基于应用网关的合型防火墙的设计与实现

哈尔滨工程大学计算机系　翁冠男　王慧强
中国联通黑龙江分公司(哈尔滨)　薛　凌

防火墙技术是解决网络安全问题的一种有效手段。本文给出了一种混合型防火墙的设计与实现方法，将分组过滤技术与应用网关技术结合起来，加入用户身份确认和数据加密等机制，形成一种高效、通用、更加安全的混合型防火墙结构。实践证明这种方法具有较好的性能／价格比。

引　言

目前，解决安全问题的方法主要有两种：一是针对TCP/IP协议在安全上的漏洞，结合加密解密技术，通过补充、修改现有协议或增加若干协议以增强安全性。如IPv4向IPv6的过渡。二是INTERNET防火墙技术。就目前来讲，防火墙技术是一种可行、有效的解决网络安全问题的方法。本文提出了一种新的防火墙设计方法，将分组过滤技术与应用网关技术结合起来，加入用户身份确认和数据加密等机制，形成一种高效、通用、更加安全的混合型防火墙结构。实践证明这种方法具有较好的性能/价格比。

混合型防火墙的设计与实现

通过对目前较成熟的防火墙技术的分析，可以看到各种类型的防火墙模式各有其优缺点。只用将各种技术有机地结合起来，并根据自身网络的结构、特点和实际情况的变化，制订出相关的安全策略，才能有效地保护自身网络的安全。由于我国在硬件设计和制造上的限制，因此我们应集中力量，着重安全产品软件的开发，以软代硬，走出一条符合我国国情的开发之路。考虑到网络层防火墙和应用层防火墙各有利弊，因此将IP包的分组过滤技术与应用网关技术结合起来，加入用户身份确认和数据加密等机制，形成一种高效、通用、更加安全的混合型防火墙结构。

1．防火墙的安全策略

防火墙作为一组网络安全设备，并不是独立的，它必须作为机构整体安全策略的一部分。基于网络安全策略的要求，我们为应用系统制订如下访问控制策略：

(1)除非特别限定，否则允许所有的出TCP连接，如果该连接不是内部网连接，防火墙主机对输出数据报文进行解密；

(2)除非特别指定，否则只允许内部网的入TCP连接，如果该连接不是内部网连接，防火墙主机对输入数据报文进行加密；

(3)允许入SMTP（port=25）到MAIL_HOST，入FTP（port=21）到FTP_HOST，入HTTP（port=80）到WWW_HOST；

(4)保护高端口服务。该访问控制策略实现的核心在于：在防火墙主机上构造访问控制配置表和端口使用表，实施动态分组过滤，防范外部攻击；对内部网中IP层的信息数据单元(IDU）的数据信息进行加密，从而实现虚拟子网内信息的安全传输；分组在防火墙主机处进行加/解密，以实现内外网络的兼容通信；采用一次性口令系统(OTP)进行虚拟子网内的用户认证，最大限度地减少来自内部网络的威胁。该访问控制策略运用了多重保护的思想，并给用户配置以较大的灵活性，可适用于多种安全策略。

2．动态分组过滤技术

在防火墙主机上构造访问控制配置表和端口使用表，通过分组过滤算法实现动态分组过滤。配置表分为入配置表和出配置表，包括源主机地址、目的主机地址、端口号、协议类型和允许／禁止选项等信息。如表1所示。入配置表的作用是告诉防火墙主机哪些外部分组可以通过防火墙流入内部网络。在此，源主机指的是请求使用内部网络服务的外部主机，而目的主机、端口、协议类型则表示一个内部网络主机上所提供的网络服务。允许/禁止选项默认为“允许”。出配置表的作用是告诉防火墙主机哪些内部分组不可以通过防火墙流向外部网络。在此，源主机指的

是请求使用外部网络服务的内部主机，而目的主机、端口、协议类型则表示一个外部网络主机上所提供的网络服务。允许／禁止选项默认为 “禁止”。

表 1 配置表

源主机	目的主机	端口	协议类型	允许／禁止
202.97.230.45	202.118.178.11	21	TCP	允许
202.99.167.32	202.118.178.11	21	TCP	允许
*	202.118.178.15	25	UDP	允许
…	…			

TCP/IP 协议用一个 16 位无符号整数的端口表示一种网络服务。有些网络服务的端口号是固定的，对于这类端口，防火墙主机可以根据数据包包头的基本信息利用配置表进行过滤。但是有些网络服务只是在一个固定的端口上进行监听，而在另外一个临时申请到的端口提供服务。因此很容易遭受“欺骗”攻击。为解决这一问题，我们对非固定端口号的网络服务建立了端口使用表。如表 2 所示。通过动态跟踪信息包的源／目的主机地址、源／目的端口号和协议类型等，将这些信息与配置表、端口使用表中的信息相比较，防火墙只让那些配置表许可且在端口使用表中登记的分组通过。在防火墙内部进行网络地址翻译(NAT)并对端口号建立映射关系，从而隐藏提供网络服务的真正主机和端口，有效地防止了“欺骗”攻击。

表 2 端口使用表

源主机	口的主机	源端口	目的端口	协议类型	映射后端口号
202.97.230.45	202.118.178.41	1674	6932	TCP	39700
202.99.167.32	202.118.178.41	5997	8453	TCP	41221
202.99.167.35	202.118.178.45	9012	5761	UDP	38529
…	…				

分组过滤算法如下:

/* 当防火墙主机接收到一个分组时 */

if 该分组来自外部网

{ if 源／目的主机地址、源／目的端口和协议类型已在端口使用表中登记

{ if 该分组的目的地址为防火墙主机地址

{ 将该分组的目的地址置为端口使用表中的提供服务的真正主机地址；将该分组的目的端口号置为端口使用表中的映射后端口号

}

发向内部网

}

else if 入配置表允许该分组通过

在端口使用表中登记该分组，然后发向内部网

else 抛弃该分组

}

else

{ if 源／目的主机地址、源／目的端口和协议类型已在端口使用表中登记

{ if 该分组的源地址不是一个提供公共服务（如 WWW 服务）的主机的地址

{ 将该分组的源地址置为防火墙主机的地址；将该分组的源端口号置为端口使用表中的映射后端口号

}

发向外部网

}

else if 出配置表允许该分组通过

{

用 harsh 函数对该分组的源端口号进行映射;

将该分组的源地址置为防火墙主机的地址;

将该分组在端口使用表中登记，然后发向外部网

}

else 抛弃该分组

}

3. IP层的包加密技术

既要享受INTERNET的服务，又要确保内部网的数据安全，这是INTRANET的设计目标。为了实现这一需求，我们在内部网中的两台主机对等进程进行通信时，发送方进程对IP层协议数据单元（PDU）的数据信息进行加密，然后在通信对方对等协议层解密，从而实现虚拟子网内信息的安全传输。如图 1 所示。当 IP 数据包发向外部网络时，在防火墙主机处解密，以实现内外网络的兼容通信。同时保证了当防火墙被骗过后，仍能确保内部网络信息的安全性。

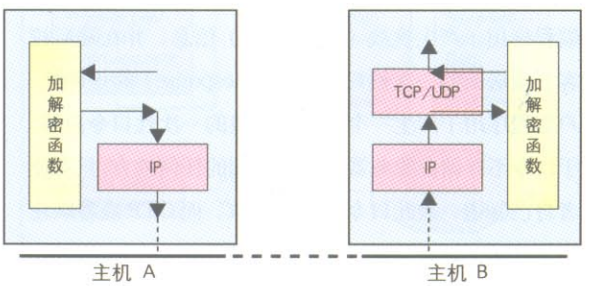

图 1 IP 数据包加密示意图

基于TCP/IP协议，实现上述功能需要修改内部网通信主机的TCP/IP驱动软件，使TCP协议模块的输入函

数tcp_input、输出函数tcp_output和UDP模块的输入函数udp_input、输出函数udp_output能够调用加/解密函数，具有对TCP报文、UDP报文的加/解密功能。定义该加/解密函数的接口标准，使该加/解密函数可重链接，从而针对不同的网络安全系统和安全策略，可以选择不同的加密方法，形成一种开放的安全结构。同时，在启动加密系统后，用户无需考虑传输细节，对用户透明。

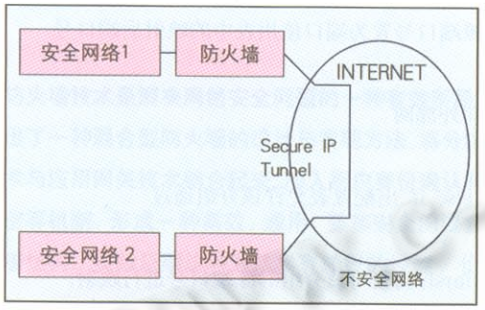

图 2 安全IP通道结构示意图

可以利用该加密系统实现安全IP通道，如图2所示。两个私有网络内部运行相同的具有加密功能的TCP/IP协议，由于在两个防火墙主机之间的通信子网上，信息始终处于加密状态，从而使数据能够穿过外部不安全网络安全地传输，在公共网络上建立一个虚拟的安全通道。

4. 用户认证

防火墙是一种被动式防御的访问控制技术，它是通过在网络边界上建立起来的相应的网络通信监控系统来实现其功能的。它假设被保护的网络具有明确定义的边界和服务，并且网络威胁仅来自外部网络。因此防火墙技术对来自内部网络的威胁不具备防范作用，这是它的一个局限。为了解决来自内部网络的安全威胁，我们采用一次性口令（OTP）系统对虚拟子网内的用户进行身份认证。OTP系统一般包括两个部分，即服务端和客户端。服务器端程序用于产生挑战（Challenge）信息，并在随后校验客户端送来的一次性口令应答（Response）的正确性。客户端程序用于产生一个对用于挑战的一次性口令应答。由于口令不存储在服务器端及客户端的任何地方，只有使用者自己知道，故此口令不会被窃取，而OTP应答既使在网络传输中被获取，也无法再次使用。

在防火墙上一次性口令的实现如图3所示，我们采用流行的客户机/服务器模式来实现防火墙上OTP的认证。认证服务器提供第三方的认证服务，即可以将内部网中的某台主机用作认证服务器，但一般也可把认证服务器同防火墙程序安装在同一台防火墙堡垒主机上。

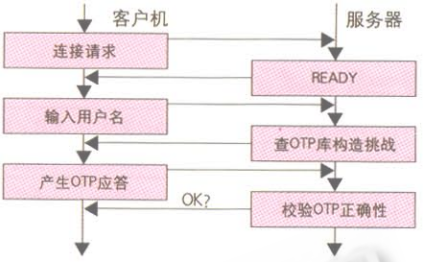

图 3 一次性口令实现示意图

在认证服务程序的实现中，主要包括以下部分：

(1)在OTP库中查找函数：int otplookup (char * user);

在OTP库中查找指定用户user的信息，若找到，返回1，库中文件指针指向对应记录；若未找到，返回0，库中文件指针指向库尾；出错则返回-1。

(2)挑战函数：int otpchallenge (char * challenge, int ic, char * seed)； 根据用户记录构造挑战信息串challenge。

(3)OTP校验函数：int otpverify(char * challenge, char * ok);

校验OTP应答的正确性，如正确则返回“OK”，否则返回“ERROR”。

我们利用S/KEY一次性口令系统库函数中的skeylookup()、skeychallenge ()、skeyverify ()等函数实现了上面的函数。■

参考文献

1 Internet/Intranet firewall security—policy, architecture and transaction services, Ray Hunt, Computer Communications 21 (1998), 1107-1123

2 Computer Network, Andrew S. Tanenbaum, 1996, 412-438, 521-544, 577-622

3 Internetworking with TCP/IP Vol. 1: principles, protocols and architecture, Douglas E. Comer, 140-169

4 Internetworking with TCP/IP Vol. 2: Design, Implementation and Internals, Douglas E. Comer, 5-19, 160-301

5 Internet防火墙与网络安全, Chris Hare, Karanjit Siyan, 1998