一种新型的安全网关模型的设计

A New Model of Secure Gateway

陈 兵[1] 万 晖[2] 王立松[1] 丁秋林[1]

(南京航空航天大学计算机科学和工程系 南京210016)[1]

(摩托罗拉南京软件中心 南京210029)[2]

Abstract With the growing popularity of the corporate Intranets, network security is a foremost concern for most group and industry today. The message must be authentic, confidential, integrated, reliable and undeniable when they are transferred by networks connected to Internet. Up till now, firewalls and VPN have served as the primary sources of network security. Although the firewall and VPN protect the users' private networks, they limit the communications of subnets distributed in the corperate. The traditional firewall will discard packages sent to private subnet. At first this paper analyses the limitations of firewall which used in the envirement of mutiple subnets, and then brings up a new module of secure gateway with low cost, high package transform efficiency and mechanism of user authentication and access control.

Keywords VPN, Firewall, Gateway, Network security

随着 Internet 访问的增加，传统的 Internet 接入服务已越来越满足不了用户需求，因为传统的 Internet 提供浏览、电子邮件、文件传送等相对比较单一的服务，没有服务质量保证，没有权限和安全机制，VPN(虚拟专用网)的提出就是来解决这些问题。VPN 利用不可靠的公用互联网络作为信息传输媒介，通过附加的安全隧道、用户认证和访问控制等技术实现与专用网络相类似的安全性能，从而实现对重要信息的安全传输，是对企业内部网的扩充。通过 VPN，企业的 Intranet 能够与供应商、客户的 Intranet 通过 Internet 进行安全的数据传输，同时，企业的移动用户也能够通过 Internet 访问企业的 Intranet。比较常用的 VPN 实现方式是采用具有加密功能的防火墙。

防火墙[1]是设置在用户网络和外界之间的一道屏障，防止不可预料的、潜在的破坏侵入用户网络。防火墙在开放和封闭的界面上构造一个保护层，属于内部范围的业务，依照协议在授权许可下进行；外部对内部网络的访问受到防火墙的限制。尽管防火墙能够有效防止来自外部的非法入侵，但是防火墙并不是万能的，它也存在众多的缺陷。

本文以我们实施 CIMS 工程的某集团大公司的应用环境为背景，分析了在这种环境下使用防火墙所存在的问题，提出了一种新型的安全网关模型。

1 防火墙体系的缺陷

在文[2]中，丁轶凡等给出了基于 SOCKS V5[3]防火墙的 VPN 系统的实现；在文[3]中，NEC 实验室提出了 SOCKS 服务器作为边界网关的方法。这两种方法的主要思想是通过设置一个 SOCKS 服务器，实现企业和供应商以及客户之间跨越 Internet 的网络连接。这里，SOCKS 服务器实际就是一个防火墙。这种方法能够有效地解决企业之间通过 Internet 进行资源互访的安全问题，并强化了用户认证和信息的加密传输。但是，这种方法同其它采用防火墙机制的模型一样，如果应用在集团大公司或者行业用户背景下，则存在一些问题：

问题1：IP 包的不可达问题。考虑图1所示的拓扑结构，子网1和集团总部通过防火墙与 Internet 隔离，而集团总部有若干较大的部门，这些部门也建立了子网，并且通过防火墙与总部网络隔离。在这种情况下，子网1的 IP 包不能到达子网2或者子网3，因为这些访问内部子网的 IP 包将被防火墙隔离。而对于集团公司的众多局域网而言，它们之间应该可以根据授权进行互相访问。

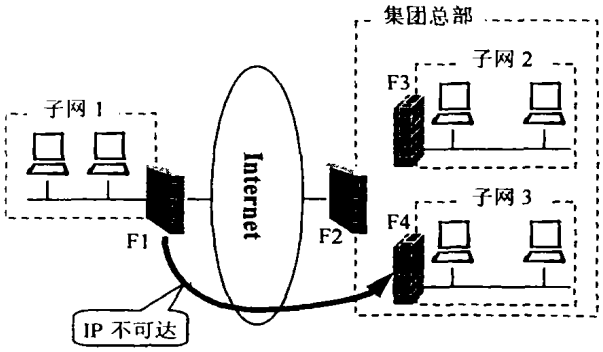

图1 多子网的防火墙体系

问题2：包的传输效率问题。对于图1，如果需要解决 IP 包不可达问题，则可以用多 VPN 和防火墙解决，如图2所示。

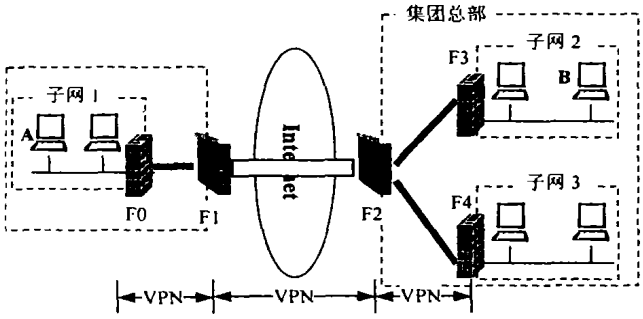

图2 基于防火墙的多 VPN 体系

陈 兵 讲师，博士研究生，主要从事计算机网络和信息安全研究。万 晖 软件工程师。王立松 讲师，博士研究生。丁秋林 教授，博士生导师。

子网1和集团总部之间通过 VPN 连接，子网2和子网3与集团总部之间也通过 VPN 连接，在这种体系中，子网1和集团总部的各个部门之间可以进行安全的通信。现在假设 A 发送数据给 B，来自子网1的数据包经过防火墙 F0后，IP 包将被加密，到达 F1后，IP 包将再次被加密，送到 F2，F3对其进行解密，并送给子网2中的 B 用户。可以将 IP 包在传送过程中的变化用图3来表示。

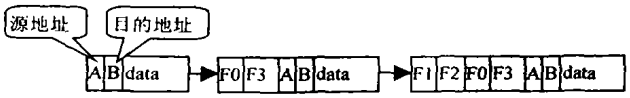

图3　IP 包在传输过程中的变化

从图3可以看出：①IP 包在传送过程中，在 VPN 的入口处需要加上相关的协议头，然后通过 VPN 隧道进行传输，因此，在传输过程中，IP 包头不断增长，使得包的传送效率降低；②在 VPN 入口处，IP 包将被加密后再送到隧道传输，到达出口处再进行解密。IP 包经过两次加解密操作，这实际上是没有必要的，同时，VPN 体系中加解密操作需要开销系统较多的资源。

因此，本文提出的安全网关(SGW：Secure Gateway)模型将着重解决以上两方面的问题。

2　安全网关模型

首先给出基于安全网关的应用模型，如图4所示。每个子网都通过安全网关连接。对每个子网内的某节点 A 而言，如果希望访问目标节点 B，则整个工作流程包括：

①A 发出请求，试图直接与 B 连接，如果成功(B 与 A 在一个子网内)，则继续；否则根据节点配置的安全网关列表，查找到本域内的安全网关 GW1，A 向 GW1发出连接请求；

②安全网关 GW1收到 A 的连接请求，首先进行身份认证，判断该用户是否具有访问节点 B 所在域的权限以及 B 是否允许访问 A 所申请访问的服务，如果认证通过，则 GW1首先试图与 B 进行直接连接，如果连接成功，则转发来自 A 的 IP 包；如果不成功，则 GW1查找安全网关列表，找到 B 所在域的安全网关 GW2；

③GW2对节点 A 的身份同样需要进行认证，根据存取控制表确认 A 是否有权限访问 B 的服务，如果同意 A 的访问，则此时 A 可以与 B 进行通信；

④A 根据与 GW1协商的加密方法和密钥对 IP 包进行加密，GW1转发 IP 包到 GW2，GW2进行解密，并将来自 A 的 IP 包转发给 B。

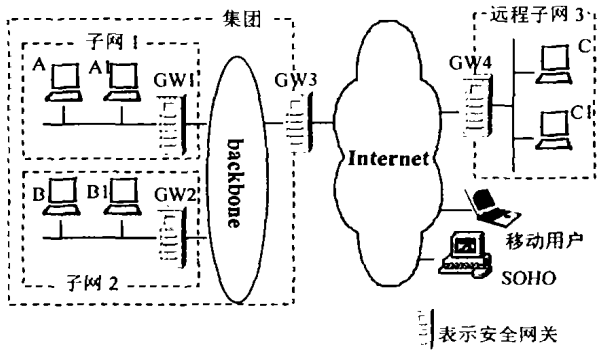

图4　基于安全网关的应用模型

至此，整个访问过程结束。在此模型中，可以归纳出安全网关的特点：

①基于用户身份进行认证，从而保证了只有合法用户才能访问内部子网的资源；

②加密在源节点进行，目的节点连接的安全网关进行解密，在传输过程中不会多次加解密，减少了协议开销，提高了包传送的效率；

③除了目的节点连接的安全网关外，其它安全网关仅仅是进行包的转发，大大减少了安全网关的系统开销。

3　安全网关的关键技术

根据上面的讨论，实现安全网关的主要关键技术包括：

3.1　存取控制表 ACT(Access Control Table)的制定

存取控制表类似于包过滤防火墙的过滤规则，通过设置存取控制表来对资源的访问进行管理。存取控制表可以支持三种方式：①基于源 IP 地址和目的 IP 地址的控制；②基于要求服务的名称和服务端口号的控制；③基于用户 ID 的控制。安全网关在存取控制方面最大的突破是可以基于用户 ID 进行控制，这比一般防火墙基于 IP 地址和服务的控制策略要方便得多。存取控制表的数据结构如下：

```
typedef AccessControlTab{
    char srcIP[48];   /* 源 IP 地址    */
    char dstIP[48];   /* 目的 IP 地址   */
    char service[20];   /* 服务名称    */
    unsigned int port;   /* 服务端口号    */
    char userID[16];   /* 用户 ID    */
    char accessFlag;   /* 存取控制位，表示是否允许    */
}ACT;
```

存取控制表在每个安全网关都可以进行设置和维护，不同网关的存取控制表根据需要可以不同。即每个安全网关根据子网用户的安全策略进行制定。

3.2　安全网关映射表的设置

安全网关映射表用来存储域和安全网关之间的对应关系。表结构如下：

```
typedef MappingList{
    char domain[255];/* 域名 */
    char sgw[50];/* 安全网关名/或者网关 IP 地址 */
    unsigned int port;/* 安全网关服务端口号 */
}ML;
```

安全网关映射列表存储在每个安全网关中，安全网关根据用户请求的目的 IP 所在的域寻找对应的网关名或者该网关的 IP 地址。因此，采用这种网关映射方式，完全独立于网络的拓扑结构和路由协议，系统的构成对网关透明。例如，在图4的模型中，假设子网1的域为 a.X.com，子网2的域为 b.X.com，子网3的域为 c.Y.com。安全网关映射表如下：

域	安全网关
a.X.com(包括主机 A、A1等)	GW1
b.X.com(包括主机 B、B1等)	GW2
c.Y.com(包括主机 C、C1等)	GW4
not X.com(不在 X.com 域中)	GW3

例如，A 希望与 C 通信，则使用的安全网关包括 GW1、GW3和 GW4，这些网关都对 A 进行身份认证，一旦认真通过后，GW1和 GW3仅仅负责包的转发，GW4将来自 A 的加密 IP 包解密后发送给 B。

3.3　端到端的数据加密

在安全网关模型中，加密在源节点进行。源节点在通过安

(下转第109页)

神经网络理论为基础，用 MATLAB 语言构造典型神经网络的激活函数，如 S 型、线性、竞争层、饱和线性等激活函数，使设计者对所选定网络输出的计算变成对激活函数的调用。另外，根据各种典型的修正网络权值的规则，加上网络的训练过程，用 MATLAB 编写出各种网络设计与训练的子程序，网络的设计者则可以根据自己的需要去调用工具箱中有关神经网络的设计训练程序，使自己能够从烦琐的编程中解脱出来，从而提高效率和解题质量。

对于本地电话网，它的可靠性指标集包括如下指标[4]：全网接通率、出中继可用率、用户关于设备质量申告率、传输设备月平均故障率、交换设备平均每百门故障率等5个性能指标。我们采用文[4]的基础数据，对我国 A、B、C、D、E 五市本地电话网可靠性指标集合作优序评价。

表1　5个本地电话网1995年的可靠性指标统计数据[5]

序号	指　标	特　征　值				
		A	B	C	D	E
1	全网接通率	0.572	0.612	0.678	0.566	0.586
2	出中继可用率	0.992	0.991	0.998	0.996	1
3	用户关于设备质量申告率	0.071	0.031	0.016	0.079	0.132
4	传输设备月平均故障率	0.018	0.022	0.013	0.029	0.019
5	交换设备平均每百台故障率	0.074	0.051	0.020	0.148	0.149

可靠性指标特征矩阵 $X_1^{(1)}$ 化为无量纲矩阵 $A_1^{(1)}$：

$$A_1^{(1)}=\begin{bmatrix} 0.4594 & 0.4923 & 0.5449 & 0.4551 & 0.4717 \\ 0.4983 & 0.4978 & 0.5014 & 0.4999 & 0.5022 \\ 0.2526 & 0.6782 & 0.8302 & 0.1698 & 0.6688 \\ 0.5724 & 0.4953 & 0.6869 & 0.3131 & 0.5491 \\ 0.5621 & 0.6982 & 0.8817 & 0.1243 & 0.1183 \end{bmatrix}$$

令神经网络输入节点 $m=5$，输出节点 $n=1$，$\varepsilon=0.14$，以 Matlab 5.3的神经网络工具箱的工具对神经网络训练5万次后，对训练样本的识别率达100%，利用训练好的 Hamming 神经网络，对测试样本其正确识别率达98%，识别效果相当理想。利用训练好的 Hamming 神经网络，可以得到 A、B、C、D、E 五市本地电话网可靠性指标集优序结果为：

(C,B,A,E,D)

从该结果看与文[4,5]的结果是一致的。因此该方法是有效的、准确的。

结论　随着通信网络技术与规模的不断发展，通信网络的复杂性也越来越高，对通信网络的可靠性的管理也越来越重要。目前电信网络可靠性评价研究对电信服务提供商也显得越来越重要，同时 ITU 也对通信网络可靠性的测度、评价和管理也引起了高度的重视。本文利用 Hamming 神经网络对具有复杂拓扑结构的本地电话网络的可靠性指标集进行评价与排序，这一种评价方法也同样适用于其它的通信网络的性能评价，例如长途电话网络、IP 网络、移动通信网络、LAN 等。评价理论方法在通信网络管理、网络规划的方案优选中是具有现实意义的，因为可以通过对不同的规划方案进行评价，选出最优的网络规划方案。通过5个本地电话网络可靠性指标集实际的应用表明基于神经网络理论的评价方法是准确、有效和方便的。

参考文献

1　熊蔚明，刘有恒. 关于通信网可靠性的研究进展. 通信学报，1990，11(4)：43～49
2　张学渊，梁雄健，丁开盛. 物元分析方法在通信网可靠性评价中的应用. 通信学报，1998，12：54～57
3　张学渊，梁雄健. 基于运行统计的通信网可靠性的综合实用评价方法. 电子学报，1999，4：43～46
4　丁开盛，梁雄健. 本地电话网可靠性综合评价的熵权双基点法. 电子学报，1999，10：116～118
5　Zhou Zhongding，Liang Xiongjian. Fuzzy Synthesis Evaluation on Reliability of Communication Networks. Proceeding of ICM'2001. pp376～379，Xian，China
6　梁雄健，张彬. 电信网可靠性及突发故障管理. 电信软科学研究，2000，10(10)：5～13
7　张学渊，梁雄健. 通信网可靠性管理框架. 北京邮电大学学报，2000，23(1)：85～89
8　梁雄健，张学渊. 关于通信网可靠性管理. 通信技术政策研究，2000，3：41～51
9　张学渊，梁雄健. 关于通信网可靠性定义的探讨. 北京邮电大学学报，1997，20(2)：30～35
10　张学渊，梁雄健. 关于通信网可靠性的研究方法. 通信学报，1997，18(4)：54～58
11　Ilyas M. Performance Evaluation of Computer Communications Networks. IEEE Communications，Magazine，1985，23(4)
12　Debany W H. Network Reliability Evaluation Using Probability Expressions IEEE Trans. On Reliability，1986，R-35(2)
13　Spragins J D. Current Telecommunication Network Reliability Models：A Critical Assessment. IEEE J. on Selected Areas in Communications，1986，SAC-4(7)
14　Bonaventura V. Service Availability of Communication Networks. In：Proc. IEEE NTC'80，Houston，TX，Vol. 1，Session-15. 2，Nov. 1980
15　Park Y J，Tanaka S. Reliability Evaluation of a Network with Delay. IEEE Trans. On Reliability，1979，R-28(4)
16　沈世镒. 神经网络系统理论及应用[M]. 北京：科学出版社，1998
17　焦李成. 神经网络计算[M]. 西安：西安电子科技大学，1993

（上接第111页）

全网关的身份验证并协商加密方法后，使用协商成功的方法对 IP 包进行加密，并传递给安全网关，到达目的节点连接的安全网关后，该安全网关进行解密操作，并将解密后 IP 包传送给目的节点。因此，加解密操作只进行一次，这样减少了包头的长度，同时也减轻了安全网关的运算开销。加密方法和密钥的协商可以采用 GSS-API[5]方法进行。

结束语　通过上面的讨论可以看出，本文提出的安全网关模型具有以下特点：①它工作在传输层之上，与 SSL、SOCKS V5属于同一层次；②与网络拓扑结构无关，与网络上层应用无关；③只需一次加解密，安全网关系统开销少，包传送效率高；④具有完善的用户身份认证和权限控制机制。因此，这种网关模型比较适合于行业用户或者集团大用户在建立跨越 Internet 的大型网络时使用。

参考文献

1　陈兵，王立松，钱红燕. 网络安全与电子商务. 北京大学出版社，1999. 12. 73～76
2　丁轶凡，吉逸，等. 基于 SOCKS 的 VPN 系统的研究与实现. 东南大学学报，2000. 2：12～16
3　NEC Systems Laboratory. SOCKS----The Border Service Enabler. 1998. 9 http：//www. socks5. nec. com
4　Leech M，et al. SOCKS Protocol Version 5 (RFC1928). 1996. 4
5　Baize E. The Simple and Protected GSS-API Negotiation Mechanism. RFC2068，1998. 12