IPSEC主模式交互过程中，报文及debug信息含义

IPSec VPN 聂骋 2023-01-12 发表

组网及说明

不涉及，就IPSEC就行。

告警信息

无

问题描述

IPSEC中ike协商

过程分析

在IPSEC主模式中，防火墙的debugging可以看到报文交互的情况，也就是到哪一步了，6个报文交互到哪里了。命令是debugging ike all

。

防火墙作为发起方debugging的发包流程是init——send1——send3——send5——est
防火墙作为向远方debugging的发包流程是init——send2——send4——est

debugging想看的话可以按照如下格式搜索。这个例子就是send3变成send5的。那如果看到这个debugging，那说明ike已经到send5这个阶段了，下面说的排查也是看最终状态。最终状态是5，那么就检查5-6包的内容。
IKE SA state changed from IKE_P1_STATE_SEND3 to IKE_P1_STATE_SEND5.

而在整个ike主模式过程中，1-2个包是协商算法，以及ike密钥选择，因此如果debugging看到1-2个包，就没下文了，那大概率是算法错误，或者ike密钥中的匹配条件错了，没有选择到密钥。
这就只需要对比配置，然后检查密钥配置，特别是密钥中的匹配条件，地址或者name，是不是配置对了。

3-4个包是协商生成密钥，一般不会出现错误，如果到这里没有下文，说明密钥配置不一致，这就可能是配错了，或者在防火墙配置多个密钥，而匹配条件有完全相同的，可能匹配错了。
这个就需要检查密钥配置中，是否存在完全一样的地址，或者name配置，如果完全一样，那么就可能出现选错密钥。并且这里会进行算法的校验，如果设备存在多个算法完全一样的ike提议，那么设备选择后，会再次和ike profile下的配置校验，如果配置的和选择的不一样，也会出错，因此还要检查是否有算法完全一样的ike 提议，如果有，就删除，所有需要这个算法的都共用就行。

5-6个包只有identity身份校验，因此只用检查身份配置是否对称，比如我本地配置的是local-identity 1.1.1.1，那么无论对端收到的报文，地址是多少，对端都要配置remote identity 1.1.1.1。因此检查这个即可。

解決方法

如上