利用 OpenVPN 搭建省级业务系统远程维护通道的预研

王 省，刘乖乖，王丽霞
（国家气象信息中心系统工程室，北京 100081）

摘要：首先介绍了 OpenVPN 的核心原理，然后介绍了利用 OpenVPN 开源软件搭建省级业务系统远程维护通道的实验，最后介绍了基于搭建的 VPN 通道进行 OpenVPN 远程访问权限控制功能的测试，并得出结论：OpenVPN 能够实现点对网络、点对点和点对端口三级访问权限的控制，能够满足建立省级业务系统远程维护通道的技术要求。

关键词：OpenVPN；VPN 远程访问权限控制；TUN/TAP
中图分类号：TP302 **文献标识码**：A **文章编号**：1673-1131（2013）01-0019-02

Build a provincial business system remote maintenance channel using OpenVPN

Wang Xing, Liu Guaiguai, Wang Lixia
（System Engineering office of National Meteorological Information Center，Beijing 100081）

Abstract:This article first introduced the OpenVPN core principle, then introduced the use of Open VPN open source software to build the provincial business system remote maintenance channel experiment, finally introduced OpenVPN remote access control function test based on the experiment, and the conclusion: OpenVPN can realize the point to the network, point to point and point to port three level access control, and can meet the technical requirements of establishing provincial business system remote maintenance channel.

Key words: OpenVPN；VPN remote access control；TUN/TAP

0 引言

近年来随着气象事业的飞速发展，中国气象局先后承担了多个投资过亿的全国性的建设项目，比如气象监测与灾害预警工程、新一代天气雷达信息共享平台、突发公共事件预警信息发布系统等。每个项目的实施都将伴随着大批软硬件系统的全国部署。一方面全国气象业务水平得到了整体的提升，另一方面计算机设备的更新换代也增加了省级技术人员的维护难度。由于各省技术力量不均衡，项目的全国技术培训又往往滞后，这样会导致新的业务系统已经部署在省级，但省级对这些业务系统的软硬件设备还一无所知的情况，出现了问题也无法及时解决，必须依靠国家级以及设备和软件开发商的技术人员的远程指导或现场维护。因此，建立一个省级业务系统远程维护通道势在必行。

目前国家级技术人员实现远程维护的手段主要是通过登录国家级内网的服务器，然后一级一级地跳转到省级的业务服务器。这种方式会导致两个问题：第一是不方便，国家级、省级的网络和系统管理人员必须事先对防火墙和服务器进行相应的配置；第二是只能实现命令行方式的操作，无法使用设备提供的图形化管理界面，这样会增加维护的难度。而通过 VPN 的方式，就可以方便地使用这些管理工具。

OpenVPN 是近年来发展势头最为迅猛的 VPN 技术。它采用虚拟网卡技术作为隧道机制，摒弃了 IPSEC VPN 沉重冗余的安全机制，使用 OpenSSL 库加密数据和控制信息，不仅具有良好的性能，而且提供友好的用户 GUI。最重要的是作为 Linux 下开源 VPN 的先锋，用户能够很方便地下载各种 OpenVPN 的免费版本进行应用方面的研究和测试。

本文首先介绍了 OpenVPN 的核心原理，然后就利用 OpenVPN 提供的免费版本搭建省级业务系统远程维护通道的试验进行了介绍，并对 OpenVPN 技术在气象行业的应用进行了探讨。

1 OpenVPN 核心原理介绍

OpenVPN 是一款功能强大的开源软件。它利用虚拟网卡将网络 2、3 层的数据包传送到用户空间，然后使用应用层 SSL/TLS 技术加密传输，从而实现隧道功能。其中虚拟网卡是通过 TUN/TAP 驱动程序实现的。TUN 表示虚拟的点对点设备，TAP 表示虚拟的以太网设备。TUN/TAP 驱动程序中包含两个部分，一部分是字符设备驱动，另一部分是网卡驱动。网卡驱动可以用来接收来自 TCP/IP 协议栈的网络包并发送出去，或者将接收到的网络包传送给协议栈处理；而字符驱动可以实现网络包在内核与用户空间之间传送，模拟物理链路的数据接收和发送，如图 1 所示。

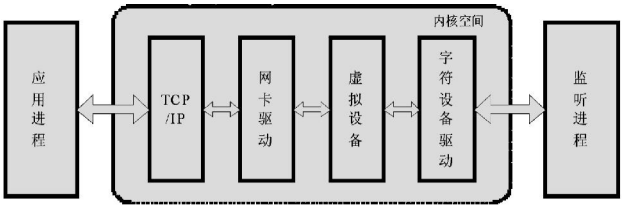

图 1 TUN/TAP 实现原理图

图 1 说明了使用 TUN/TAP 技术构建 VPN 隧道的流程。为了在两个节点之间建立 VPN 通道，这两个节点必须安装 TUN/TAP 虚拟设备。TUN/TAP 设备主要用于为节点分配虚拟专用网范围内的 IP，并将发送到该设备的数据包传送到用户空间。

当本地应用进程向虚拟专用网范围内的 IP 发送数据包时，路由信息的所有数据都会发送到 TUN/TAP 虚拟设备。而监听此虚拟设备的本地 VPN 进程就能够由 TUN/TAP 虚拟设备中读取应用程序发出的网络数据包。VPN 进程将这个数据包使用隧道协议封装后，经由真实通信链路发送到虚拟专用网对方节点。对方节点上的 VPN 进行拆包后，将这个数据包写入该节点的 TUN/TAP 虚拟设备，此时该节点上的远程进程就可以接收到这个数据包。整个过程实现了本地进程经由隧道直接将数据包发送到了对方节点。尽管说 TUN/TAP 设备是虚拟设备，但在操作系统看来，它与真实设备没有任何区别。

因此，防火墙对 TUN /TAP 设备依然有效。也就是说可以为 TUN /TAP 设备设置防火墙规则来保证该设备上的通信安全。

2 利用 OpenVPN 软件搭建省级业务系统远程维护通道实验

2.1 实验部署图

利用 OpenVPN 软件搭建省级业务系统远程维护通道的部署图为图 2 所示：

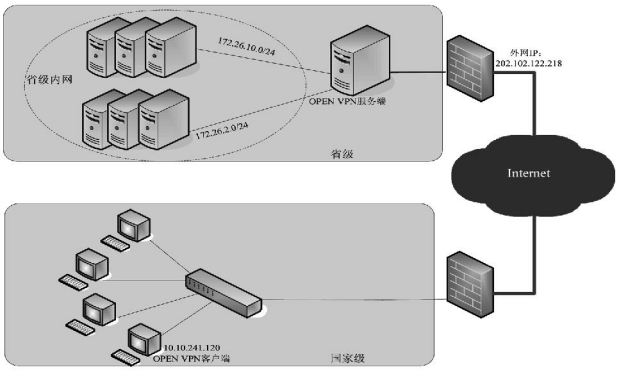

图 2 省级业务系统远程维护通道部署图

其中省级部署 OpenVPN 服务端的服务器是省级内网的边界服务器。该服务器具有多个网卡，一方面与省级内网相连，一方面与 Internet 相连。它的操作系统为 R edHat，Internet ＩＰ地址为 202.***.122.218。国家级中只要能连接 Internet 的终端均可作为 OpenVPN 的客户端。

2.2 实验步骤

利用 OpenVPN 软件搭建省级业务系统远程维护通道的步骤为：

(1) 从 OpenVPN 的官方网站(http://openvpn.net)下载基于 RedHat 平台的 OpenVPN 软件包。

(2) 在 OpenVPN 服务器上安装 OPENVPN 软件包，安装命令为：

rpm -i openvpn-as-1.8.4-RHEL5 .x86_64.rpm

(3) 对 OpenVPN 服务端进行初始化，初始化命令为：

/usr/local/openvpn_as/bin/ovpn-init － force

初始化过程中会提出一些问题，选择默认即可。

(4) 初始化完成后，OpenVPN 软件包在 OpenVPN 服务器上建立了用户名为“OpenVPN”的用户，需要为该用户设置密码。

(5) 用“OpenVPN”用户登录 OpenVPN 的 web 管理界面 https://202.***.122.218 :943/admin。在管理界面中的配置客户端的用户名和密码。

(6) 从国家级终端用客户端的用户名和密码登录省级 OpenVPN 服务端 https://202.***.122.218:943,登录后客户端会自动下载并安装 OpenVPN 客户端软件。

(7) 从客户端发起连接请求，建立 VPN 通道。

(8) 国家级客户端能够直接访问省级业务系统。

3 OpenVPN 软件个人用户远程访问权限控制

使用省级业务系统远程维护通道的用户有本省的业务人员、国家中心的业务人员和项目承建商的技术人员。针对不同用户，应该赋予不同的权限，以保障省级气象业务系统的安全。其中本省的业务人员应该能够访问整个省级业务系统，国家中心的业务人员能够访问省级业务系统中的指定服务器，项目承建商的技术人员应该只能访问省级业务系统中某个服务器上的指定应用。综上所述，OpenVPN 应该具有点对网络、点对点、点对端口三个级别的访问权限控制。因此需要对 OpenVPN 的访问权限控制功能进行专门测试。

OpenVPN 是通过组权限和用户权限的结合实现用户访问权限的控制。其中组权限的定义包括三级：网段、IP 地址和端口号。属于该组的用户都拥有该组定义的组权限。在用户权限中可以开通除组中已定义网段外的其他网段的访问权限，但是用户权限只能增加网段，不能增加 IP 地址和端口号。

基于上述原理我们在搭建的 VPN 实验环境中进行了 OpenVPN 个人用户远程访问权限控制功能的测试。其中国家级客户端的 IP 地址为 10.10.241.120，所属组的名称为 test1，省级 OpenVPN 服务端联通的网段有 172.26.2.0/24 和 172.26.10.0/24，172.26.2.1 服务器上安装 ORACLE 数据库，端口号为 1521，并启动了 ftp 服务。

3.1 网段访问权限控制测试

组权限	用户权限	测试方式	预期结果	测试结果
172.26.2.0/24	无	Ping 172.26.2.1	成功	成功
		Ping 172.26.10.1	不成功	不成功
172.26.2.0/24	172.26.10.0/24	Ping 172.26.2.1	成功	成功
		Ping 172.26.10.1	成功	成功

3.2 IP 地址访问权限控制测试

组权限	用户权限	测试方式	预期结果	测试结果
172.26.2.0/24 172.26.10.1	无	Ping 172.26.2.1	成功	成功
		Ping 172.26.10.1	成功	成功

3.3 端口访问权限控制测试

组权限	用户权限	测试方式	预期结果	测试结果
172.26.2.0/24 172.26.10.1 172.26.2.1：1521	无	通过 SQL PLUS 访问 172.26.2.1 的 ORACLE 数据库	成功	成功
		ftp 登录 172.26.2.1	不成功	不成功

综上所述，OpenVPN 软件对个人用户的远程访问权限实现了点对网络、点对点和点对端口的控制，完全符合省级业务系统远程维护通道的要求。

4 结语

虽然 OpenVPN 在性能上与专用的硬件 VPN 设备还有差距，但是 OpenVPN 提供的免费版本具备了基本的访问控制功能和日常管理维护功能，除了在搭建省级业务系统远程维护通道上可以考虑使用该技术外，还可以考虑在气象部门的市、县两级采用。随着对 OpenVPN 技术了解的逐步深入，相信 OpenVPN 能够在气象行业发挥更加重要的作用。

参考文献：

[1] Markus Feilner.OpenVPN Building and Integrating Virtual Private Networks. 2006.

[2] Jon C.Snader.VPNs Illustrated:Tunnels,VPNs,and IPsec. 2004

[3] 郭学超，濯正军. OpenVPN 体系安全性研究[J]. 科学技术与工程, 2007(4)：1671-1819

[4] 唐黎，朱正超. 利用 OpenVPN 实现在系统中的多种安全访问[J].计算机与信息技术，2006

作者简介：王省(1978-)，男，北京人，工程师，研究方向是计算机科学与技术。