

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：

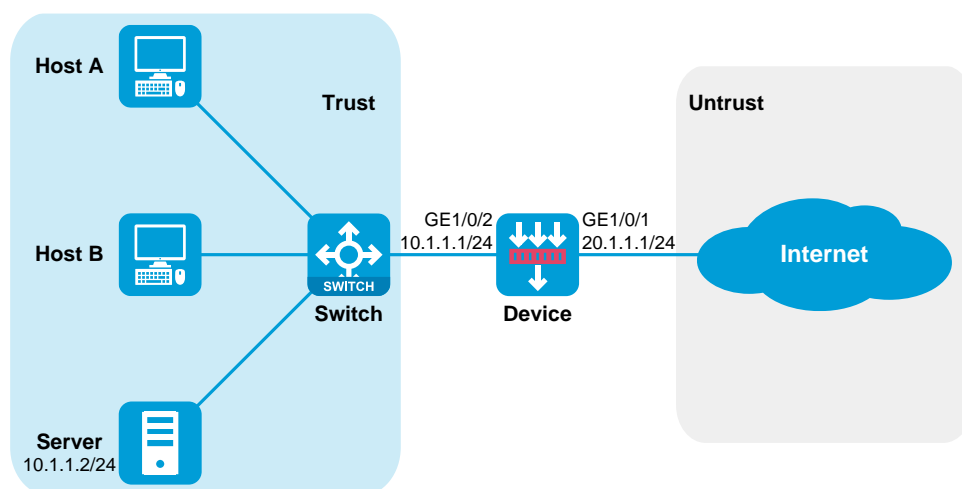
- Switch 透传 Host、Server 与 Internet 之间的流量。
- Device 作为 Host 的 DHCP 服务器，为 Host 动态分配网段为 10.1.1.0/24 的 IP 地址，DNS 服务器地址为 20.1.1.15，网关地址为 10.1.1.1。
- Device 拥有 20.1.1.1/24 和 20.1.1.2/24 两个外网 IP 地址，内部网络中 10.1.1.0/24 网段的 Host 使用 20.1.1.2/24 地址访问 Internet 地址。
- Server 的内网 IP 地址是 10.1.1.2，Server 使用外网 IP 地址 20.1.1.2 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

修改接口设置

名称

GE1/0/1

链路状态

☒ Up
 ☐ 禁用

描述

GigabitEthernet1/0/1 Interface

工作模式

三层模式

安全域

Untrust

不受控协议

本机接收

☐ Telnet
 ☐ Ping
 ☐ SSH
 ☐ HTTP
 ☐ HTTPS
 ☐ SNMP
 ☐ NETCONF over HTTP
 ☐ NETCONF over HTTPS
 ☐ NETCONF over SSH

本机发起

☐ Telnet
 ☐ Ping
 ☐ SSH
 ☐ HTTP
 ☐ HTTPS

基本配置

IPv4地址

IPv6地址

物理接口配置

保持上一跳

☐ 开启
 ☒ 关闭

IP地址

☒ 指定IP地址
 ☐ DHCP
 ☐ PPPoE

IP地址/掩码长度

20.1.1.1

/

255.255.255.0

网关

指定从IP地址
 删除从IP地址

☐ 从IP地址
 掩码
 编辑

应用

确定

取消

- 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

修改接口设置

名称GE1/0/2

链路状态Up禁用

描述GigabitEthernet1/0/2 Interface

工作模式三层模式

安全域Trust

不受控协议?

本机接收

TelnetPingSSHHTTPHTTPS

NETCONF over HTTPNETCONF over HTTPSNETCONF over SSH

本机发起

TelnetPingSSHHTTPHTTPS

基本配置IPv4地址IPv6地址物理接口配置

保持上一跳

开启关闭

IP地址指定IP地址DHCPPPPoE

IP地址/掩码长度205.191.1.1/255.255.255.0

网关

指定从IP地址删除从IP地址

从IP地址掩码编辑

应用确定取消

- (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

新建IPv4静态路由

VRF

公网

目的IP地址

0.0.0.0

掩码长度

0

下一跳

下一跳所属的VRF

出接口

请选择...

下一跳IP地址

20.1.1.3

路由优先级

60

路由标记

0

描述

(1-255, 缺省为60)

(0-4294967295, 缺省为0)

(1-60字符)

确定

取消

(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

DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 用来为网络设备动态地分配IP地址等网络配置参数。

DHCP服务

开启

- 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

1

删除

新建地址池

地址分配

地址池选项

已分配地址

租约有效期限

无限制

1天

0小时

0分

0秒

域名后缀

(1-50字符)

网关

新建

删除

网关

编辑

10.1.1.1

DNS服务器

新建

删除

DNS服务器

编辑

20.1.1.15

(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

修改策略NAT

规则名称

1

(1-63字符)

规则描述

(1-63字符)

规则类型

☒ NAT44

☐ NAT64

☐ NAT66

转换模式

源地址转换

原始报文

源安全域

Trust

[多选]

目的安全域

Untrust

[多选]

源地址

☒ 地址

☐ 地址对象组

10.1.1.0/24

目的地址

☒ 地址

☐ 地址对象组

服务

Any

[多选]

源地址转换

转换方式

动态 IP+端口

确定

取消

- 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

新建NAT地址组

地址组编号

0

*

(0-65535)

地址组名称

(1-63字符)

VRRP备份组

(1-255)

端口范围

1

-

65535

端口块大小

(1-65535)

增量端口块数

(1-5)

地址检测

地址组成员

添加

删除

起始IP地址

结束IP地址

☐

20.1.1.2

20.1.1.2

排除地址组成员

添加

删除

起始IP地址

结束IP地址

确定

取消

- 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

修改策略NAT

规则名称

2

(1-63字符)

规则描述

(1-63字符)

规则类型

☒ NAT44☐ NAT64☐ NAT66

转换模式

目的地址转换

原始报文

源安全域

Untrust

[多选]

源地址

☒ 地址?☐ 地址对象组

目的地址

☒ 地址?☐ 地址对象组

20.1.1.2

*

服务

ftp

[多选]

- 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

修改策略NAT

目的地址

☒ 地址?

☐ 地址对象组

20.1.1.2

服务

ftp

[多选]

目的地址转换

转换方式

IP地址转换

转换为地址

10.1.1.2

转换为端口

21

(1-65535)

IPv4目的备份组

(1-255)

启用规则

☒

统计

☐

高级设置

转换前报文所属VRF

公网

转换后报文所属VRF

公网

确定

取消

(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。

新建安全策略

?

×

常规配置

源IP/MAC地址

目的IP地址

服务

应用与用户

操作

名称 ?

类型

所属策略组

描述信息

源安全域

地址对象组

IPv4地址 ?

目的安全域

地址对象组

IPv4地址 ?

常规配置

名称

dhcpin

☐ 自动命名

类型

☒ IPv4

☐ IPv6

所属策略组

请选择策略组

描述信息

(1-127字符)

源IP/MAC地址

Trust

[多选]

地址对象组

请选择或输入对象组

IPv4地址

目的IP地址

Local

[多选]

地址对象组

请选择或输入对象组

IPv4地址

确定

取消

新建安全策略

常规配置

源IP/MAC地址

目的IP地址

服务

应用与用户

操作

协议/端口号

应用

终端

用户

时间段

VRF

dhcp-client

请选择应用

请选择终端或终端组

请选择或输入用户

请选择时间段

公网

应用与用户

[多选]

[多选]

操作

动作

☒ 允许

☐ 拒绝

Web应用防护配置文件

入侵防御配置文件

数据过滤配置文件

文件过滤配置文件

防病毒配置文件

URL过滤配置文件

APT防御策略

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

确定

取消

- 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。

新建安全策略

常规配置

源IP/MAC地址

目的IP地址

服务

应用与用户

操作

名称①

类型

所属策略组

描述信息

源安全域

地址对象组

IPv4地址②

目的安全域

地址对象组

IPv4地址②

常规配置

源IP/MAC地址

目的IP地址

dhcpout

☒ IPv4

☐ IPv6

请选择策略组

Local

请选择或输入对象组

Trust

请选择或输入对象组

☐ 自动命名

(1-127字符)

[多选]

[多选]

确定

取消

新建安全策略

常规配置

源IP/MAC地址

目的IP地址

服务

应用与用户

操作

协议/端口号

应用

终端

用户

时间段

VRF

dhcp-server

请选择应用

请选择终端或终端组

请选择或输入用户

请选择时间段

公网

应用与用户

[多选]

[多选]

动作

☒ 允许☐ 拒绝

Web应用防护配置文件

入侵防御配置文件

数据过滤配置文件

文件过滤配置文件

防病毒配置文件

URL过滤配置文件

APT防御策略

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

操作

确定

取消

- 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

新建安全策略

常规配置

源IP/MAC地址

目的IP地址

服务

应用与用户

操作

名称

类型

所属策略组

描述信息

源安全域

地址对象组

IPv4地址

目的安全域

地址对象组

IPv4地址

常规配置

源IP/MAC地址

目的IP地址

应用与用户

操作

trust-untrust

IPv4

IPv6

请选择策略组

(1-127字符)

Trust

请选择或输入对象组

10.1.1.0/24

Untrust

请选择或输入对象组

确定

取消

图18 配置安全策略 trust-untrust 的动作

新建安全策略

常规配置

源IP/MAC地址

目的IP地址

服务

应用与用户

操作

协议/端口号

应用

终端

用户

时间段

VRF

动作

Web应用防护配置文件

入侵防御配置文件

数据过滤配置文件

文件过滤配置文件

防病毒配置文件

URL过滤配置文件

APT防御策略

应用与用户

操作

请选择协议和端口号

请选择应用

请选择终端或终端组

请选择或输入用户

请选择时间段

公网

允许

拒绝

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

确定

取消

- 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。

新建安全策略

?

×

常规配置

源IP/MAC地址

目的IP地址

服务

应用与用户

操作

名称?

类型

所属策略组

描述信息

源安全域

地址对象组

IPv4地址?

目的安全域

地址对象组

IPv4地址?

常规配置

源IP/MAC地址

目的IP地址

untrust-trust

IPv4

IPv6

请选择策略组

(1-127字符)

Untrust

请选择或输入对象组

Trust

请选择或输入对象组

10.1.1.2

确定

取消

新建安全策略

常规配置

源IP/MAC地址

目的IP地址

服务

应用与用户

操作

协议/端口号

应用

终端

用户

时间段

VRF

应用与用户

操作

请选择添加协议和端口号

请选择应用

请选择终端或终端组

请选择或输入用户

请选择时间段

公网

应用与用户

操作

动作

Web应用防护配置文件

入侵防御配置文件

数据过滤配置文件

文件过滤配置文件

防病毒配置文件

URL过滤配置文件

APT防御策略

☒ 允许☐ 拒绝

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

--NONE--

确定

取消

- (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

IPv4	ALL	会话总条数: 3条	删除会话	清除过滤条件	按CLI显示导出	按页面显示导出
发起方源IP	发起方源端口	发起方目的IP	发起方目的...	发起方VPN...	接收安全域	发起方协议
10.1.1.3	4099	20.1.1.3	2048	VPN:公网	Trust	ICMP

- 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

IPv4	NAT	会话总条数: 5条	删除会话	清除过滤条件	按CLI显示导出	按页面显示导出
发起方源IP	发起方源端口	发起方目的IP	发起方目的...	发起方VPN...	接收安全域	发起方协议
10.1.1.3	4099	20.1.1.3	2048	VPN:公网	Trust	ICMP