# IPSec的2种模式2种冗余备份和几种应用典型组网

播报文章

网络安全学习
2021-11-09 13:02

关注

IPSec传输模式和隧道模式的区别在于：

1、从安全性来讲，隧道模式优于传输模式。它可以完全地对原始IP数据报进行验证 和加密。隧道模式下可以隐藏内部IP地址，协议类型和端口。

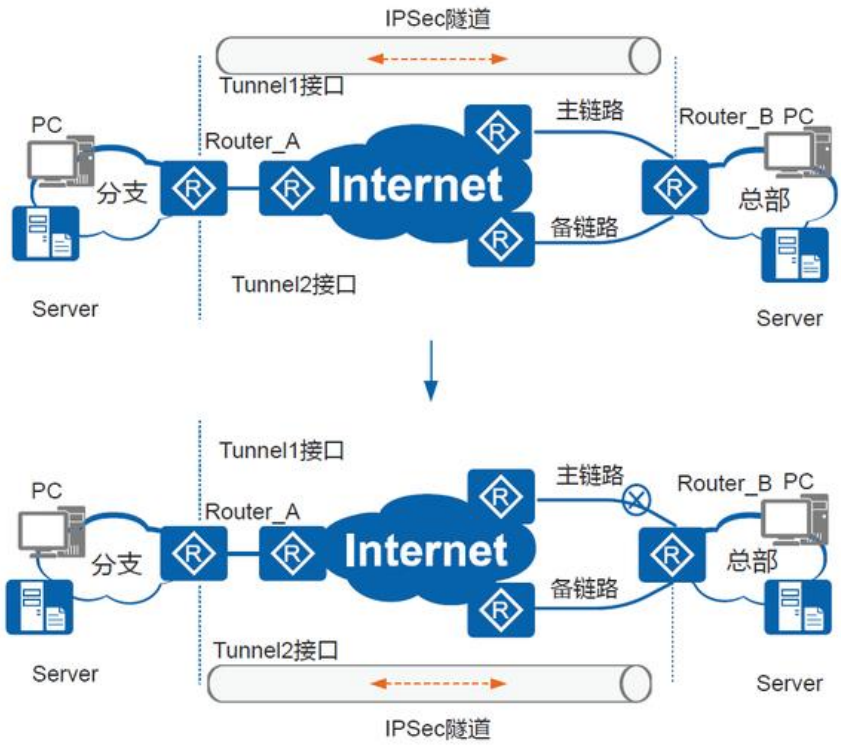
2、从性能来讲，隧道模式因为有一个额外的IP头，所以它将比传输模式占用更多带 宽。

3、从场景来讲，传输模式主要应用于两台主机或一台主机和一台VPN网关之间通 信；隧道模式主要应用于两台VPN网关之间或一台主机与一台VPN网关之间的通 信。

当安全协议同时采用AH和ESP时，AH和ESP协议必须采用相同的封装模式。

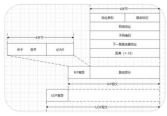
**IPSec**主备链路冗余备份

Router_A通过主备两条链路连接Router_B。在Router_A上创建两个Tunnel接口，借用同一个物理接口的IP地址，分别应用不同的IPSec安全策略，在Router_B的两个物理接口上也分别应用不同的IPSec安全策略，这样可以创建主备两条IPSec隧道。正常情况下，流量通过由主链路和Tunnel1接口建立的IPSec隧道传输；当主链路故障时，Router_A感知变化，采用Tunnel2接口与Router_B的备份链路建立IPSec隧道，旧的IPSec隧道被拆除，流量切换也随之完成。如下图




**IPSec** 多链路冗余备份

## 作者最新文章



内部网关协议RIP的相关知识与应用

2022-03-30 24阅读

外网不能访问内网FTP服务器报错解...

2022-02-17 216阅读

华为路由器系列介绍

2021-10-17 605阅读

## 相关推荐

发那科数控系统采集网关WTGNet-...

望天观科技

一个总部，两个异地分公司，三台华为...

IT狂人日志

工业机器人远程监控解决方案

北京东用科技有限公司


各大平台公开的“IP属地”，能准确知...

北京科技报

城市燃气管网无线监测方案

北京东用科技有限公司

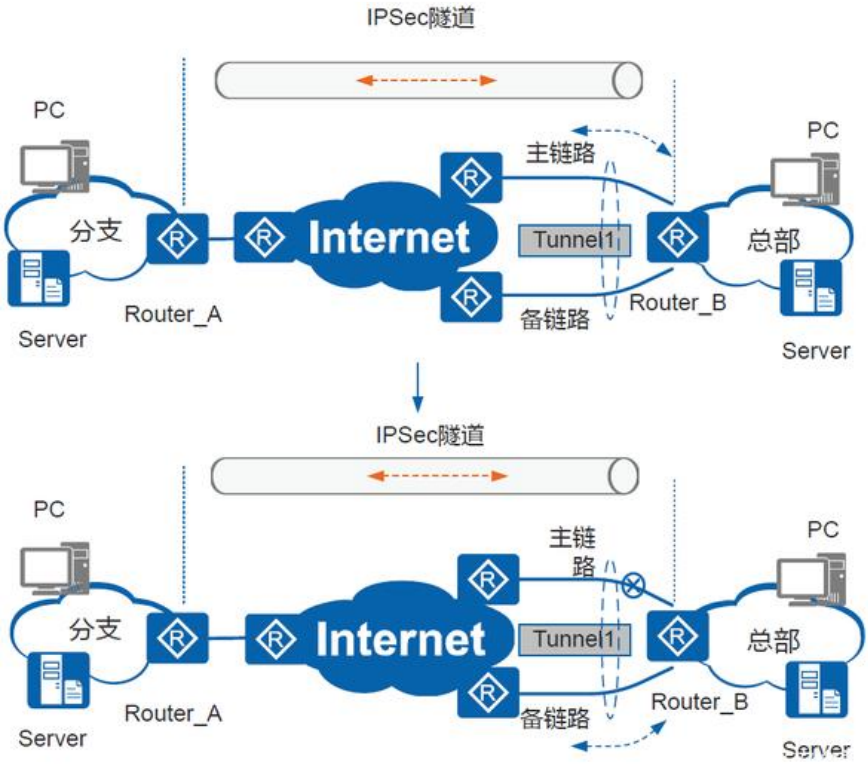
## 百度热搜

换一换

1 中国孩子用三国演义谈俄乌冲突
2 上海又一检测机构核酸准确性遭...
3 #又是一年512# 热
4 iPod在中国官网售罄
5 周杰伦的《稻香》是写给汶... 新
6 朝鲜首现新冠确诊病例 全国... 热
7 金正恩首次戴口罩出席会议 新
8 云南过桥米线肉片厚度不能... 新
9 长沙17层楼楼顶被曝建千余平厂房
10 谷爱凌称已信仰佛教

Bai du 百度 百度首页 登录

下，IPSec隧道不需要进行重协商，故可快速完成流量切换。

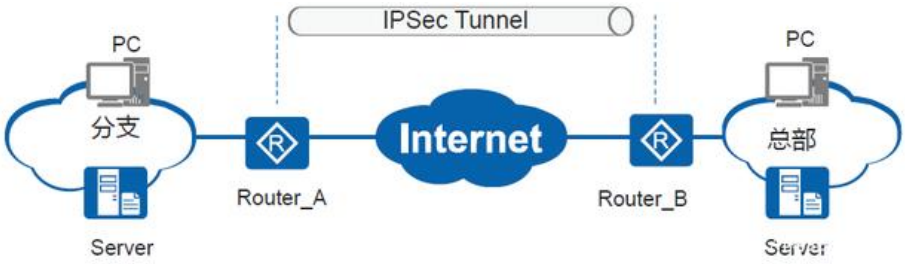



注：通过Tunnel接口进行链路冗余备份可以实现多条链路的冗余备份，而且与主备链路冗 余备份相比，配置更简单，流量切换速度更快。

**IPSec** 应用场景

点到点 **VPN—IPSec**

点到点VPN也称为局域网到局域网VPN，网关到网关VPN，主要用于两个网关之间建 立IPSec隧道，从而实现局域网之间安全地互访。点到点VPN两端网关必须提供固定的IP地址或固定的域名。通信双方都可以主动发起 连接。

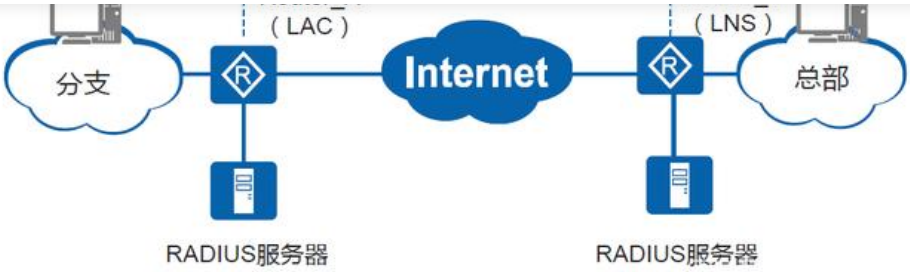



点到点 IPSec VPN 典型组网

点到点 **VPN—L2TP over IPSec**

L2TP over IPSec，即先将报文用L2TP封装再用IPSec传输。L2TP和IPSec这两种VPN经 常一起使用，可以实现优势互补。L2TP用于拨号并获取总部内网的IP地址，但是L2TP 本身不够安全，正好可以通过IPSec保障通信的安全性。L2TP over IPSec适用于分支网 络通过LAC拨号接入VPN并进行安全访问的场景。分支接入总部的L2TP over IPSec组网如图所示。LAC和LNS的出接口IP地址固定， 分支用户通过PPPoE拨号到LAC。由LAC通过Internet向LNS发起建立隧道连接请求。在 LAC和LNS之间建立L2TP over IPSec隧道。LAC侧对用户的身份进行验证，LNS侧还可 以对用户的身份进行二次验证。验证通过后由LNS为接入用户分配总部内网的IP地址。

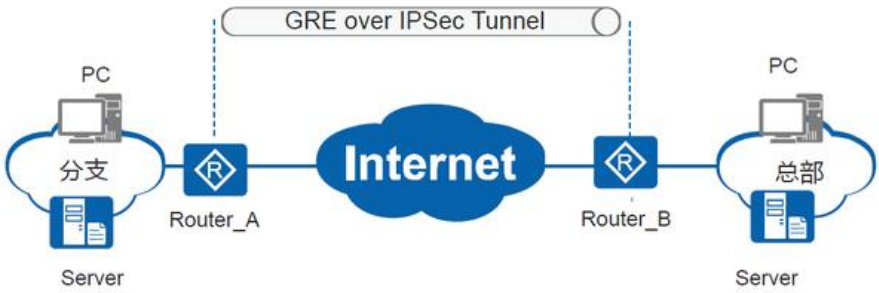
百度首页 登录




分支通过 L2TP over IPSec 接入总部网络

点到点 **VPN - GRE over IPSec**

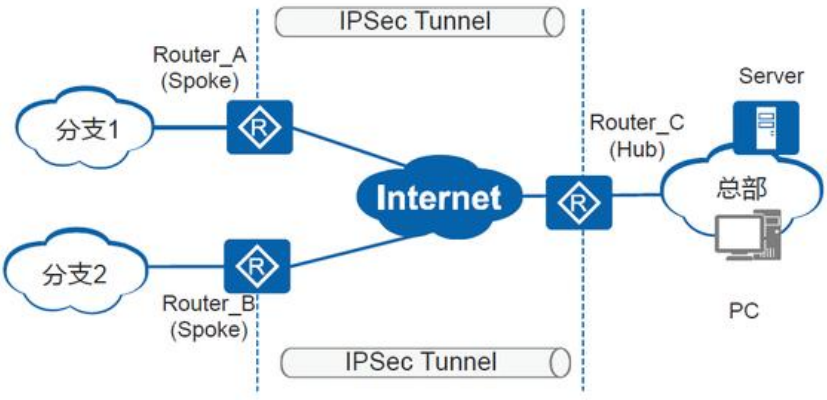
GRE是常用的隧道封装协议，可以很好的实现对于组播、广播和非IP报文的数据承 载，但是GRE只有简单的密码验证，没有加密功能，数据传输安全性较低。IPSec虽具 备很高的数据安全传输能力，但其本身不支持封装组播、广播和非IP报文。当需要在 IPSec VPN上传输组播、广播和非IP报文时，如在总部和分支之间开视频会议等组播业 务，可以采用GRE over IPSec。GRE over IPSec利用了GRE和IPSec的优势，利用GRE将 组播、广播和非IP报文封装成普通的IP报文，通过IPSec将封装后的IP报文安全地传 输。GRE over IPSec使用的封装模式为可以是隧道模式也可以是传输模式。因为隧道模式跟 传输模式相比多增加了IPSec头，导致报文长度更长，更容易导致分片。所以推荐采用 传输模式GRE over IPSec。




GRE over IPSec 组网图

点到多点 **VPN（Hub-Spoke VPN）**

实际组网中最常见的是公司总部与多个分支机构通过点到多点IPSec VPN互通，典型组 网如所示




点到多点 IPSec VPN 典型组网

总部的IP地址通常为固定公网IP地址或提供固定域名，分支的IP地址可以为静态公网IP 也可以为内网IP或动态公网IP。此时网络内数据流量可能存在如下几种情况：

各分支机构之间不需要通信 此时只需要在总部和分支之间部署IPSec VPN。

源紧张；另外，总部要对分支间的流量进行封装和解封装，会引入额外的网络延 时。通过部署DSVPN可以解决Hub-Spoke组网方式下动态IP的分支之间建立VPN隧道的 难题，但由于mGRE隧道本身不具备安全加密功能，无法保证通信安全。因此， 可以在部署DSVPN的同时绑定IPSec安全框架，即部署DSVPN over IPSec，以此达 到安全通信的目的。

举报/反馈

## 发表评论

发表神评妙论

发表

设为首页 © Baidu 使用百度前必读 意见反馈 京ICP证030173号
京公网安备11000002000001号