# 过防火墙TFTP协议不通

ASPF 聂鹏 2021-10-12 发表

## 组网及说明

不涉及，普通组网

## 问题描述

过防火墙后TFTP不通，放全通策略或者放通双向策略后能通。

## 过程分析

debugging查看，发现首包正常放通，但是回包被丢弃。

*Oct  9 12:04:59:187 2021 HF-CORE-FW-ADMIN FILTER/7/PACKET: -COntext=12-Slot=2; The packet is permitted. Src-ZOne=Untrust, Dst-ZOne=Trust;If-In=Route-Aggregation10.1002(158), If-Out=Route-Aggregation10.1012(159); Packet Info:Src-IP=1.1.1.1, Dst-IP=1.1.1.2, VPN-Instance=,Src-Port=38611, Dst-Port=69, Protocol=UDP(17), Application=tftp(27), ObjectPolicy=Untrust->Trust, Rule-ID=31101.

*Oct  9 12:04:59:184 2021 HF-CORE-FW-ADMIN FILTER/7/PACKET: -COntext=12; The packet is denied. Src-ZOne=Trust, Dst-ZOne=Untrust;If-In=Route-Aggregation10.1012(159), If-Out=Route-Aggregation10.1002(158); Packet Info:Src-IP=1.1.1.2, Dst-IP=1.1.1.1, VPN-Instance=, Src-Port=46541, Dst-Port=38611, Protocol=UDP(17), Application=general_udp(2087), ACL=none, Rule-ID=none.

通过debugging可以看到，首包是38611端口发给69端口，回包服务器直接使用了一个46541端口回给38611端口。五元组变化，导致防火墙无法匹配会话导致。

## 解决方法

新建ASPF策略，开启tftp功能，防火墙默认只开启FTP，因此没有对tftp进行关联。

```
aspf policy 1
 detect ftp
 detect tftp
```

域间策略下调用。

```
zone-pair security source Untrust destination Trust
 aspf apply policy 1
```

这个故障原因是TFTP协议导致，TFTP协议基于UDP，控制通道端口是69，数据通道需要换端口，但是由于是UDP，所以不会进行协商通知，服务器是直接使用自己的空闲端口回复终端，就相当于告知终端用这个端口传输数据。而防火墙会话关联五元组，并且服务器是直接使用空闲端口回复，防火墙事先无法知晓使用什么端口，因此会话无法关联。必须在ASPF中专门打开TFTP功能才能进行创建关联会话。

而域间策略下的ASPF优先级低于安全策略，策略匹配后会进行域间策略下的ASPF检查，因此可以实现。