HZ BOOKS

Check Point FireWall-1 Administration Guide

网络与信息安全技术丛书

Check Point FireWall-1

管理指南

(美) Marcus Goncalves
Steven A. Brown 著

贺卫东 周沛龙 吴亚飙 译

附赠 CD-ROM

机械工业出版社 China Machine Press

McGraw-Hill

网络与信息安全技术丛书

Check Point FireWall-1 管理指南

(美) Marcus Goncalves
Steven A.Brown 著

贺卫东 周沛龙 吴亚飙 译

吴世忠 审校

机械工业出版社
China Machine Press

本书详细介绍Check Point公司推出的防火墙技术——FireWall-1。主要内容包括FireWall-1的基本功能、安装与配置，管理FireWall-1的方法、规则库、加密技术、安全策略，FireWall-1高级功能等。本书内容丰富、条理清晰，为网络安全提供了有效的方法与策略。本书适合网络应用开发人员、网络安全技术人员等参考。

Marcus Goncalves, Steven A.Brown: Check Point FireWall-1 Administration Guide(ISBN 0-07-134229-X).

本书版权登记号：图字：01-2000-1729

图书在版编目（CIP）数据

Check Point FireWall-1管理指南 /(美) 刚卡瓦斯(Goncalves, M.)，(美) 布朗(Brown, S.)著；贺卫东等译. - 北京：机械工业出版社，2001.3

(网络与信息安全技术丛书)

书名原文：Check Point FireWall-1 Administration Giude

ISBN 7-111-08766-6

Ⅰ.C… Ⅱ.①刚… ②布… ③贺… Ⅲ.计算机网络-安全技术-应用软件，FireWall-1 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2001)第13545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：张鸿斌 李援南

北京昌平奔腾印刷厂印刷 · 新华书店北京发行所发行

2001年4月第1版第1次印刷

787mm × 1092mm 1/16 · 18印张

印数：0 001-5 000册

定价：45.00元(附光盘)

前　言

读者

很可能要利用本书的专业人员是：

- 几年或多年前毕业的关心安全问题或寻求FireWall-1认证的懂计算机的专业人员。
- 编程人员/分析人员/软件开发人员，工程师/测试工程师编程人员和项目经理。
- 管理信息系统（MIS）和信息系统与技术（IS&T）专业人员。
- 涉及内联网和互联网的建立，执行和管理的专业人员。
- Web网站管理人员。
- 想了解互联网如何工作而不是如何使用互联网的刚入门（从计算机知识上说）的专业人员。
- 可能会将此书当作快速参考资料使用的精通计算机知识的人员。

第1部分　FireWall-1概述及其结构

第1章为你提供了防火墙技术和Check Point公司的FireWall-1的概述。

第2章论述了Check Point公司的检查技术和FireWall-1的检查模块。它还论述了FireWall-1的全状态戒备，和如何保障无状态和无连接的协议，如用户数据协议（UDP），以及动态配置的端口的连接。

第3章论述了FireWall-1的结构和安装。

第2部分　管理FireWall-1的安全策略

第4章是针对FireWall-1的安全策略的。

第5章说明了建立目标程序和将它们装入FireWall-1的规则库的过程。

第6章论述了FireWall-1的先进的安全主题，如信息存储向量协议（CVP）。

第7章论述了加密技术，它在与FireWall-1进行虚拟专用连网时是需要的。

第8章说明如何在不同的防火墙设置之间建立虚拟专用网（VPN）。

第9章说明FireWall-1的VPN对远程用户的扩展，使可远程访问VPN。

第10章论述了FireWall-1的INSPECT语言，该语言可使管理人员写入他们自己的策略。

第3部分　先进的结构配置

第11章Check Point公司的OPSEC，这是一种保证不同的安全产品安全互用的工业标准。

第12章论及了先进的FireWall-1的拓扑学，如负载的平衡，纠错和记录。

第13章谈到所有管理人员都应知道的先进的防火墙的安全技术。

Check Point软件技术公司（Check Point Software Technologies Inc.）不仅在美国市场，而且在全世界都是防火墙软件最大的销售商，占有市场份额的47%。公司是制造防火墙的公司，更广泛地说，是整个互联网安全方面的领头羊。Check Point公司的主导产品就是FireWall-1，它是通过原始设备制造商（OEM）合伙销售的，这包括SUN微系统、BAY网络、Hewlett Packard和

TimeStep。它的大约54%的产品用在Window的NT平台上，并且根据该公司的说法，这个市场部分还在增长。因此，根据Check Point公司的FireWall-1在市场上的如此巨大的主导地位，有一本涵盖FireWall-1的结构和管理这个题目的书也是势在必行的了。

除了FireWall-1外，Check Point技术公司还开发适用于任何机构的基础设施的一套互联网技术。这些技术包括Provider-1，它可以让某个机构在一个地点监测数百个单独的安全策略；FloodGate-1，它是为关键应用的需要提供所需的带宽的应用带宽策略管理技术；Check Point公司的VPN-1，它是为某个机构提供企业级的VPN技术的一个系列产品，也是为达到安全通信的OPSEC众多产品。

本书通过提供安全专业人员甚至在试图安装防火墙前就应知道的防火墙技术的潜在观点，使Check Point公司关于FireWall-1的说明书更添价值。它还根据FireWall-1的安装和结构，提供了以环境为导向的企业内联网/互联网安全威胁和解决方法的梗概。

因此，本书不仅提供了有关FireWall-1的安装和管理的额外信息，而且也论及了包括FireWall-1的VPN的实施、安全策略的开发、代理服务以及所有使用FireWall-1方面的问题。本书应该是专业人员获得认证，安装、维护和扩展FireWall-1 提供的多种特性的好帮手。

本书由三部分组成。第一部分包括了FireWall-1的技术和结构方面，第二部分包括了安全策略和FireWall-1的规则库，而第三部分包括了先进的结构和管理。

目　录

第一部分 FireWall-1概述与配置

第1章 防火墙技术介绍

在当今形势之下，各公司必须保护其在公司网内外的数据。为了从内部保护自己，必须依赖于内部检查、口令保密性等。而要从外部保护自己，则必须采用特殊技术。这种特殊技术就是防火墙，它能够防止内部网络受到外界的侵害，只允许为公司安全策略所许可的协议与服务进入。当今的防火墙具备许多其他有益的功能，如认证、检查病毒、侵入检测等，其主要目的是进行安全保障。

首先应当理解什么是防火墙，其次是决定使用哪种类型的防火墙。目前关于防火墙的书籍不胜枚举，任何人通过阅读这些书都可了解防火墙技术，但要决定某公司应使用哪种防火墙，则必须拥有更深层次的知识，而这正是本书力图提供的。本书介绍Check Point FireWall-1，这是目前最先进的防火墙技术，足以消除任何安全缺陷，其灵活性可允许管理员在任何公司设置背景下进行防火墙的配置。本书假定读者了解防火墙技术、路由选择、IP地址及常用的Internet 通信，如HTTP、SMTP、DNS等。我们将基于这些基础来讨论Check Point的FireWall-1技术。

本章概述了防火墙技术，具体说是Check Point的FireWall-1技术。将涉及到Check Point的状态检查技术与FireWall-1模块；还将讨论FireWall-1的全状态检查，以及如何保密无状态与无连接的协议(如UDP)，以及动态分配的端口连接。最后，说明安装 FireWall-1的系统要求，并评价其性能。以后章节将详细讨论Check Point的FireWall-1技术的各个方面。

注意 要详细了解Check Point技术公司的产品，请与以下地址联系：

Check Point Software Technologies Ltd.

(Check Point软件技术有限公司)

美国总部

400 Seaport Court，Suite 105

Redwood City，CA (加利福尼亚州)94063

Tel: 800-429-4391

415-562-0400

Fax: 415-562-0410

电子邮件: info@checkpoint.com

http://www.Checkpoint.com

国际总部

3A Jabotinsky

Ramat Gan 52520，Israel（以色列）

Tel: 972-3-613 1833

Fax: 972-3-575 9256

1.1 防火墙技术概述

防火墙是为了禁止不必要的且未经授权的信息包从一个未加保护的网络(如Internet)进入一个专用网(如LAN或WAN)。同时，允许本地网用户访问Internet服务，并允许Internet服务(如 SMTP

与DNS)，进入内部网络。图1-1显示了防火墙的基本功能。

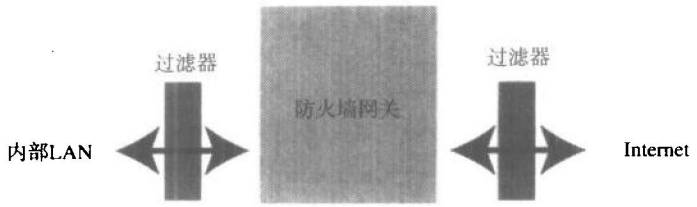

图1-1　防火墙基本功能

图1-1还显示了入站与出站过滤器。防火墙设置规则与安全策略来控制入站或出站信息包。这些将在后面详细讨论。

有些防火墙仅仅是路由器，用来过滤进来的数据报。该过滤是基于数据报包含的信息，如源地址、目的地址、较高层协议、专用网安全管理器或安全策略指定的其他标准。尽管路由器无法取代防火墙，但有些公司仍将路由器当作防火墙使用，以过滤安全策略。这一点是通过在路由器上设置访问表来实现的，如图1-2所示。可惜，在路由器上设置访问表会导致性能严重降低。

图1-2描述了包过滤的另一个问题。许多公司采取将其网络地址隐藏在其他地址后面的作法。这意味着路由器，除执行正常的路由选择职能之外，必须通过访问表来执行包过滤。另外，路由器必须执行网络地址转换(NAT)，这会增加其负担。

注意　*后面我们将看到如何在Check Point FireWall-1上设置NAT。如果你不了解NAT或需要更多信息，请阅读RFC 1918。*

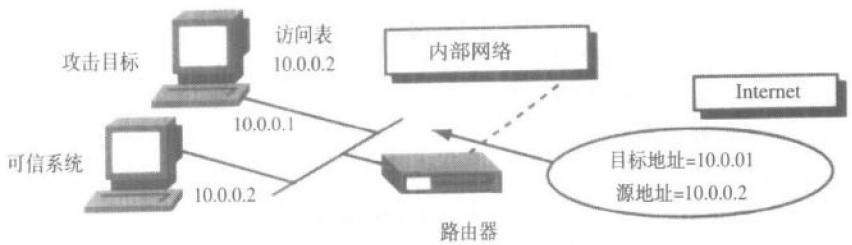

图1-2　路由器级的包过滤

有些防火墙采用代理服务器，也称为堡垒主机，如图1-3所示。堡垒主机防止内部用户直接访问Internet服务，自己则充当他们的代理者，同时过滤掉未经授权的外来 Internet 信息包。

防火墙的作用如同一道安全门，确保门内组件的安全，控制谁（或什么）进入这个被保护的环境，同时也控制什么输出。它就像一个站在前门的门卫，控制和认证谁可以或不可以访问该场所。

设置它是为了对网络信息包执行可控过滤，限制对某些Internet 端口号的访问，并可阻止对几乎任何东西的访问。为此目的，它必须具备单进入点的功能。而这正是防火墙常常与路由器集成一块的原因。

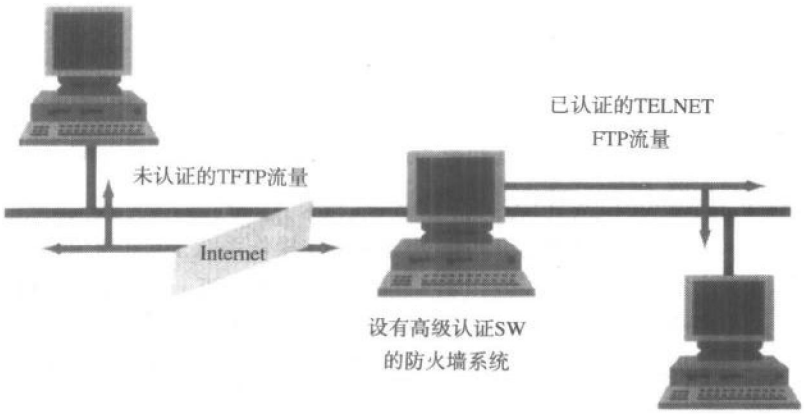

图1-3 代理服务器防止进入Internet与来自Internet的直接访问

选择防火墙系统最好要基于站点已经安装的硬件、部门现有的技术力量，以及销售商的信誉。通常，配置防火墙是为了防止来自“外界”的未经认证的交互式登录。使用防火墙来保护站点是设置一道“门”以强化安全和检查的最方便的手段。

设置了防火墙，就可能使站点防止外界使用追踪工具对其任意连接，通过简要日志了解外来连接来源、服务器的流量以及是否有任何闯入意图。

防火墙的基本功能之一是保护站点，防范黑客。如前讨论，任何站点都面临众多的威胁，而防火墙可保护站点。然而，防火墙无法对付旁路的连接。因此，要注意后门，如调制解调器对LAN的连接，尤其在基于Microsoft Windows NT的网络上，当远程访问服务器 (RAS)位于被保护的LAN之内时。

甚至前门也易受攻击。配置防火墙时，创建允许入站服务的通道。公司能够从Internet上接收电子邮件，是因为防火墙设置已允许SMTP协议 (端口25) 进入其网络。接收 Internet 邮件需要此服务，但此服务也允许黑客远程登录到邮件服务器 (通过端口25)。除安装在防火墙上的安全策略外，还必须考虑所允许的任何入站访问，并采取措施来强化在机器上使用这些服务的安全性。

然而，防火墙可以强化安全，但无法绝对保证安全！如果LAN上有重要的信息，那么首先不能允许 Web服务器连接它。要注意那些允许从组织内部访问Web服务器的群件应用程序。

还有，如果Web服务器位于内部 LAN之内，则要注意自身以及公司服务器上的内部攻击。防火墙无法对付来自组织内部的威胁。例如，一个心烦意乱的雇员就可能拔掉公司服务器的电源插头，将之关机，而防火墙对此无能为力！

包过滤一直是一种过滤不必要的入站信息包的简单而高效的手段，它可截取和读取数据包，并拒绝那些在路由器上与编程标准不相符的数据包。可惜，包过滤已不足以保证站点的安全。有众多的威胁，还有众多协议创新，可以毫不费力的旁路这些过滤器。

例如，包过滤对FTP协议无效，因为FTP为了完成数据传输，允许连接外部服务器，再将之回接至端口20。甚至路由器已加了一条规则，而内部网络机的端口 20仍暴露于外界的探查。此外，如前所见，黑客能够轻易的“愚弄” 这些路由器。防火墙可以使这些企图更难达成，但并

非绝不可能。

决定实施防火墙时，首先要确定将要使用的防火墙类型及设计。本书介绍的Check Point FireWall-1是市场上最好的防火墙。

提示 如果需要更多防火墙类型和品牌方面的信息，请参考《FireWalls Complete》一书，Marcus Goncalves著，McGraw-Hill，1998。

有些商用防火墙产品，通常称为OS 防护，可安装在操作系统上。它们颇受欢迎。它们将包过滤与代理应用程序相结合，能够监控任何协议的数据与指令流，以此保护站点。但因其特殊的配置，它们并不非常成功。由于其配置是在核心层进行，所以管理员无法看到。管理员不得不使用附加的产品来管理服务器的安全。防火墙技术发展由来已久，Check Point FireWall-1是典范之一。除“传统”的或静态的防火墙外，今天我们有了“动态”防火墙技术。静态防火墙的主要用途是“允许任何服务，除非它被明确拒绝”或“拒绝任何服务，除非它被明确允许。”而动态防火墙会“根据需要来允许/拒绝任何服务，”其适应网络传输与设计的能力使其明显优于静态包过滤型。

1.1.1 Check Point优点

关于防火墙技术，有很多可说的，本书无法全部囊括。但我想指出，防火墙并非毫无缺点，尤其老防火墙技术，因为事实上，它们都存在基础问题。它们能够控制在特定时间和特定授权条件下，哪些站点可以与哪些服务交谈。但是向整个Internet提供的服务，其开放性可能达到令人惊讶的地步。这是FireWall-1的一大优点，具备对付这些问题的增强特性，我们在后面将会看到这一点。

目前市场上的许多防火墙无法识别通过它们的数据是否为有效数据，例如，一则电子邮件消息仅是一则电子邮件消息。幸运的是，FireWall-1 提供了一项最新发明，称为数据过滤，本章后面将对此加以讨论。这里不妨说，防火墙过滤器已成为可能，它能够删除每条带有诸如“给你的重要消息” 或“应答你的查询”之类报头的消息。今天的许多攻击与病毒都以送达个人且带有此类报头的电子邮件形式而存在。当打开此电子邮件后，你的计算机系统就会染上病毒。FireWall-1 可解决此问题。

然而，目前市场上的许多防火墙还有另一个缺点：它们没有能力过滤 applet（Java的小程序）——当今它是对设防的公司网的一大威胁。而FireWall-1具备这种能力。

FireWall-1 还具备另一个其他防火墙并不具备的特性。如果黑客连接防火墙内某个系统的有效服务或端口，如前面讨论过的SMTP端口，许多防火墙会允许黑客使用有效的数据攻击或shell指令来占用该服务。FireWall-1 增强了对这些攻击的防范。

以Web服务器为例。例如，国际计算机安全协会，就曾遭受过一次“phf”攻击。此“phf”是一个缺省的实用程序，与服务器在一起，允许攻击者使用该实用程序来执行该系统的指令。此攻击看似一个正常的Web查询。不像FireWall-1，目前许多防火墙不会阻止这种攻击，除非管理员对“phf”实施邮件过滤，但这对防火墙要求甚高。

对付此类缺陷的关键在于让防火墙理解内部服务的配置。防火墙只允许Internet上的用户访

问特定的服务。可以对这些已知的服务给予特别关注，确保它们都是最新最安全的版本。如此，可以把焦点从加固整个网络转移到加固仅仅一小部分内部机器与服务上。

1.1.2 谈谈非军事区

一个DMZ (非军事区)是一个网络，它直接与安全访问点连接。它往往是网关上的另一个接口或一个运行安全应用程序的设备。实施DMZ 可确保所有信息包通过安全访问点，这使对抗黑客威胁达到最高水平。如果没有实施DMZ，所有资源在安全网络上都处在防火墙的背后。在此情形下，一旦允许一个接入试呼穿过防火墙与某个资源通信，它就处在防御范围之内。如果该资源出现故障，整个网络的安全就可能受到损害。

在图1-4所示的图中，如果网络资源位于防火墙背后而不是位于DMZ之中，任何触及这些资源的恶意攻击则可能早已突破了安全访问点。然而，如果网络资源位于DMZ之中，所有通向或来自这些网络资源的信息包则必须通过访问点，而该点得到了安全策略的巩固。这可能是最安全的配置了。

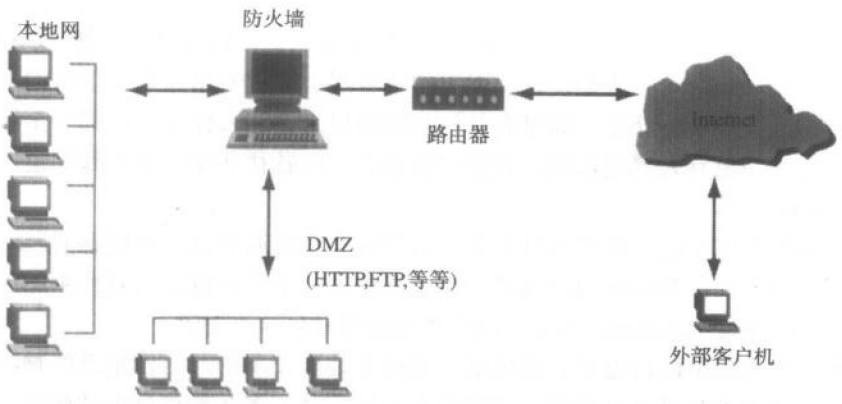

图1-4 典型DMZ的拓扑

使用DMZ的情况是一小部分机器服务于Intranet，而其余机器位于某些设备之后，通常是一道防火墙。这些机器要么处在“露天”之下，要么有另一道防火墙来保护DMZ。从安全角度看，这可能是一种不错的安排，因为只有接受入站连接的机器才是“牺牲的羔羊”。

如果不必对这些机器费力，那些成为高风险目标的组织则可以从这种设计上获益。此设计经证明对保证内部资源安全极其有效。

设置DMZ的唯一缺点在于这些机器的维护方面。多数管理员喜欢从本地访问某个文件系统来更新Web服务器与FTP服务器。在两者之间加入一道防火墙会使达到此目的稍微难一些，尤其当负责维护这些服务器的不止一个人时 (务必要有一本日志！)。总而言之，外部信息会更加稳定，而管理上的麻烦不会那么频繁。

1.1.3 认证问题

防火墙与过滤路由器倾向于以二进制的方式进行工作。要么允许，要么不允许对某个系统的

某次连接。认证允许基于用户认证的服务连接，而不是基于它们的源或目的地址。对于有些软件，一个经认证的用户允许到达特定的服务和机器，而其他用户只能访问基本系统。防火墙通常在基于用户的服务认证方面扮演重要的角色，但有些服务器加以配置后也可理解此信息。目前的Web服务器加以配置后可理解哪些用户被允许访问哪些子树，并将用户限制于适当的安全级。

认证的种类繁多，可以采取的形式包括：加密令牌、一次性口令以及最常用但最不安全的简单文本口令。站点的管理员负责确定对哪些用户采用哪种认证形式，但应该清楚有些认证必须使用。适当的认证可允许外站点的管理员进入网络并解决问题。此类连接属于应严格认证的首要对象，如应采用加密令牌的形式。

Check Point 赋予管理员在设置认证上的高度灵活性。除支持所有RFC 标准，如TACAS、S/Key及RADIUS认证方案之外，防火墙还赋予管理员在设置防火墙本身的用户认证方案方面的灵活性。Check Point防火墙支持防火墙上的用户、客户及话路认证方案，这些均在本书后面部分加以讨论。

1.1.4 对周边的信任

当今公司安全的焦点是对准周边。在安装许多防火墙时，我们常常会看到“Godiva 巧克力”的作法：外硬里软。防火墙、认证设备、强大的拨号层、虚拟专用通道、虚拟网络以及其他隔离网络的手段构成了坚硬的外壳。而里面却往往甜得出奇，任人掠夺。内部安全管理欠妥，我们常怀恐惧之心：如果有人突破边境，城堡将会崩溃。问题往往是每个人都知道这一点，但内部巩固却要等到明天！

关于此问题的解决方法，确实谈得不多。内部安全策略通常是一片敏感问题的沼泽地，大家不情愿投资加以解决。解决此问题的唯一方法寄希望于老式的游说与对此事的浓厚兴趣。政治问题很少会解决得既快又彻底。然而，信任周边最终只会导致失望。

突破防火墙的问题早已讨论过，而认证手段远非是防傻瓜的。信任站点的物理安全可能会导致灾难。对外来者的认证水平往往欠缺得令人可怕。我们多久检查过电话修理工？我们会允许一个修理工访问一个组织的最敏感的部分么？底线是周边并非保证安全的唯一地方。

1.1.5 防火墙类型

市场上有众多的防火墙，从低技术的“自己动手”方式的防火墙到较大型厂商设计的高技术咨询密集型防火墙，不一而足。防火墙所用的基础技术对其安全性和完整性是极其重要的。目前，防火墙技术主要有三种：包过滤、应用级和Check Point的状态检查。基于所采用的技术不同，防火墙可分为四类。

1. 包过滤器

这种防火墙可提供IP层的访问控制，接受、拒绝或扔掉主要基于源、目的网络地址和应用类型的包。包过滤防火墙以较低价格提供简单级别的安全。这种防火墙还具备高性能以及对用户的正常透明度。

包过滤防火墙的缺点包括：

1) 易受到那些针对网络级协议之上协议的攻击，因为这种防火墙只能理解网络级的协议。

2) 网络级协议要求了解其技术细节，而并非每个管理员都能做到这点，因此，包过滤防火墙通常更难以配置与检验，这就增加了系统误配置、安全漏洞与故障的风险。

3) 它们无法隐藏专用网的拓扑，因此，让专用网暴露给外界。

4) 这些防火墙的审计能力极其有限，而审计在一个公司的安全策略中却扮演着主角。

5) 包过滤防火墙并非支持所有的Internet 应用程序。

6) 这些防火墙并不总是支持某些安全策略条款，如用户级认证与日历访问控制。

2. 应用级防火墙

应用级防火墙提供应用级的访问控制，在两个网络间充当应用级网关。由于应用级防火墙是在应用层发挥作用，它们有能力详细的检查信息包，因此，比包过滤防火墙更安全。同时，由于这些防火墙要详细检查信息包，所以通常要比包过滤防火墙慢。因而，在某种程度上，它们是插入的，有局限性，通常要求用户要么改变其行为，要么使用专门软件来实现策略目标。应用级防火墙因此对用户不透明。

应用级防火墙的优点包括：

1) 由于它们理解应用级协议，它们能够防御各种攻击。

2) 它们通常比包过滤防火墙更容易配置，因为它们不要求了解较低级协议的所有详情。

3) 它们能够隐藏专用网的拓扑。

4) 它们具备全部的审计设施，拥有监控传输与操作日志文件的工具。这些日志文件包含的信息包括源、目的网络地址、应用程序类型、用户认证与口令、访问起止时间，以及向各方向传输的信息字节数。

5) 它们可支持更多安全策略，包括用户级认证与日历访问控制。

3. 混合型防火墙

认识到包过滤与应用级防火墙的这些缺点后，有些销售商拿出了混合型防火墙，它结合了包过滤与应用级防火墙的技术。这些混合型产品希望解决上述缺点中的一部分，但其他缺点仍然存在。

因为混合型防火墙仍然依赖包过滤机制来支持特定的应用程序，所以它们具有同样的安全缺点。

1.1.6 第二代应用级防火墙

这类防火墙仍是一种应用级防火墙，但属于第二代。它解决了早期版本存在的透明度问题，但并不降低性能。

第二代应用级防火墙的优点包括：

1) 由于其透明度与通常更高的性能，它们可用作Intranet防火墙。

2) 除可隐藏网络拓扑外，它们还可提供全网络地址转换。

3) 它们支持更高级的用户级认证机制。

1.2 Check Point的状态检查

Check Point FireWall-1的状态检查技术是基于状态检查结构，它具备防火墙的全部功能，并

确保最高级的网络安全。FireWall-1强大的检查模块分析所有包通信层，并摘录相应的通信与应用的状态信息。第2章将更详细的阐述状态检查的工作原理。在本概述中，你可领略到所有的防火墙技术。状态技术名符其实：它可监控通信状态信息。图1-5显示了Check Point 站点的屏幕浏览。

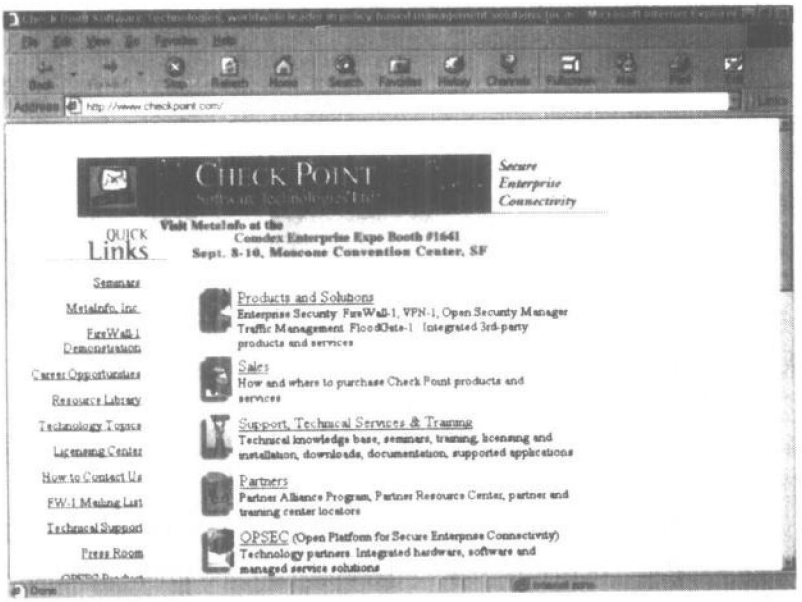

图1-5　Check Point的Web站点；大量关于安全信息以及状态检查背后的技术

1.3　选择Check Point FireWall-1的原因

在选择一种防火墙之前，首先要制定一个公司安全策略，然后选择可执行这些策略的防火墙。评估防火墙时，应注意了解在防火墙中使用的基础技术，因为有些技术在安全性方面比其他产品差。

防火墙的基本概念总是一样的，评估防火墙要基于其提供的安全水平与实施特性。所说的安全特性是指防火墙产品基于公司安全目标与策略而提供安全的能力。选择防火墙时，要看它是否具备下述特征。这些特征FireWall-1都具备：

- 安全保证——相应的防火墙技术实现其技术规范并适当安装的独立保证。这种防火墙产品是否通过了国际计算机安全协会 (ICSA http://www.ncsa.com/)的认证？是否有通信安全机构 (CSE)的评估？
- 特许控制——产品施加用户访问限制的程度是很重要的。
- 认证——该技术包括安全特性，如源/目的计算机网络地址认证、口令认证、访问控制卡和指纹验证设备。
- 审计能力——产品监控网络传输——包括未经授权的访问企图——以生成日志，并提供统计报告与报警能力。

至于实施特性，要看产品符合网络管理要求的能力。好的防火墙产品必须具备：