1.1 Device透明直路部署

1.1.1 适用产品和版本

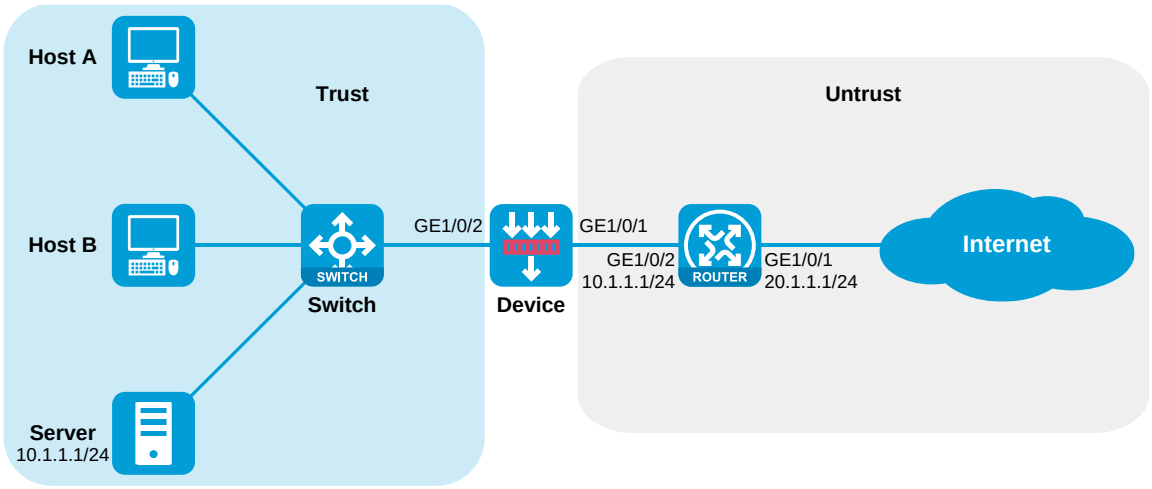
本举例是在 F1060 的 R9360P23 版本上进行配置和验证的。

1.1.2 组网需求

Host A、Host B 和 Server 通过接入交换机 Switch、Device 和路由器 Router 与 Internet 通信，应用需求如下：

- Switch 和 Device 透传 Host、Server 与 Internet 之间的流量。
- Router 做 Host A、Host B 和 Server 的网关，查路由表转发 Host、Server 与 Internet 之间的流量。
- Router 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。
- Router 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。
- 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。

图1-1 Device 透明直路部署组网图



1.1.3 配置步骤

1. 配置 Device

(1) 配置接口的工作模式

切换 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的工作模式为二层。

```
<Device> system-view
[Device] interface range gigabitethernet 1/0/1 gigabitethernet 1/0/2
```

```
[Device-if-range] port link-mode bridge
[Device-if-range] quit
```

(2) 配置接口加入安全域

将 GigabitEthernet1/0/1 的 VLAN1 加入安全域 Untrust，GigabitEthernet1/0/2 的 VLAN1 加入安全域 Trust。

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

(3) 配置安全策略

配置安全策略允许 trust 安全域访问 untrust 安全域。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-0-trust-untrust] action pass
[Device-security-policy-ip-0-trust-untrust] source-zone trust
[Device-security-policy-ip-0-trust-untrust] destination-zone untrust
[Device-security-policy-ip-0-trust-untrust] quit
```

配置安全策略允许 untrust 安全域访问 trust 安全域。

```
[Device-security-policy-ip] rule name untrust-trust
[Device-security-policy-ip-1-untrust-trust] action pass
[Device-security-policy-ip-1-untrust-trust] source-zone untrust
[Device-security-policy-ip-1-untrust-trust] destination-zone trust
[Device-security-policy-ip-1-untrust-trust] quit
[Device-security-policy-ip] quit
```

2. 配置 Router

(1) 配置接口 IP

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

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 20.1.1.1 24
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.1.1.1 24
[Router-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）。

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

(3) 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。

```
[Router] dhcp server ip-pool 1
[Router-dhcp-pool-1] network 10.1.1.0 24
[Router-dhcp-pool-1] gateway-list 10.1.1.1
[Router-dhcp-pool-1] dns-list 20.1.1.15
```

```
[Router-dhcp-pool-1] forbidden-ip 10.1.1.2
[Router-dhcp-pool-1] quit
```

开启 DHCP 服务。

```
[Router] dhcp enable
```

(4) 配置 NAT 服务

配置地址组 0，包含外网地址 20.1.1.2。

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

配置 ACL 2000，仅允许对内部网络中 10.1.1.0/24 网段的用户报文进行地址转换。

```
[Router] acl basic 2000
[Router-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Router-acl-ipv4-basic-2000] quit
```

在接口 GigabitEthernet1/0/1 上配置出方向动态地址转换，允许使用地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] nat outbound 2000 address-group 0
```

配置内部 FTP 服务器，允许外网主机使用地址 20.1.1.2、端口号 21 访问内网 10.1.1.2 的 FTP 服务器。

```
[Router-GigabitEthernet1/0/1] nat server protocol tcp global 20.1.1.2 21 inside
10.1.1.2 ftp
[Router-GigabitEthernet1/0/1] 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: 10.1.1.6/240
  Destination IP/port: 20.1.1.3/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/1/-
```

```
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust

Initiator:
  Source     IP/port: 10.1.1.7/237
  Destination IP/port: 20.1.1.3/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/1/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust

Total sessions found: 3
```

在 Router 上检查 NAT 会话的简要信息。

```
[Router]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: 3
```

1.1.5 配置文件

1. Device

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
interface GigabitEthernet1/0/2
 port link-mode bridge
#
security-zone name Trust
 import interface GigabitEthernet1/0/2 vlan 1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/1 vlan 1
#
security-policy ip
 rule 0 name trust-untrust
  action pass
  source-zone trust
  destination-zone untrust
 rule 1 name untrust-trust
  action pass
  source-zone untrust
  destination-zone trust
```

```
#
```

2. Router

```
#
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
 nat outbound 2000 address-group 0
 nat server protocol tcp global 20.1.1.2 21 inside 10.1.1.2 21
#
interface GigabitEthernet1/0/2
 ip address 10.1.1.1 255.255.255.0
#
 ip route-static 0.0.0.0 0 20.1.1.3
#
acl basic 2000
 rule 0 permit source 10.1.1.0 0.0.0.255
#
```