分布式防火墙的网络安全系统研究

刘 喆，王蔚然

(电子科技大学电子工程学院 成都 610054)

【摘要】针对单一的网络安全技术已经无法很好的解决日益复杂的网络安全问题，提出了一种新型的安全系统。该系统基于分布式防火墙环境，结合分布式入侵检测技术，并利用专家系统使两者协同工作，实时检测并响应动态的网络安全事件，弥补了单一网络安全系统的不足，可以很好的满足网络安全的要求。

关 键 词 分布式防火墙； 分布式入侵检测； 专家系统

中图分类号 TP393 文献标识码 A

Study of Distributed Firewall Based Security System

LIU Zhe，WANG Wei-ran

(School of Electronic Engineering, UEST of China Chengdu 610054)

Abstract Traditional single security technology is becoming obsolete with the complexity of network security problems increased. To address this problem , a new security system architecture is proposed. This new system is based on the distributed firewall environment, and distributed network intrusion detection technology is integrated. Furthermore, Expert System is utilized to make them work coordinated and intelligently respond the real-time dynamic network security situations. This scheme can make up for the shortcomings of single security system and fulfill the requirement of network security. Description of this system architecture and some important system details are presented in this paper.

Key words distributed firewall; distributed intrusion detection system; expert system

网络攻击主要以网络协议自身的不安全性和操作系统、应用程序的bug或弱点这两种途径作为切入点，采用的形式越来越复杂。而网络攻击工具在网络上广为传播，人们可以很容易的利用这些工具对计算机网络系统造成破坏，造成严重损失。CSI/FBI Computer Crime and Security Survey调查结果显示，被调查组织由网络安全造成的经济损失逐年增加，网络安全形势日益严峻[1]。在这种情况下，相应的网络安全措施也层出不穷，然而网络安全事件的数量和影响并没有因此而减少。其原因是：(1) 由于当今的网络安全产品往往基于单一的安全技术，产品之间缺乏协作能力，只能提供一定程度的安全保护；(2) 无法动态适应网络安全事件的动态变化特性。针对此，本文以分布式防火墙为基础[2]，结合分布式入侵检测技术[3]，提出一种新型的安全系统。

1 分布式防火墙

防火墙是一种基于安全策略的访问控制机制。传统防火墙根据其在网络中驻留的位置，可以分为边界

收稿日期：2004 – 09 – 28
基金项目：信息产业部电子信息发展基金项目
作者简介：刘 喆(1978 –)，女，硕士，助教，主要从事网络安全方面的研究.

防火墙和主机防火墙两种。边界防火墙驻留在可信网络(受保护网络)与不可信网络之间，并成为其通信的唯一接入点，依据安全策略，过滤其通信流量信息，以此为可信网络提供安全屏障。传统主机防火墙驻留在主机中，依据安全策略过滤进出该主机的网络数据，保护单个主机系统的安全。

1.1 传统防火墙

传统防火墙作为一种成熟有效的安全技术，是解决网络安全问题的一个行之有效的方法，但是传统防火墙存在着先天缺陷。边界防火墙依赖于网络拓扑结构，形成网络流量瓶颈，只能提供粗粒度(gross granularity)的安全保护，且无法防御来自受保护网络的内部攻击；主机防火墙自身的处理能力往往十分有限，它的安全策略可以由主机使用者自行设置，这样作为一个组织或企业，无法对主机防火墙进行集中、有效的安全配置，来实现本组织的网络安全保护。

1.2 分布式防火墙

分布式防火墙(Distributed FireWall，DFW)基于传统防火墙技术，集中管理、分布防御，即集中制定安全策略、由分布于网络中的各个防火墙实施策略。DFW内外皆防，可以提供细粒度(fine granularity)的网络安全保护，已成为防火墙技术发展的一个重要方向。

分布式防火墙，可以分为狭义分布式防火墙和广义分布式防火墙两种。狭义DFW即是分布式的主机防火墙，安全策略的执行主体是主机防火墙。广义DFW是分布式的主机防火墙、边界防火墙。在集中的管理下，主机和边界防火墙均作为安全策略的执行主体。两种类型的DFW最大的差别就是是否使用边界防火墙作为执行主体。狭义DFW相较广义DFW，其长处是由于摈弃了边界防火墙，该体系结构完全不依赖于网络拓扑。然而，广义DFW在安全性和处理能力的综合性能上比狭义分布式防火墙具有更多的优点：(1) 广义DFW为网络用户提供了一个多层次的安全保护。广义DFW中的边界防火墙模块(简记为D-BFW)通常作用在受保护网络的边界，为受保护网络提供第一层基本的安全保护，可以对来自外部的大多数攻击进行防范；广义分布式防火墙中的主机防火墙模块(简记为D-HFW)，则运行于受保护网络中需要进一步保护的主机和服务器或者网络外远程受保护主机上，提供更细粒度的安全保护。(2) 广义DFW中D-HFW的处理负荷相较狭义DFW大大减少。广义DFW中受保护网络的D-HFW只需要针对不同的要求，来处理已经被D-BFW过滤的网络数据。(3) 广义DFW中的D-BFW在过滤某种针对整个网络的攻击等方面更为有效，如拒绝服务攻击，碎片攻击等。

2 基于分布式防火墙的网络安全系统

2.1 建立协同工作的网络安全系统

网络安全问题是一个动态的过程。DFW自身仍然是一个静态防御系统，主要是完成访问控制功能，在入侵检测、动态实时获知安全状况方面的能力薄弱，也就难以动态的调整其安全策略以有针对性的采取措施进行防御，使安全损失达到最小。因此单一的DFW系统在网络防御上能力有限，必须结合其他的网络安全技术。

入侵检测系统(Intrusion Detection System，IDS)是动态发现系统，是为保障网络系统的安全而设计与配置的一种能够及时发现并报告网络中异常或未授权现象的系统。分布式入侵检测(Distributed Intrusion Detection System，DIDS)则是利用多个检测主体，采用多种检测方法，依靠分布于网络中的多个入侵数据来源，通过协同工作来实现检测。当前的网络入侵行为通常表现出相互协作入侵的特点，采用分布式入侵检测，利用多个检测主体协作，可以更全面的、更准确的检测入侵。然而，DIDS的防御能力有限，通常对检测到的入侵事件仅能提示、报警。

由此可见，DFW与DIDS两种技术各有所长，可以把两者相结合形成一种新型的网络安全系统：首先，DFW的分布式架构为DIDS提供了良好的平台。DFW自身的分布性，适合于将分布在网络各个受保护节点的防火墙与DIDS的各个检测主体共同整合在一起，进而可以使之协同工作。其次，DFW为网络以及网络中各主机提供了一个多层次的防御体系，而且DFW可以过滤掉大量无用的数据，减少传递各个入侵检测主体的数据量，增强了入侵检测的检测能力。因此DIDS的实时检测结果可以动态的反映网络的安全状况，以此作为DFW安全策略的设置依据，可以提升其机动性和实时反应能力。

2.2　基于DFW的安全系统

据上述，提出一种新型的网络安全系统，系统结构如图1所示。本系统主要由四个部件组成：分布式防火墙部件(DFW部件)，分布式入侵检测部件(DIDS部件)，信息综合部件，管理决策部件。其中DFW部件采用广义分布式防火墙的结构。DIDS部件的主机入侵检测模块(D-HIDS)与DFW部件的主机防火墙模块(D-HFW)在一个受保护主机中共同构成主机防御子系统；DIDS部件的网络入侵检测模块(D-NIDS)和DFW部件的边界防火墙模块(D-BFW)在一个受保护网络的边界，共同构成了边界防御子系统。信息综合部件与管理决策部件共存于系统服务器中。系统服务器集中管理各个分布在网络中的防御子系统。

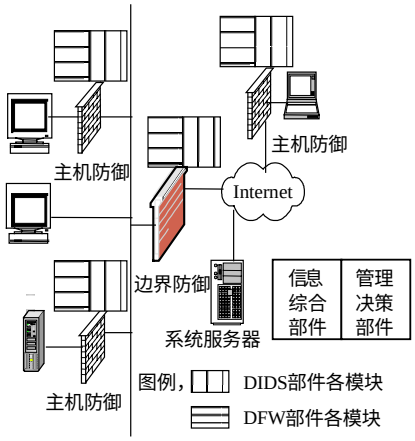

图1　安全系统结构示意图

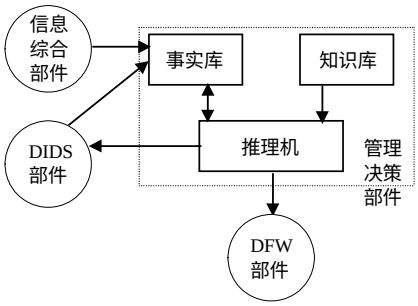

图2　应用专家系统的管理决策部件

系统中DFW部件是该系统防御功能的主要实施者，DFW部件的D-HFW、D-BFW各模块接收并执行管理决策部件的安全策略，过滤网络数据。DIDS部件实时监控网络安全状况，它与管理决策部件、信息综合部件结合，采用了分层的结构。DIDS部件的D-NIDS、D-HIDS模块分布于网络中，其工作方式是：首先彼此独立地检测入侵，将检测结果传送到系统服务器；而后由信息综合部件、管理决策部件对其检测结果进行进一步地综合处理。信息综合部件的功能作用，实际上是记录整个系统的日志数据、入侵告警数据、事务信息，并实施进一步的综合分析，从而可以发现DIDS部件各个模块自身无法独立发现的可能入侵(例如对多个主机的并行扫描)；检测到入侵后，及时将入侵信息传送给管理决策部件，以对其进行响应。管理决策部件是整个网络防御系统的控制决策中心，是使系统各个部件协同工作、有机互动的关键。

管理决策部件有两个功能：(1) 系统安全管理员配置DFW、DIDS部件的各个模块的安全策略和规则，这一功能根据组织内部制定的安全政策，通过设置良好的管理员界面即可以实现，(2) 该部件针对DIDS部件和信息综合部件发送来的入侵告警信息，进行安全防御的响应决策。响应决策的任务包括：确定具体的响应执行模块；确定响应执行模块应当执行的响应动作；将响应动作转换为安全策略和规则的形式分发给响应执行模块。因此针对网络安全状况，实时、智能地调整系统其他各个部件的安全策略，是对这个部件的一个基本要求。对此，管理决策部件应用专家系统作为实施方案。

如图2所示虚线框内部分是采用了专家系统的管理决策部件的结构图，其中知识库中存储的是关于入侵事件－响应对(Incident-Response Parings)的知识。知识库中的知识可以预先通过系统提供的人机界面来手工设定，而后根据实际网络安全状况以及组织安全政策的变化，进行动态的刷新。事实库负责存储来自信息综合部件和DIDS部件的入侵事件，以及推理机推理生成的事件。推理机是该部件的核心，根据事实库中的入侵事件，利用知识库中的知识，进行推理，以确定对入侵事件的响应，再设置DIDS、DFW各部件的策略，及时防御入侵并追踪入侵源。这样，利用专家系统，结合动态更新的专家知识，不需人为介入，即可实现对检测到的入侵或攻击行为的自动响应。

3　结 束 语

本文论述的安全系统，以分布式防火墙为基础，结合分布式入侵技术与专家系统，提供一个立体的防

护体系，动态的适应不断变化的网络环境；在规模上，该系统采用分级管理的方法，能够容纳、处理企业级以上规模的网络用户。目前该安全系统原型已经完成并试验成功，进一步完善、丰富管理决策部件的功能以及提升系统整体处理性能是今后工作的重点。

参 考 文 献

[1] Lawrence A, Martin P, William L, et al. CSI/FBI Computer Crime and Security Survey 2004[EB/OL]. http: //www. cybercrime. gov/CSI_FBI.htm, 2004-06-20

[2] Bellovin S M. Distributed Firewalls[EB/OL]. http://www.research.att.com/~smb/papers/distfw.pdf, 2004-06-25

[3] 蒋建春, 马恒太, 任党恩, 等. 网络安全入侵检测: 研究综述[J]. 软件学报, 2000, 11(11): 1 460-1 466

[4] Joseph G, Gary. 专家系统原理与编程[M]. 北京: 机械工业出版社, 2000

编 辑 徐安玉

(上接第342页)

参 考 文 献

[1] Senzaki J, Kojima K, Harada S, et al. Excellent effects of hydrogen postoxidation annealing on inversion channel mobility of 4H-SiC MOSFET fabricated on $(11\bar{2}0)$ face[J]. IEEE Electron Device letter, 2002, 23(1): 13-15

[2] Watanae S, Shigemo M, Nakayama N, et al. Silicon-monohydride termination of Silicon-111 surface formed by boiling water[J]. Japanese Journal of Applied Physics, 1991, 30(12B): 3575-3579

[3] 罗小蓉, 李肇基, 张 波, 等. 表面氢化对SiC/金属接触的作用机理[J]. 固体电子学研究与进展, 2004, 24(2): 164-167

[4] Trucks G W, Krihsdnan R, Higashi G S, et al. Mechanism of HF etching of Si surface: a theoretical understanding of hydrogen passivation[J]. Physical Review Letter, 1990, 65(4): 504-507

[5] Tsuchida H, Kamata I, Izuml K, Infraed spectroscopy of hydride on the 6H-SiC surface[J]. Applied Physics Letter, 1997, 70(23): 3 072-3 074

[6] Berger H H. Models for contacts to planar devices[J]. Solid-State Electron, 1972, 15: 145-148

[7] Teraji T, Hara S, Okushi H, et al. Ideal ohmic contacts to n-type 6H-SiC by reduction of Schottky barrier height[J]. Applied Physics Letter, 1997, 71(5): 689-691

[8] Wahab Q, Macak E B, Zhang J, et al. Improvements in the electrical performance of high voltage 4H-SiC Schottky diodes by hydrogen annealing[C]. 3rd European Conference on Silicon Carbide and Related Materials: Materials Science Forum, Trans Uetikon-Zuerich, Switzerland: Tech Publications Ltd, 2001: 691-694

编 辑 许宣伟