

# Novell BorderManager 3.7

## Controlling Access Inside and Out

by Cheryl Walton



**A**s a network administrator, you are undoubtedly—perhaps even painfully—aware that the first and most important step of securing your company's network is controlling access to that network. In fact, an unidentified respondent to *Information Security Magazine's* fourth annual Industry Survey asserts that if your company's network is connected to the Internet, *security* and *controlled access* are virtually synonymous terms.

The results of this survey (to which more than 2,500 security officers, managers, consultants, engineers, and administrators responded) probably offer few surprises. For example, you probably aren't surprised that more than half of the respondents reported internal users had, within the past year, used network resources for illegal or illicit purposes.

Sixty-three percent of respondents reported offenses such as pornography, surfing, and e-mail harassment, and 60 percent of respondents reported abuses such as gambling, spamming, managing personal e-commerce sites, and online investing. Given the so-called success of viruses such as Melissa and, more recently, CodeRed and Nimda, you are probably not surprised that nearly 90 percent of respondents experienced attacks that originated outside their company's network.

In other words, this survey affirms what you—a seasoned IT professional—already know about network security: You need to control access to network resources for users inside and outside your company's firewall. (For more information about this survey, see "2001 Industry Survey," *Information Security Magazine*, Oct. 2001. You can download this article from [www.infosecuritymag.com/articles/october01/images/survey.pdf](http://www.infosecuritymag.com/articles/october01/images/survey.pdf).)

Novell BorderManager can help you secure your company's network. With an installed base of more than 5.2 million users, Novell BorderManager is one of the top firewall and virtual private network (VPN) products on the market. In fact, a recent IDC bulletin, "Who's the Lord of the Rings? Worldwide Firewall/VPN Software Market Forecast and Analysis, 2001-2005," ranks Novell BorderManager number five in a field of 20 Firewall and VPN products. (IDC provides IT industry and market analysis and IT consulting services. For more information about IDC, visit [www.idc.com](http://www.idc.com).)

Novell BorderManager 3.7, the latest version of Novell BorderManager, will be available this month as a standalone

product and as part of Novell Secure Access, Novell's new suite of access management and security products. (For information about Novell BorderManager availability and licensing, see "Come and Get It" on p. 14.) All of the products included in Novell Secure Access are directory-based and each is designed to help you simplify access management and eliminate one or more specific security vulnerabilities. (For more information about Novell Secure Access, visit [www.novell.com/products/secureaccess](http://www.novell.com/products/secureaccess).)

### THE DIRECTORY HAS IT

One particularly effective way to control network access is to use a directory. Directories enable flexible access control that hardware-based access control devices simply can't offer. Of course, Novell eDirectory arguably offers you more flexibility than any other directory on the market today. eDirectory enables you to control access for a virtually unlimited number of users, enabling you to securely extend your company's network resources to the Internet. In addition, eDirectory simplifies access management because you can manage access through the directory rather than through each individual resource.

Because eDirectory runs on multiple platforms, it can control access to resources running on your company's NetWare, Linux, Solaris, and Windows servers. eDirectory is also extensible, so you can include an almost unlimited variety of information in eDirectory objects and can then base access to resources on that information.

Not surprisingly, eDirectory provides the foundation for all of the products in Novell Secure Access, including, of course, Novell BorderManager. Using eDirectory's access management capabilities, Novell BorderManager 3.7 provides the following services:

- Proxy services to control and accelerate users' access to Internet content

- VPN services to enable external sites or individual users to securely access resources inside your company's firewall
- Firewall services to protect your company's network from external and internal attacks

### IT'S ONE NET—WHAT ELSE IS NEW?

Because Novell BorderManager is based on eDirectory, all versions of Novell BorderManager—including versions that predate Novell's one Net vision—are Net services software. That is, all versions of Novell BorderManager help you simplify, secure, and accelerate the process of extending your company's network to the Internet.

Novell BorderManager 3.7 runs on NetWare 6 and 5.1 and includes several new features. The remainder of this article outlines some of these new features and explains how these new features can benefit your company. (For more information about previous versions of Novell BorderManager, see "Novell's Border Services," *Novell Connection*, May 1997, pp. 25–36 and "BorderManager 3.0: Patrolling the Borders of Your Network," *Novell Connection*, Oct. 1998, pp. 6–21. You can download these articles from [www.ncmag.com/past](http://www.ncmag.com/past).)

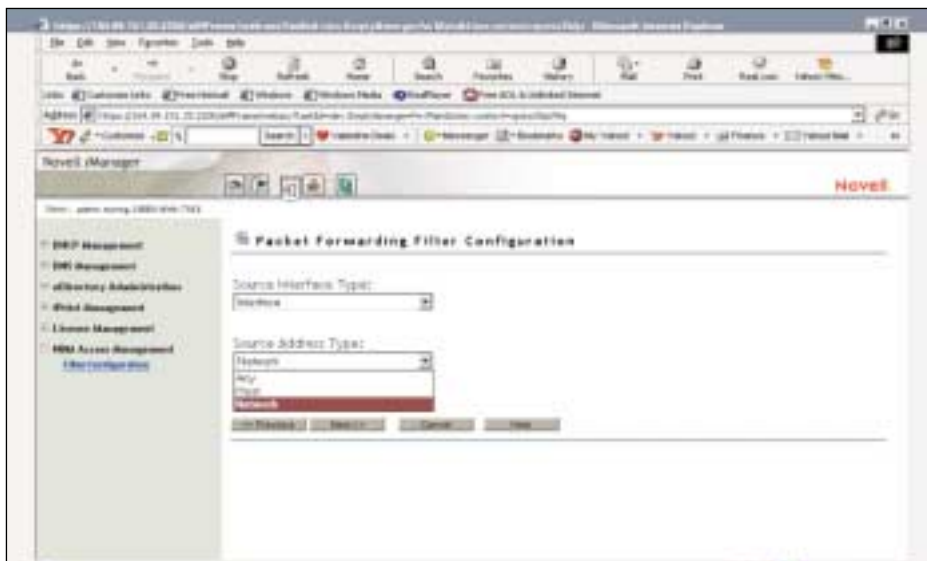
### CH-CH-CHANGES THAT SIMPLIFY INSTALLATION

To simplify the process of getting a Novell BorderManager 3.7 server up and running, the Novell BorderManager 3.7 installation program includes a few important changes. For example, before installing the BorderManager components, the Novell BorderManager 3.7 installation program detects whether or not the INETCFG utility has ever been loaded on the server on which you plan to install Novell BorderManager 3.7. (Whereas NetWare uses the AUTOEXEC.NCF file to manage internetworking configurations, such as the IP addresses of network servers, Novell BorderManager uses the INETCFG utility to manage this information.)

If the installation program detects that the INETCFG utility has never been loaded, it prompts you to exit the installation program and load the INETCFG utility. To load the INETCFG utility, you type the following command at the server console:

```
LOAD INETCFG
```

When you load the INETCFG utility,



**Figure 1.** Novell BorderManager 3.7 includes the Filter Configuration utility, a browser-based utility that includes a graphical user interface (GUI) that can simplify the filter configuration process for Novell BorderManager 3.7 firewall services on NetWare 6.

it creates startup files that define the internetworking configurations. The INETCFG utility asks you if you want to import these configuration settings from

the NetWare server's AUTOEXEC.NCF file; you should select Yes.

As Novell product manager Scott Jones explains, because previous versions

Visit our advertiser, Biscom, at  
[www.biscom.com](http://www.biscom.com).

## Come and Get It

When Novell BorderManager 3.7 ships later this month, you will be able to purchase Novell BorderManager 3.7 as either a separate product or as part of Novell Secure Access, Novell's new suite of access management and security products. (For more information about Novell Secure Access, visit [www.novell.com/products/secureaccess](http://www.novell.com/products/secureaccess).)

### ALONE

You can purchase Novell BorderManager 3.7 online through either shopNovell or through an online Novell reseller. Visit shopNovell—Novell's online store—at <http://shop.novell.com>. To view a list of online Novell resellers, visit [www.novell.com/partners/onlinesales](http://www.novell.com/partners/onlinesales).)

You can also purchase Novell BorderManager 3.7 through your local Novell channel partner or a Novell sales office. To purchase Novell BorderManager 3.7 directly from Novell, contact the Novell Customer Resource Center. (In the Americas, call 888-321-4272. Outside the Americas, please call your local Novell sales office.)

Pricing and licensing for Novell BorderManager 3.7 follows pricing and licensing for Novell BorderManager 3.6, with the following two exceptions:

1. Novell BorderManager 3.7 is not available with server-based pricing

and licensing. Instead, you need a license for every user who authenticates to Novell BorderManager 3.7. If users are accessing only Novell BorderManager services that don't require authentication-routing, network address translation (NAT), and packet filtering services, for example, these users don't require a license.

2. Novell BorderManager 3.7 is a single product that includes all of the BorderManager components that were previously sold separately.

Because Novell BorderManager 3.6 is included in Novell Small Business Suite 6, Novell plans to extend upgrade pricing to Novell Small Business Suite 6 customers. As you probably know, and as its name suggests, Novell Small Business Suite 6 is a suite of products for businesses that have 50 or fewer users. This suite includes NetWare 6, Novell BorderManager 3.6, and other Novell and third-party products.

### IN GOOD COMPANY

As mentioned above, Novell BorderManager 3.7 is one of the products included in Novell Secure Access. To purchase Novell Secure Access, contact your local Novell channel partner or a Novell consultant and system integrator partner.

For a limited time, you can purchase Novell Secure Access for \$159 per user (manufacturer's suggested retail price). ●

of the Novell BorderManager installation program do not prompt you to load the INETCFG utility (if you haven't previously done so), many Novell BorderManager customers simply don't. As a result, these customers invariably experience difficulties when they try to configure Novell BorderManager services.

In fact, if you have never loaded the INETCFG utility, you can't configure Novell BorderManager VPN services at all. Furthermore, configuring Novell BorderManager to use network address translation (NAT), static routing, modems, and adapters could pose significant—if not outright insurmountable—difficulties.

### Success Hinges on the Gateway

The Novell BorderManager 3.7 installation program also checks the GATEWAYS file in the server's SYS:\ETC

directory for the IP address of a default gateway. If the installation program does not find a default gateway, it prompts you to provide one.

**Note.** The NetWare 6 and 5.1 installation programs do not require you to provide a default gateway. Therefore, this gateway may not exist in your server's configuration.

Because the default gateway enables access to and from the Internet, all Novell BorderManager services use this gateway. For example, the HTTP forward proxy service forwards requests for Internet content to this gateway.

By prompting you to provide this information, the Novell BorderManager 3.7 installation program can save a considerable amount of your time and energy. For example, you may not realize that you need to provide a default gateway until

you discover that none of the Novell BorderManager services work and call Novell Support to find out why.

To then provide a default gateway after you install Novell BorderManager 3.7, you complete the following steps:

1. Load the INETCFG utility.
2. Select Protocols.
3. Select TCP/IP.
4. Enable LAN Static Routing and select Insert.
5. Select Default Route.
6. Enter the IP address of the default gateway.

### Manual Labor? Not Here

The Novell BorderManager 3.7 installation program also performs configuration tasks that, with previous versions of BorderManager, you must perform manually. For example, the installation program enables you to select any or all of the individual proxy services available in Novell BorderManager 3.7. (For a list of the proxy services available with BorderManager 3.7, see "Services by Proxy" on p. 17.)

When you select one or more of these proxy services, the installation program automatically enables the selected services. Assuming you have selected the option to secure the Novell BorderManager 3.7 server's public interfaces, the installation program then configures the minimum number of packet filter exceptions necessary to open the ports that these services use.

**Note.** By default, when you select the option to secure the server's public interfaces, the installation program blocks all traffic through these interfaces.

Using previous versions of Novell BorderManager, in contrast, you must use the Novell BorderManager snap-in module for the NetWare Administrator (NWADMIN) utility to manually enable each proxy service you want to use. You must then use the Novell BorderManager FILTCFG utility to manually configure filter exceptions for the ports these services use. (You can download a list of the ports NetWare 6 applications and services use from <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10065719.htm>.)

### Goodbye FILTCFG!

Even if you need to configure packet filters and filter exceptions after you have installed Novell BorderManager 3.7, you

may not need to use the FILTCFG utility. Novell BorderManager 3.7 includes the browser-based Filter Configuration utility, which snaps in to Novell iManager. Novell iManager is a NetWare 6 utility that enables you to manage objects in eDirectory using a TCP/IP connection and a standard web browser. (For more information about iManager, visit [www.novell.com/documentation/lg/nw6p/index.html?setupenu/data/acq86jm.html](http://www.novell.com/documentation/lg/nw6p/index.html?setupenu/data/acq86jm.html).)

The Filter Configuration utility has a point-and-click, plain-language interface that simplifies the task of managing Novell BorderManager 3.7 firewall services on NetWare 6. (See Figure 1 on p. 13.) In contrast, the Novell BorderManager FILTCFG utility has a text-based interface and uses the rather arcane language of various Internet Engineering Task Force (IETF) Request For Comments (RFC) documents that describe packet types. For example, HTTP packets are described in RFC 1945, and Simple Network Management Protocol (SNMP) packets are described in RFC 1067. (You can download these RFC documents from

[www.ietf.org/rfc/rfc1945](http://www.ietf.org/rfc/rfc1945) and [www.ietf.org/rfc/rfc1067](http://www.ietf.org/rfc/rfc1067) respectively.)

As Jones half-jokingly explains, the FILTCFG utility can be so difficult for packet-filtering novices to use that using it has been likened to a black art. Of course, if you are adept at using the FILTCFG utility and want to continue doing so, you can.

Suppose you have deployed a new Novell GroupWise e-mail system inside your company's Novell BorderManager 3.7 firewall and now want to enable users to access GroupWise WebAccess through that firewall. Further, suppose Novell BorderManager 3.7 is running on NetWare 6. To use the Novell BorderManager 3.7 snap-in for iManager, you launch a supported web browser. (iManager supports Microsoft Internet Explorer 5.5 and Netscape 6.1, 4.7, and 4.6. iManager supports Netscape 4.7 and 4.6 only in Simple mode, which has a less complex web interface than Regular mode does.) You then type one of the two following addresses in your browser's URL field, depending on the type of browser you are using:

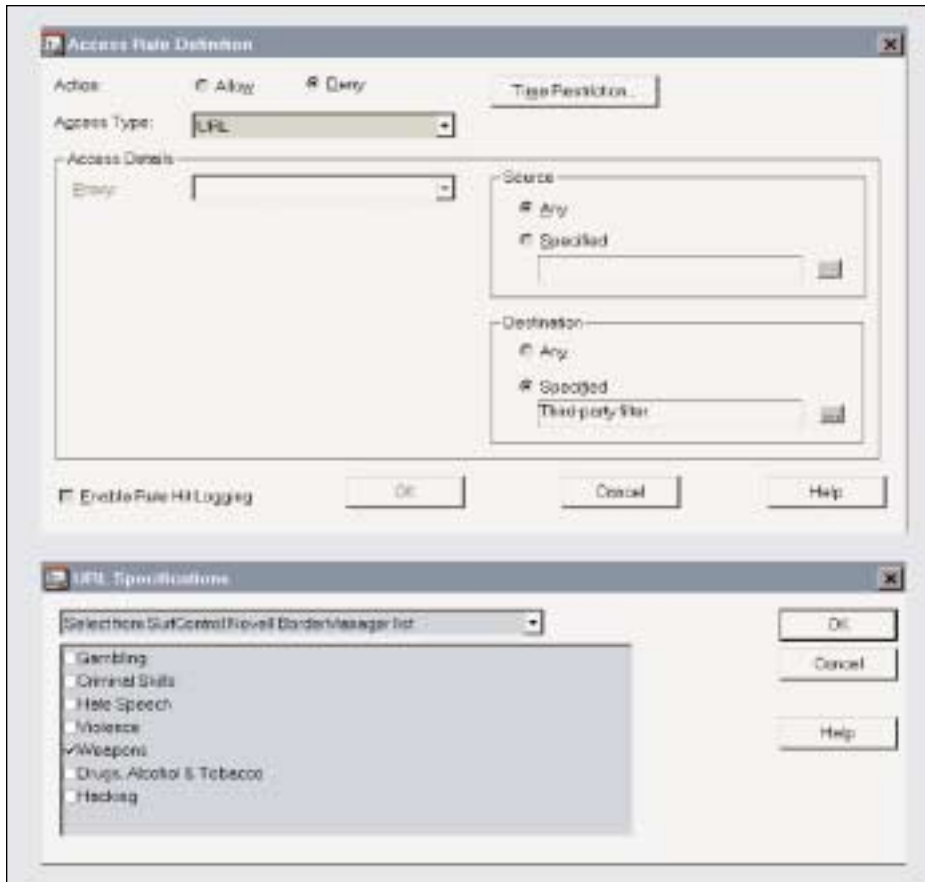
- <https://yourserverIPaddress:2200/eMFrame/iManage.html> (for Regular mode)
- <https://yourserverIPaddress:2200/eMFrame/Simple.html> (for Simple mode)

**Note.** Although you can enable Internet access to your company's Novell BorderManager 3.7 firewall through Novell iManager, doing so presents a considerable security risk. Therefore, Novell recommends that you enable access only from inside your company's network.

At the time this article was written, the user interface for the Novell BorderManager 3.7 Filter Configuration utility was in usability testing. Therefore, the exact procedure for enabling access to GroupWise WebAccess was not available. However, the following steps give you a general idea of how simple it will be to perform this task using the Filter Configuration utility:

1. From the iManager menu, select Filter Configuration, which is under the

Visit our advertiser, Laptop Career Certification,  
at [www.laptopCC.com](http://www.laptopCC.com).



**Figure 2.** Using the Novell BorderManager 3.7 snap-in module for NWADMIN, you can configure access rules that, among other things, allow or deny user access to specific Internet sites. You can also use this snap-in module to allow or deny user access to SurfControl content categories.

- NBM Access Management selection. (See Figure 1 on p. 13.)
2. Browse to select the server for which you want to configure access.
  3. Select Add from the summary table that lists all of the filters that are currently configured for this server.

The Filter Configuration utility walks you through the process of providing the information that Novell BorderManager 3.7 needs to enable a new service. For example, the Filter Configuration utility prompts you to specify the type of service you want to enable. GroupWise Web-Access requires two types of services: web services and secure web services. When you specify these services, the Filter Configuration utility configures the packet filter exceptions necessary to allow these services through your company's BorderManager 3.7 firewall. In other words, using this utility, you don't need a vocabulary that includes the names of specific packet types.

**The Good Book**

To further simplify the process of installing and configuring Novell BorderManager, Novell BorderManager 3.7 ships with a condensed edition of *The Beginner's Guide to BorderManager 3.x* by Craig Johnson. Although not a complete edition, the condensed edition does include comprehensive information about setting up the most popular Novell BorderManager services, such as Novell BorderManager forward proxy services and access rules. If you need more information than this condensed version provides, you can purchase the complete edition of *The Beginner's Guide to BorderManager 3.x* at [www.caledonia.net](http://www.caledonia.net).

**CONTROL FREAK? YOU'RE IN GOOD COMPANY!**

According to Jones, the majority of companies that purchase Novell BorderManager do so primarily for its HTTP proxy service, which in forward proxy mode enables you to control user access

to Internet content. Specifically, the HTTP forward proxy service enables you to control access based on the four Ws:

- Who
- What
- Where
- When

You can use the Novell BorderManager snap-in module for the NWADMIN utility to configure access rules and then associate these rules with functional roles—or groups of users whose network access requirements are the same. With Novell BorderManager 3.7, as with previous versions of Novell BorderManager, you configure access rules using the NWADMIN utility. However, later this year Novell plans to provide web-based management tools that snap in to Novell iManager as a free update for Novell BorderManager 3.7.

Using Novell BorderManager 3.7 access rules, you can specify the following. (See Figure 2.)

- The client computers from which users can access the Internet
- The protocols users can access over the Internet
- Specific URLs users can access
- The specific days and times these rules are in effect

For example, you can configure an access rule for your company's president that enables her to access all available Internet content from any workstation on your company's network at any time of day. (She is, after all, the boss.)

If you give every user on your company's network this same freewheeling access to Internet content, however, these users may spend time surfing the web when they ought to be working. Furthermore, the content these users may access (for example, MP3 or MPEG files) could seriously impact network bandwidth.

To prevent these potential problems, you can configure access rules that enable users to access only the specific job-related sites they need. Of course, such a draconian lockdown of Internet access may damage employee morale and may even prompt your company's most valuable workers to seek a more liberal work environment. These workers might resent not having the ability to download personal information on their own time—or

## Services by Proxy

Novell BorderManager 3.7 includes the following proxy services:

- HTTP Proxy. This forward proxy service requests content on behalf of users' browsers and stores this content in its cache. The HTTP Proxy service then delivers requested content from its cache to users' browsers.
- HTTP Accelerator. This reverse proxy service caches static content from your company's web server and delivers that content (on behalf of the web server) to users' browsers.
- FTP Proxy. On users' behalf, this forward proxy service requests and caches anonymous FTP content. It then delivers this content to requesting users.
- FTP Accelerator. This reverse proxy service caches your company's FTP content and delivers that content to requesting users.
- Mail Proxy. This service provides Simple Mail Transfer Protocol (SMTP) services for incoming and outgoing e-mail. (The Mail Proxy service does not cache mail.)
- News Proxy. This service requests Usenet content on behalf of internal users. The News Proxy also uses Network News

Transfer Protocol (NNTP) to provide forward and reverse proxy services for news articles. (This proxy service does not cache news articles.)

- Telnet proxy. This forward and reverse proxy service provides Telnet content to requesting users.
- Generic Proxy. This forward and reverse proxy service uses HTTP to tunnel protocols that are not included in other Novell BorderManager proxy services—rlogin, for example. The Generic Proxy service does not cache this content.
- DNS Proxy. The DNS Proxy service acts as a DNS server for client machines on your company's intranet.
- RealAudio and RealTime Streaming Protocol (RTSP) Proxies. These forward proxy services request RealAudio and RTSP content, respectively, on behalf of users' browsers.
- SOCKS Client. This service enables you to configure BorderManager proxy services as clients to a SOCKS server. (SOCKS is a protocol that proxy servers can use to receive requests from client machines inside a firewall and to then access requested resources outside the firewall without compromising the security of the requesting client machines.) You can configure the Novell IP gateway on a Novell BorderManager server to function as a SOCKS server, or you can configure Novell BorderManager as a client machine to a SOCKS server. ●

even on company time.

In a recent survey, 72 percent of workers who use the Internet at work for personal reasons at least once a day claim that this practice makes them happier, less stressed, and therefore better able to perform well on the job. Although this survey doesn't verify these workers' claims of increased productivity, it does demonstrate the positive impact that Internet access can have on workers. (See "Number of American Workers Online Increases," *CyberAtlas*, Aug. 2001. You can download this article from [http://cyberatlas.internet.com/big\\_picture/geographics/article/0,,5911\\_872091,00.html#table](http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_872091,00.html#table).)

To keep users happy, you can use the Novell BorderManager snap-in module for the NWADMIN utility to configure two sets of rules: one restricting Internet access during business hours and one enabling unrestricted access during lunch hour and before and after work.

Although this alternative doesn't guarantee that users will spend their working hours productively, it does eliminate the potential distraction of unlimited Internet access. This alternative can also help ensure that your company has the bandwidth it needs to conduct business during business hours.

This alternative doesn't solve a more serious problem: If the Internet content that users access—even on their own

time—is illegal or offensive, this content can have legal ramifications for your company. Novell BorderManager 3.7 enables you to configure rules that deny access to specific URLs, but with tens of millions of individual sites available, you can't possibly identify all of the potentially dangerous Internet sites and then configure rules to block those sites.

Fortunately, you don't even have to try. Novell BorderManager 3.7 includes content-filtering software from SurfControl. (According to an IDC report, "WorldWide Internet Access Control for 1999 & 2000," SurfControl is the market leader in Internet-filtering software. For more information about SurfControl, visit [www.surfcontrol.com](http://www.surfcontrol.com).)

This software enables you to control access to more than 60,000 sites, which are organized into the following seven categories:

- Criminal Skills
- Drugs, Alcohol & Tobacco
- Gambling
- Hacking
- Hate Speech
- Violence
- Weapons

The Novell BorderManager 3.7 installation program automatically copies the SurfControl software to the server's

SYS:\SURFCTRL directory. You can then install this software by running the setup program from that directory. Among other things, this setup program loads the SurfControl Content Database categories into eDirectory.

You can then use the Novell BorderManager 3.7 snap-in module for the NWADMIN utility to prevent or allow access to the URLs in none, one, or more of these seven categories. (See Figure 2 on p. 16.) For example, if your company is a security agency, you may want to allow access to the URLs in some of these categories—such as the Weapons and Criminal Skills category. If your company is a financial institution, on the other hand, you may want to prohibit users from accessing URLs in all seven categories.

The SurfControl Content Database that ships in the Novell BorderManager 3.7 box never expires. However, sites falling into these seven categories come online daily. In addition, you may want to prohibit access to sites in other categories. For example, suppose you are using a reporting tool such as the SurfControl reporting tool or WebTrends Firewall Suite by NetIQ to monitor Internet access through your company's BorderManager HTTP proxy server.

**Note.** The SurfControl reporting tool is included with SuperScout Web Filter

## Now You See It

As you probably know, you can configure Novell BorderManager 3.7 to generate log files for its HyperText Transfer Protocol (HTTP) proxy services. These log files contain a plethora of useful information. For example, these logs can tell you which users accessed the Internet through the Novell BorderManager HTTP proxy service, when, and what sites the users requested. (For more information about Novell BorderManager HTTP proxy service log files, see "Understanding Novell BorderManager's HTTP Proxy Logs," *Novell AppNotes*, Jan. 2002, pp. 27–37. You can download this article from <http://developer.novell.com/research>.)

However, when you enable logging for Novell BorderManager HTTP proxy service, this service logs every request it receives. Obviously, these log files can be very, very large. As a result, finding the particular information you need in these files can be daunting.

To make the data stored in Novell BorderManager log files truly accessible, you need reporting software that works with Novell BorderManager proxy services, such as WebTrends Firewall Suite from NetIQ. (NetIQ provides network infrastructure management and reporting software. For more information about NetIQ, visit [www.netiq.com](http://www.netiq.com).)

WebTrends Firewall Suite runs on Windows XP, 2000, and NT and works with Novell BorderManager 2.x and 3.0. (WebTrends Firewall Suite has not yet been tested with BorderManager 3.7. Because there are no major architectural changes in BorderManager 3.7, however, WebTrends Firewall Suite should run with this version.) To use WebTrends Firewall Suite with Novell BorderManager, you must make Novell BorderManager HTTP proxy service log files available to Web Trends Firewall Suite. You can make these log files available by performing any of the following tasks:

- You can map a drive from WebTrends Firewall Suite to Novell BorderManager log files.
- You can configure Novell BorderManager to export log files to another server, to which you can then point WebTrends Firewall Suite. (For information about how to export log files, see "Understanding Novell BorderManager's HTTP Proxy Logs," pp. 37–38.)

and CyberPatrol Web Filter, SurfControl's content-filtering software for business and education customers, respectively. (For more information about this reporting tool, see "You May Wanna Go There—Sometimes!" on p. 20.) NetIQ provides e-business infrastructure software, such as management and reporting tools. (For more information about NetIQ, visit [www.netiq.com](http://www.netiq.com). For more information about WebTrends Firewall Suite, see "Now You See It" on p. 18.)

Further suppose your reporting tool reveals that a certain user accesses sexually explicit material several times a day, on company time, despite your company's Internet usage policy, which prohibits accessing such sites at any time. To pre-

vent this user and other users from accessing this content, you may want to add an Adult/Sexually Explicit category to the seven SurfControl categories that ship with BorderManager 3.7. SurfControl provides a way for you to add this category.

As a BorderManager 3.7 customer, you can contact SurfControl for a key that unlocks a free 45-day evaluation of either SuperScout Web Filter or CyberPatrol Web Filter, which are full-scale versions of SurfControl's content-filtering software.

SuperScout Web Filter and CyberPatrol Web filter include 23 additional categories of Internet content—including an Adult/Sexually Explicit category—containing more than one million URLs. Furthermore, SurfControl enables you to

update the URLs in these categories by downloading daily updates from the SurfControl web site. (Previous versions of SurfControl's content-filtering software for BorderManager included only weekly updates. For more information about SuperScout Web Filter and CyberPatrol Web Filter, see "You May Wanna Go There—Sometimes!" on p. 20.) At the end of the 45-day evaluation period, you can contact SurfControl to purchase a yearly subscription to SuperScout Web Filter or CyberPatrol Web Filter. (If you choose not to subscribe to the service, however, you can continue to use the SurfControl Content Database of 60,000 URLs that ships with Novell BorderManager 3.7.)

- You can copy log files to the computer upon which WebTrends Firewall Suite is running.

After you configure WebTrends Firewall Suite to use Novell BorderManager, this software can help you create the following types of reports:

- Bandwidth analysis. Bandwidth analysis reports can display information about the amount of bandwidth users consume while accessing Internet content. These reports can also display usage by the amount of data transferred, the number of web sites visited, and web page views. You can also create summary reports that show usage trends by time of day. (For more information about bandwidth analysis reports, visit [www.webtrends.com/samplerreports/Firewall\\_bandwidth/FWbandwidth.htm](http://www.webtrends.com/samplerreports/Firewall_bandwidth/FWbandwidth.htm).)
- Internet usage compliance. These reports can display information about what Internet sites users visit, top Internet users, the resources users access, and other user-related topics. For example, if you are using web-filtering software that categorizes web sites according to the content these sites contain, Web Trends Firewall Suite can report Internet usage for these categories.

If you install the SurfControl Content Database—which is included with Novell BorderManager 3.7—for example, you can create a report that ranks Internet usage in the seven content categories that this database includes. (For more information about the SurfControl content database, see the "Control Freak? You're In Good Company!" section on p.16. For more information about Internet usage compliance reports, visit [www.webtrends.com/sampleReports/employee\\_net\\_usage/empprod.htm](http://www.webtrends.com/sampleReports/employee_net_usage/empprod.htm).)

What Web Trends Firewall Suite reports can do, NetIQ business development manager Craig Graunard explains, is help you understand how internal and external users are consuming your company's resources. "Companies are keen to know who is using the resources they're paying for and whether those resources are being used wisely or are being wasted," Graunard adds. (For more information about Web Trends Firewall Suite, visit [www.webtrends.com](http://www.webtrends.com).)

Visit our advertiser, Novell eProvisioning, at  
[www.novell.com/e provisioning](http://www.novell.com/e provisioning).

## You May Wanna Go There—Sometimes!

The decision to block user access to Internet content that could result in legal action against your company, or worse, is easy. Most companies don't think twice about blocking access to sites containing hate speech, violence, or other dangerous content, which you can block using the SurfControl Content Database included with Novell BorderManager 3.7. (According to an IDC report, "WorldWide Internet Access Control for 1999 & 2000," SurfControl is the market leader in Internet filtering software. IDC provides IT industry and market analysis and IT consulting services. For more information about IDC, visit [www.idc.com](http://www.idc.com). For more information about SurfControl, visit [www.surfcontrol.com](http://www.surfcontrol.com).)

This database includes seven categories of illegal or potentially dangerous Internet content and a total of over 60,000 sites that fall into these categories. (For more information about the SurfControl Content Database, see the "Control Freak? You're In Good Company!" section on p.16.)

As you know, however, illegal or otherwise dangerous sites aren't the only sites your company needs to consider. Almost any kind of personal Internet content could become a problem for your company—even content that seems benign.

To manage user access to all manner of personal Internet content, you can contact SurfControl for a software key that unlocks a full-scale version of either SuperScout Web Filter or CyberPatrol Web Filter. SuperScout Web Filter and CyberPatrol Web Filter are content filtering software for business and education users, respectively.

SuperScout Web Filter and CyberPatrol Web Filter include more than a million sites containing content to which your company probably wants to control—if not outright prohibit—access. These sites fall into 30 content categories, including the seven content categories included with Novell BorderManager 3.7.

For example, SuperScout Web Filter and CyberPatrol Web Filter include sites that fall into SurfControl's Hate Speech and Hacking categories, which are sites that your company probably wants to block altogether. Your company may also want to block user access to sites falling into the web-based e-mail category.

As SurfControl vice president of global product management Kelly Haggerty explains, web-based e-mail skirts the antivirus

software that scans messages coming into your company's e-mail system. Therefore, Haggerty adds, "from a security standpoint, companies want the ability to say no," to web-based e-mail.

However, SuperScout Web Filter and CyberPatrol Web Filter also include content categories to which your company may want to say yes—sometimes. For example, SuperScout Web Filter and CyberPatrol Web Filter include categories such as Finance & Investment, Hobbies & Recreation, News, Shopping, Religion, and Travel. (For a comprehensive list of SuperScout Web Filter and CyberPatrol Web Filter categories, see "What's New in Novell BorderManager 3.7?" *Novell AppNotes*, Mar. 2002, p.39. You can download this article from <http://developer.novell.com/research>.)

Providing managed access to these sites enables users to keep up with topics that interest them and, therefore, can elevate user morale. In fact, providing access to these sites may even help users be more productive. (See "Number of American Workers Online Increases," *CyberAtlas*, Aug. 2001. You can download this article from [http://cyberatlas.internet.com/big\\_picture/geographics/article/0,,5911\\_872091,00.html#table](http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_872091,00.html#table).)

### THE BABY STAYS, THE BATHWATER GOES

Every site listed in the SuperScout Web Filter and CyberPatrol Web Filter databases has been verified by human eyes. Therefore, you don't need to worry about inadvertently blocking or controlling access to legitimate business sites, as you do when you deploy web-filtering software that uses key words to filter sites.

For example, suppose your company provides reports about the activities of various government agencies and you want to block access to sites containing hacking and criminal skills content. If you deploy SuperScout Web Filter to block this content, you don't need to worry about blocking access to content your company needs, such as content on the U.S. Department of Justice's Computer Crime and Intellectual Property site ([www.usdoj.gov/criminal/cybercrime](http://www.usdoj.gov/criminal/cybercrime)).

Web filtering software that looks for key words, on the other hand, could possibly block this site because it contains key words—hacking and crime, for example—that this software would probably be looking for.

continued on p. 21

### FASTER! FASTER! BUT WITH CONTROL, PLEASE

The Novell BorderManager HTTP forward proxy service also includes Novell FastCache—Novell's proxy caching technology. Novell FastCache can speed employees' access to Internet content from 10 to 200 times and, coincidentally, save bandwidth. However, you may not know you can also use the Novell BorderManager HTTP forward proxy cache and Volera Excelerator ([www.volera.com](http://www.volera.com)) together in a hierarchical proxy caching architecture to further speed Internet access and free up bandwidth. (See Figure 3 on p. 22.)

Volera Excelerator is a high-speed caching platform that can handle up to 12,000 requests per second. Arranged in a caching hierarchy, Volera Excelerator can speed Internet content delivery for a greater number of users than a single BorderManager 3.7 forward proxy server can. Novell BorderManager 3.7, on the other hand, can control access to that content as Volera Excelerator can't. (For more information about using BorderManager 3.7 and Volera Excelerator together in a proxy caching hierarchy, see "Novell BorderManager and Volera Excelerator." You can download this white paper from [www.novell.com/info/](http://www.novell.com/info/collateral/docs/4621223.01/4621223.pdf)

[collateral/docs/4621223.01/4621223.pdf](http://www.novell.com/info/collateral/docs/4621223.01/4621223.pdf).)

You can also use Novell BorderManager 3.7 in reverse proxy mode to speed outside-the-firewall access to your company's web site. You may know that another Novell product, Novell iChain, also provides reverse proxy caching. Using Novell iChain to perform reverse proxy caching has distinct advantages.

Novell iChain is specifically designed to provide secure access to your company's web-based resources and therefore includes features that Novell BorderManager, which primarily provides forward proxy services, does not provide. For example, iChain includes SSLizer, a

continued from p. 20

Of course, most content filtering software—including SuperScout Web Filter and CyberPatrol Web Filter—provide a means by which you can override the software to allow access to particular web sites that would otherwise be blocked or controlled. The point is, because a human being accesses each site before that site is included in a SuperScout Web Filter or CyberPatrol Web Filter content category, you won't have to perform this task often.

#### **KNOW WHEN TO SAY WHEN**

Because SuperScout Web Filter and CyberPatrol Web Filter integrate with Novell eDirectory and Novell BorderManager, you can include SurfControl content categories in access rules for Novell BorderManager HTTP proxy services. That is, you can use the Novell BorderManager 3.7 snap-in module for the NetWare Administrator (NWADMIN) utility to configure rules that specify not only which content categories you want to allow or block, but also the time of day and day of week these rules are in effect.

Before you configure access rules for SurfControl content categories, however, you may want to know who is accessing content in these categories, and for how long. For example, it probably is not necessary to configure a rule that allows limited access to games if the users on your company's network don't play games at work.

On the other hand, users may be spending hours a day downloading music and, in the process, chewing up enormous amounts of your company's valuable bandwidth. In May 2000, public-relations firm Golin/Harris International discovered it had this particular problem. When the company deployed software that tracks users' Internet usage, this company discovered that 80 percent of the bandwidth at a branch office was devoted to downloading music files. (See "Workers, Surf at Your Own Risk," *BusinessWeek Online*, June 12, 2000. You can download this article from [www.businessweek.com/2000/00\\_24/b3685257.htm](http://www.businessweek.com/2000/00_24/b3685257.htm).)

If your company has a similar problem, it is obviously worth your time to configure a rule restricting access to sites in SurfControl's Streaming Media and Remote Proxies categories. (The Remote Proxies category contains the URLs of proxy servers through which users can participate in peer-to-peer file

sharing. These servers also enable users to download services, such as on-demand streaming media.)

To find out what sites users visit, when, and for how long, you can use the offline reporting and monitoring tool included with SuperScout Web Filter and CyberPatrol Web Filter. This tool also provides real-time bandwidth monitoring, which can help you troubleshoot bandwidth problems. According to Haggerty, "a lot" of SuperScout Web Filter and CyberPatrol Web Filter customers use this tool for precisely that purpose.

You can download the SurfControl reporting and monitoring tool when you contact SurfControl for the software key that unlocks the free 45-day evaluation copy of SuperScout Web Filter or CyberPatrol Web Filter. The SurfControl reporting and monitoring tool runs on Windows 2000 and NT and monitors TCP/IP traffic coming through your company's Novell BorderManager servers.

If you then subscribe to SurfControl's update service, which enables you to continue using either SuperScout Web Filter or CyberPatrol Web Filter (depending on which market your company is in: corporate or education), this reporting tool is included as a free component. (If you don't subscribe after 45 days, the reporting tool and SuperScout Web Filter or CyberPatrol Web Filter no longer work. However, the SurfControl Content Database that ships with Novell BorderManager will remain fully operational.)

#### **ALREADY A SUBSCRIBER? NO PROBLEM**

If you are currently a Novell BorderManager customer, you may have already purchased a subscription to a previous version of CyberPatrol Web Filter for Novell BorderManager. (This previous version is included with previous versions of Novell BorderManager and contains fewer sites and content categories than does the content-filtering software available to Novell BorderManager 3.7 customers.)

In this case, when you upgrade to Novell BorderManager 3.7, SurfControl plans to offer a free technology upgrade to the latest version of either SuperScout Web Filter or CyberPatrol Web Filter. This free upgrade remains in effect for the duration of your company's current subscription, providing that you also purchase a one-year subscription to the latest version of SuperScout Web Filter or CyberPatrol Web Filter. The new one-year subscription will take effect after your current subscription runs out. ●

Novell technology that uses Secure Sockets Layer (SSL) to encrypt your company's private content as it travels across the Internet.

Incidentally, Novell iChain is also included with Novell Secure Access. (For more information about iChain, visit [www.novell.com/products/ichain](http://www.novell.com/products/ichain).)

#### **Immunize Web Servers**

If you choose to use Novell BorderManager 3.7's reverse proxy caching service to accelerate your company's web content, however, Novell BorderManager 3.7 can help keep the servers that provide that content virus free. The Novell Bor-

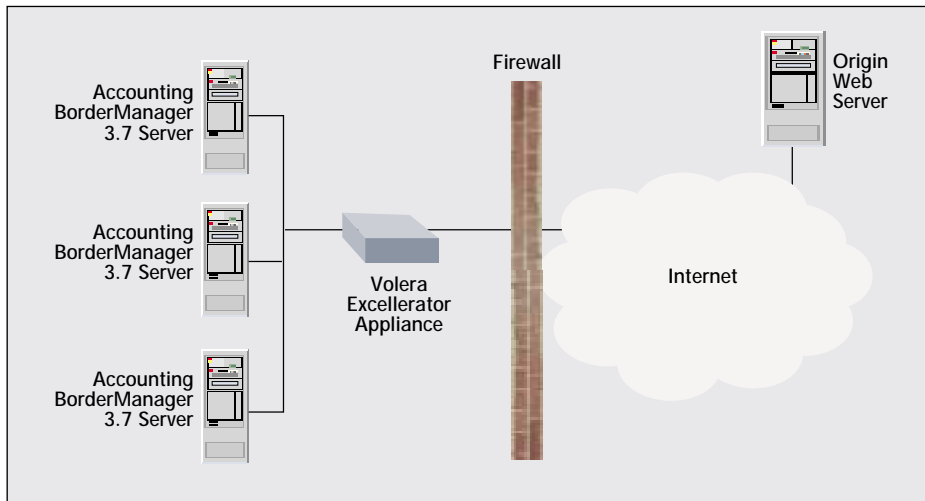
derManager 3.7 PROXY.NLM includes the Virus Request Blocking feature, which can help prevent your company's web servers from contracting HTTP-based viruses such as Nimda and CodeRed.

These viruses—which are also called worms—randomly generate TCP/IP requests for HTTP ports. For example, a web server infected with the CodeRed virus generates random TCP/IP requests for services at port 80, the nonsecure port over which web servers communicate.

If this infected web server establishes a connection to a Microsoft Internet Information Server (IIS) web server, the infected server sends an HTTP GET

request containing code that can, in turn, infect the IIS web server. (This code exploits a vulnerability in a Microsoft IIS buffer overflow, which enables attackers to execute code on these web servers. You can download a patch that eliminates this vulnerability at [www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-033.asp](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-033.asp).) These HTTP GET requests contain a recognizable pattern called a virus-request pattern.

When a Novell BorderManager 3.7 reverse proxy server receives HTTP requests, the Virus Request Blocking feature examines those requests, comparing the patterns in those requests with



**Figure 3.** Used in an HTTP forward proxy-caching hierarchy, Novell BorderManager 3.7 and Volera Excellerator can work together to speed and control access to Internet content.

known virus request patterns. When the Virus Request Blocking feature finds a pattern in a request that exactly matches a known virus request pattern, this feature automatically blocks that request.

At the time this article was written, the database included in the Novell BorderManager 3.7 PROXY.NLM contained request patterns for approximately 160 known HTTP-based viruses. Novell plans to provide additional virus request patterns in updates to the PROXY.NLM.

As you know, new viruses are created every day, and old viruses can sometimes alter their request patterns to evade detection. Fortunately, the Virus Request Blocking feature includes an Auto Update feature that can automatically detect requests from viruses—even if these viruses' request patterns are not included in the virus-request pattern database.

Viruses that attack web servers typically generate a substantially higher number of requests for web services in a shorter period of time than do legitimate applications, such as web browsers. The Auto Update feature counts the number of identical requests the Novell BorderManager 3.7 reverse proxy service receives in a specified amount of time.

The Auto Update feature then compares the number of identical requests with a threshold value. By default, this value is considerably higher than the average number of requests your company's web server receives from legitimate applications. If the number of identical requests in the specified time exceeds this threshold value, the Auto Update feature refers this request to a background process that examines the

request for known virus character strings, which are called *key words*.

Although request patterns may vary for a particular virus, the virus' requests are all likely to include the same key words. If this background process detects a virus key word, the Auto Update fea-

*“Given the obvious popularity of VPN services in general, it isn't surprising that the second most popular Novell BorderManager service is the Novell BorderManager VPN service.”*

ture adds this virus-request pattern to the virus-request pattern database, and the Virus Request Blocking feature blocks this request. (For information about how to enable and configure the Virus Request Blocking and Auto Update features and how to manually add virus request patterns and key words, see “Blocking Virus Requests in Novell BorderManager's HTTP Accelerator,” *Novell AppNotes*, Feb. 2002. You can download this article from [www.novell.com/research/completearchive.htm](http://www.novell.com/research/completearchive.htm).)

#### NEW FEATURES FOR A HOT ITEM

In a recent survey of 554 Chief Information Officers (CIOs), Chief Technology Officers (CTOs), and vice presidents of IT, 62.7 percent reported that their company has deployed or is planning to deploy VPN services for remote users. In addition, 52.9 percent of these respondents reported that their company has deployed or plans to deploy site-to-site VPN services to connect remote offices. (See “Security,” *CIO Insight Magazine*, Aug. 1, 2001. You can download this article from [www.cioinsight.com/article/0,3658,s=304&a=12879,00.asp](http://www.cioinsight.com/article/0,3658,s=304&a=12879,00.asp). To view only the results of this survey, visit [http://common.ziffdavisinternet.com/download/0/1191/feature0107\\_security\\_cost.pdf](http://common.ziffdavisinternet.com/download/0/1191/feature0107_security_cost.pdf).)

Given the obvious popularity of VPN services in general, it isn't surprising that the second most popular Novell BorderManager service is the Novell BorderManager VPN service. In Novell BorderManager 3.7, these VPN services are updated and enhanced in several important ways. For example, Novell BorderManager 3.7 adds support for two additional VPN client software platforms: Windows XP and ME. (Windows ME is an operating system designed expressly for home computers.)

#### HELLO NICI

Novell BorderManager 3.7 VPN client software also includes support for Novell International Cryptographic Infrastructure (NICI), the modular cryptographic infrastructure that NetWare and many NetWare applications use. (For More information about NICI, see “With NICI, It's All Holes Barred,” *Novell Connection*, Dec. 1998, pp. 8–20. You can download this article from [www.ncmag.com/past/](http://www.ncmag.com/past/).)

Previous versions of Novell BorderManager, on the other hand, use a cryptographic infrastructure that is unique to Novell BorderManager. Like NICI, this cryptographic infrastructure provides a full complement of cryptographic algorithms such as Data Encryption Standard (DES), Triple DES, RC2, and RC5.

Using NICI to provide cryptographic services offers one major advantage: By using NICI, Novell BorderManager VPN client software will be able to integrate with other Novell applications that use NICI. Notably, in the future, you will be able to integrate Novell BorderManager VPN client software with Novell Modular Authentication Services (NMAS).

NMAS, which is also included in Novell Secure Access, enables you to require more methods of authentication for your company's most confidential network resources than does Novell BorderManager Authentication Services (BMAS). BMAS, the Novell BorderManager component that currently provides Remote Dial-In User Service (RADIUS) services for Novell BorderManager, integrates with Novell BorderManager VPN client software to provide token-based and eDirectory username-and-password authentication.

By using NMAS to provide authentication services for Novell BorderManager VPN client computers, your company will be able to select from a greater variety of authentication methods, including eDirectory username and password, token, digital certificate, and biometric authentication. In fact, with NMAS, you will be able to require a sequence of up to three login methods to provide secure remote access to your company's top-secret network resources, such as the resources only your company's president and board of directors are authorized to see. NMAS 2.0 and later also include RADIUS services. (For more information about NMAS, see "NMAS: It's What Spy Movies Are Made Of," *Novell Connection*, Feb. 2000, pp. 6-21. You can download this article from [www.ncmag.com/past](http://www.ncmag.com/past).)

#### GUARD THAT BACKDOOR

Novell BorderManager 3.7 also includes Norman Personal Firewall from Norman Data Defense Systems. (Norman Data Defense Systems provides data security products, including antivirus software and risk analysis. For more information about Norman Data Defense Systems, visit [www.norman.com](http://www.norman.com).)

As you probably know, although VPNs ensure a secure connection between a remote user's computer and your network, VPNs can't ensure that the user's computer is secure. Therefore, a user's computer can provide a backdoor into your company's network. Cyber criminals can use this backdoor to gain access to the very resources VPNs are designed to secure.

For example, a cyber criminal could upload a malicious listening program through an unprotected File Transfer Protocol (FTP) port, which could then detect communications between this computer and your company's network. As a result of a previous virus infection, this user's com-

puter could also be harboring a Trojan horse, which could use this computer to access and damage your company's network. (A *Trojan horse* is a malicious program that is contained within another program, such as a computer virus.)

Norman Personal Firewall protects users' computers at the packet and application levels. For example, you can configure Norman Personal Firewall to block incoming FTP requests, thereby preventing would-be attackers from uploading malicious programs via FTP. Norman Personal Firewall also works at the application level to alert users when an unauthorized application—such as a Trojan horse—tries to establish an Internet connection.

Therefore, by using the Norman Personal Firewall to secure users' computers, you can protect your company's network. (For more information about what the Norman Personal Firewall can do, see the "Personal Firewall" section of "What's New in Novell BorderManager 3.7?" *Novell AppNotes*, Mar. 2002, pp. 41-42. You can download this article at <http://developer.novell.com/research>.)

#### CONCLUSION

Perhaps your company is uncommonly lucky and therefore hasn't experienced the problems your fellow IT professionals reported in the Information Security Magazine Industry Survey for 2002. However, your luck may not hold. If your company hasn't yet deployed software that can control access to its network resources, from inside and outside, your company is probably headed for trouble. Don't take my word for it. Check out the survey, and run the numbers.

Admittedly, creating an access control policy can be difficult. Novell BorderManager 3.7 and other products in Novell Secure Access can't answer some of the particularly thorny (and often political) questions involving access control—such as who gets access to what, when, and where. What these products can do, however, is give you a great deal of flexibility in how you exercise access control.

*Cheryl Walton works for Niche Associates, an agency that specializes in writing and editing technical documents. Niche Associates is located in Sandy, UT. ●*

Visit our advertiser, Ecora, at [www.ecora.com](http://www.ecora.com).