**ERG2路由器IPSEC野蛮模式典型配置**

# 组网需求

在某公司总部出口路由器ER8300G2和分支出口路由器ER6300G2路由器之间建立IPSEC隧道，同来对总部私网网段192.168.2.0/24和分支私网网段192.168.1.0/24之间的数据流量进行安全保护。

* 两个出口路由器之间利用IKE野蛮模式协商建立IPSEC SA。
* 使用缺省的IKE提议。
* 使用缺省的预共享秘钥认证方法。

# 组网图

下图为ER8300G2和ER6300G2的IPSEC组网图：



# 配置步骤

## ER8300G2配置

# 配置LAN口地址，作为总部内网的网关地址





#配置WAN口地址，作为总部出口地址



#配置虚接口，绑定到WAN1口上





#配置IKE安全提议p1



#配置IKE对等体，将总部本端对等体标识为rta，调用ipsec0虚接口，选用野蛮模式，如果分支对等体无静态地址则不用填写对端地址，如果分支有静态地址则填写分支地址为对端地址，填写分支对等体标识名rtb，调用安全提议p1，使用预共享秘钥h3c



#配置IPSEC安全提议po1



#配置IPSEC安全策略ppp，填写被保护的数据流，总部私网到分支私网的网段，填写本端标识名rta，调用安全提议po1，注意最后一定要启用安全策略





#配置总部到分支私网的静态路由，出接口为虚接口ipsec0口





## ER6300G2配置

# 配置LAN口地址，作为分支内网的网关地址





#配置WAN口地址，作为分支出口地址，如果分支没有固定静态地址，也可选用PPPoE拨号或者动态地址



#配置虚接口，绑定到WAN1口





#配置IKE安全提议p1



#配置IKE对等体，将分支本端对等体标识为rtb，调用ipsec0虚接口，填写总部的静态地址100.1.1.1，然后选用野蛮模式，填写总部对等体标识名rta，调用安全提议p1，使用与总部相同的预共享秘钥h3c



#配置IPSEC安全提议po1



#配置IPSEC安全策略ppp，填写被保护的数据流，分支私网到总部私网的网段，填写本端标识名rtb，调用安全提议po1，注意最后一定要启用安全策略





#配置分支到总部私网的静态路由，出接口为虚接口ipsec0口





# 验证配置

## 结果验证

完成上述配置之后，在总部PC上ping分支的PC，将会有数据流触发IPSEC隧道，IPSEC隧道成功建立，现象如下：



先在分支PC2上ping分支PC1，分支成功访问总部，现象如下：



然后在总部PC1上ping分支PC2，总部成功访问分支，现象如下：



## 结论

ERG2路由器IKE野蛮模式典型配置，使用对等体标识ID寻找对端，因为ERG2设备是web页面操作，所以操作时要注意两边的协商类型、加密算法和预共享秘钥等参数要保持一致，正确的配置被保护数据流的网段和去往私网网段的静态路由。

# 关键配置点

在配置完成后，如果是分支没有固定地址的情况，则需要分支内网PC主动ping总部内网PC，才能触发隧道建立；ERG2路由器有防WAN口ping扫描功能，如果需要ping路由器WAN口地址，则需要关闭此功能，功能目录如下所示：



