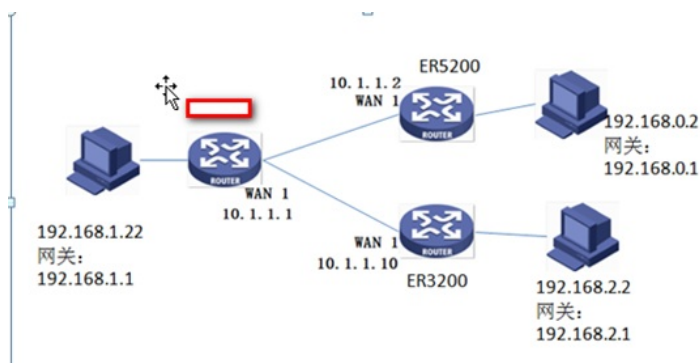


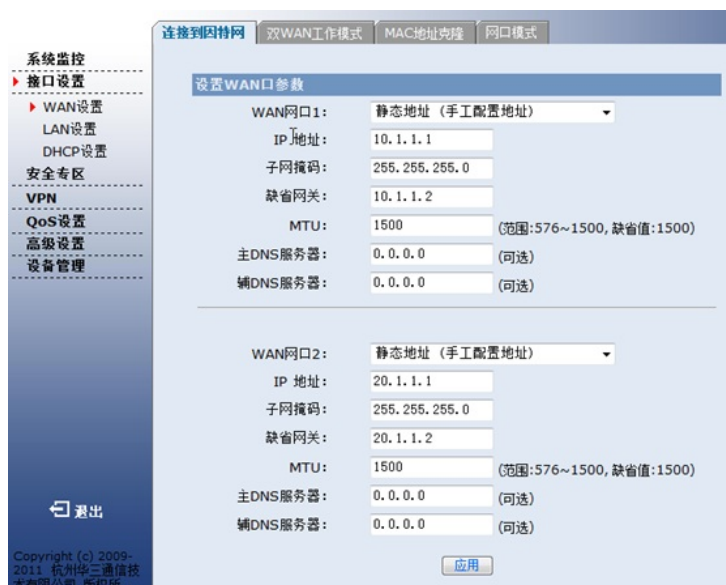
ER路由器间实现IPSEC VPN配置案例

王鑫 2015-10-25 发表

某公司需求总部路由器（WAN 1）ER6300要分别和ER5200，ER3200建立IPSEC VPN，组网图如下：



ER6300 配置：
WAN口设置：



LAN口设置：



设置虚接口：设置两个虚接口IPSEC 0和IPSEC1用来和分别和ER5200，ER3200建立VPN



设置IKE安全提议123，认证算法选择MD5，加密算法选择3DES，DH组选择DH2



设置两个IKE对等体，对等体10.1.1.2对端地址为ER5200的WAN 1口地址，虚接口为IPSEC0。对等体10.1.1.10的对端地址为ER3200的WAN 1地址10.1.1.10，虚接口为IPSEC1，两个对等体的协商模式都为主动模式（两端为静态IP），IKE安全提议为之前创建好的123，预共享密钥设置为123456



设置IPSEC安全提议456：选择协议ESP，加密算法为3DES，验证算法为MD5



设置两条IPSEC安全策略：第一条安全策略的对等体为10.1.1.2，本地子网设置为ER6300的局域网192.168.1.0/24，对端子网为ER5200的局域网192.168.0.0/24，协商类型采用IKE协商，安全策略采用之前创建好的456。第二条安全策略的对等体为10.1.1.10，本地子网设置为ER6300的局域网192.168.1.0/24，对端子网为ER3200的局域网192.168.2.0/24，协商类型采用IKE协商，安全策略采用之前创建好的456



设置静态路由：

设置两条静态路由：第一条目的地址为ER5200的局域网192.168.0.0/24，出接口为IPSEC0，第二条目的地址为ER3200的局域网192.168.2.0/24，出接口为IPSEC 1



ER5200配置:

WAN口设置:



LAN口设置:



虚接口设置:



设置IKE安全提议123: 认证算法选择MD5, 加密算法选择3DES, DH组选择DH2



设置对等体: 对等体10.1.1.1对端地址为ER6300的WAN 1口地址10.1.1.1, 虚接口为IPSEC0等体的协商模式都为主动模式 (两端为静态IP), IKE安全提议设置为之前创建好的123, 预共享密钥设置为1234



设置IPSEC安全提议：选择协议ESP，加密算法为3DES，验证算法为MD5



设置IPSEC安全策略：安全策略的对等体为10.1.1.1，本地子网设置为ER5200的局域网192.168.0.0/24，对端子网为ER6300的局域网192.168.1.0/24，协商类型采用IKE协商，安全策略采用之前创建好的456。



设置静态路由：目的地址为ER6300的局域网192.168.1.0/24，出接口为IPSEC0



ER3200配置：
WAN设置：



LAN设置：



设置虚接口IPSEC 0:



设置IKE安全提议: 认证算法选择MD5, 加密算法选择3DES, DH组选择DH2



设置IKE对等体: 对等体10.1.1.1对端地址为ER6300的WAN 1口地址10.1.1.1, 虚接口为IPSEC0。对等体的协商模式都为主动模式 (两端为静态IP), IKE安全提议设置为之前创建好的123, 预共享密钥设置为123456



设置IKE安全提议: 选择协议ESP, 加密算法为3DES, 验证算法为MD5



设置IKE安全策略：安全策略的对等体为10.1.1.1，本地子网设置为ER3200的局域网192.168.2.0/24，对端子网为ER6300的局域网192.168.1.0/24，协商类型采用IKE协商，安全策略采用之前创建好的456



设置静态路由：目的地址为ER6300的局域网地址192.168.1.0/24，出接口为IPSEC0



测试结果：

ER3200的VPN状态



ER5200的VPN状态



ER6300的VPN状态



总部路由器需要设置两个虚接口，两个对等体，两个IPSEC安全策略用来建立两条隧道