基于 3G 网络的企业数据通信安全方案

邓霄博，杜　勇，朱伟光，陆自强

（迈普通信技术股份有限公司研究院　成都 610041）

摘 要　随着运营商对 3G 投资的不断增加，3G 业务的成熟度及信号质量将会不断地获得提升。凭借其强大、灵活的部署能力，低廉的线路成本以及不断增加的带宽优势，3G 路由器必将在多个行业中得到更广泛的应用，然而，随之而来的安全问题也从未间断过。本文针对 3G 网络在数据通信中的应用、3G 网络的安全机制、3G 路由器安全部署原则和方案等方面，详细地阐述了基于 3G 网络开展企业数据通信应用的安全解决方案。

关键词　3G；路由器；安全；VPDN

1　前言

随着 3G 业务的不断普及，针对企业用户“3G 移动专用网”的需求，运营商推出了 3G 的 VPDN（virtual private dial network）业务，即基于 3G 无线接入方式的虚拟专用拨号网业务，它是利用 L2TP 隧道传输协议，在现有的拨号网络上构建一条虚拟、不受外界干扰的专用通道，实现类似采用有线专用网络的方式访问企业内部网资源。数据通信设备厂商也及时地推出了 3G 路由器来适应行业用户的这个应用趋势，企业网已经全面进入 3G 联网时代。

类似金融、政府这类网点众多、拥有大量离行 ATM 接入、边远乡镇接入和移动网点接入需求的行业用户，都把目光放到了 3G 接入上，因此，如何提高基于 3G 网络开展企业数据通信的安全性，成为对数据安全性要求较高行业大规模应用 3G 网络的最大障碍。

2　3G 网络数据通信应用概述

基于 3G 的数据通信应用有以下几种组网模式。

（1）访问 Internet

3G 路由器配置 3G 模块，使用公用的 APN 名称、用户名密码，通过运营商无线基站接入 Internet 网络，配置 NAT 地址转换功能，3G 路由器内网 PC 通过 3G 网络访问公网资源，如网页浏览、公网邮箱、即时通信、网络下载等资源，如图 1 所示。

（2）Internet +VPN 隧道

3G 路由器配置 3G 模块，使用公用的 APN 名称、用户名密码，通过运营商无线基站接入 Internet 网络。对于需要访问公网资源的数据流，经过配置 NAT 地址转换后直接与 Internet 进行通信；对于需要访问总部机构私网资源的数据流（如公司 VoIP 语音电话、视频会议系统、内部办公 OA 系统等），通过 3G 路由器与总部路由器建立的 IPSec VPN 加密隧道进行直接通信。如图 2 所示。

（3）3G VPDN 专网

如图 3 所示，为保证企业大客户 3G 接入网的业务安全需求，运营商可向用户提供专线 APN（access point name）传输方式，为用户提供专用的接入点名称，并可提供

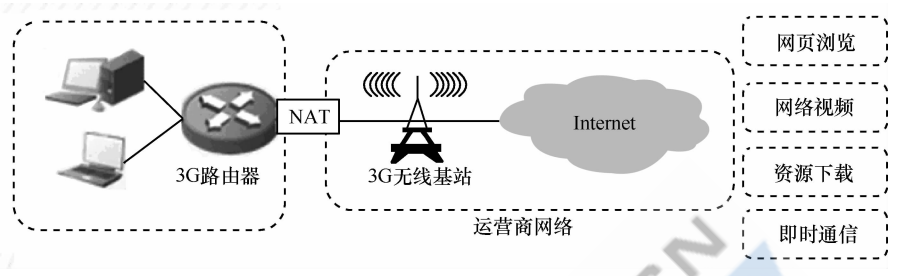

图 1 访问 Internet

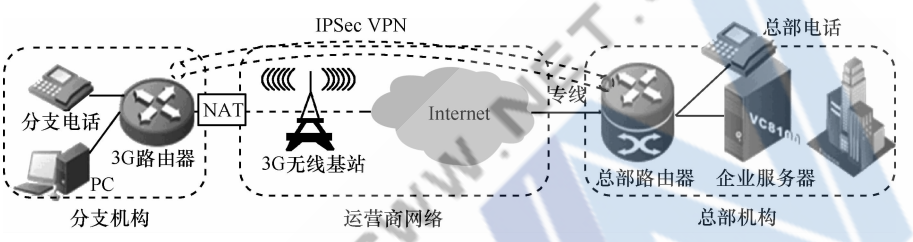

图 2 Internet+VPN 隧道

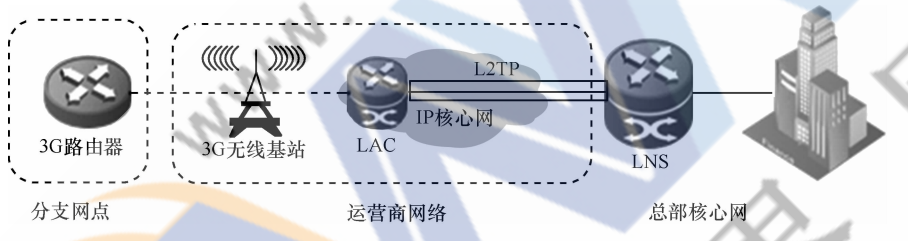

图 3 3G VPDN 专网

用户名、密码、IMSI 的多重安全认证功能。LNS 为用户总部端设备(路由器、VPN 设备)通过专线与运营商网络互连，分支网点的 3G 路由器配置 3G 模块，使用企业申请的专用 APN 名称、用户名密码接入 3G 网络。运营商通过 APN 名称或用户名密码判断该用户是否为企业专网用户，之后交由 LAC 设备触发与用户端 LNS 设备的 L2TP 认证协商，并最终由 LNS 设备为分支网点 3G 路由器分配私网 IP 地址，实现与分支网点与总部私网的专线互通。

基于 3G VPDN 的专网是运营商主推的一种模式，本文将着重分析基于 3G VPDN 专网应用的安全部署问题，下面首先分析 3G 的安全机制。

3 3G 的安全机制

无线通信本身的特点是既容易让合法用户接入，也容易被潜在的非法用户窃取，因此，安全问题总是同移动通信网络密切相关。针对无线通信存在的安全问题，3G 系统进行了如下优化：

- 实现了双向认证，不但提供了基站对 MS 的认证，也提供了 MS 对基站的认证，可有效地防止伪基站的攻击；
- 提供了接入链路信令数据的完整性保护；
- 密钥长度增加为 128 bit，改进了算法；
- 3GPP 接入链路数据加密延伸至无线接入控制器(RNC)；
- 3G 的安全机制具有可拓展性，为将来引入新业务提供安全保护措施；
- 3G 能向用户提供安全可视性操作，用户可随时查看自己所用的安全模式及安全级别。

在密钥长度、加密算法选定、鉴别机制和数据完整性检验等方面，3G 的安全性能远远优于 2G。但是 3G 的这些安全机制仅仅局限于无线部分，针对基于 3G 接入的无线企业网而言，无线部分的安全是远远不够的，需要保证数据在整个传输过程中的安全性，即端到端的安全性。

4 3G 路由器接入安全部署探讨

随着 3G 数据通信应用的发展，数据通信厂家推出了 3G 安全路由器，能够很好地解决 3G 网络数据安全传输问题。下面以 3G 安全路由器在金融离行 ATM 的应用为例做

一个分析。

如图 4 所示，金融离行 ATM 网点使用 3G 路由器无线接入 3G 无线网络，通过运营商 3G 无线基站及 IP 核心网连接金融一级或二级网汇聚路由器，实现了离行 ATM 与金融一级或二级网的业务互访。

3G 接入安全部署如图 5 所示。

根据应用模式，3G 接入安全部署需要基于以下几点考虑。

(1)接入认证安全

要求在进行 3G 网络登录时，提供基于用户名、密码、IMSI(international mobile subscriber identity，国际移动用户识别码)的多重身份认证绑定功能，保证接入用户的惟一性，防止非法用户利用 3G 网络接入用户专用网络。

(2)端到端的私有性

为了保证用户业务的私密性，必须要求解决方案从网点 3G 路由器到金融、政府行业一级或二级网汇聚路由器提供端到端的私有专用通道，以保证网点业务在运营商网络传输过程中的私有性。

(3)端到端的安全加密

为了进一步保证网点业务数据在运营商 3G 无线网络以及 IP 核心网传输过程中的安全，防止黑客利用其他非法手段截取金融、政府等行业敏感数据，要求安全解决方案必须提供网点 3G 路由器到金融、政府行业一级或二级网汇聚路由器端到端的加密安全。特别是金融和政府类信息敏感行业，这种加密安全更需要国家密码管理委员会办公室(以下简称国密办)加密算法的支持，以保障国家信息安全的高度机密性。

5 3G 路由器安全接入解决方案

如图 6 所示，网点的 3G 安全接入部署方案，分别通过

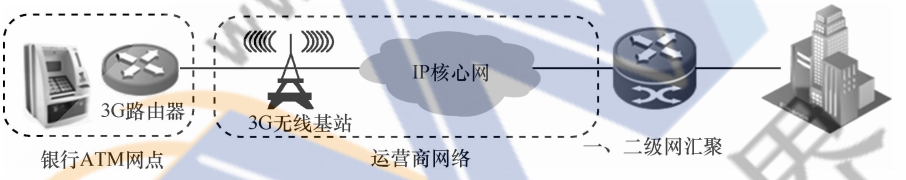

图 4 3G 路由器接入

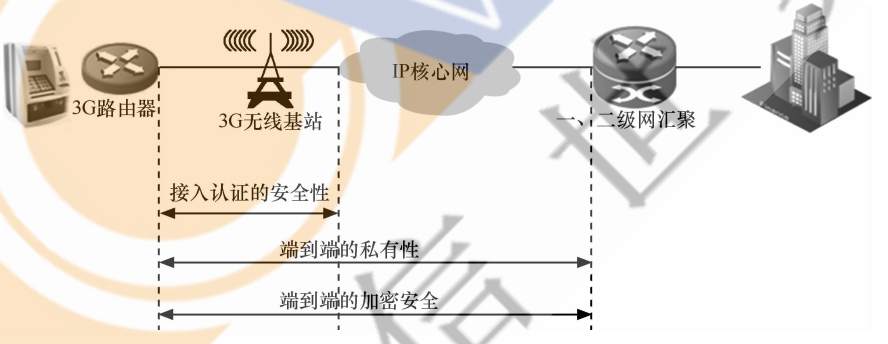

图 5 3G 接入安全部署

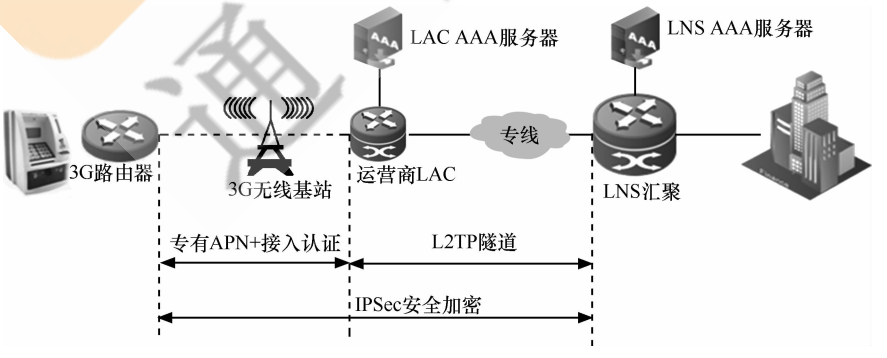

图 6 3G 安全接入解决方案

专有 APN+绑定接入认证、L2TP 私有隧道、IPSec 安全加密技术来实现 3G 部署时对接入认证、端到端的私有性、端到端安全加密的安全原则，具体部署方案如下。

(1)专有 APN+绑定接入认证

在进行网点的 3G 无线接入部署时，需要先向运营商申请分配的专网 APN，类似行业专用的 3G 无线局域网，保证网点接入 3G 网络后，只能访问行业专用网络，保证无法与其他网络进行通信。网点采用 3G 路由器接入方式，运营商会将网点用户的 IMSI 信息(IMSI 是在运营商网络中惟一识别移动用户的号码，由 15 位数字组成，存于 SIM 卡中)、终端用户的账号和密码事先配置在运营商的认证服务器上。当网点的 3G 路由器发起无线连接时，只允许绑定信息合法的用户通过用户名、密码的 AAA 认证后接入 3G 专用网络，防止非法 SIM 卡用户拨入用户 3G 专网。

此外，可进一步通过 3G 路由器设置 SIM 卡的 PIN 码保护功能，只有知道 SIM 卡的 PIN 码才能触发 3G 拨号，防止非法用户获取到用户 SIM 卡后进行非法操作，保证了 SIM 卡使用的安全。

(2)L2TP+IPSec VPN 私有隧道

为了保证 3G 接入网点的数据业务在运营商 IP 核心网中传输的的私有性，用户向运营商申请企业集团用户 3G 的 VPDN 业务，基于 3G 无线接入方式的虚拟专用拨号网业务，它是利用安全的 L2TP 隧道传输协议，在现有的拨号网络上构建一条虚拟、不受外界干扰的专用通道，从而能够安全地访问企业内部网资源。

运营商会为行业用户的 3G VPDN 业务提供 L2TP 的 LAC 端路由器及配套的 AAA 服务器。金融、政府等行业一级或二级网汇聚层采用一台路由器作为 L2TP 的 LNS 端，并部署一台 AAA 服务器。LAC 路由器主要负责对 3G 用户的接入认证，与该用户所属企业的专有 LNS 建立 L2TP 隧道。一级或二级网汇聚层的 AAA 服务器主要存放网点路由器建立连接时所需要的用户名和密码。用户名的格式为 xx@xx.com，其中 @ 前面的字符串可以由用户自行定义，@ 后面的字符串即域名。运营商 AAA 服务器通过域名确认该用户的接入权限。运营商 AAA 服务器与企业 AAA 服务器的用户名和密码必须一致。

L2TP 私有隧道建立过程如图 7 所示，过程如下：

- 网点路由器通过 3G 网络完成对接入用户的 APN 认证；
- 路由器启动 PPP 拨号向 LAC 发出认证请求；
- LAC 把认证请求转至运营商 LAC AAA 服务器；
- AAA 服务器将会回复认证结果并返回该用户所属的 LNS 地址、VPDN 隧道属性等信息；
- LAC 向返回的 LNS 地址发出 L2TP 隧道建立请求，隧道建立成功(请求建立隧道的认证可选)；
- LNS 对网点路由器的用户名和密码进行重新认证(LNS 对网点路由器的重认证可选)；
- L2TP 隧道建立完成。网点路由器对应的拨号接口 UP，建立正常私有隧道通信；

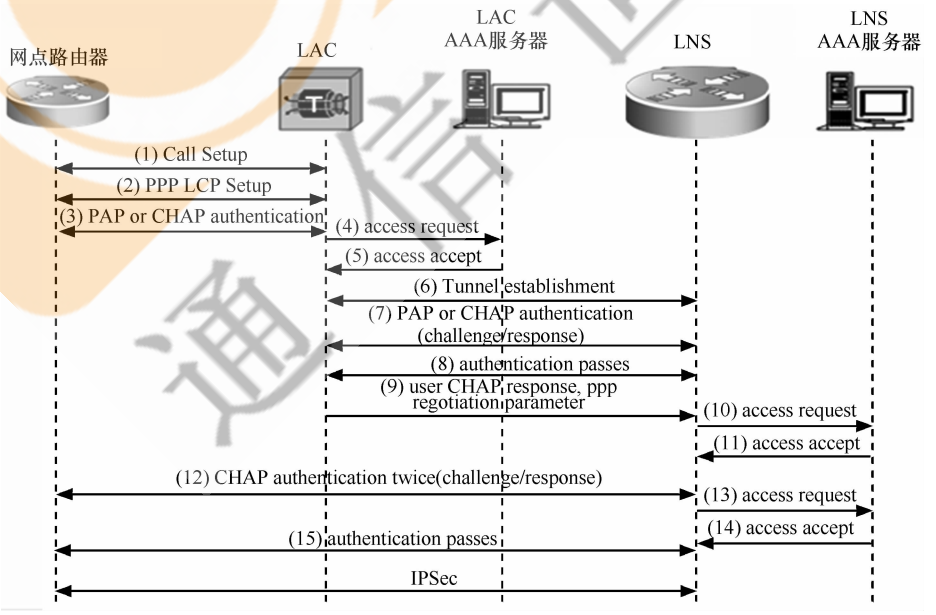

图 7　加密隧道建立过程

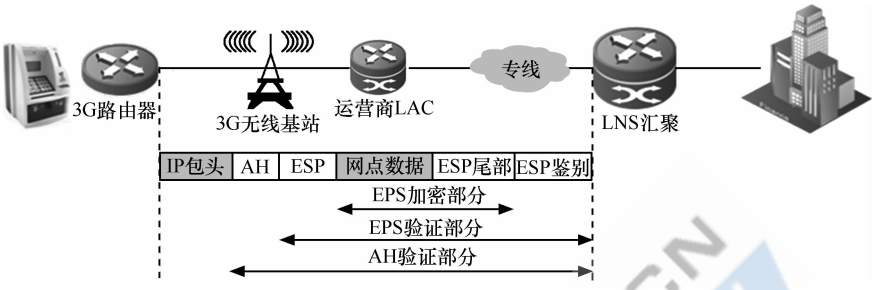

图 8　IPSec 安全加密

· 如果网点发起了能够触发 IPSec VPN 的流量，则 IPSec VPN 隧道建立过程启动，网点路由器与 LNS 发起 IPSec VPN 连接请求。

(3)IPSec 安全加密

针对端到端的安全加密原则，如前文所述，3G 技术自身具有加密验证技术，但是 3G 的加密验证技术只针对无线部分，而在 IP 核心网部分，从 LAC 到 LNS 之间的 L2TP 隧道是不加密的，数据还是明文传送。而从 LAC 到网络中间还有可能经过运营商的 IP 网络，为了达到端到端的加密传输，需要在网点和总部路由器之间，采用 IPSec 实现端到端的加密，如图 8 所示。

IPSec 通过 AH、ESP 协议保证了数据的安全传输。

· 私有性：用户的敏感数据以密文形式传送；
· 完整性：对接收的数据进行验证，判断数据是否被篡改；
· 真实性：验证数据源，判断数据来自真实的发送者；
· 防重放：防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。

按照 IPSec VPN 技术要求，支持的加密算法主要有 DES、DES、AES128、AES192、AES256 等，要求支持的 HASH 算法为 MD5 和 SHA 等。此外，拥有国家商用密码管理办公室颁发的商用密码产品资质的设备商，除了常见的加密算法外，还能够为金融、政府等行业用户的 3G 接入提供符合国密办加密算法的支持，并遵照国密办 IPSec VPN 技术规范要求对路由器进行设计，能进一步确保国家信息安全。

6　结束语

企业网进入 3G 无线联网时代，更加完善的网络安全解决方案有利于基于 3G 接入的无线企业网得到真正的规模应用。在信息安全已经上升到国家战略层面的今天，如何在通信技术不断发展的情况下，始终维持一个相称、可控的安全机制，是一个需要持续讨论的话题。相信在政府和企业的推动下，坚持建设自己的安全网络，牢牢把握住信息安全竞争中的主动权，更有利于基于 3G 网络的企业数据通信的蓬勃发展。

Security Solution of Data Communication Based on 3G Network

Deng Xiaobo, Du Yong, Zhu Weiguang, Lu Ziqiang
(R&D Institute of Maipu Communication Technology Co., Ltd., Chengdu 610041, China)

Abstract　With more investment in 3G from mobile operating enterprises, business maturity and signal quality will continue to increase. 3G routers are wildly used in various sectors because of the characteristics such as deployment flexibility, cost-saving maintenance and ever increased band-width. However, people always doubt the security of 3G router when using them. By focusing on the application of data communication based on 3G network, 3G security mechanism, safe deployment principle and solution of 3G router, this article explains the security solution of data communication based on 3G network.

Key words　3G, router, security, VPDN
(收稿日期：2010-07-22)