1 Device 三层旁挂部署

1.1 适用场景

适用于用户使用安全设备（Device）强化网络安全性，将业务流量引入三层旁挂的 Device 做安全业务处理。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。

1.1 组网需求

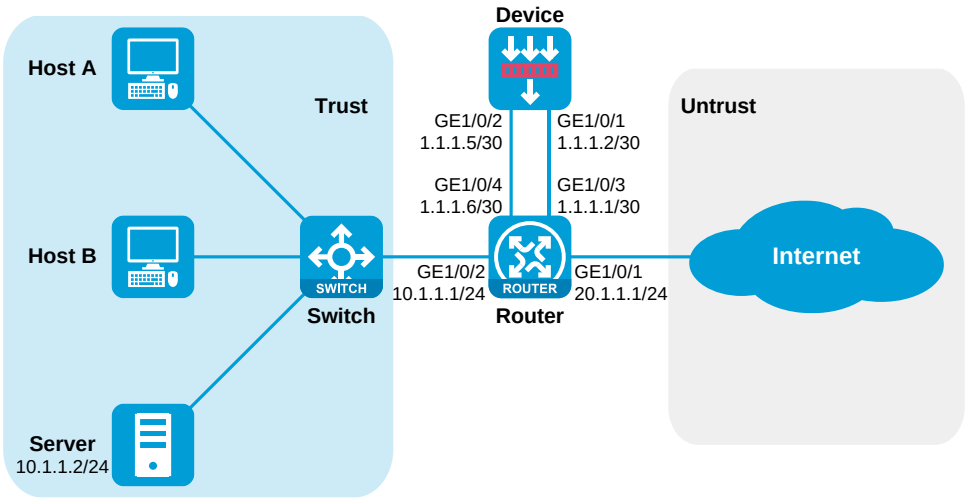
Host A、Host B 和 Server 通过接入交换机 Switch、路由器 Router 与 Internet 通信。出于安全考虑，需要在路由器 Router 上部署 Device 起安全防护作用，应用需求如下：

- Switch 透传 Host、Server 与 Internet 之间的流量。
- Router 与 Host、Server、Internet 和 Device 三层对接，将上下行流量通过策略路由重定向到 Device，对 Device 转发回来的流量查路由表转发。
- 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。
- Device 与 Router 三层对接，查静态路由表转发 Host、Server 与 Internet 之间的流量。

说明

本举例使用 F1060 设备 R9360P23 版本进行验证。

图1 Device 三层旁挂部署组网图



1.2 配置步骤

1. 配置 Router

(1) 配置接口 IP

配置接口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 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
[Router] interface gigabitethernet 1/0/3
[Router-GigabitEthernet1/0/3] ip address 1.1.1.1 30
[Router-GigabitEthernet1/0/3] quit
[Router] interface gigabitethernet 1/0/4
[Router-GigabitEthernet1/0/4] ip address 1.1.1.6 30
[Router-GigabitEthernet1/0/4] 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] 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
```

(5) 配置策略路由

关闭快转负载分担功能（防止三层环路）。

```
[Router] undo ip fast-forwarding load-sharing
```

创建 IPv4 高级 ACL 匹配上下行流量。

```
[Router] acl advanced 3000
[Router-acl-ipv4-adv-3000] rule permit ip source 10.1.1.0 0.0.0.255
[Router-acl-ipv4-adv-3000] quit
[Router] acl advanced 3001
[Router-acl-ipv4-adv-3001] rule permit ip destination 10.1.1.0
0.0.0.255
[Router-acl-ipv4-adv-3001] quit
```

配置策略路由，并将策略路由绑定到接口上。

```
[Router] policy-based-route host-internet permit node 10
[Router-pbr-host-internet-10] if-match acl 3000
[Router-pbr-host-internet-10] apply next-hop 1.1.1.5
[Router-pbr-host-internet-10] quit
[Router] policy-based-route internet-host permit node 10
[Router-pbr-internet-host-10] if-match acl 3001
[Router-pbr-internet-host-10] apply next-hop 1.1.1.2
[Router-pbr-internet-host-10] quit
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip policy-based-route internet-host
[Router-GigabitEthernet1/0/1] quit
```

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip policy-based-route host-internet
[Router-GigabitEthernet1/0/2] quit
```

2. 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 1.1.1.2/255.255.255.252，单击<应用>。

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 1.1.1.5/255.255.255.252，单击<应用>。

图3 编辑 GE1/0/2 安全域和 IPv4 地址

(3) 配置默认路由指导上行流量转发，配置静态路由指导下行流量转发：

- 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 1.1.1.1，单击<确定>完成默认路由配置。

图4 配置默认路由

- 选择“网络>路由>静态路由”，单击<新建>，配置目的 IP 地址为 10.1.1.0，掩码长度为 24，下一跳 IP 地址为 1.1.1.6，单击<确定>完成静态路由配置。

图5 配置静态路由

(4) 配置安全策略放通用户的业务报文：

- 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 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6 配置安全策略 trust-untrust

图7 配置安全策略 trust-untrust 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 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8 配置安全策略 untrust-trust

图9 配置安全策略 untrust-trust 的动作

1.3 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：

- 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10 检查 Device 的 IPv4 会话信息