某局点F1000防火墙对接第三方设备IPSEC VPN起不来

IPSec VPN 于宛盈 2022-12-31 发表

问题描述

现场反馈我司设备对接第三方设备建立IPSEC VPN（野蛮模式）失败，本端（我司）设备去触发流量，现场反馈隧道连第一阶段都建立不起来。

过程分析

查看debug 信息，发现是预共享密钥地址找不到，从而没有可用的提议导致IPSEC VPN隧道建立失败。

*Dec 23 20:00:07:847 2022 F1000 IKE/7/EVENT: vrf = 0, local = xxx.xxx.xxx.xxx, remote = xxx.xxx.xxx.xxx/500 Pre-shared key matching address xxx.xxx.xxx.xxx not found. *Dec 23 20:00:07:847 2022 F1000 IKE/7/ERROR: vrf = 0, local = xxx.xxx.xxx.xxx, remote = xxx.xxx.xxx.xxx/500 No available proposal. *Dec 23 20:00:07:847 2022 F1000 IKE/7/ERROR: vrf = 0, local = xxx.xxx.xxx.xxx, remote = xxx.xxx.xxx.xxx/500 Failed to negotiate IKE SA.

检查配置后，发现ike keychain的pre-shared key匹配条件，配置为hostname。

ike keychain xxxxx_IPv4_1 match local address GigabitEthernet1/0/4 pre-shared-key hostname xxxxx key cipher c3$pL+6yXmFbuo3x01Md3mFJPc9XqJPFvP6qdG+

官网资料说明，以hostname方式设置预共享密钥时，IKE协商只能采用野蛮模式，设备本身只能作为响应方，且对端IKE身份ID需采用FQDN方式来匹配主机名。但本端设备是以发起方去触发流量，所以不能配置为hostname。

解决方法

现场后续修改pre-shared key的匹配条件为address后，IPSEC VPN隧道成功建立起来。注意的是，pre-shared key的匹配条件address需得和ipsec policy的remote-address保持一致。