**一、访问控制列表**

管理网络当中的数据流量，实现数据过滤的重要手段。可以在路由器、三层交换、二层交换和防火墙上实现。

**隐藏规则：**当前面的规则都匹配不上，华为默认允许，思科默认拒绝。

|  |  |  |
| --- | --- | --- |
| 分类 | 规则描述 | 编号范围 |
| 基本ACL | 仅使用报文中的源IP地址、分片信息和生效时间段信息来定义规则 | 2000~2999 |
| 高级ACL | 渴作用源IP地址、目的IP地址、协议类型、TCP/UDP源/目端口号来定义规则 | 3000~3999 |
| 二层ACL | 根据IP报文中的以太网帧头来定义、如源/目MAC，以太网帧协议类型等 | 4000~4999 |
| 用户高级ACL | 要实现更复杂、更特殊的定义 | 5000~5999 |

ACL在系统视图下配置，并且需要被应用在具体接口上才能生效。

***（基本/高级ACL下午案例考的比较多）***

**基本ACL配置（华为）**

1、acl [number]*acl-number(2000~2999)* [match-order] {auto|config}

2、rule [*rule-id*] permit|deny source *IP地址 反向子网掩码*

**其中：any表示任意网段；表示主机用:192.168.10.1 0**

**例：**

已配置如下

rule permit source 192.168.1.0 0.0.0.255

rule deny source 192.168.1.1 0.0.0.0

如果配置config，则192.168.1.1数据会被转发，如果配置auto，则不会被转发

**说明：**

match-order:可选参数，说明匹配顺序。

**auto（深度优先）**表示按照自动排序，**config**表示安全配置顺序匹配（默认）

***注：auto如果是基本ACL，先比较源IP地址的范围，如果两条规则源IP地址一致，则依照配置顺序匹配（了解即可）。***

**rule**:匹配规则，**rule-id**可选参数，指定规则的编号

**permit|deny**：匹配操作，允许|拒绝

**ACL默认步长为5**，可在ACL视图下通过step *step*进行调整。

**//实现云讯源IP为172.16.10.3的主机报文通过，拒绝源IP为172.16.10.0/24网段的其他报文通过，并配置表述信息为permit only 172.16.10.3 through**

[HUAWEI]acl 2020

[HUAWEI-acl-basic-2020]rule permit 172.16.10.3 0.0.0.0

[HUAWEI-acl-basic-2020]rule deny 172.16.10.0 0.0.0.255

[HUAWEI-acl-basic-2020]description permit only 172.16.10.3 through

//描述信息

最后再把这个ACL应用在路由器的某个接口上

[接口视图]**traffic-filter** **outbound** acl 2020

**二、ACL在接口上的应用**

访问控制列表在接口应用的方向

**出：**已经过路由器的处理，正离开路由器接口的数据包：outbound

**入：**已经到达路由器接口的数据包，将被路由器处理：inbound

**注意：**设备自身产生的流量不会检测ACL

**三、高级ACL配置（华为）**

1、acl [number] acl-number(3000~3999) [match-order] {auto|config}

//设置访问控制列表号

2、rule [rule-id] permit|deny {*protocol*} source *源IP地址 反掩码* destination *目的IP地址 反掩码* destination-port eq *端口号*

说明：

**protocol：**制定对应的协议如，TCP、UDP、ICMP、IP等

**destination-port:**目的端口，若是源端口source-port

**eq** 等于 gt 大于 lt小于 neg 不等于 range 指定范围

端口号：可直接写端口好或协议对应的关键字，如telnet/WWW/dns

**例：**

**配置允许源IP是172.16.10.3到目的IP是172.16.20.0/24网段的ICMP报文通过。**

[HUAWEI]acl 3000

[HUAWEI-acl-adv-3000]rule permit icmp source 172.16.10.3 0.0.0.0 destination 172.16.20.0 0.0.0.255

**在路由器接口上应用这个ACL**

[接口视图]traffic-filter inbound acl 3000

**四、基于时间的ACL**

**例：**

[HUAWEI]time-range mytime 09:00 to 12:00 working-day

[HUAWEI]time-range mytime 14:00 to 17:00 workting-day

[HUAWEI]acl 2000

[HUAWEI-acl-basic-2000]rule permit source 192.168.10.0 0.0.0.255

[HUAWEI-acl-basic-2000]rule permit source 192.168.20.1 0 time-range mytime

[HUAWEI-acl-basic-2000]rule deny source any

[HUAWEI-acl-basic-2000]quit

[HUAWEI]interface g0/0/2

[HUAWEI-Gigabitethernet 0/0/2]traffic-filter outbound acl 2000

**五、命名的ACL**

**命名访问控制列表允许在标准和扩展访问控制列表中使用名称代替标号**

**1、基本命名ACL：**

acl name *acl-name* {basic acl-numble} [match-order{auto|config}]

例如：

acl name csai 2000

**2、高级命令ACL：**

acl name *acl-name* {advance acl-numble} [match-order{auto|config}]

例如：

acl name csai advance

**六、ACL部署的位置（考点）**

* 高级ACL应该尽量放置在接近数据流的源的地方；
* 基本ACL应该尽量放置在接近数据流的目的的地方，以免引起错误。

**七、流分类、流行为、流策略（考一次）**

一些华为的三层交换机（S系列）ACL无法直接应用在接口上

* **配置ACL**

[HUAWEI]acl 3000

[HUAWEI-acl-adv-3000]rule deny ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255

* **基于ACL的流分类**

[HUAWEI]traffic classifilter **c\_xs//名称**

[HUAWEI-classifilter-c\_xs]if-match**acl 3000**

* **配置流行为，动作为拒绝报文通过**

[HUAWEI]traffic behavior **b\_xs**

[HUAWEI-behavior-b\_xs]**deny**

* **配置流策略，将流分类与流行为进行关联**

[HUAWEI]traffic policy **p\_xs**

[HUAWEI-trafficpolicy-p\_xs]classifilter **c\_xs** behavior **b\_xs**

* **应用流策略，实现相应的访问控制**

[HUAWEI]interface e0/0/1

[接口视图]**traffice-policy p\_xs inbound**

**八、自反ACL（思科时代考过）**

概念：设备根据一个方向的ACL，自动创建一个反方向的ACL。只能根据高级ACL来进行自反，并且只能根据TCP/UDP/ICMP报文来生成ACL规则。

**特点：**

内网发起的流量，设备会根据流量的第三层和第四层信息，生成一个临时性的反向ACL，并且保持一段的时间，此临时性的ACL中，协议类型不变，而源IP和目的IP、源端口和目的端口与初始的ACL进行对调，而且可以设置老化周期，如果老化周期内没有相对应的流量返回，则自反的ACL会被删除，增加老化的安全性。

***（也就是配置了自反ACL后，主机发送给服务器流量后，服务器才能返回流量给主机，而服务器主动发起的流量则会被ACL丢弃。）***

***配置：***

* **创建高级ACL3000并配置ACL规则，允许UDP报文通过**

[HUWEI]acl 3000

[HUAWIE-acl-adv-3000]rule permit udp

[HUAWIE-acl-adv-3000]quit

* **由于来自Internet的报恩从接口g2/0/1进入路由器，所以可以在接口g2/0/1的出方向配置自反ACL功能，对UDP报文进行自反。**

[HUWEI]interface gigabitethernet 2/0/1

[接口视图]traffic-reflect outbound acl 3000

***//自反ACL应用在接口出方向***

**九、扩展-防火墙上应用ACL（华为）**

* **华为防火墙默认分为3个安全区域**

trust区（85）：本区域内的网络受信程度高，通常用来定义内网

DMZ区（50）：本区域内的网络受信程度中等，通常用来定义公共服务器所在的区域。

untrust区（5）：本区域代表的是不受信的网络，通常来定义外网

***防火墙自身的local区域优先级为100***

* **安全域间的数据流动具有方向性，包括inbound和outbound**

入方向：数据由低优先级的区域向高优先级区域传输

出方向：数据由高优先级区域向低优先级区域传输

* **其中安全区域的配置命令主要是：**

[FW]firewall zone name test ***//创建安全区域TEST***

[FW-zone-test]set priority 10 ***//安全级别设置为10***

[FW-zone-test]add interface g0/0/1 ***//把接口g0/0/1加入安全区域***

**配置举例：**

**要求在安全区域到非安全区域的方向上，拒绝源地址为192.168.0.100的主机报文，允许源网段为192.168.0.0/24到网段172.16.0.0/24的报文通过。**

[FW]acl 3000

[FW-acl-adv-3000]rule deny ip source 192.168.0.100 0

[FW-acl-adv-3000]rule permit ip source 192.168.0.0 0.0.0.255 destination 172.16.0.0 0.0.0.255

[FW-acl-adv-3000]quit

[FW]**firewall interzone trust untrust**

[FW-interzone-trust-untrust]**packet-filter 3000 outbound**

**十、NAT地址转换技术**

* **静态NAT：固定的一对一IP地址映射**

[R1]interface e0/0/1

[接口视图]ip address 192.1.1.1 30

[接口视图]**nat static global 192.1.1.2 inside 10.1.1.2**

* **动态NAT：basic NAT （也是一对第一做转换）**

[R1]nat address-group 1 192.1.1.2 192.1.1.4 ***//定义公网地址池***

[R1]acl 2000

[R1-acl-basic-2000]rule permit source 10.1.1.0 0.0.0.255

***//该ACL并不是对数据报进行过滤，而且标注哪些地址需要做NAT转换***

[R1-acl-basic-2000]quit

[R1]interface e0/0/1

[接口视图]**nat outbound 2000 address-group 1 no-pat**

***//实现ACL2000中定义的IP可以与地址池中的地址进行一对一转换***

* **动态NAT-PT（华为）**

**PAT基于端口的地址转换**

[R1]nat address-group 1 192.1.1.2 192.1.1.4

[R1]acl 2000

[R1-acl-basic-2000]rule permit source 10.1.1.0 0.0.0.255

[R1-acl-basic-2000]quit

[R1]interface e0/0/1

[接口视图]nat outbound 2000 address-group 1

***//在出接口上做PAT***