

3.8

N·O·V·E·L·L B·O·R·D·E·R·M·A·N·A·G·E·R
O·P·E·N·I·N·G U·P A·N·D T·Y·I·N·G D·O·W·N
R·E·M·O·T·E A·C·C·E·S·S S·E·C·U·R·I·T·Y

BY CHERYL WALTON
PHOTOGRAPH BY HOLLY LINDEM



With more than 20,000 customers and ten million seats in production, Novell BorderManager is one of the top firewall and virtual private network (VPN) products available today—and these impressive numbers are about to get even better.

Novell BorderManager helps you control users' access into and out of your network based on their role in or relationship to your organization. To provide this identity-based access control, Novell BorderManager uses Novell eDirectory, one of the oldest and most respected directories on the market.

Novell BorderManager includes Network Address Translation (NAT) and ICSA Labs-certified firewall services, which provide packet filtering and basic reverse proxy services. (ICSA Labs is a division of TruSecure Corporation and offers vendor-agnostic testing and certification of security products. For more information, visit www.icsalabs.com.)

While these firewall services offer an effective first line of defense, most companies that purchase Novell BorderManager do so for its forward proxies, which sit between the users and the Internet. Proxies retrieve Web pages and other requested content on behalf of the users, so that users never access the Internet directly. BorderManager 3.8 includes HTTP, FTP, Mail, News, Telnet, RTSP/RealAudit, DNS, Generic TCP and Generic UDP proxies. Not surprisingly, these proxies remain intact in Novell BorderManager 3.8—the latest version of Novell BorderManager and part of the Novell Nsure secure identity management family of solutions. (For more information about Novell Nsure, visit www.novell.com/solutions/nsure.)

Available in public beta since July and scheduled for release in mid-November, Novell BorderManager 3.8 includes several new and improved features, including the following:

- New VPN services that support open standards
- Bundled Novell Client Firewall to lock down VPN clients
- Support for more than 50 authentication methods

These three features are arguably the most exciting new features in Novell BorderManager 3.8. (For a complete list of new and enhanced features, see *The Art of Improving a Good Thing* on p. 30.) More important, these three features underscore the Novell BorderManager 3.8 claim to fame: Novell BorderManager 3.8

offers everything remote users need for secure, role-based access to your non-Web applications—regardless of where these users are—while offering the same popular proxies you might already use to safeguard your network against undesirable Internet content.

OPEN-MINDED TUNNEL VISION

Novell BorderManager 3.8 features new VPN services that support open standards, including Internet Protocol Security (IPSec) and Internet Key Exchange (IKE). IPSec is a framework for a set of security protocols that function at the packet layer of the network communications model. The use of IPSec is mandatory with the Internet Engineering Task Force (IETF) IPv6 standard (which is slowly being adopted) and optional with IPv4.

Officially an IETF-proposed standard, unofficially IPSec is widely accepted as the de facto standard for gateway-to-gateway (or site-to-site) VPNs. (You can download the IPSec Requests for Comments [RFCs] 2401, 2402 and 2406 from www.ietf.org/html.charters/ipsec-charter.html.)

To set up these secure communication channels, IPSec VPN servers commonly use IKE. Specified in IETF RFC 2409, the IKE protocol defines the method for the key exchange that servers use to set up a shared secret over an insecure communication channel. (You can download this RFC from www.ietf.org/html.charters/ipsec-charter.html.) From this shared secret, the servers then derive the cryptographic keys that enable them to set up a secure communication channel. (Of course, Novell BorderManager 3.8 continues to support Simple Key Management for Internet Protocol [SKIP] to ensure backward compatibility with Novell BorderManager 3.7 and older versions.)

SITE-TO-SITE INTEROPERABILITY

In a word, the benefit of Novell BorderManager 3.8 support for these open standards is interoperability. Through its support for IPSec and IKE, Novell BorderManager 3.8 VPN enables you to establish site-to-site VPNs with companies using other IPSec-certified VPNs. In fact, the point of ICSA Labs IPSec certification, which Novell is currently seeking for Novell BorderManager 3.8, is to ensure interoperability between products.

Novell BorderManager helps you control users' access into and out of your network based on their role in or relationship to your organization.

With Novell BorderManager 3.8 VPN, you can set up secure channels for communication between your company and its business partners and customers, and between it and companies with which it has merged. As long as the other site is also running an IPSec-certified VPN gateway, you can rest assured that your NBM server and the other site's VPN gateway will work well together.

Within your own network boundaries, you'll find that a Novell BorderManager 3.8 server works well together with all of your other network services—including NAT. In fact, with Novell BorderManager 3.8, your deployment options are virtually limitless: you can place the Novell BorderManager 3.8 VPN server (and clients) literally anywhere on your network—regardless of where you handle NAT. (For more information, visit www.novell.com/connectionmagazine/2003/12/tech_talk_2.html for online material and click the link to *Anywhere You Want It—Really.*)

Of course, enabling business partners and customers to access

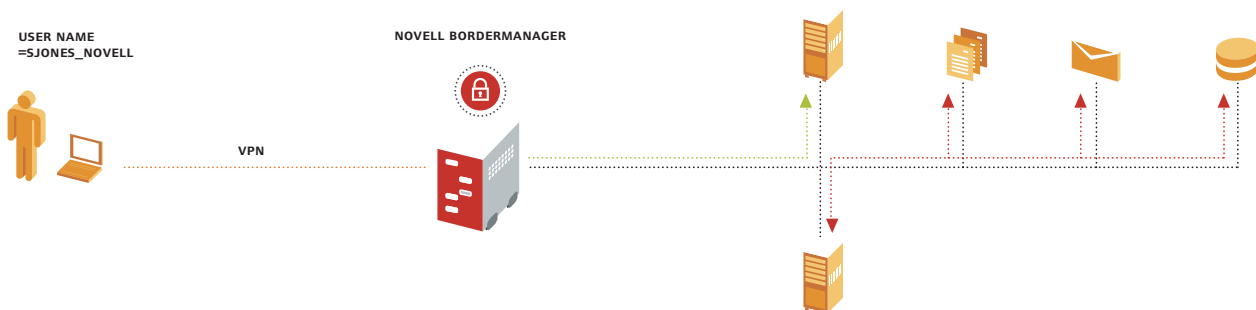
your network can be risky unless you control VPN users' access to specific network resources. Novell BorderManager 3.8 enables you to do precisely this. (See Figure 1.) With Novell BorderManager 3.8, you create traffic rules (stored in eDirectory) to allow or deny access to each resource based on its IP address, address range, subnet and port number. To control VPN users' access, you associate eDirectory User, Group and Container objects or digital certificates (assuming you use these for authentication) with these traffic rules.

CLIENT-TO-SITE INTEROPERABILITY

Novell BorderManager 3.8 also provides some assurance of VPN client-to-site interoperability. For example, the Novell BorderManager 3.8 VPN client interoperates with many third-party VPN gateways. As you might guess, successful interoperability hinges upon the third-party server's support for IPSec. Also, to ensure interoperability, the third-party server must,

NOVELL BORDERMANAGER 3.8 VPN: IDENTITY-BASED TRAFFIC RULES

TRAFFIC RULES: **From:** users, groups, containers, digital certificate **To:** IP address, address range, subnet, port



With Novell BorderManager 3.8, you create traffic rules to allow or deny access to each resource based on its IP address, address range, subnet and port number.

FIGURE 1

for authentication purposes, use either pre-shared secrets (via IKE or SKIP) or digital certificates that support the X.509 standard.

The Novell BorderManager 3.8 VPN client runs on Microsoft Windows 98, Me, NT 4, 2000 and XP (both Professional and Home Edition). However, you are not restricted to Windows clients. With Novell BorderManager 3.8 VPN services, you can also connect to the Novell BorderManager 3.8 server using third-party VPN clients for other platforms, including the following:

- Linux desktops and laptops
- Macintosh desktops and laptops

The Art of Improving a Good Thing

Novell BorderManager 3.8 includes the following features:

Virtual Private Network (VPN)

- IPSec-based VPN services
- Interoperability with IPSec-certified products
- Authentication against any LDAP directory
- Granular control of where VPN users can go on the private network, based on identity

Internet Access Control/Forward Proxies

- Support for SurfControl Content Database and N2H2 Category
- ServerSupport for free URL databases via Connectotel's LinkWall

Security

- Built on Novell International Cryptographic Infrastructure (NICI)
- Support for more than 50 authentication methods
- Stronger remote access security with Public Key Infrastructure (PKI) through provisioning and de-provisioning of X.509 certificates
- Secure access to internal and external resources based on users' identity in any LDAP directory

Firewall

- ICSA Labs-certified firewall on server
- Bundled Novell Client Firewall 2.0

Even when products are based on open standards, interoperability isn't necessarily a foregone conclusion. As you might expect, Novell tests its products to make sure they work flawlessly with partner products in practice, not just in theory. To date, Novell has confirmed interoperability between Novell BorderManager 3.8 and the following VPN clients for these platforms:

PRODUCT NAME	PLATFORM	NOVELL PARTNER INFORMATION
VPN Tracker	Macintosh OS	Equinox USA, Inc. www.equinux.com
Linux FreeS/WAN	Linux	www.freeswan.org

Novell supports the operation of the Novell BorderManager 3.8 VPN server when working with these clients, as long as the clients use either pre-shared secrets or X.509 certificates for authentication. (As you might expect, these clients' vendors provide the support for their products.)

ENSURING TROJANS DON'T WORM THEIR WAY IN

While the actual connection between a VPN client and server might be faultlessly secure, the fact is that a client-to-site VPN connection is only as secure as the client using it. It takes only one remote user opening an infected attachment and logging into your network by way of a VPN client for a virus to worm its way into your network—snug as a bug (pun intended).

To help you guard the access points to your network, Novell BorderManager 3.8 bundles the new Novell Client Firewall 2.0, which is Novell's first step into the end-point security (EPS) arena. End-point security refers to an emerging group of products that enable you to extend and enforce your network security policy all the way to the nodal level.

For its part, Novell Client Firewall enables you to extend your security policy to any workstation running Windows NT 4, 2000, and XP. Novell Client Firewall is compatible with—but does not require—Novell Client 32.

In the initial release of Novell Client Firewall, Novell has taken steps toward integrating this client firewall with the Novell

It takes only one remote user opening an infected attachment and logging into your network by way of a VPN client for a virus to worm its way into your network.

BorderManager 3.8 VPN server. For example, you can configure Novell BorderManager 3.8 to allow VPN connections only when Novell Client Firewall 2.0 is running on the client requesting the connection. (For information about managing Novell BorderManager 3.8 using Novell iManager 2.0, see www.novell.com/connectionmagazine/2003/12/tech_talk_2.html for online material and click the link to *Convenient and Secure*.)

On the client, Novell Client Firewall 2.0 enables you to allow or deny activity based on the requested port, protocol or application. (See Figure 2.) When you block, allow or partially allow an application, Novell Client Firewall 2.0 begins tracking not only the main executable for this application, but all of the application's dependent components, for example, associated .dll files. Novell Client Firewall 2.0 alerts users of any changes to an application's dependent components, thereby protecting VPN clients (and hence your network) from viruses or Trojans that otherwise sneak past firewalls by masquerading as application components.

Novell Client Firewall 2.0, bundled with Novell BorderManager 3.8, enables you to allow or deny activity based on the requested port, protocol or application.

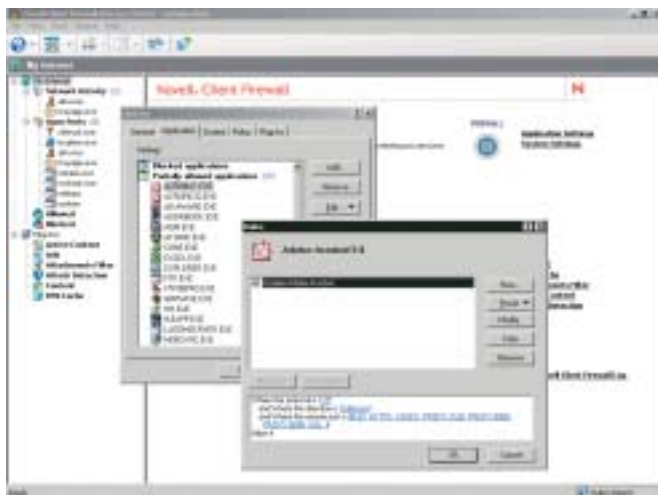


FIGURE 2

Of course, most users know nothing about ports and protocols, making firewall configuration a potential nightmare for these users—and for your company's helpdesk personnel. To avoid this situation, you can use the firewall's management interface to create one or more configuration files. (See Figure 2.) You can then copy these files to the firewall before distributing it to users. Alternately, you can offer these files along with Novell Client Firewall, and users can then copy the configuration file of choice to the firewall's application files. Either way, users won't need to worry about firewall configuration.

You can also password protect your configuration files to minimize the possibility of technically savvy users changing your configuration—or you can use Novell ZENworks for Desktops to distribute and lock down this configuration. Otherwise, users can modify the configuration file.

In future releases, you will also be able to centrally manage the Novell Client Firewall using Novell iManager. (For more information on planned enhancements, visit www.novell.com/connectionmagazine/2003/12/tech_talk_2.html for online material and click the link to *Going Forward*.)

WHO'S WHO? MORE THAN 50 WAYS TO KNOW

Novell Client Firewall secures an otherwise unguarded network access point, and Novell BorderManager 3.8 secures the channel between this client and your network, leaving only one potentially weak link in this VPN chain: the VPN user. How can you be sure that the user is who she claims to be, particularly if she is using only a password to authenticate? After all, passwords alone can be weak modes of authentication if you have users who fight forgetfulness by writing down their password or choosing a too-simple one.

Novell BorderManager 3.8 strengthens this potentially weak link by offering you the opportunity to deploy additional or alternative modes of authentication. In fact, Novell BorderManager 3.8 supports more than 50 advanced authentication methods (which is about 40 more methods than any other VPN product supports), including methods that incorporate tokens, smart cards and biometrics. Of course, Novell support for such a wide variety of advanced authentication methods isn't new. What's new is the packaging for

Novell BorderManager 3.8 strengthens this potentially weak link by offering you the opportunity to deploy additional or alternative modes of authentication.

this support. The support for these advanced authentication methods stems from Novell Modular Authentication Services (NMAS) Enterprise Edition 2.2, which Novell BorderManager 3.8 includes. In fact, as soon as Novell BorderManager 3.8 goes on the shelf, NMAS EE 2.1 (the previous version of NMAS EE) comes off the shelf. (Incidentally, NMAS EE 2.1 customers with upgrade protection have never been so lucky: these customers will receive Novell BorderManager 3.8 as the replacement product.)

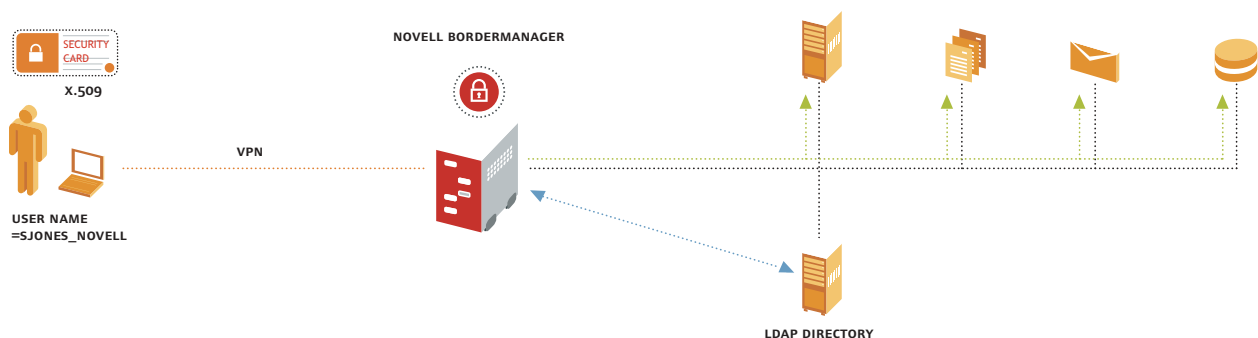
Although you can find some Novell-supported authentication methods in other Novell products, you can find them all only in Novell BorderManager 3.8. Novell BorderManager 3.8 includes (and will continue to incorporate) all of the NMAS components. That is, Novell BorderManager 3.8 offers Remote Authentication Dial-In User Service (RADIUS) server and all of the NMAS authentication methods—including Advanced X.509, Universal Smart Card, pcProx, Secure Workstation and LDAP authentication.

You can guess what most of these methods enable based on their names. For example, the X.509 method enables users to authenticate to eDirectory using an X.509 certificate. Similarly, the pcProx method enables you to use the pcProx proximity card and reader (from RF Ideas Inc.) to authenticate to the network. (For more information about pcProx cards and readers, visit www.pcprox.com.)

It's also easy to guess that the LDAP authentication method enables users to log in to Novell BorderManager 3.8 by way of any LDAP directory, including eDirectory Active Directory, and iPlanet. (See Figure 3.)

By pairing LDAP authentication with Novell BorderManager 3.8, you can render its services, most notably its VPN services, virtually directory neutral. In other words, by enabling users to log in to Novell BorderManager 3.8 by way of any LDAP directory, you can deploy Novell BorderManager 3.8 as an appliance (with no

NOVELL BORDERMANAGER 3.8 VPN: LDAP AUTHENTICATION METHOD



The LDAP authentication method enables users to log in to Novell BorderManager 3.8 by way of any LDAP directory, including eDirectory, Active Directory and iPlanet.

FIGURE 3

users in its single tree) and then point this appliance to your LDAP directory. As Novell product manager Scott Jones says, “all you need is the IP address for your LDAP server and, boom, you’re off.”

The details of the Secure Workstation method are not as immediately apparent. Secure Workstation runs on Windows 2000 or Windows XP workstations and responds to two types of events: the removal of an authentication device or an automatic timeout because of user inactivity. Depending on how you configure it, Secure Workstation responds to these events in one of the following ways:

- It locks the workstation, logs out of Windows, closes all programs and logs out of the network.
- It closes all programs and logs out of the network.

(For more information, visit www.novell.com/documentation/lq/nmas22/pdfdoc/secureworkstation.pdf.)

WHAT’S IN IT FOR YOU?

To reiterate, with its standards-based VPN, client firewall and support for more than four dozen authentication methods, Novell BorderManager 3.8 offers you the ability to secure remote access. It does this and more for your network, but what does it do for you? Novell BorderManager 3.8 offers you the opportunity to simplify your work life and improve user productivity in the process.

Novell BorderManager 3.8 simplifies your work life in part because it supports open standards. For example, because

Novell BorderManager 3.8 supports IPSec, it interoperates with other IPSec-certified products, such as VPN equipment from Cisco, CheckPoint and Nokia. This translates directly into saving your company money because you can use the Novell BorderManager 3.8 VPN service to establish secure connections with business partners using equipment that you might already have, without combating compatibility and new hardware obstacles. By enabling you to use your existing investments, Novell BorderManager 3.8 saves you time (and again, your company money) and spares you from facing what would otherwise be a hassle.

Similarly, because Novell BorderManager 3.8 can authenticate users against any LDAP-compliant directory, you can deploy the remote access solution that makes the most sense for your environment. Again, because you can set up an access solution without ripping and replacing what you already have, you save yourself time and save your company money.

And finally, Novell BorderManager 3.8 can improve employee productivity. For example, Novell BorderManager 3.8 enables you to grant mobile users secure, role-based access to non-Web applications from any location—thus enabling them to access the resources they need to be productive at the office, at home or on the road. As both a network administrator and a network user, you benefit from this capability by making your environment more secure giving your users access from anywhere, and did I mention that it can save you and your company money? **N**

www.
grouplink.
net