文章编号：1006-4354（2010）05-0037-02

VPN 技术在气象网络中的应用

陈艺宏，林荣惠，张 磊
（漳州市气象局，福建漳州 363000）

中图分类号：P409 文献标识码：B

1 VPN 技术

1.1 VPN 概念

VPN（virtual private network）是指以公用开放的网络（如 internet）作为基本传输媒体，当需要传输机密数据时，通过端点上的 VPN 设备在公共网上建立一条虚拟专用网络通道，通过加密和验证网络流量来保护数据在公共网络上传输不被窃取和篡改，从而向最终用户提供类似于私有网络（private network）性能的网络服务技术。

1.2 隧道技术

隧道技术模仿点对点连接技术，依靠互联网服务提供商（ISP）和其它网络服务提供商（NSP）在公用网中建立自己专用的数据包传输隧道。隧道协议用附加报头封装帧并提供路由信息，封装后的包能够通过中间公网[1]，到达公网的目的地后，帧被解除，数据包被继续送到最终目的地。

1.3 IPSec 协议

VPN 的隧道协议可分为第二层隧道协议和第三层隧道协议。典型的第二层隧道协议有 PPTP、L2F、L2TP 等，第三层隧道协议有 GRE、IPSec 等，使用包作为交换基础，用附加的 IP 报头封装 IP 包，通过 IP 公网发送出去。

福建省气象部门目前所使用的 NetEye 东软防火墙的 VPN 功能是按照 IPSec 协议标准开发，IPsec 提供了两种安全机制：认证和加密。认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据传输过程中是否遭篡改；加密机制通过数据加密运算来保证数据的机密性，以防数据在传输过程中被窃听[2]。IPsec 协议中的 AH 协议定义了认证的应用方法，提供数据源认证和完整性保证；ESP 协议定义了加密和可选认证的应用方法，提供数据可靠性保证。

2 VPN 在气象网络中的应用

福建省气象局于 2007 年 6 月为各市局配备东软（NetEye）FW4016 硬件防火墙，县局配备东软（NetEye）SG500 硬件防火墙，省气象信息中心配置东软（NetEye）FW4120 硬件防火墙。防火墙自带 VPN 功能，通过防火墙建立 VPN 连接，实现远程数据传输、共享，为远程访问气象内部网络提供便捷、易行、经济、有效的数据传输途径。

2.1 NetEye VPN 的特点

NetEye VPN 同时集成了防火墙和 VPN 的功能，具有 NetEye 防火墙先进的体系结构和可靠的安全性，可防御各种攻击，保护 VPN 自身的安全性，具有与防火墙一致的身份验证机制，具有 VPN 产品数据传输的完整性和机密性。

NetEye 防火墙对信息传输的安全性保护体现在 4 个方面。

（1）数据机密性 由于防火墙间传输的信息是加密的，从一台防火墙发出的信息除指定的接收方外其它第三方不能偷听或者窃取到有意义的信息。

（2）数据完整性 防火墙验证由对等的防火墙发来的数据包，以确认在传输期间数据没有被

收稿日期：2010-05-08

作者简介：陈艺宏（1984—），男，福建漳州人，本科，主要从事信息网络与装备保障。

改变。

(3) 数据来源认证 能够验证发送过来的IP数据包的源地址，以防止IP欺骗。

(4)防重放 能够检测并拒绝重发的数据包，从而防止DoS攻击。

2.2 NetEye VPN 工作原理

如图1所示，与网关（NetEye）相连的内部网是受保护的网络，另一端则是不安全的公用互联网或专用网络，两个这样的路由器（网关）建立起一个安全通道，通信就可以从本地受保护子网发送到另一个远程保护子网，形成了一个VPN。网关(NetEye)C、D上运行隧道模式ESP，保护两个网内的主机通信，所有主机可不必配置IPSec。当主机A向主机B发送数据包时，网关(NetEye)C要对数据包封装，封装后的包通过隧道穿越公用网络后到达网关(NetEye)D，由D对该数据包解封，再转发给主机B，反之亦然[3]。

图1 通过NetEye防火墙实现VPN

2.3 气象VPN组建思路

福建省气象系统信息化建设已具有一定的规模，从省气象信息中心到各市县气象局全部使用SDH专线连接，保证数据实时传递，但这样的专线网络仍存在一些问题：一是大量的雷达、区域自动站信息传输，使得线路容易出现拥堵；二是现有网络一旦出现故障，没有合理的线路作为补充备份。针对这些问题，气象VPN组建思路：①一旦专线出现故障，能快速切到VPN线路；②实现气象系统决策者远程移动办公；③成本低廉、资料传输安全可靠；④VPN网络结构为二级，即各县市气象局直接连到省局网络中心，不需要地市级中转，减少层次，提高稳定性。

2.4 气象VPN网络的系统结构

各县市局与省气象局采用VPN设备通过互联网实现互联，SDH专网出现故障后，VPN备份网络可接替业务信息传输工作。全省各地市县PC机通过VPN连接与省局内部网络通信时，先由ISP将所有的数据传送到VPN中心网关NetEye FW4120，最终NetEye FW4120将所有的数据传送到目标计算机。

各县市局的测报主机生成IP包，目的地址是省局的服务器。该包从起始测报主机被发送到本地网络边缘的NetEye防火墙。防火墙根据安全策略强制加上AH或ESPN头，对没有SA的安全策略利用IKEA建立新的SA，进行IPSec的处理，并将网包打包，添加外层IP包头。外层包头的源地址是本地防火墙，目的地址是省局服务器网络边缘防火墙，该包被传送到服务器的防火墙，中途的路由器只检查外层IP包头。服务器网络的防火墙把外层IP包头除掉，利用分组的AH或ESP头调用IPSec处理，进而决定IPSec处理的应用是否正确，验证正确，解密恢复到原始数据并转发到服务器。

2.5 安全和管理

由于互联网的接入，安全管理问题显得更为突出。各县市局通过防火墙、路由器配置相应的规则策略，防止黑客、病毒攻击[4]；定制访问控制规则，解决网络访问控制问题，保证信息访问的安全性；配置安全策略，封禁不用端口，将IP地址和计算机网卡物理地址捆绑。此外，严格执行计算机安全管理制度，加强业务人员的工作责任心和安全防范意识也非常重要。

3 结语

VPN备份网络可在主干链路出现故障时及时切换，保障气象信息的传输。通过VPN建立远程连接具有架设方便、投入费用低、组网简单、资料传输安全可靠等优点，对实现气象实时数据和资源的共享，加快气象业务网络化的进程具有重要意义。

参考文献：

[1] 张千里，陈光英．网络安全新技术[M]．北京：人民邮电出版社，2003：127-159.

[2] 邓少鲲，唐宏伟，孙彩霞．虚拟专网技术与解决方案[M]．北京：中国电力出版社，2003：31-87.

[3] 戴宗坤，唐三平．VPN与网络安全[M]．北京：电子工业出版社，2002：57-98.

[4] 王达．虚拟专用网（VPN）精解[M]．北京：清华大学出版社，2004：112-164.