

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：

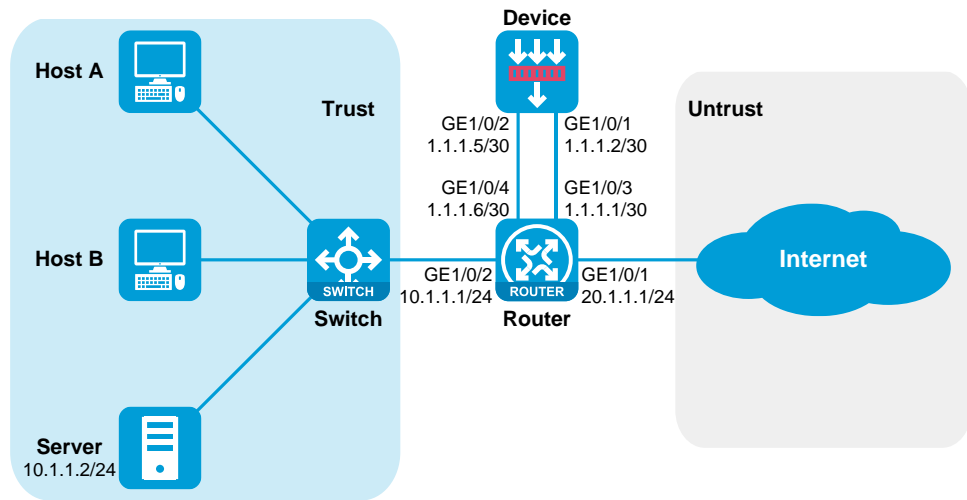
- Switch 透传 Host、Server 与 Internet 之间的流量。
- Router 与 Host、Server、Internet 和 Device 三层对接，将上下行流量通过策略路由重定向到 Device，对 Device 转发回来的流量查路由表转发。
- Router 作为 Host 的 DHCP 服务器，为 Host 动态分配网段为 10.1.1.0/24 的 IP 地址，DNS 服务器地址为 20.1.1.15，网关地址为 10.1.1.1。
- Router 拥有 20.1.1.1/24 和 20.1.1.2/24 两个外网 IP 地址，内部网络中 10.1.1.0/24 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

关闭快转负载均衡功能（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

The screenshot shows the '修改接口设置' (Modify Interface Settings) window for interface GE1/0/1. The interface is currently 'Up'. The description is 'GigabitEthernet1/0/1 Interface'. The working mode is '三层模式' (Layer 3 mode) and the security domain is 'Untrust'. There are checkboxes for protocols that are not controlled, such as Telnet, Ping, SSH, HTTP, HTTPS, SNMP, and NETCONF over various protocols. Below this, there are tabs for '基本配置' (Basic Configuration), 'IPv4地址' (IPv4 Address), 'IPv6地址' (IPv6 Address), and '物理接口配置' (Physical Interface Configuration). The 'IPv4地址' tab is active, showing options to '保持上一跳' (Keep previous hop) as '开启' (On) or '关闭' (Off), and 'IP地址' (IP Address) as '指定IP地址' (Specify IP address), 'DHCP', or 'PPPoE'. The IP address is set to '1.1.1.2' with a subnet mask of '255.255.255.252'. There is a table for managing IP addresses with columns for '从IP地址' (From IP address), '掩码' (Mask), and '编辑' (Edit). At the bottom, there are buttons for '应用' (Apply), '确定' (OK), and '取消' (Cancel).

- 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

The screenshot shows the '修改接口设置' (Modify Interface Settings) window for interface GE1/0/2. The interface is currently 'Up'. The description is 'GigabitEthernet1/0/2 Interface'. The working mode is '三层模式' (Layer 3 mode) and the security domain is 'Trust'. Under '不受控协议' (Uncontrolled Protocols), there are checkboxes for '本机接收' (Local Receive) and '本机发起' (Local Initiate) for Telnet, Ping, SSH, HTTP, HTTPS, and SNMP. Below this, there are tabs for '基本配置' (Basic Configuration), 'IPv4地址' (IPv4 Address), 'IPv6地址' (IPv6 Address), and '物理接口配置' (Physical Interface Configuration). The 'IPv4地址' tab is active, showing options for '保持上一跳' (Keep Previous Hop) set to '关闭' (Off), and 'IP地址' (IP Address) set to '指定IP地址' (Specify IP Address). The IP address is '1.1.1.5' with a mask of '255.255.255.252'. There is a '网关' (Gateway) field and a table for '指定从IP地址' (Specify from IP Address) with columns for '从IP地址' (From IP Address), '掩码' (Mask), and '编辑' (Edit). At the bottom, there are buttons for '应用' (Apply), '确定' (OK), and '取消' (Cancel).

- (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

新建IPv4静态路由 ? ×

VRF	公网	
目的IP地址	0.0.0.0	*
掩码长度	0	* (0-32)
下一跳 ?	<input type="checkbox"/> 下一跳所属的VRF <input checked="" type="checkbox"/> 出接口 请选择... 下一跳IP地址 1.1.1.1	*
路由优先级 ?	60	(1-255, 缺省为60)
路由标记 ?	0	(0-4294967295, 缺省为0)
描述		(1-60字符)

确定 取消

- 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

新建IPv4静态路由

VRF: 公网

目的IP地址: 10.1.1.0

掩码长度: 24 (0-32)

下一跳

- 下一跳所属的VRF
- 出接口: 请选择...
- 下一跳IP地址: 1.1.1.6

路由优先级: 60 (1-255, 缺省为60)

路由标记: 0 (0-4294967295, 缺省为0)

描述: (1-60字符)

确定 取消

(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

The screenshot shows the 'New Security Policy' configuration window. The left sidebar has '常规配置' (General Configuration) selected. The main area is divided into sections: '常规配置' (General Configuration) with fields for Name (trust-untrust), Type (IPv4 selected), and Description; '源IP/MAC地址' (Source IP/MAC Address) with fields for Source Security Domain (Trust), Address Object Group, and IPv4 Address (10.1.1.0/24); and '目的IP地址' (Destination IP Address) with fields for Destination Security Domain (Untrust), Address Object Group, and IPv4 Address. '确定' (OK) and '取消' (Cancel) buttons are at the bottom.

图7 配置安全策略 trust-untrust 的动作

The screenshot shows the 'New Security Policy' configuration window, specifically the 'Action' section. The left sidebar has '服务' (Service) selected. The main area shows '应用与用户' (Application and User) settings: Application, Terminal, User, Time Range, and VRF. Below is the '操作' (Action) section with radio buttons for '允许' (Allow) and '拒绝' (Deny), and several dropdown menus for configuration files: Web application protection, Intrusion prevention, Data filtering, File filtering, Anti-virus, URL filtering, and APT defense strategy. '确定' (OK) and '取消' (Cancel) buttons are at the bottom.

- 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

The screenshot shows the 'New Security Policy' configuration window. The left sidebar has '常规配置' (General Configuration) selected. The main area is divided into sections: '常规配置' (General Configuration) with fields for '名称' (Name: untrust-trust), '类型' (Type: IPv4), '所属策略组' (Policy Group), and '描述信息' (Description); '源IP/MAC地址' (Source IP/MAC Address) with '源安全域' (Source Security Domain: Untrust), '地址对象组' (Address Object Group), and 'IPv4地址' (IPv4 Address); and '目的IP地址' (Destination IP Address) with '目的安全域' (Destination Security Domain: Trust), '地址对象组' (Address Object Group), and 'IPv4地址' (IPv4 Address: 10.1.1.2). At the bottom are '确定' (OK) and '取消' (Cancel) buttons.

图9 配置安全策略 untrust-trust 的动作

The screenshot shows the 'New Security Policy' configuration window with the '服务' (Service) tab selected in the sidebar. The '应用与用户' (Application and User) section includes '应用' (Application), '终端' (Terminal), '用户' (User), '时间段' (Time Period), and 'VRF' (VRF: 公网). The '操作' (Action) section has '动作' (Action: 允许) and several configuration options: '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', and 'APT防御策略', all set to '--NONE--'. At the bottom are '确定' (OK) and '取消' (Cancel) buttons.

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

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
<input type="checkbox"/> 10.1.1.3	4099	20.1.1.3	2048	VPN:公网	Trust	ICMP