某据点M9000建立IPSEC VPN，两阶段都有，但是内网不通

IPSec VPN　L2TP over IPSec VP　孔德飞　2023-09-26 发表

组网及说明

组网如下

内网终端----M9000----公网------对端公网设备----对端VPN设备

告警信息

暂不涉及

问题描述

问题描述:
两台M9000冗余主备，只有冗余组备份组没有冗余口
目前虚墙跨VPN实例与对端云桌面建立IPSEC
外网口
interface Route-Aggregation1
description external
ip binding vpn-instance external_vpn
ip address 10.0.9.7 255.255.255.0

内外口
interface Route-Aggregation2.1013
description SDN_SUBIF_Route-Aggregation2.1013
ip binding vpn-instance 6vo2is9s3v9c7rqf1oqrgq9jcg
ip address 10.0.12.14 255.255.252.0
vlan-type dot1q vid 1013
#

检查了一下现场配置，配置没有问题（**我之前模拟器做过实验，确认现场配置没问题**）
IPSEC配置如下
ipsec transform-set jiuyuan
esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha256
 pfs dh-group2
#
ipsec policy jiuyuan-policy 10 isakmp
transform-set jiuyuan
 security acl 3100
 local-address 124.166.230.117
remote-address 36.134.77.16
ike-profile jiuyuan
#
ike profile jiuyuan
keychain jiuyuan
local-identity address 124.166.230.117
match remote identity address 36.134.77.16 255.255.255.255 vpn-instance **external_vpn**
proposal 2
 inside-vpn vpn-instance **6vo2is9s3v9c7rqf1oqrgq9jcg**
#
ike proposal 2
encryption-algorithm aes-cbc-256
dh group2
authentication-algorithm sha256
#
ike keychain jiuyuan vpn-instance **external_vpn**
pre-shared-key address 36.134.77.16 255.255.255.255 key cipher c3$rHS3ZKmgb38M/74WR0ME
Z6d8I82J719+cylvD/zaBSM=

现场的IKE SA insideVPN是错误的，并且profile为空
<H3C>dis ike sa v
<H3C>dis ike sa verbose

  Connection ID: 10
  Outside VPN: external_vpn
  Inside VPN: external_vpn

Profile:
Transmitting entity: Responder
Initiator COOKIE: 4e0794f2a1aeb252
Responder COOKIE: 5b38ab1482db714d
Local IP: 124.166.230.117
Local ID type: IPV4_ADDR
Local ID: 124.166.230.117

Connection ID: 10
Outside VPN: external_vpn
Inside VPN:
Profile:
Transmitting entity: Responder
Initiator COOKIE: 4e0794f2a1aeb252
Responder COOKIE: 5b38ab1482db714d

Local IP: 124.166.230.117
Local ID type: IPV4_ADDR
Local ID: 124.166.230.117
Remote IP: 36.134.77.16
Remote ID type: IPV4_ADDR
Remote ID: 10.254.96.141
Encapsulation mode: tunnel
Perfect Forward Secrecy: dh-group2
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Path MTU: 1416
Tunnel:
local address: 124.166.230.117

过程分析

问题分析

经过分析IP：发现本端A8000是作为响应方的，IKE作为响应方的时候，ike profie中的match remote identity必须配置为对端的IKE local identity

<H3C>dis ike sa verbose

Connection ID: 10

Outside VPN: external_vpn

Inside VPN:

Profile:

Transmitting entity: Responder

Initiator COOKIE: 4e0794f2a1aeb252

Responder COOKIE: 5b38ab1482db714d

Local IP: 124.166.230.117

Local ID type: IPV4_ADDR

Local ID: 124.166.230.117

Remote IP: 36.134.77.16

Remote ID type: IPV4_ADDR

Remote ID: 10.254.96.141

Encapsulation mode: tunnel

Perfect Forward Secrecy: dh-group2

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1416

Tunnel:

local address: 124.166.230.117

现场的IPSEC SA的Inside VPN是空的

<H3C>display ipsec sa

Interface: Route-Aggregation1

IPsec policy: luyuan_policy

Sequence number: 10

Mode: ISAKMP

Flow table status: Active

Tunnel id: 1

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1416

Tunnel:

local address: 124.166.230.117

Authentication method: PRE-SHARED-KEY Local ID: 124.166.230.117

正常情况下IKE SA与IPSEC SA应该是下面的样子

<H3C>dis ike sa verbose

Connection ID: 1

Outside VPN: test

Inside VPN: test1

Profile: profile1

<H3C>display ips

<H3C>display ipsec sa

Interface: GigabitEthernet1/0/1

IPsec policy: policy1

Sequence number: 1

Mode: ISAKMP

Tunnel id: 0

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN: test1

debug是被IPSEC模块丢弃，我分析是因为IKE SA与IPSEC SA虽然建立了，但是建立错误有关

[H3C]dis acl 3888

Advanced IPv4 ACL 3888, 2 rules,

ACL's step is 5

rule 0 permit ip vpn-instance 6vo2is9s3v9c7rqf1oqrgq9jcg source 192.168.200.226 0 destination 172.16.3.15 0 (9571 times matched)

解决方法

debug ip packet transmit ip vpn-instance 6vo2is9s3v9c7rqf1oqrgq9jcg source 172.16.3.15 0 destination 192.168.200.226 0

解决方案：

将本端ike profile中的match remote identity地址改为10.254.96.141之后，查看ike sa与ipsec sa之后，恢复正常

*Sep 26 00:43:19:248 2023 H3C SESSION/7/TABLE: -COntext=8;
Tuple5(EVENT): 192.168.200.226/15627-->172.16.3.15/2048(ICMP(1))
Session entry was created.
*Sep 26 00:43:19:248 2023 H3C SESSION/7/TABLE: -COntext=8;
Tuple5 (FSM): 192.168.200.226/15627-->172.16.3.15/2048(ICMP(1))
FSM:NONE-->ICMP_REQUEST, dir:ORIGIN, PacketType:REQUEST(8)
*Sep 26 00:43:19:248 2023 H3C SESSION/7/TABLE: -COntext=8;
Tuple5(EVENT): 192.168.200.226/15627-->172.16.3.15/2048(ICMP(1))
Session entry was deleted.
*Sep 26 00:43:19:248 2023 H3C IPFW/7/IPFW_INFO: -COntext=8;
MBUF was intercepted! Phase Num is 8(post routing beforefrag), **Service ID is 26(ipsec), Bitmap is 2000000000, return 1**(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is Route-Aggregation1, s= 192.168.200.226, d= 172.16.3.15, protocol= 1, pktid = 40684.
*Sep 26 00:43:20:248 2023 H3C IPFW/7/IPFW_PACKET: -COntext=8;
Receiving interface = Route-Aggregation2.1013
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 41537, offset = 0, ttl = 63, protocol = 1
checksum = 24765, s = 192.168.200.226, d = 172.16.3.15
channelID = 0, vpn-InstanceIn = 1, vpn-InstanceOut = 1.
prompt: Receiving IP packet from interface Route-Aggregation2.1013.
Payload: ICMP
type = 8, code = 0, checksum = 0x82c9.

ike profile jiuyuan
keychain jiuyuan
local-identity address 124.166.230.117
match remote identity address **10.254.96.141** 255.255.255.255 vpn-instance **external_vpn**
proposal 2
inside-vpn vpn-instance **6vo2is9s3v9c7rqf1oqrgq9jcg**

<H3C>display ike sa verbose
Connection ID: 35
Outside VPN: external_vpn
Inside VPN: 6vo2is9s3v9c7rqf1oqrgq9jcg
Profile: jiuyuan
Transmitting entity: Responder
Initiator COOKIE: c38ecfef1c2107e1
Responder COOKIE: 456d6a90fc000fd5
Local IP: 124.166.230.117
Local ID type: IPV4_ADDR
Local ID: 124.166.230.117
Remote IP: 36.134.77.16
Remote ID type: IPV4_ADDR
Remote ID: 10.254.96.141

<H3C>display ipsec sa
Interface: Route-Aggregation1
IPsec policy: jiuyuan-policy
Sequence number: 10
Mode: ISAKMP
Flow table status: Active
Tunnel id: 2
Encapsulation mode: tunnel
Perfect Forward Secrecy: dh-group2
Inside VPN: 6vo2is9s3v9c7rqf1oqrgq9jcg

实验室验证如下

组网拓扑 F1090 11.11.11.1----11.11.11.2 vpn:kdf M9000 vpn:management 172.31.0.17----172.31.0.22 F5020 loopback10.0.0.1

M9000与F5020建立IPSEC，感兴趣流为11.11.11.1-----10.0.0.1

ipsec一阶段的 IKE SA的协商与二阶段的IPSEC的SA协商本质上是连个独立的过程

如果作为发起方，第一个上来的感兴趣流报文，会去查路由，找到应用IPSEC的出接口，然后去匹配IPSEC POLICY下的源目ip发送IKE协商报文，此时即使是错误的配置（本端的ike profile的remote与对端的local identity不匹配），本端触发对端，也会协商出IKE SA与IPSEC SA，
并且流量是通的

本端 ike profile配置如下（远端是172.31.0.2）

ike profile test
keychain test
local-identity address 172.31.0.17
match remote identity address 172.31.0.22 255.255.255.255 vpn-instance management
proposal 1
inside-vpn vpn-instance kdf