访问控制列表【ACL】

一、访问控制列表的概念

1、应用于网络设备的接口上，指定哪些属于感兴趣流量，可以转发；哪些不属于感兴趣流量，予以拒绝

2、读取网络层头部中的源IP地址及目的IP地址；传输层头部中的源端口号码及目的端口号码信息

3、根据管理员预先定义好的规则进行逐一匹配

二、访问控制列表的作用

1、提供基本的安全手段，是防火墙最基础的应用

2、配合IPSec VPN，匹配感兴趣流量

3、配合QoS，控制数据流量

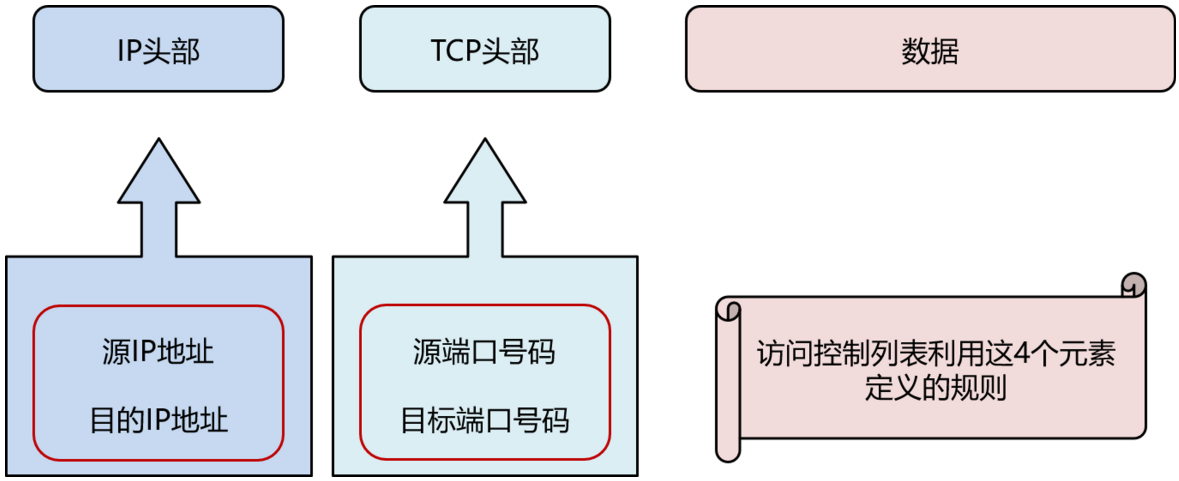
4、配合分布控制列表，匹配定义流量

5、控制通信量等

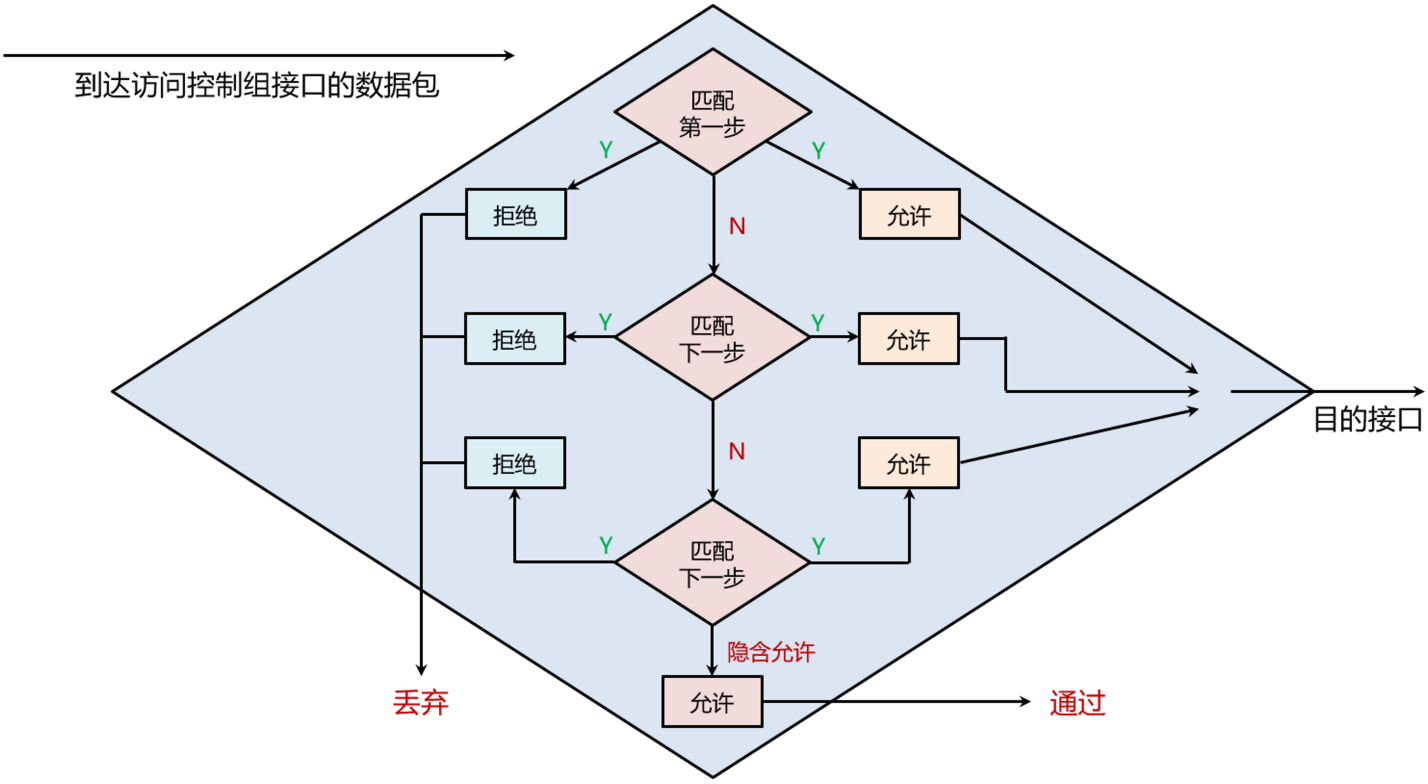
三、访问控制列表的核心原理

1、通过分析网络层头部中的信息及传输层头部中的信息进行判断

2、基于SIP（源IP）、DIP（目的IP）、SPort（源端口号码）、DPort（目的端口号码），这4元素进行过滤



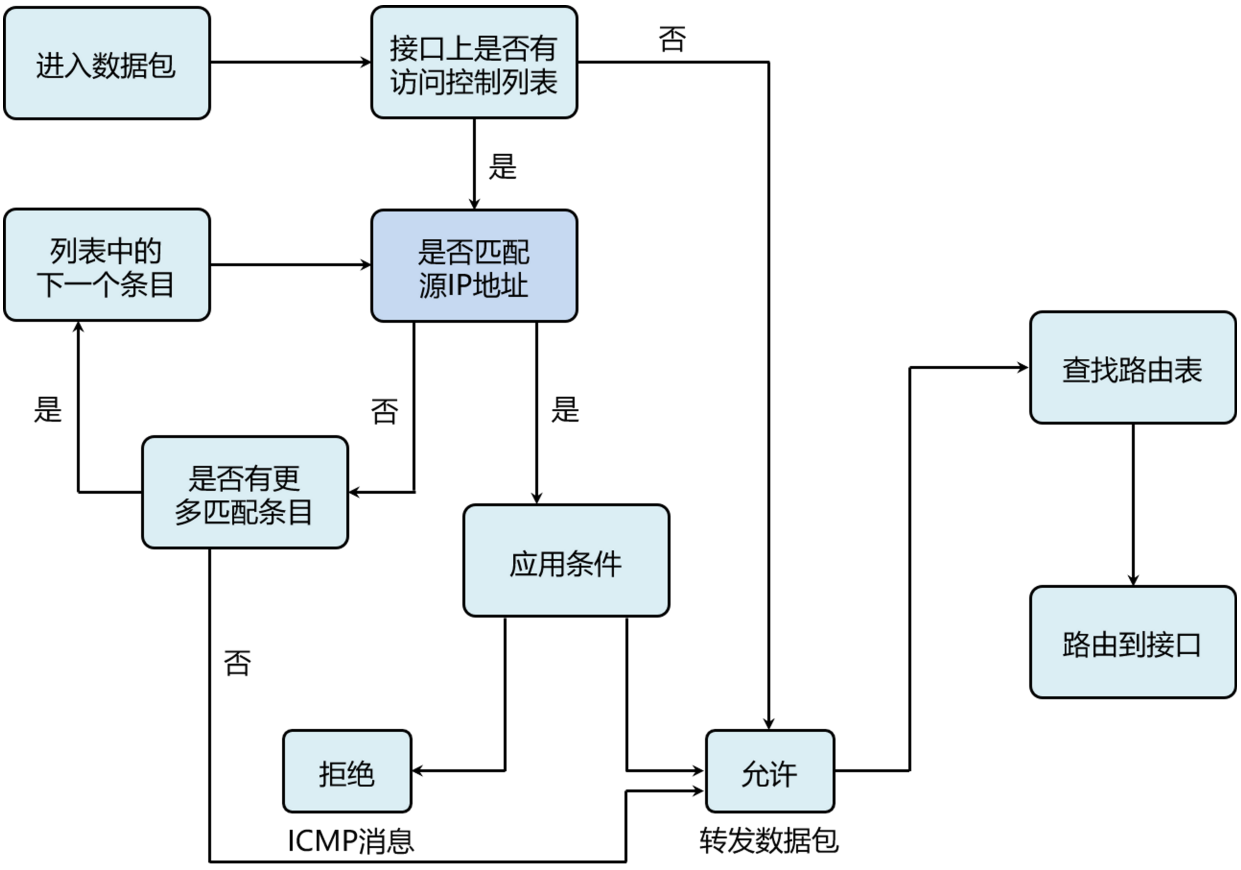
四、网络设备对访问控制列表的处理过程



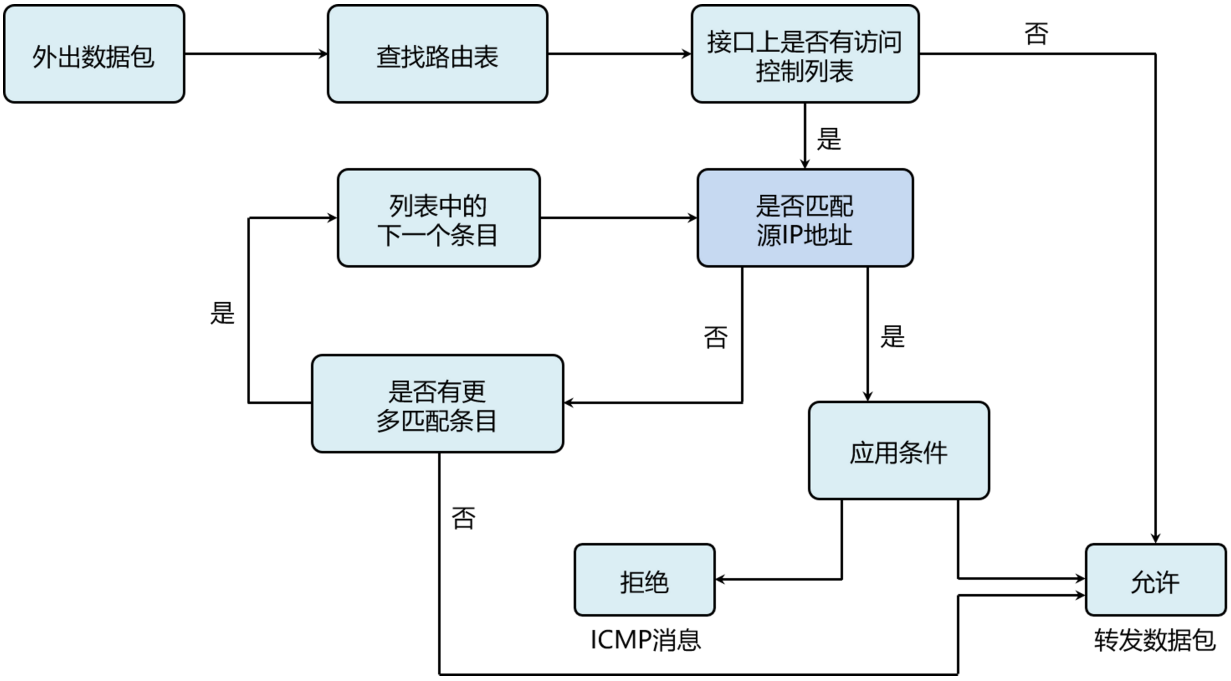
五、访问控制列表的入与出

1、访问控制列表可以应用在入口上，亦可应用在出口上

2、应用在入口上，网络设备先检查是否有ACL，再查找路由表



3、应用在出口上，网络设备先查找路由表，再检查是否有ACL



六、访问控制列表的关键命令

1、permit：允许放行的流量

2、deny：拒绝通过的流量

七、访问控制列表的通配符

1、通配符【any】可代替 0.0.0.0 255.255.255.255

2、通配符【0】表示检查IP地址的所有位

八、访问控制列表的种类

1、基本类型的访问控制列表

2、高级类型的访问控制列表

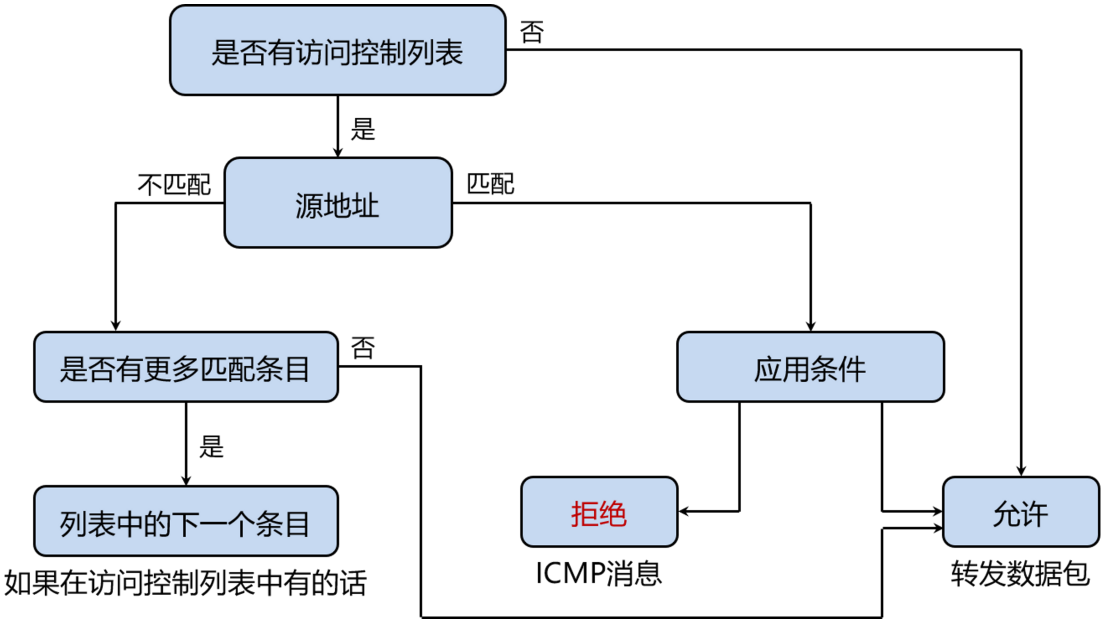
3、适配二层的访问控制列表

4、基于时间的访问控制列表

九、基本访问控制列表

1、仅根据源IP地址来允许或拒绝流量

2、列表号从2000至2999



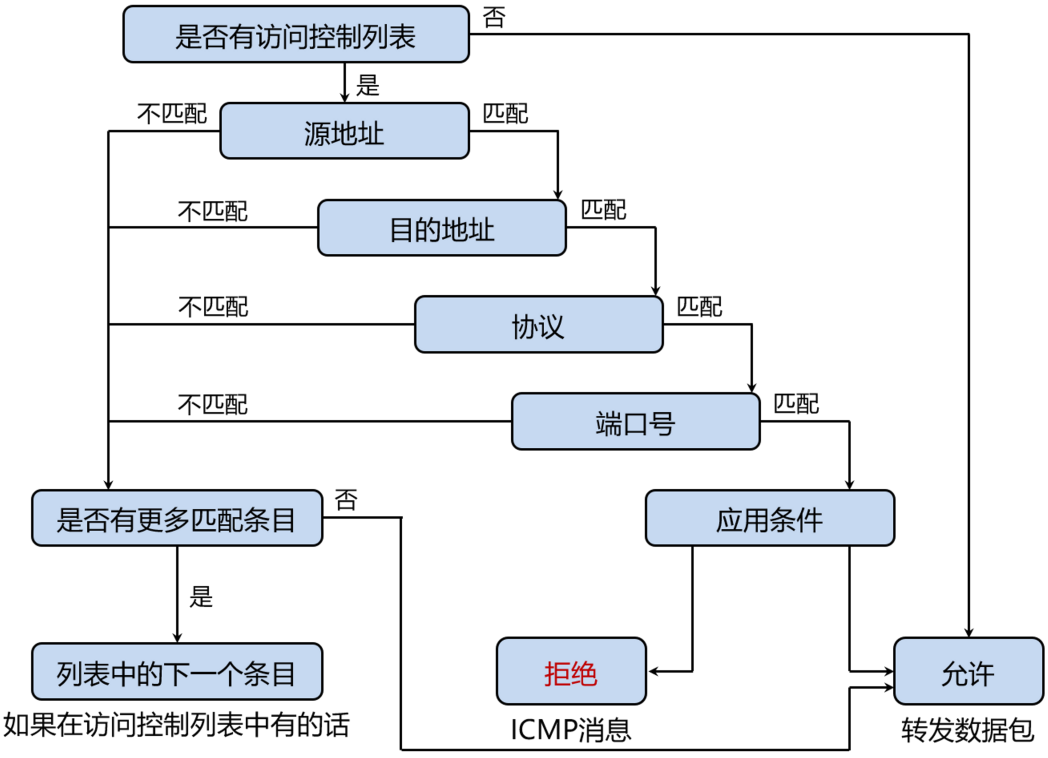
十、高级访问控制列表

1、同时根据源及目的IP地址、传输层协议和应用端口号进行过滤

2、每个条件都必须匹配，才会施加允许或拒绝条件

3、访问控制列表号从3000至3999

4、高级ACL可以实现更加精确的流量控制



十一、常见的服务及其所使用的端口号

端口号码	关键字	具体阐述	TCP / UDP
20	FTP-Data	【文件传输协议】FTP【数据】	TCP
21	FTP	【文件传输协议】FTP	TCP
23	Telnet	终端连接	TCP
25	SMTP	简单邮件传输协议	TCP
41	NameServer	主机名服务	UDP
53	Domain	域名服务【DNS】	TCP / UDP
69	TFTP	简单文件传输协议【TFTP】	UDP
80	WWW	万维网	TCP

十二、访问控制列表的操作符

操作符及语法	表达含义
eq port-number	等于端口号 port-number
gt port-number	大于端口号 port-number
lt port-number	小于端口号 port-number
neq port-number	不等于端口号 port-number

十三、ACL的配置

详细配置见实验手册