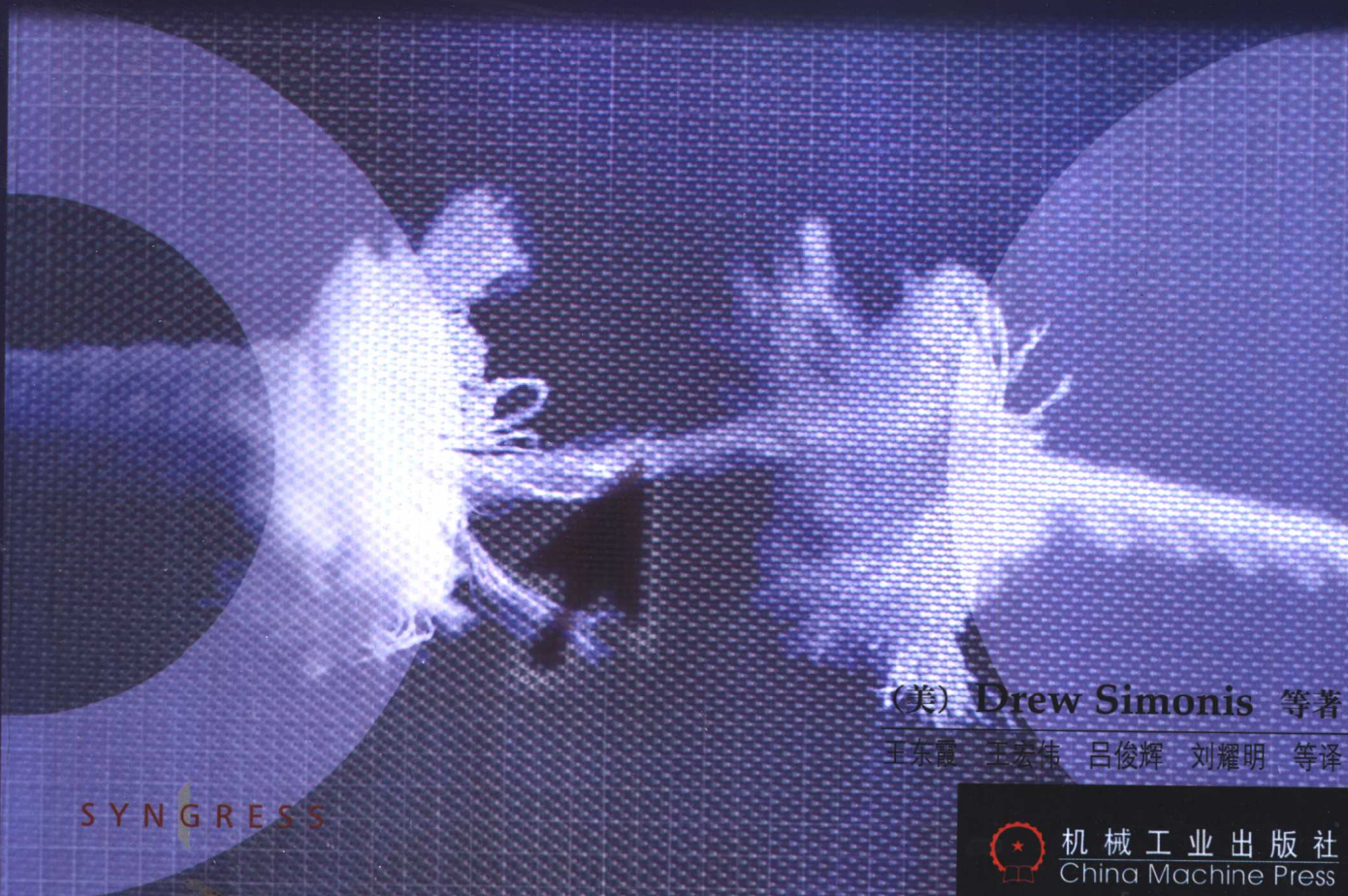
HZ BOOKS

Check Point Next Generation Security Administration

网络专业人员书库

Check Point NG 安全管理



(美) Drew Simonis 等著

王东霞 王宏伟 吕俊辉 刘耀明 等译

SYNGRESS

机械工业出版社
China Machine Press

网络专业人员书库

Check Point NG 安全管理

（美）Drew Simonis 等著

王东霞 王宏伟 吕俊辉 刘耀明 等译

机械工业出版社
China Machine Press

本书是关于Check Point VPN-1/FireWall-1 NG 的权威参考书。主要内容包括：Check Point VPN-1/FireWall-1 NG 套件的介绍、安装、GUI使用、安全策略、网络地址转换、配置和管理工具、开放安全和内容过滤、管理策略和日志、跟踪和报警、远程客户端的安全保护和相关的高级配置，附录还提供了子网掩码表和基于可信任身份的攻击等内容。

本书可读性强，章节编排自然，针对性极强，各章既相互依赖又自成体系，是一本不可多得的好书。适合于安全管理员、安全技术人员、对Check Point产品感兴趣者，可帮助读者直接在桌面使用Check Point VPN-1/FireWall-1 NG，并建立牢固的安全解决方案。

Drew Simonis, et al: Check Point Next Generation Security Administration (ISBN 1-928994-74-1).

Original English language edition published by Syngress Publishing, Inc.

本书版权登记号：图字：01-2002-1879

图书在版编目(CIP)数据

Check Point NG 安全管理 / (美) 西蒙斯 (Simonis, D.)等著；王东霞等译. - 北京：机械工业出版社，2003.1

(网络专业人员书库)

书名原文：Check Point Next Generation Security Administration

ISBN 7-111-11185-0

Ⅰ. C… Ⅱ. ① 西… ② 王… Ⅲ. 计算机网络 - 安全技术 - 软件工具，Check Point NG Ⅳ. TP393.08

中国版本图书馆CIP数据核字(2002)第092140号

机械工业出版社 (北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑：周 睿

北京市密云县印刷厂印刷 · 新华书店北京发行所发行

2003年1月第1版第1次印刷

787mm × 1092mm 1/16 · 26印张

印数：0 001- 4 000册

定价：49.00元

译 者 序

在计算机网络安全界，没有人不知道Check Point。

作为业界最优秀的防火墙提供者，甚至是因特网安全方面的领头羊，Check Point不断地提高其产品的功能、性能和易用性，突破技术上的难点，以保证其在市场上的优势和在人们心目中的地位。Check Point 的主导产品是FireWall-1。VPN-1/FireWall-1 Next Generation（简称NG）的隆重推出，比以前的版本有了许多增强和改进，旨在为企业安全解决方案的开发和实施提供必需的工具。人们都希望了解它的有关知识，这本书正是关于NG的一本很好的指南。

本书的特点是详细描述了Check Point NG的多个层面。如果想了解防火墙原理及NG的新技术理论，可以参考本书；如果想知道NG的实现方法和技巧，可以参考本书；如果想懂得如何使用和管理NG，还是可以以本书作为参考。

本书是由多个作者合作完成的，他们都是网络安全专家，也是Check Point的认证安全专家，同时还是网络安全的宣传家和活动家，因而在书中，他们不仅将防火墙的原理、SVN体系、状态检查机制等理论与技术讲述得清晰、透彻、深入浅出；而且对NG产品也描述得十分详尽，对它的新特征以及如何安装、配置、使用GUI、管理及升级等等均一一示例说明。从而使得本书既具有知识性，又不枯燥，一旦阅读，很自然深入其中，十分易于理解和掌握。

本书安排很具有条理性，通读全书将会给读者一个全面的理解，每一章同时又是相对独立的。读者可以直接阅读感兴趣的章节。而且并不需要有多少经验，也不要求以前使用过此类产品，因而本书在作为NG技术全面指南的同时，也可以作为防火墙技术、NG技术的入门书。特别是如同作者所希望的那样，拿着这本书，直接就可以使用Check Point VPN-1/FireWall-1来建立一个牢固的安全解决方案。

参与本书翻译工作的还有李林、李卓林、聂宛析、田敏、金光、吴小光、龚露娜、吴新鸣、张小冰、李海涛、文静、李祥、刘海宁、丁镇兴、万仁伟、刘晶晶、方平、邓盛骋、陈小冲、郭龙永、王冶等。本书的出版是集体劳动的结晶，前导工作室全体工作人员共同完成了本书的录排、校对等工作。由于时间仓促，且译者的水平有限，在翻译过程中难免会出现一些错误，请读者批评指正。

如果您在阅读中碰到了什么问题，请同我们联系：qiandaobook@163.com。我们会尽力解决您的问题。

译 者

2002年9月

前　言

我们生活的世界正在变得越来越小。感谢Internet的无处不在，使得我们与越来越多的人们比世界文明史的任何时候都要接近。我们可以同地球另一端的合伙人进行着商业交易，而同时我们又可以同我们的邻居聊天。十年前这被认为是一件奇迹，今天却已经成为屡见不鲜的现象。然而所有这些便利之处并不是可以自由获取的。

尽管这个世界正变得越来越小，但我们还是不能把它看成是童话中的小镇。我相信每个人都听说过有这么一个地方，每个人都相互认识，而且路不拾遗、夜不闭户。不幸的是，我们面临着网络安全问题，我们所处的环境可不是这种地方。为了更好地解决网络安全问题，必须首先假设我们是住在一个有偏执狂以及精神紊乱病人的城市里。我们不认识我们的邻居，但我们知道许多人希望通过非法途径获得我们的利益。这样，我们不仅要锁紧家门，还得焊紧门缝，在窗户上加上栅栏。我们不希望任何人在未经许可的情况下进入，当有人进来时我们需要非常近距离地观察他们。

Check Point为我们提供了解决目前数字世界所处困境的方法。其优秀的VPN-1/FireWall-1安全产品可以在很长时间内消除由于担心有人从家中伸出一个小木棍通向外界，从而导致家被暴露在外而带来的恐惧。作为最新的产品，领先市场的VPN-1/FireWall-1产品不采用常规的版本号，而是用“Next Generation”（即NG）来代替。这个名称很好地体现了产品的特色，比以前的版本有了许多增强和改进的地方。这些改进之处包括支持新的AES加密标准（DES的替代者），一个功能丰富的新GUI以及提高了配置的易用性。

本书的目的是给读者以指导。我们希望读者拿着这本书，直接就可以使用Check Point VPN-1/FireWall-1建立一个牢固的安全解决方案。阅读本书不需要多少经验；也不必担心以前没用过此类产品。本书的每一章都建立在前面章节的基础上，所以通读全书将会得到一个全面的理解，但本书每一章同时又自成一体，这意味着读者可以直接阅读感兴趣的章节，以便快速查找到结果。

在第1章中，我们将首先介绍Check Point NG产品套件。读者可学习NG提供的各种组件，以及它们是如何使用Secure Virtual Network（SVN）作为基础进行通信的。NG在主管理台使用一个内部认证授权，它使用Secure Internal Communication（SIC）生成、发布和认证授权。读者可以初步了解Security Dashboard（安全模板）和Visual Policy Editor（可视化策略编辑器）。我们将阐述VPN-1/FireWall-1体系结构，描述它如何检查数据包，并讨论其性能和可扩展性。

在第2章，我们将引导读者安装VPN-1/FireWall-1产品。我们将讨论许可、如何保证防火墙主机安全、网络以及DNS。在做好准备后，我们将一步一步地描述如何在Windows、Solaris和Nokia平台上安装VPN-1/FireWall-1软件。该章将为那些必须安装VPN-1/FireWall-1 NG（无论是在单机还是在分布式环境下安装）的读者提供非常有价值的参考。

这个产品一旦安装完毕，而且已经完成了基本的配置，就需要使用管理GUI。第3章将让读

者熟悉Check Point VPN-1/FireWall-1 NG的每个GUI Client：Policy Editor（策略编辑器）、Log Viewer（日志浏览器）、System Status（系统状态）以及SecureUpdate（安全更新）。我们将介绍如何登录和使用每个界面，以及在创建安全策略前需要定义的一长串对象的细节。这些将是创建下一章要讨论的规则的基础。

在开始创建构成FireWall-1规则库的安全策略之前，需要有一个企业级范围内的信息安全策略，包括一个由标准、指导方针和规程组成的Executive Security Policy（可执行安全策略），它用于实现和维护信息安全程序。第4章将引导读者熟悉这个过程。一旦完成策略的文档制定，就可以将其转换为Check Point VPN-1/FireWall-1 NG策略编辑器可以执行的安全策略。该章剩下的内容主要讨论Check Point策略编辑器的使用。从一个空策略开始，该章将引导读者利用一些必需的工具创建和维护一个安全规则库。

接下来，我们将在第5章详细讨论Network Address Translation（NAT）。NAT能解决网络面临的一部分困难，它允许机构在防火墙内部使用私有的地址并防止它们的公开地址对外开放。FireWall-1以前的版本总是使用服务器端的NAT，它要求管理员在使用NAT前配置操作系统中的主机路由，将网络流量推向一个给定的网络接口。Check Point VPN-1/FireWall-1 NG产品则能提供在客户端配置NAT的能力，这意味着在需要NAT时不必再为连接添加一个路由。还可以配置系统使得ARP可以自动完成。我们将讨论所有这些内容，并将详细讨论hide（隐藏）和static（静态）NAT以及manual（手动）和automatic（自动）NAT。

第6章提供了在VPN-1/FireWall-1中配置和管理用户需要使用的工具。我们将讨论不同类型的用户名/口令认证模式，以及如何实现它们（例如FireWall-1口令、RADIUS等等）。我们将引导读者在规则库中配置User Auth（用户认证）、Client Auth（客户认证）以及Session Auth（会话认证），并讨论各种认证方法的优劣。最后我们还将重点描述LDAP认证，并介绍如何配置防火墙来管理和认证LDAP用户。

接下来的第7章主要介绍Check Point的Open Security（OPSEC）标准及其支持的应用和内容安全。如果希望在防火墙中使用病毒扫描软件、使用如同WebSense一样的内容过滤器来过滤基于目录的Web站点，或者使用报告工具，那么阅读该章将非常有用。我们将审视使用FireWall-1安全服务器、不用第三方应用参与的内容安全功能。

第8章主要讲述管理策略和日志。我们将给读者提供一些重要的管理工具来维护Check Point VPN-1/FireWall-1 NG系统。我们还将讨论一些主题，包括如何管理日志、维护策略编辑器中的安全策略、对重要的防火墙文件进行备份以及易于实现的性能调节。该章还向读者推荐一些疑难解答工具，以帮助读者诊断系统中的系统问题。

第9章主要讲述如何配置各种各样的日志记录和警报。可以在各种地方进行跟踪，如策略编辑器GUI中的规则、用户属性以及策略的全局属性等等。该章将定义警报并描述NG中各种警报机制的不同之处。

第10章将带领读者进入虚拟专用网（Virtual Private Network，VPN）的世界。该章首先介绍一些VPN的背景，提供有关加密的发展概况并描述在Check Point VPN-1中所用的各种加密机制及算法。该章还将讨论网关到网关的VPN以及SecuRemote VPN，并指导读者如何对它们进行配置。

第11章同第10章紧密相连，通过Check Point的策略服务器、桌面安全选项以及SecureClient软件对远程客户端进行保护。SecureClient同SecuRemote一样，添加了个人防火墙功能。策略编辑器中的Desktop Security页面用来为远程客户的桌面创建一个细粒度安全策略。该章同时还提供SecureClient软件包工具的有关信息，为创建一个自定义的SecuRemote/SecureClient软件包提供详细的步骤说明。

第12章讨论NG防火墙的高级配置。该章将讨论Single Entry Point（SEP，单入口点）和Multiple Entry Point（MEP，多入口点）VPN设计，并详细介绍它们在VPN-1/FireWall-1中的配置。该章将设置Check Point High Availability（CPHA，Check Point高可用性）模块并讨论其他的高可用方法，如在Nokia平台上的路由和VRRP以及像Foundry ServerIron XL内容交换机之类的硬件设备等。

附录A为读者提供了有用的网络掩码清单，在处理网络地址和子网掩码时很有用。附录B中的内容稍微有点偏离我们的主题，不是讲述用Check Point的产品来提供安全，而是集中讨论欺骗攻击（spoofing attack）的理论和方法。为了成功地保护自己的网络系统，必须对那些网络恶意攻击者的动机和手段有所了解。在该附录中，Dan "Effugas" Kaminsky，世界著名的加密专家（他经常在Black Hat Briefings和DEF CON大会上演讲），提供了对欺骗攻击深入而极有价值的讲述。

编著本书是个愉快的经历。我想对任何Check Point VPN-1/FireWall-1产品感兴趣的人来说，本书都是强大的资源。我希望读者能从中汲取丰富的知识。

——Cherie Amon，技术编辑和作者之一
Check Point 认证安全专家（CCSA、CCSE、CCSI）
资深网络安全工程师/安全导师、活动家
——Drew Simonis，作者之一
Check Point 认证安全专家（CCSA、CCSE）
资深安全工程师，RL Phillips Group，LLC

关于作者

Drew Simonis（CISSP、CCNA、SCSA、SCNA、CCSA、CCSE、IBM CS）是RL Phillips Group，LLC的高级安全工程师，他为美国海军提供高级安全咨询、并负责大型企业级网络的工作。Drew是一个安全全才，在系统管理、因特网应用发展、入侵检测和防范以及渗透测试方面资历深厚。他是《Hack Proofing Your Web Applications》（Syngress 出版社出版，ISBN:1-928994-31-8）和《Hack Proofing Sun Solaris 8》（Syngress出版社出版，ISBN:1-928994-44-X）两本书的作者之一。Drew的背景包括担任过Fiderus各种各样的咨询职位、AT&T的安全体系结构设计师以及IBM的技术部门经理。Drew从South Florida大学获得学士学位，是美国MENSA的成员。他目前同他的妻子Kym和女儿Cailyn、Delany居住在Virginia州的Suffolk。

Daniel Kligerman（CCSA、CCSE、Extreme Network GSE、LE）是TELUS的咨询分析专家。作为TELUS Enterprise Solutions Inc.的一位成员，他的专业涉及路由、交换、负载平衡和Internet主机环境的网络安全。他毕业于多伦多大学，拥有计算机科学、统计学以及英文语言学学士学位。Daniel目前居住在加拿大的多伦多，在此他要感谢Robert、Anne、Lorne和Merita对他的支持。

Corey S.Pincock（CISSP、MCSE、GSEC、MCDBA、CCSA、CCNA）是位于Florida州Tampa的CastleGarde公司的一个高级信息安全设计师。作为一位Graham-Leach-Bliley和HIPAA信息安全方面的专家，Corey为国家级的金融和卫生机构提供咨询，设计实现包括安全策略开放、风险评估和安全基础结构设计、实现、培训以及监视等内容的安全程序。其他涉及的领域包括防火墙评估和审计、Windows 2000和密码系统。Corey曾经是CommerceQuest的网络管理员、MicroAge的系统工程师以及Certified Tech Trainers的高级讲师。Corey从华盛顿大学获得学士学位并是ISSA成员。Corey目前和他的妻子以及两个女儿居住在Florida州的Tampa。在这里他要感谢他的妻子Shelly，感谢她鼓励他努力工作，并对Certified Tech Trainers的Allen Keele表示感谢。

Dan "Effugas" Kaminsky（CISSP）在Cisco Systems工作了两年，主要是为大规模网络监控系统设计基础安全结构。Dan在几个主要的专业协会都有论文发表，包括Linuxworld、DEF CON和Black Hat Briefings。他还对OpenSSH作出过贡献，OpenSSH是当今使用的最重要的密码系统之一。他于1997年建立了交叉学科研究DoxPara Research（www.doxpara.com），试图结合心理学和科技理论为非理想但真实的环境创建一个更有效的系统。他以硅谷为研发基地，目前在California的Santa Clara大学研究信息系统的运行和管理。Dan同时也是畅销书《Hack Proofing Your Network》（Syngress出版社出版，ISBN：1-928994-70-9）的作者之一。

Jeff Vince（CCSA，CCSE）是Ontario的Waterloo的安全咨询顾问，其工作内容主要涉及中等或者大规模安装网络的安全网络结构和防火墙配置。他的专长主要集中在从防病毒软件到入侵检测以及运行在Microsoft Windows和Linux平台上的企业级安全管理软件等一系列安全产品上。除了一般的客户咨询工作，Jeff还是一个专业安全队伍的一员——对那些从高级金融机构和宽带服务提供商到小型软件开发公司所使用的网络进行成功的攻击和渗透测试。同时作为外部的攻击

者试图突破网络和内部的安全管理者努力保护公司的资产，这两种角色使得Jeff在网络安全上见解独特。关于安全问题的双重视角使得他可以帮助客户构建在今天的Internet环境中可以提供高可用和满足安全需求的基础网络结构。

Doug Maxwell（CCSI）是Connecticut州East Hartford的Activis，Ltd.公司的高级网络工程师。他是技术支持部门的第三级工程师，同时是获得Check Point证书的讲师。他的研究涉及UNIX网络安全和防火墙网络集成。Doug从Amherst的Massachusetts大学获得计算机科学学士学位，是Association for Computing Machinery（ACM）、USENIX、SAGE以及System Administrator's Guild的成员。他目前同他的妻子和一岁的儿子快乐地居住在Connecticut州的Ellington。

Simon Desmeules（CCSE、ISS、MCSE+I、CNA）是一个独立的有关计算机安全领域的专家。他目前为加拿大和美国财富1000的几个公司提供安全领域技术支持，包括体系结构设计、技术咨询和处理应急事件。他曾经是加拿大早期网络安全、Maxon服务以及管理安全客户的防火墙/入侵检测方面的安全专家。他是FW-1、ISS & Snort邮件列表的一个积极成员，他经常同邮件列表中的安全专家们探讨发现的新问题。

技术编辑

Cherie Amon（CCSA、CCSE、CCSI）是Integralis的高级网络工程师和安全讲师。她是Check Point的授权安全讲师，从1997年以来就一直进行Check Point产品的安装、配置和支持工作。Cherie在Connecticut州East Hartford的Integralis Authorized Training Center（ATC）讲授Check Point课程，这是该州惟一的一个Check Point ATC。在到Integralis工作之前，她曾经在IBM Global Dialer（即现在的ATT Global Dialer）做技术支持。Cherie居住在Florida州的Tampa，并在Tampa的South Florida大学就读，现在正准备获得数学学位。她在此感谢她的丈夫Kyle Amon和父亲Jerry Earnest，感谢他们使她走上了计算机技术之路。

技术审编

Allen Keele是一个作家和演讲家，拥有20多个技术认证，包括CISSP、SCNP、CCSE+、CCSI、CCNP、CCDA、NSA、NVGA、MCSE、CCEA、CCI和PSE。Allen早年在Georgia大学因为风险管理方面的成就获得商业学位，并从1998年开始为美国和西欧的一些国家提供高级技术和安全培训。现在他领导Certified Tech Trainers，Inc公司，为美国和欧洲提供有关Check Point（CCSE/CCSE/CCSE+）和安全认证程序（SCNP/SCNA）技术认证的全面的InfoSec培训。

目　录

第1章 Check Point NG 介绍

本章内容概要：

- Check Point NG 产品套件简介
- 理解VPN-1/FireWall-1 SVN组件
- 防火墙技术概览

☑ 小结

☑ 本章内容快速浏览

☑ 常见问题解答

1.1 简介

Check Point Next Generation (NG) 套件是便于开发和配置企业安全方案的必要工具。多年来，Check Point VPN-1/FireWall-1一直在努力超越它的竞争对手，NG套件提高了该软件的视觉、外观以及易于使用的特点。最值得一提的是，现在它有一个新的安全面板，可以在一个窗口中为安全管理员提供一个更为详细的安全策略和管理对象视图。该用户界面易于理解，并集中提供了所有优化的功能。

使用NG软件，可以从一个中心管理服务器管理多个防火墙，并且能通过SecureUpdate应用程序集中管理许可证和软件升级。NG套件中其他实用工具包括LDAP账号管理、SecuRemote VPN、带宽使用服务、DNS/DHCP服务、报表、日志和高实用性配置工具。

本章将介绍这些工具，较为详细地讨论VPN-1/FireWal-1的各种组件。从中可以学到代理防火墙、包过滤防火墙和Check Point NG所采用的名为状态检查(Stateful Inspection)技术之间的差别。通过学习将逐渐熟悉检查引擎，它是整个软件的核心，并且了解它是如何分析通过防火墙的网络数据的。

1.2 Check Point NG 产品套件简介

Internet每天都在向前发展，随之而来的是新的网络安全和网络管理的挑战。几年前，当我第一次和防火墙打交道的时候，很容易将网络定义和想像成简单的安全区："信任"防火墙之后的任何事物，"不信任"防火墙之前的任何事物。在那时网络安全看起来很容易：在内部网络访问Internet的地方加入防火墙，也可为Web和邮件服务器加上非军事区(De-Militarized Zone，DMZ)。但是现在新的因特网应用程序、外部网络和VPN已经变得很普通，我发现DMZ不能令人信任，甚至我过去认为是可信任的网络也不能信任。为了适应新的网络安全需要，我们不仅需要安全的、可扩展的防火墙技术，还需要提供服务质量(Quality of Service, QoS)、网络管理以及对网络基础设施的使用和状况进行日志记录及报告的工具。

Check Point Next Generation套件由几个不同产品捆绑而成，用来创建完整的企业安全解决

方案。这些特定工具的组合，使得NG套件能够解决今天网络管理员所面临的主要网络安全和网络管理问题。Check Point不是只从防火墙和VPN角度解决网络安全问题，而是提出了自己的安全虚拟网络(Secure Virtual Network，SVN)体系，将企业安全领域的所有问题用一个简单易用的产品来解决。直到最近，很多企业安全管理员还认为在通向Internet的连接处加上简单的防火墙就可以实现他们所需要的所有安全。在今天的网络世界里，除了考虑内部网络(Intranet)和外部网络(Extranet)的安全，还有远程拨号和VPN访问需要考虑。SVN体系结构瞄准整个企业网络，不仅包括局域网(Local Area Network, LAN)和广域网(Wide Area Network，WAN)连接，而且扩展到单个的VPN用户连接。这种新型的企业级安全可视的解决方案定义了一个完整、可扩展和安全的体系结构，这需要将几个产品集成起来才能达到目的。

NG产品套件就是按照SVN体系结构进行设计，用来满足网络安全和网络管理的需要。使用VPN-1/FireWall-1在网络间建立防火墙并且为VPN通信提供一个强健的端点，可以满足绝大多数公司主要的安全需要。保护好前门之后，添加到NG套件中的SecuRemote就可作为一个桌面应用程序来简化VPN的设置。Secure Client被设计成建立在SecuRemote功能基础之上，允许安全管理员为连接到VPN服务的桌面计算机设置和实施桌面安全策略。解决了绝大多数公司需要的防火墙和VPN能力之后，NG转向解决用户管理问题。在此套装软件中增添了两个工具，可以使得安全管理员很方便地管理用户和账号。增加的账号管理(Account Management)组件可以管理存储在LDAP服务器上的用户账号；用户授权工具(UserAuthority，UA)可以使得其他应用程序获得VPN-1/FireWall-1所拥有的认证信息。为了帮助管理IP网络，NG套件中增加了另外两个工具。Meta IP可以很方便地管理DNS和DHCP服务器，而FloodGate-1提供VPN和Internet网络所需的QoS管理。最后，为了提供详细的安全和使用情况报表，Check Point增加了报表模块(Reporting Module)工具。该工具所提供的信息不仅可以源于NG套件产品，而且可以来源于所支持的第三方应用程序。通过把这八个工具组合进一个套件中，NG为网络和安全管理员提供了一个集成的可扩展的软件包，用于今天企业网络中所需要的安全和管理任务。

为了将这些产品捆绑成一个易于管理的解决方案，NG包含了一个新的安全面板(Security Dashboard)，它将策略编辑器(Policy Editor)中的优点和附加的对象显示窗口以及可选的可视化策略编辑器(Visual Policy Editor)集成在一起。如图1-1所示，安全面板不仅提供了管理整个NG套件的统一窗口，而且由于不同产品集成在一起，各应用程序可以快速方便地移动并共享配置信息。

1.2.1 VPN-1/FireWall-1

当人们提到Check Point这个名字的时候，绝大多数人想到的是作为NG套件基础的VPN-1/FireWall-1。VPN-1和FireWall-1产品是设计用来阻止连接到防火墙的、来自或是通向网络的非授权访问的，它基于安全管理员所定义的规则。VPN-1/FireWall-1使用一套规则来创建安全策略。这个策略装载到防火墙的检查引擎(Inspection Engine)组件中并且检查通过防火墙网络接口的所有数据流。

尽管有人通常将VPN-1和FireWall-1看成是一个产品，尽管很多人使用FireWall-1(FW-1)一词来同时指代两个产品，但是它们的功能有很大的不同。FireWall-1提供了任何防火墙都必需的数据过滤、日志和访问控制功能。VPN-1紧密集成到FireWall-1中，用来增加防火墙之外的虚拟专

用网工具。将VPN-1和FireWall-1组合起来，能够让Check Point提供功能更为强大的防火墙和VPN产品，并且将功能无缝集成在一起可以通过单一管理程序进行管理。VPN-1和FireWall-1捆绑在一起使得你可以将VPN网关内建到防火墙中，而不是去维护两个单独的机器分别提供防火墙和VPN服务。这可以简化网络的复杂性和安全策略，更易于管理并会减少配置失误的可能性。

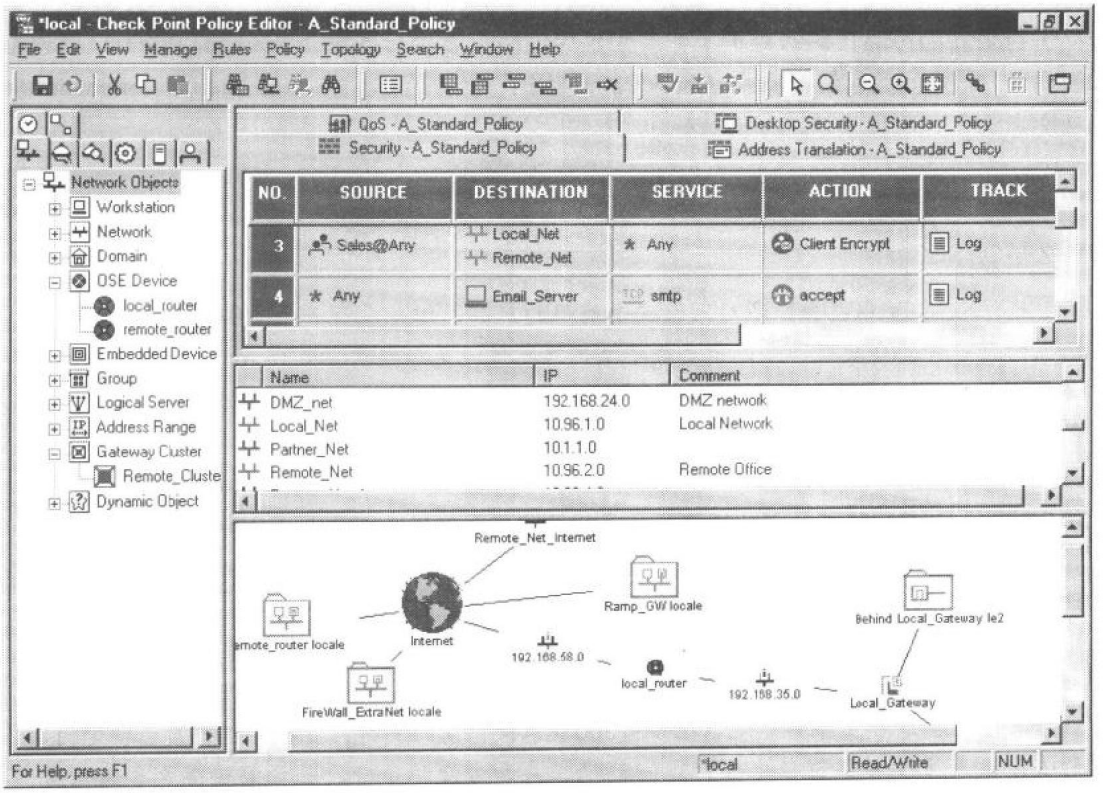


图1-1 NG 安全面板

虽然VPN-1提供了支持站点到站点的VPN所需的所有工具，甚至改进了对第三方防火墙产品设置的支持，但是单个的用户到站点的VPN连接仍然存在问题。为了确保在使用用户到站点VPN连接的时候VPN-1能够提供所需的标准加密、安全和访问控制级别，Check Point升级了SecuRemote和Secure Client软件包。通过将SecuRemote、SecureR Client和VPN-1紧密集成，Check Point不仅提供了确保用户到站点VPN连接所需的安全工具，而且能够确保它在VPN市场上的持续优势。

在NG套件中，Check Point提供了在分布式环境中管理VPN-1/FireWall-1所需的工具，这就允许安全管理员在整个企业中定义并且执行单一的安全策略。通过以分布的方式建立FireWall-1，Check Point设计的产品在大型、多个防火墙网关网络中工作时，功能和一个独立的网关产品一样优异。这种分布式特性允许从单个管理工作站来管理多个VPN-1和FireWall-1网关，不仅简化了安全策略的定义，而且简化了日志功能，因为所有网关的日志都可以从中心服务器获得。

通过创建安全面板，可以简化NG产品的管理。这个新的应用程序充分利用了FireWall-1

4.1(CP2000)中策略编辑器的特性，同时增添了新的工具来简化防火墙和其他产品的管理。全新的拖放式列表和可视化策略编辑器不仅加快了规则的创建过程，而且为用户提供了易于理解的可视化界面，有助于减少策略错误引起的安全漏洞。在NG套件中增加了几个工具，用于进一步加强在分布式环境中VPN-1/FireWall-1的可管理性。Secure Update使得安全管理员在一个中心位置就可对在FireWall-1上的产品以及在开放安全平台(Open Platform for Security，OPSEC)上认证的产品进行最新的产品代码级维护工作。为了保证防火墙执行点(Enforcement Point)、管理工作站和管理客户端之间的通信可靠性，Check Point使用了安全内部通信(Secure Internal Communication，SIC)功能来加密和验证模块之间的数据包。

设计与规划

什么是OPSEC?

尽管NG套件中包含很多对网络安全有用的产品，但是没有一个提供商会考虑到你将面临的每一种安全挑战，无论是负载平衡网络硬件还是双因素(two factor)认证软件，总还是需要使用第三方应用程序以达到所需的安全和健壮水平。使用OPSEC认证方案将可以保证所实现产品的集中管理、互操作性以及易用性。

Check Point安全合作联盟开放式平台(Open Platform for Security Partner Alliance)可以使得Check Point能通过使用认证过的第三方的硬件和软件来扩展其安全套件，从而超过了任何一个公司单独提供的能力，这些认证产品涉及安全实施、网络管理、报表生成、性能、高可用性以及电子商务领域等方面。

要想通过OPSEC认证，必须测试应用程序，保证和既定OPSEC标准以及SVN体系的一致性，这就确保了现在所投资的解决方案可以与现有合法的OPSEC程序以及将上市的新产品进行集成和互操作。现在已经有300多家提供商的支持，要找到适合自己特定问题的安全解决方案并保证兼容性，是一件很容易和方便的事情。如希望获得更多的信息，包括认证厂商清单，可以参考：www.checkpoint.com/opsec。

尽管表面上看起来VPN-1/FireWall-1 NG只是4.1版本的一个升级版，稍做一点儿深入的研究就会发现FireWall-1的核心技术——状态检查仍然是系统的核心，但是新增的工具和升级后的应用程序合在一起提供了一套完整的安全解决方案。VPN-1/FireWall-1 NG 提供了企业内部安全管理员所需的易于管理的安全工具。在进入FireWall-1核心前，我们先用接下来的几页来看看另外的几个产品，它们使得FireWall-1真正成为一套完整的解决方案，这些突出的技术和特性让Check Point成为因特网和VPN网关解决方案市场中的领导者。

1.2.2 账号管理应用程序

VPN-1和FireWall-1显著区别于其他产品的特性之一就是能够很方便地进行用户认证。无论是简单的Internet用户访问认证还是敏感的VPN连接认证，管理用户账号已经成为企业安全策略中的一大部分。为了让用户管理更加方便，Check Point提供了账号管理器(Account Management)应用程序。账号管理器允许一个或多个与OPSEC兼容的轻量级目录访问协议(Lightweight