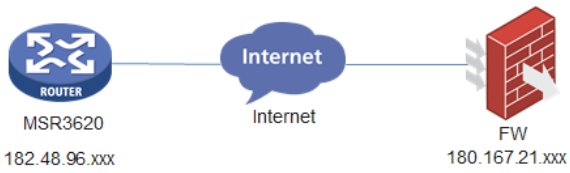
MSR3600路由器和第三方防火墙ipsec建立失败经验案例

IPSec VPN　孙兆强　2019-03-29 发表

组网及说明



MSR3620和第三方防火墙建立主模式ipsec。

问题描述

MSR3620路由器和第三方防火墙w无法建立ipsec，IKE已经建立但是显示Unknown 。根据用户反馈的配置，各种参数均配置正确。

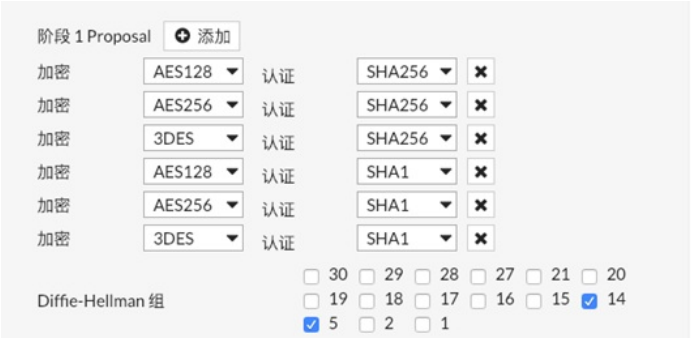
过程分析

过程分析

查看ike协商情况，显示Unknown怀疑是参数问题，查看协商参数均正确。

PEK1-CO-AGG-R1]display ike sa

Connection-ID	Remote	Flag	DOI
1171	180.167.21.xx	Unknown	IPsec



ike proposal 10

encryption-algorithm aes-cbc-128

dh group14

[H3C]display ipsec transform-set
IPsec transform set: transform
State: complete
Encapsulation mode: tunnel
ESN: Disabled
PFS: dh-group14
Transform: ESP
ESP protocol:
Integrity: SHA1
Encryption: AES-CBC-128

开始设备的debug，信息显示如下
*Mar 7 19:06:05:789 2019 PEK1-CO-AGG-R1 IKE/7/PACKET: vrf = 0, local = 182.48.96.xxx, remote = 150.107.71.xx/500
Received packet from 150.107.71.xx source port 500 destination port 500.
*Mar 7 19:06:05:789 2019 PEK1-CO-AGG-R1 IKE/7/PACKET: vrf = 0, local = 182.48.96.xxx, remote = 150.107.71.xx/500

I-COOKIE: eb15fd1dc262aa5e
R-COOKIE: 0000000000000000
next payload: SA
version: ISAKMP Version 1.0
exchange mode: Main
flags:
message ID: 0
length: 292
*Mar 7 19:06:05:789 2019 PEK1-CO-AGG-R1 IKE/7/EVENT: IKE thread 1099142849200 processes a job.
*Mar 7 19:06:05:789 2019 PEK1-CO-AGG-R1 IKE/7/EVENT: Phase1 process started.
*Mar 7 19:06:05:789 2019 PEK1-CO-AGG-R1 IKE/7/PACKET: vrf = 0, local = 182.48.96.xxx, remote = 150.107.71.xx/500
Begin a new phase 1 negotiation as responder.
……

*Mar 7 19:06:05:792 2019 PEK1-CO-AGG-R1 IKE/7/PACKET: vrf = 0, local = 182.48.96.xxx, remote = 150.107.71.xx/500
Sending an IPv4 packet.
*Mar 7 19:06:05:792 2019 PEK1-CO-AGG-R1 IKE/7/EVENT: vrf = 0, local = 182.48.96.xxx, remote = 150.107.71.xx/500
Sent data to socket successfully.
*Mar 7 19:06:05:792 2019 PEK1-CO-AGG-R1 IKE/7/ERROR: vrf = 0, local = 182.48.96.xxx, remote = 150.107.71.xx/500
Failed to negotiate IKE SA.
*Mar 7 19:06:05:848 2019 PEK1-CO-AGG-R1 IPSEC/7/ERROR:
Tunnel10239: Failed to check source address because of valid address.
*Mar 7 19:06:08:542 2019 PEK1-CO-AGG-R1 IPSEC/7/EVENT:
Found block-flow node.
*Mar 7 19:06:08:542 2019 PEK1-CO-AGG-R1 IPSEC/7/PACKET:
Failed to find SA by SP, SP Index = 0, SP Convert-Seq = 655360.
*Mar 7 19:06:08:542 2019 PEK1-CO-AGG-R1 IPSEC/7/ERROR:
The reason of dropping packet is no available IPsec tunnel.
*Mar 7 19:06:10:848 2019 PEK1-CO-AGG-R1 IPSEC/7/ERROR:
Tunnel10239: Failed to check source address because of valid address.
*Mar 7 19:06:11:041 2019 PEK1-CO-AGG-R1 IKE/7/PACKET: vrf = 0, local = 182.48.96.xxx, remote = 180.167.21.xx/500
Retransmit phase 1 packet.
*Mar 7 19:06:11:041 2019 PEK1-CO-AGG-R1 IKE/7/PACKET: vrf = 0, local = 182.48.96.xxx,remote = 180.167.21.xx/500
Sending packet to 180.167.21.xx remote port 500, local port 500.

从debug信息看我们设备收到的对端发过来的报文原地址为150.107.71.xx，设备检查报文原地址错误。设备重传第一阶段报文发送的目的地址为180.167.21.xx。而我们设备上配置的对端地址180.167.21.

xx，说明对端发包的地址错误。

解决方法

对端修改路由，让ipsec的流量从180.167.21.xx发出。