文章编号:1674－2869(2015)06－0073－06

虚拟专用网中语音电话的应用及网络性能

李清平
浙江育英职业技术学院信息技术与应用系,浙江 杭州 310018

摘　要:为研究虚拟专用网(VPN)基于 Internet 协议安全性(IPSec)进行语音电话(VoIP)数据的输送及网络性能的影响,在分析 IPSec 技术、隧道封装技术和 VPN 技术原理的基础上,设计了一个企业的 VPN 网络拓扑,对语音路由器、语音交换机和外网服务器的配置及其作用进行了说明,利用 OPNET 平台对网络性能进行了仿真和分析.结果表明,VPN 的隧道封装技术以及数据机密性、数据完整性、起源认证等加密措施使得网络配置变得复杂,语音数据在 VPN 隧道的传输过程中,丢包率不高,但传输速率变得缓慢,网络延迟加大,IPSec 采用的安全策略导致网络抖动明显,收敛速度慢,语音质量也随之减低.

关键词:协议安全性;虚拟专用网;语音电话;网络性能;网络延迟
中图分类号:TP391　　**文献标识码**:A　　**doi**:10. 3969/j. issn. 1674-2869. 2015. 06. 015

0　引　言

基于 TCP/IP 体系的 Internet 存在网络安全的缺陷,企业通过 Internet 来连接远程站点和传输数据,容易对内部网络构成安全威胁.IPSec-VPN 技术能够让企业在互联网的基础上创建私有网络来提供机密性和安全性[1-4].目前,采用 IPSec 标准的VPN 技术日臻成熟,得到国际上几乎所有主流网络和安全供应商的鼎力支持,可以断定,IPSec 将成为未来相当一段时间内企业构筑 VPN 的主流标准[1-4].

VoIP 将模拟的语音讯号经过压缩与封包之后,经过 IP 网络将数据包传送到目的地.VoIP 可以低资费甚至免费传送语音、传真和视频等业务,提供比传统业务更多、更好的服务[5-6].因此,一方面在企业内部尤其是远程站点中,VoIP 的应用具有机密性和安全性的需求, 利用现有的 IPSec-VPN 技术来提供支持和保障,不失为一种便捷经济的选择,另一方面由于加载 VoIP 负荷而对网络性能产生的影响以及语音在虚拟专用网中的传输质量也是需要考量的因素.

1　技术原理和隧道封装模式

1.1　工作原理

IPSec 的工作原理类似于包过滤防火墙,当接收到一个 IP 数据包时,通过查询 SPD(Security Policy Database,安全策略数据库)决定对数据包进行丢弃或转发的处理[1,7].通信双方如果用 IPSec 建立一条安全的传输通道,需要双方事先协商好采用的安全策略,包括加密算法、密钥、密钥的生存期等,安全策略可以由 AH 或 ESP 提供.IPSec 既可以仅对 IP 数据包进行加密或认证,也可以同时实施二者,但无论是加密还是认证,其工作模式都有两种:传输模式和隧道模式.传输模式仅对 IP 有效负载进行加密,只适合 PC 到 PC 的场景,而隧道模式对 IP 报头和有效负载进行加密,可以适用于任何场景[1-2,8].

1.2　隧道封装模式

隧道是封装、路由与解封装的整个过程.隧道将原始数据包隐藏(或封装)在新的数据包内部,该新数据包可能会有新的寻址与路由信息,从而使其能够通过网络进行传输.封装的数据包到达目的地后,会拆除封装,原始数据包头用于将数据包路由到最终目的地.隧道是不可见的,而只能看到网络路径中的点对点连接,连接双方并不关心隧道起点和终点之间的任何路由器、交换机、代理服务器或其它安全网关等.隧道模式下的 IPSec 报文要进行分段和重组操作,将隧道和数据保密性结合使用时,可用于提供 VPN[8-9].

1.3　VPN 技术原理

VPN(Virtual Private Network,虚拟专用网).虚拟专用网络可以理解为虚拟出来的企业内部专线,它可以通过特殊加密的通讯协议使 Internet 上

收稿日期:2014-10-15
作者简介:李清平(1969-),男,江西萍乡人,副教授. 研究方向:计算机网络技术.

位于不同地方的多个企业内部网络之间建立一条专有的通讯线路[1,10].VPN 通过公众 IP 网络建立私有数据传输通道,将远程的分支办公室、商业伙伴、移动办公人员等连接起来，减轻了企业的远程访问费用负担,节省了电话费用开支,提供了安全的端到端数据通信.

2 网络部署与配置

2.1 背景资料及拓扑图

某公司总部和分部分别接入 Internet，但总部和分部都只有一个公网 IP 地址,如图 1 所示.总部和分部之间除了日常通信业务外,内部还设置了语音话机,分别配置了语音交换机和语音路由器,并通过 VPN 集线器建立私有网络进行数据传输.要保证公司总部和分部的用户都能访问 Internet,同时综合考虑办公、安全性和费用等方面的要求,公司总部和分部的内部 PC 和 VoIP 话机通过 VPN 互访.

2.2 主要配置命令及解析

2.2.1 企业语音路由器的配置 以企业总部路由器 Voice Enabled Router1(简称 VR1)的主要配置命令为例进行解析,分部路由器 Voice Enabled Router2 的配置可以参考总部路由器,不再赘述.

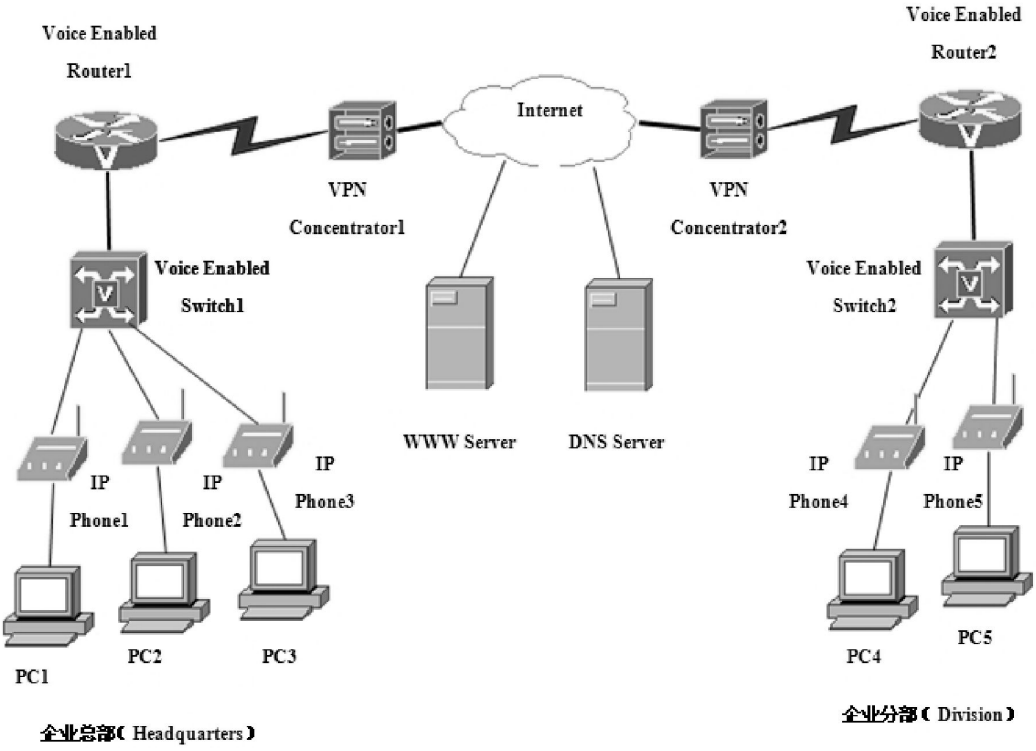

图 1 企业 IPSec-VPN 虚拟专用网拓扑图

Fig.1 The network topology of the enterprise's IPSec-VPN

在 VR1 设置两个 DHCP 池，分别为企业 PC 和语音话机动态分配 IP 地址、网关和 DNS 服务器地址.Cisco 语音话机需要从 TFTP 服务器下载配置文件，如果没有相应的 TFTP 服务器，则向 DHCP 动态池发送 option 150 命令请求配置信息,配置命令如下.

VR1 (config)#ip dhcp pool //动态池名称

VR1 (dhcp-config)#network //动态分配的地址范围

VR1 (dhcp-config)#default-router //语音话机动态获取的默认网关

VR1 (dhcp-config)#ip dhcp excluded-address //在获取的动态 IP 中剔除网关地址

VR1 (dhcp-config)#option 150 ip //Cisco 语音话机请求配置信息

Cisco IP 电话的呼叫控制由 Cisco CallManager 完成,支持各种标准通信协议的语音网关,如 H.323/MGCP/SIP 等,提供电话号码注册分配,完成信令控制和通话控制,配置命令如下:

VR1 (config)#telephony-service //开启电话服务

VR1 (config-telephony)#max-ephones //容许的最大电话数

VR1 (config-telephony)#max-dn //容许的最大目录号

VR1 (config-telephony)#ip source-address //

注册到 Callmanager 上的 IP 和端口号

VR1 (config)#ephone-dn　//逻辑电话目录号

VR1 (config-ephone-dn)#number　//电话号码

VR1 (config)#ephone　//电话物理参数配置

VR1 (config-ephone)#mac-address　//绑定 IP 电话的 MAC 地址

VR1 (config-ephone)#type 7960　//IP Phone 电话类型

VR1 (config-ephone)#button 1:1　//电话按钮与电话目录号绑定

VR1 (config)#dial-peer voice 1 voip　//定义拨号对等体之间的端对端呼叫为语音

VR1 (config-dial-peer)#destination-pattern　//指定通信对方的 IP 地址

VR1 (config-dial-peer)#session target ipv4:　//定义 VoIP 路由

IPSec-VPN 虚拟专用网提供的保护功能有数据机密性、数据完整性和认证等.

数据机密性(Data Confidentiality)用于对发送和接收的数据进行加密和解密，加密算法大致可以分为对称式加密和非对称式加密两类，对称式加密算法包括 DES、3DES、AES，非对称式加密算法为 RSA.数据完整性(Data Integrity)用于保证数据在传输过程中不被修改,发送方在发送数据时,为消息附加一个 Hash 值 1,接收方在接收数据时,根据消息内容和共享密钥计算出 Hash 值 2,两者相符则说明数据内容没有被篡改,目前常用的 Hash 值算法（散列算法）有两种:HMAC-MD5 和 HMAC-SHA-1.认证(Authentication)也叫起源认证，即对对等体进行验证，也称对等体验证(Peer Authentication)，是指对数据发送者的身份识别,确保信息的来源真实可靠,目前有两种方法:预共享密钥(PSK)、RSA 签名,配置命令如下:

VR1 (config)#crypto isakmp policy　//建立 isakmp 策略

VR1 (config-isakmp)#hash md5　//数据完整性加密算法

VR1 (config-isakmp)#encryption des　//数据机密性对称式加密算法

VR1(config-isakmp)#authentication pre-share　//预共享密钥认证

VR1(config)#crypto isakmp key　//IKE 验证密码,对等体两端需一致

VR1 (config)#crypto ipsec transform-set * ah-md5-hmac esp-des　//为交换集命名和设定封装方式,* 为交换集名称(下同),两端可以不同,但 ah-md5-hmac esp-des 必须一致

VR1(config)#crypto map * 1 ipsec-isakmp　//创建密码图,调用密钥策略号, * 为密码图名称(下同)

VR1(config-crypto-map)#set peer　//密码图指向对端外网端口 IP

VR1(config-crypto-map)#set transform-set *　//调用交换集

VR1(config-crypto-map)#match address　//应用访问控制列表 ACL

企业总部和分部的 PC,除了通过虚拟专用网进行通信外,还有访问外网获取信息的需求,通过问控制列表(ACL)和 NAT 地址转换技术来实现这两个目的.

VR1(config)#access-list　//配置 ACL,控制企业私网内部数据的流向

VR1(config-if)#ip nat outside

//配置 NAT，除 VPN 隧道外的其它流量都允许访问外网

VR1 (config-if)#crypto map *　//将密码图放置在 ACL 上,迫使内网流量(包括语音流量)走 VPN 隧道

VR1(config)#ip route　//默认路由用于本地私网访问外网

2.2.2　企业语音交换机的配置　Cisco 语音交换机支持一种独特的功能,称为语音 VLAN,它将 Cisco IP 电话和工作站加入不同的 VLAN 中.通过使用语音 VLAN,可将端口的 VoIP 通信流加入到另一个 VLAN 中,而且只需要配置交换机,无需在 Cisco IP 电话上做额外的配置.企业总部语音交换机 Voice Enabled Switch1(简称 VS1)的主要配置命令如下,分部语音交换机 Voice Enabled Switch2 的配置可参考之.

VS1 (config-if)#switchport access vlan　//在 Cisco IP 电话连接交换机的端口设置 VLAN

VS1 (config-if)#switchport voice vlan 1　//语音 VLAN

VS1 (config-if)#switchport mode trunk　//语音路由器连接交换机的端口设置 trunk 干道

2.2.3　外网服务器的配置　在 WWW 服务器中制作一个简单网页 index.html,网页域名 http://www.lqp.com,作为企业内网主机访问外网服务器中 Web 页面的验证. 在 DNS 服务器中建立对应 http://www.lqp.com 的域名解析,并使用公网 IP 地址 202.101.172.1,如图 2 所示.

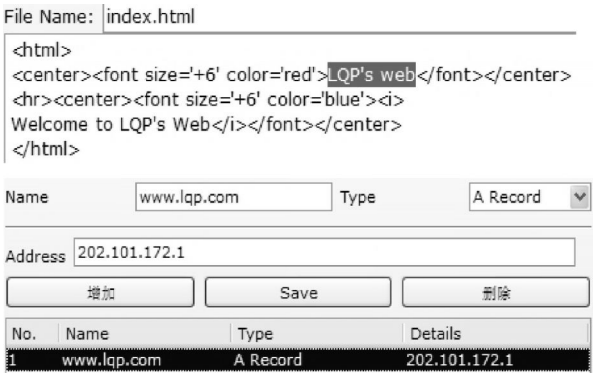

图 2 WWW 和 DNS 服务器的配置

Fig.2 The configuration of WWW server and DNS server

3 测试结果

企业总部的 IP phone1 及分部的 IP phone4 之间能相互通话.

企业内网的 PC 通过域名 http://www.lqp.com 访问 WWW 服务器中的 Web 页面,如图 3 所示.

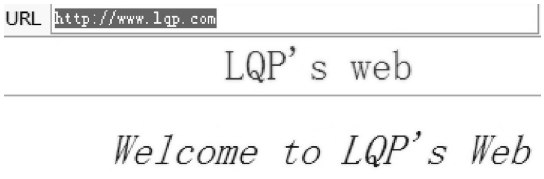

图 3 企业内网 PC 访问 WWW 服务器中的 Web 页面

Fig.3 The web page in WWW server accessed by the enterprise intranet PC

隧道模式中,IPSec 的 AH 头或 ESP 头插入原来的 IP 地址之前,加密和认证之后重新产生的 IP 头加到 AH 头或 ESP 头之前.通过"show ip route"命令查询 VR1 的路由信息可以看出,真正的 IP 源地址和目的地址都隐藏在 Internet 传送的普通数据中,如下所示.

Gateway of last resort is 20.0.0.2 to network 0.0.0.0

C 20.0.0.0/8 is directly connected, Serial1/0

C 192.168.10.0/24 is directly connected, FastEthernet0/0.1

C 192.168.20.0/24 is directly connected, FastEthernet0/0.2

S* 0.0.0.0/0 [1/0] via 20.0.0.2

4 网络性能影响

IPSec-VPN 是需要消耗资源的保护性措施,一方面隧道模式加密的复杂性需要占有一定的网络带宽,另一方面 IPSec 保护的兴趣流会触发协商,触发的过程通常是将数据包中的源、目的地址、协议以及源、目的端口号与 ACL 进行匹配,协商的内容主要包括双方身份的确认、密钥种子刷新周期、AH/ESP 的组合方式及各自使用的算法、封装模式等,这些都是网络延迟的影响因素.

在 OPNET 平台上对网络性能进行仿真和分析[10~11],图 4 显示,企业总部网络的吞吐量和分部网络的吞吐量基本相当, 说明在 IPSec-VPN 隧道中数据的丢包率比较低,VoIP 语音数据基本上能完整到达对方.

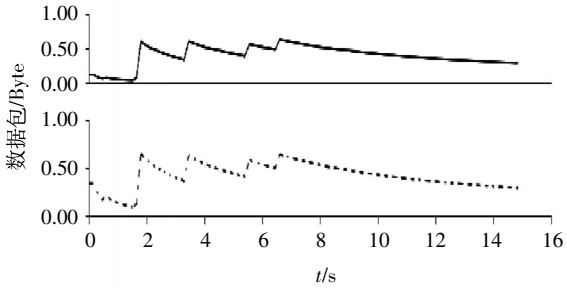

图 4 企业总部和分部网络的吞吐量

Fig.4 The network throughput of HQ and division

注: —— 企业分部网络的吐量(bits/sec);

---- 企业总部网络的吐量(bits/sec)

从图 5 可以看出,企业总部 PC 机开始时数据包的发送速度很快,VR1 路由器接到数据包后进行加密、封装,接收速率逐渐缓慢下来,一直到数据发送完毕.在接收方,开始时由于与发送方建立会话和协商,数据包的传输速率比较平缓,当发送方的数据全部发送完成后,接收方 VR2 路由器进行解密和解封装,还原数据,企业分部 PC 机的输送速率陡然提高,直到全部接受数据完毕.

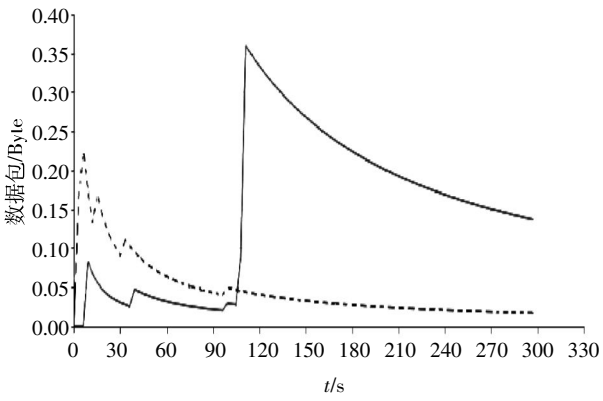

图 5 企业总部和分部 PC 数据包的传输速率

Fig.5 The data packet transmission rate of HQ and division

注: ···· 企业总部 PC1 数据包发送速率(packet/neo);

—— 企业分部 PC1 数据包发送速率(packet/neo)

IPSec-VPN 的机制对网络延迟的影响比较明显.图 6 显示,企业总部网络随着 IPSec 的会话协

商、数据的加密认证和 VoIP 数据包的发送出现 3 次较为明显的延迟现象,分部网络由于没有 VPN 隧道的数据发送,网络延迟有所减缓.

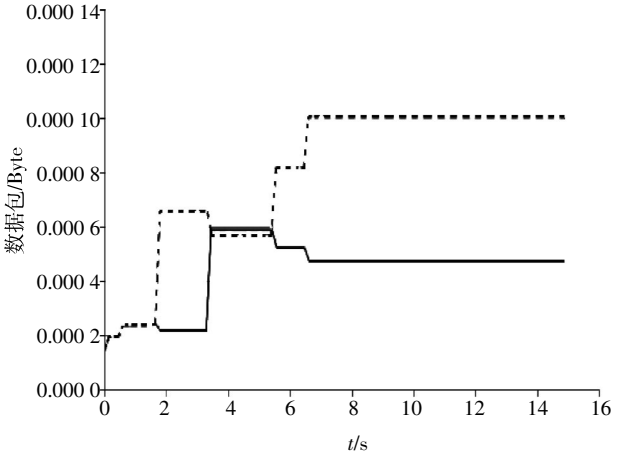

图 6　企业总部和分部网络的网络延迟

Fig.6　The network delay of HQ and division

注: ---- 企业总部网络的网络延迟(aco);
—— 企业分部网络的网络延迟(aco)

5　结　语

随着企业组织机构区域性扩展及员工日益分散,分支机构采用 VPN 方式与总部建立一个大的虚拟专用网并进行集中管理操作,从而达到节省成本和实时管理的目的. 基于 IPSec 标准的 VPN 技术为企业内部网络数据的安全传输提供了技术保障,但 VPN 的数据机密性、数据完整性、起源认证等加密措施和隧道封装技术使得网络配置变得复杂. 在 IPSec-VPN 专用网中虽然数据包的传送基本上是完整的,但 IPSec 采用的安全策略对数据包的传输速率尤其是网络延迟的变化无疑会产生较大的影响,导致网络抖动明显,收敛速度慢,VoIP 语音的质量也随之减低.因此,采取诸如数据高速透明压缩、流量整形、智能带宽分配、VPN 数据双向加速等技术,提高上/下行带宽速度,减少网络延迟,以获得高速应用性能,是 IPSec-VPV 技术关注和研发的重点.

致　谢

感谢学院同仁和合作企业提供的大力支持和帮助!

参考文献:

[1] 崔北亮.CCNA 认证指南(640-802)[M].北京:电子工业出版社,2009:551-556.
CUI Bei-liang.CCNA certification guide (640-802)[M].Beijing: Electronic Industry Press,2009:551-556.(in Chinese)

[2] 王妍.基于 IPSec 的 VPN 系统设计与实现[D].成都:电子科技大学,2013:5-28.
WANG Yan.Design and implementation of VPN system based on IPSec[D].Chengdu:Electronic Technology University,2013:5-28.(in Chinese)

[3] 郭赛球,陈伟宏,文乾德.基于 IPSec VPN 的应用性组网研究与设计[J].湖南城市学院学报:自然科学版,2013,22(6):70-74.
GUO Sai-qiu,CHENG Wei-hong,,WEN Qian-de.The research and design of virtual private network application construct based on IPSec VPN [J].Journal of Hunan City University:Natural Science,2013,22 (6):70-74.(in Chinese)

[4] 李淑梅.中小企业基于 IPSec VPN 的网络构建[J].现代计算机,2011(5):99-101.
LI Shu-mei.Network construction based on IPSec VPN in small and medium-sized enterprises [J].Modern Comupter,2011(5):99-101.(in Chinese)

[5] 张光剑,李军英,李仁发,等.基于 VPN 的安全 VoIP 述评[J].计算机应用研究,2004(2):1-3.
ZHANG Guang-jian, LI Jun-ying, LI Ren-fa1,et al. Introduction to secure VoIP based on VPN[J].Application Research of Computers,2004(2):1-3.(in Chinese)

[6] 司聿宣,苏远兴,杨正芳.分布式环境实时语音通讯系统的设计与实现 [J]. 武汉工程大学学报,2012,34(5):60-63.
SI Yu-xuan,SU Yuan-xing,YANG Zheng-fang.Design and realization of real-time audio communication system based on distributed environment [J].Journal of Wuhan Institute of Technology,2012(5):2012,34(5):60-63.(in Chinese)

[7] 肖耿毅.IPSec 虚拟专用网络服务质量研究与仿真[J].计算机仿真,2009,26(8):137-142.
XIAO Geng-yi.Research and simulation of QoS of IPSec virtual private network[J].Computer Simulation,2009,26(8):137-142.(in Chinese)

[8] 王泽泽.基于 IPSec 的 IKE 协议研究与实现[D].太原:太原理工大学,2011:5-35.
WANG Ze ze.Based on IPSec research and implementation of IKE protocol[J].Taiyuan:Taiyuan University of Technology,2011:5-35.(in Chinese)

[9] 张莉.采用 IKE 协议提高 IPSec 安全性的应用[J].网络安全技术与应用,2011(7):12-14.
ZHANG Li.Adopt IKE protocol to increase application of IPSec's security [J].Network Security Technology & Application,2011(7):12-14.(in Chinese)

[10] 邢金萍. 基于 OPNET 的 IPSec VPN 的性能分析[J].

通信技术,2009,42(9):91-93.
XING Jin-ping.Performance analysis of IPSec VPN based on OPNET [J].Communications Technology, 2009,42(9):91-93. (in Chinese)
[11] 李清平.隧道技术在新增 IPv6 校园网中的实现及分析[J].计算机系统应用, 2010,19(6):162-165.
LI Qing ping.Implementation and analysis of newly added IPv6 campus network based on tunneling technique[J].Computer Systems & Applications, 2010,19(6):162-165. (in Chinese)

Application of voice-over-IP in virtual private network and network performance

LI Qing-ping
Department of Information Technology & Application,Zhejiang Yuying College of Vocational Technology,Hangzhou 310018,China

Abstract: To study the voice-over- internet protocol (VoIP) data transmission through virtual private network(VPN) based on internet protocol security (IPSec) and the influence on network performance, an enterprise's VPN network topology was designed based on the analysis of IPSec technology , tunnel encapsulation technology and VPN technology. The configuration and the function were explained on the voice router and the voice switch and the outgoing server, the network performance was simulated and analyzed based on OPNET performance. The results show that VPN can further complicate the configuration because of its tunnel encapsulation technology and encryption measures, such as data confidentiality, data integrity and authentication, etc.;in the process of the VPN tunnel transmission, VoIP voice data has low packet lost rate, but the transfer rate becomes slow and the network delay increases;the obvious network jitter, slow convergence speed, low VoIP quality are caused by IPSec security policy.

Keywords:internet protocol security;virtual private network;voice-over-IP;Network Performance;Network Delay

本文编辑:陈小平