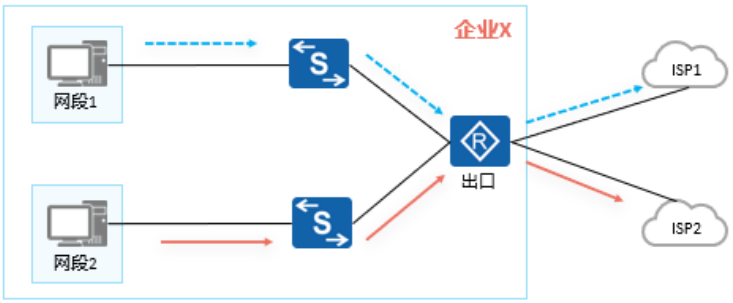
流量过滤与转发路径控制

- 传统的路由转发原理是首先根据报文的目的地址查找路由表，然后进行报文转发。随着业务的发展，用户更加希望能够在传统路由转发的基础上根据自己定义的策略进行报文转发和选路。
- 为提高网络安全性，用户希望能够控制进入网络的报文，将没有权限进入网络或存在安全隐患的报文隔离在网络边界。
- 本课程将会学习流量过滤技术、策略路由以及使用 MQC（Modular QoS Command-Line Interface，模块化 QoS 命令行）的方式控制报文的转发路径和进行流量过滤。

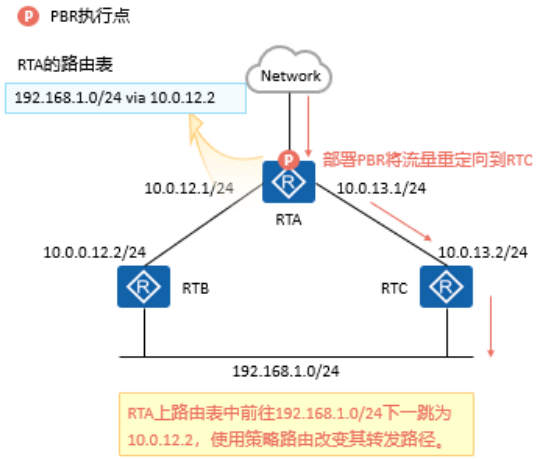
策略路由技术背景

在某些场景中我们希望一些特定用户、特定业务的流量走指定的转发路径，而其余用户或业务的流量则依旧根据路由表进行转发。



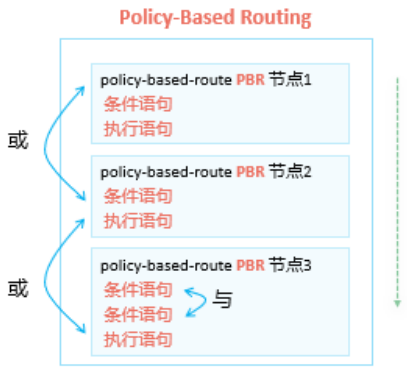
示例：双ISP接入的企业，想要实现内网网段1访问Internet通过ISP1、内网网段2访问Internet通过ISP2，该需求无法通过传统的路由技术实现。

PBR介绍 - 基本概念



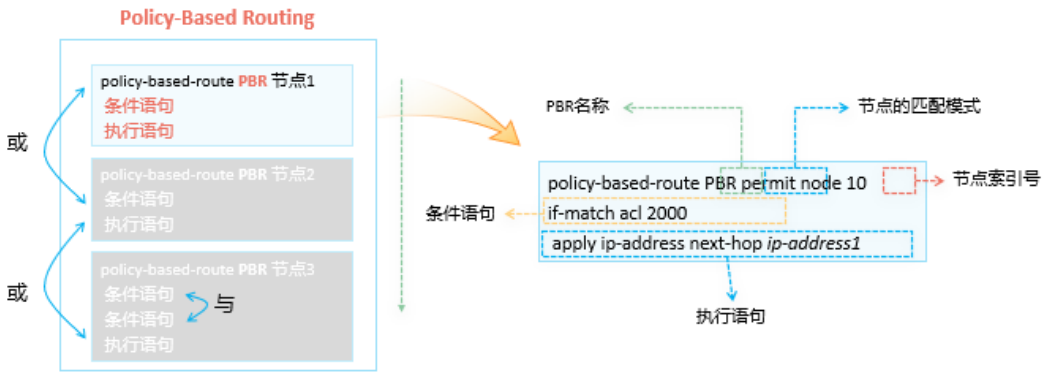
- PBR（Policy-Based Routing，策略路由）：PBR使得网络设备不仅能够基于报文的目的IP地址进行数据转发，更能基于其他元素进行数据转发，例如源IP地址、源MAC地址、目的MAC地址、源端口号、目的端口号、VLAN-ID等等。
- 用户还可以使用ACL匹配特定的报文，然后针对该ACL进行PBR部署。
- 若设备部署了PBR，则被匹配的报文优先根据PBR的策略进行转发，即PBR策略的优先级高于传统路由表。

PBR介绍 - 结构



- PBR与Route-Policy类似，由多个节点组成，每个节点由匹配条件（条件语句）和执行动作（执行语句）组成。
- 每个节点内可包含多个条件语句。
- 节点内的多个条件语句之间的关系为“与”，即匹配所有条件语句才会执行本节点内的动作。
- 节点之间的关系为“或”，PBR根据节点编号从小到大顺序执行，匹配当前节点将不会继续向下匹配。

PBR介绍 - 命令语法



- PBR 的节点匹配模式：
- permit 表示对满足匹配条件的报文进行策略路由
- deny 表示对满足匹配条件的报文不进行策略路由

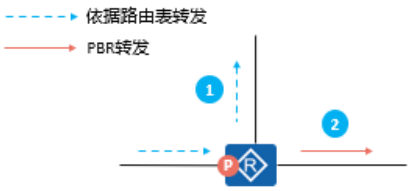
PBR与路由策略区别

名称	操作对象	描述
路由策略 (Route-Policy)	路由信息	路由策略是一套用于对路由信息进行过滤、属性设置等操作的方法，通过对路由的操作或控制，来影响数据报文的转发路径
PBR	数据报文	PBR直接对数据报文进行操作，通过多种手段匹配感兴趣的报文，然后执行丢弃或强制转发路径等操作

PBR的分类

接口PBR

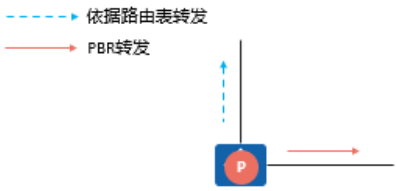
PBR执行点



- 接口PBR只对转发的报文起作用，对本地始发的报文无效。
- 接口PBR调用在接口下，对接口的入方向报文生效。缺省情况下，设备按照路由表的下一跳进行报文转发，如果配置了接口PBR，则设备按照接口PBR指定的下一跳进行转发。

本地PBR

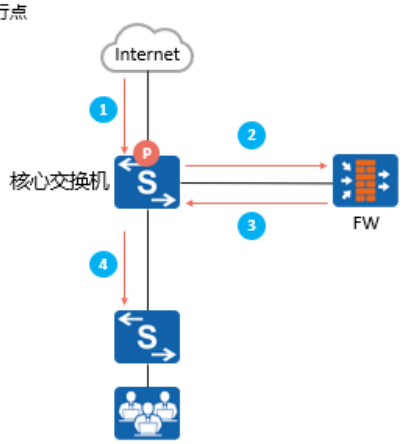
PBR执行点



- 本地PBR对本地始发的流量生效，如：本地始发的ICMP报文。
- 本地PBR在系统视图调用。

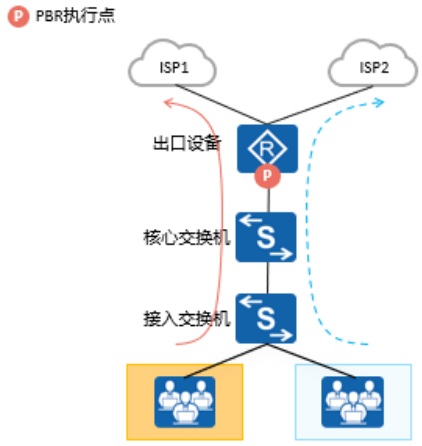
PBR典型应用场景 (1)

PBR执行点



- 内网防火墙旁挂部署在核心交换机，为防护内网在核心交换机的三层接口上部署PBR，将来自外部网络的流量牵引到防火墙上进行安全检查，检查完的流量再发送回核心交换机，由核心交换机依据路由表转发到内网。
- 将流量牵引到别的设备进行安全检查等类似的行为我们称之为“引流”，PBR是一种常见的引流工具。

PBR典型应用场景 (2)



当企业存在多个网络出口时，若想指定部分网段访问Internet时的网络出口，可以使用PBR：在出口设备的内网接口配置PBR，匹配来自内网的流量，为其指定不同的下一跳公网地址。

配置介绍 (1)

1. 创建PBR

```
[Huawei] policy-based-route policy-name { deny | permit } node node-id
```

创建策略路由和策略点，若策略点已创建则进入本地策略路由视图。

2. 设置IP报文的匹配条件

```
[Huawei-policy-based-route-PBR-10] if-match acl acl-number
[Huawei-policy-based-route-PBR-10] if-match packet-length min-length max-length
```

缺省情况下，策略路由中未配置匹配条件，可以设置使用ACL匹配IP地址，也可以设置匹配报文长度。

3. 指定PBR中报文的出接口

```
[Huawei-policy-based-route-PBR-10] apply output-interface interface-type interface-number
```

缺省情况下，策略路由中未配置报文出接口。配置成功后，将匹配策略点的报文从指定出接口发送出去。
报文的出接口不能为以太接口等广播型接口。

- 当 ACL 的 rule 配置为 permit 时，设备会对匹配该规则的报文执行本地策略路由的动作：
- 本地策略路由中策略点为 permit 时对满足匹配条件的报文进行策略路由；
- 本地策略路由中策略点为 deny 时对满足匹配条件的报文不进行策略路由，即根据目的地址查找路由表转发报文。
- 当 ACL 配置了 rule，如果报文未匹配上任何规则，则根据目的地址查找路由表转发报文。
- 当 ACL 的 rule 配置为 deny 或 ACL 未配置规则时，应用

该 ACL 的本地策略路由不生效，即根据目的地址查找路由表转发报文。

配置介绍 (2)

4. 设置PBR中报文的下一跳

```
[Huawei-policy-based-route-PBR-10] apply ip-address next-hop ip-address1 [ ip-address2 ]
```

用户可以指定报文的下一跳。当该策略点未配置出接口时，匹配策略点的报文被发往指定的下一跳。

5. 全局PBR调用

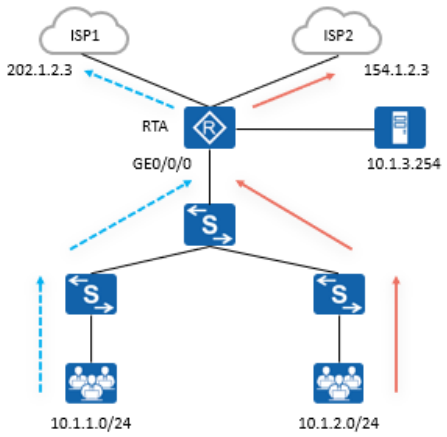
```
[Huawei] ip local policy-based-route Policy-name
```

6. 接口PBR调用

```
[Huawei-GigabitEthernet0/0/0] ip policy-based-route Policy-name
```

- 除了该方式之外，接口策略路由还可以使用 MQC 的方式进行配置。

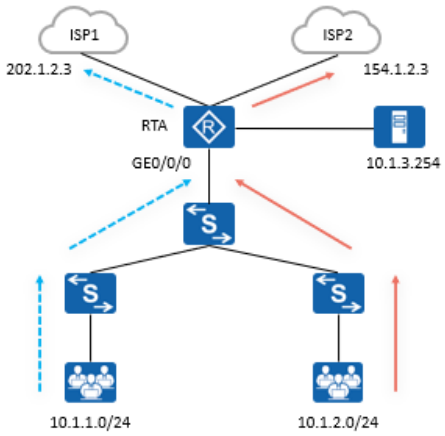
配置案例 (1)



需求：

- 内网存在两个网段，网段1：10.1.1.0/24，网段2：10.1.2.0/24，在RTA的GE0/0/0接口部署PBR，实现网段1访问Internet通过ISP1、网段2访问Internet通过ISP2。
- RTA上旁挂了一台服务器，要求在RTA上部署的策略路由不影响内网用户访问该服务器。

配置案例 (2)



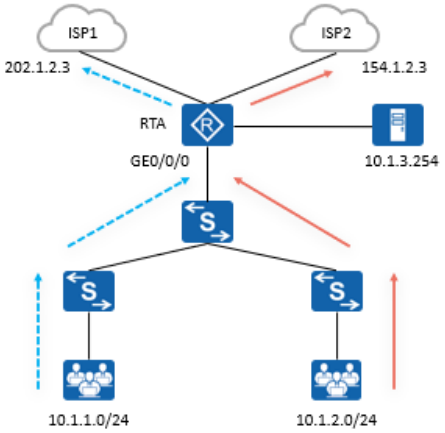
1. 配置ACL 3000，其中rule 1 deny网段1访问服务器的流量，rule 2匹配网段1访问Internet的流量。

```
[RTA] acl number 3000
[RTA-acl-adv-3000] rule 1 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.3.254 0
[RTA-acl-adv-3000] rule 2 permit ip source 10.1.1.0 0.0.0.255 destination
0.0.0.0 0
```

2. 配置ACL 3001，其中rule 1 deny网段2访问服务器的流量，rule 2匹配网段2访问Internet的流量。

```
[RTA] acl number 3001
[RTA-acl-adv-3001] rule 1 deny ip source 10.1.2.0 0.0.0.255 destination 10.1.3.254 0
[RTA-acl-adv-3001] rule 2 permit ip source 10.1.2.0 0.0.0.255 destination
0.0.0.0 0
```

配置案例 (3)



3. 创建PBR hcip，创建节点10，调用ACL 3000，指定其转发下一跳为202.1.2.3

```
[RTA] policy-based-route hcip permit node 10
[RTA-policy-based-route-hcip-10] if-match acl 3000
[RTA-policy-based-route-hcip-10] apply ip-address next-hop 202.1.2.3
```

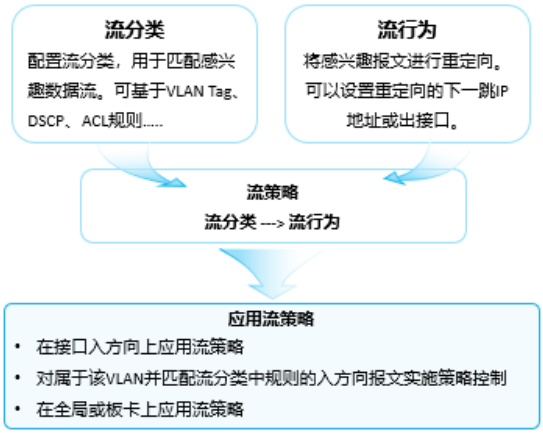
4. 创建PBR hcip节点20，调用ACL 3001，指向其转发下一跳为154.1.2.3

```
[RTA] policy-based-route hcip permit node 20
[RTA-policy-based-route-hcip-20] if-match acl 3001
[RTA-policy-based-route-hcip-20] apply ip-address next-hop 154.1.2.3
```

5. 在GE0/0/0接口调用PBR hcip

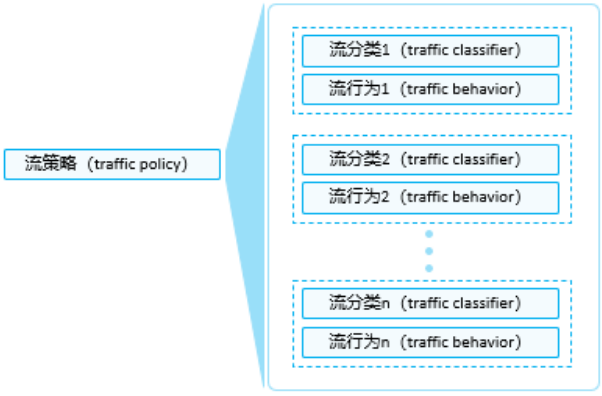
```
[RTA]interface GigabitEthernet 0/0/0
[RTA-GigabitEthernet0/0/0] ip policy-based-route hcip
```

MQC介绍 (1)



- MQC（Modular QoS Command-Line Interface，模块化QoS命令行）是指通过将具有某类共同特征的数据流划分为一类，并为同一类数据流提供相同的服务，也可以对不同类的数据流提供不同的服务。
- MQC包含三个要素：流分类（traffic classifier）、流行为（traffic behavior）和流策略（traffic policy）。
- MQC的流行为支持重定向报文，因此可以使用MQC实现IP单播策略路由。

MQC介绍 (2)



- 流策略：将流分类和流行为绑定，对分类后的报文执行对应流行为中定义的动作。
- 一个流策略可以绑定多个流分类和流行为。

MQC - 流分类

流分类：定义一组流量匹配规则，以对报文进行分类。流分类支持的匹配项如下所示。

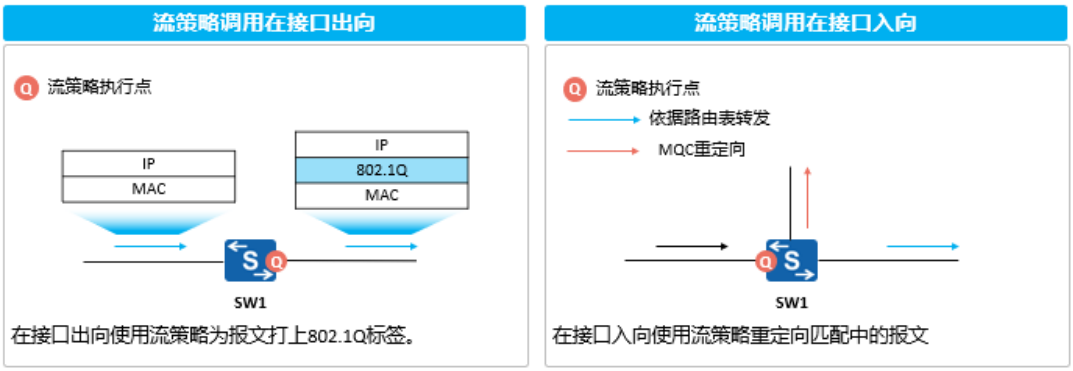
- 流分类中各规则之间的关系分为：and 或 or，缺省情况下的关系为 or。
- and：当流分类中包含 ACL 规则时，报文必须匹配其中一条 ACL 规则以及所有非 ACL 规则；当流分类中没有 ACL 规则时，报文必须匹配所有非 ACL 规则。
- or：报文只要匹配了流分类中的一个规则，设备就认为报文匹配中该流分类。

MQC - 流行为

流行为：用来定义执行的动作，支持报文过滤、重标记优先级、重定向、流量统计等动作。

MQC - 流策略

- 流策略：流策略支持在接口上调用。
- 流策略存在方向(inbound、 outbound)的概念，策略中的流行为匹配入、出方向的报文，对匹配中的报文执行相应的流动作。



- 流策略不同于 PBR，PBR 只能调用在三层接口，而流策略支持调用在二层接口。

配置介绍

1. 创建流分类

   [Huawei] **traffic classifier** *classifier-name* **[operator { and | or }]**

   缺省情况下，流分类中各规则之间的关系为“或” （or）。流分类中的匹配规则配置可查阅产品手册。

2. 创建流行为

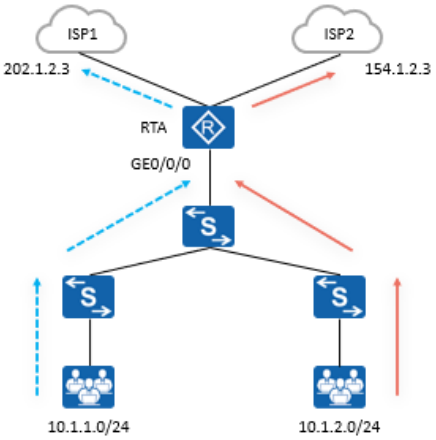
   [Huawei] **traffic behavior** *behavior-name*

   根据实际情况定义流行为中的动作，只要各动作不冲突，都可以在同一流行为中配置。流行为具体配置可查阅产品手册。

3. 创建流策略，并绑定流分类与流行为

   [Huawei] **traffic policy** *policy-name*
   [Huawei-trafficpolicy-policyname] **classifier** *classifier-name* **behavior** *behavior-name*

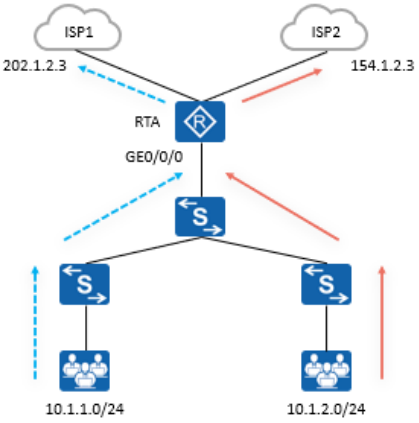
使用MQC实现策略路由 (1)



需求：

- 内网存在两个网段，网段1：10.1.1.0/24，网段2：10.1.2.0/24，在RTA上通过MQC实现策略路由，实现网段1访问Internet通过ISP1、网段2访问Internet通过ISP2。
- 将MQC调用在RTA的GE0/0/0接口

使用MQC实现策略路由 (2)



RTA的配置如下：

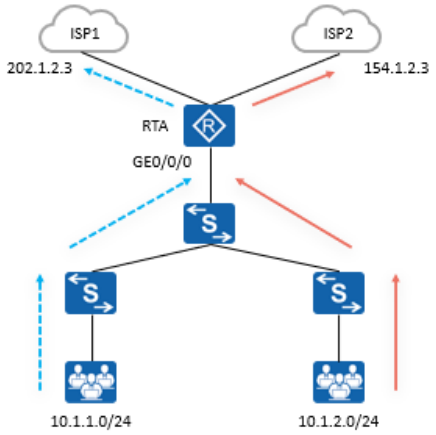
1. 配置ACL3000、3001分别匹配网段1、网段2访问Internet的流量。

```
[RTA] acl number 3000
[RTA-acl-adv-3000] rule 2 permit ip source 10.1.1.0 0.0.0.255 destination
0.0.0.0 0
[RTA] acl number 3001
[RTA-acl-adv-3001] rule 2 permit ip source 10.1.2.0 0.0.0.255 destination
0.0.0.0 0
```

2. 创建流分类1、2分别匹配ACL3000、ACL3001。

```
[RTA] traffic classifier 1
[RTA-classifier-1] if-match acl 3000
[RTA] traffic classifier 2
[RTA-classifier-2] if-match acl 3001
```

使用MQC实现策略路由 (3)



3. 创建流行为1、2分别执行将报文重定向到202.1.2.3、154.1.2.3的动作。

```
[RTA] traffic behavior 1
[RTA-behavior-1] redirect ip-nexthop 202.1.2.3
[RTA] traffic behavior 2
[RTA-behavior-2] redirect ip-nexthop 154.1.2.3
```

4. 创建流策略Redirect，将流分类1、2与流行为1、2一一绑定。

```
[RTA] traffic policy Redirect
[RTA-trafficpolicy-Redirect] classifier 1 behavior 1
[RTA-trafficpolicy-Redirect] classifier 2 behavior 2
```

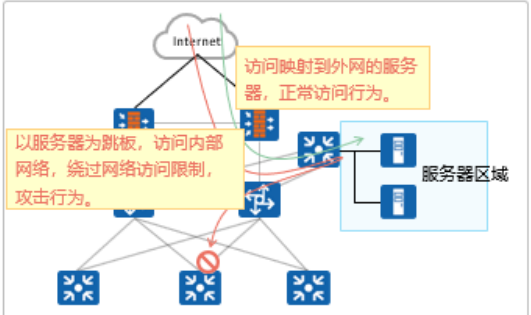
5. 在GE0/0/0接口入方向调用流策略Redirect

```
[RTA] interface GigabitEthernet 0/0/0
[RTA-GigabitEthernet0/0/0] traffic-policy Redirect inbound
```

需求背景

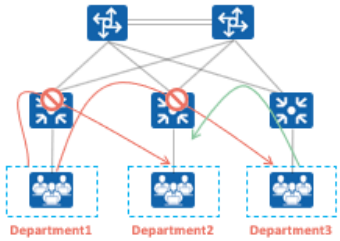
为提高网络安全性，管理人员需要控制进入网络的流量，将不信任的报文丢弃在网络边界。所谓的不信任报文是指对用户来说存在安全隐患或者不愿意接收的报文。同时保证数据访问安全性，企业网络中经常会要求一些部门之间不能相互访问。

丢弃不信任报文



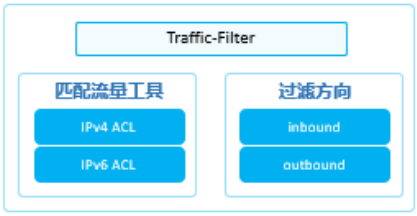
限制服务器访问内网，防止出现跳转攻击。

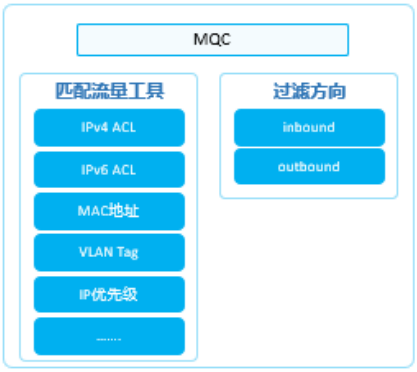
限制部门间相互访问



根据业务要求，限制不同部门之间的访问。

流量过滤工具

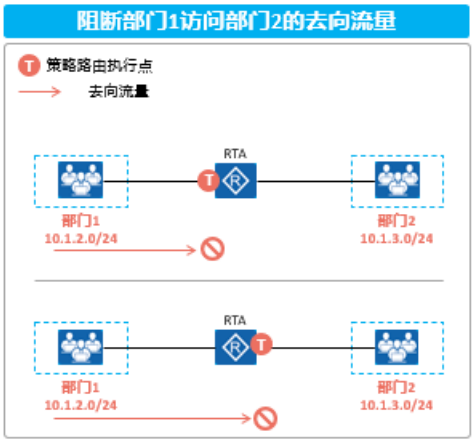


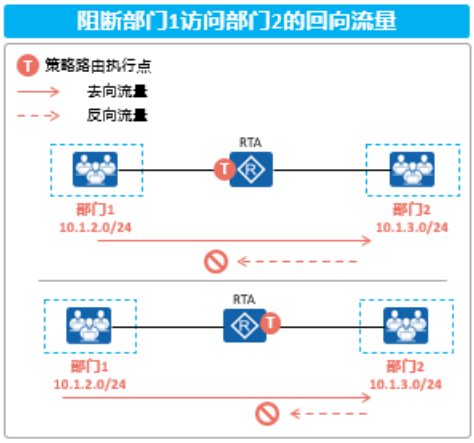


Traffic-Filter只能应用在接口视图下，而MQC可以调用在多种视图。

Traffic-Filter部署位置

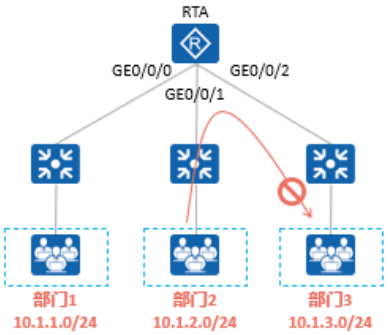
使用Traffic-Filter过滤流量可以灵活地选择部署位置，在流量进入设备或者离开设备的接口上执行过滤动作，双向访问的业务禁止其中一个方向即可实现阻断业务的需求。





- Traffic-Filter 部署的位置不同，其调用的 ACL 内容也不相同。

使用Traffic-Filter过滤流量



部门1、2、3的网关都在RTA上，现要求在RTA上使用Traffic-Filter限制部门2与部门3之间的相互访问。

RTA的配置如下：

1. 配置ACL拒绝部门2访问部门3，并放通其余所有流量。

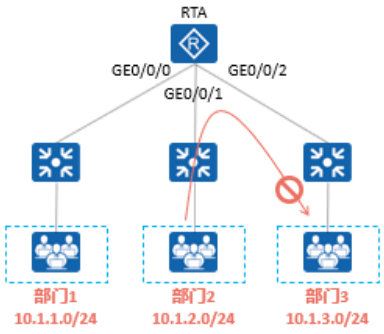
```
[RTA] acl number 3000
[RTA-acl-adv-3000] rule 1 deny ip source 10.1.2.0 0.0.0.255 destination
10.1.3.0 0.0.0.255
[RTA-acl-adv-3000] rule 2 permit ip
```

2. 在GE0/0/2接口调用Traffic-Filter

```
[RTA] interface GigabitEthernet 0/0/2
[RTA-GigabitEthernet0/0/2] traffic-filter outbound acl 3000
```

思考：ACL的写法、Traffic-Filter调用的接口是否还有别的可能?

使用MQC过滤流量 (1)



部门1、2、3的网关都在RTA上，现要求在RTA上使用Traffic-Filter限制部门2与部门3之间的相互访问。

RTA的配置如下：

1. 配置ACL匹配部门2访问部门3的流量

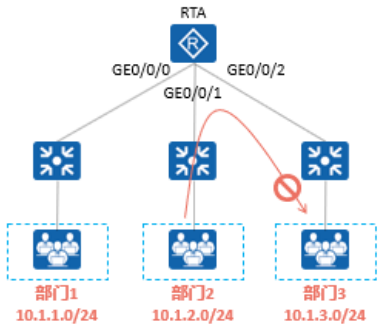
```
[RTA] acl number 3000
[RTA-acl-adv-3000] rule 1 permit ip source 10.1.2.0 0.0.0.255 destination
10.1.3.0 0.0.0.255
```

2. 创建流分类2_3、流行为2_3

```
[RTA] traffic classifier 2_3
[RTA-classifier-2_3] if-match acl 3000
[RTA] traffic behavior 2_3
[RTA-behavior-2_3] deny
```

为匹配ACL规则的报文指定报文过滤动作时，如果此ACL中的rule规则配置为permit，则设备对此报文采取的动作由流行为中配置的deny或permit决定；如果此ACL中的rule规则配置为deny，则无论流行为中配置了deny或permit，此报文都被丢弃。

使用MQC过滤流量 (2)



部门1、2、3的网关都在RTA上，现要求在RTA上使用Traffic-Filter限制部门2与部门3之间的相互访问。

3. 创建流策略，绑定流分类2_3与流行为2_3

```
[RTA] traffic policy 2_3
[RTA-trafficpolicy-2_3] classifier 2_3 behavior 2_3
```

4. 在接口GE0/0/1入向调用流策略2_3

```
[RTA] interface GigabitEthernet 0/0/1
[RTA-GigabitEthernet0/0/1] traffic-policy 2_3 inbound
```

思考题：

- （简答题）本地策略路由与接口策略路由的区别在于？
- （简答题）使用 MQC 方式过滤流量时，流分类中匹配的 ACL 与 Traffic-Filter 调用的 ACL 有何区别？

答案：

- 本地策略路由对本地始发的流量生效，而接口策略路由只会对接口入方向的流量生效。
- MQC 调用的 ACL 里 permit、deny 只代表是否匹配流量，不代表是否放通、拒绝流量，而 Traffic-Filter 调用的 ACL 里 permit、deny 代表放通、拒绝流量。
-