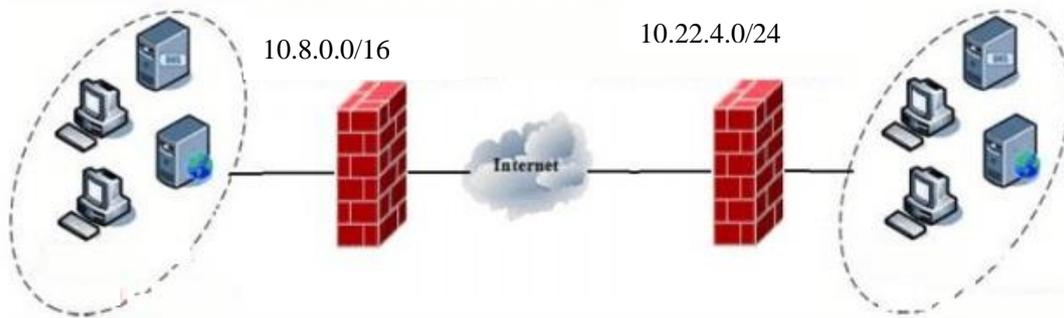


用户场景

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

中心用深信服设备，网段 10.8.0.0/16

分支用启博设备，网段 10.22.4.0/24



深信服设备 VPN-2050 ipsec 参数设置

高级选项 -- 网页对话框

ISAKMP存活时间:	3600	秒
重域次数:	10	
支持模式:	野蛮模式	
D-H群:	MODP1024群(2)	
我方身份类型:	域名字符串(FQDN)	
我方身份ID:	server	
对端身份类型:	域名字符串(FQDN)	
对方身份ID:	faker	
<input checked="" type="checkbox"/> 启用DPD	<input checked="" type="checkbox"/> 启用NATT穿透	
DPD/NATT设置		
检测间隔:	5	秒(5-60)
超时次数:	5	次(1-6)
ISAKMP算法列表		
认证算法:	MDS	加密算法:
		3DES

入站策略设置 -- 网页对话框

策略名称: qibo

描述:

源IP类型: 子网+掩码

子网: 10.22.4.0

掩码: 255.255.255.0

对端设备: qibo

入站服务: 所有服务

生效时间: 全天

在时间生效范围内允许 在时间生效范围内拒绝

启用过期时间

过期时间: 0-00-00 0 : 0 : 0

启用该策略

确定 取消

出站策略设置 -- 网页对话框

策略名称: qibo

描述:

源IP类型: 子网+掩码

子网: 10.8.0.0

掩码: 255.255.0.0

对端设备: qibo

SA生存时间: 28800 秒

出站服务: 所有服务

安全选项: qibo

生效时间: 全天

在时间生效范围内允许 在时间生效范围内拒绝

启用过期时间

过期时间: 0-00-00 0 : 0 : 0

启用该策略

启用密钥完美向前保密

确定 取消



启博 MR-1200-C ipsec 参数设置

注意标识符务必带@ 如图例:@faker、@server



对接成功会显示“建立”

网络 转发规则 第三方互联 VPN 路由功能 EPN 无线 上网行为管理 防火墙 系统管理 状态

第三方互联

IPSEC设置

编号	名称	类型	通用名称	状态	操作
1	test	隧道-client	10.22.4.0/24-[(null)] 180.168.198.2-[10.8.0.0/16]	建立	   

添加

IPSEC设置
L2TP客户端
L2TP服务端
PPTP客户端
PPTP服务端
IPSEC日志
L2TP状态
PPTP状态