

知 ERG2固定地址跟ERG3不固定地址建立IPSec隧道典型配置案例

IPSec VPN 孙轶宁 2021-05-31 发表

组网及说明

总部为ERG2，有固定公网地址，分部为ERG3，通过PPPoE动态获取地址，现在总部和分部需要建立IPSec VPN实现内网互访需求。



配置步骤

ERG2配置

H3C H3C ER3200G2 路由器

安全联盟 虚接口 IKE安全提议 IKE对等体 IPsec安全提议 IPsec安全策略

系统导航 系统监控 接口管理 AP管理 上网管理 云WiFi 安全专区 VPN IPsec VPN L2TP VPN QoS设置 高级设置 设备管理 用户FAQ 退出

对等体名称: ipsec1 (范围:1~16个字符)
 虚接口: ipsec1
 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: G2 (范围:1~32个字符)
 对端ID: G3 (范围:1~32个字符)
 安全提议一: DC
 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): 12345 (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)

修改 取消

H3C H3C ER3200G2 路由器

安全联盟 虚接口 IKE安全提议 IKE对等体 IPsec安全提议 IPsec安全策略

安全提议

安全提议的配置修改后, 需要重新启用(先禁用再启用)引用该安全提议的IPSEC安全策略或重新使能IPSEC功能, 新的配置才能生效。

关键字: 名称

操作	序号	名称	认证算法	加密算法	DH组
	1	XZKJ	MD5	3DES	DH2 modp1024
	2	DC	MD5	3DES	DH1 modp768

第 1 页/共 1 页 共 2 条记录 每页 10 行 1 Go

编辑IPSEC安全策略列表

安全策略名称: DC (范围:1~16个字符)
 是否启用: 启用
 本地子网IP/掩码: 192.168.1.0 / 255.255.255.0
 对端子网IP/掩码: 192.168.20.0 / 255.255.255.0
 协商类型: IKE协商 手动模式
 对等体: ipsec1
 安全提议一: XZKJ-ESP
 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: 禁止
 生命周期: 28800 秒(范围:120~604800, 缺省值:28800)
 触发模式: 流量触发

修改 取消

安全提议

安全提议的配置修改后, 需要重新启用(先禁用再启用)引用该安全提议的IPSEC安全策略或重新使能IPSEC功能, 新的配置才能生效。

关键字: 名称

操作	序号	名称	安全协议	AH算法	ESP算法
	1	XZKJ-ESP	ESP	----	3DES-MD5

第 1 页/共 1 页 共 1 条记录 每页 10 行 1 Go

H3C H3C ER3200G2 路由器

安全联盟 虚接口 IKE安全提议 IKE对等体 IPsec安全提议 IPsec安全策略

系统导航
系统配置
安全策略
VPN
QoS设置
高级搜索

虚接口

虚接口的配置修改后，需要重新启用(先禁用再启用)引用该虚接口的IPsec安全策略或重新使能IPSEC功能，新的配置才能生效。

为在不清楚对端地址的时候，对等体填写全零即可，类似MSR的ipsec policy-template

ERG2侧安全提议/虚接口的配置修改后，需要重新启用（先禁用再启用）引用该安全提议/虚接口的ipsec安全策略或重新使能ipsec功能，新的配置才能生效。

ERG3侧同样在修改后，禁用重新启用“管理状态”。

操作	序号	名称	绑定接口	描述
		WAN1		ipsec0
		WAN1		ipsec1

第 1 页 / 共 1 页 共 2 条记录 每页 10 行 1 Go