某局点WX3510H 和CISCO 对接IPsec不定时出现中断问题处理经验案例

wlan接入 刘文峰 2021-01-29 发表

组网及说明

无

问题描述

某局点采用WX3510H和对端CISCO设备对接IPsec，实现内网无线终端业务流量能访问对面，之前使用都是正常的，但是最近发现ipsec 业务不定时中断，出现中断的时候dis ike sa 没有了，只有dis ipsec sa，初步怀疑是两边ike 协商有问题，但是由于现场cisco 设备暂无法登入，无法查看对端配置，只能在本端收集debug信息查看。

过程分析

第一次故障时查看dis ike sa 没有，但是dis ipsec sa 还有。

```
<AC-WX3510H-F>dis ike sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------
<AC-WX3510H-F> dis ipsec sa
------------------------------
Interface: Vlan-interface100
------------------------------
 ----------------------------
 IPsec policy: 1
 Sequence number: 1
 Mode: ISAKMP
 ----------------------------
   Tunnel id: 0
   Encapsulation mode: tunnel
   Perfect Forward Secrecy:
   Inside VPN:
   Extended Sequence Numbers enable: N
   Traffic Flow Confidentiality enable: N
   Path MTU: 1428
   Tunnel:
      local  address: x.x.x.x
      remote address: x.x.x.90
   Flow:
      sour addr: 172.x.x.0/255.255.252.0  port: 0  protocol: ip
      dest addr: 192.x.x.0/255.255.255.0  port: 0  protocol: ip
```

后续在8:23的时候dis ike sa 已协商正常，并且业务已恢复正常，

```
*Jan 21 08:23:52:828 2021 AC-WX3510H-F IPSEC/7/PACKET:
Outbound IPsec processing: Packet encapsulated successfully.
dis ike sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------
   4783          x.x.x..90        RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<AC-WX3510H-F>*Jan 21 08:23:54:827 2021 AC-WX3510H-F IPSEC/7/PACKET:
```

在08:28 查看时，发现dis ike sa 又消失了，业务再次中断

```
*Jan 21 08:28:54:999 2021 AC-WX3510H-F IPSEC/7/PACKET:
Outbound IPsec processing: Packet encapsulated successfully.
<AC-WX3510H-F>
<AC-WX3510H-F>dis ike sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------
<AC-WX3510H-F>dis ipsec sa
------------------------------
```

查看故障时的debug信息，发现在ike 第一阶段协商的时候，协商的存活时间为60s，但是查看设备侧没有做特殊配置，采用的是默认配置，但是由于对端暂无法登入，无法查看配置确认。

```
*Jan 21 08:23:41:702 2021 AC-WX3510H-F IKE/7/EVENT: Vendor ID NAT-T rfc3947 is matched.
*Jan 21 08:23:41:702 2021 AC-WX3510H-F IKE/7/PACKET: vrf = 0, local = x.x.x.202, remote = x.x.x.
90/500
Process SA payload.
*Jan 21 08:23:41:702 2021 AC-WX3510H-F IKE/7/PACKET: vrf = 0, local = x.x.x.202, remote = x.x.x.
90/500
Check ISAKMP transform 1.
*Jan 21 08:23:41:702 2021 AC-WX3510H-F IKE/7/PACKET: vrf = 0, local =  x.x.x.202, remote = x.x.x
.90/500
  Encryption algorithm is AES-CBC.
*Jan 21 08:23:41:702 2021 AC-WX3510H-F IKE/7/PACKET: vrf = 0, local =  x.x.x.202, remote = x.x.x
.90/500
  Key length is 128 bytes.
```

*Jan 21 08:23:41:703 2021 AC-WX3510H-F IKE/7/PACKET: vrf = 0, local = x.x.x.202, remote = x.x.x.90/500

解决方法

HASH algorithm is HMAC-SHA1.

后续协商客户登入CSCO设备查看发现CISCO上的isakmp时间改为60s了，对端60s就出现重新协商，但是我司设备不会重新协商，导致业务中断。

Jan 21 08:23:41:703 2021 AC-WX3510H-F IKE/7/PACKET: vrf = 0, local = x.x.x.202, remote = x.x.x.90/500

最终把我司的ike sa duration 改为60s 之后，问题解决。

Life duration is 2

ike proposal 1

encryption-algorithm aes-cbc-128

dh group 2

Authentication method is Pre-shared key.

sa duration 20

Jan 21 08:23:41:703 2021 AC-WX3510H-F IKE/7/PACKET: vrf = 0, local = x.x.x.202, remote = x.x.x.90/500

Lifetime type is 1.

*Jan 21 08:23:41:703 2021 AC-WX3510H-F IKE/7/PACKET: vrf = 0, local = x.x.x.202 remote = x.x.x.90/500

Life duration is 60.

*Jan 21 08:23:41:704 2021 AC-WX3510H-F IKE/7/EVENT: vrf = 0, local = x.x.x.202, remote = x.x.x.90/500

Found pre-shared key that matches address x.x.x.90 in keychain 1.