Global Information Assurance Certification Paper

Securing the perimeter using Novell BorderManager

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b

By
Alan Buchanan CNE
August 24, 2003

Table of Contents

1) Abstract

With the introduction of inexpensive broadband to the corporate market, small to medium size businesses are moving to migrate from desktop dial-up internet to network-wide routed connections using DSL or cable. The connection between the corporate network and the internet must be protected from unwanted and unauthorized access. For those companies already running Novell Netware 5.x or higher, Novell BorderManager is a logical choice for securing the network.

This document will step the reader through a BorderManager installation, configuration and administration making note of areas of policy consideration. The BorderManager used is version 3.6 which is included in the Netware 6 Small Business edition.

2) Considerations

It is assumed that the server in question is already locally secure as described in GSEC document http://www.sans.org/rr/paper.php?id=908 and contains two Network Interface Cards (NICs). The server will be acting as a router and will require the use of both NICs. There are several components to the BorderManager suite of services. Each of the following questions will need to be addressed before installation or configuration of the firewall.

- Is a VPN required?[1] This can be site-to-site or client-to-site.
- Is proxy authentication required?
- Which applications require proxy?
- Are there internal services required by outside hosts? This could be web or ftp services.
- Does the server require any additional hardware to perform these functions?
- Are any specific Access Control Lists (ACLs) required?

Case study[2] would indicate that a DSL router is preferable over a DSL modem for use with BorderManager. DSL routers from business Internet Service Providers usually have static configurations and multiple IP addresses. DSL modems use a DHCP connection to a statically assigned dynamic address database hosted by the provider and assign a specific IP address to a MAC address. Cable modem connections to the Internet will require a statically assigned address from the ISP. Frame and T1 (including partial), although more of an expense to the small business, have static addressing and a more stable physical connection usually directly to the Internet instead of through a service provider's network.

3) Pre-installation

Before installing BorderManager, the server needs to be prepared to ensure proper function of the firewall.

a) Disk

BorderManager caches all proxy traffic to disk. Sufficient disk space is required to cache Internet traffic. In building a new server it is advisable to set aside a non-NSS partition of approximately 2 Gigabytes for the cache volume for a network of 30-50 users. If adding BorderManager to an existing server there needs to be enough free space on the current volume(s) to cache the traffic. If there is insufficient disk space, an additional drive can be added to the system for cached traffic. The default cache volume is sys: in the etc/proxy/cache directory. This setting can be changed later using Netware Administrator.

b) RAM

The Netware server will also require sufficient RAM to handle the increase in network and disk traffic. Adding RAM to the server will reduce the chance of cache traffic diverting to the swap file (disk traffic is slower than RAM traffic) and reducing the overall performance of the cached traffic.

c) Alternate server

It is preferable, but not mandatory, that the BorderManager server on the network be on a server separate from the main file/print host. This will further insulate the file server from the Internet and separate the network traffic (figure 1) from the Internet traffic. The cost of additional hardware is minimal and current versions of Netware SB[3] (Small Business) allow for two licensed servers out of the box.

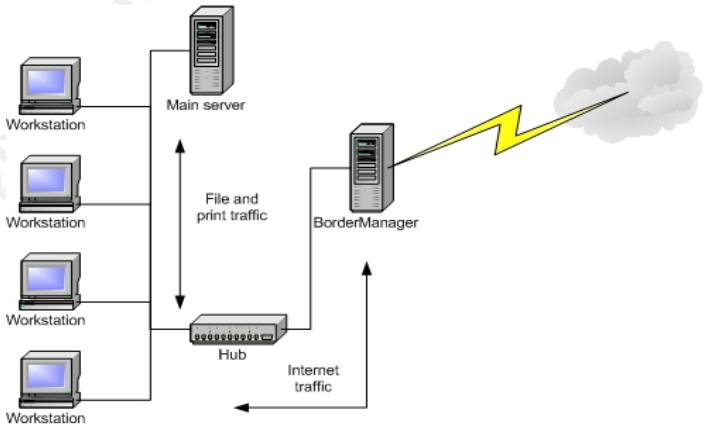

Figure 1 showing traffic patterns

4) Installation

The BorderManager CD must be mounted as a volume, either on the target server or on a server on the local network. The volume must be accessible by the admin user. The installation routine can be invoke by running "nwconfig" from the system console prompt and choosing "Product Options" then "Install a product not listed" and pressing esc to bypass the list of source volume names. Press F3 to enter the volume name "bmee36" (typing

volumes at the server prompt will list all locally mounted volumes – locate the correct spelling of the BM mounted CD to enter into the dialogue. This can be done at the console of the remote server if the CD is mounted on another system, which would make the syntax \\servername\volumename). This will begin the installation process by reading the install file at the root of the CD and continue into the Java runtime graphics environment.

The installation can also be started directly from the X-Server graphical console if it is already running. Choose "Install…" from the "Novell" button. Choose "Add" from the list of installed services dialogue. Point the source path dialogue to the BorderManager CD mounted locally or remotely and choose ok. This will take you directly to the GUI portion of the install.

Pass the welcome and copyright notification screen by clicking "Next" and read through the software license agreement. Press the "Accept" button to move to the services and licensing screen. This screen needs to know which services are to be installed. Place a check mark next to the items required (all checked by default) and make sure the license disk is in the floppy drive (default). The BorderManager Firewall/Caching Services will install packet filtering, IP Gateway, SOCKS and Proxy services. The BorderManager VPN Services will install client to site and site to site VPN software. The BorderManager Authentication Services are RADIUS and token authentication services. This installation requires only the BorderManager Firewall/Caching services check mark.

You will now be required to authenticate to the tree. The user must be admin or admin equivalent and you will need to know the context of the admin object (i.e. .ou=office.cn=admin). Enter the information and proceed to the network configuration screen. You will now be required to choose your public and private network interfaces. Place a check mark in the appropriate boxes beside each displayed NIC. There are two more choices on this screen. Make sure that "Set Filters to secure all public interfaces" is enabled. The "Enable HTTP Proxy for all Private Interfaces" option is not required at this point, but is a quick and easy way to have HTTP proxy already running after the installation. The next screen gives you the option of setting "Access control" and will set up enforcement of Access Control Lists.

If the system is running on an internal domain, enter the DNS domain name on the next screen. If there are no internal DNS servers and your server simply forwards to ISP servers, you can leave this field blank. You will need to enter 1-3 internal DNS server addresses on the next screen if you choose to use the DNS service. BorderManager caches DNS requests to speed access to name resolution for commonly viewed sites.

The next screen will summarize the installation and display the services to be installed. Clicking the "Finish" button will start the file copy process and

installation. There may be notification during the file copy that newer files are about to be overwritten. It is advisable to set the "Never overwrite newer files" option and let the copy process continue.

The BorderManager installation is now complete. The command to load BorderManager is added to the autoexec.ncf file and services will be loaded on server start up. A reboot of the server is required to make sure all newer NLMs are loaded into memory. Remove the license diskette from the floppy drive and the CD from the CD-ROM drive before restarting the system. It is imperative that the latest service packs[4] are also installed before the proxy is put into production. This will ensure that the services are using the most up-to-date files.

5) Configuration

BorderManager configuration is accomplished by running the Netware Administrator application found in the \\server\sys\public\win32 directory. The executable is nwadmn32.exe and will bring you to a view of the NDS tree. Locate the server in the tree and either double-click, or right click, and choose properties to view the server configuration. The button bar down the right side of the window will open different areas of configuration. Figure 2 shows the BorderManager setup configuration – the area of configuration we will review next. Highlight the desired proxy to configure and click the "Details…" button to see the dialogues displayed in each section. Proxy connections other than those required to perform daily corporate functions may require policy change. Some connections to the Internet have limited monthly bandwidth allowances causing an increase in billing by the ISP if thresholds are exceeded.

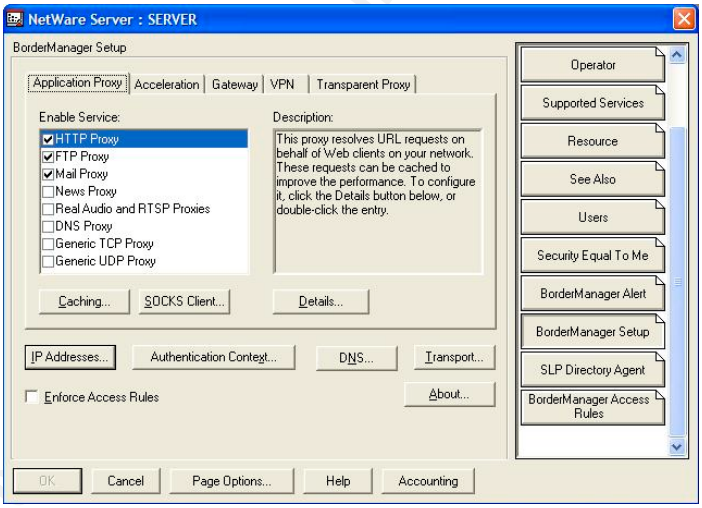

Figure 2 BorderManager configuration main

a) Application Proxy

i) HTTP Proxy

HTTP proxy is the only proxy that can be setup during the installation process. This provides a quick and easy use of web browsers from within the network by configuring the client station to browse to the

proxy address and port. The default port for HTTP proxy is 8080. If the "Enforce Access Rules" check box in figure 2 is chosen, the users will not be able to "browse past" the proxy. This enforcement works well with proxy authentication. The clients will then have to provide a username and password to view the site requested. The authentication browser page can be viewed in Java format or HTML format. The proxy authentication is enabled in the dialogue displayed by clicking the "Authentication Context…" button.

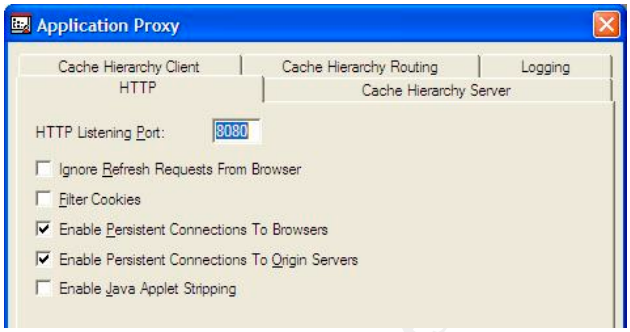

Figure 3 HTTP proxy port setting

HTTP proxy logging can be tailored to meet specific needs. Logs can be rolled by time or size settings. If the proxy authentication is not enabled, the log will reflect only the host IP address that accessed the web site. Proxy authentication will record the user name in the log with the site viewed. All HTML, file and image traffic from the web site is recorded in the log. Using the raw log data would be very time consuming. There is a Border Statistics application available that will provide a brief and concise report of logged information. The application is reviewed in the "administration" section.

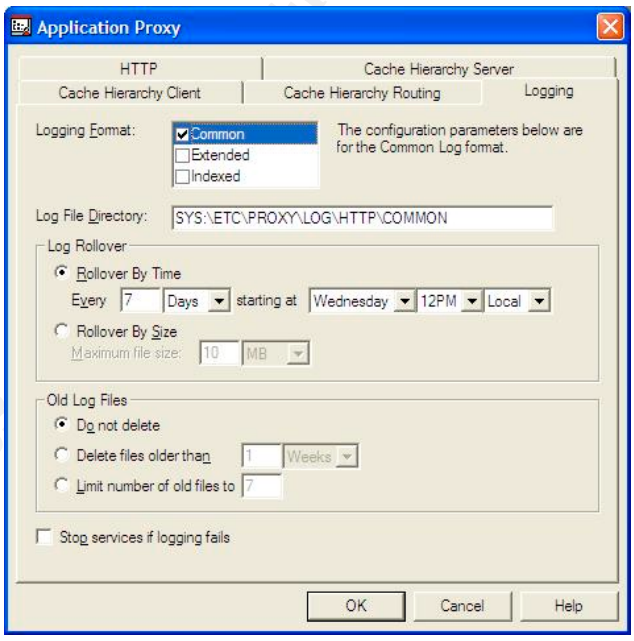

Figure 5 HTTP Proxy log settings

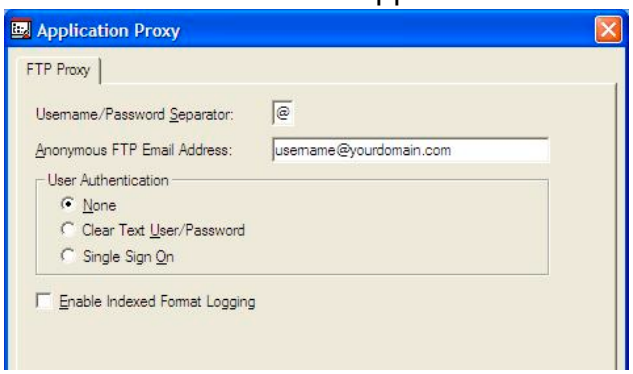

Figure 4 FTP proxy settings

ii) FTP Proxy

FTP Proxy configuration sets the anonymous email address used as password for anonymous connection to sites (figure 5). FTP client applications, browsers and command line FTP connections are valid for use with the proxy.

iii) Mail Proxy

Most small business networks will have their mail hosted outside the LAN and will require connection via the proxy. All that is required is the mail server name added to the proxy configuration and a section added to the etc\proxy\proxy.cfg file.

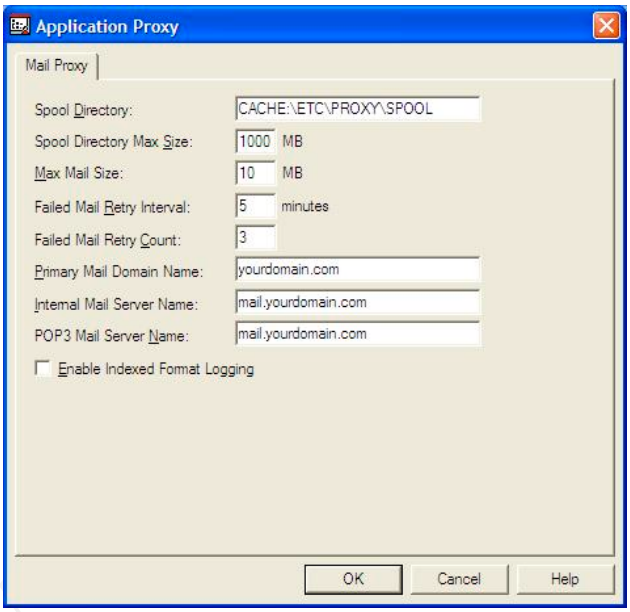

Figure 6 Mail proxy settings

The default mail message size and spool directory size can be adjusted to reflect user requirements based on attachment types and mail volume. The location of the mail spool directory is also set here. The format is volumename\directory. The directory should already exist prior to setting this option if configured for other than default.

The proxy.cfg file found in the \etc\proxy directory requires an addition to ensure proper operation of the proxy. The following lines should be added:

[BM Mail Proxy]
BM_Domain=yourdomain.com
BM_Incoming_Relay=0
BM_Proxy_Domain=mail-proxy.fs1.yourdomain.com

Between the brackets [ ] is the section header.
The **BM_Domain=** is your domain name.
The **BM_Incoming_Relay=** 0 stops relay from occurring – 1 allows relay with syntax john.doe%xyz.com@yourdoamin.com (definitely not recommended)
The **BM_Proxy_Domain=** is the fully qualified DNS name of the proxy server

iv) Other Proxy

Various other proxy configurations are standard with BorderManager. It is quite easy to set up proxy for streaming audio using the Real Audio and RSTP proxy dialogue. News servers can also be used through proxy by configuring the NNTP proxy settings. If the proxy you require is not listed, BorderManager gives you the option of configuring custom TCP or UDP proxy rules.

b) Access Control Lists

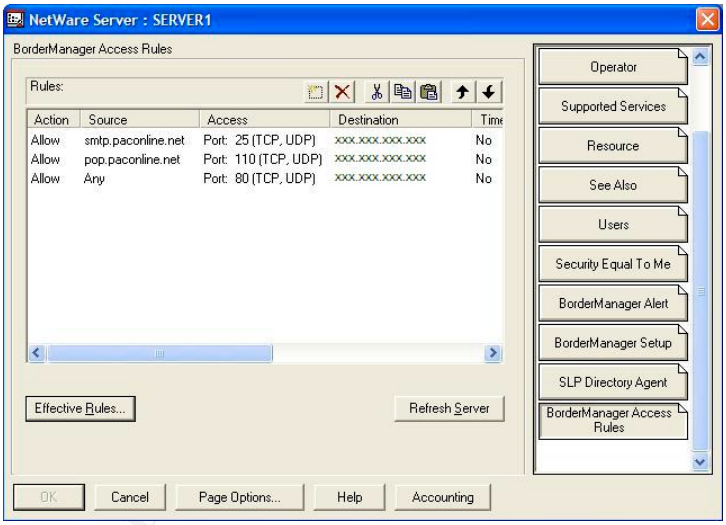

Figure 7 ACL Main screen

Access control lists (ACLs) are managed through the BorderManager Access Rules dialogue. Choosing the Access Rules button on the right side of the server configuration page will show you the list of rules. Rules will have to be configured and added to the list. Rules are not enforced unless the "Enforce Access Rules…" check box is enabled in the main BorderManager configuration dialogue. Examples given are for an email access rule and configuration for URL filtering (blocking). This is an area of concern when addressing corporate policy. These rules need to be clearly delineated and maintained for consistency.

i) Email ACL

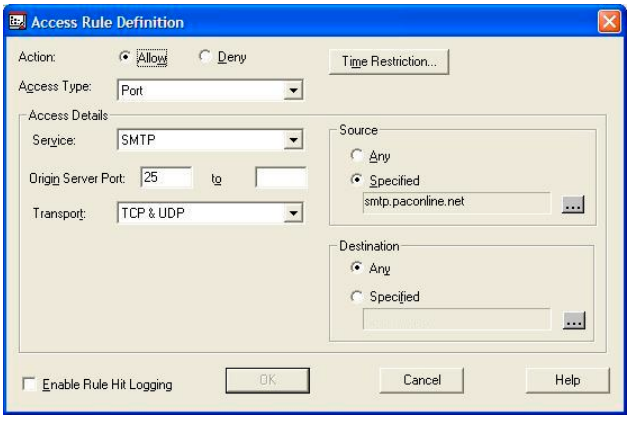

Figure 8 ACL rule for mail

The email proxy setup can be further hardened against relay and attacks by allowing only the external email server to connect on ports required by mail services. In this example (public IP address covered to protect client installations), the external mail host address is used to tell BorderManager that communication on mail ports is only allowed from that source. Port 25 traffic (SMTP) is allowed only from external IP

address of BorderManager to IP address of mail host. Port 110 traffic (POP) is set the same. Figure 8 shows port 25 for both TCP and UDP allowing traffic from a mail host on the Internet. The reverse of this rule is required to allow port 25 traffic to flow from BorderManager to the host.

ii) URL Filtering

The default rule for HTTP proxy is to "allow any" access to all web addresses. This rule can be countered by specifically blocking URLs in the BorderManager Access Control List. The following images show a URL list created to block sites of a specific nature and a site of a specific name. Administrators can populate the list with wildcard entries in an attempt to block all sites containing particular strings of characters. This is a proactive approach and can lead to some legitimate sites being disallowed. A reactive approach can be taken by using the web logs to compile lists of undesired sites frequented by users and adding the site name to the list of blocked URLs. Note that each site listing contains a trailing /*. This wildcard means that all pages under this site name are banned. If the wildcard is left off of the string, specific pages on that site can be viewed by entering them into the browser address line.

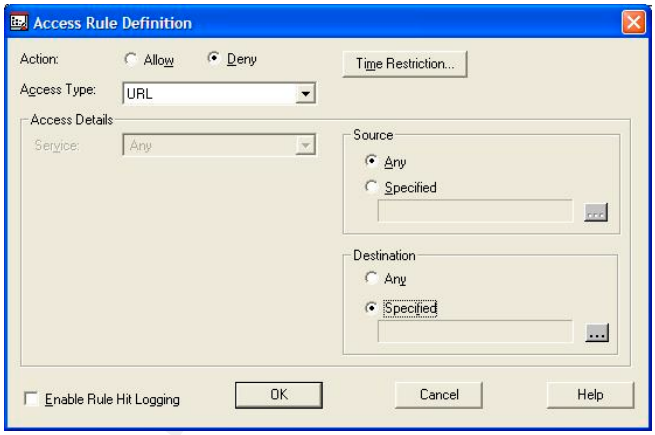

Figure 9 URL filtering ACL

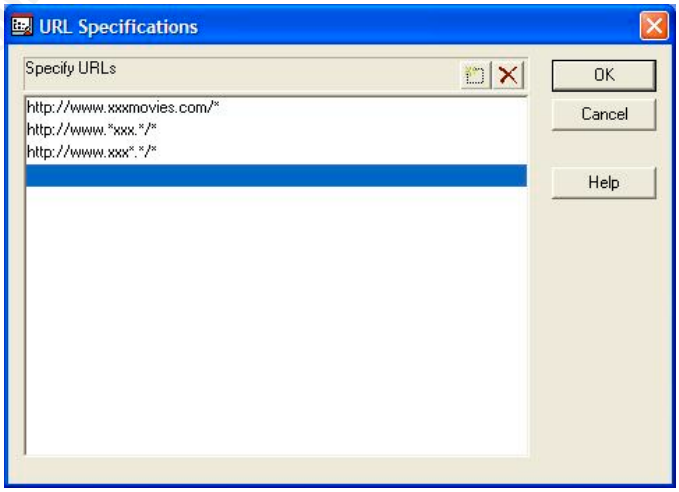

Figure 10 URL Filter list

The default page for response to a blocked site can be customized as required for a more corporate look. The files for editing are in the \\server\sys\proxy\data directory.

Figure 9 shows the URL filter rule that denies any URL placed in the specified list. Clicking the "…" button beside the entry will bring up the list in figure 10. This list can be tailored to suit the specific site. To add a site to the list, click the add button beside the delete button at the top right of the list window. This will add one line to the list and start the entry with http:// for you.

The alternative is to create a rule that denies all web access on port 80 and another rule that allows only a specific list of sites for access. This would allow administrators to screen requested sites before adding them to the list. This would have to be sanctioned by corporate officers before implementation as corporate policy of this nature can be difficult to deploy upon users that are already surfing at free will to any site on the Internet.

c) *Reverse Proxy*

Internal FTP and Web servers can be cached and accelerated to the Internet using reverse proxy in BorderManager. All that is required is the internal address and port of the server that requires external access. Reverse proxy insulates the source server from direct contact via the Internet by caching the outgoing data at the firewall. This is not a NAT style connection with the firewall forwarding packets directly to the internal server on the private network. The data viewed from outside the private network is held at the cache for viewing. The following figures show the configuration of a reverse proxy web site.

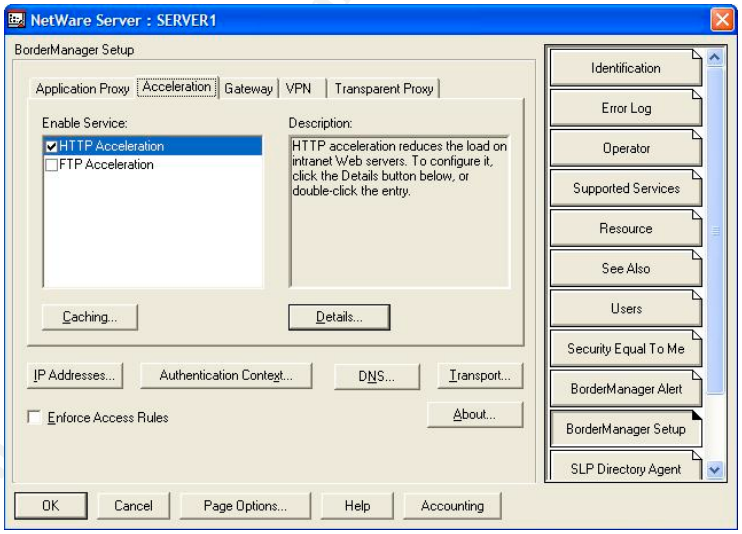

Figure 11 Accelerator main

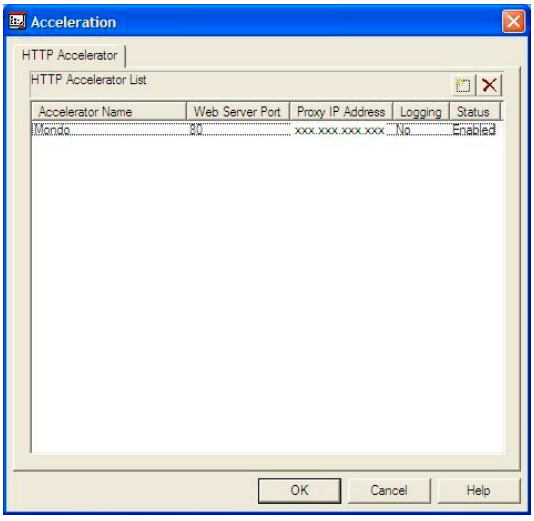

Figure 12 Accelerated sites listed

From the main dialogue shown in figure 11, click the details button to open the accelerator dialogue. This is the list of sites cached to the Internet (IP addresses blanked to protect client installations). If there is more that one site to cache, each site will require its own port for access. The URL would be http://xxx.xxx.xxx.xxx:portnum where xxx is the IP address or DNS entry for your server and portnum is the port the site is accelerated on.

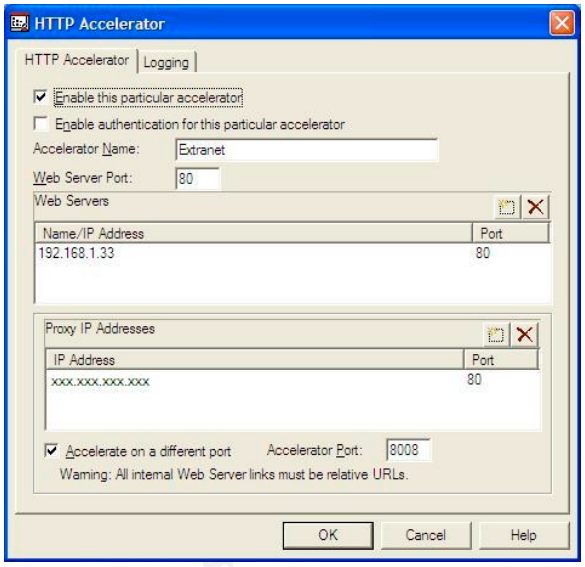

Figure 14 Accelerated site details

To add a site to the accelerator, click the add button next to the delete button at the top right of the list dialogue. The entry must have a name and will not let you save or move to the logging tab without an entry. If you have multiple accelerated sites, try to name them so that identification is easy. Enter the internal address and port in the Name/IP Address window. Adding an entry in the Proxy IP Address window brings up a dialogue to choose the proxy address. Choose the external address and click okay. If the accelerator requires a port number other than default, check the "accelerate on a different port" box and enter the port number required. Choosing OK saves the site to the list.

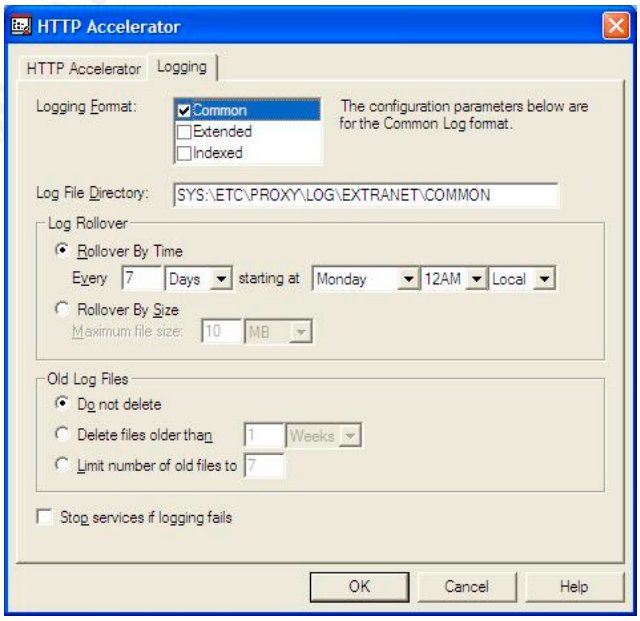

Figure 13 Accelerated site logging

Access to the accelerated site can be logged. Figure 14 shows the setup for logging configuration for a particular reverse proxy. Logs are named by the site name in the accelerator list and can be viewed using a text

editor. Common data shows host address and port, date, time and file accessed.

d) Caching sites

If the business has (a) particular web site(s) that it uses on a daily basis to perform or compete in the market place, the site can be accelerated to the client desktop using BorderManager caching. These dialogues show the setup of a site for download on a daily basis. Clicking the "Caching…" button shown in figure 2 will bring up the window shown right. This is the list of downloaded sites. Initially this list is blank and sites will have to be added.

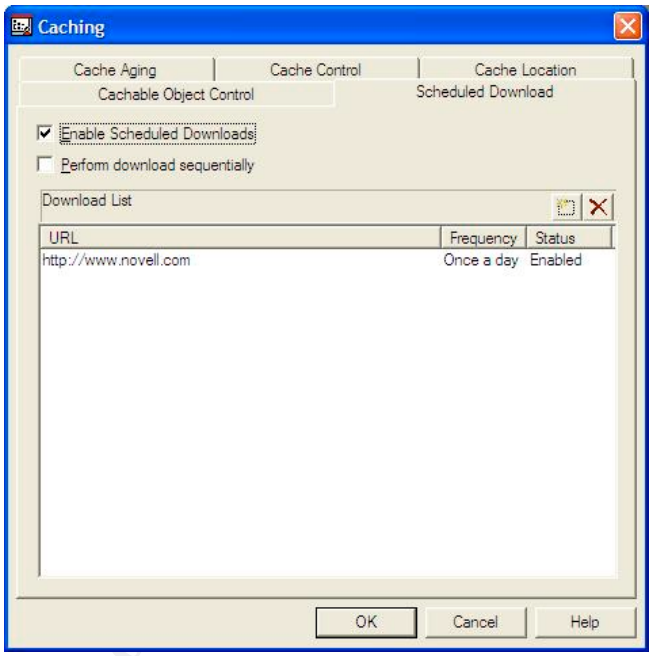

Figure 16 Download sites for caching

Click the add button next to the delete button (X) at the top right of the list. The add dialogue asks for the name of the site and how much of the site and what quantity of data to download (figure 16). Any specific download can be enabled or disabled by checking the box at the top of the dialogue.

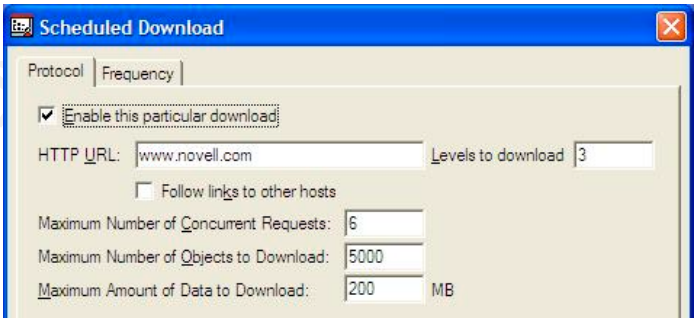

Figure 15 Download site configuration

The frequency of the download is set on the next screen. Sites can be downloaded hourly, daily or only once if desired. It depends on the site and the

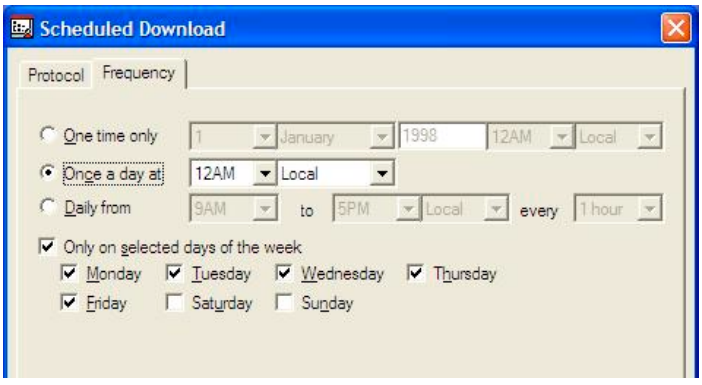

Figure 17 Caching frequency

content. A bidding system for an electrical contractor may require a refresh part way through the day to keep up the cached site current as new data is posted to the source site.

6) Administration

BorderManager is configured through the Netware Administrator application. All figures but the first are screen shots taken from different sites using NWAdmin. Management of VPN statistics, connections, tunnels and keys is accomplished through NWAdmin. Monitoring the proxy information can be done through the Proxy Console and applications that parse the log files.

HTTP proxy logging for inbound and outbound traffic can be compiled into HTML reports using the Border Stats utility available through the cool solutions section for BorderManager at the Novell web site. The Border Stats utility can parse the logs into a concise report that can show user (if proxy authentication is enabled) or IP address access to sites, data traffic volumes charted by time and day, top URLs, top users, etc. The utility runs from within the log directory and will work for accelerated sites as well as proxy sites accessed by users.

BorderManager activity can be monitored in real time using the RTMonitor v3.1.4 application. This program can put on the screen from the most current log file, the top 20 URLs by user, users IP address, users NDS name (with proxy authentication), HTTP status codes, HTTP server loading, and will help manage URL filtering and results.

Proxy server logs can also be parsed into a PostgreSQL database on a Linux system using an Open Source Initiative reporting tool developed by EIT Systems. The logging information is compiled and ported to HTML files for viewing with a browser.

All proxy and cache statistics and information can be viewed at the console (or with a remote console) at the Proxy Console screen. This is the heart of the BorderManager system and can reveal HTTP proxy statistics, FTP proxy statistics, DNS and DNS caching Statistics, Proxy memory usage and real time connection and user data statistics. The appnote for management of BorderManager through the Proxy Console is very detailed and gives insight (http://developer.novell.com/research/appnotes/2002/august/03/a020803.htm) into the different statistics and what they mean.

7) Summary

Inexpensive broadband for business generates a need for protection from the Internet. Firewalls can; protect the network from unwanted intrusion, monitor and track Internet usage, enforce corporate policy through filtering and access control lists, and enhance the response times of frequently used Internet resources. All functions of BorderManager, from accelerating an

Intranet to providing secure communication between sites and users, enhance the Internet experience without adding undue complexity or overhead to the IT administration required to maintain the services. Using BorderManager as firewall/proxy in a Netware environment provides a secure environment for users and data with added benefits and features not found in many other products.

8) Resources

Novell BorderManager and Netware Hints, Tips and files
http://nscsysop.hypermart.net/

Monitoring Proxy Information on Novell BorderManager (appnote)
http://developer.novell.com/research/appnotes/2002/august/03/a020803.htm

BorderManager 3.6 Read me
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10058173.htm

Mail proxy with internal mail server
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10023303.htm

Proxy configuration options
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10059667.htm

How to configure FTP proxy
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10061427.htm

How to create access control rules
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10056700.htm

Changing the BorderManager Error Page
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10018668.htm

IP Routing Troubleshooting
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2908890.htm

Novell Cool Solutions → BorderManager real time monitor
RTMonitor v3.1.4
http://www.novell.com/coolsolutions/tools/1611.html

Novell Cool Solutions → BorderManager HTTP proxy reports
BorderStats v1.5
http://www.novell.com/coolsolutions/tools/1004.html

Novell Cool Solutions → Redhat Proxy Log Parser
http://www.novell.com/coolsolutions/tools/1582.html

Novell's BorderManager Administrator's Handbook
Author Laura Y. Pan
Publisher John Wiley & Sons ISBN 0-7645-4565-5

Novell's Guide to BorderManager
Authors J.D. Marymee and Sandy Stevens
Publisher Hungry Minds, Inc. ISBN 0-7645-4540-X

Novell's Netware 6 Administrator's Handbook
Authors Jeffery Harris and Kelley J.P. Lindberg
Publisher John Wiley & Sons ISBN 0-7645-4882-4

[1] This document will not deal deeply with the topic of VPN access to the network. The installer does not require this question answered to complete the installation of BorderManager. The administrator of the server will be required to perform certain steps to initiate VPN access after the proxy/firewall is installed.
[2] Changes to the hosted DHCP database or loss of connection for extended periods can cause downtime while the server and services are reconfigured for a new address. A faulty NIC that requires replacement will also cause a complete reconfiguration of services due to a change in the MAC address. A statically configured router maintains the same IP addresses regardless of connection status or NIC MAC address.
[3] Novell Netware 6 SB includes Netware 6, BorderManager 3.6, GroupWise 6 and Tobit Faxware. The licensing model is based on the number of users in the Directory tree to a maximum of 50.
[4] As with all operating systems and network applications, the latest service packs that are available should be installed on the server before running the services in a production environment.