过防火墙TFTP传输数据为空

ALG FTP/TFTP 吴欣 2024-01-23 发表

组网及说明

不涉及，普通组网

问题描述

过防火墙使用TFTP，可以进行数据传输，tftp服务器中可以看到文件名称，但是打开是空白，无数据

过程分析

经过了解，绕过防火墙使用tftp服务即会出现该问题。
怀疑报文在防火墙上在丢弃，收集debug信息及诊断：
[FW]acl advanced 3XXX
[FW-acl-ipv4-adv-3010]rule 0 permit ip source X.X.X.X 0 destination Y.Y.Y.Y 0
[FW-acl-ipv4-adv-3010]rule 5 permit ip source Y.Y.Y.Y 0 destination X.X.X.X 0
[FW-acl-ipv4-adv-3010]rule 10 permit ip source A.A.A.A 0 destination Y.Y.Y.Y 0
[FW-acl-ipv4-adv-3010]rule 15 permit ip source Y.Y.Y.Y 0 destination A.A.A.A 0
由于设备过了nat，acl需要转换前与转化后都写
以安全策略security-policy为例，分别进行以下debug调试：
<FW>debugging ip packet acl 3XXX # 查看报文具体从哪个接口，哪个slot上来和发出的情况
<FW>debugging ip info acl 3XXX # 如果有丢包则会打印信息丢包的具体模块，如果没有丢包则不打印
<FW>debugging aspf packet acl 3XXX # 如果报文状态不合法，则会显示被aspf丢弃，需检查流量来回是否一致
<FW>debugging security-policy packet ip acl 3XXX # 如果是对象策略则用object-policy，如果是包过滤则用packet-filter
如果没有会话，但是debug有报文上来，还需要收集：
<FW>debugging session session-table all acl 3XXX # 可以查看会话被删除的具体情况

收集debug信息进行分析：
设备对同一个报文的转发无问题，没有报文被丢弃的记录，且转换也正确。

*Jan 4 17:34:14:290 2024 FW_NEXT_ZXX_YWtoOA IPFW/7/IPFW_PACKET: -COntext=1;
Receiving, interface = Vlan-interface18
version = 4, headlen = 20, tos = 0
pktlen = 64, pktid = 6045, offset = 0, ttl = 127, protocol = 17
checksum = 52160, s = 154.102.17.118, d = 154.102.18.13
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface Vlan-interface18.
Payload: UDP
 source port = 3347, destination port = 1988
 checksum = 0xb83e, length = 44.

*Jan 4 17:34:14:290 2024 FW_NEXT_ZXX_YWtoOA SESSION/7/TABLE: -COntext=1;
Tuple5(EVENT): 154.102.17.118/3347-->154.102.18.13/1988(UDP(17))
Session entry was created.
*Jan 4 17:34:14:290 2024 FW_NEXT_ZXX_YWtoOA SESSION/7/TABLE: -COntext=1;
Tuple5 (FSM): 154.102.17.118/3347-->154.102.18.13/1988(UDP(17))
FSM:NONE-->UDP_OPEN, dir:ORIGIN, PacketType:GENERAL(0)
*Jan 4 17:34:14:290 2024 FW_NEXT_ZXX_YWtoOA IPFW/7/IPFW_PACKET: -COntext=1;
Sending, interface = Vlan-interface999
version = 4, headlen = 20, tos = 0
pktlen = 64, pktid = 6045, offset = 0, ttl = 126, protocol = 17
checksum = 17315, s = 10.10.102.232, d = 10.10.102.113
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface Vlan-interface18 at interface Vlan-interface 999.

Payload: UDP

source port = 3347, destination port = 1988

checksum = 0x2f21, length = 44.

后续了解到：

通常情况下，NAT只对报文头中的IP地址和端口信息进行转换，不对应用层数据载荷中的字段进行分析。然而一些特殊协议，它们报文的数据载荷中可能包含IP地址或端口信息，这些内容不能被NAT进行有效的转换，就可能导致问题

解决方法

开启 TFTP的ALG功能。

[FW]nat alg TFTP