H3C ER G3 系列路由器

典型配置案例集

新华三技术有限公司
http://www.h3c.com

资料版本：6W100-20201120

环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

前 言

本配置指导主要介绍 H3C ER G3 系列路由器 典型配置案例。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

3. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

4. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

1 典型配置举例 导读

H3C ER G3 系列路由器 典型配置举例共包括 6 个文档，介绍了 ER G3 系列路由器常用特性的典型配置举例，包含组网需求、配置步骤和验证配置等内容。

1.1 适用款型及软件版本

本手册所描述的内容适用于 ER G3 系列路由器 Release 0107 及其以上版本。

1.2 内容简介

手册包含的文档列表如下：

编号	名称
1	H3C ER G3系列路由器登录Web界面典型配置举例
2	H3C ER G3系列路由器管理账户典型配置举例
3	H3C ER G3系列路由器静态路由典型配置举例
4	H3C ER G3系列路由器IPsec VPN典型配置举例
5	H3C ER G3系列路由器NAT一对一映射典型配置举例
6	H3C ER G3系列路由器包过滤防火墙典型配置举例

登录 Web 界面典型配置举例

目 录

1 简介

本文档介绍登录路由器 Web 界面的典型配置举例。

设备支持 HTTP（Hypertext Transfer Protocol，超文本传输协议）和 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）两种 Web 访问方式。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

3 使用限制

- 建议使用以下浏览器访问 Web：Chrome 57.0 及以上版本、Firefox 35.0 及以上版本、Internet Explorer 10.0 及以上版本。
- 使用的浏览器必须要设置能接受第一方 Cookie（即来自站点的 Cookie），并启用活动脚本（或 JavaScript），才能正常访问 Web。以上功能在不同浏览器中的名称及设置方法可能不同，请以实际情况为准。
- 使用 Internet Explorer 浏览器时，还必须启用以下两个功能，才能正常访问 Web：对标记为可安全执行脚本的 ActiveX 控件执行脚本、运行 ActiveX 控件和插件。
- 更改设备的软件版本后，建议在登录 Web 页面之前先清除浏览器的缓存，以便正确地显示 Web 页面。

4 配置举例

4.1 组网需求

本举例适用于首次登录设备 Web 界面。

如图 1 所示，Host 与设备通过直连方式相连。通过本配置，使 Host 可以通过 Web 方式登录设备。

图1 登录 Web 界面配置组网图

4.2 使用版本

本举例适用于 Release 0107 及其以上版本。

4.3 配置步骤

1. 使用缺省的 Web 登录信息登录 Web 界面

(1) 连接设备和 Host

用以太网线将 Host 和设备上的 LAN 口相连。

(2) 配置 Host 为自动获取 IP 地址，或手工配置 Host 的 IP 地址为 192.168.1.2/24（即与设备 IP 地址在同一个网段），保证其能与设备互通。

(3) 启动浏览器

在 Host 上启动浏览器，在浏览器的地址栏中输入“http://192.168.1.1”，然后回车，进入设备的 Web 登录页面。

(4) 输入登录信息

首次登录时，请输入缺省用户名和密码进行登录。缺省的 Web 登录信息包括：

- 用户名：admin
- 密码：admin
- 用户角色：network-admin
- 管理 IP 地址：192.168.1.1/24

在登录页面中输入用户名 admin、密码 admin，单击<登录>按钮登录 Web 页面。登录成功之后，即可通过 Web 页面对设备进行管理。

图2 Web 登录页面

(5) 修改缺省 Web 登录密码。

首次登录 Web 页面后，系统会提示修改缺省登录密码，设置新密码后，单击<确定>按钮，完成缺省 Web 登录密码修改并进入设备的 Web 管理页面。

图3 修改缺省 Web 登录密码

管理账户典型配置举例

目 录

1 简介

本文档介绍通过 Web 界面配置路由器管理账户的配置方式。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解管理账户特性。

3 使用版本

本举例适用于 Release 0107 及其以上版本。

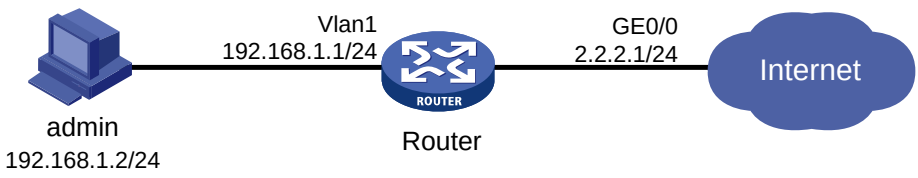
4 配置举例

4.1 组网需求

在 Router 上配置一个管理账户，用于登录 Router 的 Web 管理页面，具体要求如下：

- 用户使用管理账户登录时，Router 对其进行本地认证；
- 管理账户名称为 webuser，密码为 admin12345；
- 通过认证之后，用户被授予角色 Administrator。

图1 管理账户配置组网图



4.2 配置步骤

(1) 选择场景

在页面左侧导航栏选择“网络设置 > 外网配置”，进入外网配置页面。在配置接口模式页面选择单 WAN 场景、双 WAN 场景或者多 WAN 场景。（本举例以单 WAN 场景为例，用户可以根据实际情况进行选择。）

图2 选择场景

(2) 配置 WAN 口

在页面左侧导航栏选择“网络设置 > 外网配置 > WAN 配置”，点击指定线路对应的操作列编辑图标，进入修改 WAN 配置页面。选择连接模式，选择固定地址，配置 IP 地址、子网掩码以及开启 NAT 地址转换功能，其他配置项均保持默认情况即可。单击<确定>按钮，完成 WAN 配置。（本举例以配置固定 IP 地址方式为例，用户可以根据实际情况进行选择。）

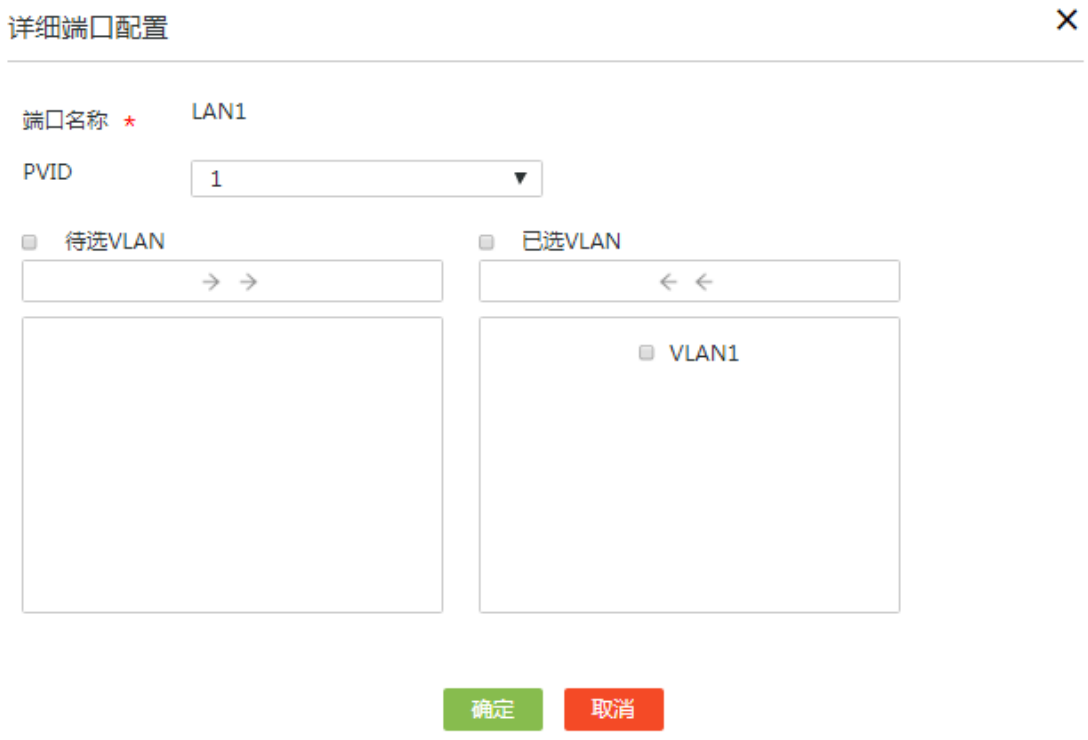
图3 修改 WAN 口

(3) 配置 LAN 口

在页面左侧导航栏选择“网络设置 > LAN 配置”，单击“VLAN 划分”页签，进入 VLAN 划分页面，然后在端口列表中，点击指定端口对应的操作列编辑图标配置端口加入 VLAN1。单击“VLAN 配置”页签，进入 VLAN 配置页面，点击<添加>按钮，进入添加 LAN 的配置页面。选择需要配置的接口 VLAN1，配置 IP 地址、子网掩码，开启 DHCP 服务，配置 IP 地址范围、网关地址以及 DNS，其他配置项均保持默认情况即可。单击<确定>按钮，完成 LAN 配置。

图4 配置 LAN 口

图5 详细端口配置



(4) 开启 HTTP/HTTPS 服务

在页面左侧导航栏选择“系统工具 > 远程管理”进入远程管理页面，然后选择 HTTP/HTTPS 进入 HTTP/HTTPS 页面，选择用户登录的接口并指定允许 HTTP/HTTPS 远程登录。在“管理员列表”区段，点击<添加/编辑>按钮，添加允许访问 Web 管理页面的管理员 IP 地址或地址段。

图6 开启 HTTP/HTTPS 服务

图7 添加/编辑管理员 IP 地址

静态路由典型配置举例

目 录

1 简介

本文档介绍路由器静态路由典型配置举例。

静态路由是一种特殊的路由，由管理员手工配置。配置静态路由后，去往指定目的地的数据报文将按照管理员指定的路径进行转发。

在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。

静态路由的缺点在于：不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IP 静态路由特性。

3 使用限制

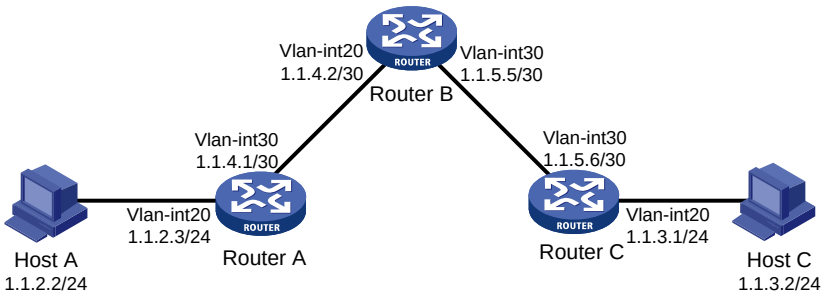
静态路由的配置必须确保下一跳网络可达，并且下一跳设备也必须存在到本设备和目的地址的路由。

4 配置举例

4.1 组网需求

如图 1 所示，在 Router A、Router B、Router C 上配置静态路由，实现 Host A 以及 Host C 的相互访问。

图1 静态路由配置组网图



4.2 使用版本

本举例适用于 Release 0107 及其以上版本。

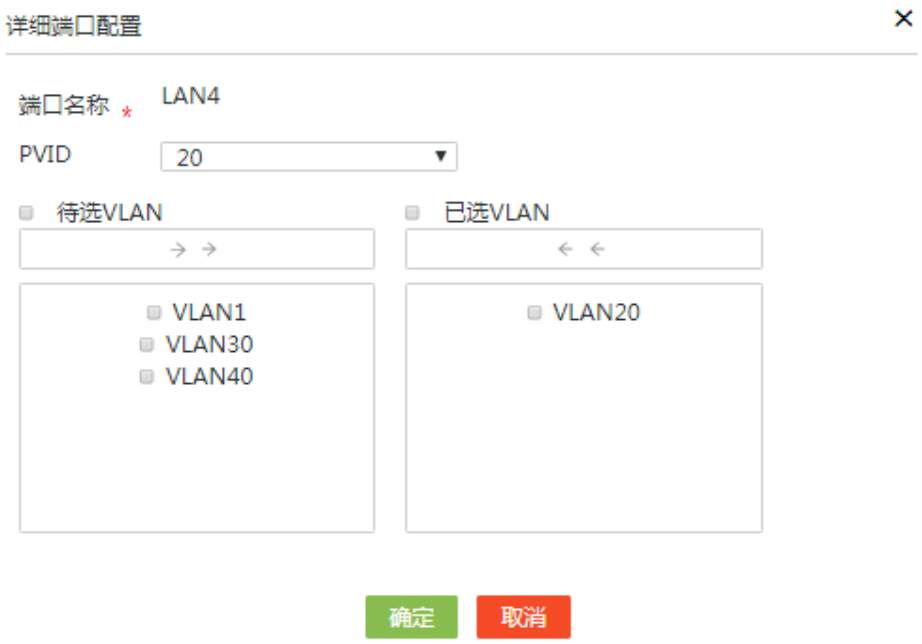
4.3 配置步骤

4.3.1 配置 Router A

(1) 接口 IP 地址配置

在页面左侧导航栏选择“网络设置 > LAN 配置”，单击“VLAN 划分”页签，进入 VLAN 划分页面，然后在端口列表中，点击指定端口对应的操作列修改图标配置端口加入 VLAN。

图2 将 LAN4 口加入 VLAN 20



单击“VLAN 配置”页签，进入 VLAN 配置页面，点击<添加>按钮，进入配置 VLAN 的配置页面。选择需要配置的接口 VLAN，配置 IP 地址、子网掩码，开启 DHCP 服务，配置 IP 地址范围、网关地址以及 DNS，其他配置项均保持默认情况即可。单击<确定>按钮，完成 LAN 配置。

图3 配置 VLAN 20 的接口 IP 地址

按照同样的步骤配置接口 LAN5，配置如下：

图4 将 LAN5 口加入 VLAN 30

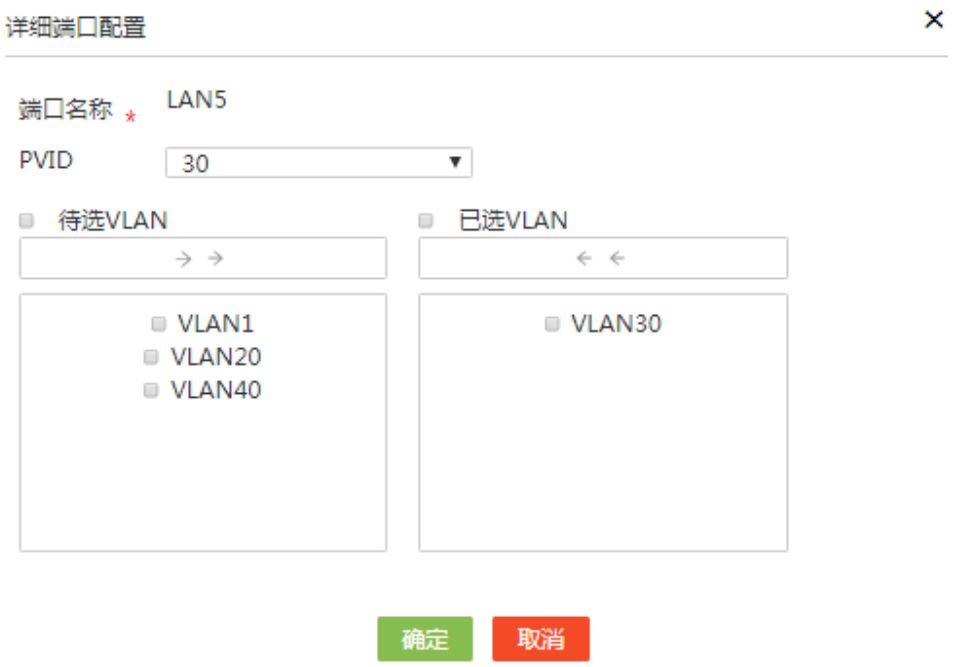


图5 配置 VLAN 30 的接口 IP 地址

(2)　配置静态路由

选择“高级选项 > 静态路由”，进入静态路由配置页面, 单击<添加>按钮，配置如下图所示。

图6 配置静态路由

单击<确定>按钮，完成静态路由配置。

4.3.2 配置 Router B

#配置接口 IP 地址，配置步骤参考 Router A 的配置。

配置两条分别到 Router A 1.1.2.0/24 网段和 Router C 1.1.3.0/24 网段的静态路由，确保 RouterB 和 Router A、Router C 路由可达，配置步骤参考 Router A 的配置。

4.3.3 配置 Router C

#配置接口步骤参考 Router A 的配置。

配置到 Router A 1.1.2.0/24 网段的静态路由，配置步骤参考 Router A 的配置。

5 验证配置

Host A 主机可以 Ping 通 Host C 的地址。

```
C:\Users\abc>ping 1.1.3.2

正在 Ping 1.1.3.2 具有 32 字节的数据:
来自 1.1.3.2 的回复: 字节=32 时间=1ms TTL=252
来自 1.1.3.2 的回复: 字节=32 时间=1ms TTL=252
```

来自 1.1.3.2 的回复: 字节=32 时间=1ms TTL=252
来自 1.1.3.2 的回复: 字节=32 时间=1ms TTL=252

1.1.3.2 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms，最长 = 1ms，平均 = 1ms

IPsec VPN 典型配置举例

目 录

1 简介

本文档介绍路由器 IPsec VPN 功能的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IPsec VPN 特性。

3 使用版本

本举例适用于 Release 0107 及其以上版本。

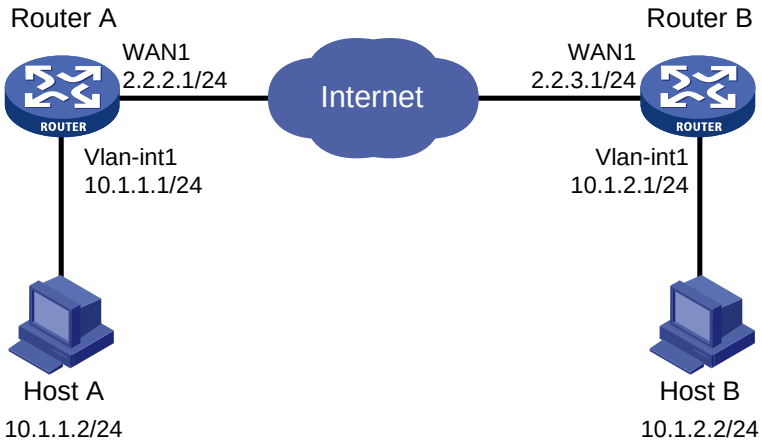
4 配置举例

4.1 组网需求

出于安全因素，需要对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护，因此需要在 Router A 和 Router B 之间建立一条 IPsec 隧道，如图 1 所示。具体要求如下：

- 组网方式为点到点。
- IKE 协商方式建立 IPsec SA。

图1 IPsec VPN 典型配置组网图



4.2 配置步骤

1. 配置 Router A

(1) 配置 LAN 口的 IP 地址

说明

修改 Vlan-interface1 接口 IP 地址会导致 web 登录异常，需要用新的 Vlan-interface1 IP 地址登录 web。

选择“网络设置 > LAN 配置”，进入 LAN 配置页面。单击“VLAN 配置”页签，进入 VLAN 配置页面，点击指定端口对应的操作列编辑图标，进入修改 LAN 配置页面，配置如下参数：

- IP 地址：10.1.1.1；
- 子网掩码：255.255.255.0；
- IP 地址范围：10.1.1.2~10.1.1.254；
- 网关地址：10.1.1.1；
- DNS1：10.1.1.1；
- 其它配置项均保持默认情况即可。单击<确定>按钮保存配置。

图2 修改 LAN 配置

(2) 配置 WAN 口的 IP 地址

选择“网络设置 > 外网配置”，进入外网配置页面。根据实际应用场景，在配置接口模式页面选择单 WAN 场景、双 WAN 场景或者多 WAN 场景。以单 WAN 场景为例，线路 1 选择 WAN1，单击<应用>按钮确定。

图3 配置 WAN 场景

在外网配置页面单击“WAN 配置”页签，进入 WAN 配置页面，点击指定端口对应的操作列编辑图标，进入修改 WAN 配置页面，配置如下参数：

- 连接模式：固定地址；
- IP 地址：2.2.2.1；
- 子网掩码：255.255.255.0。
- 其它配置项均保持默认情况即可。单击<确定>按钮保存配置。

图4 配置 WAN 场景

(3) 配置到达 Host B 所在子网的静态路由

选择“高级选项 > 静态路由”，进入静态路由配置页面。配置步骤为：

- 单击<添加>按钮，进入添加 IPv4 静态路由页面。
- 在添加 IPv4 静态路由页面中配置如下，其中 2.2.2.3 为本例中直连下一跳地址：
  - 目的 IP 地址：10.1.2.0；
  - 掩码长度：24；
  - 出接口：WAN1；
  - 下一跳 IP 地址：2.2.2.3；
  - 其它配置项均保持默认情况即可。单击<确定>按钮保存配置。

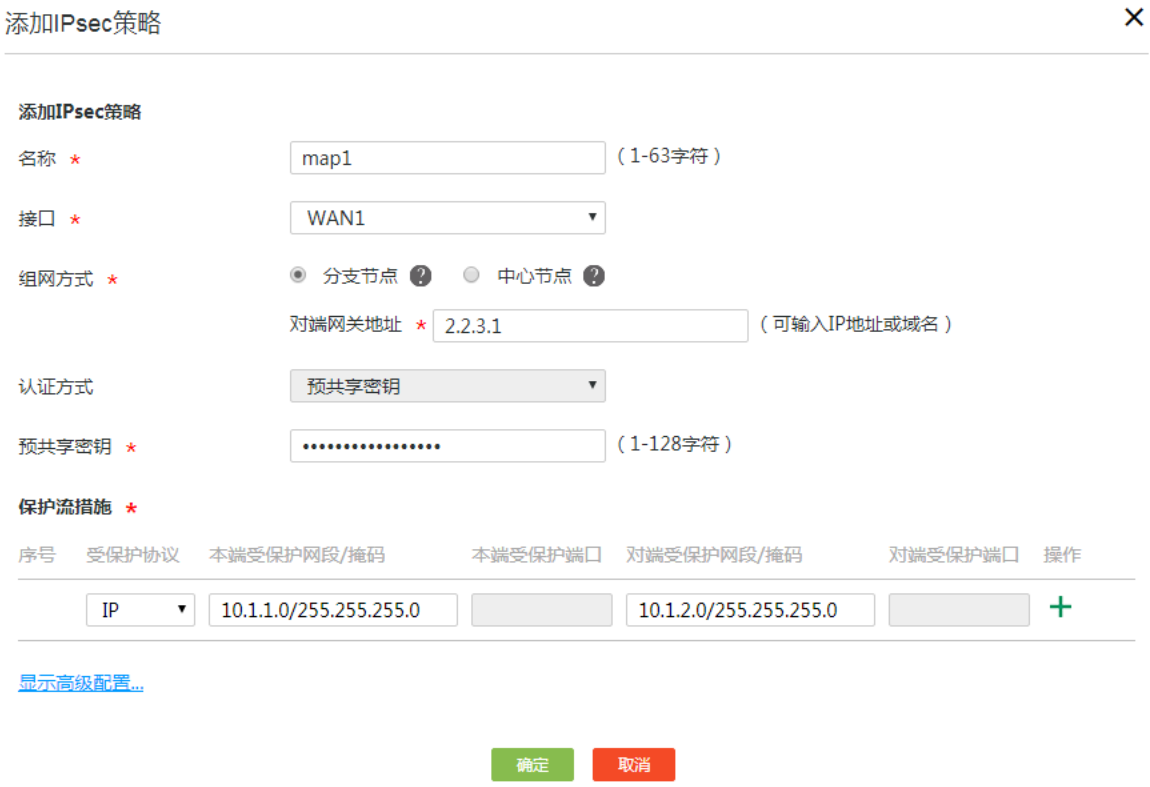
图5 添加静态路由

(4) 配置 IPsec 策略

选择“虚拟专网（VPN） > IPsec VPN”，进入 IPsec 策略配置页面。配置步骤为：

- 在 IPsec 策略页签下单击<添加>按钮，进入添加 IPsec 策略页面。
- 在添加 IPsec 策略页面的基本配置中配置内容如图 6 所示：
  - 名称：map1；
  - 接口：WAN1；
  - 组网方式：分支节点；
  - 对端网关地址：2.2.3.1；
  - 预共享密钥：123456TESTplat&!；
  - 保护流配置：定义保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流，受保护协议选择 IP。本端受保护网段/掩码为 10.1.1.0/0.0.0.255，对端受保护网段/掩码为 10.1.2.0/0.0.0.255。单击<确定>按钮确定添加。

图6 配置 IPsec 策略



- 单击<显示高级配置>按钮，在添加 IPsec 策略页面高级配置的 IKE 配置页签中配置内容如下：
  - 协商模式：主模式；
  - 对端身份类型：选择 IP 地址，且 IP 地址为 2.2.3.1；
  - 对等体存活检测（DPD）：选择关闭；
  - 其它配置项均保持默认情况即可。如图 7、图 8 所示：

图7 定义 ACL 规则保护数据流

图8 修改高级配置

- 先单击<返回基本配置>按钮，再单击<确定>按钮，完成 IPsec 策略的创建。

2. 配置 Router B

(1) 配置 LAN 口的 IP 地址

说明

修改 Vlan-interface1 接口 IP 地址会导致 web 登录异常，需要用新的 Vlan-interface1 IP 地址登录 web。

选择“网络设置 > LAN 配置”，进入 LAN 配置页面。单击“VLAN 配置”页签，进入 VLAN 配置页面，点击指定端口对应的操作列编辑图标，进入修改 LAN 配置页面，配置如下参数：

- IP 地址：10.1.2.1；
- 子网掩码：255.255.255.0。
- IP 地址范围：10.1.2.2~10.1.2.254
- 网关地址：10.1.2.1
- DNS1:10.1.2.1
- 其它配置项均保持默认情况即可。单击<确定>按钮保存配置。

图9 修改 LAN 配置

(2) 配置 WAN 口的 IP 地址

选择“网络设置 > 外网配置”，进入外网配置页面。根据实际应用场景，在配置接口模式页面选择单 WAN 场景、双 WAN 场景或者多 WAN 场景。以单 WAN 场景为例，线路 1 选择 WAN1，单击<应用>按钮确定。

图10 配置 WAN 场景

在外网配置页面单击“WAN 配置”页签，进入 WAN 配置页面，点击指定端口对应的操作列编辑图标，进入修改 WAN 配置页面，配置如下参数：

- 连接模式：固定地址；
- IP 地址：2.2.3.1；
- 子网掩码：255.255.255.0。
- 其它配置项均保持默认情况即可。单击<确定>按钮保存配置。

图11 配置 WAN 场景

(3) 配置到达 Host A 所在子网的静态路由

选择“高级选项 > 静态路由”，进入静态路由配置页面。配置步骤为：

- 单击<添加>按钮，进入添加 IPv4 静态路由页面。
- 在添加 IPv4 静态路由页面中配置如下，其中 2.2.3.3 为本例中直连下一跳地址：
  - 目的 IP 地址：10.1.1.0；
  - 掩码长度：24；
  - 出接口：WAN1；
  - 下一跳 IP 地址：2.2.3.3；
  - 其它配置项均保持默认情况即可。

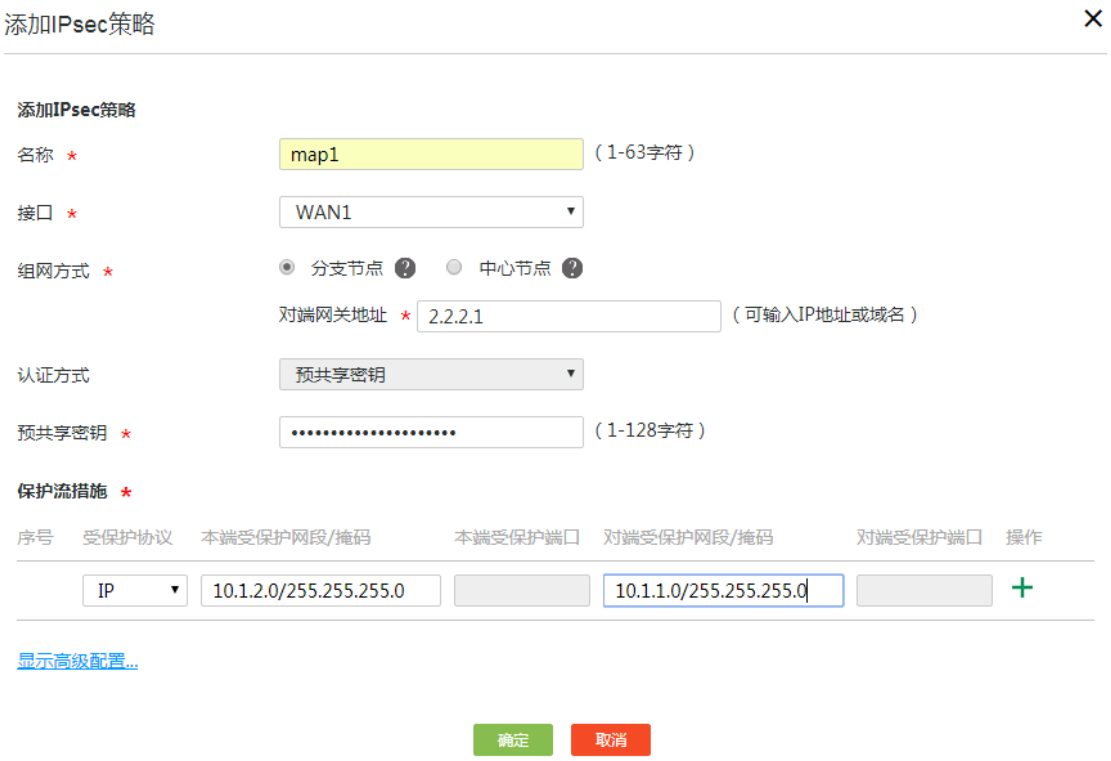
图12 添加静态路由

(4) 配置 IPsec 策略

选择“虚拟专网(VPN) > IPsec VPN”，进入 IPsec 策略配置页面。配置步骤为：

- 在 IPsec 策略页签下单击<添加>按钮，进入添加 IPsec 策略页面。
- 在添加 IPsec 策略页面的基本配置中配置内容如图 13 所示：
  - 名称：map1；
  - 接口：WAN1；
  - 组网方式：分支节点；
  - 对端网关地址：2.2.2.1；
  - 预共享密钥：123456TESTplat&!；
  - 保护流配置：定义保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流，受保护协议选择 IP。本端受保护网段/掩码为 10.1.1.0/0.0.0.255，对端受保护网段/掩码为 10.1.2.0/0.0.0.255。单击<确定>按钮确定添加。

图13 配置 IPsec 策略



- 单击<显示高级配置>按钮，在添加 IPsec 策略页面高级配置的 IKE 配置页签中配置内容如下：
  - 协商模式：主模式；
  - 对端身份类型：选择 IP 地址，且 IP 地址为 2.2.2.1；
  - 对等体存活检测（DPD）：选择关闭；
  - 其它配置项均保持默认情况即可。如图 14、图 15 所示：

图14 定义 ACL 规则保护数据流

图15 修改 IPsec 配置

- 先单击<返回基本配置>按钮，再单击<确定>按钮，完成 IPsec 策略的创建。

4.3 验证配置

(1) Host A 可以 Ping 通 Host B。

```
C:\Users\abc>ping 10.1.2.2

Ping 10.1.2.2 (10.1.2.2): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 10.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 10.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 10.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 10.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 10.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 10.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
C:\Users\abc>
```

(2) 完成上述配置后，在“虚拟专网(VPN) > IPsec VPN >”的监控信息页签上可以看到添加成功的 IPsec 策略，以 Router A 为例，状态列显示为 Active。

图16 IPsec VPN 监控信息

NAT 一对一映射典型配置举例

目 录

1 简介

本文档介绍路由器 NAT 一对一映射的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 NAT 特性。

3 使用版本

本举例适用于 Release 0107 及其以上版本。

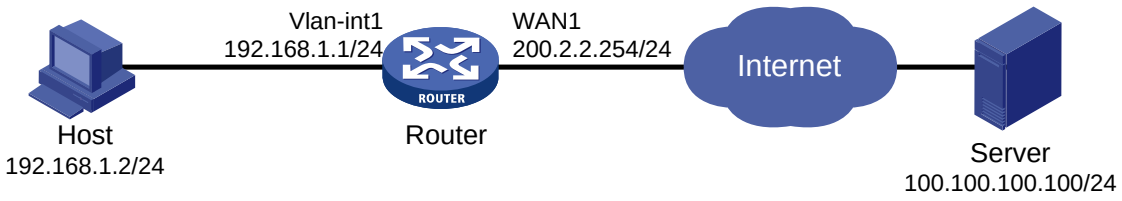
4 配置举例

4.1 组网需求

Host 所在网络的出口处部署了一台路由器设备。现需要使用一对一映射功能，实现将内网用户地址转换为出口公网地址来访问外网。具体需求如下：

内部用户 192.168.1.2/24 使用出口公网地址 200.2.2.254/24 访问 Internet 中地址为 100.100.100.100/24 的 Server。

图1 一对一映射配置组网图



4.2 配置步骤

选择“网络设置 > NAT 配置 > 一对一映射”，勾选开启“一对一映射”。单击<添加>按钮，在弹出的添加 NAT 一对一映射配置对话框中，进行如下配置：

- 内部地址：192.168.1.2
- 外部地址：200.2.2.254
- 接口：WAN1
- 是否启用：启用

单击<确定>按钮，完成配置。

4.3 验证配置

完成上述配置后，NAT 配置页面生成如下表项，且 Host 能顺利访问外网。

包过滤防火墙典型配置举例

目 录

1 简介

本文档介绍路由器包过滤防火墙功能的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解包过滤防火墙特性。

3 使用版本

本举例适用于 Release 0107 及其以上版本。

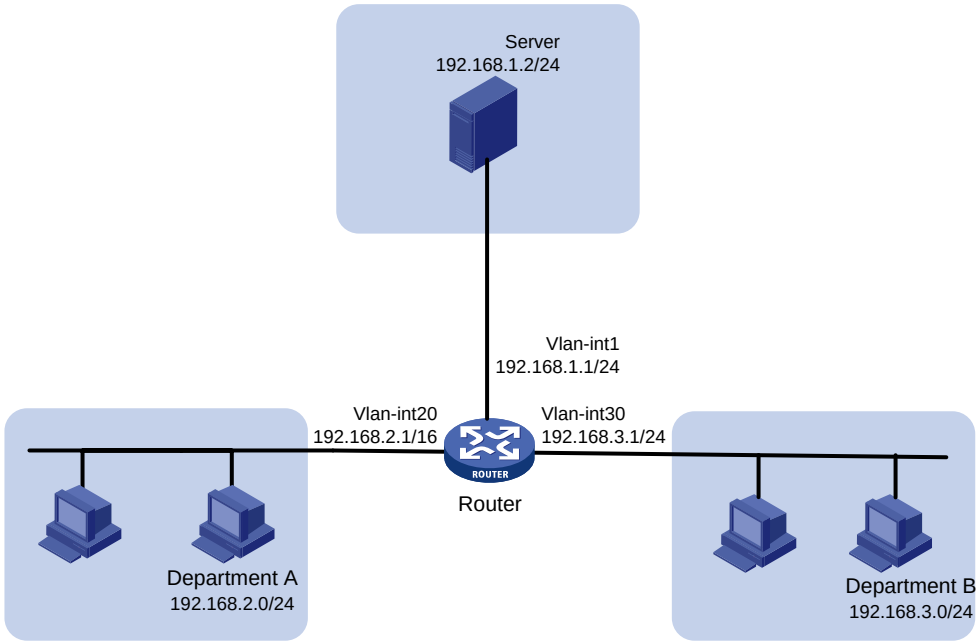
4 配置举例

4.1 组网需求

如图 1 所示，用户通过 Router 连接了 Server 与内网中各部门的 PC，需要根据各部门的业务对访问 Server 的权限进行控制。具体要求如下：

- 允许 Department A 的 PC 在工作时间访问 Server。
- 不允许 Department B 的 PC 在任何时间访问 Server。

图1 包过滤防火墙典型配置组网图



4.2 注意事项

- 当一个接口上配置了多条包过滤防火墙的安全规则时，报文会按照规则的优先级（数值越小优先级越高）从高到低与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程，并对此报文执行规则中的动作。
- 根据包过滤防火墙安全规则的匹配原理，为使接口上配置的安全规则对流经设备的报文能够达到更好、更精准的过滤效果，需要在配置安全规则时遵循“深度优先”的原则，即先配置范围小的，再配置范围大的。

4.3 配置步骤

(1) 配置接口的 IP 地址

选择“网络设置 > LAN 配置”，单击“VLAN 配置”页签，进入 VLAN 配置页面，单击<添加>按钮，进入新建 LAN 配置页面。配置如下参数：

- 名称：VLAN1；
- IP 地址：192.168.1.1；
- 子网掩码：255.255.255.0。

单击<确定>按钮，单击“VLAN 配置”页签，进入 VLAN 配置页面，单击<添加>按钮，进入新建 LAN 配置页面。配置如下参数：

- 名称：VLAN20；
- IP 地址：192.168.2.1；
- 子网掩码：255.255.255.0。

单击<确定>按钮，单击“VLAN 配置”页签，进入 VLAN 配置页面，单击<添加>按钮，进入新建 LAN 配置页面。配置如下参数：

- 名称：VLAN30；
- IP 地址：192.168.3.1；
- 子网掩码：255.255.255.0。

(2) 配置时间组

选择“网络设置 > 时间组”，进入时间组配置页面。配置步骤为：

单击<添加>按钮，进入新建时间组页面。

在新建时间组创建中配置内容如图 2 所示：

- 时间组名称：worktime；
- 生效时间设置：周期性生效；
- 选中周一到周五；
- 输入工作时间段，单击<+>按钮

单击<确定>按钮完成添加。

图2 配置时间组

(3) 配置包过滤防火墙。

选择“网络安全 > 防火墙”，进入包过滤防火墙配置页面。配置步骤为：

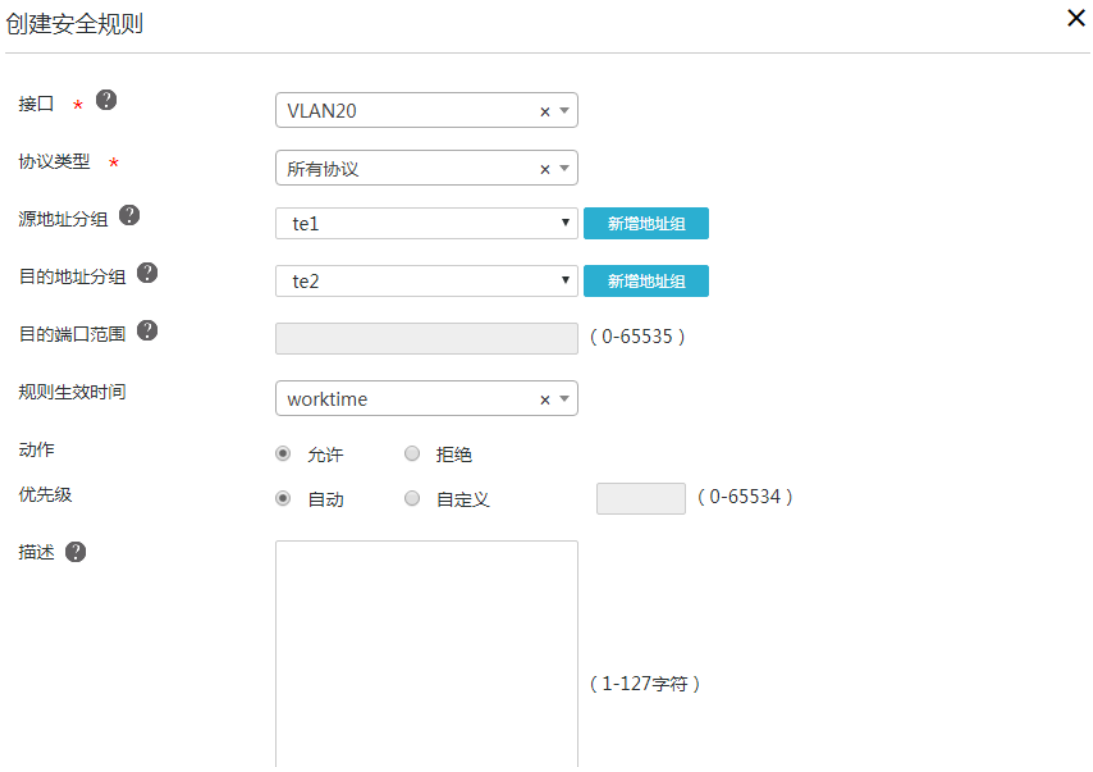
单击<添加>按钮，进入创建安全规则页面。

在创建安全规则页面中配置内容如图 3 所示：

- 接口：VLAN20；
- 协议：所有协议；
- 源地址分组：根据需要选择或者新增地址组；
- 目的地址分组：根据需要选择或者新增地址组；
- 规则生效时间：worktime；
- 动作：允许；
- 优先级：自动；

单击<确定>按钮完成添加。

图3 创建安全规则



单击<添加>按钮，进入创建安全规则页面。

在创建安全规则页面中配置内容如图 4 所示：

- 接口：VLAN30；
- 协议：所有协议；
- 源地址分组：根据需要选择或者新增地址组；
- 目的地址分组：根据需要选择或者新增地址组；
- 动作：拒绝；
- 优先级：自动；

单击<确定>按钮完成添加。

图4 创建安全规则

4.4 验证配置

(1) Department A 的 PC 在工作时间可以 Ping 通 Server。

```
C:\Users\abc>ping 192.168.1.2

Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break

56 bytes from 192.168.1.2: icmp_seq=0 ttl=254 time=0.320 ms

56 bytes from 192.168.1.2: icmp_seq=1 ttl=254 time=0.213 ms

56 bytes from 192.168.1.2: icmp_seq=2 ttl=254 time=0.194 ms

56 bytes from 192.168.1.2: icmp_seq=3 ttl=254 time=0.160 ms

56 bytes from 192.168.1.2: icmp_seq=4 ttl=254 time=0.187 ms


--- Ping statistics for 192.168.1.2 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss

round-trip min/avg/max/std-dev = 0.160/0.215/0.320/0.055 ms
```

(2) Department B 的 PC 不可以 Ping 通 Server。

```
C:\Users\abc>ping 192.168.1.2

Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break

Request time out

Request time out
```

```
Request time out
Request time out
Request time out
```