

MSR设备 V7 实现ipsec野蛮模式穿越NAT组网

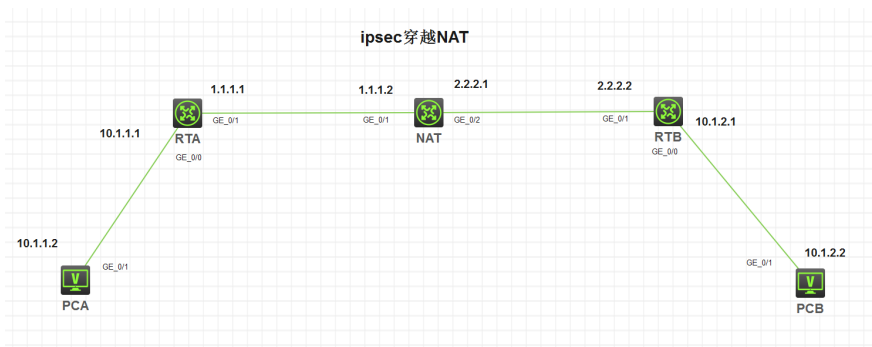
IPSec VPN

NAT

苏清秀

2020-02-20 发表

组网及说明



问题描述

MSR设备在ipsec野蛮模式穿越NAT的组网环境中，只有当发起方持久的ping响应方的时候，响应方向发起方发送业务流量是可以发送的，发起方停止后，即使是在ipsec隧道正常建立的情况下，响应方也不能给发送方发送业务流量。

过程分析

实验结果显示：

(1) 能正常看到NAT会话。NAT源地址能够正常的转换。换言之，PCA将s10.1.1.0 d10.1.2.0的报文，发送给RTA，因为在RTA与RTB之间建立ipsec隧道，所以，RTA上将报文进行封装，封装成s1.1.1.1 d2.2.2.2的报文，经NAT设备发送给RTB，而NAT设备会将报文的源地址进行转换成s2.2.2.1 d2.2.2.2，发送给RTB，在RTB上进行解封装，再发送给PCB。同样的流程，回程的报文也是这样的。在下图中还可以看到报文的类型是UDP_READY，查询NAT session的老化时间，对应该协议报文的老化时间默认的是60s。

```
[NAT]dis nat session verbose
Slot 0:
Initiator:
  Source      IP/port: 1.1.1.1/4500
  Destination IP/port: 2.2.2.2/4500
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: GigabitEthernet0/1
Responder:
  Source      IP/port: 2.2.2.2/4500
  Destination IP/port: 2.2.2.1/1026
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: GigabitEthernet0/2
State: UDP_READY
Application: OTHER
Role: -
Failover group ID: -
Start time: 2020-01-16 12:34:20    TTL: 54s
Initiator->Responder:            0 packets        0 bytes
Responder->Initiator:            0 packets        0 bytes
Total sessions found: 1
```

(2) ike sa和ipsec sa能够正常建立。实验是当发起方发起请求，触发隧道正常建立之后，发现NAT会话没有老化过，一直存在，这样的话，隧道只要是正常建立的时候，由响应方向发起方发送业务流量，就能正常发送。因此，在RTA上抓包发现，在正常的ipsec报文交互完成之后，有周期性的NAT-Keepalive报文，由RTA周期性的发送给RTB。

2060	15478.611281	2.2.2.2	1.1.1.1	ESP	158 ESP (SPI=0x70c01a95)
2061	15478.621089	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II
2062	15480.432705	58:03:e3:20:02:04	Broadcast	0xb003	22 Ethernet II
2063	15480.712082	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II
2064	15482.487805	58:03:e3:20:02:04	Broadcast	0xb003	22 Ethernet II
2065	15482.804128	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II
2066	15484.527127	58:03:e3:20:02:04	Broadcast	0xb003	22 Ethernet II
2067	15484.885154	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II
2068	15486.578250	58:03:e3:20:02:04	Broadcast	0xb003	22 Ethernet II
2069	15486.978531	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II
2070	15488.618255	58:03:e3:20:02:04	Broadcast	0xb003	22 Ethernet II
2071	15489.061655	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II
2072	15490.649685	58:03:e3:20:02:04	Broadcast	0xb003	22 Ethernet II
2073	15491.140586	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II
2074	15492.693432	58:03:e3:20:02:04	Broadcast	0xb003	22 Ethernet II
2075	15493.220541	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II
2076	15494.738284	58:03:e3:20:02:04	Broadcast	0xb003	22 Ethernet II
2077	15495.299577	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II
2078	15496.778256	58:03:e3:20:02:04	Broadcast	0xb003	22 Ethernet II
2079	15497.375734	1.1.1.1	2.2.2.2	UDPENCAP	43 NAT-keepalive
2080	15497.415985	58:03:d7:2e:01:04	Broadcast	0xb003	22 Ethernet II

(3) 没有配置任何的保活机制，ipsec的keepalive 和dpd默认是没有开启功能的。所以查询命令手册发现：

ike nat-keepalive 命令用来配置向对端发送 nat-keepalive 报文的时间间隔。

undo ike nat-keepalive 命令用来恢复缺省情况。

【命令】

ike nat-keepalive seconds

undo ike nat-keepalive

【缺省情况】

向对端发送 nat-keepalive 报文的时间间隔为20秒。//显然是小于NAT session老化时间60s的

【参数】

seconds：指定向对端发送 nat-keepalive 报文的时间间隔，取值范围为5~300，单位为秒。

【使用指导】

该命令仅对位于 nat 之后的设备（即该设备位于 nat 设备连接的私网侧）有意义。nat 之后的IKE网关设备需要定时向 nat 之外的IKE网关设备发送 nat-keepalive 报文，以便维持 nat 设备上对应的IPsec流量的会话存活，从而让 nat 之外的设备可以访问 nat 之后的设备。

也就是说野蛮模式情况下，我的发起方，需要向响应方定时的发送NAT-Keepalive报文，使得NAT会话表项一直存在，这样的话，就使得响应方向发起方发送业务报文的时候，不会因为NAT会话表项老化后，不能发送报文了。又因为我用的是EasyIP的NAT配置，所以NAT会话表项只能是有私网侧先发起流量触发建立。

另外，建议 nat-keepalive 报文的时间间隔小于NAT会话的老化时间，这样才有效。

【举例】

配置向对端发送 nat-keepalive 报文的时间间隔为5秒。

<Sysname> system-view

[Sysname] ike nat-keepalive 5

初步怀疑是NAT会话表项老化，导致的隧道正常建立的情况下，响应方都无法ping通发起方。

解决方法

解决方案（以现场情况为准）：

(1) 建议检查一下NAT设备或者中间链路是否有防火墙？

(2) MSR设备是做响应方的角色，对端发起方角色的设备非我司，建议排查一下友商设备是否有像我司设备这样的NAT默认的保活机制，能够保证在隧道正常建立的时候，NAT会话不老化的。

设备相关配置如下：

##各设备的IP地址，接口的IP地址，配置省略。

RTA：

#sys

ip route-static 2.2.2.0 24 1.1.1.2

ip route-static 10.1.2.0 24 1.1.1.2

acl advanced 3000

rule 0 permit ip source 10.1.1.0 0.0.0.255 dest 10.1.2.0 0.0.0.255

qu

ipsec transform-set t1

enca-mode tunnel

protocol esp

esp encry 3des-cbc

esp authen md5

qu

ike keychain k1

pre-shared-key address 2.2.2.2 24 key simple h3c

qu

ike profile p1

keychain k1

exchange-mode aggressive

local-identity fqdn rta

match remote identity address 2.2.2.2 24

```

qu
ipsec policy m1 1 isakmp
    security acl 3000
    transform-set t1
    ike-profile p1
    remote-add 2.2.2.2
qu
int g 0/1
    ipsec apply policy m1
qu
NAT设备配置:
sys
acl advanced 3000
    rule 0 permit ip source 1.1.1.1 0
qu
int g 0/2
    nat outbound 3000
RTB:
sys
ip route-static 1.1.1.0 24 2.2.2.1
ip route-static 10.1.1.0 24 2.2.2.1
acl advanced 3000
    rule 0 permit ip source 10.1.2.0 0.0.0.255 dest 10.1.2.0 0.0.0.255
qu
ipsec transform-set t1
    encr-mode tunnel
    protocol esp
    esp encr 3des-cbc
    esp authn md5quike keychain k1
    pre-shared-key address 2.2.2.1 24 key simple h3c
qu
ike profile p1
    keychain k1
    exchange-mode aggressive
    local-identity address 2.2.2.2
    match remote identity fqdn rta
qu
ipsec policy-template tem1 1
    security acl 3000
    ike-profile p1
    transform-set t1
    local-address 2.2.2.2 // 这边要注意的是如果是主模式的话，这里使用的是直接配置策略的形式，所以要加remote-address 2.2.2.1，也就是NAT转换后的地址
ipsec policy n1 1 isakm
p template tem1
int g 0/1    ipsec apply policy n1
qu

```

附件下载: 拓扑图和结果表项图.rar