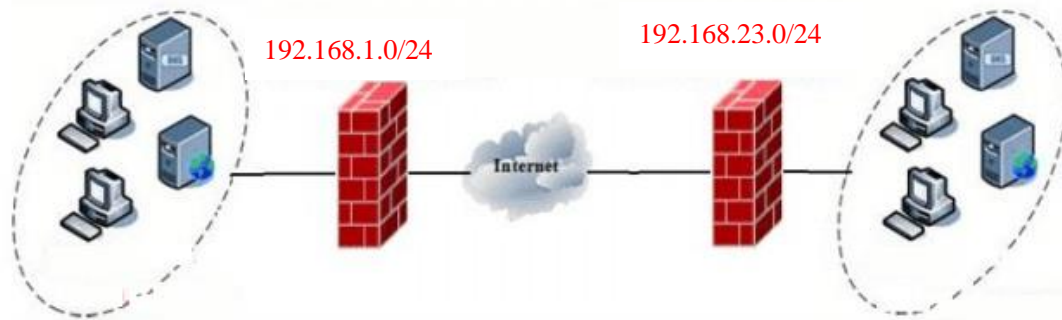


用户场景

企业通过 H3C 和启博设备构建 VPN 通道，保证总部和分支机构的安全通信，均作为出口网关。

中心用 H3C 设备，网段 92.168.1.0/24

分支用启博设备，网段 192.168.23.0/24



H3C 作为网关，主要参数设置如下

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

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

全选 新增 删除 关键字: 名称 查询 显示

操作	序号	名称	绑定接口	描述
	1	ipsec0	WAN1	test

编辑虚接口列表

虚接口名称: ipsec0

绑定接口: WAN1

描述: test

修改 取消

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

全选 新增 删除 关键字: 名称 查询 显示全部

操作	序号	名称	认证算法	加密算法	DH组
	1	test1	MD5	3DES	DH2 modp1024

编辑IKE安全提议列表

安全提议名称: test1 (范围:1~16个字符)

IKE验证算法: MD5

IKE加密算法: 3DES

IKE DH组: DH2 modp1024

修改 取消

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

对等体

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

全选 新增 删除 关键字: 名称 查询 显示全部

操作	序号	名称	虚接口	对端地址	模式	ID类型	安全提议	DPD
	1	dg	ipsec0	0.0.0.0	野蛮模式	NAME	test1	开启

编辑IKE对等体

对等体名称: dg (范围:1~16个字符)

虚接口: ipsec0 如果没有公网IP填0.0.0.0

对端地址: 113.116.120.161 (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: dg (范围:1~32个字符)

对端ID: sz (范围:1~32个字符)

安全提议一: test1

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: 3600 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

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。

全选 新增 删除 关键字: 名称 查询 显示全部

操作	序号	名称	安全协议	AH算法	ESP算法
	1	test2	ESP	----	3DES-MD5

编辑IPSEC安全提议列表

安全提议名称: test2 (范围:1~31个字符)

安全协议类型: AH ESP AH+ESP

ESP验证算法: MD5

ESP加密算法: 3DES

修改 取消

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**

启用IPSec功能

安全策略
虚接口、IKE安全提议、IKE对等体和IPSec安全提议的配置都修改完成后，只需要重新启用(先禁用再启用)相关的IPSec安全策略一次或重新使能IPSEC功能一次，新的配置就能生效；另外，修改IPSEC安全策略的配置也能使新的配置生效。

安全策略列表

操作	序号	名称
	1	ceshi

编辑IPSec安全策略列表

安全策略名称: (范围:1~16个字符)

是否启用:

本地子网IP/掩码: /

对端子网IP/掩码: /

协商类型: IKE协商 手动模式

对等体:

安全提议一:

安全提议二:

安全提议三:

安全提议四:

PFS:

生命周期: 秒 (范围:120~604800, 缺省值:28800)

触发模式:

组网成功之后，可以看到两边的信息

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**

安全联盟SA
通过安全联盟SA，IPSec能够对不同的数据流提供不同级别的安全保护。在这里可以查询到相应隧道当前状态，了解隧道建立的各个参数。

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
ceshi	out	183.63.111.0/24 =>113.116.120.161	----	----	0xd7480e00	3DES_MD5	192.168.1.0/24 =>192.168.23.0/24
ceshi	in	113.116.120.161 =>183.63.111.0/24	----	----	0xc3904124	3DES_MD5	192.168.23.0/24 =>192.168.1.0/24

第 1 页 / 共 1 页 共 2 条记录

添加静态路由

静态路由 | 策略路由

静态路由表

关键字:

操作	序号	目的地址	子网掩码	下一跳地址	出接口	描述
	1	10.0.0.0	255.0.0.0	192.168.1.4	VLAN1	epn10
	2	192.168.2.0	255.255.255.0	192.168.1.4	VLAN1	VPN2
	3	192.168.3.0	255.255.255.0	192.168.1.4	VLAN1	VPN3
	4	192.168.10.0	255.255.255.0	192.168.1.4	VLAN1	vpn10
	5	172.16.255.0	255.255.255.0	192.168.1.4	VLAN1	考勤
	6	192.168.23.0	255.255.255.0	192.168.1.4	ipsec0	sz

第 1 页 / 共 1 页 共 6 条记录 每页 10 行

MR-1300 作为网关上网, 的所有配置参数 (当二级路由和透明模式也可以的)

添加IPSEC连接

类型:

IPSEC功能: 客户端 服务端

名称:

启用:

本端WAN接口:

本端子网:

本端标志符:

对端地址:

对端子网:

对端标志符:

启用DPD检测:

时间间隔: (秒) 超时时间: (秒) 操作:

第一阶段
 加密: 完整性: DH小组: 生命周期: 小时

第二阶段
 加密: 完整性: 生命周期: 小时

模式:

会话密钥向前加密(PFS):

使用预共享密钥:

组网成功之后会显示建立

编号	名称	类型	通用名称	状态	操作
1	sztest	隧道-client	192.168.23.0/24--[null] 183.63.1.1--[192.168.1.0/24]	建立	

[添加](#)