



可管可控的移动 VPDN 方案研究

黄 粤,魏颖琪

(中国电信股份有限公司广东研究院 广州 510630)

摘 要:移动 VPDN 也称为无线 IP 专网或 3G IP 专网,为广大企业客户提供了基于 3G 宽带网络的数据专网服务。本文对移动 VPDN 的组网构建、安全认证及业务保障等方面进行了分析研究,并提出了移动 VPDN 在行业信息化建设中可管可控的新组网模型。

关键词:移动 VPDN;MPLS;可管可控

doi: 10.3969/j.issn.1000-0801.2013.04.027

Research on Manageable and Controllable Mobile VPDN Solution

Huang Yue, Wei Yingqi

(Guangdong Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China)

Abstract: Mobile VPDN is also known as wireless IP private network or 3G IP private network. It offers data private network service based on 3G network to all enterprise customers. Key factors of mobile VPDN, such as flexible network building, the policies of security authentication and service guarantee, were analyzed. A security-enhanced model and a controllable networking solution were introduced.

Key words: mobile VPDN, MPLS, manageable and controllable

1 引言

2012 年,美国电信供应商 Verizon 的官方微博披露的一则新闻引起了广泛热议。Verizon 受一家基础建设建筑公司委托,对其在 Verizon 设立的 VPN (virtual private network,虚拟专用网络)系统中的一个反常 VPN 登录情况进行调查。该 VPN 系统建设于 2010 年,目的是让员工在一定时期内可在公司以外的地方远程办公。调查过程中,对反常 VPN 连接情况的监测结果显示,公司的 VPN 服务主机经常被来自中国沈阳的客户访问,几乎每天登录,登录时间偶尔会从上班持续到下班。而同时使用该登录账号的程序员却坐在美国公司本部的办公桌边。一切看起来颇

为蹊跷,但真相却令人大跌眼镜,原来正是拥有该 VPN 账号的程序员用其 1/5 的薪水,雇佣了沈阳的一家软件公司帮助其完成日常工作。这样,该程序员在工作期间就有充足的时间网上冲浪,同时他因为代码整洁、质量良好、提交及时还成为了公司的明星程序员。

这则新闻虽然令人啼笑皆非,却也从一个侧面反映出了如下所述的企业管理与运作信息化发展现状。

- “世界”真的是“平的”。身处地球各地的人,无论他在美国某个州还是在中国沈阳,只要信息网络触手可及,都可协同工作,共同完成一项任务。
- 企业 VPN 大行其道。正是 VPN,使移动办公、远程办公成为了可能,促成了上面现状的迅猛发展。

* 国家“核心电子器件高端通用芯片及基础软件产品”科技重大专项基金资助项目“移动智能终端操作系统研发”(No.2012ZX01039002-001)



- 不加控制与管理的 VPN 是对企业信息安全的一个重大威胁。

因此,在信息网络日益发达的今天,企业对 VPN 有何要求以及如何构建安全可控的 VPN 是值得深入探讨与研究的课题。

2 构建企业 VPN 的关键因素

VPN 指在公用网络(如互联网)上建立专用网络,之所以称其为“虚拟”,是因为 VPN 的任意两个节点之间的连接都没有端到端的物理链路,而是架构在公用网络服务商所提供的网络平台上。企业构建自己的 VPN 主要基于以下 4 个因素的考虑。

(1)组网因素

一般企业无法自行铺设管线,组建一张属于自身的信息网络,最简单、省事的方法是使用网络服务商提供的公用网络,在其上构建一张虚拟专网,连接企业总部与各分支、各在外员工,以达到企业员工可远程访问企业 ERP、OA 等系统,快速存取企业内部数据,提升企业运作效率的目的。

(2)安全因素

由于现有的基于互联网的信息交换缺乏相应的安全保护机制,各类黑客攻击、侵入(如系统注入、拒绝服务、网页挂马、钓鱼攻击等)猖獗,各种计算机病毒横行。企业需要让远程接入点实现其机密数据及资源的共享,因此涉及企业机密的数据交换必然面临严重的安全威胁。

(3)移动因素

随着 3G 通信技术的日趋完备、无线网络覆盖的持续优化和移动终端的推陈出新,移动互联网得到快速发展,使得多样化的移动商务应用成为现实。企业员工使用的信息终端也从单一的手机、笔记本电脑扩展至各种手持移动终端。由于手持移动终端携带方便、使用简单、开机启动和联网迅速、移动性更强、更为轻便,使得专业应用由台式或笔记本电脑逐步向手持终端延伸成为一个不可扭转的趋势。

(4)管理因素

虽然大部分非信息领域的专业企业没有实力自己构建 VPN,需要依赖于网络服务商提供的 VPN 服务,但其希望能对 VPN 实现自助管理,提升对信息安全的管控能力。如通过定义健全的服务认证机制建立较高安全级别的身份认证体系、对不同等级的企业员工或用户开放不同范围

的企业内网访问权限等,这些个性化需求要求企业 VPN 实现差异化的服务。

3 基于 MPLS 的移动 VPDN 解决方案

根据对企业客户具体需求的深入了解以及对当前信息网络宽带化、移动化趋势的把握,基于 MPLS (multiprotocol label switching,多协议标签交换)的移动 VPDN(virtual private dial-up network,虚拟专有拨号网络)将是企业构建 VPN 的一个行之有效的解决方案,也是未来企业 VPN 发展的一个重要方向。通过基于 MPLS 的移动 VPDN,能在远程访问的无线终端、传输通道、企业内网之间建立一条专有的、端到端的、安全快捷的数据通道,从而有效地保障企业机密数据在整个传送与交换过程中的时效性及安全性。

以 cdma2000 1x/3G 网络为例,基于 MPLS 的移动 VPDN 架构如图 1 所示。

基于 MPLS 的移动 VPDN 架构大致可以分为 3 部分。

(1)用户接入无线 VPDN

无线 VPDN 是基于 cdma2000 1x/3G 高速分组数据网络,利用 L2TP(layer 2 tunneling protocol,二层隧道协议)技术为企业客户构建与公用互联网隔离的虚拟专用网络。网络连接主要包括无线空中通道、无线接入网、核心网。企业员工或用户使用的移动终端通过这段网络连接,利用 L2TP 技术,建立了一条与所属专网连接的虚拟隧道,隧道源于用户终端,止于网络服务商的共享 LNS(L2TP network server,支持 L2TP 的网络服务器)。这样,远程的移动终端或 PC 通过无线 VPDN 安全地拨入访问企业网络或应用系统。

(2)MPLS VPN

企业采用 MPLS VPN 连接各分支、业务网点及无线 VPDN 部分的共享 LNS,MPLS VPN 承载在网络服务商的基础网络(如中国电信的 CN2 网络)上。MPLS VPN 是一种基于 MPLS 技术的 IP VPN,其采用标签交换的方式,一个标签对应一个用户数据流,非常易于实现企业 VPN 与公用网络的数据隔离、不同企业 VPN 之间的数据隔离,区别于在公用网络之上依靠封装与加密技术的传统 VPN(如 IPSec VPN)。同样,因其不依赖于终端对数据的封装与加密,属于网络侧的 VPN,MPLS VPN 无需接入的终端运行客户端程序,加快了接入速度,提高了传输效率。而 MPLS VPN 强大的组网灵活性及扩展性,也易于实现企业 VPN

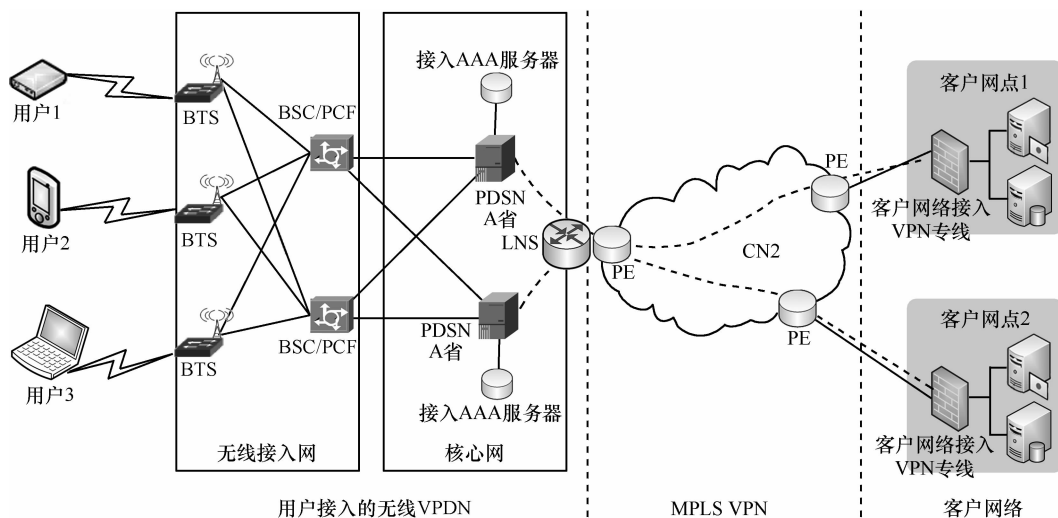


图1 基于MPLS的移动VPDN架构

服务的差异化。

(3)企业客户网络

企业总部及各分支机构、业务网点通过MPLS VPN组成各种拓扑结构的企业VPN。

建设好以上基于MPLS的移动VPDN，企业员工及用户只需在自己的移动终端上做简单拨号，即可接入企业内网，获取数据。具体拨入流程如图2所示。

具体的拨入流程如下所述。

- 移动终端进行无线拨号，接入核心网的PDSN (packet data server node, 分组数据业务节点)。

- PDSN向接入AAA (authentication, authorization and account, 认证、授权、计费)服务器查询移动终端账号的VPDN信息，接入AAA服务器给出LNS信息及L2TP参数等。
- PDSN根据接入AAA服务器给出的信息，找到相应的LNS，在VPDN AAA服务器进行账号密码鉴权，鉴权成功后与LNS建立加密的L2TP传输数据。
- 移动终端获取IP地址后，接入目标网络，即成功建立如图3所示的专网通道，实现拨号接入企业VPN。

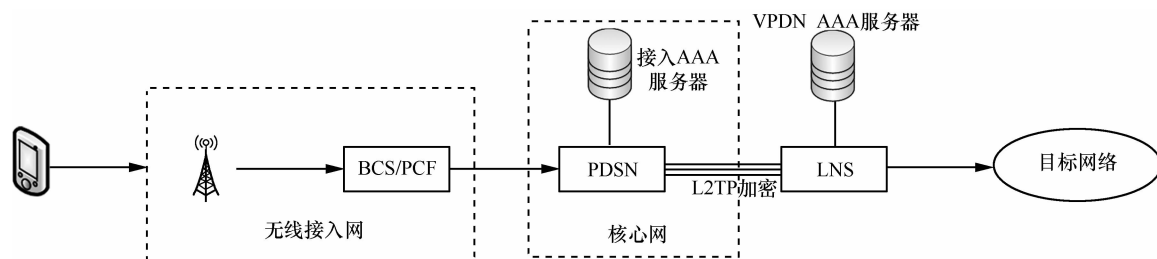


图2 移动终端至企业内网的拨入流程

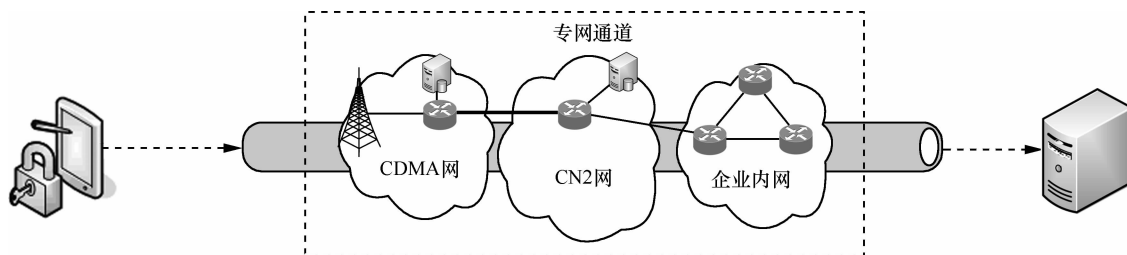


图3 移动终端至企业内网的专网通道



4 可控可管的增强型 VPDN

基于 MPLS 的移动 VPDN 方案的研发,成功解决了企业 VPN 构建时在组网、安全及移动因素等方面的困扰。随着 3G 网络的发展与优化,移动 VPDN 以速度快、覆盖广、使用方便、安全性高等特点,逐渐在工商、金融、警务、工业监控等众多部门及行业扩展了应用,为各行各业的信息建设注入新动力。但随着远程办公、移动办公应用的不断增加,企业对移动 VPDN 提出更多的要求,特别是在 VPN 的管理、控制及个性化的实现方面提出了更高的要求。

4.1 灵活、严格的身份认证新方案

一方面,传统的 VPDN 拨号接入,由 VPDN AAA 服务器根据企业用户的账号密码进行身份识别,如果账号和密码被盗,则第三方可通过该账号和密码进入企业内网,存在风险隐患;另一方面,在互联网时代,用户需要保管大量各类移动互联网服务的账号和密码,新增的移动 VPDN 账号密码会增加用户负担,特别是采用定期更换密码方式实现接入安全的企业用户。

移动智能终端不是简单的计算移动化,它提供了很多 PC 所不具备的功能和特性,手机作为随身携带的微型通信设备,提供以下两种基于硬件的唯一身份标识码。

- IMSI (international mobile subscriber identification number, 国际移动设备识别码), 存储在 SIM (subscriber identity module, 客户识别模块) 卡中, 网络服务商通过 IMSI 识别用户的手机号码。
- 设备硬件识别码, 可以是 ESN (electronic serial number, 电子序列号), 如每台手机都会被分配一个 ESN、MAC (medium access control, 媒体接入控制) 地址等。

利用两种基于硬件的唯一身份识别码,结合 VPDN 的账号和密码,根据企业对身份认证的要求,在移动智能终端上可提供新的、灵活的、更为严格的身份认证。

(1) 绑定手机号码的 VPDN 拨号增强安全绑定模式

网络服务商提供的移动 VPDN 拨号,除 VPDN 账号密码外,可选增加 IMSI 绑定,即 VPDN AAA 服务器在进行身份验证的同时,也验证手机 IMSI 是否匹配,只有两者均通过,才允许接入。

(2) 用户免 VPDN 账号/密码输入的便捷使用模式

用户需在手机的 APN (access point name, 接入点名

称)配置中设置 VPDN 的账号和密码,不但麻烦,且要求用户具备一定的 IT 技能,同时也加重企业对移动 VPDN 的运维的成本(如需要指导用户如何进行配置),而用户通常只在第一次使用时进行输入,将账号和密码保存在手机本地存储中,在下次拨号时自动接入。

为实现用户零配置,一键拨号的便捷实用,在用户首次拨号时,利用 IMSI 绑定,从 VPDN AAA 服务器中查找 VPDN 的账号和密码,返回给客户端,再由客户端记录在手机本地存储,自动进行拨号接入。

这种方式是在不改变现有 VPDN 接入流程的基础上,利用 IMSI 绑定关系,将用户的身份认证由 VPDN 账号转为手机的 IMSI。

(3) 绑定手机设备的 VPDN 拨号增强安全绑定模式

传统的 VPDN 业务,即使要求 IMSI 绑定,企业用户仍可通过无线数据卡,在 PC 上接入企业内网,存在病毒入侵等安全问题。某些企业由于其行业特殊性,对安全要求特别高,希望用户只能在指定的设备上访问企业内网,即要求 VPDN 拨号过程中增加设备绑定。

读出手机设备识别码,如 ESN,上报 VPDN AAA 服务器进行匹配验证,就可实现手机设备的绑定。为了避免在实际操作 VPDN AAA 服务器中配置用户手机设备识别码过程的困难,用户在首次拨号时,访问 VPDN AAA 服务器发现尚未进行绑定,则根据上报的设备识别码自动完成绑定设定。

4.2 差异化组网新模型

在信息化不断普及的新形势下,企业 VPN 不仅仅提供给自身员工使用,同时也可提供给其他与企业密切相关的用户群使用(如一个企业的用户群可能是企业员工、代理商、供货商、VIP 用户等)。因此,对不同用户群需设置不同的企业 VPN 内的访问权限,以降低安全隐患。如一般企业员工可访问公司总部与分部,VIP 客户只允许访问营业网点,而供货商只需访问备货仓库。

基于 MPLS 的移动 VPDN 以无线接入的 VPDN 域区分用户群,通过 MPLS 基于网络拓扑的访问控制,对不同用户群实现了差异化的网络访问范围限制,如图 4 所示。

首先,无线 VPDN 侧的共享 LNS 将具有不同访问权限的用户群射到不同的 VPDN 域中。如上面的例子中,某企业的 VPDN 终端用户有 3 类,一般企业员工、VIP 客户、供货商,这 3 类用户的 VPDN 账号分别为

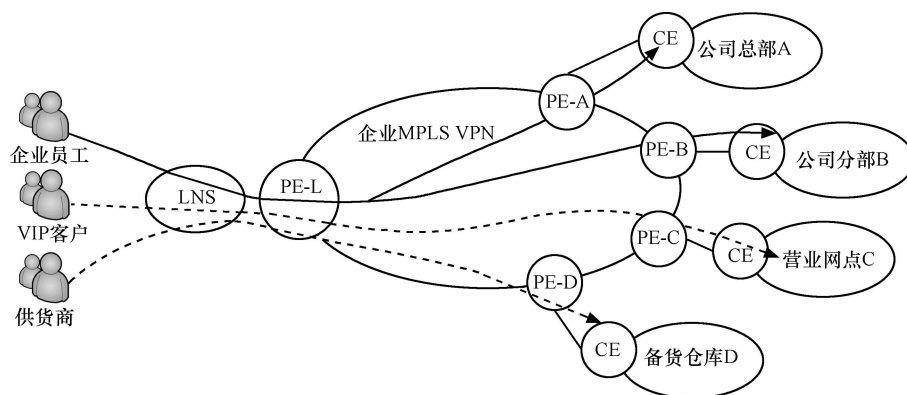


图4 差异化组网应用示例

user@domain1、user@domain2 和 user@domain3。不同的 VPDN 域对应不同的逻辑 LNS。不同的逻辑 LNS 为同一 MPLS VPN 中不同的网络节点。因此,不同用户群的路由映射为 MPLS VPN 中网络节点 LNS 的路由策略,实现了不同用户群的识别与隔离。

其次,根据 MPLS VPN 精确的路由控制,可控制某用户群可访问的企业 VPN 中的不同网点。如图 4 所示,通过 MPLS VPN 个性化的路由控制,一般企业员工可以访问节点 A 与 B,即公司总部与分部,VIP 客户只能访问节点 C——营业网点,而供货商只能访问节点 D——备货仓库。

最后,企业各网点的内网侧防火墙也可自定义地址访问列表,进一步控制具有合法 IP 地址的终端接入该网点的企业内网。

经过用户群访问权限控制机制的实施后,移动终端接入流程延伸了 4 个步骤。

(1)移动终端无线拨号,建立虚拟 IP 通道接入至共享 LNS,LNS 通过用户拨号域名,完成不同用户群的区分。

(2)通过共享 LNS 与企业网络各网点之间搭建的 MPLS VPN,用户移动终端可直接访问客户网络。

(3)MPLS VPN 采用基于网络拓扑(多个星型组网、星型组网与部分网状组网结合)的路由访问控制,限定共享 LNS 不同用户群的不同网络访问范围。

(4)移动终端接入至企业网络侧网络,通过企业网点侧防火墙的访问列表,进入该网点的企业内网。

通过对移动终端身份认证新方案及基于用户群的访问权限控制的实施,企业 VPN 的可管可控性大大增强,做到了只有合法的终端才能接入企业 VPN 以及被允许接入

的终端只能访问被允许的企业内网。

5 结束语

基于 MPLS 的移动 VPDN 为企业客户提供了基于移动宽带网络之上的 VPN 数据专网,为企业的移动终端建立了连接到企业内部的私密隧道,实现了企业内部数据安全、高速、便捷的传输。基于 MPLS 的移动 VPDN 还实现了对移动终端身份的严格认证及对企业不同用户群的访问权限控制,增强了企业 VPN 的可管可控性。但是,技术并不是万能的。企业 VPN 的信息安全真正取决于企业管理制度的完善及员工职业素质的培养,否则,企业中要是出现了引言中介绍的“明星程序员”,那么就是再先进、再安全可控的 VPN 也无济于事。

[作者简介]



黄粤,男,学士,中国电信股份有限公司广东研究院工程师,主要研究方向为政企产品和行业应用解决方案等。



魏颖琪,女,硕士,中国电信股份有限公司广东研究院高级工程师,主要研究方向为移动智能终端技术、通信技术等。

(收稿日期:2013-02-28)