Novell NetWare 5 系列书

BorderManager 企业版

将您的业务安全地扩展到因特网

Novell BordManager 使用指南

〔美〕Novell公司 著
希望图书创作室 译

本书配套光盘内容包括

Novell BorderManager 企业版3.0

60天试用软件

北京希望电脑公司
北京希望电子出版社
WWW.bhp.com.cn

Novell NetWare 5 系列书

将您的业务安全地扩展到因特网

Novell BorderManager 使用指南

BorderManager 企业版

[美] Novell 公司 著

希望图书创作室 译

本书配套光盘内容包括：

Novell BorderManager 企业版 3.0 60 天试用软件

北京希望电脑公司

北京希望电子出版社

1 9 9 9

内 容 简 介

BorderManager 企业版是针对企业因特网业务的一个完整的安全管理解决方案，它不仅强化了 Novell 目录服务（NDS）的功能，而且它所具有的许多业界领先的性能区别于其他厂商的产品。本指南的编写目的就是希望帮助那些使用人员尽快了解和掌握 BorderManager 的先进特性，并体验其独特的功能所带来的乐趣。

本指南共分为四个章节。第 1 章首先对类似 BorderManager 这样的产品在市场需求状况进行讨论，并概要地介绍了 BorderManager 解决方案；第 2 章重点介绍 BorderManager 各主要部件的特点，包括防火墙服务、虚拟专用网络服务、代理缓存服务，以及基于策略的管理、验证、报警、登录和报告等功能；第 3 章通过七个典型示例具体介绍了 BorderManager 所具备的灵活性，每个示例反映了 BorderManager 的一个的侧面；第 4 章则对 BorderManager 的安装和设置步骤进行了详细的说明。

本书配套光盘内容包括：Novell BorderManager 企业版 3.0 60 天试用软件。

本书适合所有已经建立和正在建立局域网环境的政府机关、企事业单位、大专院校师生、科研技术人员及网络工作者使用，也适合作为 NetWare 网络管理员的培训教材。

系 列 书：	Novell NetWare 5 系列书
书 名：	**Novell BorderManager 使用指南**
总 策 划：	希望图书创作室
文本著作者：	Novell 公司
CD 制作者：	Novell 公司
CD 测试者：	希望多媒体测试部
责任编辑：	龙启铭
出版、发行者：	北京希望电脑公司　　北京希望电子出版社
地 址：	北京海淀路 82 号　100080
	网址：www.bhp.com.cn
	E-mail: lwm.hope.com.cn
	电话：010-62562329,62541992,62637101,62637102（图书发行，技术支持）
	010-62633308,62633309（多媒体发行，技术支持）
	010-62613322-215（门市）
	010-62531267（编辑部）
经 销：	各地新华书店、软件连锁店
排 版：	希望图书输出中心
CD 生产者：	文录激光科技有限公司
文本印刷者：	北京双青印刷厂
规格 / 开本：	787×1092 毫米　16 开本　5.625 印张　126 千字
版次 / 印次：	1999 年 4 月第 1 版　1999 年 4 月第 1 次印刷
印 数：	0001-5000 册
本 版 号：	新出音管[1998]109 号　ISBN 7-980019-60-1/TP・27
定 价：	40.00 元（1CD）

目　录

第1章 概 述

1.1 安全服务集成解决方案的需求分析

媒体的鼓吹和咨询人员的煽动使众多的企业一窝蜂地进入了因特网（Internet），他们不仅将企业网络接入因特网，并且还在企业网络中采用了诸如 Web 和 FTP 服务器等因特网络技术，建立了内联网（Intranet）。这的确给企业带来了不少的好处。因特网加强了与客户的沟通，外联网（extranet）密切了与业务合作伙伴的关系，而内部的 Web 服务器使雇员间的关系更加紧密。另外，许多企业还将因特网作为廉价的广域网（WAN）链接手段，通过虚拟专用网络（VPN）技术实现了其局域网的互联。

但企业在实现与因特网联接，以及采用内联网和外联网之前，必须解决一个关键问题，这就是网络的安全性。因特网所存在的安全问题是众所周知的，将企业网络与因特网集成，无疑是将企业网络暴露在了外部入侵者的面前。为了提供对企业网络的保护，许多厂商都提供了防火墙产品，以便在因特网和企业网络之间建立一种保护壁垒。

除此以外，在安全方面还存在着比因特网黑客更加微妙，也更难对付的问题。那些在企业网络中采用了诸如因特网 Web 服务器等因特网网络技术的公司，实际上等于将存储在服务器上的信息完全暴露在来自企业内部的入侵者面前。对于这种情况，因特网的防火墙是绝对无能为力的，因为这些入侵者已经在防火墙里面了。而且这些内部的入侵者知道资源的存放位置，并有机会接近内部的桌面系统，这就使问题变得更为严重。而令人恼火的是，据国际计算机安全协会（ICSA）统计，在所有发生的侵入事件中，有 80%是来自防火墙内部。尽管大多数的 Web 服务器都提供有自己的安全机制，诸如口令保护等，但这些机制往往十分脆弱，非常容易被突破。

因此，除了防火墙之外，企业还应该具备内部的隔离措施，以便对内联网实行分段保护。（如果我们仔细琢磨一下，就会发现我们所使用的“防火墙”一词十分有意思。它的原本意思是一种置于建筑物墙体内部的物理屏障，诸如钢门等，其作用是阻止建筑物内部火焰的向外扩散。）

与安全问题紧密相关的另一个问题是性能问题。防火墙的过滤作用延缓了信息通过它的速度，这就如同液体在经过过滤器时会降低流速一样。而实际上，防火墙的作用越严密，它所带来的延迟作用也就越大。这就迫使企业不得不在安全和性能之间做出折衷选择。针对这一问题，软件厂商也采取了诸如代理缓存（proxy caches）等多种性能强化手段，以减缓防火墙对性能的影响。

另外，软件厂商还提供有 VPN（虚拟专用网络），这种 VPN 具有各种网络拓扑形式，企业可以通过它们将不同地点的网络链接起来，构成企业内联网（Intranet），远程用户也可以通过因特网来访问内联网。企业还可以通过外联网（extranet）与他们的业务伙伴链接在一起。所有这些拓扑结构都是采用因特网作为廉价的链接手段。但是，由于因特网上的信息通信极易被人窃听或篡改，因此，信息的加密和确保其传输过程中的不被篡改就成为 VPN 网络保证数据保密性和完整性的主要手段。

企业与因特网络连接所带来的另一个问题是一些职员可能会在网上从事一些与工作无关活动，如在网上冲浪等，这不仅浪费时间，影响职工的生产效率，而且也无谓地增加了网络的负荷。更为严重的是，有些公司还由于从 Web 站点下载非法材料，并显示在工作场所而受到揭露和指控。所以，对于企业来讲，如何控制对因特网的外部访问也是一个非常重要的问题。为此，软件供应商提供有内容过滤器，以控制职员对某些因特网络站点的访问。

总之，为了解决由于因特网技术的采用所带来的安全和性能的问题，软件厂商们都做出了很大的努力，并提供了各种产品，包括因特网防火墙、性能加速器、VPN、以及因特网 Web 目标内容过滤器（Internet Web destination content filters）等。但这里的问题是，网络用户如果想要构成一个完整的解决方案，就必须自己将这些不同厂商的产品拼凑在一起。而这种由不同产品组成的系统的管理不仅复杂，效率低下，而且极易发生错误。事实上，据 ICSA 的报告统计，在所有的防火墙侵入事件中，有 90%是由于设置不当所引起的。另外，对于网络管理员来讲，他们不得不为每个用户管理多个目录，而用户又不得不记住自己的各种 ID 标识和口令。更为糟糕的是，尽管这种解决方案在管理和使用上既费事，又费钱，但仍无法对来自内部的侵入提供强有力的保护。

因此，企业需要一种单一集成的可管理软件包，这种软件包可以提供整套的服务，包括外部侵入保护、内部侵入保护、性能加速、安全的 VPN 能力，以及对外部因特网络访问的全面控制等。

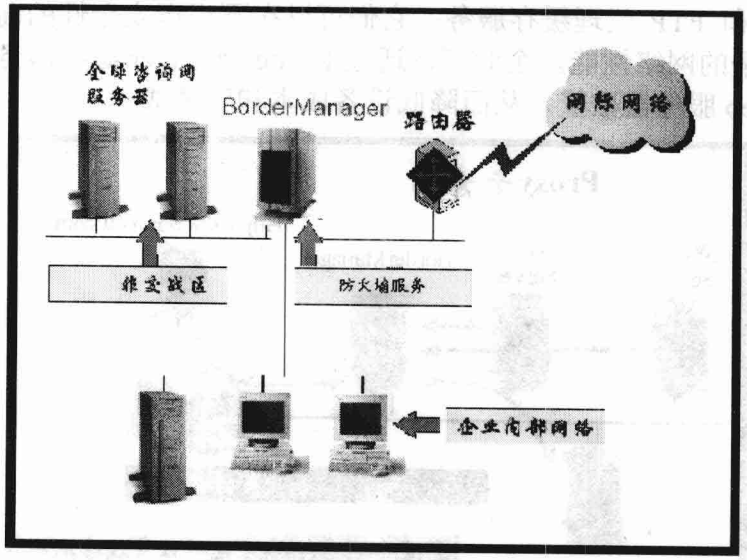
1.2 BorderManager 解决方案

Novell 的 BorderManager 正是满足了这种集成安全服务解决方案的需求，它充分利用了 Novell 目录服务(NDS)功能，是一种用于因特网络业务的完整的安全管理解决方案。通过 BorderManager，企业可以实现：

- 在充分利用因特网技术的同时保护企业信息免受内、外部的侵袭干扰。
- 用户不必再在安全和性能之间做出取舍，确保高性能。
- 通过集中的管理控制，降低网络的整体拥有成本。

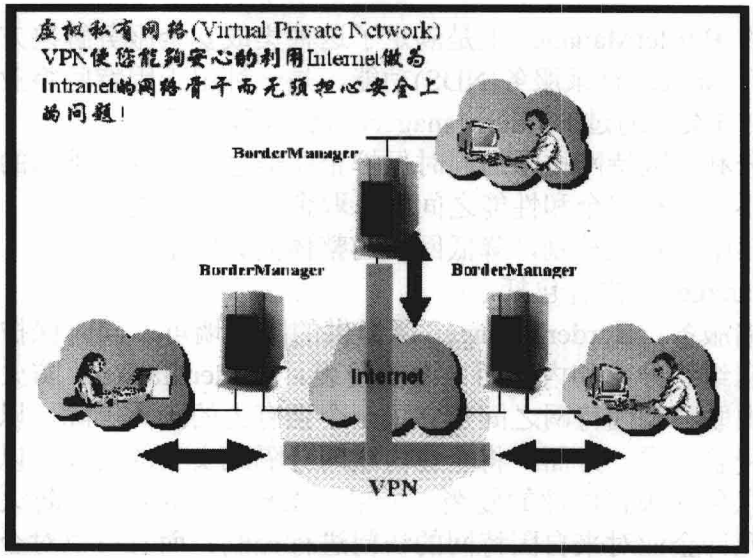
BorderManager 的内容包括：

- 防火墙服务：BorderManager 所提供的防火墙可以同时保护企业网络免受来自组织外部和内部两方面的侵袭。BorderManager 防火墙一方面在企业内联网和因特网之间建立了一个强有力的隔离屏障，以对付来自外部的侵袭；另一方面，将企业内联网分隔成安全的网段，以保护企业敏感信息免受来自内部的侵袭。所以，BorderManager 的防火墙服务不仅可以允许企业对来自因特网的访问进行控制，而且可以对企业内部的因特网访问进行控制。

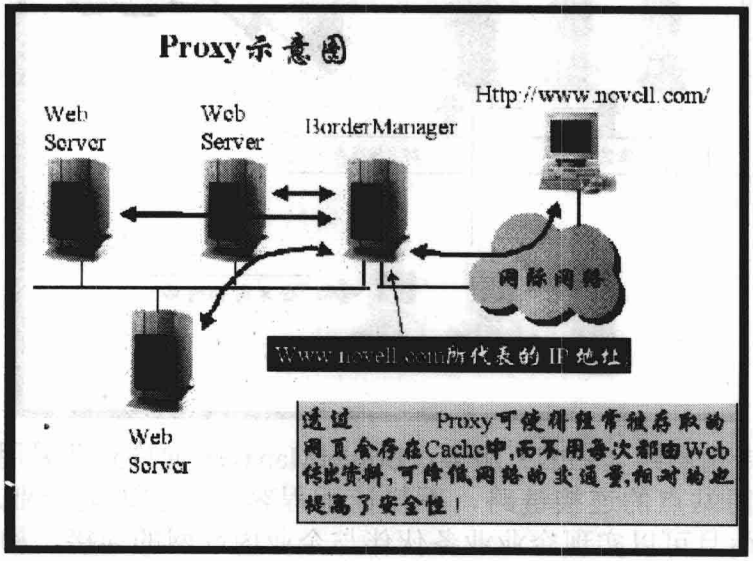


- 虚拟专用网络（VPN）服务：BorderManager 允许企业采用因特网作为其不同站点的连接链路，不仅让远程客户机实现对企业内联网的访问，而且可以实现企业业务伙伴与企业内联网的连接，构成企业外联

网（Extranet）。另外，因特网上的传输信息还可以采用加密手段来防止窃听者的非法访问，并通过对网上可能出现的破坏者的篡改进行监测检查来确保其信息的准确性。



- 代理缓存（Proxy Caching）服务： BorderManager 提供了强化性能的 Web 和 FTP 代理缓存服务，它们可以在不损害安全性的前提下，确保高水平的网络性能。企业可以通过 BorderManager 缓存服务来减少所需的 Web 服务器数量，从而降低设备成本和管理成本。



- 验证（Authentication）服务：BorderManager 验证服务（BMAS）将 RADIUS（远程验证拨入用户服务）协议的远程访问安全性与 NDS 的易用性及便利性结合在了一起，它允许远程用户通过因特网，通过单一口令的网络登录，就可以访问他们的所有网络资源，包括应用、文件、打印机、服务和其他网络资源等。

由于 BorderManager 是与 NDS 集成在一起的，网络管理员可以从一个集中点实现对整个网络的访问和安全控制。这样，他们就可以管理更多的资源，从而达到提高生产效率，降低管理成本的目的。另外，通过 NDS 进行安全管理，不仅具有良好的伸缩性，而且允许管理员通过某种可控的安全方式，将某些访问管理的职责予以下放。对于现有的 NDS 用户来说，与 NDS 的紧密集成也使 BorderManager 成为其 NDS 的一种自然延伸。

由于所有的用户身份验证都是通过 NDS 进行处理的，管理员无需再对分布在各种不同产品和目录中的大量访问控制信息和安全信息进行管理，这既减少了出错的风险，也确保了高水平的安全性能。另外，用户也可以通过对 NDS 的单一登录，实现对其授权的所有网络资源的访问，而不管他们进入网络时所处的位置或资源所在的位置如何。他们可以从任何地点，通过直接连接的 LAN 工作站，拨号连接的 LAN 工作站，或是因特网连接的远程 VPN 客户机进行登录。单一登录也就意味着用户只需记住一个口令，从而使他们能够很快地获得其所需的资源，最大限度地提高他们的生产效率。

基于 NDS 的验证要比传统的 TCP/IP 安全机制安全得多。TCP/IP 的安全性之所以比较弱，主要它是基于 IP 地址或网段的，而不是基于用户本身。例如，如果某个职员的工作站不具备对某种特殊资源的访问权限，他只要到另一个具有该访问权限的职员的工作站上去就可以了。而动态主机控制协议（DHCP）的情况就更糟，因为它的每个用户的机器地址是动态变化的，这使得这种基于标识的管理根本无法实现。而带有 NDS 的 BorderManager，它所提供的安全性是以用户为中心的，而不是以机器或 IP 网段为中心。这使得管理员可以同时依据资源标识和用户标识来建立网络的安全管理。当某个用户进行登录时，系统是根据用户标识和访问授权来确定接受或拒绝其网络资源的访问的，而与用户正在用来进行登录的工作站标识无关。

BorderManager 是运行在 NetWare 5 环境下的，这是首屈一指的因特网业务网络。为了提供一个完整的解决方案，在 BorderManager 中包含了 NetWare 5，并且不增加任何额外费用。二者均可以得到 Novell 公司遍布世界范围的 500,000 多名专业培训与技术支持人员的支持。

第 2 章　BorderManager 特色

2.1　BorderManager 防火墙服务

为了确保可靠的保护，BorderManager 在开放标准互联（OSI）模型的所有层面上均实现有访问控制部件，每个高层部件都对低层部件提供额外的安全保护。通过这些部件的集成和配合，可以提供一个安全的环境。从最高层到最低层，这些部件依次为：

- 应用代理（Application proxy）：BorderManager 包含有许多应用代理，诸如 HTTP、FTP、Gopher、Mail（电子信函）、News（新闻组）、Real Audio/Video（现实音频/视频）和 DNS 等。另外，BorderManager 还包括一个 TCP 类代理和 UDP 类代理，它们允许管理员进行诸如 LDAP 等附加应用代理的设置。应用代理负责实现用户应用与因特网/内联网之间的所有数据的中继处理。它们首先对 OSI 模型的第 7 层，也就是应用层的信息进行分析。这种分析不仅涉及数据包的地址，而且涉及数据包发送过程中的整个会话内容，并在数据中继转发之前，施加基于内容的语义访问控制。

应用代理提供了一种高级保护特性，强化了线路网关和数据包过滤器的保护功能。例如，一旦某个线路网关在客户机和远程主机之间建立了虚拟管道，则任何应用都可以在该连接上运行。但有了应用代理之后，它们可以依照应用，甚至应用中所使用的命令类型来对该管道上的会话进行限制。

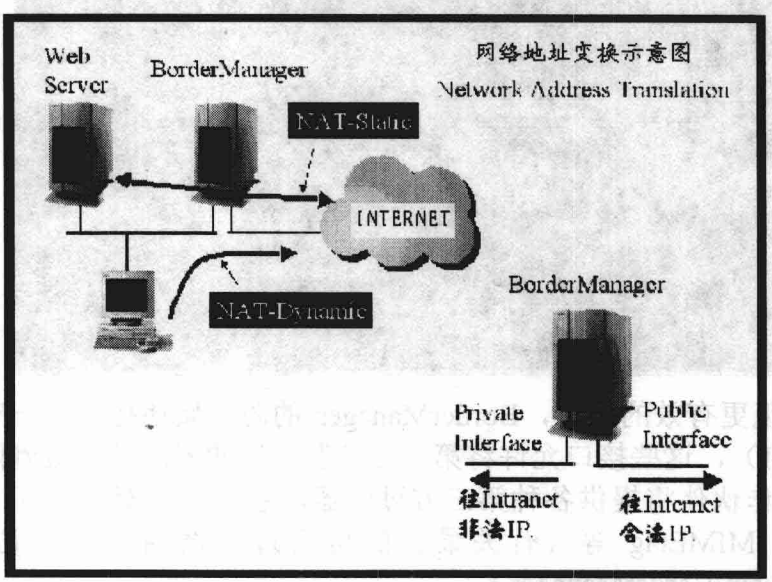
HTTP 应用代理可以支持 SSL（Secure Sockets Layer）层的隧道技术，允许在客户机和服务器之间建立一条加密通道，以保护信息免受窃听和篡改的威胁。

- 线路网关：BorderManager 提供有两个线路网关，SOCKS 网关和 Novell IP 网关。SOCKS 网关包括 SOCKS 客户机和服务器的 v4 和 v5 协议。通过对 SOCKS 的支持，可以将 BorderManager 防火墙设置成一个防火墙解决方案的部件，并可以与其他厂商的防火墙产品一道工作。BorderManager 可以用于现有防火墙的前端、中间或后端。而通过对 SOCKS 服务器的支持，可以允许 BorderManager 服务器与通用

SOCKS 客户机一道工作，为跨平台的客户机提供强有力的支持。带 SSL 的 SOCKS 为 NT、UNIX 和 NetWare 客户机提供了 VPN 的能力。

Novell IP 网关同时包括 IPX(tm) /IP 网关和 IP/IP 网关，它们提供了对 BorderManager 的透明验证功能。Novell IP 网关同时允许 IPX 和 IP 客户机对 TCP/IP 服务的访问。当某个 IPX 或 IP 客户机通过位于防火墙内（或外）的主机请求 TCP/IP 服务(诸如 HTTP、FTP、Telnet 或 Gopher 等)时，则相应的线路网关将首先负责对该请求的解释处理，然后再通过咨询 NDS 来确认该用户所具有的启动该会话的授权。访问控制可以按照协议和主机地址/域名对会话加以限制。位于 OSI 信息模型第 5 层的线路网关可以对数据包的信息进行分析，这比单纯的数据包过滤解决方案具有更高的保护能力。Novell IP 网关采用的是本地的 MS Winsock 2.0。

- 网络地址变换（Network Address Translation）：BorderManager 同时提供有动态和静态的 IP 及 IPX 网络地址变换（NAT）表。这些变换表是管理员通过公共 IP 地址集的设置构成的。BorderManager 利用这些表对目标为防火墙以外的数据包的源地址进行自动重新映射。这种地址变换是在 OSI 模型的第 3 层进行的，它对外隐藏了内部的网络地址，因而具有很强的安全性。另外，这种地址变换可以自动动态地实现未注册内部地址到注册的 IP 地址的映射，从而使管理员可以从既费时，又易出错的 IP 地址管理工作中解放出来。对于每一个接口，变换表可以并行完成 5,000 个未注册地址的映射处理。



- 数据包过滤器: BorderManager 的数据包过滤器运行在 OSI 模型的第 3 层，它可以按照访问控制要求对每一个数据包进行检查。过滤器通过对源及目标主机 IP 地址的检查来限制来自（或去向）某些 IP 主机的访问；通过对源及目标 IPX 地址的检查来限制来自（或去向）某些 IPX 主机的访问；通过对 IP 协议/端口的检查来限制对某些因特网协议和端口（诸如 HTTP、 FTP、telnet、和 Gopher 等）的访问；通过对 IPX 协议的检查来限制对某些类型的 NetWare 核心协议(NCP) 的请求访问。

BorderManager 先进的数据包过滤器引擎不仅查看数据包的地址，而且对数据包发送过程中的整个会话内容进行检查，这使得它在识别可疑数据包方面具有更高的效率。例如，对于黑客来讲，他可以很容易地利用地址骗术来骗过地址过滤器。但想要单独依靠这种手段来骗过 BorderManager 的数据包过滤器就不那么容易了。黑客还必须能够确定该数据包在发送过程中的整个会话内容，这即便不是不可能，也将是一项非常艰巨的任务。

为了实现更有效的保护，BorderManager 的防火墙还提供了一整套应用编程接口（API），这些接口允许将第三方开发的过滤器产品集成到防火墙中。Novell 的合作伙伴将提供各种第三方过滤器，包括抗病毒、Java、ActiveX、reporting 和 MIMEtag 等（有关最新的可用过滤器清单，请访问网址：www.novell.com/BorderManager.）。

另外，BorderManager 还包括一个 CyberPatrol 目标内容过滤器的测试版软件，它可以根据内容来拒绝对某些外部因特网 Web 站点的访问，例如拒绝对含有色情内容的站点的访问。对于传统的防火墙，特别是数据包过滤器来讲，它们的一个主要问题就是尽管它们可以提供严密的安全保护手段，但是，它们的设定往往非常复杂和困难。管理员们常常因此而产生防火墙的设定错误，从而造成安全上的漏洞。

BorderManager 对防火墙的设定进行了简化，这使得管理员的设定步骤变得非常简单：

1. BorderManager 防火墙自动进行初始化，使经过防火墙的两个方向都没有信号通过；

2. 然后由管理员通过 BorderManager 设置窗口对线路网关和应用代理进行设置；

3. 转到 BorderManager 规则（Rules）窗口，为线路网关和所选择的应用代理创建易于理解的高级访问规则。随后，BorderManager 利用这些规则信息自动进行数据包过滤器的设置。这就大大简化防火墙的设定过程，也堵住了这一最为常见的安全隐患。

2.2　BorderManager VPN 服务

BorderManager 的 VPN 服务可以让企业组织在因特网上安全经济地运行自己的专用网络。BorderManager VPN 可以实现三种类型的虚拟专用网络：

- 站到站（site to site）：企业可以利用因特网作为连接链路，实现两个以上站点服务器的互连。通过这种方法，可以将各个独立的 LAN 网段紧密地结合成为单一的 WAN 网络。
- 客户机/服务器：企业可以让运行 IP 或 IPX 协议的 LAN 用户、拨号用户、甚至有线调制解调器（modem）用户，通过因特网的安全连接来访问 VPN 资源。通过这种方法，企业可以让用户随时安全地访问其所需的网络资源，而不管用户所处的位置或资源所在位置如何。另外，它还有一个好处，这也是 BorderManager 所特有的好处，就是用户可以从任何地方，通过单一的登录，实现对所有资源的访问。
- 外联网（Extranet）：企业可以通过采用因特网作为连接手段，将它的企业网络与合作伙伴的网络连接在一起，构成一个紧密的外联网。

当实现一个 VPN 网络时，一个最重要的问题就是要确保只有授权的 VPN 成员才允许使用该网络。其次，就是要防止在 VPN 网络上传输的所有信息的

窃听和篡改，也就是说，要确保信息的保密性和一致性。为了确保只允许授权的 VPN 成员使用 VPN 网络，BorderManager 通过 NDS 对所有用户的身份进行验证。另外，在确保传输信息的保密性和一致性上，BorderManager VPN 采用了基于开放标准和加密技术的安全手段，诸如 IP SEC、RC2、RC5、DES、3DES 和 SKIP 等。

网络的性能和伸缩性也是十分重要的，尤其是对大型企业来讲。BorderManager VPN 可以支持对称多处理（SMP）技术，允许利用多处理硬件来提高处理的速度。为了进一步优化性能，BorderManager 还可以有选择地进行加密处理，即它可以按照管理员的指定要求，只对发往（或来自于）受保护网络的信息进行加密处理。另外，BorderManager 还采用了降低信号传输量的技术，诸如报头压缩和高效的 WAN 网络路由更新等，以提高 VPN 网络带宽。BorderManager 的每个通道可以支持多达 256 个站点连接，而每个服务器可以为 1,000 个拨号用户提供服务。

BorderManager 可以支持各种标准的通道、加密以及密钥交换技术，从而提供了一个强大灵活的安全框架。BorderManager 所支持的通道技术是基于成熟的 IP 中继机制，它采用 IP SEC 标准(RFC # 1825-1828)。BorderManager 支持的加密算法包括 RC2、 RC5、 DES 和 3DES。另外，BorderManager 还支持 SKIP（简化因特网密钥交换协议）标准，允许授权密钥在网上的安全分发。

同其他的 BorderManager 服务一样，BorderManager VPN 服务也是通过 NDS 进行管理的，这使得管理员可以通过单一的集中点实现对单个 VPN，甚至多个 VPN 的管理，从而大大降低管理成本。

2.3 BorderManager 缓存服务

当企业将他们众多分散的内部 LAN 网络连到一起，并将最终的全局网络与因特网实现集成后，他们所面临的一个主要问题就是网络性能的下降。而造成这种性能下降的一个主要原因是用于 LAN 网段互连的 WAN 链路的带宽过低。另一个原因是所有的信息都必须经过一个或多个安全防火墙，这也延缓了信息的传输速度。而 BorderManager 缓存服务可以在不牺牲安全性的前提下，创建一个具有高性能的全局企业网络。由于 BorderManager 缓存服务支持开放的因特网标准，因此，它们可以在一个多元和多厂商的环境下，与 Novell 的内联网及因特网产品一起使用，包括任何形式的浏览器和 Web 服务器。

BorderManager 缓存服务是基于因特网缓存协议（ICP）的，这是下一代 Harvest/Squid 代理缓存的研究成果，也是与第一代 CERN 代理缓存技术完全兼

容的。这种先进的技术可以在支持 HTTP、FTP、SSL 和 Gopher 协议的标准开放环境下提供超级的网络性能。另外，Novell 还针对 NetWare 平台对该项技术进行了优化，而 NetWare 本身也是经过对该网络环境的优化的。因此，它的性能远远超过应用服务器、通用操作系统（如 NT 和 Unix 等）的性能。BorderManager 缓存服务可以处理 100,000 个并行连接，其每秒的连接数量超过 6,000 个。根据 SPECWEB 96 的测定，BorderManager 缓存的每秒操作次数超过 2,2000，是目前处理速度最快，也是最具伸缩性的缓存解决方案。

BorderManager 缓存服务采用了先进的代理缓存技术，它可以使企业网络性能提高十倍。通过将数据缓存在基于 LAN 的代理上，BorderManager 缓存服务可以大大减少整个 WAN 网上的通信信号量，其典型数据可以达到 60%。这就意味着，企业在相同的物理 WAN 网络连接下，其网络的吞吐率可以达到原来的 2.5 倍。因此，也就无需再去购买昂贵的宽带 WAN 网络连接产品。

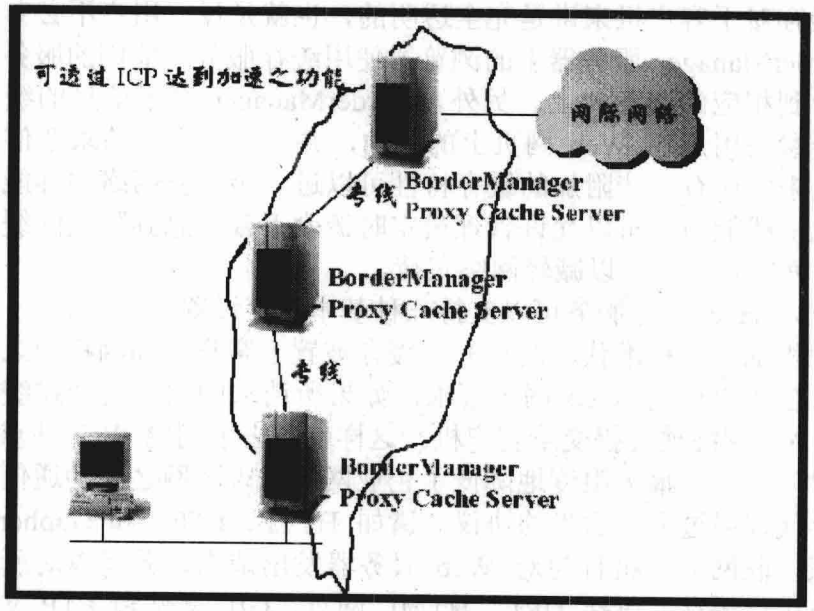
代理缓存对于客户机来讲是完全透明的，也就是说，用户不必专门去指定他们在 BorderManager 服务器上的浏览器使用缓存服务。他们的服务请求会被自动地引导到相应的服务器上。另外，BorderManager 对于信息的缓存是主动的，即它会参与用户在 Web 网页上的移动，并在用户实际请求新信息之前将它们缓存起来。还有一些附加的缓存特性可以进一步改善网络的性能。例如，它有一种批下载能力，可以允许管理员定时调度下载信息到附近的缓存中，譬如在下班时间进行下载，以减轻网络负荷。

BorderManager 缓存服务可以支持三种基本缓存设置：

- 客户机加速（标准代理缓存）：缓存被置于客户机和因特网之间，它接受来自客户机的 Web 网页请求，如果所请求的网页已经在缓存中，则以 LAN 网络速度提交给客户机。这样就省去了到原 Web 站点提取信息的时间延迟，最大限度地降低了企业网络与因特网之间的通信信号量。缓存代理通过采用适当的协议（诸如 HTTP、FTP、和 Gopher），可以按照内联网客户机行为对 Web 服务器发出请求，并可以对所有因特网对象进行缓存，包括 URL、HTML 网页、GIF 文件和 FTP 文件，以加速这些对象的后续请求的处理速度。
- Web/FTP 服务器加速（异向代理缓存）：BorderManager 服务器位于一台或多台 Web 或 FTP 服务器的前端，并对所有属于这些服务器的静态信息进行缓存。当某台客户机向 Web 或 FTP 服务器请求信息时，该请求会被转移到 BorderManager 代理上，则代理可以高速向客户机提供其缓存的网页。缓存代理通过这种运行方式可以大大加快网页的访问速度。另外，它也降低了 Web 和 FTP 服务器的请求负荷，使网络可以用

较少的服务器服务更多的用户。BorderManager 缓存服务可以对所有厂商的 Web 和 FTP 服务器提供加速服务，并且与这些服务器的组合形式无关。

- 网络加速（ICP 分层缓存）：在这种设置下，多个 BorderManager 服务器被设置成分层的（网状）拓扑结构。当客户机所请求的信息没有在代理缓存时，代理缓存会与网络中的其他服务器进行联系，确定是否有哪台服务器缓存了所请求的信息。如果有的话，那么，位于最近的那台拥有所需信息的代理缓存会将信息转发给发出请求的代理缓存，再后者再转发给提出请求的客户机。ICP 分层缓存大大减少了 WAN 网上的通信信号量，并释放了宝贵的网络带宽。另外，由于所请求的信息都是从最近的 BorderManager 服务器送出的，这就使网络延迟降到了最小，从而节省了用户时间，提高了用户的生产效率。



2.4 基于策略的管理

所有的 BorderManager 服务都是由管理员通过 NDS 进行管理的，他们通过存储在 NDS 中的访问控制表（ACL）规则对访问进行控制。这些策略规则既可以应用于网络资源（诸如机器等），也可以应用于用户和工作组。这种控制十分灵活，可以按照各种协议、站点（URL）、类别（诸如色情和暴力）和

每天的时间组织限制条件。另外，由于管理员所管理的都是一些易于跟踪的高级规则，并且不需要分服务进行管理，所以，使管理工作也变得十分简单。

访问控制规则是分布在 NDS 中的，它们分别与每个用户或工作组构成关联关系，而不是与机器相关联。因此，当雇员在网络中移动时，他们是“带着访问控制一起走的”。不管他们从哪里进入网络，他们都可以在相同的访问控制规则下进行操作。另外，访问规则还可以自动地在整个网络的 NDS 中进行复制，以提供高级的容错能力。

管理员在建立规则时，既可以针对每个 NDS 对象，也可以针对 NDS 容器。这些规则按照 NDS 的限制具有继承性，所以，有效的规则集合是由针对各种 NDS 对象所建立的规则的组合。规则在表中的位置决定了其应用相对于其他规则的优先级。如果某个低优先级（在表的较低位置）的规则与某个高优先级（在表的较高位置）的规则发生冲突，则高优先级的规则优先。

位于规则表顶部的规则是在访问请求所经过的 BorderManager 服务器上定义的规则，这些规则的下面是用于 BorderManager 服务器容器的规则集。从这里开始，直到 NDS 树的根部，都是按照优先级进行工作的。在每个表的底部都有一个隐含的规则，该规则可以拒绝一切访问操作，并且不允许对其进行删除或修改。

管理员可以对规则进行增加、删除、剪切、拷贝和粘贴操作。另外，也可以修改规则在表中的位置，以提高或降低它的优先级。

2.5　用户身份验证

用户可以通过下列四种方法对 BorderManager 提供验证：

- Novell IP 网关：用户可以利用 Novell IP 网关客户机进行网络登录，提供对 NDS 的后台验证。
- Web 浏览器：用户可以通过任何 Web 浏览器进行网络登录。在这种情况下，当用户试图访问保护资源时，BorderManager 将产生一个 HTML 或 Java 登录画面（登录是通过一条 SSL 安全链路进行的）。
- VPN 客户机：用户可以通过 BorderManager 的 VPN 客户机进行网络登录。
- BorderManager 验证服务：用户可以从任何一台拨号客户机进行登录，并通过 BorderManager 验证服务所支持的 RADIUS 协议进入网络。

BorderManager 对所有用户的验证都是通过 NDS 进行的。因此，用户只要经过一次登录，就可以访问他们所授权的任何网络资源，不管其所在位置如