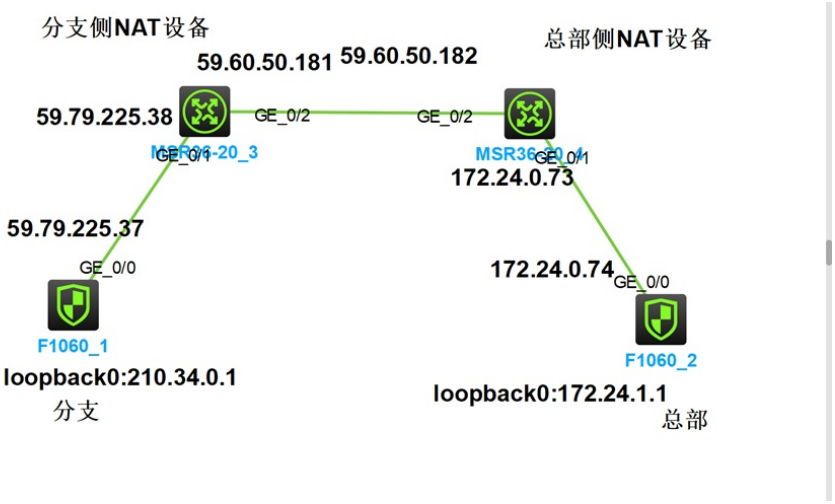
某局点ipsec隧道存在但是内网不定时不通

IPSec VPN 孔德飞 2024-04-25 发表

组网及说明

组网如下：

分支与总部建立IPSEC，并且分支与总部外侧都有NAT设备（并且分支侧NAT设备是光猫，一旦重启，公网IP地址会变化），分支侧IPSEC非模板，FQDN的方式，总部IPSEC模板方式，分支侧的NAT设备要做NAT outbound，总部的的NAT设备要做nat server,59.60.50.182 到172.24.1.1 500到500 4500到4500的映射



告警信息

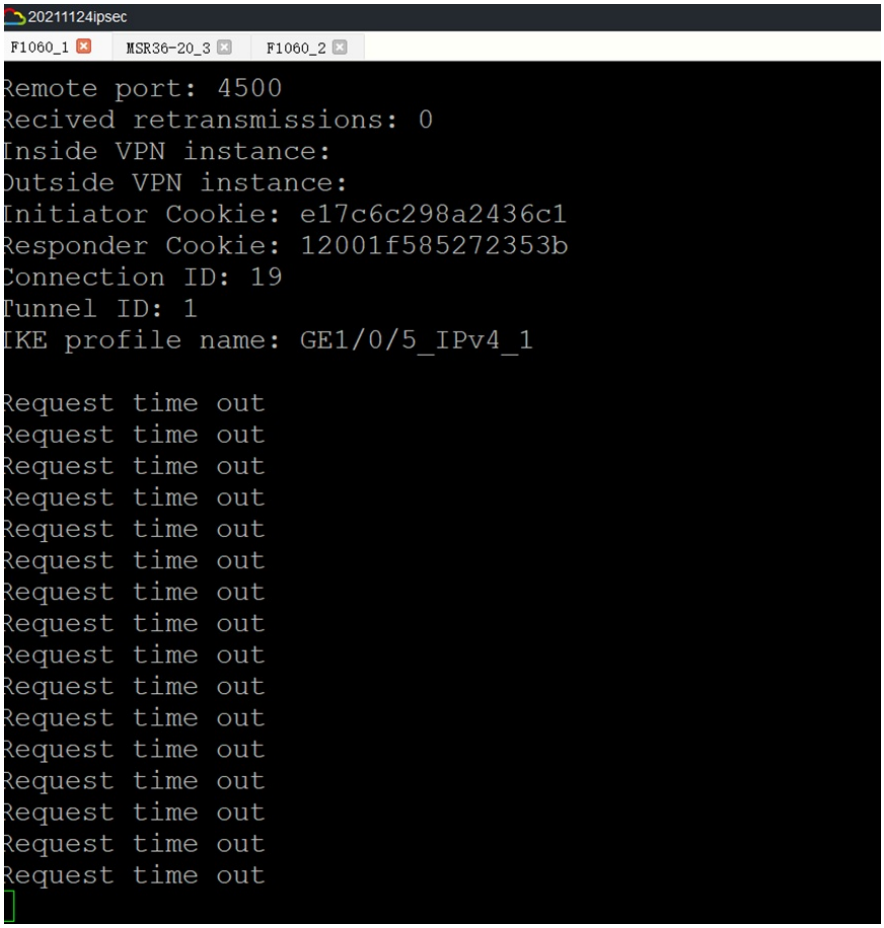
不涉及

问题描述

问题现象：

现场的现象是分支与总部的IPSEC隧道存在，但是内网不定时不通

如下分支内网ping不通总部内网



过程分析

问题排查过程

不通的时候，总部打开

调试开关，前提是全局视图下开启了如下命令：

ipsec logging packet enable

ipsec sa global-duration time-based 8000

ipsec logging negotiation enable

<H3C>terminal debugging

<H3C>terminal monitor

总部可以看到如下报错，可以看到因为源地址匹配不了ipsec sa

%Apr 25 10:11:13:090 2024 H3C IPSEC/6/log: -COntext=1;

IPsec packet discarded, Src IP:59.60.50.183, Dst IP:172.24.0.74, SPI:1840039316, SN:319, Cause:Source address of packet does not match the SA.

查看总部侧IPSEC SA，远端地址是59.60.50.181，进一步排查，发现分支测的NAT设备光猫地址发生了变化。

<H3C>display ipsec sa

Interface: GigabitEthernet1/0/0

IPsec policy: 1

Sequence number: 1

Mode: Template

Tunnel id: 0

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Transmitting entity: Responder

Path MTU: 1420
Tunnel:
local address: 172.24.0.74
remote address: 59.60.50.181
Flow:
sour addr: 172.24.1.0/255.255.255.0 port: 0 protocol: ip
dest addr: 210.34.0.0/255.255.0.0 port: 0 protocol: ip

[Inbound ESP SAs]
SPI: 1840039316 (0x6dacc594)
Connection ID: 4294967296
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843184/2633
Max received sequence-number: 169
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: Y
Status: Active

[Outbound ESP SAs]
SPI: 3266419510 (0xc2b19b36)
Connection ID: 12884901889
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843184/2633
Max sent sequence-number: 169
UDP encapsulation used for NAT traversal: Y
Status: Active

解决方法

解决方案：

对于此种场景，分支与总部要分别配置dpd检测

ike dpd interval 3 retry 2 periodic

配置完成之后，当分支侧光猫地址发生变化（模拟59.60.50.181变为59.60.50.183），总部侧的IPSEC SA可以重协商，分支侧ping包丢8个包左右

分支侧ping包

56 bytes from 172.24.1.1: icmp_seq=74 ttl=255 time=1.136 ms
56 bytes from 172.24.1.1: icmp_seq=75 ttl=255 time=1.098 ms
56 bytes from 172.24.1.1: icmp_seq=76 ttl=255 time=1.350 ms
56 bytes from 172.24.1.1: icmp_seq=77 ttl=255 time=1.138 ms
56 bytes from 172.24.1.1: icmp_seq=78 ttl=255 time=1.454 ms
56 bytes from 172.24.1.1: icmp_seq=79 ttl=255 time=1.287 ms
56 bytes from 172.24.1.1: icmp_seq=80 ttl=255 time=1.477 ms
56 bytes from 172.24.1.1: icmp_seq=81 ttl=255 time=1.381 ms
56 bytes from 172.24.1.1: icmp_seq=82 ttl=255 time=1.028 ms
56 bytes from 172.24.1.1: icmp_seq=83 ttl=255 time=1.386 ms
56 bytes from 172.24.1.1: icmp_seq=84 ttl=255 time=1.043 ms
56 bytes from 172.24.1.1: icmp_seq=85 ttl=255 time=1.795 ms
56 bytes from 172.24.1.1: icmp_seq=86 ttl=255 time=1.450 ms
56 bytes from 172.24.1.1: icmp_seq=87 ttl=255 time=0.770 ms
56 bytes from 172.24.1.1: icmp_seq=88 ttl=255 time=1.277 ms
56 bytes from 172.24.1.1: icmp_seq=89 ttl=255 time=0.787 ms
56 bytes from 172.24.1.1: icmp_seq=90 ttl=255 time=1.229 ms
56 bytes from 172.24.1.1: icmp_seq=91 ttl=255 time=1.178 ms
Request time out
Request time out
Request time out

Request time out
Request time out
Request time out
Request time out
Request time out
56 bytes from 172.24.1.1: icmp_seq=100 ttl=255 time=1.225 ms
56 bytes from 172.24.1.1: icmp_seq=101 ttl=255 time=1.245 ms
56 bytes from 172.24.1.1: icmp_seq=102 ttl=255 time=1.060 ms
56 bytes from 172.24.1.1: icmp_seq=103 ttl=255 time=1.102 ms
56 bytes from 172.24.1.1: icmp_seq=104 ttl=255 time=0.507 ms

总部侧IPSEC SA

<H3C>display ipsec sa

Interface: GigabitEthernet1/0/0

IPsec policy: 1
Sequence number: 1
Mode: Template

Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Transmitting entity: Responder
Path MTU: 1420
Tunnel:
local address: 172.24.0.74
remote address: 59.60.50.181
Flow:
sour addr: 172.24.1.0/255.255.255.0 port: 0 protocol: ip
dest addr: 210.34.0.0/255.255.0.0 port: 0 protocol: ip

[Inbound ESP SAs]
SPI: 3177502326 (0xbd64d676)
Connection ID: 30064771072
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843196/3578
Max received sequence-number: 33
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: Y
Status: Active

[Outbound ESP SAs]
SPI: 987129310 (0x3ad665de)
Connection ID: 38654705665
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843196/3578
Max sent sequence-number: 33
UDP encapsulation used for NAT traversal: Y
Status: Active
<H3C>display ipsec sa
<H3C>display ipsec sa

Interface: GigabitEthernet1/0/0

IPsec policy: 1
Sequence number: 1
Mode: Template

Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Transmitting entity: Responder
Path MTU: 1420
Tunnel:
local address: 172.24.0.74
remote address: 59.60.50.183
Flow:
sour addr: 172.24.1.0/255.255.255.0 port: 0 protocol: ip
dest addr: 210.34.0.0/255.255.0.0 port: 0 protocol: ip

当总部与多分支建立IPSEC的时候，总部要用模板，分支要用FQDN，如果分支测的地址不断变化，还要配置DPD检测，模式使用野蛮模式，并且IKE SA与IPSEC SA老化时间保持默认的24H与1H，即不对IKE 与IPSC SA老化时间做任何配置。
标准配置如下：
分支侧关键配置如下：

配置DPD检测，建议配置周期检测，以便可以及时检测远端地址是否存活，如下配置的意思是，ipsec sa协商出3秒之后，发起DPD报文检测，每2秒发一次，如果5次收不到回应，就认为对端异常，删除IKE SA与ISPEC S

ike dpd interval 3 retry 2 periodic

配置fqdn
ike identity fqdn fenzhi

开启ipsec日志
ipsec logging negotiation enable
ipsec logging packet enable

配置ike profile,除了ip地址不一样，其余照着如下配置
ike profile ge1/0/5_ipv4_1
keychain GE1/0/5_IPv4_1
exchange-mode aggressive
match remote identity address 172.24.0.74 255.255.255.255
proposal 1

配置ike proposal
ike proposal 1
encryption-algorithm 3des-cbc
authentication-algorithm sha256

配置ike keychain

```
ike keychain GE1/0/5_IPv4_1
 pre-shared-key address 59.60.50.182 255.255.255.255 key simple 123
```

配置感兴趣流

```
acl advanced name IPsec_GE1/0/5_IPv4_1
 rule 1 permit ip source 210.34.0.0 0.0.255.255 destination 172.24.1.0 0.0.0.255
```

配置ipsec 提议

```
ipsec transform-set GE1/0/5_IPv4_1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
```

配置ipsec策略

```
ipsec policy GE1/0/5 1 isakmp
 transform-set GE1/0/5_IPv4_1
 security acl name IPsec_GE1/0/5_IPv4_1
 local-address 59.79.225.37
 remote-address 59.60.50.182
 ike-profile GE1/0/5_IPv4_1
```

接口应用ipsec策略

```
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip address 59.79.225.37 255.255.255.0
 ipsec apply policy GE1/0/5
```

总部侧关键配置如下

配置DPD检测，建议配置周期检测，以便可以及时检测远端地址是否存活，如下配置的意思是，ipsec sa协商出3秒之后，发起DPD报文检测，每2秒发一次，如果5次收不到回应，就认为对端异常，删除IKE SA与ISPEC S

```
ike dpd interval 3 retry 2 periodic
```

开启ipsec日志

```
ipsec logging negotiation enable
ipsec logging packet  enable
```

配置ike profile,除了ip地址不一样，其余照着如下配置

Match remote要用分支的fqdn

```
ike profile 1_ipv4_1
 keychain 1_IPv4_1
 exchange-mode aggressive
 local-identity address 172.24.0.74
 match remote identity fqdn fenzhi
 proposal 1
```

配置ike proposal

```
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm sha256
```

配置ike keychain，要用hostname，名字要使用分支的FQDN名字

```
ike keychain 1_IPv4_1
 pre-shared-key hostname fenzhi key simple 123
```

配置ipsec 提议

```
ipsec transform-set 1_IPv4_1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
```

配置ipsec模板以及以模板的方式创建IPSEC策略

```
ipsec policy-template test 1
 transform-set 1_IPv4_1
 local-address 172.24.0.74
 ike-profile 1_ipv4_1

ipsec policy 1 1 isakmp template test
```

接口应用ipsec策略

```
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip address 172.24.0.74 255.255.255.0
 ipsec apply policy 1
```