Network Security Tool

网络安全工具及案例分析

网络安全专家
EXPERT

邱 亮 孙亚刚 编著
飞思科技产品研发中心 监制

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全专家

网络安全工具及案例分析

邱亮　孙亚刚　编著

飞思科技产品研发中心　监制

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书共分三部分内容，用理论结合案例的形式，分别介绍了网络安全工具中的三大法宝：防火墙、协议分析仪和入侵检测系统的使用。作者选用最具代表性的软件：防火墙 ISA Server 2000、协议分析仪 Sniffer Pro 和入侵检测系统 SessionWall 来构建案例，可操作性及实用性很强。读者可以在精通这些工具的基础上触类旁通，掌握保护网络安全的方法，真正提高保障网络安全的技能。

用虚拟计算机软件，管理员无需使用大量计算机和网络设备就可以完全模拟企业网络实验环境。本书的附录部分介绍了用 VMware 软件构建虚拟网络实验环境的方法，并将全书案例做了索引，以方便读者查阅。

本书语言简练，案例丰富，内容详尽且实用，可以作为网络管理员和安全管理员的工作指导书，也可供参加 CIW 网络安全专家认证考试、MCSE 认证考试、CISSP 认证考试的广大从事网络安全领域工作的人士参考。

图书在版编目（CIP）数据

网络安全工具及案例分析 / 邱亮，孙亚刚编著. —北京：电子工业出版社，2004.4
（网络安全专家）
ISBN 7-5053-9736-2

Ⅰ.网... Ⅱ. ①邱...②孙... Ⅲ.计算机网络－安全技术－应用软件 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2004）第 017102 号

责任编辑：陆舒敏
印　　刷：北京东光印刷厂
出版发行：电子工业出版社
　　北京海淀区万寿路 173 信箱　邮编：100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：24.25　字数：620.8 千字
印　　次：2004 年 4 月第 1 次印刷
印　　数：6000 册　　定价：35.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：010-68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

关于丛书

网络办公对于互联网时代的企业来说已经是一种客观的存在状态，而与此同时，来自于互联网的危险也在时时威胁着这些企业。建立起一个高效可用的、安全性能卓越的安全屏障显然是保障企业正常运转的关键因素之一。因此，网络安全问题越来越受到企业的关注。网络安全行业是新兴行业，对于正从事或者即将从事网络安全行业的人来说，掌握网络安全技术的需求越来越高。市场上各种各样的网络安全类图书应该说相当多了，但基本都是围绕进攻或者防范来编写的，还缺乏一套系列的网络安全学习丛书。为了满足读者的学习需求，电子工业出版社计算机研发部策划组织了《网络安全专家》系列丛书，该丛书目前已推出如下几本：

1. 《防黑档案》
2. 《网络服务器安全配置详解》
3. 《网络安全工具及案例分析》

丛书特色：

- 以案例分析最新网络安全技术。网络安全技术发展日新月异，书中均以最新的案例诠释专业的技术，使图书更具实用性。
- 作者队伍为一线从事网络安全的人士。如《防黑档案》作者东方飘云是业界资深网络安全专家，书中总结了他多年的实践经验。
- 横向纵深剖析网络安全最主要的应用面。后续还会陆续推出 Windows、Linux 等方面的网络安全图书。

关于本书

网络安全是当今 IT 界炙手可热而且迫在眉睫需要着手去解决的问题。网络安全涵盖面非常广泛，实现网络安全的技术手段和工具也可谓是“八仙过海，各显神通”。“菜刀既可以用来切菜，有时又成为了行凶工具”，所以说有些工具既可以作为安全工具，也可以成为黑客工具。由此可见，要写一本网络安全工具的书，选材和定位是十分重要的。

防火墙、协议分析仪器和入侵检测系统是当今网络安全工具中的三大法宝。防火墙好比是企业网络的“防盗门”，是防止外部入侵的非常有效的工具。协议分析仪就像是个“放大镜”，通过捕获数据帧分析网络通信。学习和了解协议栈是深入到网络安全领域的必经之路。入侵检测系统如同是企业内部的“巡逻兵”，可以检查网络内部是否有攻击行为或者网络的滥用。这三类安全工具，从不同的角度去治理网络，又深入扩散到网络安全的各个方面。因此，本书选用这三类安全工具，不仅具有代表性，而且能给读者一个系统了解网络安全“全貌”的视角。

在软件的选用方面，遵循了少而精的原则。每类软件选用一种大家最熟悉，使用最广泛，功能强大，具有一定“重量级”的软件：防火墙选用了 ISA Server；协议分析仪选用了 Sniffer Pro；入侵检测系统选用了 SessionWall。这样选择的目的，是让读者在精通少数具有代表性软件的基

础上，掌握保护网络安全的不依赖于具体产品的方法，从而触类旁通，真正提高保障网络安全的技能。

全书主要内容由三部分组成：第一部分是防火墙 ISA Server；第二部分是协议分析仪 Sniffer Pro；第三部分是入侵检测系统 SessionWall。

这三大部分既相互独立，又共同构成了安全工具“三大法宝”。读者阅读的时候可以把这本书当做学习安全工具软件的工具书，有针对性地阅读其中某个部分，也可以有针对性地阅读某个具体的案例或解决方案。

建议读者按照书中的案例步骤亲自操练，把书本上的知识变成工作学习过程中的技能。

另外，本书的第 10、11、14 章，由于我们是在真实网络环境中做的实验，所以在部分图中，凡是显示了真实 IP 地址的，考虑避免引起安全问题或不必要的麻烦，我们都有意把出现的真实 IP 地址涂抹掉，这并不影响图的显示，在此一并提请读者注意。

附录部分介绍了用 VMware 构建虚拟网络实验环境的方法，并将全书案例做了索引，以方便读者查阅。

本书由飞思科技产品研发中心策划并组织编写，孙亚刚老师组织策划，由具有多年网络安全管理和教学经验的邱亮老师主笔编写，另外参与本书编写的还有麻璐璐、许斌辉、崔吉春、萧殷、张天海、白煜、徐涛、高显嵩等人，在此一并表示感谢。由于编写时间仓促，书中难免会有一些疏漏，希望广大读者给予批评指正。

我们的联系方式如下：

咨询电话：（010）68134545　　68131648

答疑邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn　　http://www.fecit.net

通用网址：计算机图书、FECIT、飞思教育、飞思科技、飞思

飞思科技产品研发中心

目　录

第 1 篇　防火墙 ISA Server

第 2 篇 协议分析仪 Sniffer Pro

网络安全工具及案例分析

1 防火墙 ISA Server

防火墙是目前计算机网络中最为重要的安全工具之一。防火墙有硬件防火墙和软件防火墙两类，相应的工具和产品都非常多，本书以微软公司的软件防火墙产品 ISA Server 为例，详细介绍如何使用 ISA Server 来保证企业级网络的安全。

第1章　ISA防火墙介绍

如果要保护一片原始森林，我们可以把森林用围墙围起来，实现与外界的物理隔离。然后，我们可以在围墙上开一个门，这样，合法的旅游者必须得到门卫的批准才能从这个门出入，从而保证了森林的安全。

与此类似，如果我们要保护的是企业的网络，我们首先也需要把企业的网络和外界的因特网之间物理地隔离，然后强制所有的网络数据必须流经防火墙系统，这样就可以用防火墙系统来检查不可信任网络与可信任网络之间的数据流，并决定是允许还是阻止数据流通过，如图 1-1 所示。

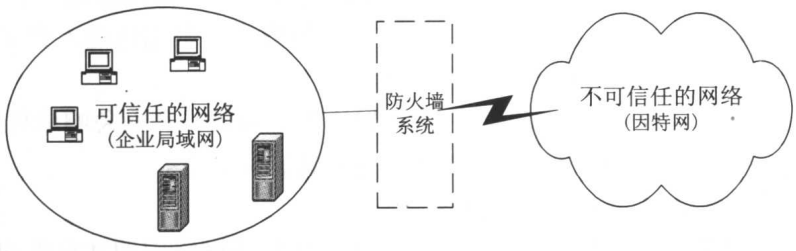

图 1-1　防火墙系统示意图

通常我们可以认为防火墙系统是可信任网络和不可信任网络之间惟一的安全屏障。防火墙系统属于可信任网络中的一部分，同时又直接面对不可信任网络，是网络中的“堡垒”。

防火墙系统可以只是一台路由器，或者是一台防火墙硬件设备，也可以是一台安装了防火墙软件的主机。复杂的防火墙则是由一系列硬件和软件设备配置到一起所形成的一个网络子系统。

1.1　防火墙的作用

在保障网络安全方面，防火墙日益起到了举足轻重的作用。我们可以就以下 4 个方面来阐明防火墙的重要性。

- 落实公司的安全策略

每个公司的网络情况不同，业务也不同，对网络安全的要求也不一样。但是，每个公司都会用自己的安全策略来规定什么站点可以访问，什么站点不能访问；什么时间可以访问，什么时间不能访问；什么应用程序可以使用，什么应用程序不能使用。诸如此类的规章制度如何去实现呢？有了防火墙，我们就可以在防火墙上面来设置规则和策略，让公司写在纸面上的安全策略真正落到实处，从技术上得以实现。

- 用防火墙建立一个“阻塞点”

防火墙物理地隔离了可信任网络和不可信任网络，强制所有在这两个网络之间的数据流必须经过防火墙，并受到防火墙的检查，从而保证了只有安全的数据流才能够通过。“阻塞点”是一个监控并记录所有流经数据的地方。如果没有这个“点”，我们就不能够有效地监控和记录网络中的这些数据流。

“阻塞点”也叫做网络边界。

可信任网络中如果有多个接入点进入到因特网中，实际上就造成了防火墙的旁路，使防火墙失去作用，这时的网络安全会受到严重的威胁。因此，要严禁防火墙内的局域网用户拨号上网。

- 记录网络间的数据包

防火墙的另一个重要作用，就是可以把所有穿过防火墙的数据包都记录下来，并保存到日志当中。有了日志，网络管理员就能够发现是否曾经有不安全的数据包进入到了企业的网络中，并能够从多个不同的角度统计出网络的使用状况。

如果不安全的数据包要穿过防火墙时，就可以实时触发警报和应急响应机制。

在记录数据包的同时，还可以对内部的用户进行认证和计费。

- 减少可信任网络在 Internet 中的暴露

通过 NAT（网络地址转换）技术，防火墙把内部可信任网络中的计算机的 IP 地址隐藏起来了。Internet 中的用户“看”不到内部计算机的存在，而只能“看”到防火墙的外部网卡的地址。这样就把整个可信任网络的暴露降低到了最小，从而减小了受到攻击的可能性。

1.2 ISA Server 简介

ISA Server 的全名是 Microsoft Internet Security and Acceleration Server 2000。它的前一个版本就是微软的代理服务器 Microsoft Proxy Server 2.0。在原来的代理服务器的基础上，ISA Server 被扩展成为一个企业级防火墙软件。

三大功能 I、S 和 A

- Internet 代表它的代理服务器功能
- Security 代表防火墙功能
- Acceleration 代表利用缓存服务器加速对 Internet 访问的功能

ISA Server 有两个版本，标准版（ISA Server Standard Edition）和企业版（ISA Server Enterprise Edition）。

ISA Server 企业版支持大规模的企业级防火墙和 Web 缓存服务器，支持服务器阵列、多层次的策略，对处理器数目没有限制。企业版可以满足大流量的 Internet 访问环境中的性能、管理要求，可扩展性要求，支持多层次的访问策略，具有容错能力。

ISA Server 标准版适用于小型商务环境、工作组和大企业中的部门。标准版也具有强健的

安全性，支持快速的 Web 访问，管理界面直观，容易操作。

在安全性、缓存、管理、性能和可扩展性方面，企业版和标准版基本上是相同的。不同之处在于，标准版在以 Stand-alone 模式安装时，仅支持本地策略，处理器的数量限制在 4 个以内。而企业版支持多服务器阵列，中央管理，企业级和阵列级策略，对处理器数量没有限制。

表 1-1 列出了 ISA Server 标准版和企业版的一些不同特性。

表 1-1 ISA Server 标准版和企业版的不同特性

特 性	标 准 版	企 业 版
规模扩展性	受限	好
分布式和分级式缓存	仅支持分级式缓存	都支持
与活动目录的集成	受限	好
层次策略	不支持	支持
多服务器管理	不支持	支持

以服务的方式与 Windows 2000 Server 紧密集成

ISA Server 的核心是由一组运行在 Windows 2000 Server 的后台服务构成：

- ISA Server 控制服务
- 防火墙服务
- Web 代理服务
- 预定 Cache 内容下载服务
- H.323 网关服务

ISA Server 可以工作在多个协议层上。在 IP 层，ISA Server 实现 IP 包过滤。当包过滤启用的时候，ISA Server 能静态地监控外部网卡上的数据流，在数据进入网络前进行过滤。如果数据被获准穿过 IP 包过滤层，就会被防火墙服务或者 Web 代理服务所接收处理。这时候，ISA Server 中的规则就会被用来决定外部请求是否应该被处理并响应。

如图 1-2 所示为 ISA 的架构和核心功能的示意图，具体说明如下。

- Web 代理客户

请求直接到达 Web 代理服务，Web 代理服务匹配规则决定是否许可客户请求。如果许可，Web 代理服务查看缓存，如果缓存中有客户请求的对象就直接把对象给客户，否则到 Internet 中下载后给客户。

- SecureNAT 客户

SecureNAT 客户的请求首先通过 NAT（Network Address Translation）驱动器。NAT 的作用就是用防火墙外部网卡的 IP 地址替代 SecureNAT 客户的局域网 IP 地址。随后，客户请求到达防火墙服务，根据规则匹配决定访问是否许可。接下来各种应用层过滤器对请求进行过滤。如果 SecureNAT 客户请求的是一个 HTTP 的对象，那么 HTTP 重定向器会把这个请求转发给 Web 代理服务。

- 防火墙客户

防火墙客户的请求直接被发到 ISA Server 计算机上的防火墙服务。在此，防火墙服务匹配规则决定访问是否被允许。随后各种应用层过滤器对请求进行过滤。如果防火墙客户请求的是一个 HTTP 的对象，那么 HTTP 重定向器会把这个请求转发给 Web 代理服务。

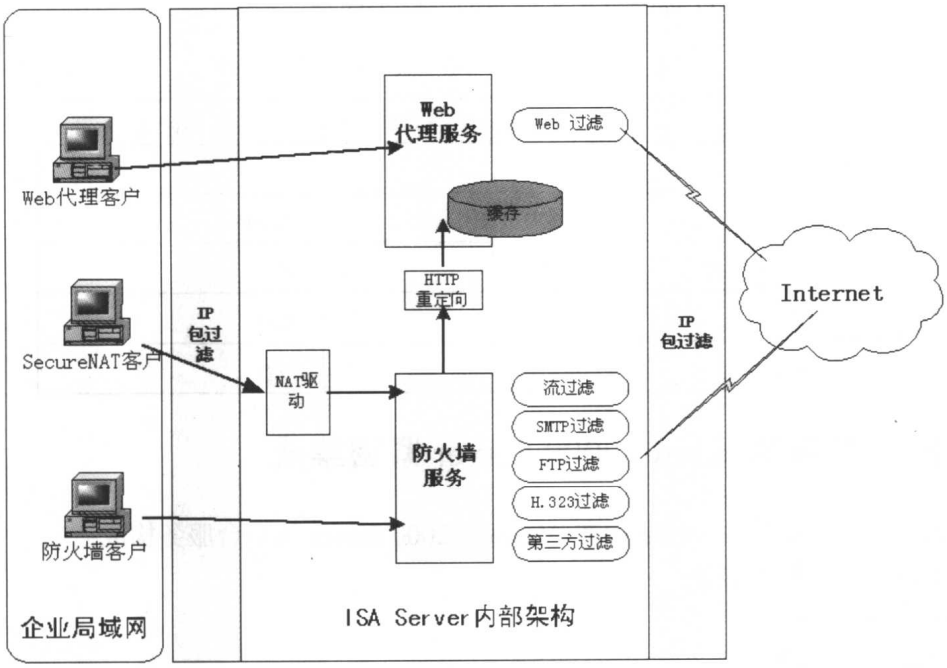

图 1-2　ISA Server 的架构与核心功能

防火墙客户和 SecureNAT 客户也可以同时配置为 Web 代理客户。如果计算机上的 Web 应用程序，例如 IE 浏览器配置为明确地指明使用 ISA Server 的 IP 地址和代理端口，那么所有的 Web 请求直接由 Web 代理服务去处理。所有其他的非 Web 请求首先由防火墙服务来处理。

1.3　实验环境配置

实际网络环境

为了实现本书的大部分实验，至少需要 3 台计算机。

- ISASERVER

外部网卡 IP 地址：10.0.0.1/255.0.0.0

内部网卡 IP 地址：192.168.0.1/255.255.255.0

- Internal

IP 地址：192.168.0.2/255.255.255.0

- External

IP 地址：10.0.0.2/255.0.0.0

网络拓扑结构如图 1-3 所示。

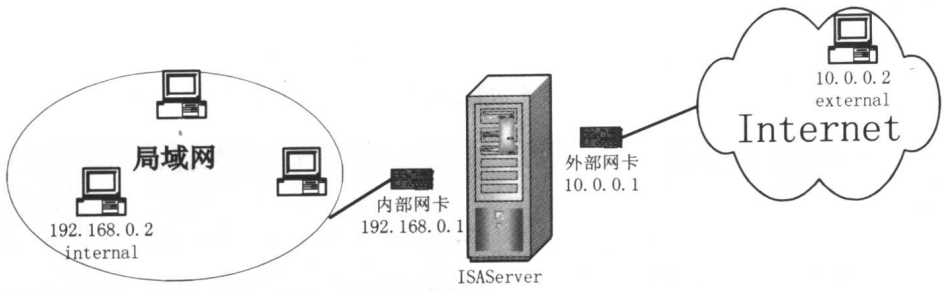

图 1-3　实验环境配置

具体到不同的案例，需要的计算机数目及其配置会有所不同。涉及到邮件服务器的发布时，还需要有另外的 Exchange Server。在 VPN 部分的实验中，还需要有路由器及接入服务器等。

虚拟机环境

如果没有实际的硬件环境，也可以在 VMware Workstation 软件中安装虚拟计算机来完成，完全可以模拟真实的实验环境。这样要求运行 VMware 的计算机的内存至少应该在 512KB 以上。否则，同时运行 3 个以上的虚拟机时，会使主机的性能下降到不能忍受的地步。

关于 VMware 的使用方法，可以参考本书的附录部分。

- 虚拟机 ISASERVER

外部网卡类型为 Custom 使用 Vmnet3，IP 地址：10.0.0.1/255.0.0.0

内部网卡类型为 Custom 使用 Vmnet2，IP 地址：192.168.0.1/255.255.255.0

虚拟计算机 ISAServer 的网卡配置如图 1-4 所示。

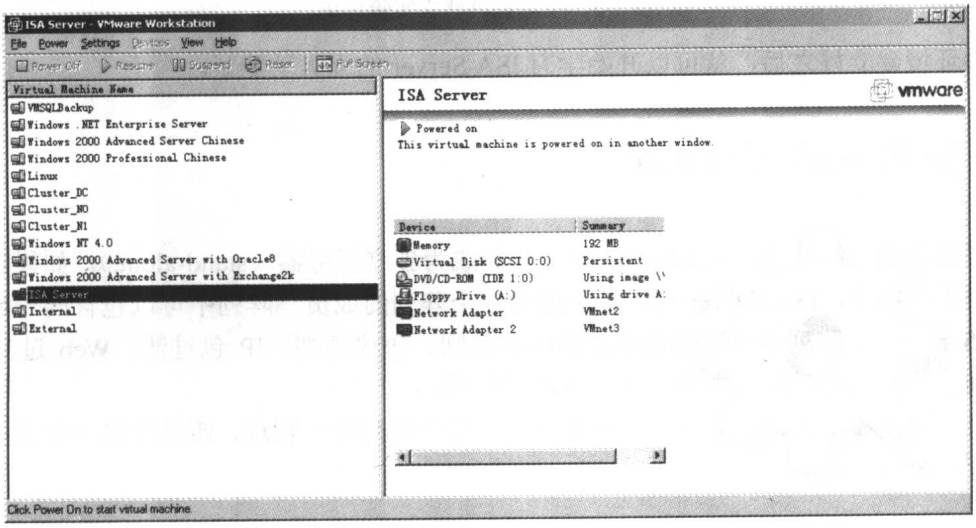

图 1-4　虚拟计算机 ISAServer 的网卡配置

- Internal

网卡类型为 Custom 使用 Vmnet2，IP 地址：192.168.0.2/255.255.255.0

- External

网卡类型为 Custom 使用 Vmnet3，IP 地址：10.0.0.2/255.0.0.0

如图 1-5 是笔者用 VMware 同时运行 3 台虚拟计算机时的截屏图。

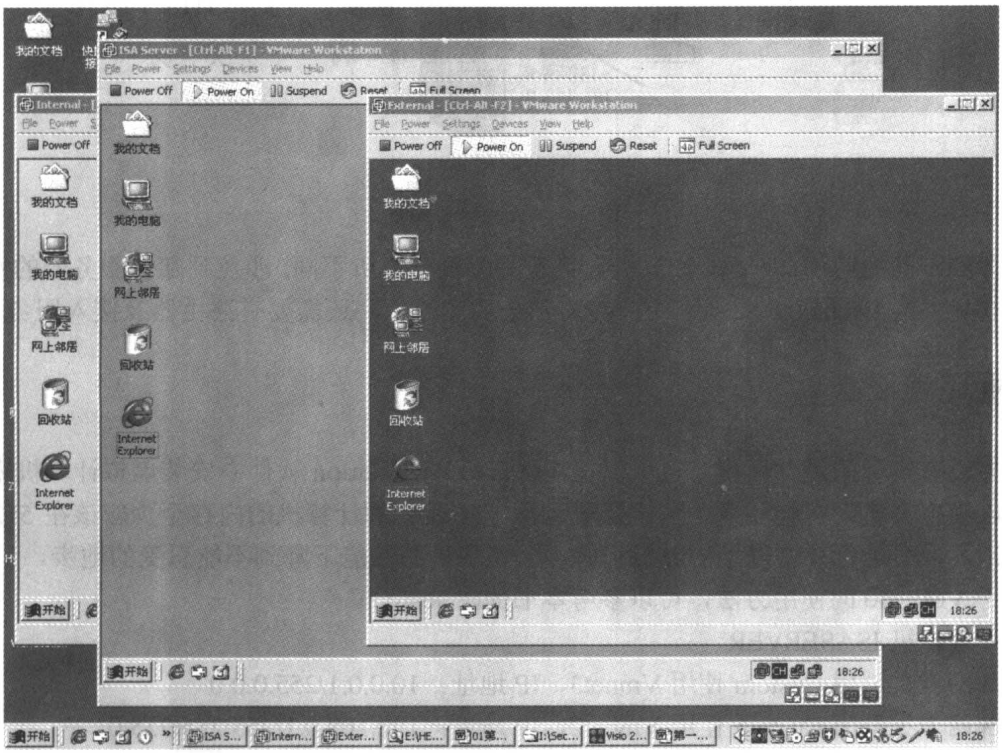

图 1-5　用虚拟机建立实验环境

实验环境建立好之后，就可以开始学习 ISA Server 的强大功能了。

1.4　安装 ISA Server

如果是小型网络环境，ISA Server 可以安装成为独立服务器（stand-alone）。如果是在企业级多用户的环境中，ISA Server 可以安装成为一个阵列的成员。阵列中可以包含同一域中的多台 ISA Server。在阵列中可以创建站点和内容规则、协议规则、IP 包过滤、Web 过滤和 Web 发布规则。阵列规则对阵列中的所有服务器起作用。

如果网络规模很大，也可将一个企业划分为几个阵列统一管理，通过设置一个或多个企业策略进行集中管理。