华为路由交换由浅入深系列(九)-华为路由器交换 ACL 的应用与经验总结

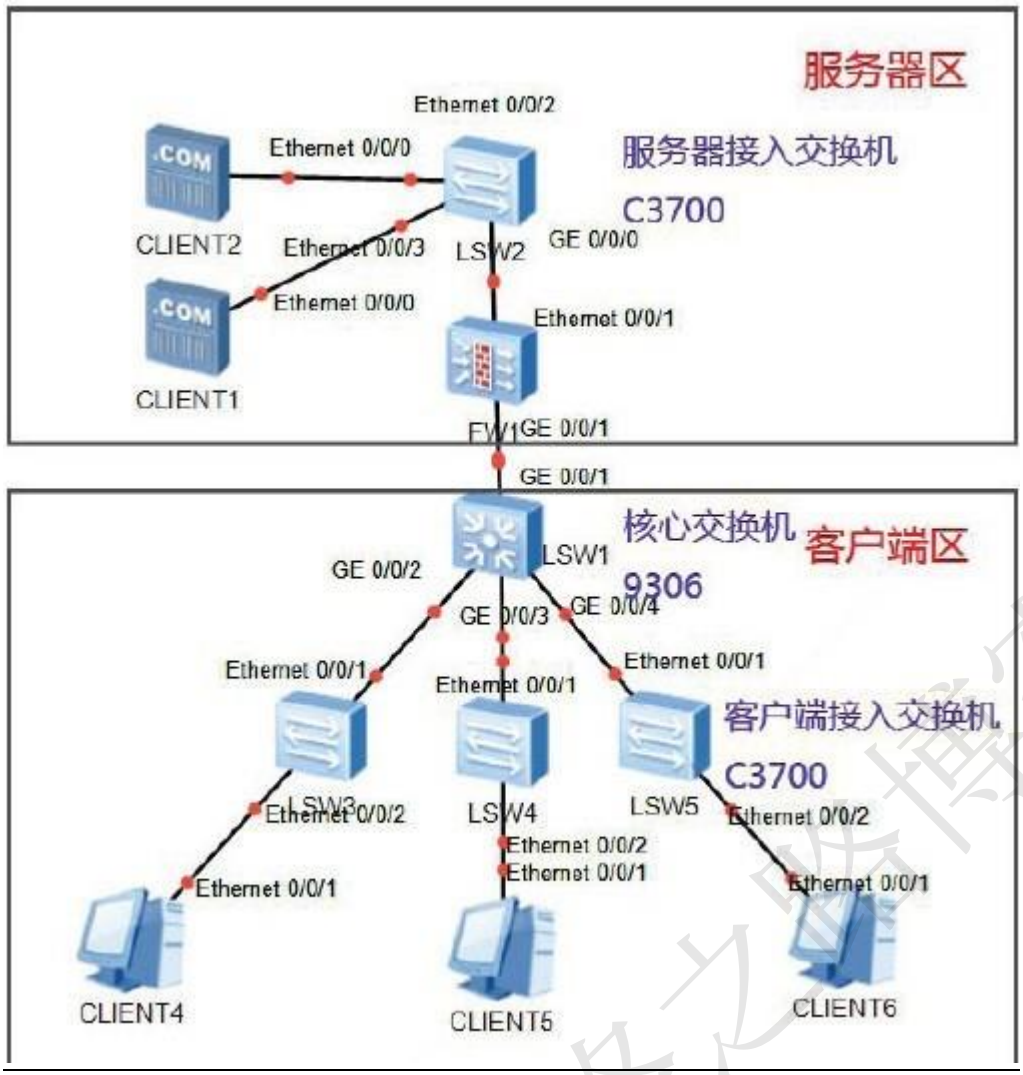
1 ACL 概述

随着网络规模的扩大和流量的增加，对网络安全的控制和对带宽的分配成为网络管理的重要内容。通过对报文进行过滤，可以有效防止非法用户对网络的访问，同时也可以控制流量，节约网络资源。ACL（Access Control List，访问控制列表）即是通过配置对报文的匹配规则和处理操作来实现包过滤的功能。

ACL 通过一系列的匹配条件对报文进行分类，这些条件可以是报文的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、端口号等。

2 案例背景[交换机]

网络环境拓扑如下（客户端接入交换机约有几十个，所有设备均采用静态 IP）



服务器区所有服务器网关均在核心交换机上，共有 9 个 Vlan，9 个网段分别如下；

Vlan10-Vlan11 网段分别为 10.0.10.0/24-10.0.11.0/24

Vlan14-Vlan19 网段分别为 10.0.14.0/24-10.0.19.0/24

交换机管理 Vlan 为 Vlan1: 10.0.13.0/24，核心交换机的管理 ip 为 10.0.13.254，其余接入交换机网关均在核心交换机上；

客户端共有 8 个 Vlan，分别为 Vlan20-Vlan100，网段分别为 10.0.20.0/24-10.0.100.0/24，网关均在核心交换机上；

3 需求一：对服务器区服务器做安全防护，只允许客户端访问服务器某些端口

由于网络环境拓扑为客户端——客户端接入交换机——核心交换机——防火墙——服务器接入交换机——服务器，

也即客户端访问服务器需要通过防火墙，所以对服务器的防护应该放到防火墙上来做，因为若用交换机来做过滤，配置麻烦且失去了防火墙应有的作用（此处不做防火墙配置介绍）；

4 需求二：交换机只允许固定管理员通过 ssh 登陆

此处做防护有较为方便的俩种方法

一：在所有交换机配置 VTY 时，调用 ACL 只允许源为网络管理员的 IP 访问，但此方法虽配置不复杂，但是配置工作量较大需要在所有交换机上配置，而且不灵活例如在网络管理员人员或者 IP 变迁时，需要重新修改所有交换机 ACL，所以并不是首选方案；

二：因为管理交换机管理 Vlan 与所有客户端 Vlan 不在同一 Vlan，也即客户端访问接入交换机必须通过核心交换机，所以可以在核心交换机上做 ACL 来控制客户端访对接入交换机的访问，核心交换机的访问通过 VTY 来调用 ACL；配置部分在下面；

5 需求三：客户端 VLAN 之间不能互相访问，客户端只允许访问服务器 VLAN

一：在核心交换机上的所有链接客户端接入交换机端口做 ACL，只放行访问服务器的流量，拒绝其余流量，但由于客户端接入交换机约有几十台，所以配置工作量大几十个端口都需要配置，所以也不是首选方案；

二：在核心交换机上的客户端 Vlan 做 Acl，只放行访问服务器的流量，拒绝其余流量，由于客户端 Vlan 共有 8 个所以相对于在物理接口上做 ACL 而言，工作量较小，所以选择此方案；

6 配置部分

6.1 ACL 配置部分

acl number 2000

rule 5 permit source 10.0.20.11 0

rule 10 permit source 10.0.21.15 0

rule 15 deny

//定义允许访问核心交换机的俩位网络管理员 IP 地址；

acl number 3000

rule 51 permit ip destination 10.0.10.0 0.0.0.255

rule 53 permit ip destination 10.0.12.0 0.0.0.255

rule 55 permit ip destination 10.0.14.0 0.0.0.255

rule 56 permit ip destination 10.0.15.0 0.0.0.255

rule 57 permit ip destination 10.0.16.0 0.0.0.255

rule 58 permit ip destination 10.0.17.0 0.0.0.255

rule 59 permit ip destination 10.0.18.0 0.0.0.255

rule 60 permit ip destination 10.0.19.0 0.0.0.255

//定义所有客户端只允许访问服务器 Vlan

rule 71 permit tcp source 10.0.20.11 0 destination 10.0.13.0 0.0.0.255 destination-port eq 22

rule 72 permit tcp source 10.0.21.15 0 destination 10.0.13.0 0.0.0.255 destination-port eq 22

//定义允许访问核心交换机的 tcp22 端口（即 SSH）的俩位网络管理员 IP；

acl number 3100

rule 5 permit ip

//拒绝除允许网段外的其余所有流量

//由于此处的 acl3000 及 3100 是给下面的 QOS 做调用的，所以此处的 permit 或 deny 不起作用，随意设置即可；

6.2 Qos 调用部分

traffic classifier 3000 operator or precedence 5

if-match acl 3000

// 定义名为 classifier 3000 的流分类，并调用 ACL3000

traffic classifier 3100 operator or precedence 10

if-match acl 3100

// 定义名为 classifier 3100 的流分类，并调用 ACL3100

//定义流分类

traffic behavior 3000

permit

//定义名为 behavior 3000 的流行为，并赋予允许值

traffic behavior 3100

deny

//定义名为 behavior 3100 的流行为，并赋予拒绝值

//定义流行为

//上面 ACL 的允许或拒绝不起作用，通过此处来定义拒绝或允许

traffic policy 634acl

classifier 3000 behavior 3000

classifier 3100 behavior 3100

//定义名为 policy 634acl 流策略，并将 classifier 3000 流分类与 behavior 3000 流行为关联，以及 classifier 3100 流分类与 behavior 3100 流行为关联（注意：允许在前，拒绝在后）；

vlan 20

description kjfzb jimi

traffic-policy 634acl inbound

//依次登录客户端 Vlan 应用流策略

至此完成了所有客户端 Vlan 之间不能互访，以及除网络管理员之外不能访问接入交换机管理网段的访问控制；

user-interface vty 0 4

acl 2000 inbound

//在 vty 界面中调用 Acl2000，即只允许俩网络管理员登录；

authentication-mode aaa

user privilege level 3

protocol inbound ssh

//至此完成了只允许网络管理员登录核心交换机的访问控制；

关于华为 ACL 日常维护中的一点点经验和大家分享下

在已经做好的 ACL 控制策略中,

如 192.168.1.0 禁止访问 192.168.2.0 3.0 4.0 5.0 网段

acl number 3001

rule 5 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255

rule 10 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255

rule 15 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.4.0 0.0.0.255

rule 20 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.5.0 0.0.0.255

rule 25 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.6.0 0.0.0.128

但是在工作需求中要重新调整,使得 192.168.1.0 中的某个 IP 如 192.168.1.10 需要访问已被禁止的网段中的某个 IP 如

192.168.6.215,那么要将 1.10 与 6.215 互通在调整过程中需要什么呢.

很显然重建建 ACL 规则是不可行的,因为将规则应用到端口上时,只能同时应用一条规则.

那么就只能从原有的 3001 规则上下手了.下面是操作步骤:

1.首先在端口上将 inbound 应用停用,如果 3001 已经在使用中,那么 rule 是不可更改的

2.清空 3001 中的所有规则,做好备份.将 permit 条目放在前端,再恢复原有的规则,原因是 acl 匹配有一个自上而下的顺序匹配,所以

必须首先 permit 后 deny

若先匹配到如 rule 25 已经是 deny,那么后面无论怎么做 permit,结果还是拒绝,那么调整后的顺序应当是

rule 5 permit ip source 192.168.1.10 0 destination 192.168.6.215 0

rule 10 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255

rule 15 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255

rule 20 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.4.0 0.0.0.255

rule 25 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.5.0 0.0.0.255

rule 30 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.6.0 0.0.0.128

3.重新应用至接口.在应用过程中注意一点

traffic behavior 上 permit 与 deny 的区别.

使用 permit 表示按照 acl 3001 的规则来进行数据放行,3001 中允许那就允许,禁止那就禁止

但是若使用 deny,则无论 3001 规则中的 permit 或者 deny,一律全都丢弃不进行转发.

关于路由器的调用，对比交换来说简单很多。

traffic-filter inbound acl 3001 【接口下调用即可】

说明：高版本的交换机 VRP 也支持该命令，可以简化 ACL 的配置。

博主也只是业余时间写写技术文档，请大家见谅，大家觉得不错的话，可以推荐给朋友哦，博主会努力推出更好的系列文档的。如果大家有任何疑问或者文中有错误跟疏忽的地方，欢迎大家留言指出，博主看到后会第一时间修改，谢谢大家的支持，更多技术文章尽在网络之路博客，http://ccieh3c.com。