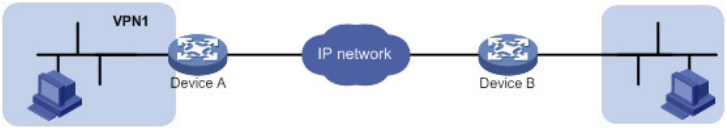
SecPath M9006 与对端ZX设备ipsec建立不成功问题处理经验案例

IPSec VPN 关萌 2018-06-24 发表

组网及说明

组网如下图



问题描述

客户使用我司M9000设备与ZX友商设备对接IPSec，对接后发现设备IPSec SA无法正常建立，M9000配置如下

```
#
 version 7.1.054, Release 9115P14
#
 sysname LQ_DTTE_center_FW
#
context Admin id 1
#
ip vpn-instance DX
 route-distinguisher 1:1
 vpn-target 1:1 import-extcommunity
 vpn-target 1:1 export-extcommunity
#
ip vpn-instance LT
 route-distinguisher 2:2
 vpn-target 2:2 import-extcommunity
 vpn-target 2:2 export-extcommunity
#
ip vpn-instance management
 route-distinguisher 1000000000:1
 vpn-target 1000000000:1 import-extcommunity
 vpn-target 1000000000:1 export-extcommunity
#
 telnet server enable
#
 security-zone intra-zone default permit
#
 system-working-mode standard
 password-recovery enable
#
vlan 1
#
interface NULL0
#
interface LoopBack0
#
interface LoopBack1
 ip binding vpn-instance DX
 ip address 192.168.2.1 255.255.255.255
#
interface GigabitEthernet3/0/1
 port link-mode route
 ip binding vpn-instance DX
 ip address 192.168.10.1 255.255.255.0
#
interface GigabitEthernet3/0/2
 port link-mode route
#
```

```
interface GigabitEthernet3/0/3
 port link-mode route
#
interface GigabitEthernet3/0/4
 port link-mode route
#
interface GigabitEthernet3/0/5
 port link-mode route
#
interface GigabitEthernet3/0/6
 port link-mode route
#
interface GigabitEthernet3/0/7
 port link-mode route
#
interface GigabitEthernet3/0/8
 port link-mode route
#
interface GigabitEthernet3/0/9
 port link-mode route
#
interface GigabitEthernet3/0/10
 port link-mode route
#
interface GigabitEthernet3/0/11
 port link-mode route
#
interface GigabitEthernet3/0/12
 port link-mode route
#
interface GigabitEthernet3/0/13
 port link-mode route
#
interface GigabitEthernet3/0/14
 port link-mode route
#
interface GigabitEthernet3/0/15
 port link-mode route
#
interface GigabitEthernet3/0/16
 port link-mode route
#
interface GigabitEthernet3/0/17
 port link-mode route
 description to ISP
 combo enable copper
 ip binding vpn-instance DX
 ip address 10.10.10.2 255.255.255.0
 nat outbound 3000 address-group 1 vpn-instance DX
 ipsec apply policy test
#
interface GigabitEthernet3/0/18
 port link-mode route
 combo enable fiber
 ip binding vpn-instance LT
#
interface GigabitEthernet3/0/19
 port link-mode route
 combo enable fiber
#
interface GigabitEthernet3/0/20
 port link-mode route
 combo enable fiber
#
```

```
interface GigabitEthernet3/0/21
 port link-mode route
 combo enable fiber
#
interface GigabitEthernet3/0/22
 port link-mode route
 combo enable fiber
#
interface GigabitEthernet3/0/23
 port link-mode route
 combo enable fiber
#
interface GigabitEthernet3/0/24
 port link-mode route
 combo enable fiber
#
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance management
 ip address 192.168.0.1 255.255.255.0
#
interface Ten-GigabitEthernet3/0/25
 port link-mode route
#
interface Ten-GigabitEthernet3/0/26
 port link-mode route
#
interface Blade2/0/1
#
interface Blade-Aggregation1
#
object-policy ip DMZ-DMZ
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 3 pass vrf management
#
object-policy ip DMZ-Local
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip DMZ-Trust
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip DMZ-Untrust
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Local-DMZ
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Local-Local
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Local-Management
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
```

```
#
object-policy ip Local-Trust
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Local-Untrust
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Trust-DMZ
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Trust-Local
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Trust-Trust
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Trust-Untrust
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Untrust-DMZ
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Untrust-Local
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Untrust-Trust
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
object-policy ip Untrust-Untrust
 rule 0 pass vrf DX
 rule 1 pass vrf LT
 rule 4 pass vrf management
#
security-zone name Local
#
security-zone name Trust
 import interface GigabitEthernet3/0/1
 import interface GigabitEthernet3/0/21
 import interface GigabitEthernet3/0/22
 import interface GigabitEthernet3/0/23
 import interface GigabitEthernet3/0/24
 import interface LoopBack1
#
security-zone name DMZ
#
security-zone name Untrust
```

```
 import interface GigabitEthernet3/0/17
 import interface GigabitEthernet3/0/18
 import interface GigabitEthernet3/0/19
 import interface GigabitEthernet3/0/20
#
security-zone name Management
 import interface M-GigabitEthernet0/0/0
#
zone-pair security source DMZ destination DMZ
 object-policy apply ip DMZ-DMZ
#
zone-pair security source DMZ destination Local
 object-policy apply ip DMZ-Local
#
zone-pair security source DMZ destination Trust
 object-policy apply ip DMZ-Trust
#
zone-pair security source DMZ destination Untrust
 object-policy apply ip DMZ-Untrust
#
zone-pair security source Local destination DMZ
 object-policy apply ip Local-DMZ
#
zone-pair security source Local destination Local
 object-policy apply ip Local-Local
#
zone-pair security source Local destination Management
 object-policy apply ip Local-Management
#
zone-pair security source Local destination Trust
 object-policy apply ip Local-Trust
#
zone-pair security source Local destination Untrust
 object-policy apply ip Local-Untrust
#
zone-pair security source Trust destination DMZ
 object-policy apply ip Trust-DMZ
#
zone-pair security source Trust destination Local
 object-policy apply ip Trust-Local
#
zone-pair security source Trust destination Trust
 object-policy apply ip Trust-Trust
#
zone-pair security source Trust destination Untrust
 object-policy apply ip Trust-Untrust
#
zone-pair security source Untrust destination DMZ
 object-policy apply ip Untrust-DMZ
#
zone-pair security source Untrust destination Local
 object-policy apply ip Untrust-Local
#
zone-pair security source Untrust destination Trust
 object-policy apply ip Untrust-Trust
#
zone-pair security source Untrust destination Untrust
 object-policy apply ip Untrust-Untrust
#
 scheduler logfile size 16
#
line class console
 user-role network-admin
#
```

```
line class vty
 user-role network-operator
#
line con 1 2
 authentication-mode scheme
 user-role network-admin
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
#
 ip route-static vpn-instance DX 0.0.0.0 0 10.10.10.1
#
 ssh server enable
 undo ssh server compatible-ssh1x enable
#
acl number 3000
 rule 6 deny ip vpn-instance DX source 192.168.2.1 0 destination 192.168.1.0 0.0.0.255
 rule 10 permit ip vpn-instance DX
#
acl number 3001
#
acl number 3010
 description to ipsec
 rule 4 permit ip vpn-instance DX source 192.168.2.1 0 destination 192.168.1.0 0.0.0.255
#
domain system
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
```

```
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash
$h$6$Y6JqR67X2KTtp6pI$3KMTtH9BpM2u10IvA6mRU80+XxxyFOMIF4xRUvISjsuigXzRFVn8nHejGj
qMwMXXeZ0Ngy558baeDySxYzLCfw==
 service-type ssh telnet terminal https
 authorization-attribute user-role level-3
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
ipsec transform-set test
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy test 1 isakmp
 transform-set test
 security acl 3010
 local-address 10.10.10.2
 remote-address 10.10.10.1
 ike-profile test
#
nat address-group 1
 address 10.10.10.2 10.10.10.2
#
ike profile test
 local-identity address 10.10.10.2
 match remote identity address 10.10.10.1 255.255.255.0 vpn-instance DX
 match local address 10.10.10.2 vpn-instance DX
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain test vpn-instance DX
 pre-shared-key address 10.10.10.1 255.255.255.0 key cipher $c$3$1DdHZtpBBsaTmC6RiozzZaZvh
SZW9w==
#
 ip https enable
#
return
```

过程分析

在M9000上开启调试开关，查看到有如下调试信息打出

```
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Received packet from 1
0.10.10.1 source port 500 destination port 500.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1;
  I-COOKIE: e308ec59ad9e32d8
  R-COOKIE: fa03a4ef576d1106
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Quick
  flags: ENCRYPT
```

```
  message ID: 3695893f
  length: 164
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/EVENT: -Slot=2.1; IKE thread 36652354832
0 processes a job.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/EVENT: -Slot=2.1; Set IPsec SA state to IK
E_P2_STATE_INIT.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Decrypt the packet.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Received ISAKMP Has
h Payload.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Received ISAKMP Sec
urity Association Payload.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Received ISAKMP Non
ce Payload.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Received ISAKMP Iden
tification Payload (IPsec DOI).
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Received ISAKMP Iden
tification Payload (IPsec DOI).
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Process HASH payload
.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/EVENT: -Slot=2.1; Validated HASH(1) succ
essfully.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Process IPsec ID paylo
ad.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Process IPsec ID paylo
ad.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/EVENT: -Slot=2.1; IPsec SA state changed f
rom IKE_P2_STATE_INIT to IKE_P2_STATE_GETSP.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IPSEC/7/EVENT: -Slot=2.1;
The policy's acl or ike profile does not match the flow, Name = test, Seqnum = 1
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/ERROR: -Slot=2.1; Failed to get IPsec polic
y for phase 2 responder. Delete IPsec SA.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/ERROR: -Slot=2.1; Failed to negotiate IPse
c SA.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/EVENT: -Slot=2.1; Delete IPsec SA.
*Jun 14 12:47:57:853 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Encrypt the packet.
*Jun 14 12:47:57:853 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Construct notification p
acket: INVALID_ID_INFORMATION.
*Jun 14 12:47:57:853 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Sending packet to 10.1
0.10.1 remote port 500, local port 500.
*Jun 14 12:47:57:853 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1;
  I-COOKIE: e308ec59ad9e32d8
  R-COOKIE: fa03a4ef576d1106
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Info
  flags: ENCRYPT
  message ID: 41d07dea
  length: 68
*Jun 14 12:47:57:853 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Sending an IPv4 packe
t.
*Jun 14 12:47:57:853 2017 LQ_DTTE_center_FW IPSEC/7/packet: -Slot=2.1;
Enter IPsec output process, Flag : 0x80, Data length : 96
```

根据调试信息分析可以看到，设备提示INVALID_ID_INFORMATION，根据报错，怀疑还是配置参数不匹配，导致IPSec无法正常建立。

```
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/ERROR: -Slot=2.1; Failed to get IPsec polic
y for phase 2 responder. Delete IPsec SA.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/ERROR: -Slot=2.1; Failed to negotiate IPse
c SA.
*Jun 14 12:47:57:852 2017 LQ_DTTE_center_FW IKE/7/EVENT: -Slot=2.1; Delete IPsec SA.
*Jun 14 12:47:57:853 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Encrypt the packet.
*Jun 14 12:47:57:853 2017 LQ_DTTE_center_FW IKE/7/PACKET: -Slot=2.1; Construct notification p
acket: INVALID_ID_INFORMATION.
```

通过检查设备配置，发现设备配置感兴趣流与对端不匹配

```
#
acl number 3010
 description to ipsec
 rule 4 permit ip vpn-instance DX source 192.168.2.1 0 destination 192.168.1.0 0.0.0.255
#
```

ZX侧感性趣流配置如下

```
$
!</switchvlan>
!<ipv4-acl>
ipv4-access-list 3010
  rule 10 permit ip 192.168.1.0 0.0.0.255 192.168.2.1 0.0.0.0
$
```

可以看到acl中一端配置了vpn实例，另一端没有配置vpn实例。

解决方法

调整中兴侧配置，将acl配置vpn实例解决。