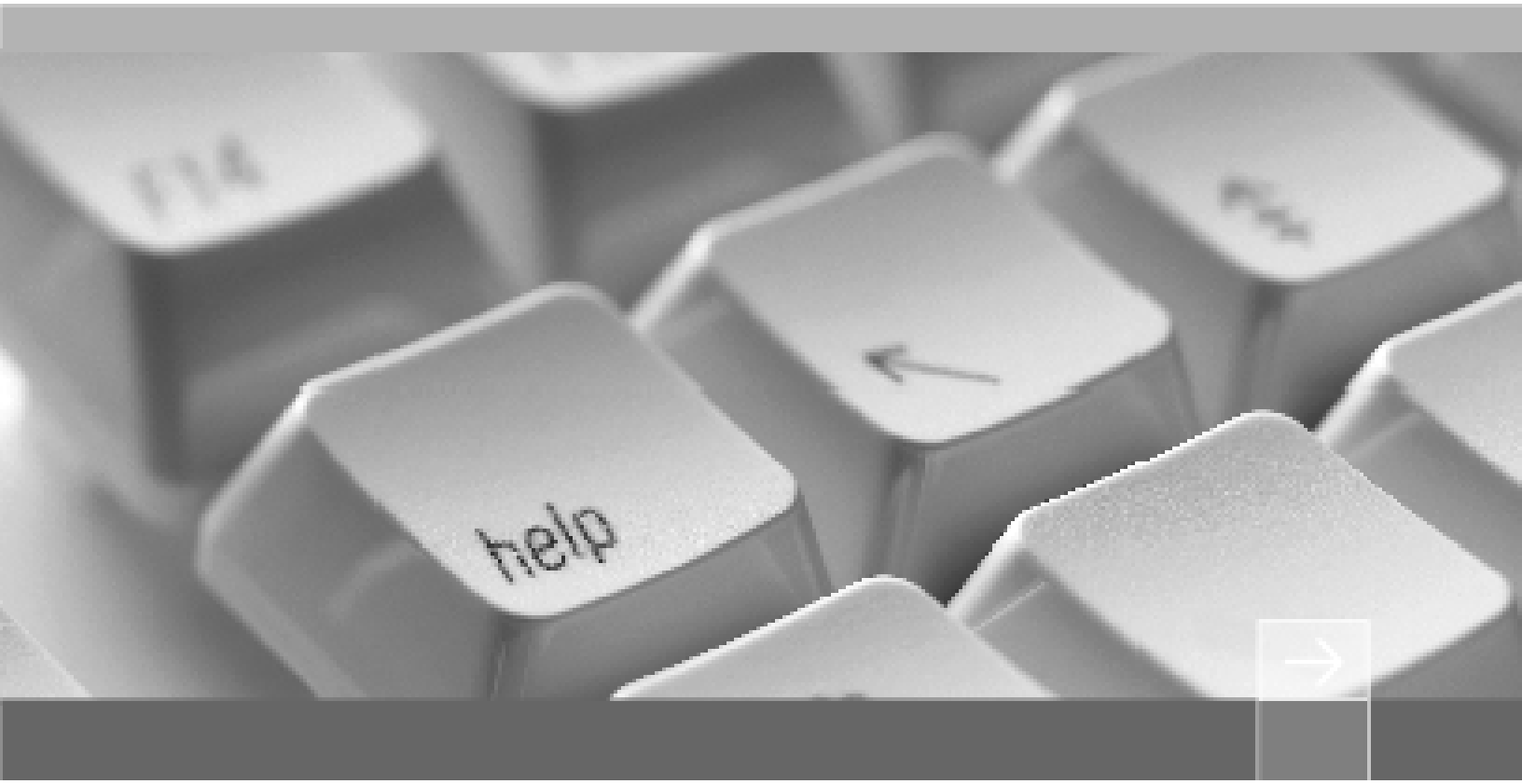
IT SOLUTIONS & SERVICES



东软 NetEye 集成安全网关入侵防御系统快速向导

Neusoft

本向导描述以下内容：

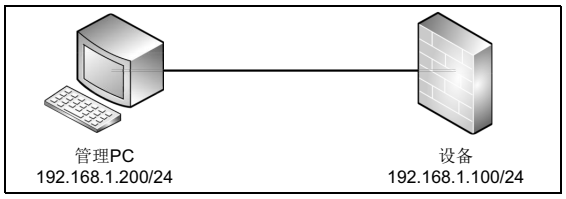
1. 安装硬件设备和系统

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。
本文以含有 MGT 口和 ETH-sxpx 接口为例进行阐述。

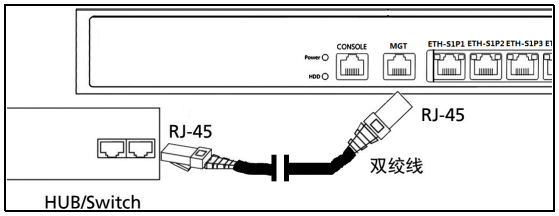
2. 连接设备和管理 PC



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。

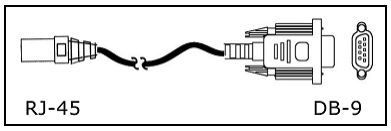
用于管理 NISG-IPS 的管理 PC 上至少安装有以下一种浏览器：

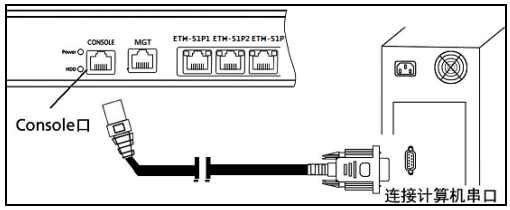
- Microsoft Internet Explorer （7.0 或更高版本）
- Mozilla Firefox （10.0 或更高版本）
- Google Chrome （9.0 或更高版本）
- Opera （11.x 或更高版本）
- Safari （5.0 或更高版本）

2.2 连接 Console 口

Console 访问默认是允许的，管理员可以通过 Console 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：

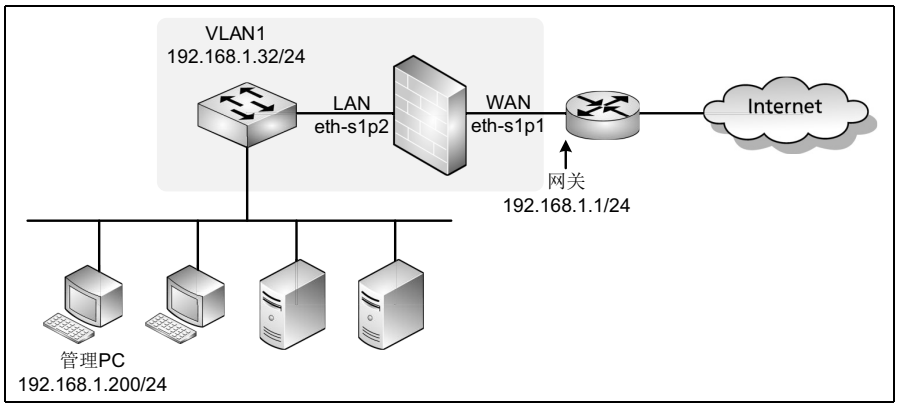
- 波特率：9600
- 数据位：8
- 奇偶校验位：无
- 停止位：1

3. 部署 NISG-IPS 到网络

选择一种工作模式，并将 NISG-IPS 部署到网络中：

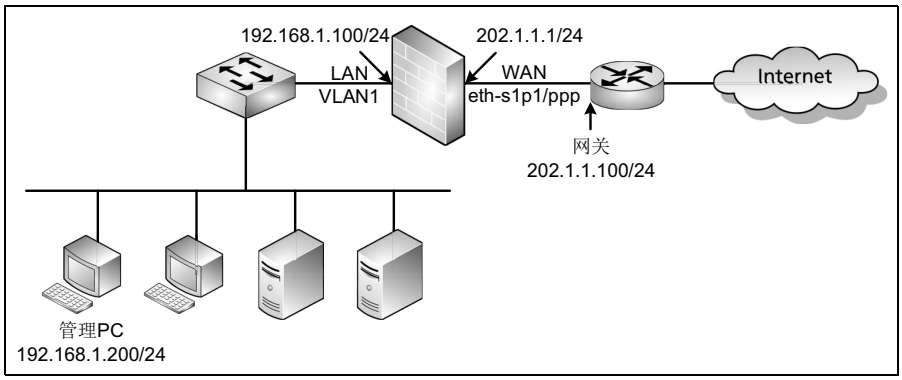
3.1 透明模式

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。



3.2 路由模式

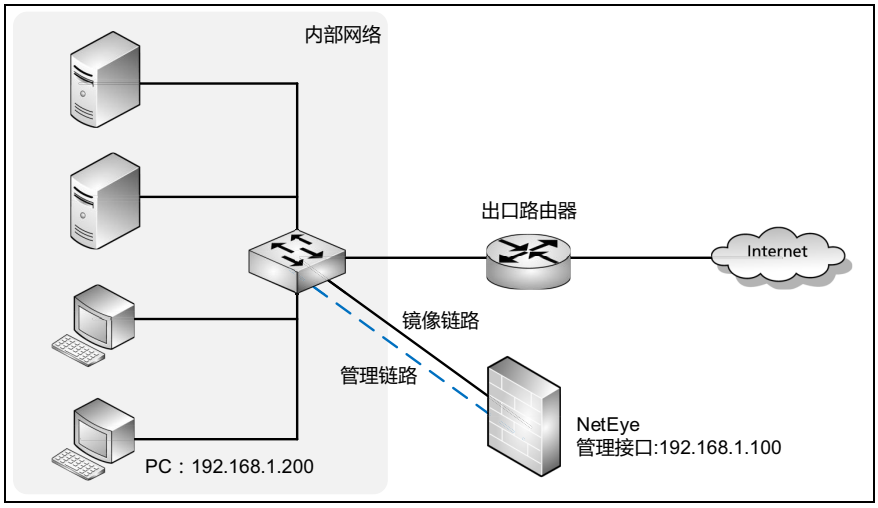
NISG-IPS 可部署在公网和私网之间，作为局域网内主机的默认网关。路由模式下，NISG-IPS 可以让工作在不同网段之间的主机以三层路由的方式进行通信。



后续小节都按照此处两种模式的拓扑描述如何对 NISG-IPS 进行配置。

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。



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。

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。

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。

4.2 设置系统语言 / 主机名 / 系统时间

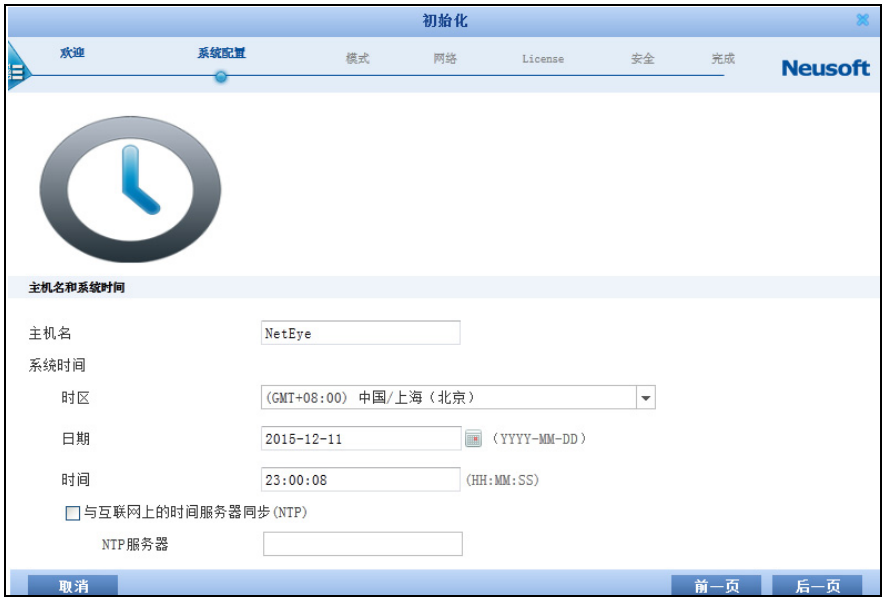
4. 登录后系统弹出**欢迎**页面。在下拉框中选择相应的语言，点击**后一页**。

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. 选择一种部署模式
   - 4.3 配置透明模式
   - 4.4 配置路由模式
   - 4.5 配置旁路模式

4.3 配置透明模式

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。

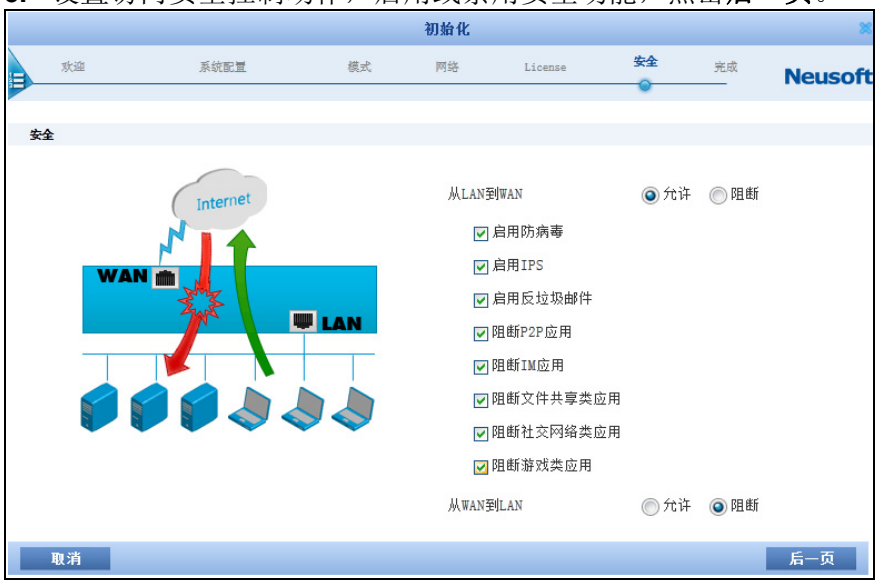
4. 点击**是**，然后点击**结束**，提交所做的基本配置并继续进行安全配置；或者点击**否**，然后点击**结束**，提交所做的基本配置并退出向导。

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。

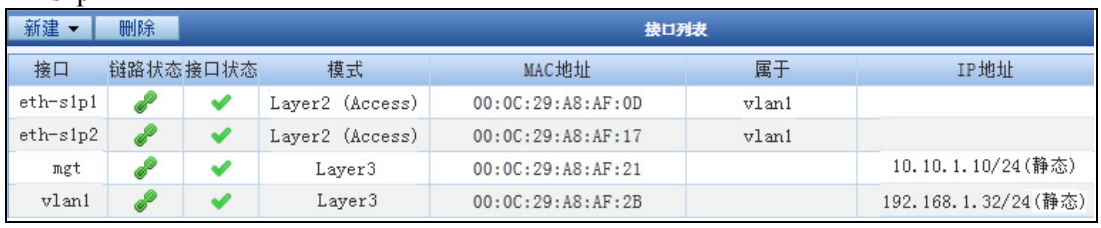
提示：如果在向导中执行了激活 License 操作，系统将出现重启提示，请根据提示重启系统。否则， License 将不会生效。重启过程将持续三分钟左右，请三分钟后再进行登录。

4.3.2 通过 WebUI 确认初始化配置

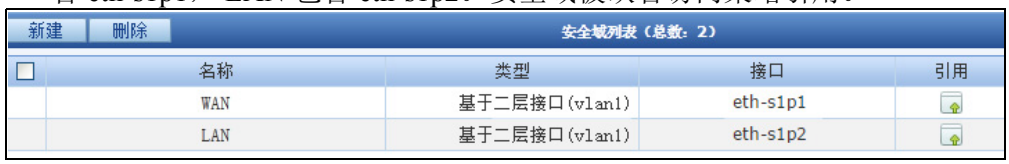
要确认初始化配置是否生效，请执行以下操作：

1. 输入缺省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。

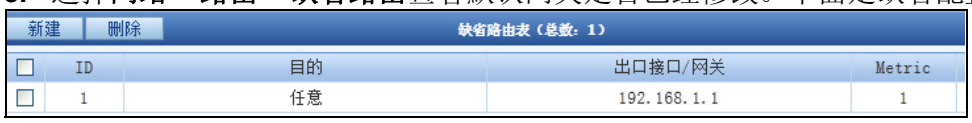
3. 选择**网络 > 接口**查看接口配置。可以看到新建 VLAN 接口 vlan1 包含 eth-s1p1 和 eth-s1p2。



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。

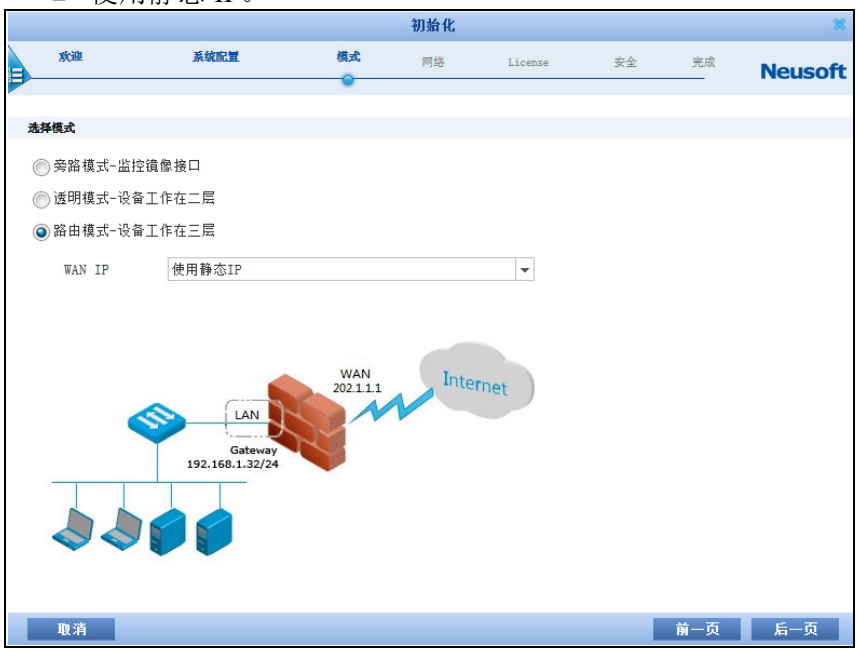
7. 选择**系统 > 服务配置 > 访问设置**查看服务是否已被启用或禁用。

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。

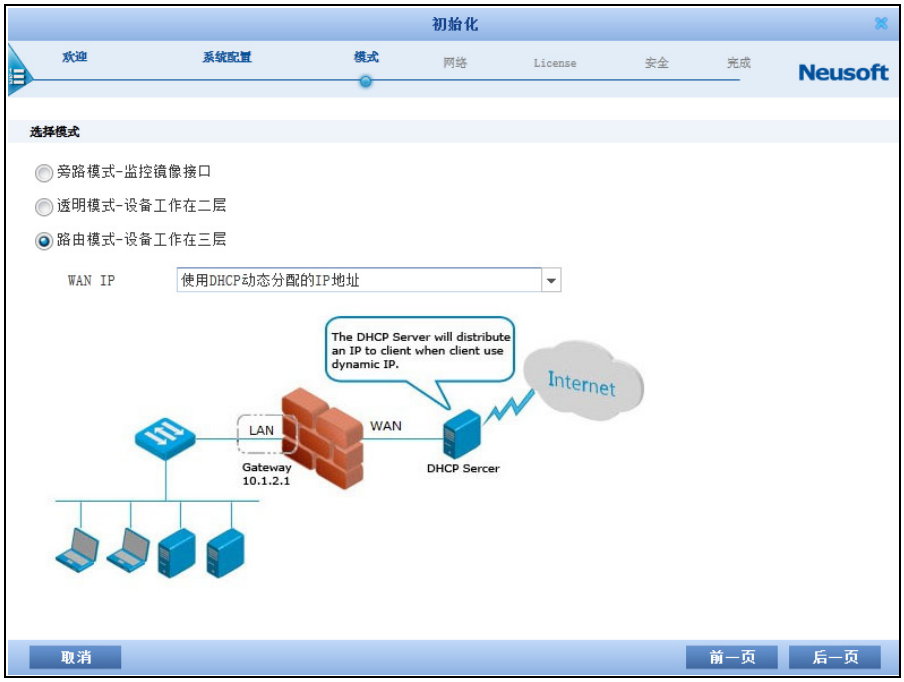
4.4 配置路由模式

4.4.1 网络和安全配置

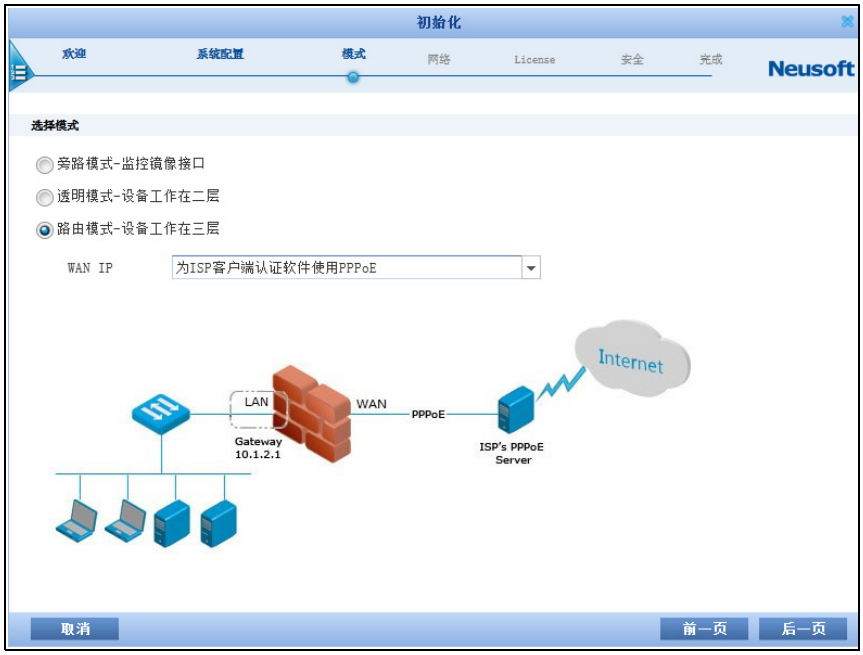
1. 选择**路由模式**。选择以下任意一种 WAN 接口获取 IP 地址的方式。点击**后一页**。
   - 使用静态 IP。



   - 使用 DHCP 动态分配的 IP 地址。

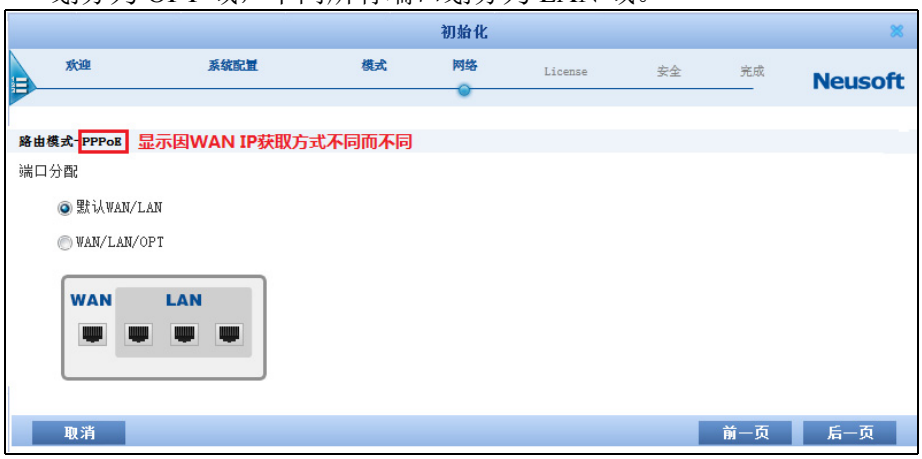


- 为 ISP 客户端认证软件使用 PPPoE。

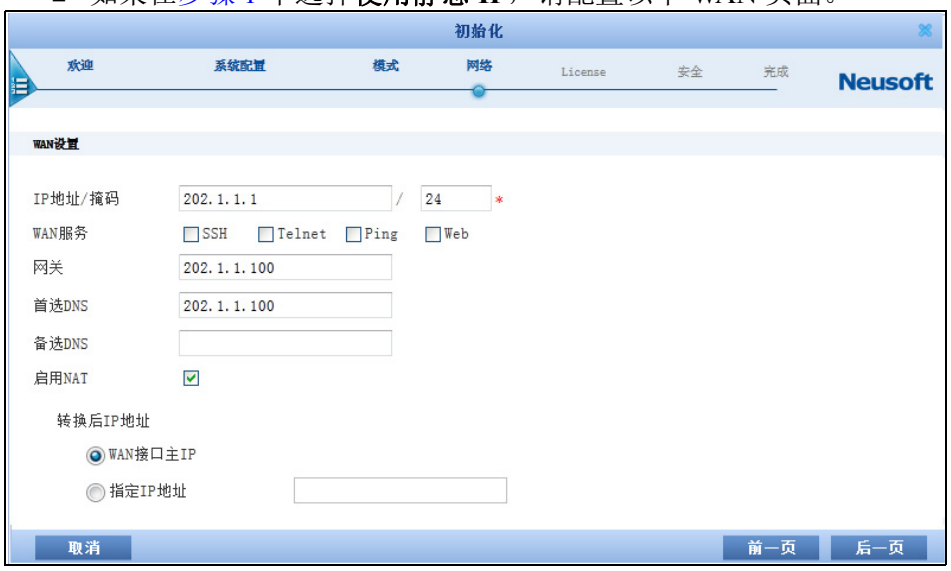


2. 配置设备端口分配，点击**后一页**。

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。

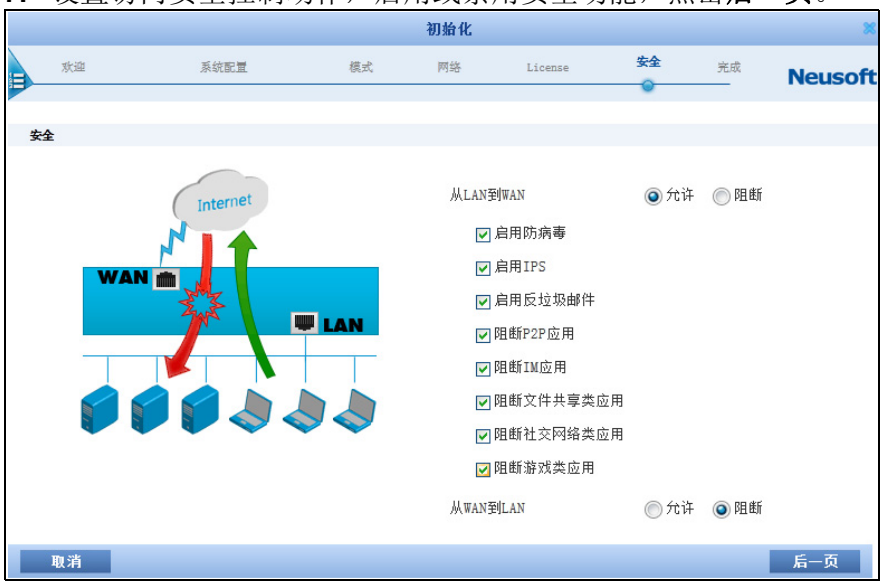
5. 点击**是**，然后点击**结束**，提交所做的基本配置并继续进行安全配置；或者点击**否**，然后点击**结束**，提交所做的基本配置并退出向导。

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。

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. 输入缺省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。

4.5 配置旁路模式

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 5.8 导入 License。

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。

5. 使用 WebUI 进行初始化配置

5.1 登录

1. 通过 WebUI 向导登录，步骤同 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。

5.2 WebUI 概述

WebUI 操作按钮如下表所示。

表 1 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		

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**。

2. 点击 修改密码。

3. 点击**确定**。新密码在下次登录时生效。

5.4 设置系统语言 / 主机名 / 系统时间

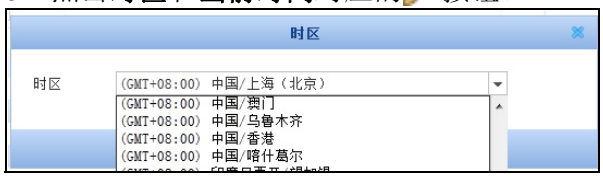
1. 选择**系统 > 概述**。

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**。点击。

5.5 配置透明模式

1. 选择**网络 > 接口**。设置接口如下：

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	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-s1p1 到 WAN，添加 eth-s1p2 到 LAN。

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：

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	✔

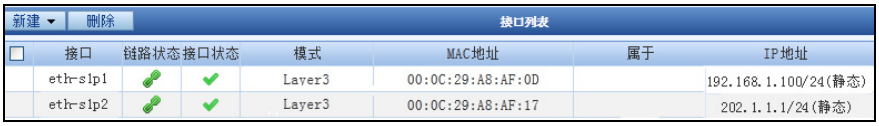
4. 点击。

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。

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。

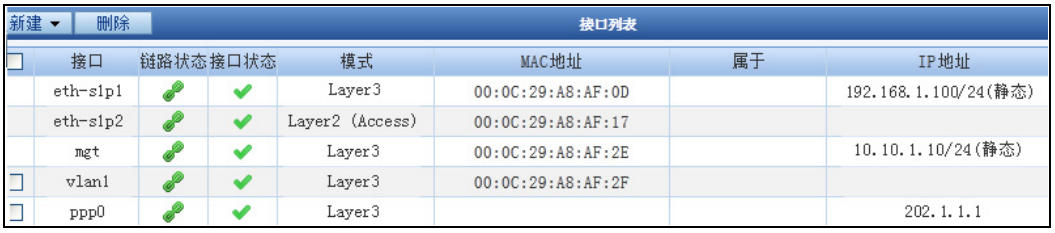
4. 创建 SNAT 规则，将 192.168.1.0/24 转换成 eth-s1p2 的 IP 地址：

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 。

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。

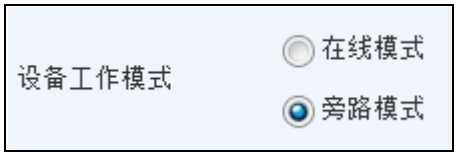
4. 创建 SNAT 规则，将 192.168.1.0/24 转换为 ppp0 的 IP 地址。

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

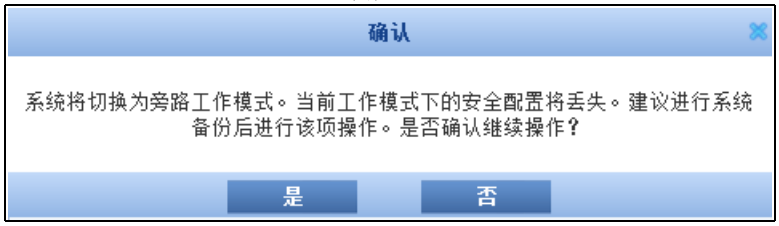
6. 点击 。

5.7 配置旁路模式

1. 选择**网络 > 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。

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。

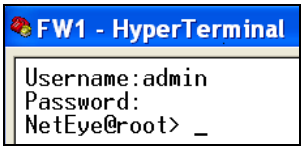
6. 使用 CLI 进行初始化配置

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。

6.2 CLI 基本信息

首次登录 CLI 会出现如下提示符：

NetEye@root>

在此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：

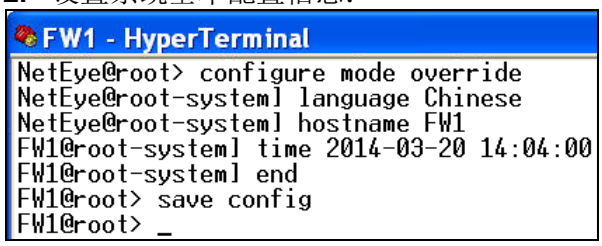
- 在关键字或参数后输入 "**?**"，系统会提示该关键字或参数的帮助信息。
- 在关键字或参数后面加空格，然后再输入 "**?**"，系统会提示下一个关键字或参数。
- 可以通过按 Tab 键，补齐当前输入的关键字。如果有多个可选关键字，按 Tab 键则显示所有关键字。
- 支持缩写。例如，可以将命令 **configure mode** 缩写为 **con mo**。

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> _
```

6.3 设置系统语言 / 主机名 / 系统时间

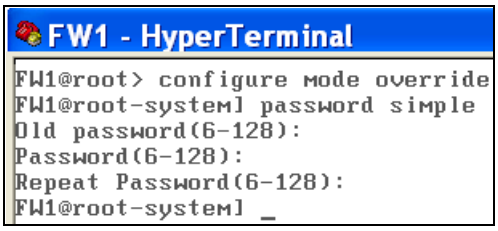
1. 使用 **show system info** 命令查看系统信息。
2. 设置系统基本配置信息：



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。



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
```

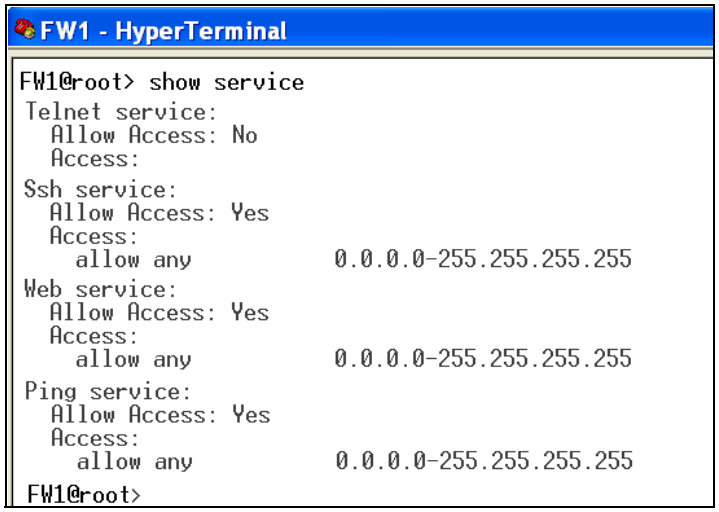
3. 查看安全域信息：

```
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。

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。

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 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。

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] bold 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。

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

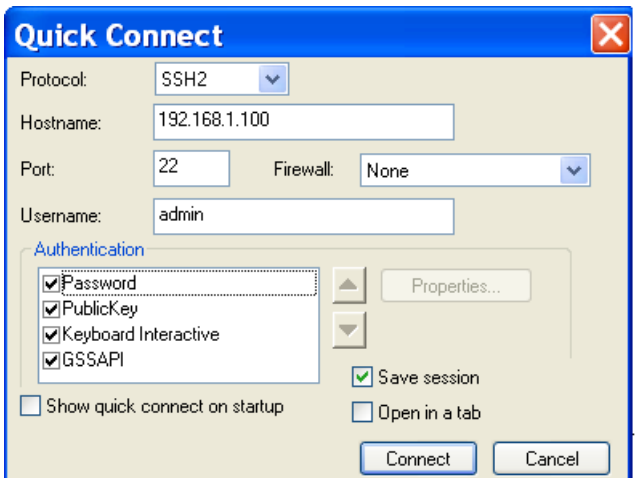
```
FW1@root-system] license import from tftp 192.168.1.200 FW1.dat

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。

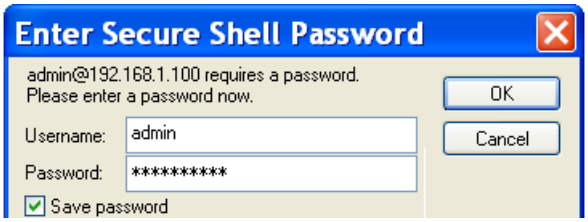
3. 重启后重新登录，并继续通过 CLI Console 配置 NISG-IPS。

6.8 使用 SSH 登录

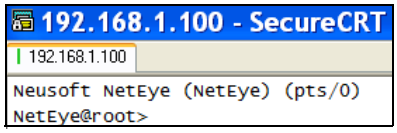
1. 打开 SecureCRT，点击 **Quick Connect**。在 **Hostname** 文本框中输入 NISG-IPS 的管理 IP 地址，在 **Username** 文本框中输入缺省用户名。点击 **Connect**。



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。



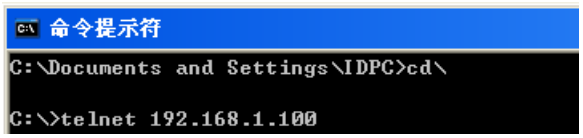
6.9 使用 Telnet 登录

Telnet 服务默认是关闭的。

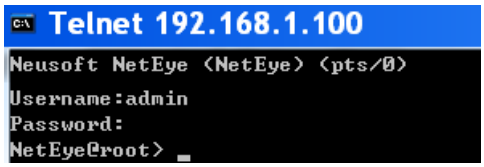
1. 使用 Telnet 连接之前，需要先通过 CLI Console 启用 Telnet 服务：

```
NetEye@root> configure mode override
NetEye@root-system1 service telnet on
NetEye@root-system1 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。



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。

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 5.8 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 服务器在同一子网。
- 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。

沈阳浑南新区新秀街 2 号
客服热线：400 655 6789
http://neteye.neusoft.com