某局点IPsec正常建立，语音业务单通典型分析

ALG NAT IPSec VPN 孔凡安 2022-07-05 发表

组网及说明

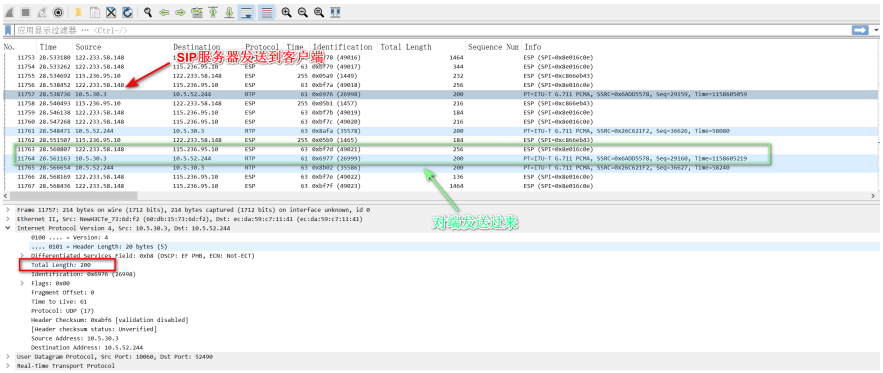
SIP服务器（10.5.52.244）---防火墙----------对端公网设备---客户端（10.5.30.3）

问题描述

客户端向SIP服务器发起访问，电话能正常接起来，但是客户端侧听不到声音，SIP服务器侧可以听到客户端的声音。

过程分析

通过在防火墙上看IPsec隧道已经正常建立，在防火墙上抓取内网侧交互以及封装后的流量看，SIP服务器有回应客户端的RTP数据流，但是并没有做IPsec封装出去。



通过在防火墙上debug进一步探究报文未做IPsec封装的原因，显示如下：

*Jul 3 17:46:05:429 2022 SecPath F1000-AK135 IPFW/7/IPFW_PACKET: -COntext=1;
Receiving, interface = GigabitEthernet1/0/6
version = 4, headlen = 20, tos = 0
pktlen = 200, pktid = 2601, offset = 0, ttl = 63, protocol = 17
checksum = 51707, s = 10.5.52.244, d = 10.5.30.3
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/6.
Payload: UDP
source port = 56822, destination port = 10062
checksum = 0x06b0, length = 180.

*Jul 3 17:46:05:429 2022 SecPath F1000-AK135 SESSION/7/TABLE: -COntext=1;
Tuple5(EVENT): 10.5.52.244/56822-->10.5.30.3/10062(UDP(17))
Session entry was created.
*Jul 3 17:46:05:429 2022 SecPath F1000-AK135 FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne=Trust, Dst-ZOne=Untrust;If-In=GigabitEthernet1/0/6(7), If-Out=GigabitEthernet1/0/4(5); Packet Info:Src-IP=10.5.52.244, Dst-IP=10.5.30.3, VPN-Instance=, Src-MacAddr=ecda-59c7-1141,Src-Port=56822, Dst-Port=10062, Protocol=UDP(17), Application=general_udp(2087), SecurityPolicy=3, Rule-ID=2.

*Jul 3 17:46:05:571 2022 SecPath F1000-AK135 SESSION/7/TABLE: -COntext=1;
Tuple5(EVENT): 10.5.50.53/58916-->58.212.179.148/443(UDP(17)) ICMP_ERROR INTERNAL MATCHED
*Jul 3 17:46:05:625 2022 SecPath F1000-AK135 IPFW/7/IPFW_PACKET: -COntext=1;
Receiving, interface = GigabitEthernet1/0/4
version = 4, headlen = 20, tos = 184
pktlen = 200, pktid = 28660, offset = 0, ttl = 63, protocol = 17
checksum = 41848, s = 10.5.30.3, d = 10.5.52.244
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/4.
Payload: UDP
source port = 10062, destination port = 56822
checksum = 0x7af7, length = 180.

*Jul 3 17:46:05:625 2022 SecPath F1000-AK135 SESSION/7/TABLE: -COntext=1;
Tuple5(EVENT): 10.5.30.3/10062-->10.5.52.244/56822(UDP(17))
Session entry was created.
*Jul 3 17:46:05:625 2022 SecPath F1000-AK135 FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne=Untrust, Dst-ZOne=Trust;If-In=GigabitEthernet1/0/4(5), If-Out=GigabitEthernet1/0/6(7); Packet Info:Src-IP=10.5.30.3, Dst-IP=10.5.52.244, VPN-Instance=, Src

-MacAddr=cccc-81c2-b239,Src-Port=10062, Dst-Port=56822, Protocol=UDP(17), Application=general_udp(2087), SecurityPolicy=5, Rule-ID=4.

*Jul 3 17:46:05:625 2022 SecPath F1000-AK135 IPFW/7/IPFW_PACKET: -COntext=1; Sending, interface = GigabitEthernet1/0/6
version = 4, headlen = 20, tos = 184
pktlen = 200, pktid = 26660, offset = 0, ttl = 62, protocol = 17
checksum = 42104, s = 10.5.30.3, d = 10.5.52.244
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet1/0/4 at interface GigabitEthernet1/0/6:
Payload: UDP
source port = 10062, destination port = 56822
checksum = 0x7a17, length = 180.

*Jul 3 17:46:05:625 2022 SecPath F1000-AK135 SESSION/7/TABLE: -COntext=1; Tuple5(EVENT): 10.5.30.3/10062-->10.5.52.244/56822(UDP(17))
Session entry was Add Hash failed.

分析原因为：RTP数据流由SIP服务器先发起，匹配到反向的nat server，转换了源地址，没有走IPsec封装。
导致反向的RTP会话冲突被丢弃。

解决方法

将nat server的配置加以进行限制，deny掉源地址为10.5.30.3的数据流量。

acl advanced 3220
rule 5 deny ip
nat server protocol udp global current-interface 6060 inside 10.5.52.244 6060 acl 3220 reversible