ENTERPRISE EDITION

Safely **extend** your business
to the Internet

BorderManager™

ENTERPRISE EDITION

Novell®

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

ABOUT THIS GUIDE

BorderManager™ Enterprise Edition is a complete security management solution for Internet-enabled businesses that leverages the power of Novell Directory Services® (NDS™). It includes a wide variety of industry-leading features that set it apart from other vendors' products. Novell has produced this document to help you, the reviewer or evaluator, visit the many advanced features of BorderManager.

The document is divided into 4 major sections. Section 1 includes a discussion of the need for a product like BorderManager followed by an overview of the BorderManager solution. Section 2 presents the highlights each of the major components of BorderManager: firewall services, virtual private network services, proxy cache services, policy-based administration, authentication, and alerting, logging and reporting. Section 3 shows the versatility of BorderManager through seven representative scenarios, each illustrating a different aspect of BorderManager. Section 4 (in separate volume) presents a step-by-step procedure for installing and configuring BorderManager.

We at Novell hope that this guide helps you "cut to the chase" quickly to discover and experience the full and unique power of BorderManager.

SECTION 1. OVERVIEW

THE NEED FOR AN INTEGRATED SECURITY SERVICES SOLUTION

Companies are rushing headlong into the Internet, driven by frenzied media coverage and the urging of consultants. Not only are companies connecting their corporate networks to the Internet but they are also deploying Internet technologies, such as Web and FTP servers, in their corporate networks to create intranets. The advantages are many, including closer interaction with customers through the Internet, closer interaction with business partners through extranets, and closer interaction with employees through internal Web servers. In addition, many companies are taking advantage of the Internet as a low-cost wide area network (WAN) link and interconnecting their local area networks (LANs) through virtual private networks (VPNs).

However, companies must address a major issue when connecting to the Internet and deploying intranets and extranets—that issue is security. The Internet is notoriously unsecure. As a result, integrating a corporate network with the Internet exposes it to intrusion from the outside. To provide protection, a number of vendors provide firewalls, which form a protective barrier between the Internet and the corporate network.

There is a much more severe and more subtle security problem, however, one that is more difficult to deal with than Internet hackers. Deploying Internet technologies, such as internal Web servers, on a corporate network exposes the information stored on them to intruders from within the company. In this case, an Internet firewall provides absolutely no protection because the intruder is already inside the firewall. Moreover, inside intruders know where resources are located and have access to internal desktops. The problem is all the more vexing because, according to the International Computer Security Association (ICSA), up to 80 percent of break-ins occur from within the firewall. Most Web servers provide their own security mechanisms, such as password protection, but these mechanisms are typically weak and easy to penetrate.

What is required in addition to a firewall is an internal barrier that allows a company to partition its intranet into protected segments.

(It's interesting to note that the word "firewall" actually describes a physical barrier, such as a steel door, that is located within the walls of a building to prevent the spread of fire within a building.)

Closely tied to the issue of security is the issue of performance. The filtering action of the firewall slows information passing through it just as liquid flow rate is decreased when a liquid is passed through a filter. In fact, the tighter the firewall, the greater the slowing effect. As a result, companies are forced to make a trade-off between security and performance. Software vendors have responded by providing proxy caches and other performance enhancers that help mitigate the performance degradation caused by firewalls.

Software vendors also provide VPNs that provide a variety of network topologies. VPNs allow companies to link multiple sites in a corporate intranet. They allow remote users to access the intranet over the Internet. And they allow companies to link with their business partners' sites in an extranet. All these topologies use the Internet as a low-cost link. Communicating information over the Internet, however, exposes it to eavesdroppers and vandals. As a result, the VPN protects the privacy of the information through encryption, and protects the integrity of the information by ensuring that it has not been altered in transit over the Internet.

Another problem companies face when connecting to the Internet is that some employees may spend time on non job-related activities such as surfing the Web. This negatively impacts employee productivity and clogs the network with unnecessary traffic. Worse yet, some companies have been exposed to liability claims because of offensive material downloaded from Web sites and displayed in the workplace. It is important that a company be able to control outgoing access to the Internet. Software vendors provide products, such as content filters, that prevent employees from accessing certain Internet sites.

In summary, software vendors as a group have addressed several aspects of the security and performance issues associated with deploying Internet technologies. They offer a variety of products, including Internet firewalls, performance accelerators, VPNs, and Internet Web destination content filters. The problem is, a network owner has to cobble together these products from multiple vendors to provide a solution. Managing a conglomeration of separate products is complicated, inefficient, and error prone. In fact, the ICSA reports that up to 90 percent of all firewall break-ins are due to configuration errors. Administrators have to deal with multiple directories for each user, and users have to deal with multiple user IDs and passwords. To make matters worse, as difficult and costly as the resulting solution is to manage and use, it still does not provide strong protection against internal break-ins.

What is required is set of services that provides protection from outside break-in, protection from inside break-in, performance acceleration, a secure VPN capability, and full control over outgoing Internet access—all in a single, integrated, and manageable package.

THE BORDERMANAGER SOLUTION

Novell's BorderManager meets the need for an integrated security services solution. This complete security management solution for Internet-enabled businesses leverages the power of Novell Directory Services (NDS). With BorderManager, a company can:

- *Take full advantage of the Internet and its technologies while protecting company information from internal and external intruders.*

- *Deliver high performance to users—without trading off strong security.*
- *Lower the total cost of network ownership through centralized administration and control.*

BorderManager includes:

- *Firewall services*. BorderManager provides a firewall that can be used to protect the corporate network from intruders both outside and inside the organization. The BorderManager firewall provides a strong barrier between the corporate intranet and the Internet to protect against outside intruders. In addition, BorderManager firewalls can be used to partition the corporate intranet into secure segments to protect sensitive information from internal break-in. BorderManager firewall services allow a company to control incoming access from the Internet as well as outgoing access to the Internet.

- *Virtual private network services*. BorderManager enables a company to use the Internet as a link to connect sites, allow remote clients to access the corporate intranet, and implement extranets that connect business partners with the corporate intranet. The information transmitted over the Internet is secured through encryption to prevent unauthorized access by eavesdroppers. In addition, the information is checked for accuracy to detect tampering by vandals.

- *Proxy caching services*. BorderManager provides performance-enhancing Web and FTP proxy caching services that provide a high level of performance without jeopardizing security. A company can use BorderManager caching services to reduce the number of Web servers it needs, lowering both equipment costs and management costs.

- *Authentication services*. BorderManager Authentication Services (BMAS) combines the remote access security allowed by the Remote Authentication Dial-In User Service (RADIUS) protocol with the ease and convenience of NDS. BMAS enables remote users to log into the network over the Internet using only a single password, and have access to all their network resources, including applications, files, printers, services and other network resources.

Because BorderManager is integrated with NDS, network administrators can control security and access globally from a single, centralized point. As a result, they can manage more resources, increasing their productivity and reducing the cost of management. In addition, security management through NDS scales easily and allows administrators to delegate certain access management responsibilities in a controlled and secure manner. Tight integration with NDS makes BorderManager a natural extension for current NDS users.

Because all authentication is performed through NDS, administrators do not have to maintain a multitude of access control and security information spread across multiple products and directories. As a result, BorderManager reduces the risk of error, which ensures a high level of security. In addition, with a single sign-on through NDS users can access all network resources to which they are authorized, regardless of their network entry point or the location of the resources. They can sign-on from a directly-connected LAN workstation, from a dial-up LAN workstation, from a remote VPN client over the Internet… from just about anywhere. Single sign-on means users have to remember only one password. They can quickly get to the resources they need, maximizing their productivity.

NDS-based authorization is far more secure than conventional TCP/IP security mechanisms. TCP/IP security is based on IP addresses or segments rather than on users. The resulting security is weak. For example, an employee whose workstation does not have access to a particular network resource can simply move to another employee's workstation that does have the desired access. Dynamic Host Control Protocol (DHCP) exacerbates the problem because each user's machine address changes dynamically, making identity-based management impossible. BorderManager with NDS, on the other hand, provides security that is user centric rather than machine or IP-segment centric. This allows administrators to establish security based on both resource identity and user identity. When a user logs in, access to a network resource is granted or denied based on the user's identity and access permissions rather than on the identity of the workstation from which he or she logs in.

BorderManager runs under NetWare® 5, the number 1 network for Internet-enabled businesses. To provide a complete solution, BorderManager includes NetWare 5 at no extra cost. Both BorderManager and NetWare 5 are backed by Novell and its more than 500,000 training and support professionals worldwide.

SECTION 2. BORDERMANAGER HIGHLIGHTS

BORDERMANAGER FIREWALL SERVICES

BorderManager implements access control components at all layers of the Open Standards Interconnection (OSI) model to provide rock solid protection. Each higher-level component provides additional security over the lower-level components. The components are integrated and work together to provide a secure environment. The components listed from the highest level to the lowest level are:

- *Application proxy*. BorderManager includes a number of application proxies, such as HTTP, FTP, Gopher, Mail, News, Real Audio/Video, and DNS. BorderManager also includes a generic TCP proxy and a generic UDP proxy to allow administrators to configure additional application proxies such as LDAP. The application proxies relay all data between user applications and Internet/intranet resources. The proxy examines information at OSI layer 7, the application layer. It looks not only at the address of a packet, but also at the entire context of the session in which the packet is being sent and applies content-based semantic access controls prior to relaying the data.

- Application proxies provide the highest level of protection, enhancing the protection provided by circuit gateways and packet filters. For example, once a circuit gateway creates a virtual pipe between a client and remote host, any application can run over that connection. The application proxy, however, can restrict sessions over the pipe based on application and even types of commands within an application.

- The HTTP application proxy supports Secure Sockets Layer (SSL) tunneling, allowing an encrypted path between the client and server to protect information from eavesdroppers and vandals.

- *Circuit gateway.* BorderManager provides two circuit gateways: a SOCKS gateway and the Novell IP Gateway. The SOCKS gateway includes SOCKS client and server v4 and v5 protocols. SOCKS support enables the BorderManager firewall to be configured as a component of a firewall solution, working in conjunction with firewalls from other vendors. BorderManager can be used in front of, within, or behind existing firewalls. SOCKS server support allows the BorderManager server to operate with universal SOCKS clients, providing strong cross-platform client support. SOCKS with SSL provides a VPN capability for NT, UNIX and NetWare clients.

The Novell IP Gateway includes both an IPX™/IP gateway and an IP/IP gateway which provides transparent authentication to BorderManager. The Novell IP Gateway allows both IPX and IP clients to access TCP/IP services. When an IPX or IP client requests a TCP/IP service (such as HTTP, FTP, Telnet, or Gopher) from a host inside or outside the firewall, the associated circuit gateway intercepts the request. It then consults NDS to verify that the user has the authorization to initiate the session. Access controls can restrict sessions based on protocol and by host address/domain name. The circuit gateway, which examines packet information at layer 5 of the OSI information model, provides a higher level of protection than just a packet filtering solution alone. The Novell IP Gateway uses native MS Winsock 2.0.

- *Network address translation.* BorderManager provides both dynamic and static IP and IPX network address translation (NAT) tables. The administrator configures the tables with public sets of IP addresses. BorderManager uses the tables to remap automatically the source address of the packet headed for a destination outside of the firewall. This address translation, which takes place at OSI level 3, hides the addresses of the internal network from the outside world for strong security. In addition, address translation relieves the administrator from the time-consuming and error prone task of managing IP addresses by dynamically and automatically mapping unregistered internal addresses to registered IP addresses. It can map up to 5,000 unregistered addresses concurrently per interface.

- *Packet filter*. The BorderManager packet filter, which operates at OSI layer 3, checks each packet against access controls. The filter checks source and destination host IP address to restrict access to and from certain IP hosts; source and destination IPX addresses to restrict access to and from certain IPX hosts; IP protocol/port to restrict access to certain Internet protocols and ports, such as HTTP, FTP, telnet, and Gopher; and IPX Protocol to restrict access to certain types of NetWare Core Protocol (NCP) requests.

BorderManager provides a stateful packet filter engine that looks not only at the address of a packet, but also at the entire context of the session in which the packet is being sent. This makes it far more effective in identifying suspicious packets. For example, a hacker could easily get through an address filter using address spoofing. But a hacker could not use address spoofing alone to get through the BorderManager packet filter. The hacker would also have to determine the entire context of the session in which the packet is being sent—a difficult if not impossible task.

For even more protection, the BorderManager firewall provides a set of application programming interfaces (APIs) that enable additional filters developed by third-parties to be integrated with the firewall. Novell partners will offer a variety of third-party filters, including anti-virus, Java, ActiveX, reporting, and MIMEtag. (For an up-to-date list of available filters, visit www.novell.com/bordermanager.)

In addition, BorderManager include a trial version of the CyberPatrol destination content filter that can deny outgoing Internet access to certain Web sites based on content, such as denying access to sites with sexually-oriented content.

One of the major problems with traditional firewalls, especially packet filters, is that although they can provide extremely tight security, setting them up is typically complex and difficult. As a result, administrators often make errors in setting up the firewall, which could cause security loopholes.

BorderManager simplifies firewall setup and administration setup with a simple sequence:

1. The BorderManager firewall automatically initializes to allow no traffic to pass through in either direction.
2. The administrator next configures the circuit gateways and application proxies to be used through the BorderManager Setup window.
3. The administrator then moves to the BorderManager Rules window and establishes easy-to-understand, high-level access rules for the circuit gateways and application proxies selected. BorderManager then uses the rules information to make the correct settings in the packet filter—automatically. This greatly simplifies the firewall setup process, eliminating a common source of security loopholes.

BORDERMANAGER VPN SERVICES

BorderManager provides VPN services that allow organizations to run private networks securely and economically over the Internet. BorderManager VPN allows a company to implement three types of virtual private networks:

- *Site to site*. A company can interconnect servers at two or more sites using the Internet as a link. In this way, independent LAN segments can be connected into a single cohesive WAN.

- *Client/server*. A company can allow LAN users, dial-up users, even cable modem users—running either IP or IPX protocol—to access VPN resources through a secure connection over the Internet. In this way, a company can give users secure access to the network resources they need, regardless of their location or the location of resources. Best of all—and this is unique to BorderManager VPN—they can access all resources from anywhere with a single sign-on.

- *Extranet*. A company can connect its corporate network with its business partners' networks into a single cohesive extranet using the Internet to link sites.

When implementing a VPN, it is essential to ensure that only authorized members of the VPN community are allowed to use it. In addition, it is necessary to ensure that all information transmitted over the VPN is safe from eavesdroppers and vandals, that is, the privacy and integrity of the information must be ensured. BorderManager authenticates all users through NDS to ensure that only authorized VPN community members are permitted to use the VPN. BorderManager VPN services employ security mechanisms based on open standards and established cryptographic techniques, such as IP SEC, RC2, RC5, DES, 3DES, and SKIP to ensure the privacy and integrity of information transmitted.

Performance and scalability are also important, especially for large organizations. BorderManager VPN supports symmetric multiprocessing (SMP), allowing it to take advantage of multiprocessing hardware to increase speed. To optimize performance further, BorderManager performs selective encryption, that is, it encrypts only the information sent to and from protected networks, as specified by the administrator. BorderManager employs maintenance traffic reduction techniques, such as header compression and efficient WAN routing updates, to deliver high bandwidth over the VPN. BorderManager can support up to 256 sites per tunnel and can service up to 1,000 dial-in users per server.

BorderManager supports a variety of standard tunneling, encryption, and key exchange mechanisms to provide a strong yet flexible security framework. It supports tunneling based on the field-proven IP relay mechanism using the IP SEC standard (RFC # 1825-1828). It supports the RC2, RC5, DES, and 3DES encryption algorithms. And it supports the SKIP (simple key exchange Internet protocol) standard to allow secure distribution of authentication keys.

Like the other BorderManager services, BorderManager VPN services are managed through NDS. This allows the administrator to manage the VPN, even multiple VPNs, from a single, centralized point to reduce administration costs.

BORDERMANAGER CACHE SERVICES

One of the major problems companies face in consolidating their many scattered internal LANs and integrating the resulting global network with the Internet is performance degradation. One of the major sources of this degradation is the low bandwidth of the WAN links used to interconnect LAN segments. Another source of performance degradation is the need to pass all information through one or more security firewalls, which can slow information transfer. BorderManager cache services enable companies to create high-performance global enterprise networks without sacrificing security. Because BorderManager Caching Services support open Internet standards, they can be used with Novell's intranet and Internet products—as well as with any browsers and web servers—in heterogeneous, multivendor environments.

BorderManager Cache Services are based on Internet Cache Protocol (ICP), a next-generation Harvest/Squid proxy cache research, which is fully compatible with first-generation CERN proxy caching. This advanced technology delivers superior performance in an open standards environment that supports HTTP, FTP, SSL, and Gopher protocols. Novell has optimized this technology for the NetWare platform. And NetWare itself is optimized for the network environment. As a result, its performance far surpasses that of application servers, general-purpose operating systems, such as NT and Unix, and other systems. BorderManager Cache Services can handle over 100,000 concurrent connections and over 6,000 connections per second. Using SPECWEB 96, BorderManager cache was rated at over 2,2000 operations per second, the fastest most scalable caching solution available.

With the advanced proxy caching technology employed in BorderManager Cache Services, organizations can achieve up to ten times improvement in performance. By caching data on a LAN-based proxy server, BorderManager Cache Services reduce traffic across the WAN—typically by more than 60 percent. That means organizations can realize 2-1/2 times as much throughput over the same physical WAN connection. As a result, they don't have to purchase expensive, higher bandwidth WAN connections.

Proxy caching is completely transparent to the client. That means users do not have to point their browsers at the BorderManager server to take advantage of caching services. Their request is directed automatically to the proper server. In addition, BorderManager caches information actively, that is, it anticipates the user's movement through Web pages, caching new information before the user actually requests it. Additional caching features further improve performance. For example, a batch download capability allows administrators to schedule downloading of information to nearby caches, such as during off-hours, to minimize network loading.

BorderManager Cache Services support three fundamental cache configurations:

- *Client acceleration (standard proxy caching)*. The cache is interposed between clients and the Internet. It intercepts requests from clients for Web pages and supplies the requested pages to the client, if cached, at LAN speed. This eliminates the delay incurred in going to the origin Web site and minimizes the traffic between the corporate network and the Internet. The proxy server makes requests of Web servers on behalf of intranet clients using appropriate protocols such as HTTP, FTP, and Gopher. It caches all Internet objects, including URLs, HTML pages, GIF files, and FTP files, to accelerate subsequent requests to the same object.

- *Web/FTP server acceleration (reverse proxy caching)*. The BorderManager server front-ends one or more Web or FTP servers and caches all static information belonging to the server(s). When a client requests information from a Web or FTP server, the request is diverted to the BorderManager proxy server. The proxy server supplies the cached pages to the client at high speed. Operating in this way, the proxy server greatly accelerates access. It also takes the request load off the Web and FTP servers, enabling the network to service more users with fewer servers. BorderManager Cache Services can provide acceleration for all vendors' Web and FTP servers—in any combination.

- *Network acceleration (ICP hierarchical caching)*. In this configuration multiple BorderManager servers are configured in a hierarchical (mesh) topology. When a miss occurs, the proxy cache contacts the other servers in the mesh to determine if any have the requested information cached. If so, the nearest proxy cache with the requested information forwards it to the requesting proxy cache which in turn forwards it to the requesting client. ICP hierarchical caching reduces the WAN traffic load significantly freeing up valuable bandwidth. In addition, because the requested information is sent from the nearest BorderManager server, network delays are minimized. This reduces user times and increases user productivity.

POLICY-BASED ADMINISTRATION

Administrators manage all BorderManager services through NDS. They control access through the use of access control list (ACL) rules stored in NDS. The policy rules can be applied to network resources, such as machines, and to users and groups. Control is flexible and includes restriction by protocol, site (URL), category (such as sex and violence), and time of day. Management is easy because administrators work with easy-to-follow, high-level rules and not by individual services.

Access control rules are distributed in NDS and are associated with individual users or groups rather then with machines. As a result, employees “take their access control with them” as they move about the network, always operating from the same access control rules, regardless of where they enter the network. Access control rules are also automatically replicated in NDS throughout the network to provide a high degree of fault tolerance.

The administrator can establish rules for individual NDS objects as well as for NDS containers. Rules are inherited through NDS containment, so the effective rule set is a composite that is built up from rules established for various NDS objects. The rule’s position in the list determines its priority of application relative to the other rules in the list. If a lower-priority rule (lower on the list) contradicts a higher-priority rule (higher on the list), the higher-priority rule supercedes the lower-priority one.

The top of the list contains rules defined on the BorderManager server through which the access request is coming. The next level contains the rules set for the BorderManager server’s container. From there, the priority works down to the root of the NDS tree. At the bottom of every list is a single default rule that cannot be deleted or modified. This default rule denies access to anything.

The administrator can add, delete, cut, copy, and paste rules. In addition, the administrator can change a rule’s position in the list to increase or decrease its priority.

AUTHENTICATION

Users may authenticate to BorderManager using any of four methods:

- *Novell IP Gateway*. Users can sign-on to the network using the Novell IP Gateway client to provide background authentication to NDS.

- *Web browser*. Users can sign-on to the network from any Web browser. In this case, BorderManager will spawn an HTML or Java sign-on screen when the user attempts to access a protected resource. (The login is performed over an SSL-secured link.)

- *VPN client*. Users can sign-on to the network from a BorderManager VPN client.

- *BorderManager Authentication Services*. Users can sign-on from any dial-in client and enter the network through the RADIUS protocols supported by BorderManager authentication services.

BorderManager authenticates all users through NDS. As a result users can access all network resources that they are authorized to access, regardless of the user’s location or the location of the resources—*all with a single sign-on*. This means users have to remember only a single user ID and password.

Because BorderManager authenticates all users through NDS, administrators can manage all access from a single, centralized point. This approach simplifies not only the addition of users, but also the deletion of users. For example, an administrator can immediately remove a terminated employee from the network by simply removing that employee's user object from NDS. This eliminates the need for the administrator to remove the user separately from each server or domain, which takes time and is error-prone. This could result in the employee retaining access rights to sensitive information long after he or she is terminated.

LOGGING, ALERTING AND REPORTING

BorderManager generates a variety of alerts that can notify the administrator of out-of-tolerance conditions in security, such as loading or unloading of security-sensitive NLMs, Ping flooding, SYN packet flooding, or CPU hogging. It also provides alerts on out-of-tolerance conditions in BorderManager components such as disk space shortage, memory shortage, ECB shortage, license errors, down ICP parent, and down SOCK server. By responding proactively to these alerts, administrators can head off problems before they result in network down time.

BorderManager also logs a wide variety of events, including security events such as attempted unauthorized access to protected network resources. (The events to be logged are specified by the administrator.) Logging uses standard log and text formats.

By examining the information contained in these logs, either directly or through selective reports, administrators can quickly detect suspicious situations, and react before they result in problems such as the compromise of sensitive information.

SECTION 3. TYPICAL DEPLOYMENT SCENARIOS

BorderManager can provide a wide range of solutions that enable companies to leverage Internet technologies, such as Web and FTP, in their enterprise networks. This section presents typical scenarios that illustrate the power and flexibility of BorderManager. Each scenario describes 1) a particular problem, 2) the deployment of the BorderManager server to provide a solution, and 3) the resulting advantages.

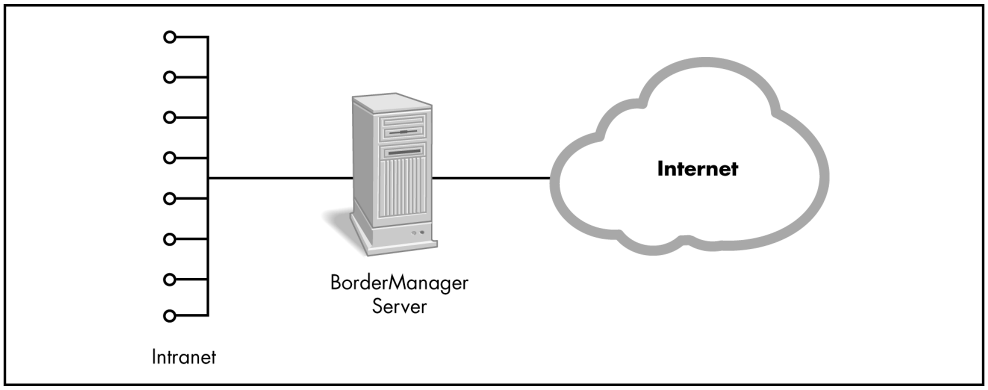
SCENARIO 1. CONNECTING AN INTRANET TO THE INTERNET

A company needs to connect its corporate network to the Internet to give its employees access to Internet resources such as the Web. It wants to ensure that the connection is secure from Internet hackers.

Figure 1 illustrates how BorderManager server is deployed to provide a solution.

Figure 1

Deploying BorderManager between the internet and a corporate intranet.



BORDERMANAGER ADVANTAGES

- Strong firewall security. BorderManager packet filter, network address translation, circuit gateways, and application proxies protect the internal network from break-in through the Internet.
- *High performance*. BorderManager forward proxy caching dramatically speeds Internet access for internal users.
- *Control of outgoing Internet access*. The BorderManager firewall and the CyberPatrol destination content filter allow the administrator to control outgoing Internet access by employees, restricting access based on a number of factors including site content, user profile, and time of day.
- *Control of inbound access from the Internet*. BorderManager's identity-based authentication allows the administrator to control inbound access to the intranet by users on the Internet.
- *Complete software solution*. BorderManager includes all you need to connect to the Internet—in a single package: a runtime version of the NetWare 5 operating system, routing capability, and remote access.

SCENARIO 2. ADDING IDENTITY-BASED CONTROL BEHIND AN EXISTING FIREWALL

A company already has another vendor's firewall installed but now wants to enhance protection of its intranet.

Figure 2 shows how the BorderManager server deployment to address this requirement.

BORDERMANAGER ADVANTAGES

- *Identity-based control*. Because it performs authentication through NDS, BorderManager permits the administrator to establish identity-based access control to the intranet rather than the address-based control provided by the existing firewall.
- *High performance*. BorderManager forward proxy caching dramatically speeds Internet access for internal users and eases the bottleneck at the existing firewall.
- *Control of outgoing Internet access*. The BorderManager firewall and the CyberPatrol

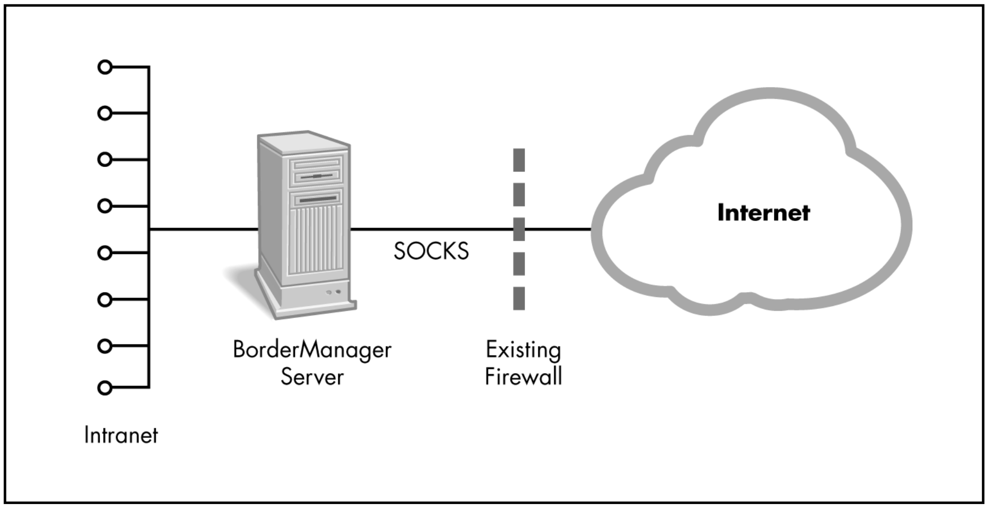


Figure 2

Deploying BorderManager to enhance protection of the intranet.

destination content filter allow the administrator to control outgoing Internet access by employees on a per user basis.

SCENARIO 3. CREATING PROTECTED INTRANET SEGMENTS

A company needs to create a protected network segment that will secure certain intranet Web and FTP servers that contain sensitive information such as financial and engineering information. The information on the servers is dynamic and requires frequent update. The servers belong to multiple departments, such as human resources and engineering. The information must be protected from unauthorized access by internal employees as well as from Internet hackers.

The existing firewall protects the servers from Internet hackers. However, it does not protect them from unauthorized access by users who are inside the firewall. In an attempt to protect the servers, the company has placed them in a secure room and uses the security mechanisms provided with the Web and FTP server software. This presents two problems. First, the Web and FTP server security mechanisms do not provide a high level of security. In addition, to update the contents, department personnel must submit the updates to the IT personnel who control the servers and all information posted on them. The procedure complicates the update process considerably and introduces delays. The departments would prefer to have the servers located in their area to facilitate content update.

To solve the problem, the company deploys the BorderManager server between the Internet firewall and the servers to be protected. This creates a secure network segment. (See Figure 3.)

BORDERMANAGER ADVANTAGES

- *Strong protection from internal break-in.* The BorderManager server protects the network segment from unauthorized access by intruders who are inside the firewall and increases protection from Internet hackers. It accomplishes this through the user identity-based control provided by NDS.

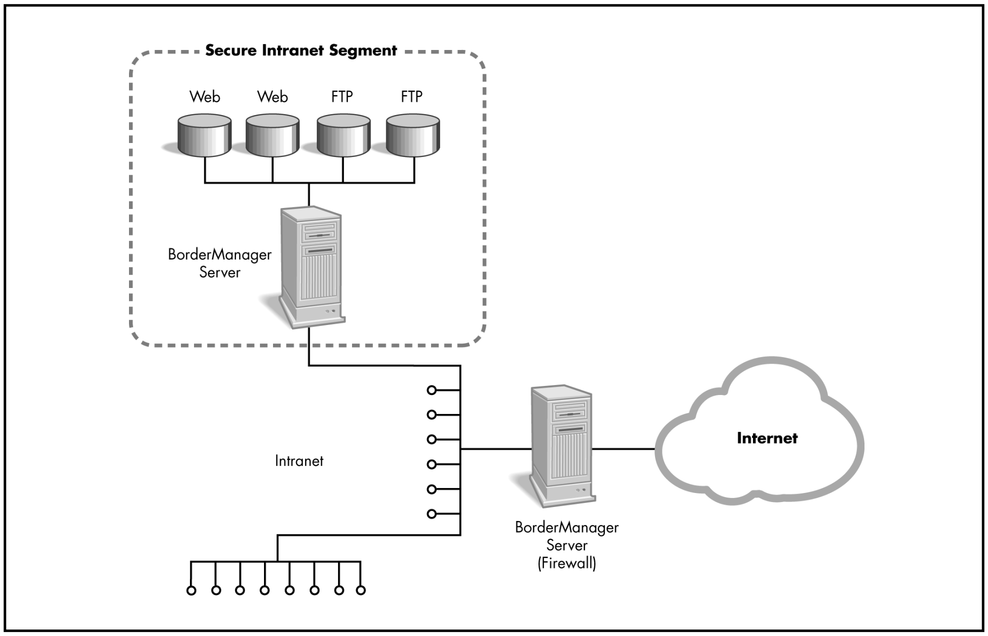


Figure 3

Protecting intranet segments.

- *High performance*. The BorderManager server's forward proxy cache dramatically speeds access to Web pages and FTP files. In addition, the BorderManager server can be configured to provide reverse proxy caching to the Web and FTP servers it front-ends.

- *Easier management*. With BorderManager, the servers can be placed right in the responsible departments' areas, enabling department personnel to update the servers directly without IT involvement. This simplifies network management considerably.

- *Single sign-on*. Authenticating through NDS enables people to use a single sign-on to access all network resources for which they have authorization, including those on secure intranet segments.

SCENARIO 4. IMPLEMENTING A VIRTUAL PRIVATE NETWORK

A company needs to connect three branch offices located at three separate sites into a single enterprise network using the Internet to provide the inter-site links. (A similar scenario would be that a company wants to implement an extranet that connects its headquarters site with the sites of two business partners.

As Figure 4 shows, three BorderManager servers are deployed. In addition, BorderManager VPN clients can be deployed as needed for remote users who need to access critical information over the Internet in a secure manner.

BORDERMANAGER ADVANTAGES

- *Strong security*. The BorderManager VPN service provides encryption tunneling and authentication to control access and protect the privacy of information transmitted over the Internet.

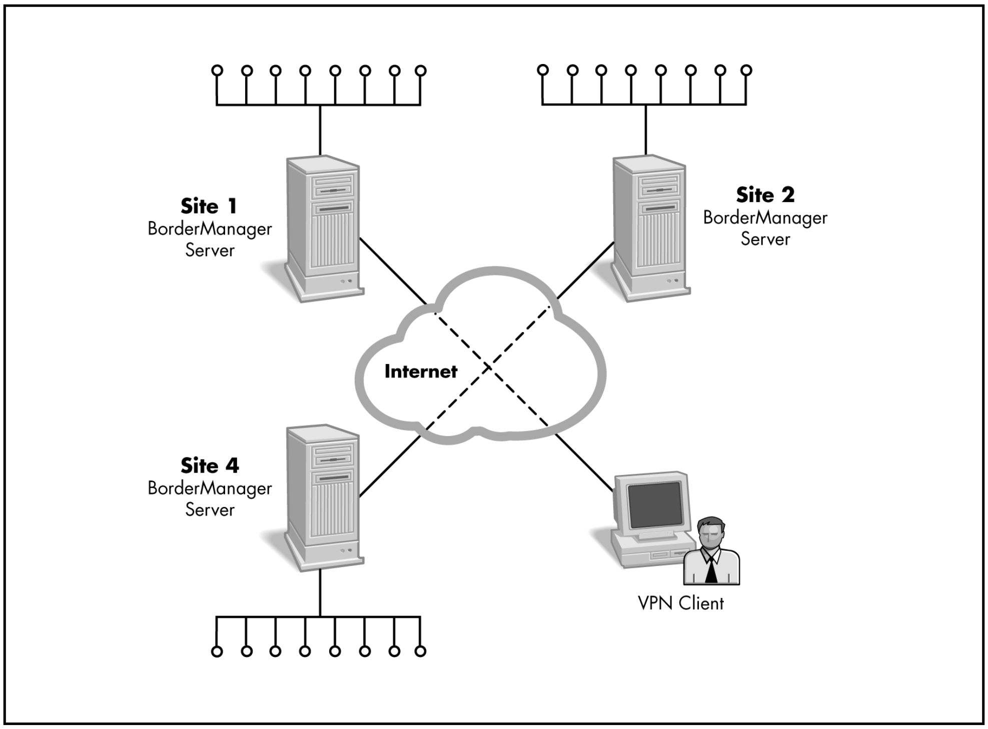


Figure 4

Implementing a VPN.

- *High performance*. BorderManager has a number of features, such as selective encryption, that enhance performance.

- *Centralized management*. The entire VPN network is managed centrally and from the same point as the other BorderManager services. This simplifies network management significantly and reduces the cost of network ownership.

- *High level of scalability*. BorderManager VPN services can support even the largest corporations—with up to 256 sites per tunnel and up to 1,000 dial-in users per server.

SCENARIO 5. INCREASING WEB AND FTP SERVER PERFORMANCE

A company is generating rapidly increasing traffic on its Web and FTP sites. To keep up with the demand, the company needs either to add additional Web and FTP servers or to accelerate its existing servers in some way. Acceleration is by far the more economical solution because it allows the same number of Web and FTP servers to handle more users, saving the acquisition and management costs of additional servers.

In this case, a BorderManager server is deployed in a reverse proxy caching configuration as shown in Figure 5.

BORDERMANAGER ADVANTAGES

- *Increased performance*. BorderManager reverse proxy caching can improve Web and FTP server performance up to tenfold.

- *Lower cost*. The BorderManager reverse proxy server takes the request load off the Web and FTP servers, enabling the network to service more users with fewer Web and FTP servers. The result is a reduction in hardware and management costs.

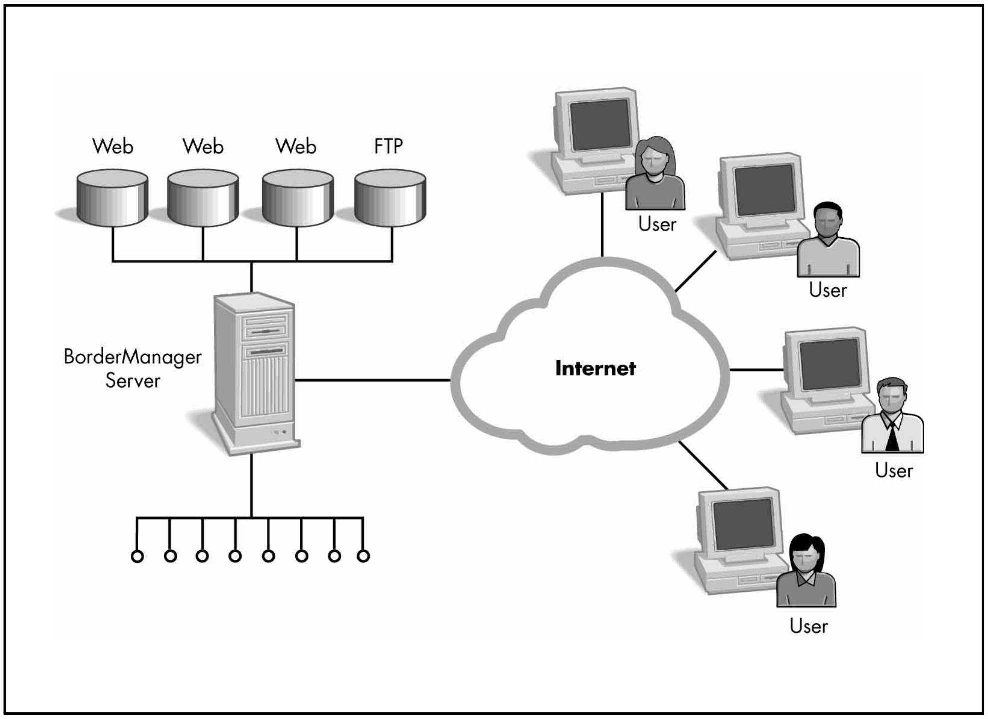


Figure 5

Boosting Web and FTP server performance.

- *Increased security*. The BorderManager server isolates the Web and FTP servers from the network, increasing their resistance to unauthorized access, even from inside the firewall.

- *Simplified management*. The administrator can manage security for all Web and FTP servers in a consistent fashion from a single point, regardless of the Web and FTP server platforms used. This greatly simplifies access management.

- *Single sign-on*. Because BorderManager authenticates through NDS, users can access all front-ended Web and FTP servers with a single sign-on.

SCENARIO 6. INCREASING INTRANET WEB SERVER PERFORMANCE OVER WIDE AREA NETWORKS

A large company has facilities scattered all over the world. The sites have LANs that are all connected through 56 kilobyte per second WAN links. Users in the international offices often access Web servers at the U.S. headquarters to keep updated on company information. Due to the low bandwidth of the WAN links and the large number of links between the user and the Web server, information access can be extremely slow.

In this case, BorderManager servers are deployed in the hierarchical proxy caching configuration in Figure 6. (The figure shows only a portion of the entire worldwide network.)

BORDERMANAGER ADVANTAGES

- *Increased performance*. BorderManager hierarchical proxy caching allows first-time access and cache-miss data to be fetched from the optimal nearby proxy server, without going all the way to the origin Web server. That reduces the number of WAN links between the user and the target Web server, dramatically increasing performance.

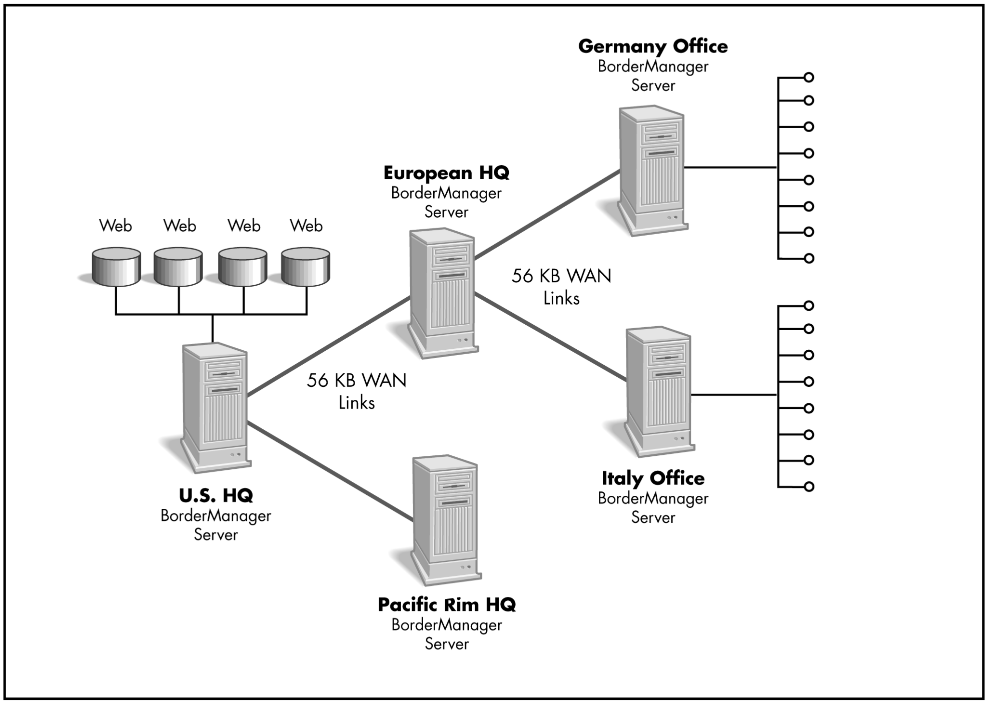


Figure 6

Increasing Web server performance over a WAN.

- *Lower cost*. Because the BorderManager reverse proxy servers takes the request load off the Web servers, a given number of Web servers can handle many more users. In addition, because it makes more efficient use of available bandwidth, it reduces the need to add expensive links to handle an increasing user load.

- *Easier management*. All BorderManager servers can be managed from a single, central point, greatly simplifying management.

SCENARIO 7. PROVIDING UNIVERSAL, SECURE DIAL-UP ACCESS TO REMOTE USERS

A company has employees scattered all over the world. Many of them are mobile computer users who dial into the Internet through an Internet service provider. They need access through the Internet to network resources that are also scattered around the world. The company wants to ensure that employees can access all the resources they are authorized to use quickly and simply—with a single sign-on.

In this case, the BorderManager server is deployed as shown in Figure 7.

BORDERMANAGER ADVANTAGES

- *Single sign-on*. BorderManager allows remote, dial-in users to access any resource they are authorized to use with a single sign-on.

- *Easier management*. With BorderManager and NDS, the administrator can manage all remote, dial-in users through a single point of administration. Without it the administrator would have to configure and manage multiple access servers and their associated user databases.

SECTION 4. INSTALLING AND CONFIGURING BORDERMANAGER

This section takes you through step-by–step instructions for installing and configuring BorderManager.

NOTE: Prior to installing BorderManager on the server: NetWare 5 must be installed and running and TCP/IP and routing must be configured and working. It is recommended that you install a minimum of 2 network interface cards (1 public and 1 private). (NetWare 5 is included with BorderManager for those users who do not already have NetWare 5 installed.)

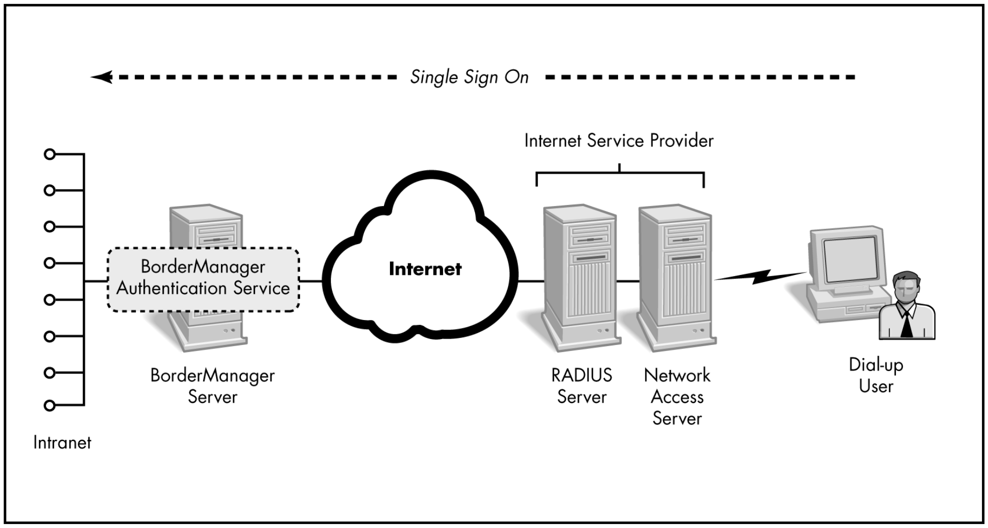


Figure 7

Single sign-on, universal access for remote users.

INSTALLING BORDERMANAGER ON THE SERVER HARD DISK

In this section , you will install BorderManager on the hard disk of the server on which BorderManager will run.

To install BorderManager:

1. Insert the BorderManager CD-ROM into your CD-ROM drive.
2. Click the Novell Start button.
3. Click the Install button.
4. Click the New Product button.
5. Click the Browse button and select the path to the CD-ROM drive in which the BorderManager CD-ROM is inserted.
6. Click the OK button. In response, the BorderManager install program will launch the BorderManager install wizard which will guide you through the install process.
7. The first dialog window will require you to establish the path to the license file. The license file, named Border3.mlf is on the CD-ROM. The install wizard will complete copying the BorderManager files to your hard disk.
8. Login to NDS as Admin with rights to the root of the tree
9. Specify the Public and Private interfaces
10. There are 2 checkboxes under the interface list. Check the box Set filters to secure all public interfaces only if you have 1 or more public interfaces. Check the box Enable HTTP proxy for all private interfaces.

NOTE: When you check Enable HTTP proxy, a screen will display on which you can configure access control.

1. Enter the DNS domain name.
2. Enter the IP addresses of the DNS servers.

This completes the install process.

INSTALLING THE BORDERMANAGER NETWARE ADMINISTRATOR SNAP-IN

BorderManager includes a snap-in to the NetWare Administrator console. The snap-in adds three properties pages to the NetWare Administrator main display: BorderManager Setup, BorderManager Alerts, and BorderManager Rules.

NOTE: Before installing the snap-ins, you must have already run NetWare Administrator at least once to ensure that it has registered with the Windows operating system. Also, be sure that the server on which you are installing the snap-ins is on the same NDS tree as the BorderManager server.

To install the BorderManager “snap-in” for NetWare Administrator 32 and complete the initial configuration:

1. Login to the BorderManager server.
2. Run SYS:PUBLIC\BRDMGR\SNAPINS \SETUP.EXE. This activates the BorderManager NetWare Administrator snap-ins install wizard.
3. Follow the step-by-step instructions of the install wizard.

NOTE: Be sure that the target directory to install the snap-ins resides in the proper NDS tree and contains NWADMN32.EXE.

1. Click Launch NWADMN32.

This completes the installation of the snap-ins and launches NetWare Administrator.

1. Open the Properties of the BorderManager Server object.
2. Select the BorderManager Setup properties page. When asked to set the default outgoing rule, select Deny.

3. From the BorderManager Setup screen, select the button IP Addresses. Configure the IP Address and click the check box for Usage Type (Private. Click OK.

CONFIGURING BORDERMANAGER FIREWALL SERVICES

This section will take you through the step-by-step procedures for configuring BorderManager firewall services.

CONFIGURING THE CIRCUIT GATEWAYS

This section will guide you through the process of configuring the circuit proxies you will use. A later section will guide you through the process of establishing the access rules for the circuit proxies you have configured.

ENABLING THE IP GATEWAY SERVER

1. Run NWAdmin32 and double-click your server object.
2. Click on the BorderManager Setup page option.
3. Click the Gateway tab.
4. Check the checkbox for the IPX/IP and/or IP/IP Gateway.
5. Click Details.
   a. Select Logging Format Common. Set the Log Level to 1.
   b. Keep the default of port 8225.
   c. Click on OK to save the changes.
6. Click on the OK action button at the bottom of the page. The IPX/IP gateway NLM’s will load at the server.

ENABLING THE IPX/IP GATEWAY CLIENT COMPONENT

NOTE: The following steps assume you have Client32 installed with IPX only.

1. Right-Click Network Neighborhood and choose Properties.
2. Click on the Add action button.
3. Click on Service for the Network Component and then click on the Add action button.
4. In the Manufacturers box, click on Novell and from the Network Services box, click on Novell IP Gateway and click on OK.
5. Click OK to Close the Network Properties box. You will asked for the location of the Client32 install directory (on the CD it’s cd:\products\win95\ibm_enu).
6. Click Yes to restart your computer.
7. Upon login, you will be presented with the Novell IP Gateway dialog box to enable services. Select Enable Gateway for IPX-to-IP and click OK.
   a. You may receive the message “WinSock is in use. Gateway will be enabled when you reboot.” Click OK.
   b. Cancel login and reboot to enable the Gateway.
8. Login to your server as Admin.

TESTING THE IPX/IP GATEWAY

1. With the IPX/IP gateway client component enabled at your workstation, start a Netscape browser session.
2. Attempt to access a Web Site. If you successfully accessed the Web server’s home page, the gateway was configured correctly.
3. Click on the Start Button from the Windows 95 desktop.
4. Click on the Novell folder and highlight the IP Gateway folder.
5. Click on the Switcher Icon, this is where you could disable the gateway.
6. Click on Cancel, to exit back to desktop.

CONFIGURING BORDERMANAGER APPLICATION PROXIES

This section will guide you through the process of configuring the application proxies you desire to use. A later section will guide you through the process of establishing the access rules for the application proxies you have configured.

Follow the procedures outlined below for the application proxies you wish to configure.

NOTE: You already configured the HTTP application proxy as part of the BorderManager install process.

CONFIGURING THE INDIVIDUAL PROXIES

For each application proxy you wish to configure, perform the following steps:

1. Start NWAdmin32, making certain that you have already configured your client with BorderManager snap-in DLLs.
2. Double click on your BorderManager server object to bring up the Details page.
3. Click on the Application Proxy tab.
4. Click on the BorderManager Setup tab to display the various proxies and gateways.
5. Click on the square next to the application proxy you wish to enable.

NOTE: As you enable each application proxy, you must also configure it as follows:

1. Click on the Details button, this will bring up the configuration options for the proxy you just checked.

The following shows the configuration settings to use for each proxy:

HTTP

1. Click on the Logging tab, and enable the Common Logging Format
2. Click on OK, once you close out of the BorderManager server object, the HTTP Proxy will be enabled.

FTP

1. Append a domain name to the Anonymous FTP Email Address.
2. Place a checkmark next to Enable User-based Authentication.
3. Place a checkmark next to Enable Indexed Format Logging.
4. Click on OK, once you close out of the BorderManager server object, the FTP Proxy will be enabled.

NOTE: In the FTP Proxy, if you have usernames, or passwords that contain the "$" character, then change the Username/Password Separator. If you enable the User-based Authentication, to FTP somewhere you would type in: FullNDSLoginID$anonymous$ftp.novell.com as the username, and the password would be: NDSpassword$ftppassword.

MAIL

1. For the Primary Mail Domain Name enter acme.com (this will cause all mail going through the Mail Proxy to have acme.com as the domain name – leave the field blank, and whatever is in the From headers of the mail message will be used)
2. For the Internal Mail Server Name enter mail.acme.com (this is the internal mail server MX record address)
3. For the POP3 Mailer Server Name enter mail.isp.com (this is the POP3 server located on the Internet that the Mail Proxy should send the outgoing mail to)
4. Enable Indexed Format Logging.
5. Click on OK, once you close out of the BorderManager server object, the Mail Proxy will be enabled.

NOTE: If you are in an environment with multiple domain names, then you would not specify the Primary Mail Domain Name. Mail data is not cached on the Mail proxy.

NEWS

1. In the Primary News Domain Name, enter the domain that you want news messages to look like they are coming from.
2. Enter the News Server Name or News Server IP Address of the internal news server (if you don't have an internal news server leave this blank)
3. Enter the Hostnames or IP Addresses of any Public (External) News Servers that news queries should be retrieved from (you need at least 1 news server listed for the News proxy to work)
4. Enable Indexed Format Logging.
5. Click on OK, once you close out of the BorderManager server object, the News Proxy will be enabled.

NOTE: News articles are not cached on the News proxy.

REAL AUDIO

1. Enable Indexed Format Logging.
2. Click on OK, once you close out of the BorderManager server object, the Real Audio Proxy will be enabled.

NOTE: You need to configure Real Audio to point to the proxy server, which the default port is 1090. No Real Audio data is cached.

DNS

1. Click on Enable Indexed Format Logging.
2. Click on OK, once you close out of the BorderManager server object, the DNS Proxy will be enabled.

NOTE: Workstations need to be configured so that their primary DNS server is the IP address of the DNS proxy server. The DNS proxy will cache DNS requests.

INSTALLING AND CONFIGURING BORDERMANAGER VPN SERVICES

This section guides you through the process of installing and configuring BorderManager VPN services. It describes the configuration of the BorderManager master and slave servers, and the installation and configuration of the BorderManager VPN client. A later section describes setting up the access rules for the VPN services you have configured.

CONFIGURING THE MASTER SERVER

1. From your server console, type LOAD NIASCFG and press <Enter>. (If prompted, <Enter> to continue and transfer LOAD and BIND statements to NETINFO.CFG.)
2. Select Configure NIAS and press <Enter>.
3. Select Virtual Private Network and press <Enter> this automatically loads VPNCFG.NLM.

NOTE: If this is the first server in the NDS tree to be configured as a VPN server, you are prompted to log into the tree. The login you use must have sufficient rights to the root directory (administrator rights to the root directory) to extend the NDS schema and define the VPN attributes.

1. Select Master Server Configuration option and press <Enter>. Confirm and Select Continue <Enter>.
2. Configure the IP addresses.
   a. In the public IP address field, type in the IP address of your server. Note: If you were setting this up in a real

environment, you would have two network interface cards (NICs), one being your public interface and the second your private interface, your public address would be your WAN connection interface.

   b. In the public IP mask field, enter the subnet mask of the server. (255.255.255.0).
   c. In the VPN Tunnel Address field, enter in 155.151.239.X, where "X" stands for the last 3 digits of your server's IP address. For Lab purposes this can be any IP address, your slaves will need to know the Virtual IP address you use and will have to use the same one.
   d. Note: This can be any local IP address within the corporate network.
   e. In the VPN Tunnel IP Mask field, enter the subnet mask. Type in "255.255.255.0", for lab purposes. In real situations, you would type in the subnet mask of the corporate network.
   f. Press <ESC> and choose Yes to save changes.
   g. Press <Enter> to continue.

3. Generate Encryption Information for the Master.
   a. Select Generate Encryption Information at the Master Server Configuration menu.
   b. Enter up to 255 characters for the random seed. This can be any combination of numbers and letters. (KEEP IT SHORT in demonstrations! This will save time when generating the encryption information.)
   c. Press <Enter> until you see the message "Generated the Encryption Information Successfully".
   d. Press <Enter> to continue. (VPN attributes/schema extensions are added.) Press <Enter>. You will see a message that the server was updated successfully in NDS. Press <Enter> to continue.
4. Copy the master encryption information file (MINFO.VPN) to a formatted diskette.
   a. Select Copy Encryption Information and press <Enter>.
   b. Enter the path in which you want to save the master encryption file. In this case, as well as most often, the path is going to be "A:/". Press <Enter>. Note: The same MINFO.VLM will be used for every slave server.
5. Give the diskette to the Slave Server. Note: Each slave server can use the same diskette.
6. Select Authenticate Encryption Information and press <Enter>.
   a. Write down the Message Digest. <Enter> to Continue.
   b. <Esc> to go back to Main Menu. You will see a message VPMASTER.NLM loaded. <Enter> to continue.
7. At this time you will wait until the slave configuration is complete to continue. Once the slave configuration is started, you will be asked to verify "out of band" certification that you are who you say by the Authenticated Encryption Information.
8. At this time you will wait until the slave configuration is complete to continue. Once the slave configuration is started, you will be asked to verify "out of band" certification that you are who you say by the Authenticated Encryption Information.
9. When the Slave administrator contacts you, you will need to Authenticate.

a. Select Authenticate Encryption Information and press <Enter>.

b. Repeat the numbers to the Slave, who will verify that these are the numbers he holds also. If all agree, press <Enter> and the <Esc> to the VPN Server configuration menu.

Exit NIASCFG. Press <Esc> at the VPN Server Configuration Menu. At the exit menu select <Yes>. Press <Esc> at the Select Component to Configure. Press <Esc> at the NIAS Options Menu. At the exit menu select <Yes>.

CONFIGURING THE SLAVE SERVER

1. From your server console, type LOAD NIASCFG and press <Enter>.
2. Select Configure NIAS and press <Enter>.
3. Select Virtual Private Network and press <Enter> this automatically loads VPNCFG.NLM.

NOTE: If this is the first server in the NDS tree to be configured as a VPN server, you are prompted to log into the tree. The login you use must have sufficient rights to the root directory (administrator rights to the root directory) to extend the NDS schema and define the VPN attributes.

4. Select Virtual Private Network option and press <Enter>.
5. Select Slave Server Configuration option and press <Enter>.
6. Configure the IP address for the Slave server.

   a. Select the Configure IP Addresses menu option and press <Enter>.

   b. In the public IP address field, type in the IP address of your server. Note: If you were setting this up in a real environment, you would have two NICs, one being your public interface and the second your private interface, your public address would be your WAN connection interface.

   c. In the public IP mask field, enter the subnet mask of the server. (255.255.255.0).

   d. In the VPN Tunnel Address field, enter in 155.151.239.X, where “X” stands for the last 3 digits of your server’s IP address. For Lab purposes this can be any IP address, you will need to know the Virtual IP address the Master slave used and will use the same network.

   e. In the VPN Tunnel IP Mask field, enter the subnet mask. Type in “255.255.255.0”, for lab purposes. In real situations, you would type in the subnet mask of the corporate network.

   f. Press <ESC> and choose Yes to save changes. Press <Enter> to continue.

7. Generate Encryption Information for the Slave.

   a. Select Generate Encryption Information at the Slave Server Configuration menu.

   b. You will then be prompted for the MINFO.VLM file, put the diskette from the Master in to the Server’s A: drive, and press <Enter>.

   c. A message screen will appear with a HEX code. This is the code that verifies that you received this file from your Master Server. Contact your Master Server administrator and repeat the numbers to verify that they are the same. If so press <Enter> to continue.

   d. Enter up to 255 characters for the random seed. This can be any combination of numbers and letters. You don’t need to remember this, so it can be anything. You do not use the same seed as the master.

   e. Press <Enter> until you see a message, "Generate the Encryption Information Successfully".
   f. Press <Enter> to continue. This will update the VPN table and load the VPSLAVE.NLM. Press <Enter>. You will see a message that the server was updated successfully in NDS. Press <Enter> to continue.
   g. Copy the slave encryption information file (SINFO.VPN) to a formatted diskette. You can rename this file to any name, the Master Server will just need to know what the file name is.

8. Select Copy Encryption Information and press <Enter>.
   a. Enter the path in which you want to save the master encryption file. In this case, as well as most often, the path is going to be "A:/". Press <Enter>.
9. Give the diskette to the Master Server.
10. Select Authenticate Encryption Information and press <Enter>.
11. At this time you will wait until the Master Slave is done configuring the Slaves. Once the slave configuration is started, you will be asked to verify "out of band" certification that you are who you say by the Authenticated Encryption Information.
12. When the Master administrator contacts you, you will need to Authenticate.
13. Select Authenticate Encryption Information and press <Enter>.
14. Repeat the numbers to the Master, who will verify that these are the numbers he holds also. If all agree, press <Enter> and the <Esc> to the VPN Server configuration menu.
15. Exit NIASCFG. Press <Esc> at the VPN Server Configuration Menu. At the exit menu select <Yes>. Press <Esc> at the Select Component to Configure. Press <Esc> at the NIAS Options Menu. At the exit menu select <Yes>.

ADDING SLAVE SERVERS TO THE VPN TABLE

Perform the following steps for each slave server you need to add to your VPN.

1. Log in to your server as Admin.
2. Double-click the NWAdmin32 program icon on your desktop.
3. Double-click your server's icon. Select BorderManager Setup.
4. Click the VPN tab. Double-click VPN Server Configuration. You will see a table consisting of VPN members. The Master Server will be the only entry.
5. Click on the Add button, which is the button next to the title of VPN Members.
6. It will bring up the "Open" box to browse for the SINFO.VLM file. Type in A:\SINFO.VLM in the file name box.
7. This will read the information and the Slave configuration to your table. Once this added, it will go out to synchronize the VPN sites.

CHECKING VPN STATUS

1. Use NWADMIN32 and double-click your server object.
2. Select the VPN tab.
3. Double-click VPN Server Configuration.
4. Click on the Status action button. This will bring up the Synchronization Status. You should see the members of your VPN and under status you will see the status of your VPN. Options:

   a. Being Configured - The server still needs to receive the newest topology and encryption information.
   b. Up-to-Date – The last server update with the newest topology and encryption information completed successfully.
   c. Being Removed – The server is being removed from the VPN.
5. Select a VPN member. Click on the Audit Log action button. Click on the Help action button to go over the options from this page. When done, click on Close action button.
6. Click on the Activity action button. Click on the Help action button to go over the options from this page. When done, click on the Close action button.
7. Click on the OK action button. This will exit you to the VPN Members page.
8. Click on Control Options action button. Click on the Help action button to go over the option for this page. When done, click on the OK action button to exit.
9. Double-click on your server entry in the VPN table. The top part of the page is a table where you can enter any static routes that this server may know about. The bottom of the page are options for your VPN server. The Key Change Interval is set to 1000. This parameter specifies how many packets are pass through the encrypted tunnel before the encryption key is changed. The number of packets that pass through the tunnel before the key changes is a random value between 75 and 100 percent of the entered value. If this value is low you will notice a performance hit.
10. Click on the OK action button to exit to the main VPN page.
11. Click on the OK action button to exit to NWADMIN.

INSTALLING THE VPN CLIENT

NOTE: Make sure that Dial-up networking and the MS ISDN accelerator pack 1.1 are installed prior to installing the VPN client.

During file copies click <Yes> to keep the newer files when version conflicts are reported.

1. Run SETUP.EXE from path: ….cd_image\border30\public\brdrmgr\vpn
   a. <Next> to pass the Welcome Screen.
   b. <Next> to pass “VPN Client Install program will…”

Note: At this point you MAY see a message such as “For this install to proceed you will need to install Microsoft ISDN Accelerator Pack 1.1…” If so,

   a. Click <Next> to continue past the message. <Yes> to “Are you sure?” <Yes> to accept license.
   b. You will see a message referring you to the setup directions, Click <OK> and <Next> to proceed.
   c. After files copy, you will be prompted for the Client 32 disks. Browse to the client directory on the hard drive.
   d. You will see a message confirming the Novell VPN Adapter has been installed. Click <Next> to continue.

NOTE: At the point, if you do NOT have Dial-Up Networking installed you will be prompted through the installation.

1. Create a New Connection in Dial-Up Networking.
   a. Type Master VPN Server for the name of the computer you are dialing and Click <Next> to continue.

   b. Fill in the area code and phone number. Click <Finish>.
   c. Select your new connection and from the dialog menu select File (Properties.
   d. Select the Server tab and set the Type of Dial-Up Server to Novell Virtual Private Network.
   e. Close the Dial-Up Networking window.
2. Choose the type of dial-up connection
   a. Select Direct. (Indirect requires the DNS name and IP address of the VPN Server.)
   b. <Next> to continue.
3. You will be prompted to read the readme file. There is no readme file in this build.
4. Click <Yes> to restart and Finish.

CONFIGURING BORDERMANAGER CACHING SERVICES

This section guides you through the process of configuring BorderManager caching services.

NOTE: BorderManager has automatically configured forward proxy caching during the install process.

CONFIGURING WEB SERVER ACCELERATION

A single BorderManager accelerator server can represent several Web servers. Therefore, an access plan that uses server acceleration typically places BorderManager servers on the same segment as the Web servers they represent. This enables traffic associated with caching Web objects between the Web servers and the BorderManager server to be concentrated on a single, dedicated, high-bandwidth segment.

1. In NetWare Administrator, double-click the server icon for the reverse proxy server.
2. Click the BorderManager Setup page button.
3. Select the Acceleration tab.
4. Check the HTTP Acceleration checkbox.
5. Click the Details button.
6. Click the Add Accelerator button.
7. In the Accelerator Name type the IP Address or name of your BorderManager server.
8. Click the Add Webserver button. Add name of web server to accelerate (i.e. www.novell.com).

Click the Add Proxy IP Address button. Select the interface of your server to serve as the accelerator.

To test, from Netscape, open the IP or Host Name of your server and see if the web page you accelerated is shown.

CONFIGURING FTP SERVER ACCELERATION

1. In NetWare Administrator, double-click the server icon for the reverse proxy server.
2. Click the BorderManager Setup page button.
3. Select the Acceleration tab.
4. Check the FTP Acceleration checkbox.
5. Click the Details button.
6. Click the Add Accelerator button.
7. In the Accelerator Name type the IP Address or name of your BorderManager server.
8. Select the Proxy IP Address to use for FTP acceleration
9. To test, from Netscape, open the IP or Host Name of your server and see if the root directory of the FTP server is opened.

CONFIGURING ICP HIERARCHICAL CACHING

1. Double-click the proxy server.
2. Select the BorderManager Setup page.
3. Click the Application Proxy tab.
4. Select the HTTP Proxy service and click Details.

5. Click the Cache Hierarchy Server tab and configure the ICP server.
6. Select the Enable ICP Server check box.
    a. Enter the ICP listening port number.
    b. Add a multicast IP address, then click OK.
    c. Add a hostname or IP address for the access control list, then click OK.
7. Click the Cache Hierarchy Client tab and configure the ICP client.
    a. Select the Enable Cache Hierarchy Client check box.
    b. Enter the ICP neighbor timeout.
    c. Click and specify one or more neighbors, then click OK.
    d. Deselect Must Only Forward Through Hierarchy if you want the proxy server to fetch the requested object directly from the origin server.
    e. Click and enter a unicast address or name and port number for the multicast responder list, then click OK.
8. Click the Cache Hierarchy Routing tab and specify the following information.
    a. Whether a URL's home site is used as a peer cache (not recommended).
    b. Click and enter the local domain name for origin servers that are in close proximity, then click OK.
    c. Click and enter a stop pattern, then click OK.
    d. Click OK.

CONFIGURING BATCH DOWNLOADS

1. Start NWAdmin32, making certain that you have already configured your client with BorderManager snap-in DLLs (run \public\brdrmgr\snapins\setup.exe).
2. Double click on your BorderManager server object, bring up the Details page.
3. Click on the BorderManager Setup tab, displaying the various proxies and gateways.
4. Click on the Application Proxy tab.
5. Highlight either HTTP Proxy, or FTP Proxy.
6. Click on the Caching button.
7. In the Caching page click on Schedule Download tab.
8. Put a check make next to Enable Scheduled Downloads.
9. On Download List, click on the new button (next to the X), bringing up the Scheduled Download page.
10. Make certain that the download is enabled but checking Enable this particular download.
11. Enter the HTTP URL you want to schedule, make certain to include http://.
12. Configure how many Levels to download you want.
13. Place a check mark next to Follow links to other hosts if you want the batch download to traverse other machines.
14. Configure any other options as far as Maximum Requests, Objects, and Data that you see fit.
15. Click on the Frequency tab, which brings up the scheduling options.
16. Click on One time only if you want to perform the scheduled download only once.
17. Click on Once a day at to repeat the scheduled download every day (or Only on selected days of the week) at a particular time start time.
18. Click on Daily from to repeat the schedule download everyday (or Only on selected days of the week), but with the flexibility of having a starting time and ending time for the download.
19. Click on OK to return back to the Caching page.

20. Click on OK to return to the BorderManager Setup page.
21. Click on OK, once you close out of the BorderManager server object, the Batch Downloads Proxy will be enabled.

NOTE: From the server, on the Proxy Console you can start a site download by selecting option #21 Site Download Options.

SETTING UP ACCESS RULES

This section will guide you through the set up of the access rules for network resources.

ENABLING BORDERMANAGER ACCESS RULES

1. Log in to your server as Admin.
2. Double-click the NWAdmin32 program icon on your desktop.
3. Double-click your server's icon.
4. Click on the BorderManager Setup tab.
5. Click on the Enforce Security box in the lower left-hand corner and click on OK.

DENYING ACCESS BASED ON AN NDS OBJECT (USER, GROUP, CONTAINER)

1. Double-click on your BorderManager server object.
2. Select the BorderManager Access Rules Tab.
3. Click on the Add a Rule to the List button (next to the X).
4. Your rule will be:
   Action: Deny
   Access Type: Application Proxy
   Proxy: HTTP
   Origin Server Port: 80 to blank
   Source: Specified – click on the "3" dots button. Select NDS Objects, click on the arrow in Source Details, and highlight any NDS Object. Click on OK, and then click on OK again.
   Destination: Any
   Do not enable logging. Press OK to save the rule.

ALLOWING COMPLETE ACCESS

1. Double-click on your BorderManager server.
2. Click on the Add a Rule to the List button (next to the X).
3. Your rule will be:
   Action: Allow
   Access Type: Port
   Service: Any
   Origin Server Port: leave this blank
   Transport: TCP & UDP
   Source: Any
   Destination: Any
   Do not enable logging. Press OK to save the rule.
4. Your server will be updated with the new rules.

DENYING ACCESS BY URL

1. Double-click on your BorderManager server object.
2. Click on the Add a Rule to the List button (next to the X).
3. Your rule will be:
   Action: Deny
   Access Type: URL
   Source: Any
   Destination: Specified – click on the "3" dots button. Then click on Add and enter the URL www.playboy.com, click OK.
   Do not enable logging. Press OK to save the rule.
4. Your server will be updated with the new rules.

DENYING ACCESS BY PORT

1. Double-click on your BorderManager server object.
2. Select the BorderManager Access Rules Tab.
3. Click on the Add a Rule to the List button (next to the X).
4. Your rule will be:
   Action: Deny
   Access Type: Port
   Service: FTP
   Origin Server Port: 21 to blank
   Transport: TCP & UDP
   Source: Any
   Destination: Specified – click on the "3" dots button. Select Host IP Addresses, and enter the IP Address range to restrict, click on Add. Click on OK, and then click on OK again.
   Do not enable logging. Press OK to save the rule.
5. Your server will be updated with the new rules.

INSTALLING CYBERPATROL

1. To install the CyberPatrol context filtering software, launch SYS:ETC\CPFILTER\CP_SETUP.EXE
2. When prompted, enter the drive letter to your SYS volume, i.e.: F
3. Don't Save the CyberPatrol registration.
4. Load the CyberPatrol NLM and place it in your autoexec.ncf file.
   a. At the server console type: load sys:\etc\cpfilter\cpfilter.nlm. This will perform the steps necessary to read the CyberPatrol database and connect to the Proxy Server.
   b. At the server console type in "Load Install", select NCF files options and press <Enter>.
   c. Select Edit AUTOEXEC.NCF file and press <Enter>.
   d. At the bottom of the file, type in "Load SYS:\ETC\CPFILTER\CPFILTER.NLM"
   e. Press F10 to save the file and exit.
   f. Press <Esc> twice to "Exit" menu.
   g. At the Exit menu, select "Yes".

DENYING ACCESS WITH CYBERPATROL

1. Double-click on your BorderManager server object.
2. Select the BorderManager Access Rules Tab.
3. Click on the Add a Rule to the List button (next to the X).
4. Your rule will be:
   Action: Deny
   Access Type: URL
   Service: Any
   Origin Server Port: leave blank
   Transport: TCP & UDP
   Source: Any
   Destination: Specified – click on the "3" dots button. Click on the down arrow in the Specify URLs box, and choose Select from Microsystems CyberNOT list. Check Sports & Leisure. Click OK, and click OK again.
   Do not enable logging. Press OK to save the rule.
5. Your server will be updated with the new rules.

APPLYING ACCESS RULES TO ALL BORDERMANAGER SERVERS

1. Highlight your top most Organization object, right mouse click for Details.
2. Click on BorderManager Access Rules tab.
3. Create an access rule (it can be anything)
4. Click OK to save the rules.
5. A pop dialog box will appear: "Updating all BorderManager Servers contained within this object could take some time. Do you want to update them now?" Click on Yes. This will apply the rule you created to all BorderManager servers under that container. Note: The rule that you defined will be appended to all BorderManager access rule lists.

CLIENT VPN – NETWARE ADMINISTRATOR CONFIGURATION

1. Configure Access Control to allow Client VPN Connections.
   a. Login to your server as Admin and run NWADMIN32.
   b. Open the server object and select BorderManager Access Rules.
   c. Click the Add button. Set up a rule to Allow. Under the "Access Type", use the drop-down list to select VPN Client.
   d. Optional: You may also select the Specified radio button under Source and select only those NDS Users you want to allow Client VPN access. "Welcome to Dial-Up Networking" dialog opens. Click <Next> to continue.
2. Configure the Client VPN connection.
   a. Click the BorderManager Setup property page. Select the VPN tab.
   b. Click the checkbox for Client Configuration and click the Details button.
   c. You should see the IP Address of the Master server (and any slave servers listed here). Click the Help button to read through further information about the VPN Client configuration options. Close help when finished.
3. Click Cancel to return to the Main VPN tab. Click Ok to exit VPN Configuration.

MOVING RULES

1. Double-click on your BorderManager server object.
2. Select the BorderManager Access Rules Tab.
3. Highlight the rule denying access to "WWW.PLAYBOY.COM" by selecting the rule with your mouse.
4. Click on the scissors icon and the rule will be cut from the list.
5. Click on OK at the bottom of the screen.
6. Highlight the top container in your tree, and press the right mouse button, click on details.
7. Select the BorderManager Access Rules Tab.
8. Select the Clipboard icon and your rule will now be pasted in the list.
9. Notice that the rule above is to allow access to all, so the deny rule needs to be moved.
10. Highlight the Deny rule by selecting the rule with your mouse and press the up arrow icon.
11. Click on OK to save the rule.
12. Select Yes from the message screen and the server will be updated.

SETTING UP AUTHENTICATION

This section will guide you through the set up of authentication.

CONFIGURING PROXY AUTHENTICATION

1. In NWAdmin32, right mouse click on your BorderManager server object, and select Details.
2. Enable Enforce Security in the lower left hand corner.
3. Click on the Authentication Context button.
4. Enable HTTP Proxy Authentication by placing a check in square.
5. For Single Sign-on to work, enable it, and then the workstation needs to be running the following application: \public\clntrust.exe. This will provide background authentication. The maximum time that Single Sign-on will wait for a reply is 60 seconds, the default is 3 seconds.
6. For SSL authentication, select in the Key ID field, the Key Material that you created in the above steps. Also enable either HTML Form or JAVA Applet as the authentication page.
7. Configure Maximum idle time before requiring a new login for the amount of time you want users idle, before prompting for authentication. The maximum time is 24 hours.
8. If you want Basic Authentication, place a check next to its square. Keep in mind that Basic Authentication is not as secure as SSL.
9. A cool option that BorderManager offers, is to require Authentication Only when user attempts to access a restricted page.
10. To define the contexts to search for users when performing authentication, click on the Context tab.
11. Click on the Add button (next to the X)
    a. Enter the NDS Context (do not put a leading dot)
    b. Enter the NDS Tree Name, click on OK.
12. Click on OK to return to the BorderManager Setup page.
13. Click on OK to have the settings take place.

www.novell.com/bordermanager

Technical specifications and availability are subject to change without notice.

For more information

Please contact your local Novell office, or visit our Web site at http://www.novell.com/bordermanager.
You may also call Novell at:
1-888-321-4272
1-801-861-5588
Fax: 1-801-861-5155

Education course information

For information on Novell BorderManager education courses, call 1-801-222-7800 or your local sales office.

Novell.