DOI:10.13878/j.cnki.jnuist.2016.02.010

陈遥[1]　杜知名[1]

# 双中心双云的 DM VPN 设计

**摘要**

针对拥有几百个分支机构的企业网络环境,其多个分支机构间需要安全可靠的通信,采用 DM VPN 这个高扩展性的 IPSec VPN 解决方案,部署 VPN 隧道加密企业网络通信.DM VPN 技术可以直接将分支机构的通信加密,不需要经过中心机构的转发,为中小型企业网络的互联节省了成本,在提高网络的可用性与安全性的同时也使得应用和管理更加简易.

**关键词**

网络安全;隧道技术;动态多点 VPN

**中图分类号** TP311

**文献标志码** A

## 0　引言

社会在不断发展,公司企业扩大,网络也在随之改变.很多企业形成了一个总部,多个分公司,甚至多个总部,多个分公司的格局,这就要求网络把这些总部和分公司连接起来,完成公司工作的合作和公司所有资源的共享,从而提高工作效率.若企业使用专线连接方式则费用高,很多是选用便宜很多的 VPN 技术[1].

同时,随着公司的规模不断扩展,网络技术的重心也渐渐从网络可用、数据传输转变到网络传输过程中数据的安全和实际管理应用方面的简便.所以,能够安全地通过网络将公司总部和分公司、公司其他各地的办事处联系起来是大多数企业希望的.早期可以通过帧中继和 ISDN 的二层网络将这些企业的各个点连接起来,从而可以使内部 IP 可以通信,但是这种二层网络的线路较贵.目前可以通过比较便宜的互联网接入方式将企业的各个点连接起来,还可以利用 IPSec 加密的隧道确保公司内部通信的安全.但是,对于 IPSec 的加密,中心的负担格外大,中心要解密分支发送的数据后,再加密数据发送给需要接受的分支,要是处在不同城市的中心和分支,经过跨市的传输网络,将加大网络通信的延时.

由此,本文将设计采用动态多点 VPN(Dynamic Multipoint VPN,DM VPN)[2]这个高扩展性的 IPSec VPN 解决方案,部署 VPN 隧道加密企业网络通信.其中,DM VPN 直接将任意两分支机构间建立隧道通信,并且确保通信的数据安全被加密,不需要经过中心机构的转发,提高了两个分部间通信的效率,为企业网络的互联节省了成本,从而在提高网络的可用性与安全性的同时也提高应用和管理的简易性.

## 1　两种传统的 IPSec VPN 模型缺陷

IPSec[3]对数据的加密是利用密钥在两端点间的共享实现的,就是说不一样的密钥在随意的两端点间都要实现共享,因此,IPSec 加密的隧道被称做点到点加密,多个点到点加密的隧道就组成了 IPSec 网络.

IPSec 网络有星型和网状两种结构形式.中心和分支间存在着大量的数据流量,然而分支与分支间存在的数据流量少很多,这是在许多网络中普遍存在的,一般采用星型结构,因为网状结构会用到很多

**收稿日期** 2015-06-13

**资助项目** 南京信息工程大学滨江学院 2015 届优秀本科毕业论文支持计划

**作者简介**

陈遥,女,副教授,主要研究方向为智能数据处理.chenyao0077@163.com

1　南京信息工程大学　滨江学院,南京,210044

的点到点线路,需要比星型结构更多的线路费用,加重网络成本.然而,分支到分支一定要通过中心来通信是星型结构的缺点,因为通过中心来通信就会消耗中心设备的性能,使通信延时增加.

传统 IPSec VPN 的星型拓扑如图 1 所示.这种解决方案,很明显不是一个高扩展的设计,不适合在拥有大量分支站点的网络中部署 IPSec VPN.

传统 IPSec VPN 网状模型如图 2 所示.该网状拓扑存在如下问题:1)分支站点在 IPSec VPN 网状模型中需要来维护很多的 IPSec SA;2)分支站点在 IPSec VPN 网状模型中需要固定的 IP 地址,但比较便宜的互联网接入的大多分支站点是动态 IP 地址.

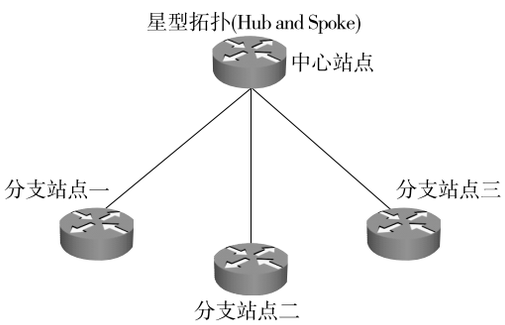


图 1 传统 IPSec VPN 星型拓扑

Fig. 1 Star topology of traditional IPSec VPN

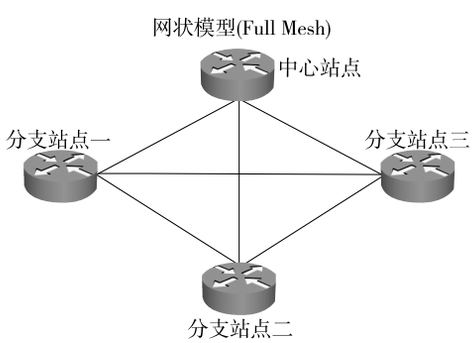


图 2 传统 IPSec VPN 网状模型

Fig. 2 Network topology of traditional IPSec VPN

## 2 DM VPN

因为有以上问题存在于 IPSec VPN 的星型模型以及网状模型中,于是提出使用动态多点 VPN 的设计.DM VPN 相比于传统的 IPSec VPN 技术有以下优点:1)分支站点可以使用动态 IP 地址建立隧道;2)当有新的分支站点添加到网络中时,中心站点的配置不需要添加修改;3)分支站点间直接建立虚拟隧道封装通信数据,不经过中心的解密重加密.

### 2.1 DM VPN 技术的 4 大组件

#### 2.1.1 动态多点 GRE 协议

GRE(Generic Routing Encapsulation)是一种典型的三层隧道封装技术,其封装结构如图 3 所示.动态多点 GRE 协议(mGRE)是一种特殊的 GRE 技术.mGRE 的全部站点的隧道接口处在相同的网段,实现虚拟网状的连通性,分支站点可以与其他的分支站点直接通信而不依赖中心.

| 外层IP头部(封装设备间公网地址) | GRE头部 | 内层IP头部(实际通信设备间地址) | 内层实际传递数据 |
|---|---|---|---|

图 3 GRE 的封装结构

Fig. 3 Encapsulation structure of GRE

#### 2.1.2 下一跳解析协议

当网络中配置了 mGRE 隧道时,系统中所有站点还不能够直接通信,因为物理地址和逻辑地址还没有映射,此时需要由网络维护人员配置这种地址映射.在 mGRE 隧道中,物理地址是各个站点的公网 IP 地址(类似于 ARP 中的 MAC 物理地址)保证物理底层通信,而逻辑地址是 mGRE 隧道的虚拟地址(类似于 ARP 中的 IP 逻辑地址)保证网络上层通信.ARP 是完成 MAC 和 IP 的解析映射关系的协议,所以设计下一跳解析协议(NHRP Next Hop Resolution Protocol,NHRP)来完成公网 IP 和隧道虚拟地址这种解析映射.

#### 2.1.3 动态路由协议

RIP、EIGRP、OSPF、ODR 以及 BGP 这些动态路由协议都可以用来部署完成 mGRE.在 NBMA 网络中不可以转发组播,而 mGRE 隧道是属于 NBMA 网络的,但几乎大部分动态路由协议传播路由信息是使用组播转发的,因此需要在 mGRE 隧道中把组播映射成单播来转发.私有网络的通告和虚拟 IP 地址的通告则要通过动态路由协议去完成,底层的通信还是要通过站点公共 IP 地址完成.

#### 2.1.4 IPSec 技术

IPSec 是一项标准的安全技术,其封装示意如图 4 所示,它通过在数据包中插入一个预定义头部的方式来保障数据在上层的安全.在传输层头部前、IP 头部后插入 IPsec 头部,可以加密传输层头部、应用层头部以及应用层数据,而且可以验证 IPsec 头部到应用层数据的完整性.IPsec 技术提供更多的安全特性,它对 VPN 流量提供 3 个方面的保护:1)私密性,使用加密算法去加密数据;2)完整性,确保数据在传

输过程中没有被第三方篡改;3)源认证,为了排除非法的源发送欺骗的数据包,就要认证那些发送数据包的源.

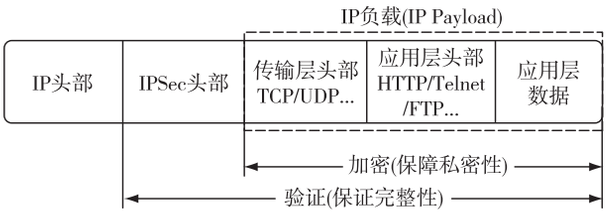


图 4　IPSec 封装示意

Fig. 4　Encapsulation diagram of IPSec

### 2.2　设计思想

本文设计思想是:DM VPN 可以发送注册通过分支到中心,再从中心获取其他分支的物理地址,分支间可以直接建立隧道,解决了架设多条线路的成本问题,也减轻了中心的负担.利用多点 GRE(mGRE)、下一跳解析协议(NHRP)和 IPSec 技术来完成 DMVPN 的实现.在实现 DM VPN 的过程中,隧道建立使用 mGRE 解决,分支节点动态地址使用 NHRP 协议,完成数据的加密使用 IPSec 技术.但是,必须申请一个静态公共 IP 地址作为中心节点的 IP,其作用是在非广播的多路访问网络上网络层源获取目的地址.

## 3　双中心双云 DM VPN 网络规划与设计

本文实现 DM VPN 的第一步就是基础网络的构建,因为搭建 DM VPN 的前提是保证基础网络通信,基础网络是每个站点间通信的基础.在本设计中,以上海和北京的总部为中心站点(即双中心),南京和天津两个地区的分部为分支地点.上海中心站点通过运营商一中国电信与两个分支站点连接,北京中心站点通过运营商二中国网通与两个分支站点连接,各点都通过运营商提供的网络来实现内网的通信.这种设计可以推广到其他区域的网络构建.具体网络构建如图 5 所示.网络构建过程中 IP 地址分配如表 1 所示.如图 5,上海和北京中心站点出口及南京和天津分支站点出口直接用路由器模拟,运营商基础网络用三台路由器模拟.公司的上海和北京总部及南京和天津分部内网使用 OSPF 路由协议,上海和北京总部是区域一,南京分部是区域二,天津分部是局域三,这样确保公司每个区域的本地内网通信.公司和 ISP 运营商使用 EBGP 路由协议,确保公司公网地址与 ISP 运营商外网的通信.ISP 运营商内部使用 EIGRP 路由协议,运营商底层网络比较复杂,很多不是直接穿过多个网络虚拟直连.

**表 1　IP 地址分配表**

Table 1　IP addressallocation

| 网络 | 具体网段 |
|---|---|
| 上海/北京总部 | 192. 168. 100. 0/24　192. 168. 200. 0/24 |
| 南京/天津分部 | 192. 168. 1. 0/24　192. 168. 2. 0/24 |
| 电信运营商 | 56. 56. 56. 0/24　57. 57. 57. 0/24　67. 67. 67. 0/24 |
| 网通运营商 | 89. 89. 89. 0/24　81. 81. 81. 0/24　91. 91. 91. 0/24 |
| 公网地址 | 202. 100. 1. 0/24 |
| 虚拟隧道一/二 | 172. 16. 1. 0/24　172. 16. 2. 0/24 |

在我国南方,中国电信的业务优于中国网通,北方恰恰相反.因此在不同地域的公司总部和分部完全可能选用不同的运营商业务,所以公司在构建 VPN 时,就需要考虑跨多个运营商的问题.在本文用 DM VPN 构建两条 VPN 隧道,分别跨越两个运营商(即双云,指两个提供 VPN 接入的运营商,运营商提供了 VPN 通信的载体,价格便宜,易实施维护,同时提供了通信的安全性,综合性价比高).隧道一穿越运营商一中国电信,隧道二穿越运营商二中国网通.配置基本步骤如下:

1)配置 mGRE.实现隧道的通信,隧道源和目的物理地址的指定.

2)配置 NHRP.实现隧道逻辑地址和物理地址的映射,NHS 的指定.

3)配置隧道间的路由协议.隧道间路由协议本文使用 OSPF 路由协议,把隧道的网络地址宣告进各个站点的内网网络,这样做就不用再双向重分发路由.当完成这一步时,各中心站点和分支站点间则可以进行通信.

4)配置 IPSec 加密数据.分两个阶段配置,第一阶段配置加密隧道本身,配置散列函数、加密协议、认证方式和加密通信对等体;第二阶段配置加密数据,配置封装协议、加密协议和传输模式.

在本设计中可以直接在路由器和 PC 上测试 DM VPN 的通信和加密,即可以用 ping 命令和 traceroute 命令测试.如在 PC3 上执行“ping 192. 168. 2. 1”和“traceroute192. 168. 2. 1”.当通信正常时,并不保证数据被加密了,所以还需要通过在 R3/R4 上执行“show crypto isakmp sa”,查看 VPN 加密隧道本身第一阶段,“show crypto ipsec sa”查看 VPN 加密传输数据第二阶段,“show crypto engineer connect active”查看 DMVPN 是否加密数据.如果控

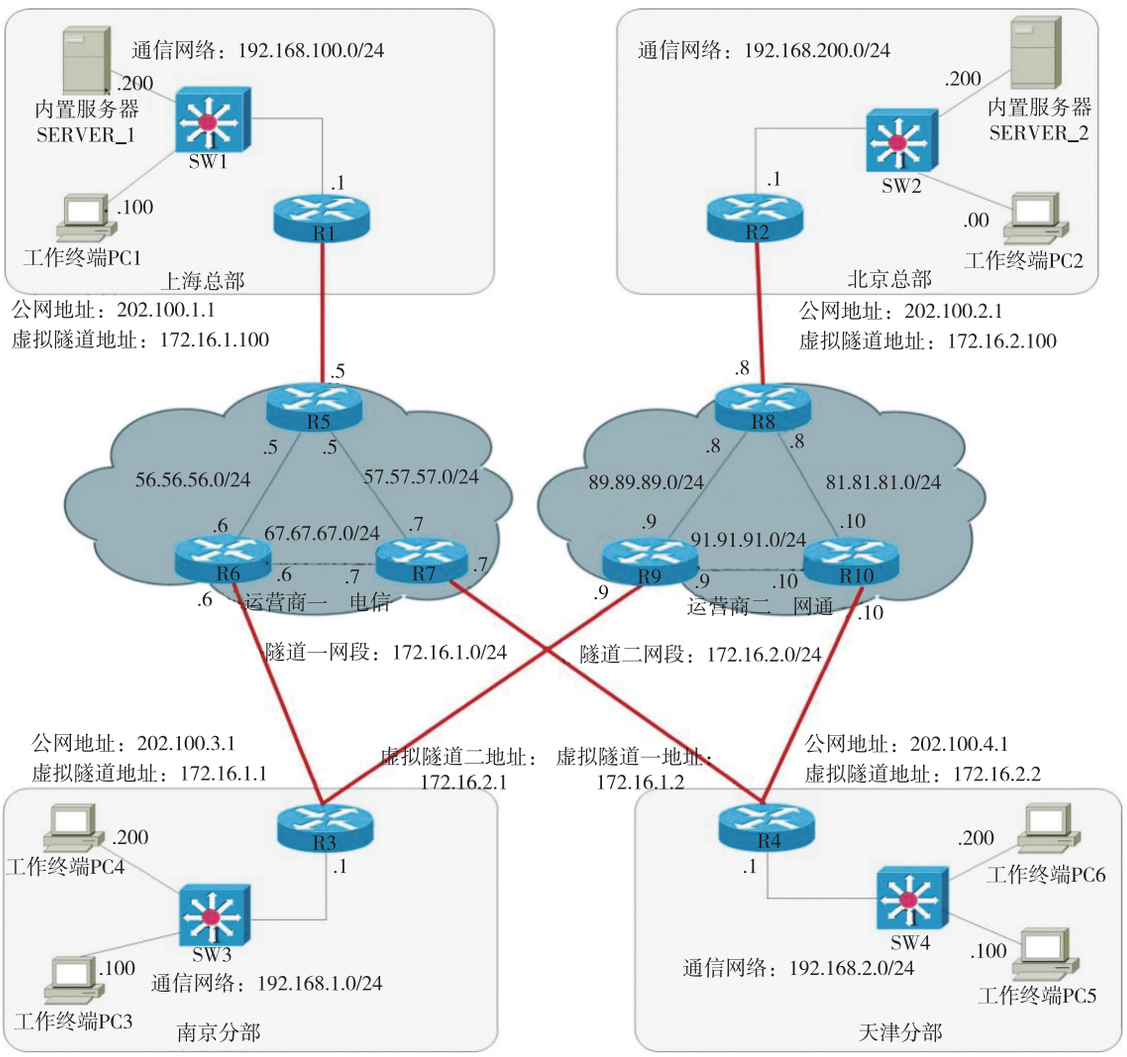


图 5　双中心双云 DM VPN 具体规划设计

Fig. 5　Design of dual center dual cloud DM VPN

制台显示加密的数据包个数量,表明数据被加密.

本文使用上述方法进行了南京和天津分部到上海和北京总部的连通性测试,南京和天津分部到上海和北京总部传输的数据包加密测试,南京分部到天津分部连通性测试,南京分部到天津分部传输的数据包加密测试,南京和天津分部间直接通信不通过上海和北京总部转发测试,以及测试查看每个站点学到所有其他站点的路由.测试结果表明这种 DM VPN 设计实现了直接将分支机构的通信加密,不需要经过中心机构的转发,为企业网络的互联节省了成本,提高了网络的可用性与安全性的同时也提高了应用和管理的简易性.

## 4　结束语

本文首先阐述了 VPN 的背景和传统的 IPSec VPN 的缺陷,以及 DM VPN 的优势,然后介绍了 DM VPN 的 4 大组件,给出了一个用 CISCO WEB-IOU 模拟实际应用的 DM VPN 网络,完成了 DM VPN 网络的设计,达到加密安全传输的要求.本文下一步工作是将 DM VPN 层次化运用到超大范围网络部署,多个分支站点到区域中心站点加密传输,然后是区域站点再到核心站点的数据加密传输,做到层次化树状结构,使超大范围网络更加系统高效.

## 参考文献

References

[1] 徐云恒.动态多点 VPN 技术[J].通信技术,2010,43(2):125-127
XU Yunheng. Dynamic multi-point VPN technology[J]. Communications Technology,2010,43(2):125-127

[2] Security Technology Group, Cisco System Inc.

Introduction to dynamic multipoint VPN. 170 West Tasman Dr. San Jose, CA 95134 [M]. USA: Cisco Press,2004

[3] 赵宁.动态多点 VPN 的设计与实现[D].北京:北京邮电大学计算机学院,2008
ZHAO Ning. The design and implementation of dynamic multi-point VPN[D]. Beijing: School of Computer, Beijing University of Posts and Telecommunications,2008

[4] 谢希仁.计算机网络[M].6 版.北京:电子工业出版社,2013:176
XIE Xiren. Computer network[M]. 6th Ed. Beijing: Publishing House of Electronics Industry,2013:176

[5] Stallings W.密码编码学与网络安全:原理与实践[M].3 版.刘玉珍,王丽娜,傅建明,等译.北京:电子工业出版社,2004:47-48
Stallings W. Cryptography and network security: Principles and practices[M]. 3rd Ed. Translated by LIU Yuzhen, WANG Lina, FU Jianming, et al. Beijing: Publishing House of Electronics Industry,2004:47-48

[6] 王蔚旻,冯剑波.基于双核心单云拓扑的 DMVPN 技术实现[J].计算机与数字工程,2014,42(7):1214-1218
WANG Weimin, FENG Jianbo. Implementation of DMVPN based on dual hub-single DMVPN cloud topology[J]. Computer and Digital Engineering,2014,42(7):1214-1218

# Design of dual center dual cloud DM VPN

CHEN Yao[1] DU Zhiming[1]

1 Binjiang College, Nanjing University of Information Science & Technology, Nanjing 210044

**Abstract** In an enterprise network, usually there are hundreds of branches, all of which need secure and reliable communications. As a highly scalable IPSec VPN solution under the network circumstance, DM VPN is used to deploylarge-scale VPN tunnel to encrypt the communication between corporate network branches. The proposed dual center dual cloud DM VPN directlyencrypts the communication in the branch networkwithout the forward process by the network center, which canreduce the cost and improves the networksecurity for medium or small scale enterprises.

**Key words** network security; tunnel technology; DM VPN