维普资讯 http://www.cqvip.com

计算机科学 2000Vol.27№.8

新型混合防火墙结构 HWT-FW 的研究*)

On the Architecture of New Hybrid Firewall HWT-FW

尹 欣 肖德宝

(华中师范大学计算机科学系 武汉 430079)

Abstract With the rapid development of Internet in the world, more and more people pay attention to the importance of the information security in the network. The thesis brings forward the architecture of new hybrid firewall including distributed concept and IPSec technology. It resolves the problems that are resolved difficultly by the traditional firewall.

Keywords Firewall, IPSec, Distribution

1 引言

传统的防火墙设计基于两大假设:①在防火墙内部各主机是受信的。②防火墙外部每一个访问都是攻击性访问,至少是有潜在攻击性的访问[1]。这种假设越来越不能适应 Internet 发展的现状。大量的事实告诉我们来自内外结合的攻击是当前企业网最大的威胁。显然传统防火墙结构是难以解除这一威胁的。由于以太网传输数据采用的是广播方式,因此局域网内部极易被窥探和欺骗[2]。大部分常用的 Internet 协议均未采取保密措施明码传输数据,这给企业内部局域网安全留下了巨大的隐患。

大型企业分布在不同地理位置的子公司通过 Internet 传递业务信息已成为 Internet 上的一个新的发展趋势,因而人们提出了"Extranet"概念。通常"Extranet"是通过虚拟专网(VPN)技术来实现的,传统防火墙设计难以适应这一需要。

分级的安全策略管理能力在传统防火墙设计中显得非常差,通常采用的方式是基于 IP 地址的管理模式。基于 IP 地址的管理模式有两大缺陷:①IP 地址盗用(虽然可以建立一个 ARP 服务器将 IP 地址与网络适配器地址锁定,但这需要额外的计算、查询开销,必将降低整个系统的运行效率);②难以支持用户级的分级安全策略管理(在现实环境中有着广泛的应用价值)。

防火墙技术领域中速度与安全是永恒的主题,通常高安全性的传统防火墙必然构成整个企业网的瓶颈,其原因是安全计算过度集中,大量的应用级检测、过滤计算使防火墙的吞吐能力大幅下降,降低了传统防火墙在大型网络中的应用效能。

基于以上问题,我们提出了一种新型混合防火墙结构,它融合了 IPSec 技术和分布式概念,在一定程度上解决了当前所面临的问题。

2 IPSec 技术

IPSec 技术在本文提出的新型混合防火墙结构中起着重要作用,我们先介绍一些 IPSec 技术基本概念。

2.1 IPSec 简述

IPSec 技术是由 IETF 组织下 IPSec 小组制定的,IPSec 为 IP 层提供安全服务,使系统能按需选择安全协议,决定服务所使用的算法及放置服务所需密钥到相应位置[3]。IPSec 用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。例如,路由器或实现了 IPSec 的防火墙,我们称之为"安全网关"。

IPSec 能提供的安全服务包括访问控制、无连接的完整性、数据源认证、抗重播保护、保密性和有限传输流保密性在内的服务。因为这些服务均在 IP 层提供,所以任何高层协议均能使用它们[4],例如,TCP,UDP,ICMP,BGP 等等。

IPSec 使用两个协议来提供传输安全——头部认证(AH)和封装安全负载(ESP)。

· IP 头部认证(AH)提供无连接的完整性验证、数据源认证、选择性抗重播服务。

· 封装安全负载(ESP)提供加密、有限传输流加密。它也提供无连接的完整性验证、数据源认证、抗重

*)本项目受教育部科学技术重点项目资助。尹欣 硕士生,主攻方向为计算机网络与通信。肖德宝 教授,系主任,硕士生导师。

维普资讯 http://www.cqvip.com

播服务。(无论 ESP 什么时间被调用,这些安全服务的某一集合必须被应用)。

·AH 和 ESP 均是基于密钥的分布和与这些安全协议相关的传输流管理,AH 和 ESP 均可作为访问控制的媒介物。

这些协议或者独立使用或者组合使用以提供 IPv4 和 IPv6 环境下所需的安全服务集。每一个协议支持两种使用模式:传输模式和隧道模式。在传输模式下,协议为高层提供基本的保护;在隧道模式下,协议使 IP 包通过隧道传输。

2.2 安全连接(Security Association)

安全连接(SA)是一个单向"连接",它为通过它的传输提供安全服务。SA 通过 AH 或 ESP 但不是两者同时使用而提供安全服务。如果 AH 和 ESP 同时用于传输流的保护,那么应该创建两个或多个 SA 为传输流提供保护。通常为了安全,两台主机间或两个安全网关间或两个安全连接间(每个方向一个)都需要双向通讯。

安全连接由三个部分内容唯一标识:安全参数索引(SPI)、IP 目的地址、安全协议(AH 和 ESP)标识符。当报文被接收时,只有接收者找到它们的安全连接后它们才能被认证或解密。

我们定义了两种类型的 SAs:传输模式、隧道模式。传输模式 SA 是两台主机间的安全连接。在 IPv4 环境中,传输模式安全协议头紧接在 IP 头和任何选项之后,在任何更高层协议之前(例如 TCP 或 UDP)。在 IPv6 环境中,安全协议头出现在基本 IP 头和扩展之后,但也许出现在目的选项的前或后,并在更高层协议之前。在采用 ESP 时,传输模式 SA 仅为更高层协议安全服务提供,而不为 IP 头或任何 ESP 头以前的扩展头提供服务。在采用 AH 时,这种保护也被扩展到 IP 头的可选部分、扩展头的可选部分和可选项(包括 IPv4 头,IPv6 Hop-by-Hop 扩展头,或 IPv6 目的扩展头)。

隧道模式 SA 必然是运用于 IP 隧道的 SA。只要安全连接的任意一端是安全网关,SA 就必须是隧道模式。因此两个安全网关之间总是隧道模式,同样主机和安全网关间也必然是隧道模式。

对于隧道模式 SA,有外部(outer)IP 头,内部(inner)IP 头。外部 IP 头定义了 IPSec 处理的目的地,内部 IP 头定义了包最终地址。安全协议头出现在外部 IP 头后内部 IP 头前。如果在隧道模式中使用 AH,外部 IP 头的部分将受到保护。同样所有隧道化 IP 包也受到保护(即所有内部 IP 头、更高层协议受到保护)。如果使用 ESP,则仅对隧道化的包给予保护而不保护外部头。

3 新型混合防火墙结构 HWT-FW

3.1 新型混合防火墙总体结构

本文提出的新型混合防火墙主要运用了 IPSec 技术和分布式计算思想。IPSec 技术运用到新型防火墙结构中,从根本上解决了企业网内部的不安全因素,大大降低了企业网内窥探和欺骗的可能性。IPSec 技术的应用也解决了企业对安全与"Extranet"的双重需求。本防火墙运用了一次一密的认证方式,很好地支持了用户级的分级安全策略管理。分布式概念的引入,使得本防火墙有效地降低了中心防火墙模块的计算负载,大大缓解了中心防火墙模块吞吐能力的瓶颈。同时在用户端布置的个人防火墙模块处理原来在传统防火墙中进行的应用级安全处理,提高了新型混合防火墙的安全处理能力。新型混合防火墙在拓扑结构上没有完全采用分布式防火墙的设计概念,而部分保留了传统防火墙的拓扑结构。这一设计思想符合企业网的需求。将企业内部局域网与 Internet 隔离能最大限度地减少外部网络对内部网络的攻击。更重要的是,内部网络的各终端主机上的应用程序可以建立在并不十分昂贵的较低安全级别操作系统上,这样能够节省大量的开销。新型混合防火墙 HWT-FW 结构示意图如图 1 所示。图 1 中,新型混合防火墙分为两大模块:①中心防火墙模块;②个人防火墙模块。

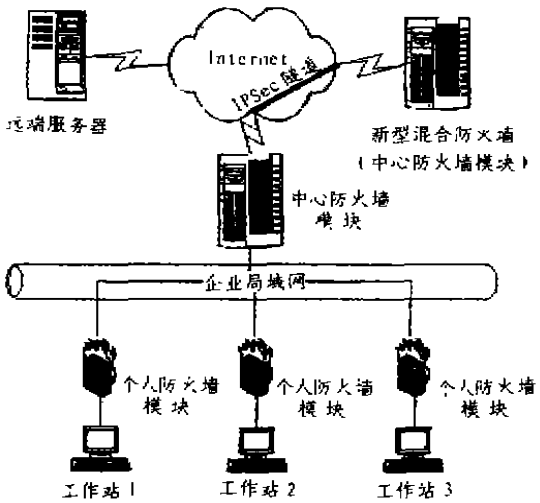

图 1 新型混合防火墙 HWT-FW 示意图

我们通过一个实例来解释新型混合防火墙的工作流程:公司职员尹瑞小姐使用 5 号工作站查找网上信息。首先,她发出认证请求,中心防火墙模块认证其身份,成功后分发该用户的用户安全策略。然后,她打开浏览器连接一个国内网站(IPSec 加密传输),安全策

维普资讯 http://www.cqvip.com

略允许其连接，则该连接请求通过防火墙，客户、服务端进行正常的信息交换。（注意：如果远端下是支持IPSec 协议的主机，则用户与防火墙间的传输是加密的，防火墙与远端主机间则是非加密的，如果远端是支持 IPSec 协议的主机，则在防火墙与远端主机间采用IPSec 隧道模式传输数据。）当她访问的某一页面中含有安全策略禁止的内容时，个人防火墙模块将丢弃该页面连接。接下来，她想访问国外某站点，但管理员级安全策略禁止这一连接企图。中心防火墙模块将根据安全策略丢弃这一请求。最后，她注销用户，完成了一次安全服务。

3.2 中心防火墙模块

我们在一个双宿主主机上布置中心防火墙模块，它由三大子模块构成：

·IPSec 安全子模块 是本防火墙中的核心部分。IPSec 技术现已广泛应用于 VPN（虚拟专网）中，但目前尚未有直接布置于"安全网关"上的产品。IPSec 技术的引入就是为了从根本上解决内部网络中窥探和欺骗的可行性。IPSec 安全子模块由 5 大功能模块构成：①IPSec/非 IPSec 转换，该功能使支持与不支持 IPSec 协议的主机间能够互相传送报文。②IPSec 引擎提供 3 大功能：IP 报文过滤；安全报文传输；一般报文传输。③IPSec 安全策略管理。IPSec 底层的安全策略的管理，在系统级安全策略管理与 IPSec 引擎之间起桥梁作用。④IPSec ISAKMP/oakley 密钥管理。对用户端与服务端间的密钥交换进行管理。⑤加密算法库，存放整个 IPSec 协议实现中需要的加密算法。

·混合防火墙安全策略管理子模块 由 3 大功能模块和 1 个安全策略数据库构成。①安全策略数据库维护。维护分两级：管理员级，供企业安全管理员制定整个系统的基本安全策略；用户级，用户注册后可以在不与管理员级安全策略相抵触的基础上修改安全策略。②安全策略描述的编码与解码。实现管理员、用户制定的形式化安全策略描述与系统内部易识别、易传输、高保密性代码间的转换。③安全策略的分发。将用户安全策略分发到用户所使用的终端主机上。

混合防火墙安全策略管理充分体现了本防火墙分布式的设计思想。为了配合新型混合防火墙的结构，安全策略管理子模块将 IP 层的安全策略留在中心防火墙模块处理，将应用层的安全策略分发到用户端工作站由个人防火墙模块处理。

·用户认证子模块 是实现基于用户级安全管理的基础。用户通过身份认证后，中心防火墙模块分发该用户的安全策略至该用户正在使用的终端主机上。这样个人防火墙模块就能根据该用户的安全策略为之提供相应的安全服务。

本防火墙采用一次一密认证机制，其原理如下：服务端与用户端均有一个密钥。用户端首先向服务端发送一个认证请求，服务端则回应一个随机串，用户端采用自己的密钥加密这一随机串并回送给服务端，服务端将之与服务端留有的密钥相比对，若匹配则认证身份成功，反之则失败。

3.3 个人防火墙模块

在用户端我们布置了个人防火墙模块，其作用有 3 点：

1）加密用户输出传输。IPSec 协议在用户端的实现为用户提供了 IP 层的安全。用户的任何数据传输均可按照安全策略的规定加密传输。这种机制很好地解决了前面提到的内部安全隐患，并且下会对已有的应用层协议产生任何副作用，即对应用层协议有良好的透明性。

2）应用级检测与过滤。将应用级检测与过滤布置到个人防火墙模块上有两大优点：①极大地降低了中心防火墙模块的计算负荷、在一定程度上解决了中心防火墙的吞吐量瓶颈；②应用级检测与过滤离用户应用越近越能提高效率，这样布置能够收集到足够的信息以做出相应的安全决策。

3）用户级安全策略管理，允许用户根据自己的需要局部地调整安全策略。这一特性使用户能够制定适合于自己需要的安全策略。安全策略的个性化在更高一个层次上提高了前面提出的分级安全策略管理能力。

结束语 本文论述了新型混合防火墙 HWT-FW 结构。研究了新型混合防火墙的底层核心技术—IPSec 技术，它从 IP 层上保护了传输信息的安全和受信。讨论了分布式防火墙概念对于解决中心防火墙模块计算瓶颈的作用。提出了中心防火墙与个人防火墙相结合的两级混合防火墙结构，得出了新型混合防火墙 HWT-FW 在保护内部网络传输安全，解决防火墙计算瓶颈，增强分级管理能力，支持"Extranet"需求方面均优于传统防火墙的结论。由于新型防火墙结构与技术涉及了网络安全大部分领域，因此我们还将在 IPSec 实现、多重中心防火墙模块均衡负载，安全策略管理个性化，应用级检测与过滤的细节上进行进一步的研究。

参 考 文 献

1 Bellovin S M. Distributed Firewalls. Login: November 1999. 39～47
2 Atkins D. 网络安全专业参考手册．机械工业出版社，1998. 8
3 Kent S. RFC2401 Security Architecture for Internet Protocol. IETF, November 1998
4 Doraswamy N, Harkins D. IPSec: the New Security Standard for the Internet, Intranet, and Virtual Private Networks. Prentice Hall PTR, 1999
5 Adaptive Proxy Firewalls-the Next Generation Firewall Architecture. Availabe at: www. nai. com
6 SSHIPSEC Express White Paper. SSH Communications Security Ltd, November 1999