通过包过滤实现ICMP和TCP流量单通

ACL packet-filter **葛松炜** 2019-08-30 发表

组网及说明

不涉及

问题描述

需求是网段A可以访问网段B，但是网段B无法访问网段A，通过ACL包过滤实现。

过程分析

ICMP流量需要请求和回应来构成一个完整的访问过程，TCP流量也需要三次握手成功来建立连接，因此我们可以针对ICMP和TCP报文的特性，配置ACL来进行过滤，从而实现报文单通。UDP报文因不像ICMP和TCP有类似的特征，所以无法通过ACL包过滤进行流量阻断。

解决方法

例如，网段A（1.1.1.0/24）想要访问网段B（2.2.2.0/24），但是网段B （2.2.2.0/24） 无法访问网段A（1.1.1.0/24），可以通过如下配置分别实现ICMP和TCP流量单通：

acl advanced 3000

rule 0 deny icmp source 2.2.2.0 0.0.0.255 **icmp-type echo** //ICMP单通，阻断2.2.2.0/24网段发起的ICMP请求

rule 10 deny tcp source 2.2.2.0 0.0.0.255 **syn 1** //TCP单通，阻断2.2.2.0/24网段发起的TCP连接请求，TCP建立连接第一次请求时会发送SYN=1的位码

然后将这条ACL在VLAN接口下或设备物理接口下使用包过滤命令调用即可