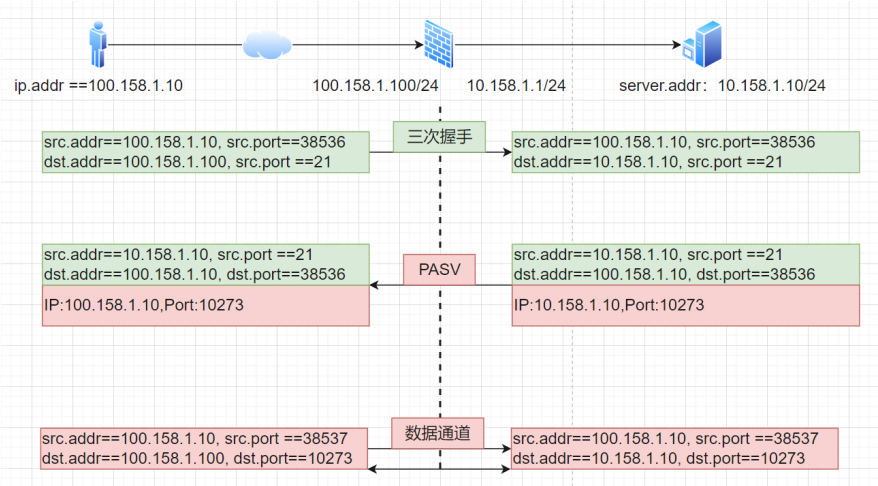
# 防火墙在FTP_PASV模式下的ALG处理

ACL NAT 孔凡安 2024-01-08 发表

## 组网及说明




## 配置步骤

FW主要配置如下，RAGG2.10为外网接口，RAGG1.10为内网接口。

```
#
interface Route-Aggregation2.10
 ip address 100.158.1.1 255.255.255.0
 nat server protocol tcp global 100.158.1.100 21 inside 10.158.1.10 21 rule ServerRul
e_1   ---配置针对内网服务器的静态映射
 vlan-type dot1q vid 10
#
interface Route-Aggregation1.10
 ip address 10.158.1.1 255.255.255.0
 vlan-type dot1q vid 10
#
```

原理解析：

PASV模式下RESPONSE报文触发建立关联表，防火墙 ALG模块对地址进行转换。

*Jan  8 16:43:49:856 2024 F5080D_1 NAT/7/ALG: -Chassis=1-Slot=2;

PACKET: (Route-Aggregation2.10) ALG payload was translated according to session table(Src-by-L3Head):

10.158.1.10/10273(VPN: 0) ---> 100.158.1.100/10273(VPN: 0) ----服务器私网地址被转化为公网映射地址

*Jan  8 16:43:49:857 2024 F5080D_1 SESSION/7/RELATION: -Chassis=1-Slot=2;

Tuple(EVENT): 100.158.1.10/0 -->100.158.1.100/10273(TCP(6))

Relation entry was backuped for fill info

*Jan  8 16:43:49:856 2024 F5080D_1 SESSION/7/RELATION: -Chassis=1-Slot=2;

**Tuple(EVENT): 100.158.1.10/0 -->100.158.1.100/10273(TCP(6))**

**Relation entry was created for module calling ----防火墙建立关联表**

*Jan  8 16:43:49:893 2024 F5080D_1 SESSION/7/RELATION: -Chassis=1-Slot=2;

Tuple(EVENT): 100.158.1.10/0 -->100.158.1.100/10273(TCP(6))

Relation entry was backuped for delete

## 配置关键点

FTP关联表一般通过disp session relation-table ipv4无法看到，关联表匹配一次就删除了。

可以通过debugging session relation-table看到对应过程。