ACG1000和comware v5防火墙ipsec建立失败

IPSec VPN　叶红兵　2024-08-26 发表

问题描述

拓扑：F100-C-G-------公网-------L1000--------ACG1000--------核心交换机
acg1000是内网设备，由于L1000负载设备做不了ipsec，所以是acg1000和F100-C-G建立ipsec隧道，建立隧道卡在第一阶段

过程分析

通过抓包，发现两端proposal的方式不一致


```
> Version: 1.0
  Exchange type: Informational (5)
> Flags: 0x00
  Message ID: 0x00000000
  Length: 44
v Payload: Notification (11)
    Next payload: NONE / No Next Payload  (0)
    Reserved: 00
    Payload length: 16
    Domain of interpretation: IPSEC (1)
    Protocol ID: ISAKMP (1)
    SPI Size: 0
    Notify Message Type: NO-PROPOSAL-CHOSEN (14)
    Notification DATA: 00000000
```

对照两端的配置

F100:

```
#
ike peer towlc
 pre-shared-key cipher $c$3$QWjxa93OXCoMFw2ZJXdRA8wonaRUo13MBQ==
 remote-address X.X.X.X
 local-address X.X.X.X
#
ipsec transform-set 2
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
 esp encryption-algorithm 3des
#
ipsec policy tykvpn 2 isakmp
```

security acl 3002

ike-peer towbs

transform-set 1

sa duration traffic-based 1843200

sa duration time-based 3600

防火墙默认的和acg1000上配置不一致

```
<firewall>display ike po
<firewall>display ike p
<firewall>display ike proposal
 priority authentication authentication encryption Diffie-Hellman duration
             method       algorithm    algorithm     group       (seconds)
--------------------------------------------------------------------------
  1          PRE_SHARED     SHA          3DES_CBC      MODP_1024     28800
  2          PRE_SHARED     SHA          DES_CBC       MODP_768      28800
  default    PRE_SHARED     SHA          DES_CBC       MODP_768      86400
<firewall>
```

```
▾ Payload: Transform (3) # 0
    Next payload: NONE / No Next Payload  (0)
    Reserved: 00
    Payload length: 36
    Transform number: 0
    Transform ID: KEY_IKE (1)
    Reserved: 0000
  › IKE Attribute (t=11,l=2): Life-Type: Seconds
  › IKE Attribute (t=12,l=4): Life-Duration: 86400
  › IKE Attribute (t=1,l=2): Encryption-Algorithm: 3DES-CBC
  › IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key
  › IKE Attribute (t=2,l=2): Hash-Algorithm: MD5
  › IKE Attribute (t=4,l=2): Group-Description: Alternate 1024-bit MODP group
```

在acg上修改加密算法和认证算法、dh组后，抓包和debug同时进行查看，发现收发的端口都是500

```
1 2024-07-01 17:12:38.706490 ... ISAKMP 266 Identity Protection (Main Mode)
2 2024-07-01 17:12:43.707445 ... ISAKMP 266 Identity Protection (Main Mode)
3 2024-07-01 17:12:48.708698 ... ISAKMP 266 Identity Protection (Main Mode)
4 2024-07-01 17:13:04.726171 ... ISAKMP 266 Identity Protection (Main Mode)
5 2024-07-01 17:13:04.728726 ... ISAKMP 126 Identity Protection (Main Mode)
6 2024-07-01 17:13:04.734791 ... ISAKMP 190 Identity Protection (Main Mode)
7 2024-07-01 17:13:04.739144 ... ISAKMP 210 Identity Protection (Main Mode)
8 2024-07-01 17:13:04.754925 ... ISAKMP 110 Identity Protection (Main Mode)
```

```
› Frame 8: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
› Ethernet II, Src: NewH3CTe_35:ff:5d (58:b3:8f:35:ff:5d), Dst: NewH3CTe_30:e3:45 (74:3a:20:30:e3:45)
› Internet Protocol Version 4, Src: ... 1, Dst: ... 6
› User Datagram Protocol, Src Port: 500, Dst Port: 500
› Internet Security Association and Key Management Protocol
```

*Jul 2 13:39:14:641 2024 firewall IKE/7/DEBUG: received message:

*Jul 2 13:39:14:642 2024 firewall IKE/7/DEBUG: ICOOKIE: 0x0cd7aa74c7d1d068

*Jul 2 13:39:14:642 2024 firewall IKE/7/DEBUG: RCOOKIE: 0xe9644cbe97a31ee9

*Jul 2 13:39:14:643 2024 firewall IKE/7/DEBUG: NEXT_PAYLOAD: ID

*Jul 2 13:39:14:643 2024 firewall IKE/7/DEBUG: VERSION: 16

*Jul 2 13:39:14:643 2024 firewall IKE/7/DEBUG: EXCH_TYPE: MAIN

*Jul 2 13:39:14:644 2024 firewall IKE/7/DEBUG: FLAGS: [ENC]

*Jul 2 13:39:14:644 2024 firewall IKE/7/DEBUG: MESSAGE_ID: 0x00000000

*Jul 2 13:39:14:644 2024 firewall IKE/7/DEBUG: LENGTH: 68

*Jul 2 13:39:14:645 2024 firewall IKE/7/DEBUG: check message duplicate

*Jul 2 13:39:14:645 2024 firewall IKE/7/DEBUG: parse payloads: payload ID

*Jul 2 13:39:14:646 2024 firewall IKE/7/DEBUG: parse payloads: payload HASH

*Jul 2 13:39:14:646 2024 firewall IKE/7/DEBUG: validate payload ID

*Jul 2 13:39:14:646 2024 firewall IKE/7/DEBUG: TYPE: 1

*Jul 2 13:39:14:647 2024 firewall IKE/7/DEBUG: DOI_DATA: 0x1101f4

*Jul 2 13:39:14:647 2024 firewall IKE/7/DEBUG: id information: type 1 proto 17 port500

*Jul 2 13:39:14:648 2024 firewall IKE/7/DEBUG: id information: IPv4 address X.X.X.X

*Jul 2 13:39:14:648 2024 firewall IKE/7/DEBUG: validate payload HASH

*Jul 2 13:39:14:648 2024 firewall IKE/7/DEBUG: exchange check: checking for required ID

*Jul 2 13:39:14:649 2024 firewall IKE/7/DEBUG: exchange check: checking for required AUTH

*Jul 2 13:39:14:649 2024 firewall IKE/7/DEBUG: P1 handle ID:Failed to find ike peer by address.

*Jul 2 13:39:14:650 2024 firewall IKE/7/DEBUG: exchange state machine:Failed to receive message.

两边nat穿越都没有配置，发现v5的防火墙默认nat穿越是关闭的

配置IKE/IPsec的NAT穿越功能	nat traversal	可选 在IPsec/IKE组建的VPN隧道中，若存在NAT安全网关设备，则必须配置IPsec/IKE的NAT穿越功能 缺省情况下，没有配置NAT穿越功能

再防火墙上加入还是不行

解决方法

查询comware平台vpn对比：

Q:Comware V3、V5、V7在配置IPsec VPN时有何不同?

A:

1) V3、V5防火墙主模式不支持NAT穿越，只有野蛮模式支持。

V7防火墙主模式和野蛮模式都支持NAT穿越（必须两端均支持）。

2) V3、V5防火墙display ike sa可以显示第一、二阶段建立情况。

V7防火墙display ike sa只显示ike总的建立情况，包含一、二阶段。

3) V3、V5防火墙必须手动开nat traversal才能支持nat穿越。

V7无需手动开启，自动支持。

4) V5老版本和v3的ike peer xxx相当于V7的ike profile xxx。

V7的预共享秘钥创建需要在全局下另配置ike keychain。

5) V3设备匹配acl感兴趣流permit后需deny其他流。

V5、V7不需要deny。

6) V7支持匹配内部VPN和外部VPN，内部VPN表示封装前报文所属VPN，外部VPN表示封装后报文所属VPN。

7) V7支持控制总共的IPSec 协商sa数量或者建立成功的sa数量，如果超过设定最大值，申请将会被拒绝。

8) V7支持IKEv2，V5和V3不支持。

将模式改为野蛮模式且防火墙上开启nat穿越后ipsec隧道成功建立

v5ipsec配置参考以下配置指导

https://dmp.h3c.com/sites/tsc/_layouts/15/WopiFrame.aspx?sourcedoc={EFEF6331-3DB7-407F-B608-5F079143A136}&file=03-SecPath%E7%B3%BB%E5%88%97%E9%98%B2%E7%81%AB%E5%A2%99IPSec%E5%85%B8%E5%9E%8B%E9%85%8D%E7%BD%AE%E4%B8%BE%E4%BE%8B.doc&action=default