某局点 MSR IPSEC VPN对接锐捷不成功

IPSec VPN　林宇阳　2023-12-20 发表

组网及说明

无特殊组网，IPSEC VPN两端点分别是H3C MSR和锐捷路由器。

告警信息

*Jul 13 23:04:20:886 2023 H3C IKE/7/EVENT: Phase1 process started.
*Jul 13 23:04:20:886 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Received ISAKMP Key Exchange Payload.
*Jul 13 23:04:20:886 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Received ISAKMP Nonce Payload.
*Jul 13 23:04:20:886 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Received ISAKMP NAT-D Payload.
*Jul 13 23:04:20:886 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Received ISAKMP NAT-D Payload.
*Jul 13 23:04:20:886 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Process KE payload.
*Jul 13 23:04:20:887 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Process NONCE payload.
*Jul 13 23:04:20:896 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Received 2 NAT-D payload.
*Jul 13 23:04:20:896 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Local ID type: IPV4_ADDR (1).
*Jul 13 23:04:20:896 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Local ID value: A.B.40.4.
*Jul 13 23:04:20:896 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Construct ID payload.
*Jul 13 23:04:20:896 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
HASH:
e14005b5 840fcd91 c6098928 168f6ea9
*Jul 13 23:04:20:896 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Construct authentication by pre-shared-key.
*Jul 13 23:04:20:897 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Construct INITIAL-CONTACT payload.
*Jul 13 23:04:20:897 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Encrypt the packet.
*Jul 13 23:04:20:897 2023 H3C IKE/7/EVENT: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
IKE SA state changed from IKE_P1_STATE_SEND3 to IKE_P1_STATE_SEND5.
*Jul 13 23:04:20:897 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Sending packet to M.N.0.14 remote port 500, local port 500, out-interface 0.
*Jul 13 23:04:20:897 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500

I-COOKIE: f6a8da06b5f8f214
R-COOKIE: 00015017ba001cf6
next payload: ID
version: ISAKMP Version 1.0
exchange mode: Main
flags: ENCRYPT
message ID: 0
length: 92
*Jul 13 23:04:20:897 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Sending an IPv4 packet.
*Jul 13 23:04:20:897 2023 H3C IKE/7/EVENT: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Send udp packet by socket 41 SrcPort 500 ifIndex 0.
*Jul 13 23:04:20:897 2023 H3C IKE/7/EVENT: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Sent data to socket successfully.

*Jul 13 23:04:20:924 2023 H3C IKE/7/EVENT: Received packet successfully.
*Jul 13 23:04:20:924 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Received packet from M.N.0.14 source port 500 destination port 500.
*Jul 13 23:04:20:925 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500

I-COOKIE: f6a8da06b5f8f214
R-COOKIE: 00015017ba001cf6
next payload: HASH
version: ISAKMP Version 1.0
exchange mode: Info
flags: ENCRYPT
message ID: b25c1d33
length: 76
*Jul 13 23:04:20:925 2023 H3C IKE/7/EVENT: IKE thread 2784412960 processes a job.
*Jul 13 23:04:20:925 2023 H3C IKE/7/EVENT: Info packet process started.
*Jul 13 23:04:20:925 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Decrypt the packet.
*Jul 13 23:04:20:925 2023 H3C IKE/7/PACKET: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Received ISAKMP Hash Payload.
*Jul 13 23:04:20:925 2023 H3C IKE/7/ERROR: 2th byte of the structure ISAKMP Hash Payload must be 0.
*Jul 13 23:04:20:926 2023 H3C IKE/7/ERROR: vrf = 0, local = A.B.40.4, remote = M.N.0.14/500
Failed to parse informational exchange packet. Reason INVALID_PAYLOAD_TYPE.

问题描述

对端锐捷配置
crypto isakmp mode-detect
cryoto isakmp policy 10
encryption sm4
authentication pre-share
hash md5
!
crypto isakmp key 7 ***** address 0.0.0.0 0.0.0.0
crypto ipsec transform-set AA_IPSEC_TS esp-sm4 esp-sha-hmac
crypto dynamic-map AA_DM 20
set transform-set AA_IPSEC_TS
reverse-route tag 30
!
crypto map AA_CP 20 ipsec-isakmp dynamic AA_DM
客户提供能正常建立的迈普设备配置：
crypto ike key *** address 192.168.0.22 (CMCC) / M.N.0.14 (CTCC)
crypto ike proposal GM
encryption sm4
integrity md5
exit
crypto ipsec proposal GM
esp sm4-old sha1
exit
现场参考迈普设备输出了以下我司配置：
#
ipsec policy SIM1(Cellular1/1) 65535 isakmp
 transform-set GM
 security acl name GM
 local-address A.B.40.4
 remote-address M.N.0.14
 description GM
 ike-profile GM
#
ike profile GM
 keychain GM
 match remote identity address M.N.0.14 255.255.255.255
 proposal 65535
#
ike proposal 65535
#
ike keychain GM
 pre-shared-key address
M.N.0.14 255.255.255.255 key cipher c3$3Xv9W4/Ro37qzSffiHs8LBt5BvIAgkxJCTgqYd7CXQ==
#

但ipsec始终无法建立，debug ike all 显示错误信息如上

过程分析

依次核对IKE和IPSEC的各配置模块。

1、ike keychain已配置且指定锐捷设备IP；

2、ike profile 已指定对端锐捷设备特征为IP地址；

3、ike proposal 在锐捷设备中未找到明确对应，但迈普设备在proposal中指定了加密算法SM4，而我司缺省的加密算法不是SM4；

解决方法

ike propose 65535下配置加密算法为SM4