

知 ER3200G3与ER5200G2对接IPsec起不来经验案例

IPSec VPN 曹圣琪 2021-06-25 发表

组网及说明

组网: ER3200G3 (分支) ——ER5200G2 (总部), 两端设备外网口均为拨号口, 分支ping总部域名可通。

问题描述

1) 故障: ipsec起不来, ike已经建立

2) 配置:

【ER3200G3侧】

修改IPsec策略

名称 * (1-63字符)

接口 *

组网方式 * 分支节点 中心节点

对端网关地址 * (可输入IP地址或域名)

认证方式

预共享密钥 * (1-128字符)

保护流措施 *

序号	受保护协议	本端受保护网段/掩码	本端受保护端口	对端受保护网段/掩码	对端受保护端口	操作
1	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/> <input type="checkbox"/>
	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/> +

[显示高级配置...](#)

确定

取消

高级配置

IKE配置

IPsec配置

IKE 版本

协商模式

本端身份类型 (1-255字符)

对端身份类型 * (1-255字符)

对等体存活检测(DPD) 开启 关闭

算法组合

认证算法 *

加密算法 *

PFS *

SA生存时间 秒 (60-604800, 缺省值为86400)

高级配置

IKE配置

IPsec配置

算法组合

基于时间的SA生存时间 秒 (600-604800, 缺省值为3600)

基于流量的生存时间 千字节 (2560-4294967295, 缺省值为1843200)

触发模式

[返回基本设置](#)

IPsec VPN

IPsec 策略

监控信息

1) 两端需要补充到对端的私网路由

静态路由

查看路由信息表

请输入关键字自动查询

高级查询

<input type="checkbox"/>	目的地址	掩码长度	优先级	下一跳	出口
<input type="checkbox"/>		23	60		WAN1

当前显示第1页, 共1页。当前页共1条数据, 已选中0。每页显示: 10

序号	目的地址	掩码长度	优先级	下一跳	出口
11	192.168.50.0	255.255.255.0			ipsec6
12	192.168.60.0	255.255.255.0			ipsec4
13		255.255.255.0			ipsec3
14	192.168.91.0	255.255.255.0	192.168.98.2		VLAN1

2) 将ERG3上的保护流协议改为IP类型, ERG2只能配地址不支持选协议

3) ERG2 ipsec策略使能了PFS, ERG3侧没配置。将ERG2关闭ipsec策略的PFS, 修改配置后需要同时关闭策略再一起打开

绑定接口: WAN1

描述: 盐城

编辑IKB对等体

对等体名称: yancheng (范围:1~16个字符)

虚接口: ipsec3

对端地址: 0.0.0.0 (IP 或 域名)

协商模式: 主模式 野蛮模式

ID类型: IP类型 NAME类型

本端ID: nanjing (范围:1~32个字符)

对端ID: yancheng (范围:1~32个字符)

安全提议一: yc

安全提议二: 请选择

安全提议三: 请选择

安全提议四: 请选择

预共享密钥(PSK): 123456 (范围:1~128个字符)

生命周期: 28800 秒(范围:60~604800秒, 缺省值:28800)

DPD: 开启 关闭

DPD周期: 10 秒(范围:1~60秒, 缺省值:10)

DPD超时时间: 30 秒(范围:1~300秒, 缺省值:30)

编辑IPSEC安全提议列表

安全提议名称: yc (范围:1~31个字符)

安全协议类型: AH ESP AH+ESP

ESP验证算法: SHA1

ESP加密算法: 3DES

编辑 IPSEC 安全策略列表

安全策略名称: yancheng (范围:1~16个字符)

1) 两端补分到对端私网路由

2) 将 ERG3 侧的保护流协议改为 IP 类型

3) 关闭 ERG2 侧 ipsec 策略的 PFS 并将策略关闭再开启

是否启用: 启用

本地子网 IP/掩码: 255.255.254.0

对端子网 IP/掩码: 255.255.255.0

协商类型: IKE 协商 手动模式

对等体: yancheng

安全提议一: yc

安全提议二: 请选择

安全提议三: 请选择

安全提议四: 请选择

PFS: DH2 modp1024

生命周期: 28800 秒 (范围:120~604800, 缺省值:28800)

触发模式: 长连模式

3) 日志 (ER5200G2侧) :

```
2021-06-09 08:57:24 [debug]: 收到 [redacted] 的 IPSEC SA 协商请求。
2021-06-09 08:57:24 [debug]: 发送已加密的 INVALID_ID_INFORMATION 通告信息到 [redacted]
2021-06-09 08:58:14 [debug]: 收到 [redacted] 的 ISAKMP 野蛮模式协商请求。
2021-06-09 08:58:14 [inform]: 69.137.134: ISAKMP SA 建立完成 (加密算法=oakley_3des_cbc_192 认证算法=oakley_md5 DH 组=DH2(modp1024))。
2021-06-09 08:58:14 [debug]: 收到 [redacted] 的 IPSEC SA 协商请求。
2021-06-09 08:58:14 [debug]: 发送已加密的 INVALID_ID_INFORMATION 通告信息到 [redacted]
2021-06-09 08:59:10 [debug]: 收到 [redacted] 的 ISAKMP 野蛮模式协商请求。
2021-06-09 08:59:10 [inform]: 9.134: ISAKMP SA 建立完成 (加密算法=oakley_3des_cbc_192 认证算法=oakley_md5 DH 组=DH2(modp1024))。
2021-06-09 08:59:10 [debug]: 收到 [redacted] 的 IPSEC SA 协商请求。
2021-06-09 08:59:10 [debug]: 发送已加密的 INVALID_ID_INFORMATION 通告信息到 49.69.137.134:500。
2021-06-09 09:01:39 [debug]: 收到 [redacted] 的 ISAKMP 野蛮模式协商请求。
2021-06-09 09:01:39 [debug]: 发送 NO_PROPOSAL_CHOSEN 通告信息到 [redacted]
2021-06-09 09:02:08 [debug]: 收到 [redacted] 的 ISAKMP 野蛮模式协商请求。
2021-06-09 09:02:08 [debug]: 发送 NO_PROPOSAL_CHOSEN 通告信息到 [redacted]
```

