FOCUS

PRODUCT

FIREWALL-1 4.0

FireWall-1 4.0 from Check Point Software Technologies Ltd. is a stateful inspection firewall that enables you to define and enforce one security policy for your company's entire network, including its Internet access points. A stateful firewall becomes an integral part of companies' business plans, the lines between the different types of networks are blurring. Increasingly, companies want to manage their web sites, extranets, and intranets as part of their enterprise network, and they want to control all of their network resources from a central location.

The obvious way to manage your company's enterprise network is to use a directory service, such as Novell's NDS eDirectory. (NDS eDirectory is the latest version of NDS.) By using NDS eDirectory as the framework for your company's enterprise network, you can view and control every aspect of that network—including Internet access and security.

Since we cannot possibly cover all of the Internet security products that are currently available, this article features some of the security products that are NDS enabled.

FireWall-1 4.0

FireWall-1 4.0 from Check Point Software Technologies Ltd. is a stateful inspection firewall that enables you to define and enforce one security policy for your company's entire network, including its Internet access points. FireWall-1 4.0 provides access control for more than 150 predefined applications, services, and protocols. In addition, FireWall-1 4.0 provides content security and complete application-layer awareness.

Using the rules outlined in your company's security policy, FireWall-1 4.0 examines every packet that passes through key network locations (such as Internet gateways, servers, workstations, routers, or switches). FireWall-1 4.0 examines data at all layers of the Open Systems Interconnection (OSI) model, checking IP addresses, port numbers, and any other information required to determine whether or not packets are permitted by your company's security policy. FireWall-1 4.0 blocks all unauthorized communications; only packets that comply with your company's security policy can enter your company's network.

FireWall-1 4.0 is integrated with Novell Directory Services (NDS). As a result, you can use the Lightweight Directory Access Protocol (LDAP) interface to NDS to manage FireWall-1 4.0, and FireWall-1 4.0 can access security information (such as usernames and passwords) that is stored in NDS. This integration simplifies network management since you no longer have to maintain separate databases for your company's firewall and directory service.

The integration between FireWall-1 4.0 and NDS has received both companies' stamp of approval: FireWall-1 4.0 has been Novell Yes, Tested and Approved for use with NDS 8 and Windows NT 4.0, thereby earning Novell's Directory Enabled certification. In addition, NDS 8 has been certified by Check Point Software and has received its Open Platform for Security (OPSEC) certification. (For more information about these certifications, visit http://developer.novell.com/solutions/yes.htm and http://www.checkpoint.com/opsec/framework.html.)

For more information about FireWall-1 4.0, visit http://www.checkpoint.com. You can also call 1-800-429-4391 or 1-650-628-2000.

NOVELL FIREWALL FOR NT

Novell FireWALL for NT from Novell combines policy-based security management, traffic management, and directory services integration. Designed for small- and medium-sized companies, Novell FireWALL for NT enables you to filter network traffic by users, groups, IP addresses, time of day, application commands, file types, and web pages.

In addition, Novell FireWALL for NT provides network address translation, which enables you to hide your company's IP addresses from the Internet. Network address translation not only enhances network security but also conserves IP addresses.

Unlike other firewalls, Novell FireWALL for NT also includes the Traffic Manager, which enables you to allocate network bandwidth: You can grant bandwidth priority to applications and users performing critical tasks.

Because Novell FireWALL for NT includes monitoring and alarm features, you can track user activity. If a security threat occurs, Novell FireWALL for NT notifies you.

Novell FireWALL for NT is integrated with NDS and Windows NT domains. If you use Novell FireWALL for NT with NDS, you can create rules based on other users and groups rather than on IP addresses. However, Novell FireWALL for NT can function as a standalone product; NDS is not required.

Novell FireWALL for NT runs on Windows NT 4.0 with Service Pack 3 or above. For more information about Novell FireWALL for NT, visit Novell's...
web site (http://www.novell.com/products/ntfirewall). You can also call 1-800-321-4272 or 1-801-228-4272.

BORDERMANAGER ENTERPRISE EDITION 3.5
BorderM anager Enterprise Edition 3.5 is a suite of services that enables you to centrally manage, secure, and accelerate users’ access to information at every network border—internal and external alike. You can use BorderM anager to secure your company’s Internet border or to implement mini-firewalls at departmental borders.

Because BorderM anager is fully integrated with N DS, you can control users’ access through these borders. You can control where users go on your company’s network or the Internet, when they can go there, and what level of access they have when they get there. You can also control when and which users can access your company’s network from the Internet.

BorderM anager also enables you to set up virtual private networks (VPN s). With BorderM anager, you can implement three types of VPN s: site-to-site VPN s, client-server VPN s, and extranet VPN s.

In addition to providing security features, BorderM anager includes proxy caching and reverse caching capabilities. As a result, you can speed up Internet access for your company’s users, and you can also improve the performance of your company’s web site. By configuring BorderM anager to cache your company’s web site, you can make this web site both easier and faster to access.

BorderM anager runs on N etW are 5 and 4 and N ovell Small Business Suite 5. For more information about BorderM anager, visit http://www.novell.com/bordermanager. You can also call 1-800-321-4272 or 1-801-228-4272.

ENTREPRISE SECURITY MANAGER 5.0 FOR NDS
Part of establishing Internet security is providing end-to-end security on your company’s network. Enterprise Security M anager (ESM ) 5.0 for N DS from Ax- Ent Technologies Inc. is a cross-platform, enterprise security management system. With ESM 5.0, you can plan, manage, and control company-wide security policies from a central location.

ESM 5.0 supports more than 35 operating systems, including N etW are, UNIX, W indows NT Server and Workstation, and O penVM S. To manage these diverse systems, ESM 5.0 uses a manager-agent architecture. ESM agents reside on each system, enabling you to manage, monitor, and report on that system’s security status. The ESM manager controls groups of agents and collects and stores the security data the agents report.

ESM managers and agents can run on different operating systems. For example, an ESM agent running on a N etW are server can control agents running on UNIX or W indows NT servers.

To control the agents and, therefore, the systems on which the agents run, you create security policies. You can use default security settings or create customized security settings to better meet the needs of your company. For example, ESM 5.0 can help you identify and prevent users from having security privileges that exceed your company’s security policy. ESM 5.0 can also examine startup files for potential security breaches, check system mail for security lapses, and protect the integrity of objects by identifying changes in ownership and permission.

ESM 5.0 is N ovell Yes, Tested and Approved for use with N etW are 5, 4.2, and 4.11. In addition, ESM 5.0 has earned N ovell’s D irectory E nabled certification for use with N DS 8 and 7.5. For more information about EM S 5.0, visit http://www.axent.com. You can also call 1-888-44-A XENT or 1-301-258-5043.

NOVELL CERTIFICATE SERVER 2.0
N ovell Certificate Server 2.0 from N ovell enables you to secure communications over the Internet. N ovell Certifi cate Server 2.0 integrates with N DS and N ovell International Cryptographic Infrastructure (NIC I) to establish a Public Key Infrastructure (PKI) on your company’s network. A PKI enables you to encrypt, digitally sign, and authenticate transactions.

To secure communications, N ovell Certificate Server 2.0 mints digital certificates that comply with the X.509 v3 certificate standard. With N ovell Certificate Server 2.0, you can use an internal certificate authority (CA) or a commercial CA. N ovell Certificate Server 2.0 supports all of the widely known CAs, including VeriSign, Entrust, N etscape CA, X cert, and G TE CyberTrust. (N ovell has officially tested N ovell Certificate Server 2.0 with VeriSign, Entrust, and N etscape CA.) (For more information about minting certificates and securing Internet communications, see “N ovell Certificate Server 2.0: Is Your N etW are Certifiably Secure?” N etW are C onnection, Jan. 2000, pp. 6–20. You can download this article from http://www.nwconnection.com/past.)

N ovell Certificate Server 2.0 is bundled with N etW are 5.1 or available for free download from http://www.novell.com/download/#N DS. For more information about N ovell Certificate Server 2.0, visit http://www.novell.com/products/certserver. You can also call 1-800-321-4272 or 1-801-228-4272.

CONCLUSION
As the lines between the Internet, extranets, and intranets blur, you will have to be increasingly vigilant in identifying and guarding your company’s borders. As you look for products to shore up your company’s defenses, you should keep in mind the advantages of leveraging your company’s N DS infrastructure. A directory service is key to managing your company’s network end-to-end.