1 Device 三层直路部署

1.1 适用场景

适用于用户使用安全设备（Device）作为网关，对内网用户使用 DHCP 分配 IP 地址和网络配置参数，对外使用全局 NAT 保证内网可以正常访问外网，并对用户内网数据进行安全防护。在用户购买并安装 Device 后，通过 Device 的 Web 管理页面，可以对业务进行快速部署完成业务开局配置。

1.2 组网需求

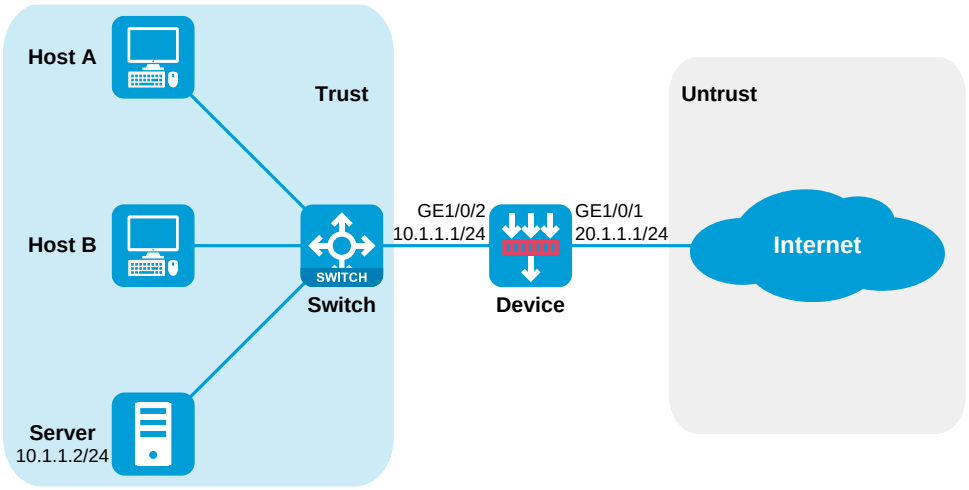
Host A、Host B 和 Server 通过 Switch、Device 与 Internet 通信，应用需求如下：

- Switch 透传 Host、Server 与 Internet 之间的流量。
- Device 作为 Host 的 DHCP 服务器，为 Host 动态分配网段为 10.1.1.0/24 的 IP 地址，DNS 服务器地址为 20.1.1.15，网关地址为 10.1.1.1。
- Device 拥有 20.1.1.1/24 和 20.1.1.2/24 两个外网 IP 地址，内部网络中 10.1.1.0/24 网段的 Host 使用 20.1.1.2/24 地址访问 Internet 地址。
- Server 的内网 IP 地址是 10.1.1.2，Server 使用外网 IP 地址 20.1.1.2 的 21 端口对 Internet 提供 FTP 服务。
- Device 通过安全策略控制匹配的报文进行转发，对不匹配的报文丢弃处理。
- Device 通过默认路由访问 Internet。

说明

本举例使用 F1060 设备 R9360P23 版本进行验证。

图1 Device 三层直路部署组网图



1.3 配置步骤

1. 配置 Device

(1) 登录设备的 Web 界面：

- 用以太网线将 PC 和设备的以太网管理口相连。
- 修改 IP 地址为 192.168.0.0/24（除 192.168.0.1）子网内任意地址，例如 192.168.0.2。
- 在 PC 上启动浏览器，在地址栏中输入 IP 地址“192.168.0.1”后回车，即可进入设备的 Web 登录页面，输入设备默认的用户名和密码（admin/admin），单击<登录>按钮即可登录。

(2) 配置接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 IP 地址，并将 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别加入安全域 Untrust 和 Trust 中：

- 选择“网络>接口>接口”，选中 GE1/0/1 接口，单击 GE1/0/1 的编辑按钮。
- 选择安全域为 Untrust，配置 IP 地址/掩码长度为 20.1.1.1/255.255.255.0，单击<应用>按钮。

图2 编辑 GE1/0/1 安全域和 IPv4 地址

- 选择“网络>接口>接口”，选中 GE1/0/2 接口，单击 GE1/0/2 的编辑按钮。
- 选择安全域为 Trust，配置 IP 地址/掩码长度为 10.1.1.1/255.255.255.0，单击<应用>。

图3 编辑 GE1/0/2 安全域和 IPv4 地址

(3) 配置默认路由使内网可以访问 Internet。

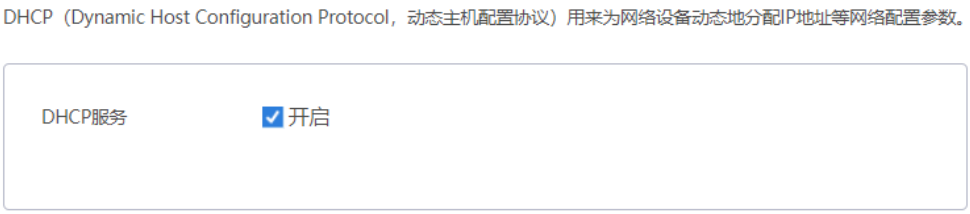
- 选择“网络>路由>静态路由”，单击<新建>，配置目的 IP 地址为 0.0.0.0，掩码长度为 0，下一跳 IP 地址为 20.1.1.3（此处以 20.1.1.3 为例，请以实际情况为准），单击<确定>完成默认路由配置。

图4 配置默认路由

(4) 开启 DHCP 服务，配置 DHCP 地址池 1，用来为 10.1.1.0/24 网段内的客户端分配 IP 地址和网络配置参数：

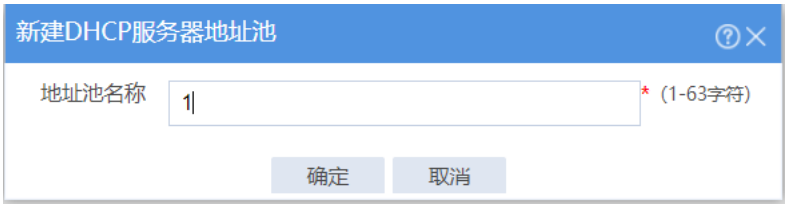
- 选择“网络>DHCP>服务”，单击 DHCP 服务<开启>按钮开启 DHCP 服务。

图5 开启 DHCP 服务



- 选择“网络>DHCP>地址池”，单击<新建地址池>，地址池名称为 1。

图6 配置 DHCP 服务器地址池名称



- 配置 DHCP 地址池动态分配的地址段为 10.1.1.0/24。

图7 配置 DHCP 服务器地址池动态分配地址段

- 配置 DHCP 地址池中不参与自动分配 FTP 服务器 10.1.1.2 的 IP 地址。

```
[Device] dhcp server ip-pool 1
[Device-dhcp-pool-1] forbidden-ip 10.1.1.2
[Device-dhcp-pool-1] quit
```

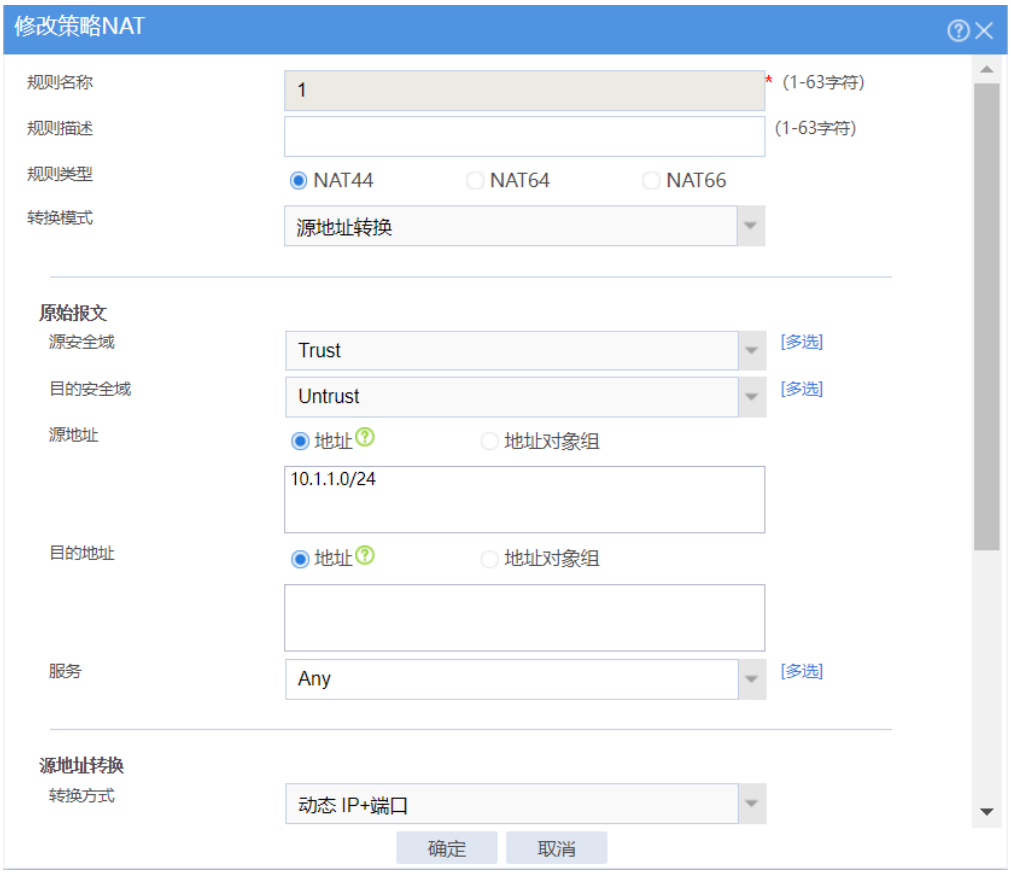
- 单击<地址池选项>，配置 DHCP 地址池的网关为 10.1.1.1，DNS 服务器为 20.1.1.15，单击底部的<确定>完成 DHCP 地址池的配置。

图8 配置 DHCP 服务器地址池网关和 DNS 服务器

(5) 配置全局 NAT 规则和 NAT 地址组，并使全局 NAT 规则使用 NAT 地址组中的地址和端口配置：

- 选择“策略>策略 NAT”，单击<新建>，配置全局 NAT 规则的规则名称为 1，源目的安全域分别为 Trust 和 Untrust，源地址为 10.1.1.0/24，源地址转换的转换方式为动态 IP+端口。

图9 配置全局 NAT 规则 1



- 配置全局 NAT 使用的地址类型为 NAT 地址组，转换为地址为新建的 NAT 地址组 0，配置地址组成员为 20.1.1.2，单击<确定>完成地址组配置，返回后单击<确定>。

图10 配置 NAT 地址组 0

- 选择“策略>策略 NAT”，单击<新建>，配置全局 NAT 规则的规则名称为 2，转换模式为目的地址转换，源安全域为 Untrust，目的地址为 20.1.1.2，服务为 ftp。转换方式为 IP 地址转换，转换为地址为 10.1.1.2，转换为端口为 21，单击<确定>。

图11 配置全局 NAT 规则 2

- 转换方式为 IP 地址转换，转换为地址为 10.1.1.2，转换为端口为 21，单击<确定>。

图12 配置全局 NAT 规则 2

(6) 配置安全策略放行 DHCP 协议报文

- 选择“策略>安全策略”，单击“新建>新建策略”，配置新建策略名称为 dhcpin，源安全域为 Trust，目的安全域为 Local，协议/端口号为 dhcp-client，配置操作动作为允许，单击<确认>完成 dhcpin 策略的配置。

图13 配置安全策略 dhcpin

图14 配置安全策略 dhcpin 的动作

- 选择“策略>安全策略”，单击“新建>新建策略”，配置新建策略名称为 dhcpout，源安全域为 Local，目的安全域为 Trust，协议/端口号为 dhcp-server，配置操作动作为允许，单击<确认>完成 dhcpout 策略的配置。

图15 配置安全策略 dhcpout

图16 配置安全策略 dhcpout 的动作

(7) 配置安全策略放行用户业务报文

- 单击“新建>新建策略”，配置新建策略名称为 trust-untrust，源安全域为 Trust，源 IPv4 地址为 10.1.1.0/24，目的安全域为 Untrust，配置操作动作为允许，单击<确认>完成 trust-untrust 策略的配置。

图17 配置安全策略 trust-untrust

图18 配置安全策略 trust-untrust 的动作

- 单击“新建>新建策略”，配置新建策略名称为 untrust-trust，源安全域为 Untrust，目的安全域为 Trust，目的 IPv4 地址为 10.1.1.2，配置操作动作为允许，单击<确认>完成 untrust-trust 策略的配置。

图19 配置安全策略 untrust-trust

图20 配置安全策略 untrust-trust 的动作

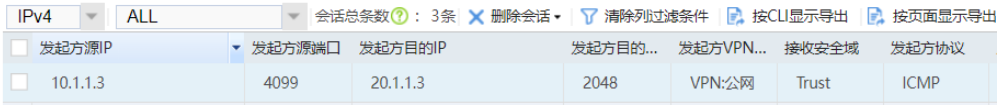
1.4 验证配置

(1) 在 Host A 上去 ping 测试 20.1.1.3 的连通性，可以 ping 通目的地址。

(2) 选择“监控>会话列表”查询 IPv4 会话列表和 NAT 会话表：

- 查询 IPv4 会话列表，发现一条发起方源 IP 地址为 DHCP 地址池中的一个 IP 地址，发起方目的 IP 地址为 20.1.1.3，发起方协议是 ICMP 的会话。

  图21 检查 Device 的 IPv4 会话信息



- 查询 NAT 会话列表，发现一条发起方源 IP 地址为 DHCP 地址池中的一个 IP 地址，发起方目的 IP 地址为 20.1.1.3，发起方协议是 ICMP 的 NAT 会话。

  图22 检查 Device 的 NAT 会话信息