

MSR810野蛮模式主动和对端华为防火墙建立ipsec vpn ike sa不起来

IPSec VPN

ChandlerBing

2024-01-19 发表

问题描述

我司路由器和对端华为防火墙建立ipsec vpn；我司路由器这边是发起方，选用的ike协商模式为野蛮模式；对端公网地址能通，但是ike sa第一阶段未起来，在路由器上debug ike all无任何回显信息

过程分析

经排查设备未有回显的原因因为出接口侧存在ACL阻断ike协商报文，现取消策略后已存在回显信息，目前ipsec邻居还未建立，在华为防火墙侧已收到相关请求包，但有协商错误的提醒，debug回显信息如下。可以看到野蛮模式的6个报文

Sending packet to 10.100.1.2 remote port 500, local port 500.

*Jan 29 11:59:06:789 2011 FS-ZYC-MSR810-01 IKE/7/PACKET: vrf = 0, local = 10.227.6.1.22, remote = 10.100.1.2/500

I-COOKIE: da8a93c49e2f6e86

R-COOKIE: 0000000000000000

next payload: SA

version: ISAKMP Version 1.0

exchange mode: Aggressive

flags:

message ID: 0

length: 492

Received packet from 10.100.1.2 source port 500 destination port 500.

*Jan 29 11:59:06:815 2011 FS-ZYC-MSR810-01 IKE/7/PACKET: vrf = 0, local = 10.227.6.1.22, remote = 10.100.1.2/500

I-COOKIE: da8a93c49e2f6e86

R-COOKIE: 6663c48bc533c066

next payload: SA

version: ISAKMP Version 1.0

exchange mode: Aggressive

flags:

message ID: 0

length: 568

**IKE SA state changed from IKE_P1_STATE_SEND1 to
IKE_P1_STATE_ESTABLISHED.**

Sending packet to 10.100.1.2 remote port 500, local port 500.

*Jan 29 11:59:07:170 2011 FS-ZYC-MSR810-01 IKE/7/PACKET: vrf = 0, local = 10.227.6.1.22, remote = 10.100.1.2/500

I-COOKIE: da8a93c49e2f6e86

R-COOKIE: 6663c48bc533c066

next payload: HASH

version: ISAKMP Version 1.0

exchange mode: Aggressive

flags: ENCRYPT

message ID: 0

length: 172

Begin Quick mode exchange.

IPsec SA state changed from IKE_P2_STATE_GETSPI to IKE_P2_STATE_SEND1.

Sending packet to 10.100.1.2 remote port 500, local port 500.

*Jan 29 11:59:07:178 2011 FS-ZYC-MSR810-01 IKE/7/PACKET: vrf = 0, local = 10.227.6.1.22, remote = 10.100.1.2/500

I-COOKIE: da8a93c49e2f6e86

R-COOKIE: 6663c48bc533c066

next payload: HASH

version: ISAKMP Version 1.0
exchange mode: Quick
flags: ENCRYPT
message ID: b5ad4591
length: 188

Received packet from 10.100.1.2 source port 500 destination port 500.

*Jan 29 11:59:07:183 2011 FS-ZYC-MSR810-01 IKE/7/PACKET: vrf = 0, local = 10.227.6
1.22, remote = 10.100.1.2/500

I-COOKIE: da8a93c49e2f6e86
R-COOKIE: 6663c48bc533c066
next payload: HASH
version: ISAKMP Version 1.0
exchange mode: Info
flags: ENCRYPT
message ID: 12f8addf
length: 76

//第五个报文之后报了INVALID_ID信息，该打印有异常

Notification INVALID_ID_INFORMATION is received.

Sending packet to 10.100.1.2 remote port 500, local port 500.

*Jan 29 11:59:12:591 2011 FS-ZYC-MSR810-01 IKE/7/PACKET: vrf = 0, local = 10.227.6
1.22, remote = 10.100.1.2/500

I-COOKIE: da8a93c49e2f6e86
R-COOKIE: 6663c48bc533c066
next payload: HASH
version: ISAKMP Version 1.0
exchange mode: Quick
flags: ENCRYPT
message ID: b5ad4591
length: 188

解决方法

步骤1、把两边acl都保留1条本端到对端的，对端到本端的删除

步骤2、ike profile中fqdn本端和对端建议都保持一致，都配成名称或者都配成address

步骤3、修改完配置后，要reset ike sa再ping

改完配置后，ike sa协商成功，ipsec sa建立，网络可通。