V7防火墙野蛮模式对接深信服建立ipsec

IPSec VPN 杨凌轩 2019-04-11 发表

组网及说明

本端V7防火墙作为公网出口，与对端深信服建立IPSEC

问题描述

配置完成后隧道无法建立。dis ike sa处于unknown状态。检查配置两端验证和加密算法一致。地址也配置正确。

过程分析

检查基础配置完整

ipsec transform-set 1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
 # ipsec policy 1 100 isakmp
 transform-set 1
 security acl 3001
 remote-address 218.26.228.237
 ike-profile 1
 sa duration time-based 28800
ipsec policy 10 100 isakmp
ike profile 1
 keychain 1
 dpd interval 5 on-demand
 exchange-mode aggressive
 local-identity fqdn sxlsj
 match remote identity fqdn sxctc
 proposal 1
ike proposal 1
 encryption-algorithm aes-cbc-128
 dh group2
 sa duration 28800
ike keychain 1
pre-shared-key hostname sxctc key cipher c3$3PPYt8wNJxkBEWyxxlg6FBXsrOPQ7LtgsdtdpMN7

查看debug信息发现有如下告错

Verify HASH payload.
*Apr 11 14:30:22:809 2019 H3C IKE/7/PACKET: vrf = 0, src = 61.134.243.207, dst = 218.26.228.237/4500 HASH: 5724f3cf ba13da08 bd705ca0 ffbe14de 1be642c5
*Apr 11 14:30:22:809 2019 H3C IKE/7/ERROR: vrf = 0, src = 61.134.243.207, dst = 218.26.228.237/4500 Failed to verify the peer HASH.
 *Apr 11 14:30:22:809 2019 H3C IKE/7/PACKET: vrf = 0, src = 61.134.243.207, dst = 218.26.228.237/4500 Construct notification packet: AUTHENTICATION_FAILED.

根据debug来看是因为hash验证失败，对端发过来的hash本端没办法识别匹配。

检查两端算法配置一致为何还会出现验证失败，怀疑是否因为厂商不同导致的处理有差别

解决方法

因为ike算法是公有算法，模式一致。检查发现预共享秘钥配置 为字母@数字的格式。

将@去掉，改为纯字母后，发现可以正常建立。

与深信服对接时，不论是域名fqdn还是秘钥都要以字母或者数字的形式进行对接，不要配置带有特殊符号。

对于debug的信息配置检查无误考虑不同厂商是否会有处理机制的差异。