3.3 | 24 | 28.57% 2 | 192.169.3.5 | 17 | 20.24% 3 | 192.169.3.7 | 15 | 17.86% 4 | 192.169.3.1 | 14 | 16.67% 5 | 192.169.3.9 | 14 | 16.67% 说明： • 检测到的攻击数量：服务器保护中 IPS 检测出的某一特定服务器被攻击的总次数。 • 百分比：服务器保护中 IPS 检测出的某一特定服务器被攻击的总次数占服务器保护中 IPS 检测到攻击总次数的比例。

17.3.4.5 应用

表 305 应用信息

类型	描述
会话最多的前 N 个应用	会话数最多的应用的信息。 序列 | 应用 | 会话数 | 百分比 1 | 魔兽世界 | 23 | 10.04% 2 | NNTP | 19 | 8.30% 3 | Daytime | 16 | 6.99% 4 | IMAP | 13 | 5.68% 5 | MSN | 12 | 5.24% 说明： • 应用：应用的名称。 • 会话数：某一特定应用的会话总数。 • 百分比：某一特定应用的会话总数占所有应用会话数的比例。
会话最多的前 N 个应用类别	会话数最多的前 N 种应用类别的信息。 序列 | 应用分类 | 会话数 | 百分比 1 | 即时通讯 | 39 | 17.03% 2 | 游戏 | 30 | 13.10% 3 | 管理软件 | 30 | 13.10% 4 | 互联网实用类 | 27 | 11.79% 5 | 电子邮件 | 23 | 10.04%
流量最高的前 N 个应用	产生流量最高的前 N 个应用的信息。 序列 | 应用 | 流量(KB) | 百分比 1 | POP2 | 2923 | 12.82% 2 | POP3 | 2538 | 11.13% 3 | 魔兽世界 | 2361 | 10.35% 4 | NNTP | 2166 | 9.50% 5 | Daytime | 2137 | 9.37% 说明： • 流量 （KB）：某一特定应用产生的总流量。 • 百分比：某一特定应用产生的总流量占所有应用流量的比例。
流量最高的前 N 个应用类别	产生流量最高的前 N 个应用类别的信息。 序列 | 应用分类 | 流量(KB) | 百分比 1 | 电子邮件 | 8619 | 37.79% 2 | 即时通讯 | 4176 | 18.31% 3 | 游戏 | 2361 | 10.35% 4 | 互联网实用类 | 2166 | 9.50% 5 | 管理软件 | 2137 | 9.37%

表 305 应用信息 (*续*)

类型	描述
被应用控制阻断次数最多的前 N 个应用	被应用控制阻断会话数最多的前 N 个应用的信息。 序列 | 应用 | 会话数 | 百分比 1 | POP2 | 35 | 14.64% 2 | POP3 | 29 | 12.13% 3 | 魔兽世界 | 26 | 10.88% 4 | NNTP | 23 | 9.62% 5 | Daytime | 22 | 9.21% 说明： • 会话数：某一特定应用的会话被应用控制阻断的总数。 • 百分比：某一特定应用的会话被应用控制阻断的总数占所有应用被应用控制阻断的会话总数的比例。
被应用控制阻断次数最多的前 N 个类别	被应用控制阻断会话数最多的前 N 个应用类别的信息。 序列 | 应用分类 | 会话数 | 百分比 1 | 电子邮件 | 97 | 40.59% 2 | 即时通讯 | 38 | 15.90% 3 | 游戏 | 26 | 10.88% 4 | 互联网实用类 | 23 | 9.62% 5 | 管理软件 | 22 | 9.21%

17.3.4.6 用户

表 306 用户信息

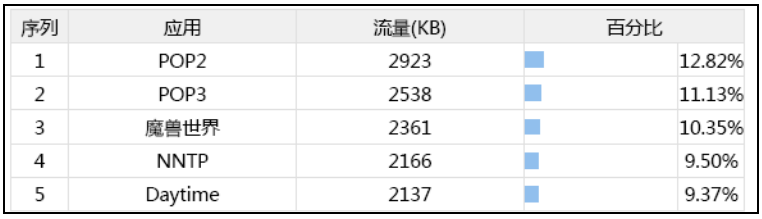
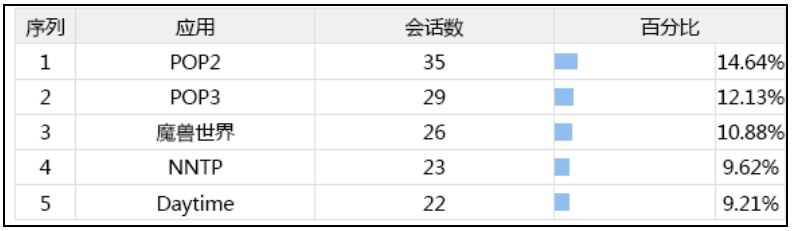
类型	描述
流量最高的前 N 个 IPSec VPN 用户	产生流量最高的前 N 个 IPSec VPN 用户的信息。 序列 | 用户名 | 流量(KB) | 百分比 1 | vpn1 | 1840 | 15.79% 2 | vpn2 | 1376 | 11.81% 3 | vpn3 | 1104 | 9.47% 4 | vpn4 | 1040 | 8.92% 5 | vpn5 | 980 | 8.41% 说明： • 流量 （KB）：某一特定 IPSec VPN 用户产生的总流量。 • 百分比：某一特定 IPSec VPN 用户产生的总流量占 IPSec VPN 用户总流量的比例。
流量最高的前 N 个 SSL VPN 用户	产生流量最高的前 N 个 SSL VPN 用户的信息。 序列 | SSLVPN 用户 | 流量(KB) | 百分比 1 | SSLVPNUser1 | 1577 | 14.14% 2 | SSLVPNUser2 | 1157 | 10.37% 3 | SSLVPNUser3 | 1070 | 9.59% 4 | SSLVPNUser4 | 1045 | 9.37% 5 | SSLVPNUser5 | 1010 | 9.06% 说明： • 流量 （KB）：某一特定 SSL VPN 用户产生的总流量。 • 百分比：某一特定 SSL VPN 用户产生的总流量占 SSL VPN 用户总流量的比例。
流量最高的前 N 个用户	产生流量最高的前 N 个 VPN 用户和 WebAuth 用户的信息。 序列 | 用户名 | 流量(KB) | 百分比 1 | test | 1995 | 8.75% 2 | test1 | 1735 | 7.61% 3 | test2 | 1537 | 6.74% 4 | test3 | 1321 | 5.79% 5 | test4 | 1271 | 5.57% 说明： • 流量 （KB）：某一特定用户产生的总流量。 • 百分比：某一特定用户产生的总流量占用户总流量的比例。
流量最高的前 N 个 WebAuth 用户	产生流量最高的前 N 个 WebAuth 用户的信息。 序列 | 用户名 | 流量(KB) | 百分比 1 | webUser1 | 1577 | 14.14% 2 | webUser2 | 1157 | 10.37% 3 | webUser3 | 1070 | 9.59% 4 | webUser4 | 1045 | 9.37% 5 | webUser5 | 1010 | 9.06% 说明： • 流量 （KB）：某一特定 WebAuth 用户产生的总流量。 • 百分比：某一特定 WebAuth 用户产生的总流量占所有 WebAuth 用户总流量的比例。

17.3.5 特定用户内容参数

管理员可以为特定用户或源 IP 地址选择与以下主题相关的内容：

17.3.5.1 应用

表 307 特定用户应用信息

类型	描述
流量最高的前 N 个应用	被指定用户或 IP 地址访问并产生最高流量的前 N 个应用的信息。  说明： • 流量 （KB）某一特定应用产生的总流量。 • 百分比：某一特定应用产生的总流量占此用户或源 IP 地址所有应用流量的比例。
被应用控制阻断次数最多的前 N 个应用	被指定用户或源 IP 地址访问且会话被应用控制阻断次数最多的前 N 个应用的信息。  说明： • 会话数：某一特定应用的会话被应用控制阻断的总数。 • 百分比：某一特定应用的会话被应用控制阻断的总数占此用户或源 IP 地址被应用控制阻断的会话总数的比例。

17.3.5.2 Web 安全

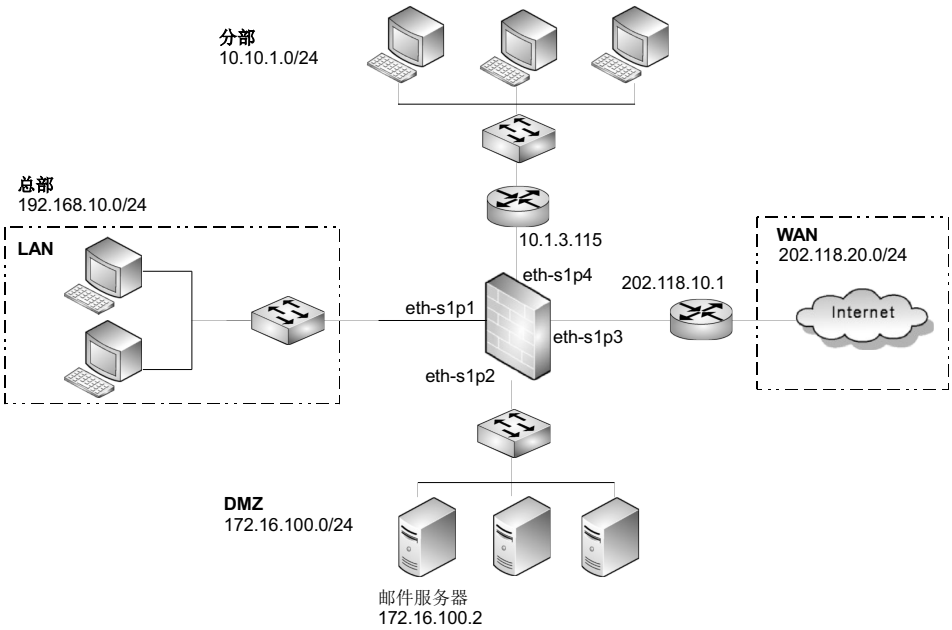
表 308 特定用户 Web 安全信息

类型	描述
会话最多的前 N 个 Web 站点	被指定用户或 IP 地址访问次数最多的前 N 个网站的信息。 序列 域名 会话数 百分比 1 www.baidu.com_1 23 11.56% 2 www.baidu.com_2 19 9.55% 3 www.baidu.com_3 16 8.04% 4 www.baidu.com_4 13 6.53% 5 www.baidu.com_5 12 6.03% 说明： • 会话数：某一特定网站的被访问的总次数。 • 百分比：某一网站被访问的总次数占此用户或源 IP 地址访问所有网站总次数的比例。
会话最多的前 N 个 URL 类别	被指定用户或 IP 地址访问的次数最多的前 N 种 URL 类别的信息。 序列 URL分类 会话数 百分比 1 烟酒 39 8.57% 2 匿名技术 33 7.25% 3 艺术 31 6.81% 4 商业 27 5.93% 5 运输 26 5.71% 说明： • 会话数：某一特定 URL 类别被访问的总次数。 • 百分比：某一 URL 类别被访问的总次数占此用户或源 IP 地址访问所有 URL 类别的总次数的比例。
被 URL 过滤功能阻断最多的前 N 个 URL 类别	被指定用户或 IP 地址访问且被 URL 过滤功能阻断次数最多的前 N 个 URL 类别的信息。 序列 URL分类 阻断的URL过滤 百分比 1 烟酒 39 8.57% 2 匿名技术 33 7.25% 3 艺术 31 6.81% 4 商业 27 5.93% 5 运输 26 5.71% 说明： • 阻断的 URL 过滤：某一特定 URL 类别被 URL 过滤功能阻断的总次数。 • 百分比：某一特定 URL 类别被 URL 过滤功能阻断的总次数占此用户或源 IP 地址访问的所有 URL 类别被 URL 过滤功能阻断的总次数的比例。
被 URL 过滤功能阻断最多的前 N 个 Web 站点	被指定用户或 IP 地址访问且被 URL 过滤功能阻断次数最多的前 N 个 Web 站点的信息。 序列 域名 阻断的URL过滤 百分比 1 www.baidu.com_6 12 18.18% 2 www.baidu.com_12 8 12.12% 3 www.baidu.com_18 7 10.61% 4 www.baidu.com_30 3 4.55% 5 www.baidu.com_24 3 4.55% 说明： 百分比：某一特定网站被 URL 过滤功能阻断的总次数占此用户或源 IP 地址访问的所有网站被 URL 过滤功能阻断的总次数的比例。

17.4 报表范例

如图 29 所示，某公司的总部 （192.168.10.0）和分部 （10.10.1.0）。总部员工可以通过 NISG-IPS 访问互联网和 DMZ 区服务器 （172.16.100.0），分部员工只能访问 DMZ 服务器。管理员需要配置 NISG-IPS 控制总部员工外网访问，保证内网安全；需要通过报表监控 NISG-IPS，了解其运行状态、网络使用状况和网络中存在的安全问题等。

图 29 某公司网络拓扑



用户需要执行如下操作：

- 17.4.1 配置 NISG-IPS
- 17.4.2 生成报表

17.4.1 配置 NISG-IPS

为实现并控制员工访问，保护内网安全，管理员在 NISG-IPS 上进行以下配置：

- 17.4.1.1 安全域
- 17.4.1.2 访问策略
- 17.4.1.3 路由
- 17.4.1.4 源地址转换
- 17.4.1.5 IPS 出口控制

17.4.1.1 安全域

1. 选择**网络** > **安全域**。
2. 点击**新建**创建安全域 LAN 和 WAN。LAN 和 WAN 分别基于三层接口 eth-s1p1 和 eth-s1p3。

- 名称 =LAN，类型 = 基于三层接口，接口 =eth-s1p1 ；
- 名称 =WAN，类型 = 基于三层接口，接口 =eth-s1p3。

3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone LAN
NetEye@root-system] zone LAN based-layer3 eth-s1p1
NetEye@root-system] zone WAN
NetEye@root-system] zone WAN based-layer3 eth-s1p3
NetEye@root-system] end
NetEye@root> save config
```

17.4.1.2 访问策略

1. 选择**防火墙** > **访问策略**。
2. 点击**新建**。创建访问策略 acpolicy1，允许总部员工通过 NISG-IPS 访问互联网和 DMZ 区服务器。创建访问策略 acpolicy2，允许分部员工通过 NISG-IPS 访问 DMZ 区服务器。
   - 名称 =acpolicy1，源安全域 =LAN，源 IP=192.168.10.0/24，目的安全域 = 任意，目的 IP/ 域名 = 任意，服务 = 任意，动作 = 允许。
   - 名称 =acpolicy2，源安全域 = 任意，源 IP=10.10.1.0/24，目的安全域 = 任意，目的 IP/ 域名 =172.16.100.0/24，服务 = 任意，动作 = 允许。
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access acpolicy1 LAN 192.168.10.0/24 any
any any any permit enable
NetEye@root-system] policy access acpolicy2 any 10.10.1.0/24 any
172.16.100.0/24 any any permit enable
NetEye@root-system] end
NetEye@root> save config
```

17.4.1.3 路由

1. 选择**网络** > **路由** > **缺省路由**。
2. 将 NISG-IPS 缺省路由出口接口设置为 eth-s1p3, 网关设置为 202.118.10.1。

   目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1，出口接口 =eth-s1p3，网关 =202.118.10.1
3. 设置 NISG-IPS 到分部 10.10.1.0/24 的路由。接口：eth-s1p4 ；网关：10.1.3.115。

   目的 IPv4 地址 =10.10.1.0，掩码长度 =24， Metric=1，出口接口 =eth-s1p4，网关 =10.1.3.135
4. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] route default interface eth-s1p3 gateway 202.118.10.1
NetEye@root-system] route 10.10.1.0 255.255.255.0 interface eth-s1p4 gateway 10.1.3.115
NetEye@root-system] end
NetEye@root> save config
```

17.4.1.4 源地址转换

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**创建源地址转换规则，保护总部内部网络安全。

   名称 =snat1，源 IP=192.168.10.0/24，转换后 IP/ 接口 =eth-s1p3，入口接口 =eth-s1p1，出口接口 =eth-s1p3
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 netmask 192.168.10.0 255.255.255.0 interface eth-s1p3 napt enable
NetEye@root-system] policy snat snat1 matching input-interface eth-s1p1
NetEye@root-system] policy snat snat1 matching output-interface eth-s1p3
NetEye@root-system] end
NetEye@root> save config
```

17.4.1.5 IPS 出口控制

1. 设置应用控制。
   a. 选择 **IPS**> **出口控制** > **应用控制** > **防护配置**。点击**新建**创建防护配置 profile1, 设置阻断多媒体类和 Google-Talk、 QQ-Base 及 PPLive 应用。
   b. 选择 **IPS**> **出口控制** > **策略**。在安全域 WAN 上开启出口控制功能。启用**应用控制**。点击**新建**创建应用控制策略。

      名称 =ap1，源安全域 = LAN，源 IP=192.168.10.0/24，防护配置 =profile1
2. 设置 URL 过滤。
   a. 选择 **IPS**> **出口控制** >**URL 过滤** > **黑白名单**。点击**新建**创建 URL 黑白名单。
      - 名称 =whitelist，类型 = 白名单，URL 包括：www.baidu.com、www.nciku.com、www.it168.com 和 www.wikipedia.org。
      - 名称 =blacklist，类型 = 黑名单， URL 包括：www.taobao.com、 www.qq.com 和 www.tieba.baidu.com。

b. 选择 **IPS**> **出口控制** >**URL 过滤** > **防护配置**。点击**新建**创建防护配置，启用 URL 分类，对广告、烟酒类相关 URL 进行阻断。

名称 =urlprofile， URL 白名单 =whitelist1， URL 黑名单 =blacklist1， URL 分类 = 启用，广告 / 烟酒 = 阻断

c. 选择 **IPS**> **出口控制** > **策略**。

启用 **URL 过滤**。点击**新建**创建 URL 过滤策略。

名称 =urlpolicy，源安全域 = LAN，源 IP=192.168.10.0/24，源用户 = 任意，防护配置 =urlprofile

3. 点击  。

17.4.2 生成报表

17.4.2.1 配置常规设置

1. 选择**监控** > **报表** > **常规设置**。设置报表要记录的内容类别，包括系统、流量、Web 安全、攻击和应用。
2. 设置 SMTP 服务器信息。

   地址 =172.16.100.2，端口 =465，发送人 =user1@test.com，用户名 =user1，密码 =123456，主题 =Security Report
3. 设置报表保留条目数为 10，使用默认的 Logo 信息。

17.4.2.2 创建报表生成计划

1. 选择**监控** > **报表** > **计划**。点击**新建**创建报表生成计划。
2. 设置报表名称等基本信息。

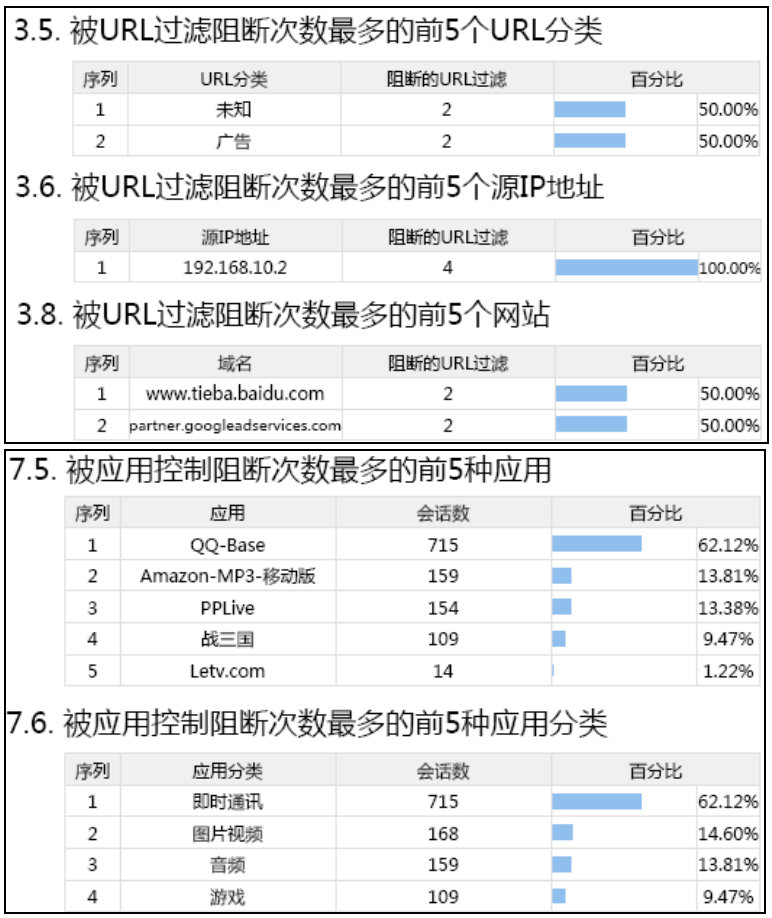
   名称 =DailyReport，报表标题 =Neusoft Security Report，报表描述 =Daily Security report，时间表 = 每天 10:00
3. 设置报表收件人、输出语言及格式。

   收件人 =admin@test.com，语言 = 简体中文，格式 =PDF
4. 在**内容设置**区域点击**全部选中**。

17.4.2.3 查看报表结果

1. 选择**监控** > **报表** > **结果**，可以查看到名称为 DailyReport 的 PDF 格式的报表文件已成功生成。
2. NISG-IPS 根据配置将生成的报表发送给收件人 admin@test.com。

3. 点击步骤 1 图中的超链接下载指定时间内的报表文件至本地。报表记录的部分监控结果如下所示：



3.5. 被URL过滤阻断次数最多的前5个URL分类

序列	URL分类	阻断的URL过滤	百分比
1	未知	2	50.00%
2	广告	2	50.00%

3.6. 被URL过滤阻断次数最多的前5个源IP地址

序列	源IP地址	阻断的URL过滤	百分比
1	192.168.10.2	4	100.00%

3.8. 被URL过滤阻断次数最多的前5个网站

序列	域名	阻断的URL过滤	百分比
1	www.tieba.baidu.com	2	50.00%
2	partner.googleadservices.com	2	50.00%

7.5. 被应用控制阻断次数最多的前5种应用

序列	应用	会话数	百分比
1	QQ-Base	715	62.12%
2	Amazon-MP3-移动版	159	13.81%
3	PPLive	154	13.38%
4	战三国	109	9.47%
5	Letv.com	14	1.22%

7.6. 被应用控制阻断次数最多的前5种应用分类

序列	应用分类	会话数	百分比
1	即时通讯	715	62.12%
2	图片视频	168	14.60%
3	音频	159	13.81%
4	游戏	109	9.47%

18 旁路 IPS

本章介绍 NISG-IPS 工作在旁路模式下的功能和配置。内容包括：

提示：旁路模式下不支持 IPv6。

18.1 系统配置

旁路模式下， NISG-IPS 提供如下系统管理功能：

- 3.3 WebUI 主页 （查看系统状态信息）
- 系统维护
  - 3.4 系统概述
  - 3.7 系统时间
  - 3.8 License
  - 3.21 备份恢复
  - 3.22 技术支持
  - 3.23 诊断工具
  - 3.24 调试工具
- 服务配置
  - 3.12 访问设置 （旁路模式下不支持安全域配置）
  - 3.13 标题信息
  - 3.14 SNMP
- 用户与认证 （旁路模式下不支持网络用户配置）
  - 3.15 管理用户
  - 3.17 用户认证
- 3.28 证书
- 报警和日志
  - 3.26 报警配置
  - 3.27 日志维护
- 系统升级
  - 3.9 系统升级
  - 3.10 安装升级包管理
  - 3.11 增强升级包管理
- 查看资产信息
  - 3.5 资产汇总
  - 3.6 版权信息

详细配置信息，请参见第 3 章， 系统配置。

18.2 网络配置

本节介绍网络配置的相关内容，包括：

18.2.1 接口管理

18.2.1.1 概述

NISG-IPS 工作在旁路模式时，不允许管理员创建任何逻辑接口，仅可以基于物理接口进行操作。所有物理接口都有如下三种工作模式：

- **管理接口**：用于设备的管理。任何物理接口都可以工作在管理模式。
- **监听接口**：用于监听需要进行 IPS 分析的网络数据流量，不能用于设备的管理。任何物理接口都可以工作在监听模式。
- **无状态接口**：既不是管理接口也不是监听接口的物理接口，不接收任何数据。

18.2.1.2 基本配置步骤

1. 选择**网络 > 接口**。

接口列表

接口	链路状态	接口状态	模式	MAC地址	IP地址	
eth-s1p1			管理	00:0C:29:A1:BC:EE	10.1.3.109/21(静态)	
eth-s1p2			监听	00:0C:29:A1:BC:F8		
eth-s1p3			无	00:0C:29:A1:BC:02		
eth-s1p4			无	00:0C:29:A1:BC:0C		
mgt			无	00:0C:29:A1:BC:02		

提示：有些机型提供带外管理口。带外管理口 （MGT）是专用管理口，只能工作在管理模式。

2. 点击以太网接口对应的图标，进入接口编辑页面。

- 配置管理接口。管理接口工作在三层模式，和在线工作模式下的三层物理接口具有相同的配置属性。

提示：当一个监听接口被指定为管理接口时，其二层物理接口属性（MAC 地址，网卡工作状态）将被继承。

- 指定监听接口。监听接口工作在二层模式，和在线工作模式下的二层接口具有相同的配置属性，但其不属于任何 VLAN。

提示：当一个管理接口被指定为监听接口时，其二层物理接口属性 （MAC 地址，网卡工作状态）将被继承，三层属性将被丢弃。

- 配置无状态接口。无状态接口工作在二层模式，仅具有基础的二层属性。

3. 点击**确定**。
4. 点击 。

18.2.1.3 配置参数说明

表 309 接口配置信息

配置信息	说明
接口	接口的名称，例如：eth-s1p2。
链路状态	接口的链路状态。 • 绿色图标 （Up）：表示已连接，且链路协商成功。 • 红色图标 （Down）：表示已断开。
接口状态	指接口的活动状态。 • 绿色图标 （开）：表示接口已启用。 • 灰色图标 （关）：表示接口已禁用。
模式	接口的工作模式，分为三种：管理、监听和无状态。
MAC 地址	接口的 MAC 地址。 替换 NISG-IPS 硬件设备或发生 MAC 冲突时，可勾选**使用特定 MAC 地址**复选框，手动指定 MAC 地址。接口工作在监听模式时，此功能不可用。
IPv4 地址	管理接口的 IP 地址。 为管理接口配置 IPv4 地址，可通过两种方式： • **静态 IP**：手动配置管理接口的静态 IP 地址，此时需要在 IP 地址列表中添加地址。管理员最多可以添加 32 个 IPv4 地址。 • **DHCP**：点击**使用 DHCP 更新 IP 地址**，系统将从 DHCP 服务器上自动获得动态分配的 IP 地址。如果同时勾选**启用 DNS 代理**复选框，则系统将根据该接口动态获取的 DNS 地址自动添加 DNS 代理。

表 309 接口配置信息 (*续*)

配置信息	说明
IPv6 地址	为管理接口配置 IPv6 地址，需要勾选**启用 IPv6** 复选框，并配置以下属性： • **接口 ID （EUI-64）**：系统根据接口 MAC 地址自动生成的一个 EUI-64 格式的接口标识，用于 IPv6 单播。 IPv6 单播地址要求接口标识为 64 位，而 MAC 地址是 48 位，因此需要在 MAC 地址的高 24 位和低 24 位之间插入十六进制数 FFFE，构成新的 64 为接口标识。 • **链路本地地址**：专门用于本地链路通讯的 IPv6 地址，可自动生成或手动指定。 当勾选**自动配置链路本地地址**时， NISG-IPS 将通过在接口的 MAC 地址前面增加链路本地地址前缀 FE80::，自动为该接口生成一个临时链路本地地址； 当取消勾选**自动配置链路本地地址**时，表示采用手动方式指定。 • **ULA 或全球单播地址**：用于网络层通讯的 IPv6 地址。 当勾选**无状态自动配置**时，系统将自动获取一个 IPv6 全球单播地址。 当取消勾选**无状态自动配置**时，表示采用手动配置方式 （缺省方式），需要在 **IP 地址列表**中配置 IPv6 地址。最多可以添加 31 个 IPv6 全球单播地址。 **类型**：表示手动配置 ULA 或全球单播地址的类型，包括手动和 EUI-64。 当指定**手动**时，表示不使用 EUI-64 格式的接口标识；当指定 **EUI-64** 时，表示使用 EUI-64 格式的接口标识。 **状态**：表示 IPv6 地址的状态，包括临时地址 （TENTATIVE）、重复地址 （DUPLICATE）、首选地址 （PREFERRED）、不推荐地址 （DEPRECATED）以及无效地址 （INVALID）。
描述	接口的描述信息。为 0 ～ 255 字节的 UTF-8 字符，不能包含以下字符：?'\"<>&。
MTU	指最大传输单元 （Maximum Transmission Unit），只有管理接口具有该属性。 接口的 MTU 只对出口接口起作用，即仅当出口接口的数据包长度大于接口的 MTU 时，才进行分片操作。 • 在 IPv4 中，管理接口的 MTU 取值范围为 68 ～ 1500 字节，缺省为 1500 字节。 • 在 IPv6 中，管理接口的 MTU 取值范围为 1280 ～ 1500 字节，缺省为 1500 字节。
NIC 模式	接口内置网卡的工作模式，包括三个属性： • **链路速率**：指接口的数据传输效率，包括 10 Mbps、100 Mbps、1000 Mbps 和自动四种模式。自动模式是指 NISG-IPS 根据实际情况自动调节接口的数据传输速率。 • **双工**：指接口的双工模式，包括全双工、半双工和自动三种模式。 全双工模式是指数据传输是双向同步进行的，即同时发送和接收数据。 半双工模式是指同一时刻只能单向传输数据，或接收数据或发送数据。 自动模式是指自动协商双工模式，根据实际双工模式传输数据。 • **流量控制**：指对接口流量的控制。当接口发生拥塞不能再接收任何数据包时， NISG-IPS 将通知接口的对端设备已经发生拥塞。对端设备收到信息后立即停止向该接口发送数据包，直到拥塞消失后再继续传输数据。管理员可以选择启用或禁用此功能。

18.2.2 工作模式

18.2.2.1 概述

NISG-IPS 支持两种工作模式：

- **在线模式**：具备 IPS 的全部功能，对网络流量进行过滤和控制。
- **旁路模式**：仅用作旁路 IPS 检测设备，对网络流量进行监听和分析。

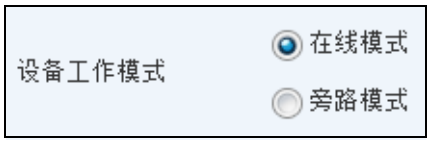
在线模式和旁路模式是两种互斥的工作模式，管理员可以根据自身需要选择任意一种工作模式。

表 310 切换工作模式的影响

模式切换	对系统的影响
在线切换到旁路	• 连接中断，安全检查终止。 • 管理接口和 IP 保持不变。 • 其他所有以太网接口工作在二层模式，逻辑接口被删除。 • 在线模式和旁路模式都具备的功能，将继承在线模式下的配置。
旁路切换到在线	• IPS 检测终止。 • 管理接口和 IP 保持不变。 • 其他所有以太网接口工作在二层模式。 • 在线模式和旁路模式都具备的功能，将继承旁路模式下的配置。 **注**：旁路模式下 IPS 自定义规则和应用的配置将被保留，下次切换回旁路模式时再生效。 • 旁路模式下不具备的安全功能，将恢复出厂默认配置。

18.2.2.2 基本配置步骤

1. 选择**网络 > 工作模式**。
2. 切换工作模式。



3. 点击**确定**。

提示：切换工作模式时，当前模式下的安全配置将丢失，建议备份系统配置后再执行模式切换。

18.2.2.3 功能差异 （旁路和在线）

图表说明：

● 表示旁路模式具备该功能，与在线模式的功能完全一致。

● 表示旁路模式具备该功能，但与在线模式的功能存在差异。

○ 表示旁路模式具备在线模式原有功能的部分内容。

表 311 旁路模式与在线模式的功能差异

功能特性			旁路模式	在线模式	功能说明
WebUI 管理			●	●	WebUI 仅体现本模式下提供的功能。
CLI 管理 （Console、 SSH 和 Telnet）			●	●	CLI 仅可以操作本模式下提供的功能。
主页			●	●	旁路模式下只能查看系统信息、资源使用情况、接口状态和系统日志。
系统管理					
	概述		●	●	
	系统维护		●	●	
	服务配置				
		本地访问控制	○	●	旁路模式不支持安全域功能。
		Banners 信息	●	●	
		SNMP	●	●	
	认证管理				旁路模式不支持网络用户功能。
		管理员	●	●	
		认证配置	○	●	旁路模式不支持针对网络用户的认证服务器。
		认证服务器管理	●	●	
	证书		●	●	
	对象			●	
	日志管理		●	●	
	系统升级		●	●	
	资产信息		●	●	
网络配置					旁路模式不支持安全域、 DHCP、 NAT 和邻居发现功能。 IPv6 支持同在线模式一致。
	接口管理		○	●	旁路模式的接口特性，请参见 18.2.1 接口管理。
	DNS 设置		○	●	旁路模式仅支持 DNS 主机功能，不支持 DNS 代理和静态缓存。

表 311 旁路模式与在线模式的功能差异 (*续*)

功能特性		旁路模式	在线模式	功能说明
	路由	○	●	旁路模式仅支持静态路由，不支持策略路由。
VPN			●	
防火墙			●	
IPS				旁路模式不支持出口控制和通知消息功能。 旁路模式的入侵检测功能，请参见 18.3 IPS 检测。
	常规设置	●		指定 IPS 检测使用的防护配置和要监控的网络。
	防护配置	○	●	旁路模式下允许创建类型为“全部”的防护配置。
	自定义规则	●		管理员可以根据攻击特征自定义正则表达式，作为 IPS 检测的规则。
	自定义应用	○	●	旁路模式下，管理员只能修改应用的端口号。
	更新	●	●	
监控		○	●	旁路模式下仅提供部分监控页面。
	接口流量	●	●	
	系统利用率	●	●	
	报警和日志			
	管理日志	●	●	
	IPS 报警	●	●	

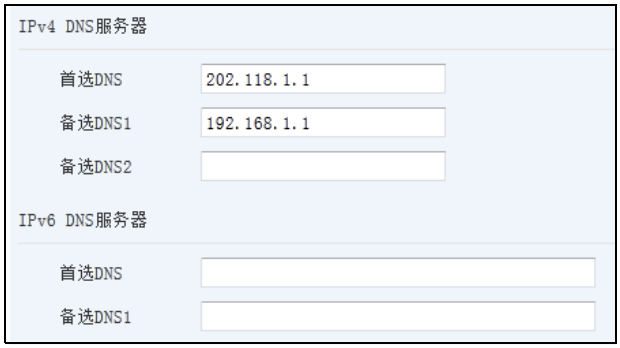
18.2.3 DNS 主机

18.2.3.1 概述

NISG-IPS 可作为 DNS 客户端从 DNS 服务器请求域名解析。管理员最多能设置三个 IPv4 DNS 服务器和两个 IPv6 DNS 服务器地址，用于域名解析服务 , 如解析 NISG-IPS 系统升级服务器、 IPS 规则升级服务器、 LDAP 服务器等域名。

18.2.3.2 基本配置步骤

1. 选择**网络** > **DNS**。
2. 配置相应的 DNS 服务器地址。



3. 点击**确定**。
4. 点击 。

表 312 DNS 主机命令

dns host	配置 NISG-IPS 域名服务器。
unset dns host	删除域名服务器配置。
show dns host	显示 DNS 服务器配置。

18.2.3.3 配置参数说明

表 313 DNS 主机属性

配置信息	说明
IPv4 DNS 服务器	IPv4 DNS 服务器的 IP 地址，包括首选 DNS、备选 DNS1 以及备选 DNS2。 可以输入的 IP 地址范围为：[1-223].[0-255].[0-255].[0-255]，不可以为 127.0.0.0~127.255.255.255 或者 192.168.255.254。
IPv6 DNS 服务器	IPv6 DNS 服务器的 IP 地址，包括首选 DNS 和备选 DNS1。 不可以为环回地址 （::1）、多播地址 （FF00/8~FFFF/8）、未指定地址 （::）、::FFFF:0:0/96。

18.2.4 缺省路由

18.2.4.1 概述

为了使工作在旁路模式下的 NISG-IPS 能够被管理员远程管理，需要为管理接口指定下一跳网关。

18.2.4.2 基本配置步骤

1. 选择**网络** > **路由**。

2. 默认存在一条目的地址为 0.0.0.0/0 的缺省路由，可点击修改出口接口和网关。

3. 如果配置多个管理接口允许管理员从不同网段进行远程管理，也可根据需要添加多条到指定网段的路由。

4. 点击**确定**。
5. 点击 。

表 314 缺省路由命令

route	添加缺省路由。
show route	显示缺省路由信息。
unset route	删除静态路由。

18.2.4.3 参数说明

表 315 缺省路由配置参数

参数	说明
类型	IP 地址的类型。 IPv4 地址或 IPv6 地址。
目的 IPv4 地址 / 目的 IPv6 地址	数据包要被发送到的目的主机或目的网络的地址。
掩码长度 / 前缀长度	目的 IPv4 地址的掩码长度或目的 IPv6 地址的前缀长度。 掩码长度的取值范围是 0 ～ 32 ；前缀长度的取值范围为 0 ～ 128。
Metric	指路由的优先级。取值范围为 1 ～ 255。 Metric 值越小，优先级越高。
出口接口 / 网关	用于为静态路由设置一个出口接口、网关或两者均设置。
常规	用于配置不带负载均衡功能的静态路由。管理员至少需要设置以下任意一项： • **接口**：用于将数据包转发出去的三层接口。如果管理员选择空接口，且不指定网关地址，数据包会被丢弃。 • **网关**：对端网络无法直达时的下一跳路由设备的 IP 地址。
负载均衡	仅在在线模式下有效。

18.3 IPS 检测

18.3.1 常规设置

NISG-IPS 作为旁路监听设备，可以通过监听接口获取网络流量的镜像，并对镜像流量进行 IPS 检测。

在常规设置页面，管理员可以指定要使用的 IPS 防护配置，是否启用自定义 IPS 规则，以及要监控的网络。

管理员可以指定多个监控网络，NISG-IPS 仅针对该网络发出或者收到的流量进行 IPS 检测。管理员最多可以指定 64 个网络。

1. 选择 **IPS > IPS > 常规设置**。
2. 选择启用的 IPS 防护配置，设置是否启用自定义 IPS 规则，指定监控网络。

若想使用自定义 IPS 防护配资，需要选择 **IPS > IPS > 防护配置**，事先添加自定义的 IPS 防护配置。

如果启用自定义 IPS 规则，还需选择 **IPS > IPS > 自定义规则**，添加自定义规则。

3. 点击**确定**。
4. 点击 。

表 316 常规设置的配置信息

参数	描述
IPS 防护配置	要启用的 IPS 防护配置，可以是缺省的，也可以是自定义的。 所有监控网络的流量都将按照所选防护配置中包含的攻击签名规则进行检测。
启用自定义 IPS 规则	设置是否启用自定义 IPS 规则。
被保护网络列表	对列表中包含的网络所发出或接收的流量进行 IPS 检测，配置属性包括： • **类型**：监控网络的地址类型，包括 IPv4 地址、 IPv4 地址范围和 IPv4 地址 / 掩码。 • **IP 地址**：监控网络的 IP 地址。

18.3.2 IPS 防护配置

NISG-IPS 工作在旁路模式时，管理员可以选择一个缺省或用户自定义的 IPS 防护配置用于 IPS 检测，所有流量都根据这个指定的 IPS 防护配置进行规则匹配及策略动作操作。

IPS 防护配置是攻击签名规则的集合，管理员可以根据需要配置不同的防护配置。管理员可以创建类型为“客户端”、“服务器”或“全部”的防护配置。当管理员选择了“全部”类型后，系统允许其配置所有类型的攻击签名规则。

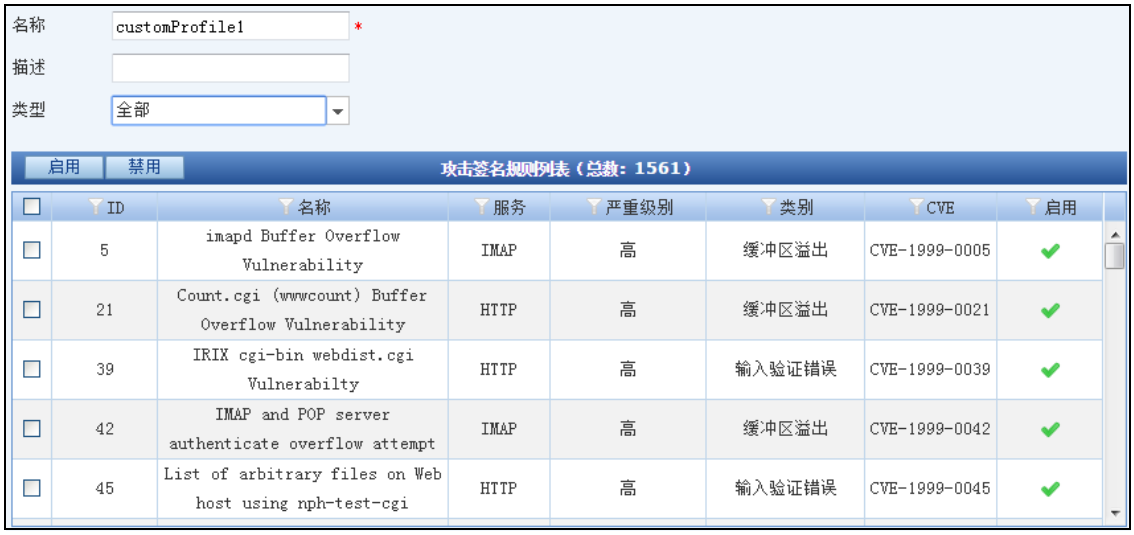
表 317 IPS 防护配置的类型

类型	描述
客户端	能够包含目标为客户端的攻击签名规则集。
服务器	能够包含目标为服务器端的攻击签名规则集。 管理员可以为 Web、DNS、FTP、Telnet 和 Mail 五种类型的服务器配置是否开启攻击签名规则和匹配规则后的动作。
全部	能够包含目标为客户端或服务器端的攻击签名规则集。

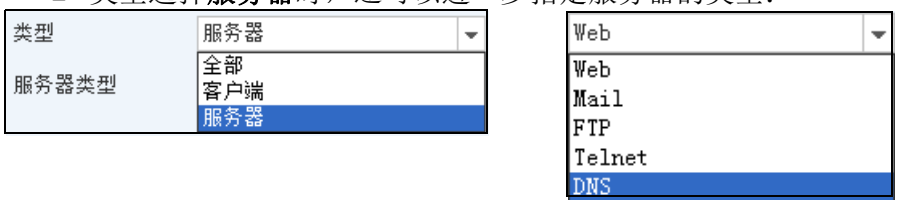
要添加 IPS 防护配置，请执行以下操作：

1. 选择 **IPS > IPS > 防护配置**。
2. 查看缺省防护配置。

3. 点击**新建**，添加自定义防护配置。

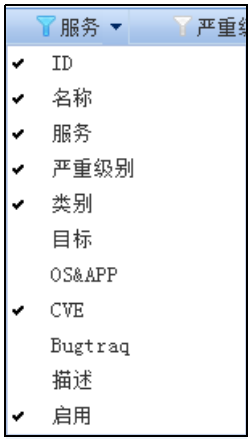


- 类型选择**服务器**时，还可以进一步指定服务器的类型：



- 为防护配置选择攻击签名规则时，可通过列表表头的 图标筛选显示的攻击签名规则。

- 将鼠标指向列表表头，可通过点击列表表头中出现的 ▼ 图标自定义显示的攻击签名规则属性。



4. 点击**确定**。
5. 点击 。

表 318 IPS 防护配置的参数信息

参数	描述
名称	IPS 防护配置的名称。 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&# 缺省 IPS 防护配置分别以 _Low， _Medium 和 _High 命名，分别表示了低、中、高三个级别的 IPS 防护。 • **低**：仅防御严重级别为高的攻击。 • **中**：防御级别为高和中的攻击。 • **高**：防御所有攻击。
描述	IPS 防护配置的描述信息。 0~255 字节， UTF-8 字符。不能包含以下字符：?"′ \<>&
类型	IPS 防护配置的类型，包括客户端、服务器和全部。
服务器类型	当 IPS 防护配置的类型为服务器时，可以进一步配置服务器的类型，包括 Web、 Mail、 FTP、 Telnet 和 DNS。
允许 / 阻断	设置攻击签名规则的动作，包括允许和阻断。 • 如果一条规则被启用且动作设为允许， NISG-IPS 将放行匹配该规则的流量。 • 如果一条规则被启用且动作设为阻断， NISG-IPS 将阻断匹配该规则的流量。
启用 / 禁用	启用和禁用攻击签名规则。

表 319 攻击签名规则属性

参数	说明
ID	规则的标识。
名称	规则的名称。
服务	规则对应的协议。
严重级别	不同严重级别的攻击发生时，按照相应的安全等级记录日志，以便管理员在进行审计配置时，可以决定哪些级别的事件以哪种方式（SysLog、 Mail、 SNMP Trap、 Local Log）进行审计。 严重级别与安全等级的对应关系为：High 对应 Critical， Medium 对应 Error， Low 对应 Warning， Info 对应 Notification。
类别	规则的类别，如 BACKDOOR/TROJAN、 BUFFER OVERFLOW、 CODE INJECTION、 DESIGN ERROR、 INPUT INVALIDATE FAILED、 MALWARE 和 UNKOWN 等。
目标	攻击的目标，包括客户端、服务器和 Both 攻击三种。
OS&APP	规则对应的操作系统和应用程序。
CVE	公共漏洞和暴露 （Common Vulnerabilities&Exposures， CVE）编号。
Bugtraq	Bugtraq 编号。
描述	规则的描述信息，包含简单的原理介绍。
启用	规则的状态。
动作	规则的处理动作，包括允许和阻断。 • **允许**：放行匹配到当前规则签名的数据包。 • **阻断**：阻断匹配到当前规则签名的数据包。

18.3.3 自定义规则

管理员可以设置一个或者多个正则表达式作为 IPS 检测规则，凡匹配到用户自定义规则的流量将被认为是攻击行为。

1. 选择 **IPS > IPS > 自定义规则**。
2. 添加或删除用户自定义规则，或双击条目进行修改。

提示：自定义规则必须是合法的正则表达式，长度为 1-255 字节。此功能要求管理员对攻击特征比较熟悉。管理员最多可以添加 256 条自定义规则。

3. 点击**确定**。
4. 点击 。

表 320 自定义规则的配置信息

参数	描述
名称	自定义规则的名称。 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
应用 （协议 / 端口）	自定义规则指定的应用协议和端口号。 协议包括 TCP 和 UDP，端口号范围为 1-65535。
规则	自定义规则指定的合法的正则表达式，长度为 1-255 字节。 匹配正则表达式的流量将被认为是攻击行为。
动作	数据命中自定义规则时 NISG-IPS 执行的动作，默认为报警且不可修改。
启用	自定义规则是否启用，默认为启用。

18.3.4 自定义应用

NISG-IPS 可以通过协议和端口区分应用。 NISG-IPS 工作在旁路模式时，系统允许管理用户根据自己的实际网络环境修改应用的端口配置。

1. 选择 **IPS > IPS > 自定义应用**。
2. 双击应用条目，编辑自定义应用的端口号。

自定义应用列表（总数：10）		
应用	TCP/UDP	端口
HTTP	TCP	80
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
IMAP	TCP	143,220
Oracle	TCP	1521
Telnet	TCP	23
TFTP	UDP	69
DNS	UDP	53
SIP	UDP	5060

提示：管理员可以配置端口属性，每个应用最多可以配置 16 个端口号，以英文逗号分隔。

3. 点击**确定**。
4. 点击 。

18.3.5 IPS 规则库更新

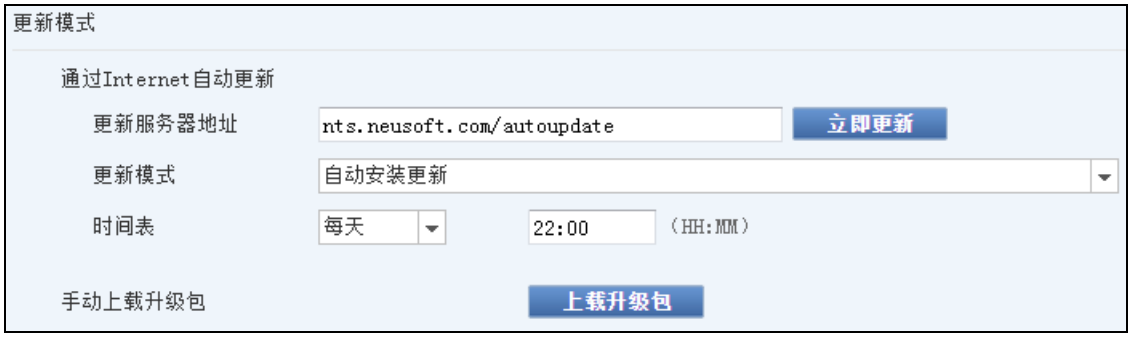
NISG-IPS 通过加载攻击签名规则升级包更新攻击签名规则。攻击签名规则升级包上载后立即生效，不需要重启系统。攻击签名规则更新需要 IPSUP License 的许可。

1. 选择 **IPS** > **IPS** > **更新**。
2. 查看规则库升级历史记录。

历史信息 显示更新历史记录

规则库	规则版本	引擎版本	上次更新时间
HTTP	2.2.1	2.2.0	2015-11-16 9:23:50
DNS	2.2.1	2.2.0	2015-11-16 9:23:50
FTP	2.2.1	2.2.0	2015-11-16 9:23:50
IMAP	2.2.1	2.2.0	2015-11-16 9:23:50
ORACLE	2.2.1	2.2.0	2015-11-16 9:23:50
OTHERS	2.2.1	2.2.0	2015-11-16 9:23:50
POP3	2.2.1	2.2.0	2015-11-16 9:23:50
SIP	2.2.1	2.2.0	2015-11-16 9:23:50
SMTP	2.2.1	2.2.0	2015-11-16 9:23:50
TELNET	2.2.1	2.2.0	2015-11-16 9:23:50
TFTP	2.2.1	2.2.0	2015-11-16 9:23:50
BACKDOOR	2.2.1	2.2.0	2015-11-16 9:23:50

3. 通过手动或自动方式更新 IPS 攻击签名规则库。
   - **手动**：点击**上载升级包**。
   - **自动**：设置升级服务器地址后，点击**立即更新**立即更新 IPS 规则库，或设置更新模式及时间表周期性更新 IPS 规则库。



提示：首次使用 IPS 检测功能时，请立即更新 IPS 攻击签名特征库（点击**立即更新**按钮或手动上传升级包）。若要立即更新或使用自动方式更新特征库，请确认设备已正确接入网络，并设置了正确的更新服务器地址和 DNS 服务器地址。设置 DNS 服务器地址请选择**网络 > DNS**。
如无法完成在线更新，请联系技术支持人员获取最新的 IPS 升级包，手动上传。

4. 点击**确定**。
5. 点击 。

表 321 攻击签名规则库参数

参数	说明
规则库	攻击签名规则库名称，默认包括 HTTP、 DNS、 FTP、 IMAP、 ORACLE、 OTHERS、 POP3、 SIP、 SMTP、 TELNET、 TFTP 和 BACKDOOR。
规则版本	最新的攻击签名规则库版本。
引擎版本	攻击签名规则库所对应的引擎版本。
上次更新时间	当前攻击签名规则库上次更新时间。
显示 / 导出更新历史记录	用于查看或导出攻击签名规则库的更新历史记录。 NISG-IPS 最大支持 50 条记录。

表 322 攻击签名规则更新模式参数

参数	说明
更新服务器地址	更新服务器的 URL 地址，可以为 IPv4/v6 地址或者域名。 缺省为 nts.neusoft.com/autoupdate。
更新模式 （自动）	攻击签名规则自动更新的模式，包括自动安装更新和从不检测更新。
时间表	NISG-IPS 自动下载并安装升级包的定时更新时间。 • 当选择**每天**、**每周**或**每月**时，系统会在指定时间点后两个小时内随机开始升级。 • 当选择**间隔**时，系统将按照设定时间间隔进行规则更新。
立即更新	当更新服务器地址和更新内容配置成功后，点击**立即更新**， NISG-IPS 立即从指定的更新服务器上获取升级包并执行安装。
手动上载升级包	上传本地的攻击签名规则更新包。

18.4 监控

旁路模式下的监控模块提供如下监控信息：

- 16.2.1 接口流量
- 16.13 系统利用率
- 报警 / 日志
  - 16.18.1 系统日志
  - 16.18.3 IPS 报警

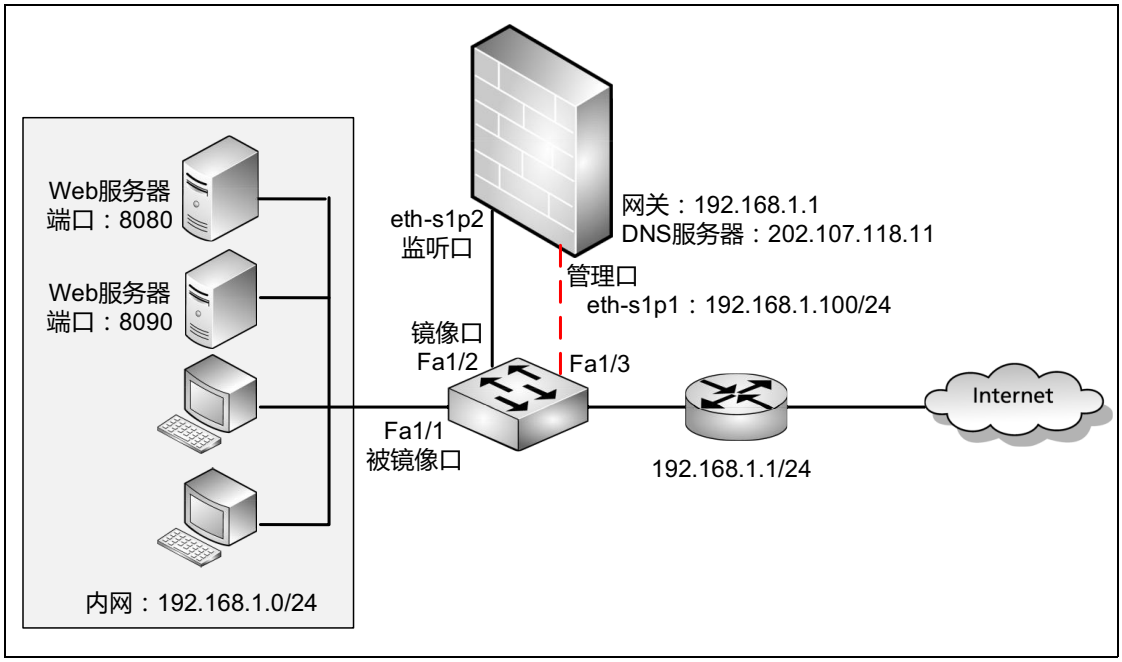
详细信息，请参见第 16 章，监控。

18.5 旁路 IPS 范例

基本需求

- 对网络进出流量进行 IPS 安全检测 （监听、扫描、记录）和审计。
- 进行安全检测的同时不影响数据包的正常转发，网络流量不受设备本身故障的影响。

组网拓扑



配置要点

- 切换工作模式
- 配置监听接口
- 配置交换机镜像端口
- 配置旁路 IPS 检测
- 监控网络流量

配置步骤

切换工作模式

1. 选择**系统 > 维护 > 工作模式**。
2. 切换到旁路工作模式。

配置监听接口

1. 选择**网络 > 接口**。
2. 指定 eth-s1p2 为监听接口。

> **提示：**系统支持的监听接口数目由 License 决定。监听接口越多，消耗的系统资源越多。

3. 点击 。

配置交换机镜像端口

配置交换机的镜像端口，将流经交换机的流量映射到 NISG-IPS 的监听接口。

下面以思科交换机为例，配置交换机的源和目的镜像端口：

```
SwitchA>enable
Password:
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA (config)#interface fastEthernet 1/1
SwitchA (config-if)#no shutdown
SwitchA (config)#
*Mar  1 00:01:36.059: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed
starte to up
SwitchA (config-if)#exit
SwitchA (config)#interface fastEthernet 1/2
SwitchA (config-if)#no shutdown
SwitchA (config)#
*Mar  1 00:04:50.283: %LINK-3-UPDOWN: Interface FastEthernet1/2, changed
starte to up
SwitchA (config-if)#exit
SwitchA (config)#interface fastEthernet 1/3
SwitchA (config-if)#no shutdown
SwitchA (config)#
*Mar  1 00:06:33.619: %LINK-3-UPDOWN: Interface FastEthernet1/3, changed
starte to up
SwitchA (config-if)#exit
SwitchA (config)#monitor session 1 source interface fastEthernet 1/1
both
SwitchA (config)#monitor session 1 destination interface fastEthernet
1/2
SwitchA (config)#exit
SwitchA#write
```

配置旁路 IPS 检测

1. 更新 IPS 攻击签名规则库。
   a. 选择**网络 > DNS**，设置 DNS 服务器地址 202.107.118.11，使 NISG-IPS 可以正常访问更新服务器的域名地址。
   b. 选择**网络 > 路由**，设置下一跳网关为 192.168.1.1。
   c. 选择 **IPS** > **IPS** > **更新**，设置更新服务器地址为 nts.neusoft.com/autoupdate，点击**立即更新**。

   提示：使用立即更新前，请确认设备已正确接入网络。如无法完成在线更新，请联系技术支持工程师获取最新的 IPS 升级包，手动上传。

2. 选择 **IPS > IPS > 自定义规则**，添加用户自定义规则，检测常见的 Exec 命令和 Simple XSS 攻击。
   - 规则 1：
     - 名称：ExecCommand
     - 应用：TCP:8080
     - 规则：exec /bin/sh -c /bin/id
     - 动作：报警
     - 启用：勾选
   - 规则 2：
     - 名称：SimpleXSS
     - 应用：TCP:8090
     - 规则：((%3C)|<)((%2F)|/)*[A-Z0-9%]+((%3e)|>)
     - 动作：报警
     - 启用：勾选
3. 选择 **IPS > IPS > 自定义应用**，双击 HTTP 应用条目，修改应用的端口号 80 为 ”8080,8090,8081”。
4. 选择 **IPS > IPS > 防护配置**，添加类型为 “ 全部 ” 的自定义防护配置，启用所有规则。
5. 选择 **IPS > IPS > 常规设置**，选择启用的 IPS 防护配置，启用用户自定义规则 CustomProfile1，指定监控网络 192.168.1.0/24。
6. 点击**确定**。
7. 点击 。

监控网络流量

1. 选择**监控 > 报警 / 日志 > IPS 报警**。
2. 如果有攻击发生，管理用户将在监控页面看到 IPS 检测的报警日志。