ERG2--MSR93X系列 V7 WEB界面ipsec 主模式

IPSec VPN　李章华　2019-09-22 发表

组网及说明

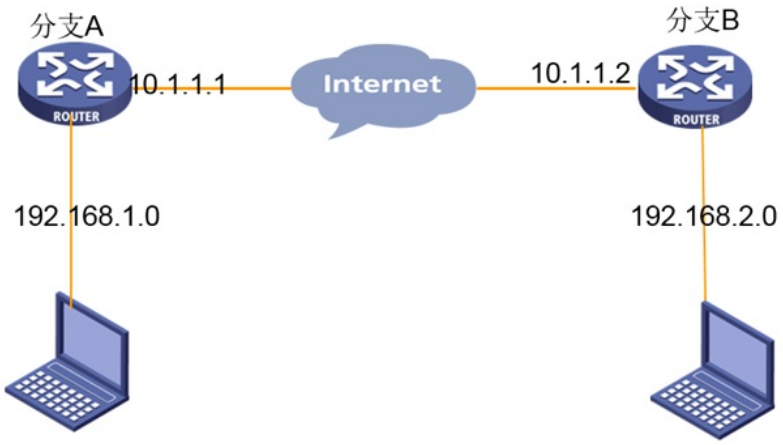
1 配置需求或说明

1.1适用产品系列

本案例适用于ERG2 产品系列路由器：ER8300G2-X、ER6300G2、ER3260G2、ER3200G2等，Comware V7平台的MSR830-WiNet系列路由器，如MSR830-10BEI-WiNet 、MSR830-6EI-WiNet 、MSR830-5BEI-WiNet 、MSR830-6BHI-WiNet 、MSR830-10BHI-WiNet等。MSR版本：0605P20

1.2配置需求及实现的效果

在总部和分部之间分别建立安全隧道，对客户总部PC所在的子网（192.168.2.0）与客户分支机构PC所在的子网（192.168.1.0）之间的数据流进行安全保护。安全协议采用ESP协议，加密算法采用3DES，认证算法采用MD5。



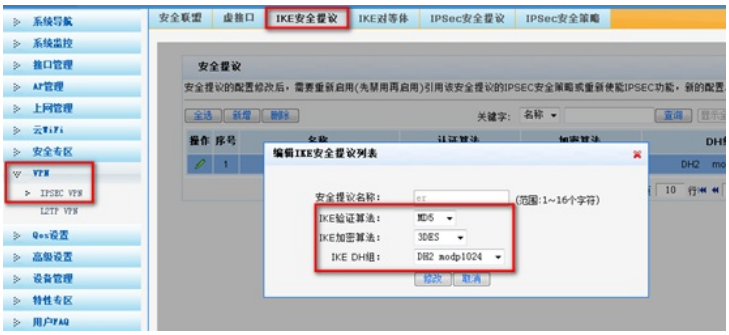
配置步骤

3 配置步骤

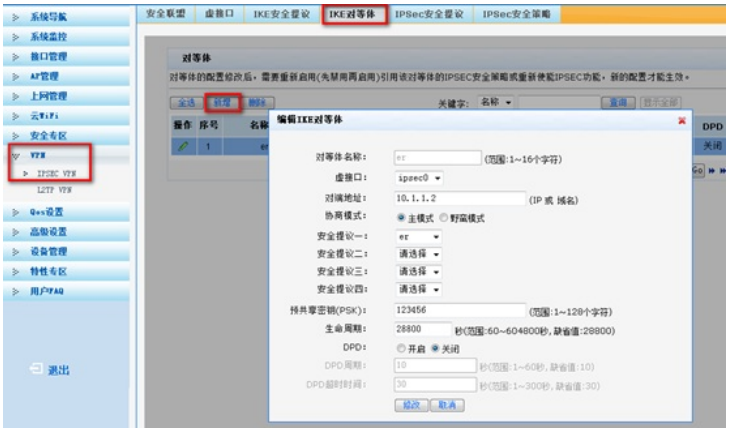
3.1配置ER G2路由器

#选择“VPN→IPSEC VPN→虚接口”。单击<新增>按钮，在弹出的对话框中选择一个虚接口通道，并将其与对应的出接口进行绑定，单击<增加>按钮完成操作

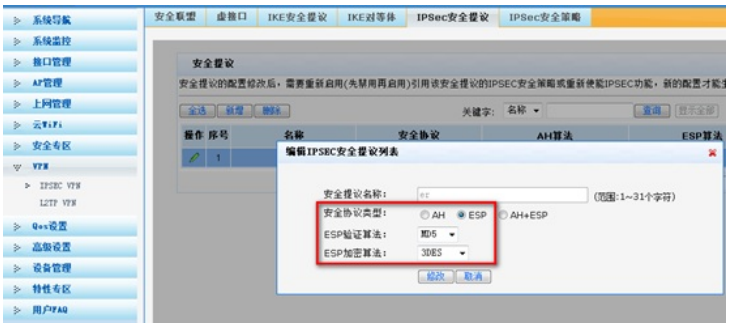
#选择“VPN→IPSEC VPN→IKE安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



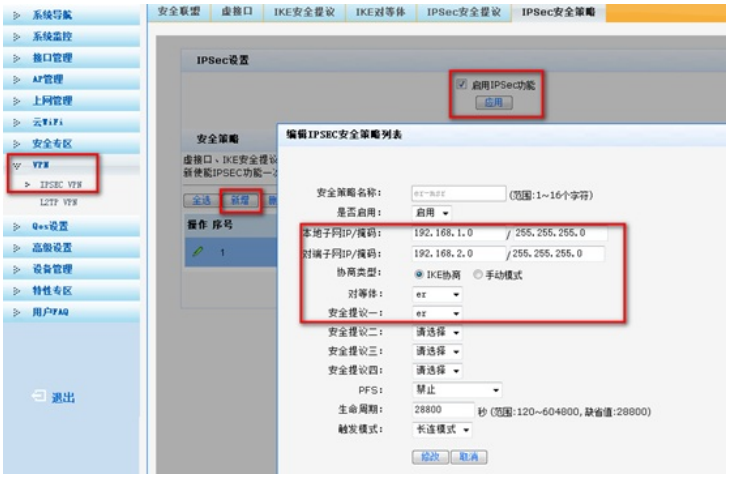
#选择“VPN→IPSEC VPN→IKE对等体”。单击<新增>按钮，在弹出的对话框中输入对等体名称，选择主模式，选择对应的虚接口。在对端地址填写对端的IP或者域名，并选择已创建的安全提议信息，预共享密钥和MSR侧保持一致，单击<增加>按钮完成操作



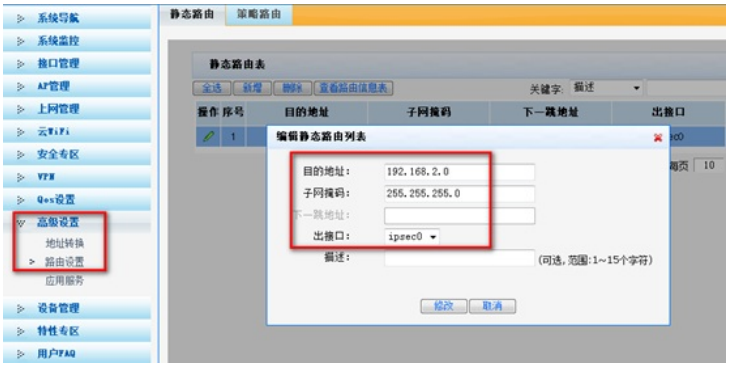
#选择“VPN→IPSEC VPN→IPSec安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



#选择“VPN→IPSEC VPN→IPSec安全策略”。选中“启用IPSec功能”复选框，单击<应用>按钮生效。单击<新增>按钮，在弹出的对话框中输入安全策略名称，在“本地子网IP/掩码”和“对端子网IP/掩码”文本框中分别输入两端对应子网信息，并选择协商类型，对等体，安全提议，单击<增加>按钮完成操作

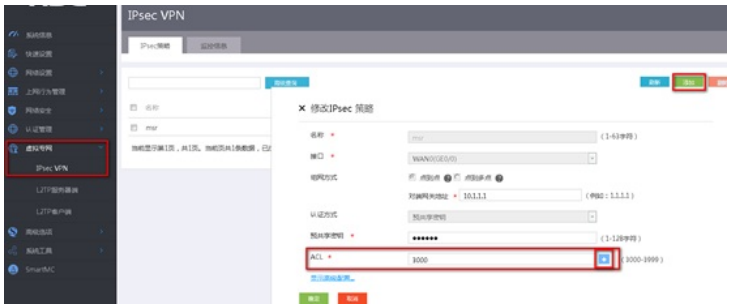


#为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择“高级设置→路由设置→静态路由”，单击<新增>按钮，在弹出的对话框中，设置目的地址、子网掩码等参数，单击<增加>按钮完成操作



3.2配置MSR路由器

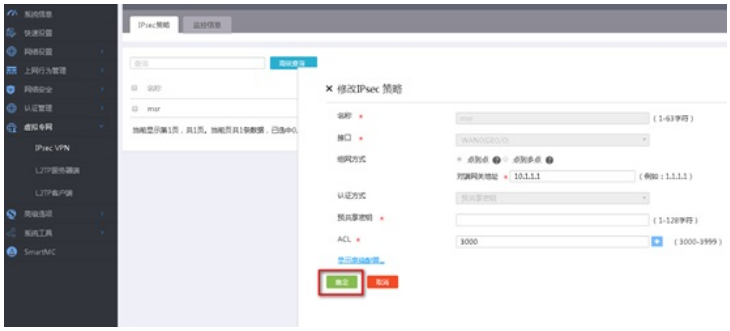
#选择“虚拟专网→IPSEC VPN→Ipsec策略”。单击<添加>按钮，在弹出的对话框中填写ipsec策略名称，单WAN默认选择WAN口，多WAN要手动选择对应WAN口，组网方式选择点到点，对端地址填写对端的IP，预共享密钥和ER侧填写一致，ACL数字写3000以上的，点击ACL后的“+”进入ACL配置页面。



#进入ACL配置页面选择受保护的协议为IP，填写两端ipsec网段信息，注意后面填写为反掩码，点击<添加>按钮添加，可以添加多条规则，完成后点击<显示高级配置>按钮进入高级配置。

#高级配置IKE配置协商模式选择主模式，本端身份类型和对端身份类型选择IP,填写两端WAN口地址，算法组合与ER侧一致，验证算法、加密算法和PFS分别为MD5、3DES、DH2，单击<Ipsec配置>按钮进行下一步操作

#Ipsec配置算法组合和ER侧保持一致，安全协议、认证算法和加密算法分别为：ESP、MD5、3DES，封装模式为隧道模式，单击<返回基本配置>按钮进入基本配置后点击<确定>完成配置。



4 验证配置

#查看VPN状态

两端均设置完成后，保护流ping后建立隧道。您可以通过选择ER路由器的“VPN→IPSEC VPN→安全联盟”页面，MSR的“ 虚拟专网→IPSEC VPN→监控信息”，并单击<刷新>按钮来查看相应的隧道是否已成功建立。

ER隧道建立图

MSR隧道建立图

配置关键点