思科交换机 acl 应用要点

ACL 访问控制列表,是交换机的基本功能,大多数厂商的交换机的 acl 是应用在端口上,如 g0/0/1 之类的物理端口,方向为 in 或 out,很容易理解,配置时不易出错。不过思科的交换机一般都是将 acl 应用在 int vlan 接口上,如 int vlan 1 之类的,方向为 in 或 out(一般二层交换机只能 in)所以容易出错,搞不好会酿成生产事故。

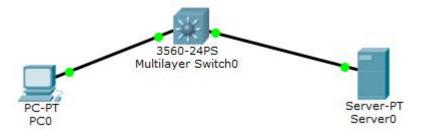
首先思科交换机的 acl 本身的配置这里就不多说了,只讲 1 点:它的每个 acl 的末尾默 认是有 deny any any 的

- 1.当我们仅配置 permit xx xx 这一条时,则默认只 permit 这一条,因为有隐含的 deny any any
- 2.当我们仅配置 deny xx xx 这一条时,则默认是无 permit 的,因为隐含有 deny any 3.所以当我们想 只过滤某条访问规则时,写完 deny xx xx 这条后,得再加上 permit ip any any,不然就全部 deny 了

然后讲它的 acl 在 int vlan 上的方向问题:

拓扑如下图:

3560 交换机为三层的,支持 in 和 out 方向的应用,作为以下 2 台计算机的网关 pc0 为客户端,ip: 10.1.1.1 接入 vlan 1,网关 10.1.1.254 server 0 为服务端,ip: 10.2.2.2 接入 vlan 2,网关 10.2.2.254



交换机上想做一条 acl,仅禁止 pc0 访问 server 0 的 80 端口,其他的流量正常通过,该怎么配置呢?

** ACL 配置如下:

Switch#conf t

Switch(config)#ip access-list extended deny_80

//创建名为 deny 80 的扩展 acl

Switch(config-ext-nacl)#deny tcp host 10.1.1.1 host 10.2.2.2 eq 80

//阻止源 ip 为 10.1.1.1,目的 ip 为 10.2.2.2,目的端口 80/tcp 的报文 Switch(config-ext-nacl)#permit ip any any

//因为末尾隐含为 deny any,所以 仅 deny 某条时,要 permit 所有 Switch(config-ext-nacl)#exit

Switch(config)#

**应用 acl 到 int vlan 接口上:

Switch(config)#int vlan 1 //进入接口配置界面 Switch(config-if)#ip access-group deny_80 in //应用 acl 到 in 方向 Switch(config-if)#exit 也可这样应用,用在 int vlan 2 上
Switch(config)#int vlan 2
Switch(config-if)#ip access-group deny_80 out //应用到 out 方向
Switch(config-if)#exit

能否同时应用到 int vlan 1 和 int vlan 2 上呢?可以,只是没必要做 2 次匹配,对速度有影响。

关于 in / out 方向的解释:

因为源 ip:10.1.1.1 发来的报文要先发给网关 int vlan 1,所以对于 int vlan 1 而言就是入站,而且 int vlan 1 收到报文后,要走路由层,因为目的 ip 不在本 vlan 里,int vlan 1 把报文发给路由层的话,不算是 out,只有发给本 vlan 里的主机时,才算 out

而在 int vlan 2 那里应用 acl 时,只能用 out,因为它收到的报文是从路由层转来的,不 算 in,int vlan 2 收到报文后,发现目的 ip 为本 vlan 里的主机的 ip,所以发给本 vlan 的主机的话,算 out 方向。

也就是说,如果报文只是经过此 vlan 的某 2 个端口,不发给此 vlan 的 int vlan x 接口的话,就没有 in,也没有 out,无法做 acl 的匹配。

或者说没有经过路由层面的报文,没法应用 acl (这也是思科交换机的一大痛点)二层交换机只能应用到 int vlan 接口的 in 方向,也就是只能对上行流量做匹配

当然,有些较新的思科交换机也是支持应用 acl 到物理端口上的。这里就不多讲了,和其他品牌的应用原理都一样。

以上就是思科交换机的 acl 应用到 int vlan 接口的 注意要点!

Cof-Lee 2020-08-21