

通过用户自定义ACL实现匹配IP报文TTL字段

ACL IPv4 倪民 2020-10-29 发表

组网及说明

不涉及

配置步骤

为了匹配IP报文TTL字段，需要通过用户自定义ACL实现，自定义ACL的序号取值范围为5000~5999。

规则配置的命令格式如下：

```
rule [ rule-id ] { permit | deny } [ [ I2 | I4 ] { rule-string rule-mask offset } &<1-8> ] [ time-range time-name ]
```

其中，

I2：从二层帧头开始偏移。

I4：从四层报文头开始偏移。

rule-string：用户自定义的规则字符串，必须是16进制数组成，字符长度必须是偶数。

rule-mask：规则字符串的掩码，用于和报文作“与”操作，必须是16进制数组成，字符长度必须是偶数。

。

offset：偏移量，指定从第几个字节开始进行“与”操作。

&<1-8>：表示一次最多可以定义8个这样的规则。

例如：

```
acl number 5000
```

```
rule 0 deny I2 80 ff 22
```

表示从二层以太网帧偏移22个字节，即TTL字段。

80 ff表示匹配TTL=128。

5335	1603774408.327962	172.18.24.108	172.18.24.254	ICMP
5336	1603774408.328871	172.18.24.254	172.18.24.108	ICMP
5455	1603774409.322967	172.18.24.108	172.18.24.254	ICMP
5456	1603774409.323703	172.18.24.254	172.18.24.108	ICMP
5545	1603774410.322928	172.18.24.108	172.18.24.254	ICMP
5546	1603774410.323644	172.18.24.254	172.18.24.108	ICMP
5726	1603774411.322898	172.18.24.108	172.18.24.254	ICMP
5727	1603774411.323610	172.18.24.254	172.18.24.108	ICMP

> Frame 5335: 1014 bytes on wire (8112 bits), 1014 bytes captured (8112 bits) on interface \Dev
> Ethernet II, Src: 0c:da:42:02:10:07 (0c:da:42:02:10:07), Dst: NewH3CTe_cb:60:88 (68:93:20:cb:60:88)
> Internet Protocol Version 4, Src: 172.18.24.108, Dst: 172.18.24.254
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1000
Identification: 0x7a49 (31305)
> Flags: 0x0000
Fragment offset: 0
Time to live: 128
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 172.18.24.108
Destination: 172.18.24.254
> Internet Control Message Protocol

0000	68 93 20 cb 60 88 0c da 42 02 10 07 08 00 45 00	h B E .
0010	03 e8 7a 49 00 00 80 01 00 00 ac 12 18 6c ac 12	. . z I l . .
0020	18 fe 08 00 3d 18 00 01 00 29 61 62 63 64 65 66	 =) a b c d e f
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	g h i j k l m n o p q r s t u v

配置关键点

- 1、偏移字节数需要根据实际报文来决定，例如报文携带有VLAN tag，则需要加4个字节，即偏移量为26。
- 2、TTL默认为255，80 ff则需要改为ff ff。