案例库

AR1200 对接防火墙 后流量不通

发布时间: 2021-09-30 | 浏览次数: 84 | 下载次数: 0 | 作者: l84196264 | 文档编号: EKB1100080025

目录

问题描述

配置ipsec 感兴趣流的流量正常需要在做nat转换的ACL里面去deny 掉，让内网的流量不通过nat 而是直接通过ipsec 隧道转发出去。

处理过程

1.查看配置信息：

```
acl number 3001
 rule 5 permit ip source 174.XX.XX.0 0.0.0.255 destination 193.XX.XX.0 0.0.0.255   //感兴趣流
acl number 3002
 rule 15 deny ip source 174.XX.XX.0 0.0.0.255 destination 193.XX.XX.0 0.0.0.255  //deny 掉了感兴趣流 配置没有问题
 rule 20 permit ip

interface GigabitEthernet0/0/12
tcp adjust-mss 1200
ip address 220.XX.XX.65 255.255.255.192
nat outbound 3002
 ipsec policy ipsec
```

ike-peer ipsec1
proposal ipsec1
route inject static
配置正常

2.查看两端使用的IPSec阶段协商算法，发现认证算法使用的是sha2-256
ipsec proposal 1
transform ah-esp
ah authentication-algorithm sha2-256
esp authentication-algorithm sha2-256
esp encryption-algorithm aes-256

查看USG侧IPSec报文统计情况，其中很多入方向报文因认证失败被丢弃了，
display ipsec statistics all-systems
2021-09-06 15:16:51.400
IPSec statistics information:
Number of IPSec tunnels: 1
Number of standby IPSec tunnels: 0
the security packet statistics:
input/output security packets: 840/2126
input/output security bytes: 0/128160
input/output dropped security packets: 512/255
……
dropped security packet detail:
can not find SA: 1, wrong SA: 0
authentication: 382, replay: 0
front recheck: 66, after recheck: 0
change cpu enc: 0, dec change cpu: 0
fib search: 0, output l3: 0
flow err: 255, slice err: 0, byte limit: 0
slave drop: 0

根因

两端认证算法加密解密的方式不同导致。

解决方案

两端IPSec使用的认证算法是sha2-256但是AR侧未启用SHA-2算法兼容性功能，AR侧使用如下命令启用SHA-2算法兼容性功能后解决，
开启SHA-2算法兼容性算法功能。
<Huawei> system-view
[Huawei] ipsec authentication sha2 compatible enable

上一篇: AR3200流表超限导致业务时断时续 下一篇: AR2240C路由器链路负载不均衡如何解决

感谢您对我们知识库文章提供的宝贵意见

该知识库文章是否解决了您的问题： ○是 ○否 ◉只是浏览

*请您为该知识库文章评分: 很差 ☆☆☆☆☆ 非常好

意 见:

华为公司可能会与您联系，以便帮助您尽快解决问题，请填写您的联系信息:

联系人： 15501752377 *邮箱： 253202****@qq.com 电话： +86****377

修改 联系方式

提交

最近反馈

y******iao 2021-09-30 18:40:53 ★★★☆☆

ok

退出登录 >

意见反馈 | 收藏此案例

相关资源

文档

软件

产品公告

相关搜索

按作者

帮助我们改进

贡献案例