策略路由与访问控制列表重定向网络流量实践应用

高　峰

摘　要：本文围绕策略路由与访问控制列表在网络流量重定向中的实践应用展开研究。通过分析策略路由和访问控制列表的基本概念，结合实际配置步骤，探讨了如何定义匹配条件，并通过路由映射实现流量的灵活控制。文章重点剖析了不同场景下的数据包转发流程，验证了策略路由与访问控制列表在优化网络路径选择、提升网络管理效率方面的有效性。研究表明，该技术组合能够满足复杂网络环境中差异化流量处理的需求，为网络架构设计提供重要参考。

关键词：策略路由；访问控制；定向网络流量

引言

作者单位为多地址办公，每个办公地址均部署防火墙、核心交换机等接入与交换设备，不同办公区域间租用通讯运营商直连光缆通讯。（见图1）

网站服务器部署在A校区，IP地址172.19.231.100，接入交换机VLAN 231网段。

A校区核心交换机路由简要配置

ip route 0.0.0.0 0.0.0.0 192.168.1.1

ip route 192.168.36.0 255.255.255.0 192.168.200.2

……

B校区核心交换机路由简要配置

ip route 0.0.0.0 0.0.0.0 192.168.100.1

ip route 172.19.231.100 255.255.255.255 192.168.200.1

……

说明：

●在各自校区内，当数据包目的地址在路由表中没有找到明确匹配的路由时，均被转发至本校区的防火墙。

●A校区访问B校区网段（如VLAN 36）的流量均路由转发至校区互联链路，192.168.200.2是B校区连接设备的地址。

●B校区访问网站服务器的流量均路由转发至校区互联链路，192.168.200.1是A校区连接设备的地址。

访问网站服务器存在的问题：因历史原因，单位网站的互联网域名解析指向B校区通讯运营商提供的IP地址，互联网用户访问单位网站的流量，从B校区防火墙进入，经两校交换机路由转发至网站服务器，网站服务

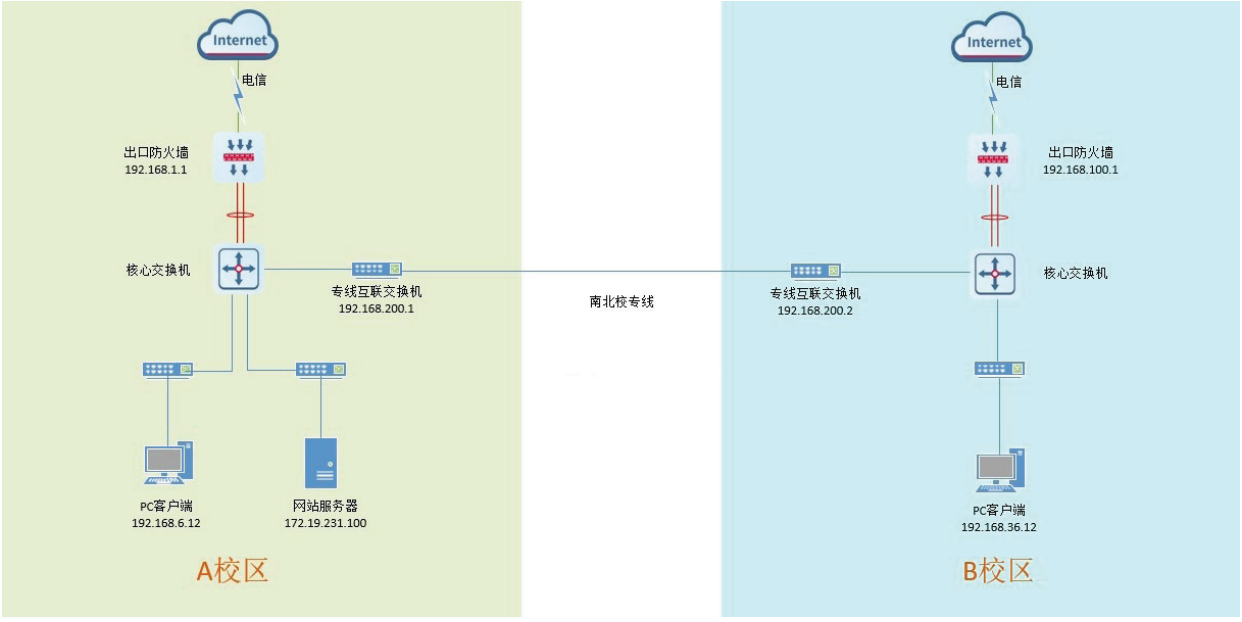

图1　网络拓扑图

作者简介：高峰（1971--），男，北京市人，大学本科，目前职称：工程师，研究方向：计算机技术。

器处理完成后，按照A校区交换机的配置，数据包被路由转发至A校区防火墙而非回到B校区防火墙返回给客户端，客户无法访问单位网站。

为解决上述问题，笔者在网站服务器所属网段配置策略路由和访问控制列表对进入该网段的流量重定向，成功解决上述问题。

一、策略路由、访问控制列表概念

策略路由（Policy-Based Routing，PBR）是一种灵活的网络流量管理机制，允许根据定义的策略（如源/目的IP、协议类型、端口等）动态选择数据包的转发路径，而非依赖传统的路由表。

表1　策略路由与传统路由对比

对比维度	策略路由	传统路由
转发依据	源IP、协议、端口等。	目的IP的最长前缀匹配。
灵活性	高（支持复杂条件）。	低（仅依赖路由表）。
典型应用	负载均衡、链路备份、服务质量优化、安全策略实施等。	常规跨网段通信。
优先级	高于普通路由表，数据包进入交换机接口时立即生效。	依赖管理距离和度量值。

访问控制列表（Access Control List，ACL）是交换机中控制网络流量的一种重要安全机制，它通过定义一系列规则决定允许或拒绝特定类型的流量通过交换机从而实现网络安全防护、流量管理、访问权限控制等功能。

二、配置策略路由、访问控制列表

（一）定义匹配条件

本案例中配置了两个访问控制列表，编号为99和100。

●编号为99的扩展访问控制列表

```
ip access-list extended 99
10 permit tcp host 172.19.231.100 192.168.6.0 0.0.0.255
……
```

说明：源IP为172.19.231.100的主机可以使用TCP协议访问列表中指定的网络（A校区所有网段均需在此列出以确保网站服务器能够访问A校区所有网段，被遗漏网段的用户将无法访问网站服务器）。

●编号为100的标准访问控制列表

```
ip access-list standard 100
10 permit host 172.19.231.100
```

说明：允许源IP为172.19.231.100的主机流量通过。

（二）创建路由映射

本案例中创建了两条路由映射条目，名称是wangzhan，序号分别是5和10（序号决定了规则的优先级，数值越小优先级越高。）；规则类型为permit，即允许符合条件的数据包通过并按策略处理。

具体配置如下：

●序号5的路由映射

```
route-map wangzhan permit 5
match ip address 99
set ip next-hop 172.19.231.254
```

●序号10的路由映射

```
route-map wangzhan permit 10
match ip address 100
set ip next-hop 192.168.200.2
```

策略路由的执行逻辑：

序号5的规则优先被处理，如果流量匹配ACL 99，则应用该规则设置下一跳为172.19.231.254，不再处理后续规则。如果流量不匹配序号5的规则，则检查序号10的规则，如果流量匹配ACL 100，设置下一跳为192.168.200.2。如果都不匹配，则根据默认路由或其它路由策略处理。

（三）应用策略路由到接口

```
interface VLAN 231
ip address 172.19.231.254 255.255.255.0
ip policy route-map wangzhan
```

说明：将策略路由wangzhan应用在VLAN 231网段，根据规则处理进入该接口的流量。

三、访问网站流量转发分析

（一）互联网客户端访问网站数据包转发分析

互联网用户访问网站的流量从B校区防火墙进入校内网络。

●客户端访问网站服务器流量

数据包转发路径：

客户端设备→B校区防火墙→B校区核心交换机→校区互联链路→A校区核心交换机→VLAN 231网段→172.19.231.100。

数据包转发说明：

数据包从B校区防火墙进入后转发至B校区核心交换机，路由表显示发往主机172.19.231.100的数据包下一跳是192.168.200.1（两校区间的链路设备），数据包经链路设备转发至A校区核心交换机。

A校区核心交换机收到数据包后查询路由表，172.19.231.0/24（VLAN 231网段）是直连网段，数据包从VLAN 231网段发出，按直连路由转发至网站服务器，不触发策略路由。

●网站服务器返回客户端流量

数据包转发路径：

172.19.231.100→VLAN 231网段→A校区核心交换机→校区互联链路→B校区核心交换机→B校区防火墙→客户端设备。

数据包转发说明：

网站服务器返回数据包从VLAN 231网段接口进入交换机，数据包被转发之前检查策略路由wangzhan，本次通讯与序号10的规则（ACL 100）相匹配，执行该策略。序号10的规则设置下一跳为192.168.200.2（两校区间的链路设备），数据包经链路设备转发至B校区核心交换机。

B校区核心交换机收到数据包后查询路由表，数据包目的地址在路由表中不能找到明确匹配的路由被转发至B校区防火墙。

B校区防火墙收到数据包后返回给互联网客户端，客户正常打开网页。

（二）A校区客户端访问网站数据包转发分析

假设A校区客户端IP地址为192.168.6.12，接入交换机VALN 6网段。

●客户端访问网站服务器流量

数据包转发路径：

192.168.6.12→VLAN 6网段→VLAN 231网段→172.19.231.100。

数据包转发说明：

客户端192.168.6.12的数据包从VLAN 6网段接口进入交换机，路由表显示172.19.231.0/24（VLAN 231网段）是直连网段，数据包从VLAN 231网段发出，按直连路由转发至网站服务器，不触发策略路由。

●网站服务器返回客户端流量

数据包转发路径：

172.19.231.100→VLAN 231网段→VLAN 6网段→192.168.6.12。

数据包转发说明：

网站服务器返回数据包从VLAN 231网段接口进入交换机，数据包被转发之前检查策略路由wangzhan。本次通讯源IP 172.19.231.100，目的地址IP属于192.168.6.0/24，通讯协议TCP，与序号5的规则（ACL 99）相匹配，执行该策略。

序号5规则设置下一跳为172.19.231.254，是交换机自身地址，触发本地处理逻辑。路由表显示192.168.6.0/24（VLAN 6网段）属于直连网段，数据包从VLAN 6网段接口发出，返回给客户端，客户正常打开网页。

（三）B校区客户端访问网站数据包转发分析

假设B校区客户端IP地址为192.168.36.12，接入交换机VALN 36网段。

●客户端访问网站服务器流量

数据包转发路径：

192.168.36.12→VLAN 36网段→B校区核心交换机→校区互联链路→A校区核心交换机→VLAN 231网段→172.19.231.100。

数据包转发说明：

客户端192.168.36.12的数据包从VLAN 36网段接口进入交换机，后续路由转发至网站服务器的过程与互联网客户访问网站流量相同。

●网站服务器返回客户端流量

数据包转发路径：

172.19.231.100→VLAN 231网段→A校区核心交换机→校区互联链路→B校区核心交换机→VLAN 36网段→192.168.36.12。

数据包转发说明：

网站服务器返回数据包从VLAN 231网段接口进入交换机，后续路由转发至B校区核心交换机的过程与互联网客户访问网站流量相同。

B校区核心交换机收到数据包后查询路由表，路由表显示192.168.36.0/24（VLAN 36网段）是直连网段，数据包从VLAN 36网段接口发出，返回给客户端，客户正常打开网页。

结束语

策略路由与访问控制列表作为网络流量管理的工具，通过规则匹配和定向转发，显著提升了网络资源的利用效率与灵活性。本文通过理论分析与实践案例结合，验证了其在复杂网络场景中的实用价值。未来，随着网络架构的复杂化，策略路由与访问控制列表的协同应用将进一步扩展，为智能化流量调度和网络优化提供更多可能性。网络管理者应深入掌握其配置逻辑与流程设计，以应对不断演进的业务需求和技术挑战。

参考文献

[1]王亮，唐永林.大规模网络集成路由重分布与路径控制技术[J].信息通信，2018，(10)：115-116.

[2]孙光懿.基于策略路由和NAT的多出口校园网仿真实验设计[J].西北民族大学学报（自然科学版），2017，38（02）：14-20.

[3]符军.访问控制列表在企业网中的应用与实现[J].轻工科技，2014，30（12）：58-59.