1.1 Device三层直路部署

1.1.1 适用产品和版本

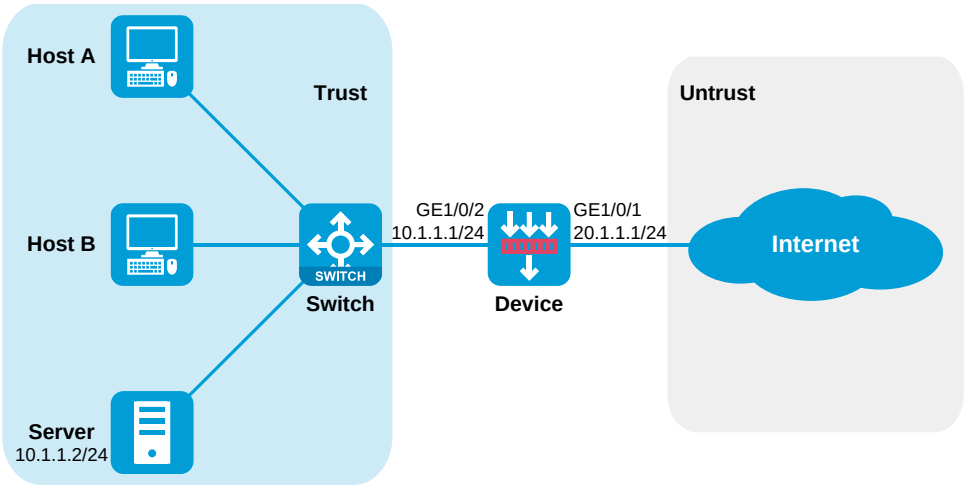
本举例是在 F1060 的 R9360P23 版本上进行配置和验证的。

1.1.2 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。

图1-1 Device 三层直路部署组网图



1.1.3 配置步骤

1. 配置 Device

(1) 配置接口 IP

配置接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 20.1.1.1 24
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] ip address 10.1.1.1 24
[Device-GigabitEthernet1/0/2] quit
```

(2) 配置静态路由

配置默认路由指导上行流量转发（此处下一跳以 20.1.1.3 为例，请以实际情况为准）。

```
[Device] ip route-static 0.0.0.0 0 20.1.1.3
```

(3) 配置接口加入安全域

将 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别加入安全域 Untrust 和 Trust 中。

```
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/1
[Device-security-zone-Untrust] quit
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/2
[Device-security-zone-Trust] quit
```

(4) 配置 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。

```
[Device] dhcp server ip-pool 1
[Device-dhcp-pool-1] network 10.1.1.0 24
[Device-dhcp-pool-1] gateway-list 10.1.1.1
[Device-dhcp-pool-1] dns-list 20.1.1.15
[Device-dhcp-pool-1] forbidden-ip 10.1.1.2
[Device-dhcp-pool-1] quit
```

开启 DHCP 服务。

```
[Device] dhcp enable
```

(5) 配置 NAT 服务

配置地址组 0，包含外网地址 20.1.1.2。

```
[Device] nat address-group 0
[Device-address-group-0] address 20.1.1.2 20.1.1.2
[Device-address-group-0] quit
```

配置全局 NAT 规则 1，允许使用地址组 0 中的地址对匹配的报文进行源地址转换。

```
[Device] nat global-policy
[Device-nat-global-policy] rule name 1
[Device-nat-global-policy-rule-1] source-zone trust
[Device-nat-global-policy-rule-1] destination-zone untrust
[Device-nat-global-policy-rule-1] source-ip subnet 10.1.1.0 24
[Device-nat-global-policy-rule-1] action snat address-group 0
[Device-nat-global-policy-rule-1] quit
```

配置全局 NAT 规则 2，允许外网主机访问 20.1.1.2 的 21 端口时进行目的地址转换，并转换为内网 FTP 服务器的 21 端口。

```
[Device-nat-global-policy] rule name 2
[Device-nat-global-policy-rule-2] source-zone untrust
[Device-nat-global-policy-rule-2] destination-ip host 20.1.1.2
[Device-nat-global-policy-rule-2] service ftp
```

```
[Device-nat-global-policy-rule-2] action dnat ip-address 10.1.1.2
local-port 21
[Device-nat-global-policy-rule-2] quit
[Device-nat-global-policy] quit
```

(6) 配置安全策略

配置安全策略 dhcpin 允许用户发送的 DHCP 协议报文通过。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name dhcpin
[Device-security-policy-ip-0-dhcpin] action pass
[Device-security-policy-ip-0-dhcpin] source-zone trust
[Device-security-policy-ip-0-dhcpin] destination-zone local
[Device-security-policy-ip-0-dhcpin] service dhcp-server
[Device-security-policy-ip-0-dhcpin] quit
```

配置安全策略 dhcpout 允许设备回复用户的 DHCP 协议报文通过。

```
[Device-security-policy-ip] rule name dhcpout
[Device-security-policy-ip-1-dhcpout] action pass
[Device-security-policy-ip-1-dhcpout] source-zone local
[Device-security-policy-ip-1-dhcpout] destination-zone trust
[Device-security-policy-ip-0-dhcpin] service dhcp-client
[Device-security-policy-ip-1-dhcpout] quit
```

配置安全策略 trust-untrust 允许 trust 安全域源地址范围为 10.1.1.0/24 的用户访问 untrust 安全域网络。

```
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-2-trust-untrust] action pass
[Device-security-policy-ip-2-trust-untrust] source-zone trust
[Device-security-policy-ip-2-trust-untrust] destination-zone untrust
[Device-security-policy-ip-2-trust-untrust] source-ip-subnet 10.1.1.0
24
[Device-security-policy-ip-2-trust-untrust] quit
```

配置安全策略 untrust-trust 允许 untrust 安全域网络访问 trust 安全域目的地址为 10.1.1.2 的 FTP 服务器。

```
[Device-security-policy-ip] rule name untrust-trust
[Device-security-policy-ip-3-untrust-trust] action pass
[Device-security-policy-ip-3-untrust-trust] source-zone untrust
[Device-security-policy-ip-3-untrust-trust] destination-zone trust
[Device-security-policy-ip-3-untrust-trust] destination-ip-host
10.1.1.2
[Device-security-policy-ip-3-untrust-trust] quit
[Device-security-policy-ip] quit
```

1.1.4 验证配置

Host A、Host B 上 ping 测试 Internet 的连通性，可以 ping 通 Internet 地址 20.1.1.3。

```
C:\>ping 20.1.1.3

Pinging 20.1.1.3 with 32 bytes of data:

Reply from 20.1.1.3: bytes=32 time=3ms TTL=254

Reply from 20.1.1.3: bytes=32 time=2ms TTL=254
```

```
Reply from 20.1.1.3: bytes=32 time=1ms TTL=254
Reply from 20.1.1.3: bytes=32 time=2ms TTL=254


Ping statistics for 20.1.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

在 Device 上检查会话表，存在 Host 与 20.1.1.3 的会话表。

```
[Device] display session table ipv4
Slot 1:
Initiator:
  Source     IP/port: 10.1.1.6/229
  Destination IP/port: 20.1.1.3/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust

Initiator:
  Source     IP/port: 10.1.1.7/229
  Destination IP/port: 20.1.1.3/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust

Total sessions found: 2
```

在 Device 上检查 NAT 会话的简要信息。

```
[Device]display nat session brief
Slot 1:
Protocol   Source IP/port        Destination IP/port   Global IP/port
ICMP      10.1.1.6/229          20.1.1.3/2048         20.1.1.2/0
ICMP      10.1.1.7/229          20.1.1.3/2048         20.1.1.2/0

Total sessions found: 2
```

外网设备可以通过 FTP 目的地址 20.1.1.2 来访问内网地址为 10.1.1.2 的 FTP 服务器。

1.1.5 配置文件

1. Device

```
#
nat address-group 0
 address 20.1.1.2 20.1.1.2
```

```
#
 dhcp enable
#
dhcp server ip-pool 1
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
 dns-list 20.1.1.15
 forbidden-ip 10.1.1.2
#
interface GigabitEthernet1/0/1
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.1.1.1 255.255.255.0
#
security-zone name Trust
 import interface GigabitEthernet1/0/2
#
security-zone name Untrust
 import interface GigabitEthernet1/0/1
#
 ip route-static 0.0.0.0 0 20.1.1.3
#
nat global-policy
 rule name 2
  service ftp
  source-zone untrust
  destination-ip host 20.1.1.2
  action dnat ip-address 10.1.1.2 local-port 21
 rule name 1
  source-zone trust
  destination-zone untrust
  source-ip subnet 10.1.1.0 24
  action snat address-group 0
#
security-policy ip
 rule 0 name dhcpin
  action pass
  source-zone trust
  destination-zone local
 rule 1 name dhcpout
  action pass
  source-zone local
  destination-zone trust
 rule 2 name trust-untrust
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 10.1.1.0 255.255.255.0
```

```
 rule 3 name untrust-trust
  action pass
  source-zone untrust
  destination-zone trust
  destination-ip-host 10.1.1.2
#
```