访问控制列表ACL

学习内容

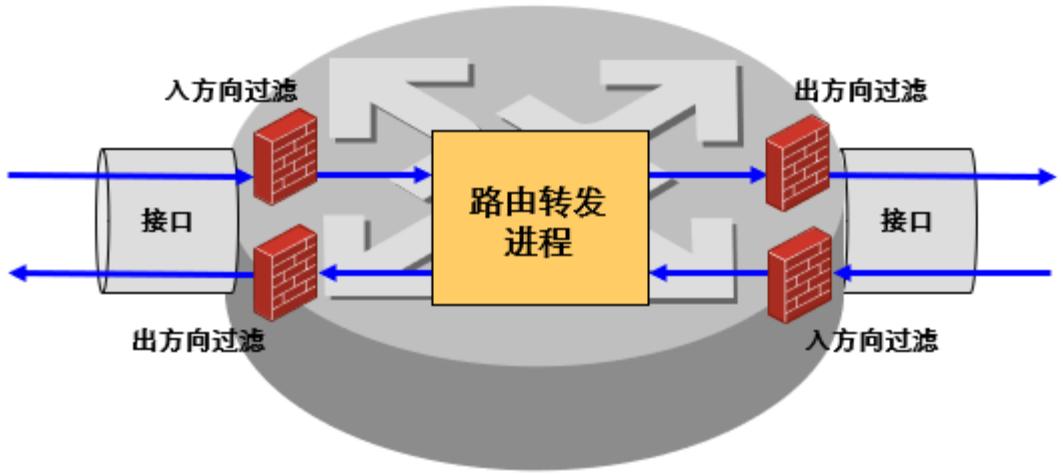
- ACL概述
- ACL包过滤原理
- ACL分类
- 配置ACL
- ACL的注意事项

ACL概述

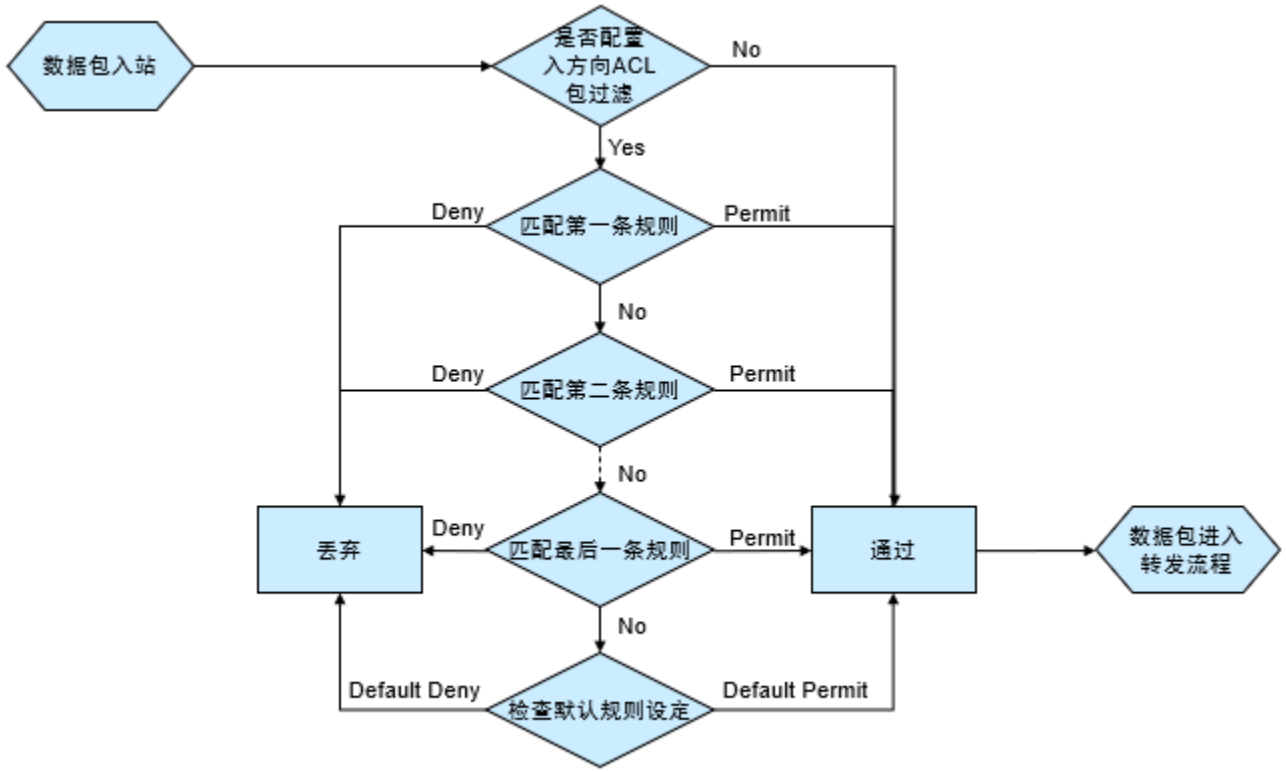
- ACL Access Control List 访问控制列表，是用来实现数据包识别功能的
- ACL的应用:
- 包过滤防火墙
- NAT
- QoS
- 路由策略和过滤
- 按需拨号

基于ACL的包过滤技术

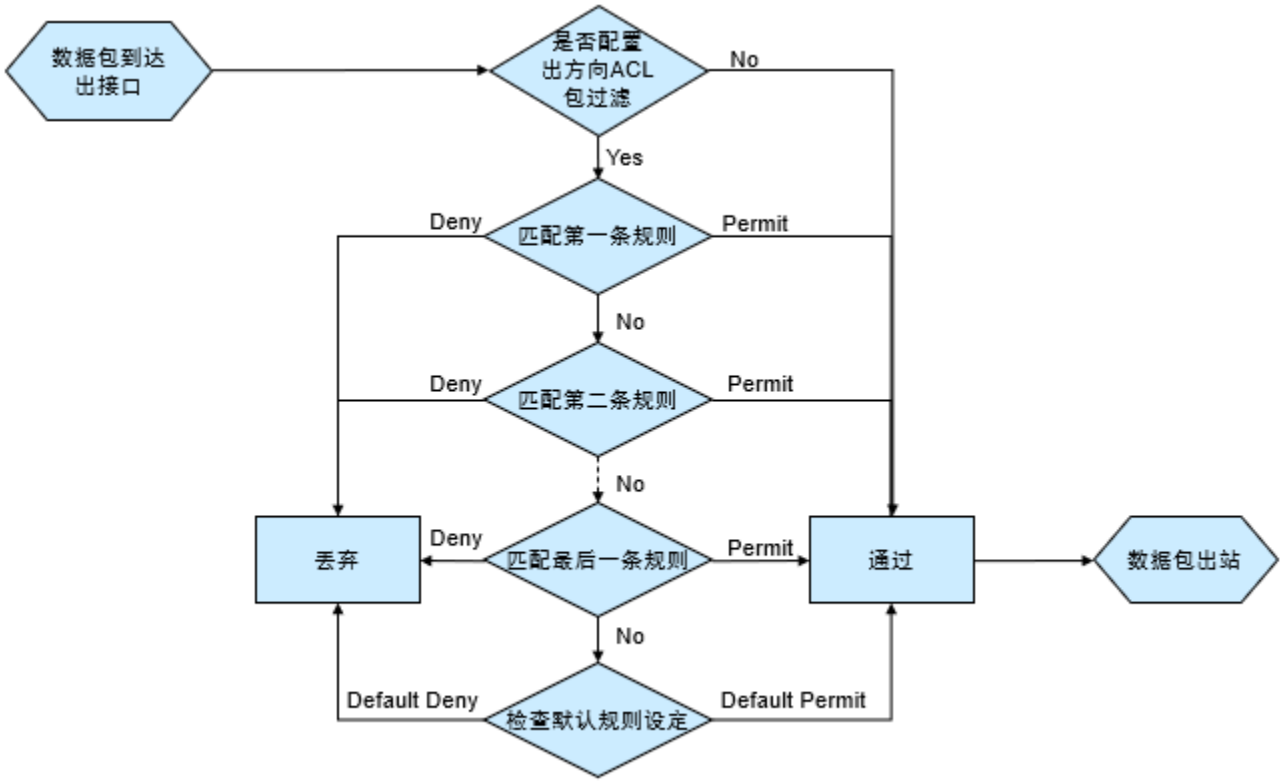
- 对进出的数据包逐个过滤，丢弃或允许
- ACL应用于接口上，每个接口的出入双向分别过滤



入站包过滤工作流程


数据包入站
是否配置入方向ACL包过滤
No
Yes
Deny
匹配第一条规则
Permit
No
Deny
匹配第二条规则
Permit
No
丢弃
Deny
匹配最后一条规则
Permit
通过
数据包进入转发流程
No
Default Deny
检查默认规则设定
Default Permit

出站包过滤工作流程


数据包到达
出接口
是否配置
出方向ACL
包过滤
No
Yes
Deny
匹配第一条规则
Permit
No
Deny
匹配第二条规则
Permit
No
丢弃
Deny
匹配最后一条规则
Permit
通过
数据包出站
No
Default Deny
检查默认规则设定
Default Permit

通配符掩码

- 通配符掩码和IP地址结合使用以描述一个地址范围
- 通配符掩码和子网掩码相似，但含义不同
  - 0表示对应位须比较
  - 1表示对应位不比较

通配符掩码	含义
0.0.0.255	只比较前24位
0.0.3.255	只比较前22位
0.255.255.255	只比较前8位

通配符掩码的应用示例

IP地址	通配符掩码	表示的地址范围
192.168.0.1	0.0.0.255	192.168.0.0/24
192.168.0.1	0.0.3.255	192.168.0.0/22
192.168.0.1	0.255.255.255	192.0.0.0/8
192.168.0.1	0.0.0.0	192.168.0.1
192.168.0.1	255.255.255.255	0.0.0.0/0
192.168.0.1	0.0.2.255	192.168.0.0/24和192.168.2.0/24

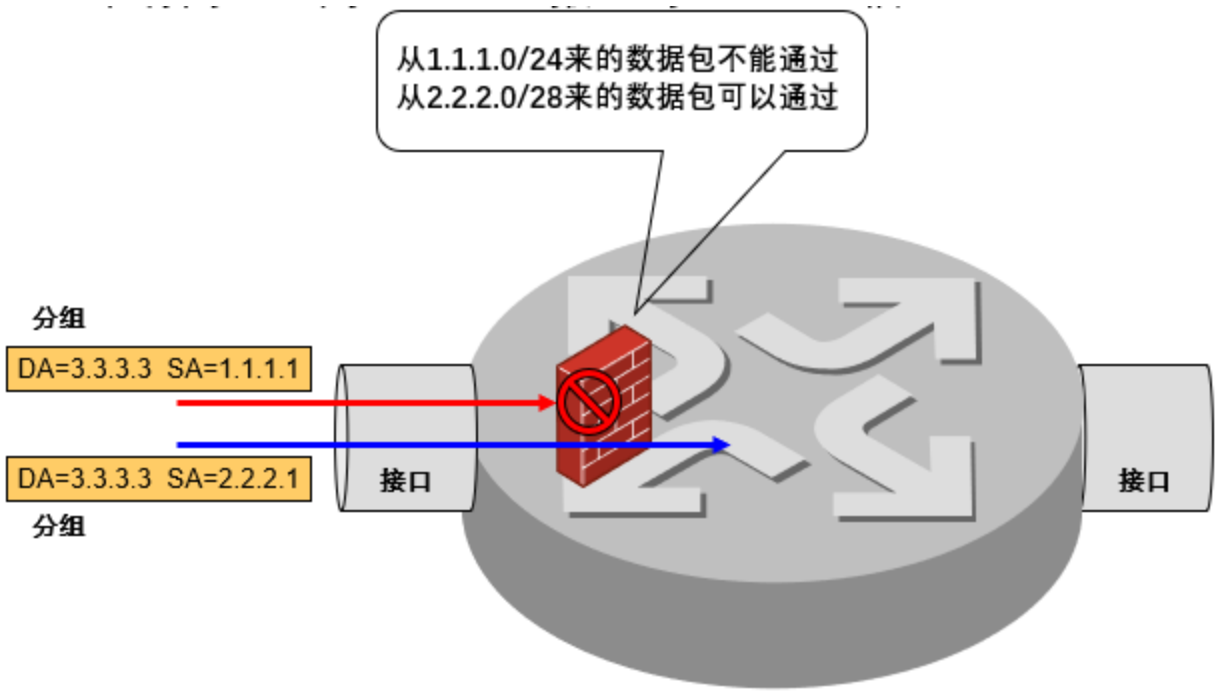
ACL分类

- ACL的标识
- 利用数字序号标识访问控制列表
- 可以给访问控制列表指定名称，便于维护

访问控制列表的分类	数字序号的范围
基本访问控制列表	2000～2999
扩展访问控制列表	3000～3999
基于二层的访问控制列表	4000～4999
用户自定义的访问控制列表	5000～5999

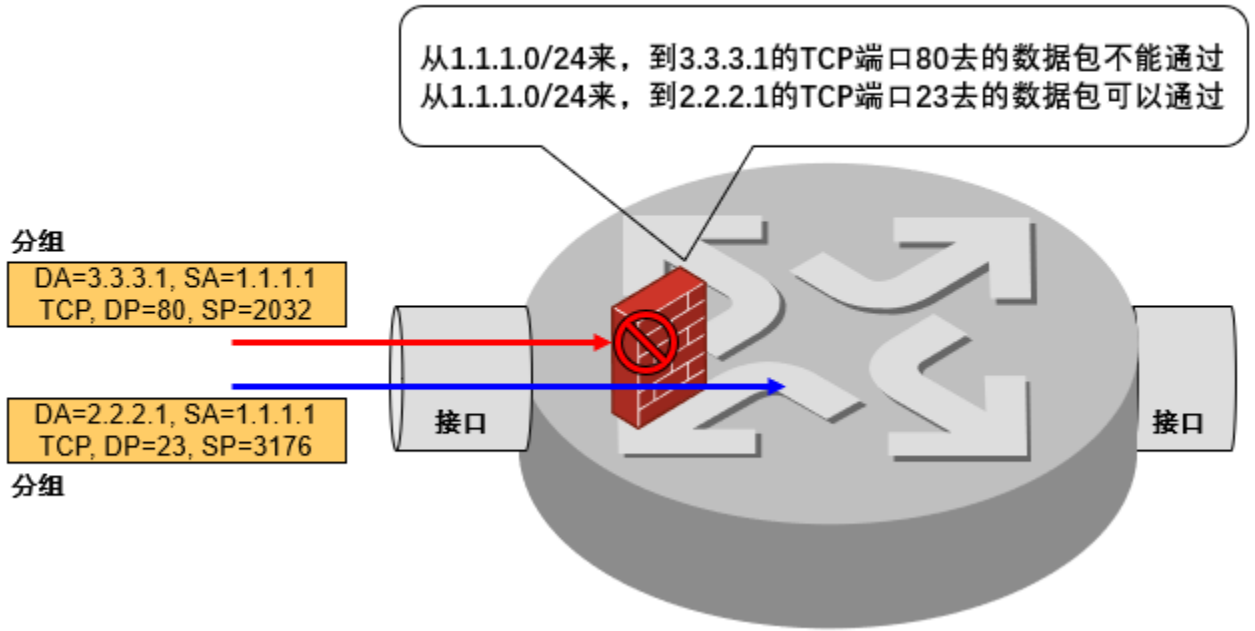
基本ACL

- 基本访问控制列表只根据报文的源IP地址信息制定规则



高级ACL

- 高级访问控制列表根据报文的源IP地址、目的IP地址、IP承载的协议类型、协议特性等三、四层信息制定规则



二层ACL与用户自定义ACL

- 二层ACL根据报文的源MAC地址、目的MAC地址、802.1p优先级、二层协议类型等二层信息制定匹配规则

- 用户自定义ACL可以根据任意位置的任意字串制定匹配规则
  - 报文的报文头、IP头等为基准，指定从第几个字节开始与掩码进行“与”操作，将从报文提取出来的字符串和用户定义的字符串进行比较，找到匹配的报文。

配置ACL过滤

- 根据需要选择合适的ACL分类
- 创建正确的规则
  - 设置匹配条件
  - 设置合适的动作（Permit/Deny)
- 在路由器的接口上应用ACL，并指明过滤报文的方向（入站/出站）

配置基本ACL

- 配置基本ACL，并指定ACL序号
  - 基本IPv4 ACL的序号取值范围为2000 ~ 2999

```
[sysname] acl acl-number
```

```
[sysname-acl-basic-2000] rule [ rule-id ] { deny | permit }
[ fragment | logging | source { sour-addr sour-wildcard | any } |
time-range time-name ]
```

配置高级ACL

- 配置高级IPv4 ACL，并指定ACL序号
  - →高级IPv4 ACL的序号取值范围为3000～3999

[sysname] acl *acl-number*

[sysname-acl-adv-3000] rule [*rule-id*] **{ deny | permit }** *protocol* **[destination** { *dest-addr dest-wildcard* **| any } | destination-port** *operator port1* [*port2*] **established | fragment | source** { *sour-addr sour-wildcard* **| any } | source-port** *operator port1* [*port2*] **| time-range** *time-name*]

在接口上应用ACL

- 将ACL应用到接口上，配置的ACL包过滤才能生效
- 指明在接口上应用的方向是Outbound还是Inbound

ACL包过滤显示与调试

操作	命令
查看防火墙的统计信息	**display firewall-statistics { all | interface** *interface-type interface-number***}**
查看以太网帧过滤情况的信息	**display firewall ethernet-frame-filter { all | dlsw | interface** *interface-type interface-number* **}**
清除防火墙的统计信息	**reset firewall-statistics { all | interface** *interface-type interface-number***}**
显示配置的IPv4 ACL信息	**display acl {** *acl-number* **| all}**
清除IPv4 ACL统计信息	**reset acl counter {** *acl-number* **| all |}**

ACL的注意事项

- 匹配顺序
- ACL支持两种匹配顺序：
  - 配置顺序（**config**）：按照用户配置规则的先后顺序进行规则匹配
  - 自动排序（**auto**）：按照“深度优先”的顺序进行规则匹配，即地址范围小的规则被优先进行匹配
- 配置ACL的匹配顺序：

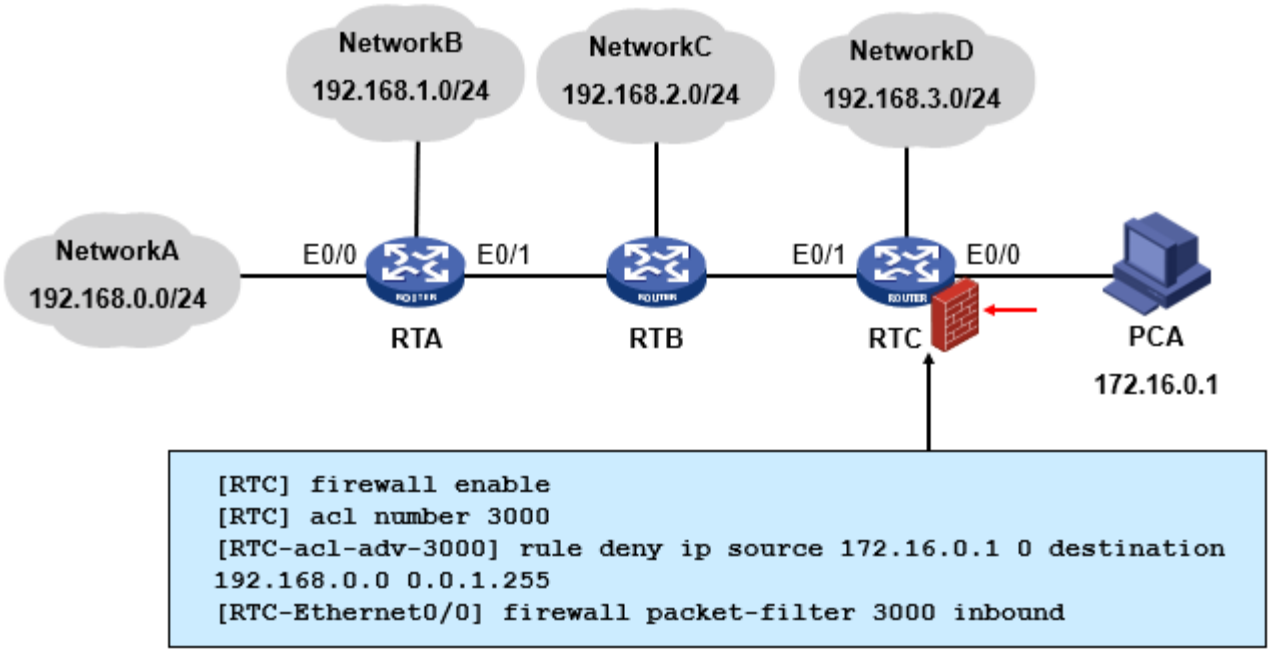
[sysname] acl number *acl-number* [**match-order { auto | config }**]

在网络中的正确位置配置ACL包过滤

- 尽可能在靠近数据源的路由器接口上配置ACL，以减少不必要的流量转发
- 高级ACL
  - 应该在靠近被过滤源的接口上应用ACL，以尽早阻止不必要的流量进入网络
- 基本ACL
  - 过于靠近被过滤源的基本ACL可能阻止该源访问合法目的
  - 应在不影响其他合法访问的前提下，尽可能使ACL靠近被过滤的源

高级ACL部署位置示例

- 要求PCA不能访问NetworkA和NetworkB，但可以访问其他所有网络



基本ACL部署位置示例

- 要求PCA不能访问NetworkA和NetworkB，但可以访问其他所有网络