Global Information Assurance Certification Paper

Overview of Novell's BorderManager Firewall Services

Tom Fast
February 8, 2001

Introduction

Novell BorderManager Firewall Services is a component of Novell BorderManager Enterprise Edition, Novell's suite of Internet/Intranet security products that also includes Authentication Services (remote dial up), VPN Services and FastCache Services. Being a Novell product it fits best in an NDS (Novell Directory Services) environment where it integrates with the authentication security features of NDS as well as giving users a single sign on.
BorderManager Firewall services are delivered through three levels. Level 1 is packet filtering, level 2 is NAT and IP gateway, level 3 is application proxy services.

Installation and Setup

BorderManager can be installed on a NetWare 4.11 or 5 server. It comes with a 2 user NetWare server license and a NWAdmin (NetWare Administrator) plug-in for administration. Installation and setup is best left to an experienced network administrator. For those brave enough to go it on their own Craig Johnson, Novell Support Connection SysOp has written a book "*A Beginner's Guide to BorderManager 3.x*" that covers the installation and configuration of BorderManager as well as the NetWare server. I haven't read the book, how ever, I found his first book on BorderManager filter configuration to be extremely helpful. A link to these books can be found in Appendix A.

When setting up BorderManager you have to alternate between the console screen and th NWAdmin screen to. This can lead to some frustration when trying to remember the where you made that change, that now needs to be reversed. The best thing to do and a good general practice all around is to document changes, where, how and when you make them. That way when you need to add a filter or tweak a setting you know exactly where to do it.

Authentication

Authentication is done through Novell NDS. This provides for a single sign on and utilizes the security features of NDS. Central to NDS security is that it is based on user authentication rather then IP addresses.

To be able to authenticate to the proxy server a Windows workstation has to be running IP, the Novell client and the clntrust.exe. The clntrust.exe and BorderManager exchange information to verify that the user logged into the workstation is authenticated to the NDS tree and has a connection to the BorderManager server.

For workstations that are unable to run the Novell client or the clntrust.exe, SSL can be enabled on BorderManager. With SSL the user will be prompted with a log in screen on the browser. They enter their NDS user name and are authenticated to the proxy server.

The only time authentication is not used is if Dynamic NAT is enabled. Care should be taken when enabling NAT that the proper filters and access rules are in place.

Filtering

Packet filters examine the header field of the packets going between the protected network and the unknown network. They are looking to identify the packet based on Protocol ID, Source IP, Destination IP Address and port, and firewall interface for incoming or outgoing packets. Based on these criteria and a set of packet filter rules, the packet will be forwarded or dropped.

If you want to firewall between private IPX networks BorderManager also does IPX packet filtering. IPX filtering is also used when using the IPX/IP gateway

BorderManager incorporates Static Packet filtering, Dynamic Packet Filtering and TCP ACK filtering. The filters are setup using the console screen and running the filtcfg.nlm. As in all good packet filters or ACL's the default settings for the filters will block most traffic. Novell puts in default filters to allow VPN, IP gateway and proxy services to function. Because of this Novell recommends setting up and configuring packet filters after normal business hours.

Static Filters

Static filters provide a limited level of protection. They cannot process higher-layer information. They do not know if the packet is the first packet from an outside source or a response from a request on the inside.
To enable a two way connection two filters have to be defined. One filter allows the outgoing and one allows the incoming.

TCP ACK Bit Filtering

When a TCP client wants to initiate a connection to a server it sends a SYN (Synchronize), the server will respond with a SYN and the ACK bit set. The TCP ACK bit filter blocks any connection attempts from the unknown network, only allowing response packets with the ACK bit set. TCP ACK bit filtering should not be applied to any inbound filters that require an external host initiating a connection to an internal host.

Dynamic Filtering

Dynamic filtering overcomes the limitations of static filtering. When a packet is first sent to the unknown network, dynamic filtering will automatically create a reverse filter to allow the response packet to return. To create the filter, the filter engine looks at the entire context of the packet, not just the address. This information is then extracted from the outgoing packet and stored in a table to be compared against the reply. The inbound filter created is a time-limited, temporary filter for that connection only.

Fragmented Packet Filtering
Fragments of IP datagrams can be used in denial-of-service attacks by flooding a network with fragment packets. A port scan can be performed on a target host by using a non-fragmented packet with the more fragment bit set. BorderManager has an automatic fragmented packet filter that check fragments based on source and destination, a combination of TCP/IP and fragment flags, and inbound and outbound interfaces.

Other Defenses
BorderManager incorporates a number of additional commands. These can be set on the server console screen or included in the AUTOEXEC.NCF startup file. They are set to ON by default.

Filter Subnet Broadcast Packets = ON/OFF
Drops all packets with a destination IP broadcast address.
Filter Local Loopback Packets = ON/OFF
All loopback packets will be dropped.
Filter Packets with IP Header Options = ON/OFF
All packets with IP header option enabled are dropped.

NAT
NAT (Network Address Translation) occurs when the firewall maps an internal host's private IP address to registered Internet IP address. When a response packet is sent back the address is again remapped to the corresponding internal address and sent to the internal host. This effectively hides the internal IP address from being seen on the Internet.
Dynamic NAT does not require a Novell or Windows client to be running on a network host and does not authenticate through NDS. This means that any network host running TCP/IP can access the Internet through the NAT.

BorderManager supports three modes of NAT.

DYNAMIC
The internal host has its address dynamically changed by the NAT every time it sends a packet out to the Internet. Dynamic NAT allows multiple internal hosts to access the Internet through one registered IP address.

STATIC
Static NAT is for making a one to one mapping of a registered IP to single internal host. Useful for any web or FTP servers you may want to make available on the Internet. Any packets coming to that IP address can only get to the host configured in the NAT.

STATIC and DYNAMIC

BorderManager allows you to have both static and dynamic NAT configured at the same time. To do this it is necessary to configure multiple registered IP addresses on the public interface. Each NAT must have it's own public IP address. By default the dynamic NAT will always use the primary address and the static will use the secondary address assigned to it.

IP Gateway

The IP gateway acts similarly to a NAT, only with authentication. The gateway forwards requests from a network host to the Internet replacing the host address with the gateways Public IP address. Authentication to the gateway is handled by NDS. There are three gateways that can be enabled.

IPX/IP

Used by clients that are running Windows workstations with IPX and the Novell Client. This is a fairly unique feature of BorderManager that lets hosts that are only running IPX access the Internet without any IP configuration.

IP/IP

Used by clients that are running Windows workstations, IP and the Novell Client.

SOCKS

Used by clients that are not running Windows workstations. They need to be running IP and either SOCKS4 or SOCKS5. NDS user objects can be created for authentication through NDS.

Application Proxy Services

A proxy serves as a go between for the users on your protected network and the unknown network you are trying to access. When a local host makes a request to a destination, the proxy intercedes and makes the request for you, retrieves the requested data from the Internet host and then sends the data to the local host. The result is the Internet host only knows the address of the proxy server and not the local host address on the protected network. The proxy will also cache the data on the server, so that any future requests for that data can be taken directly from the server instead of re requesting it from the Internet host. BorderManager proxies look at the context of the session and content-based semantic access controls are applied before sending out the data. BorderManager also has reverse HTTP and FTP proxies for web services inside the firewall.

[1]Border Manager Proxy Services includes:

- Support for HTTP (0.9, 1.0, 1.1), FTP, Gopher, DNS, and SSL clients
- Hierarchical caching based on the Internet Cache Protocol (ICP) and other protocols
- HTTP and FTP server accelerator (reverse proxy)
- Application proxies, including SMTP proxy, NNTP proxy, DNS proxy, SOCKS, HTTP Transparent proxy, Telnet Transparent proxy, and RealAudio and RTSP proxies

- SOCKS client support
- Batch downloading of URLs
- Content filtering for Java
- Simple Network Management Protocol (SNMP) Management Information Base (MIB)
- Access control lists based on NDS user identity, IP addresses, domains, and URLs
- Windows-based management console and configuration
- Event logging in Text and Relational Database Management System (RDBMS) formats

Access Rules
Access rules are used to control user access through Border Manger. These rules can be applied to a wide range of users such as individual users, IP addresses, groups of users, Organizations and Organizational Units.

Rules can specify action, access type, source, destination, time restriction and logging.

Actions
Allow or deny.

Access type
You specify port, URL, application proxy or VPN Client.

Source
Is the user/users that are being given access through Border Manager. The source can be specified with an NDS user name, NDS user group, DNS hostname, e-mail usernames, e-mail domain names, IP address, range of IP addresses, or, one or more IP Subnet addresses. To give all users access the source can be set to <Any>.

Destination
The destination can be specified as a DNS hostname, IP address or range of IP address, IP Subnet addresses, e-mail user or domain names and URL. To give access to all destinations use <Any>.

Time Restriction
Lets you set the specific hours that you want the access rules to apply. A grid is displayed that lets you set the times or choose <Any> for the rule to always apply.

Enabling Rule Hit Logging
Creates a log file of all attempts to connect to the destinations and services in the access rules.

Wildcards are allowed when specifying non-NDS source and destinations.

Server Security Considerations
As with all firewalls it is important to keep the NOS and BorderManager up to date with the latest patches. Novell also recommends the following:

- Do not configure the BorderManager server to run rconsole or xconsole
- Do not use the BorderManager server for application data or hosting
- Restrict SNMP to the server
- Change the default SNMP community string
- Control NCP (Network Core Protocol) by setting packet signatures to the highest level (3)
- Restrict physical access to the server
- Use filters to block source address spoofing

Vulnerabilities
A search for BorderManager hacks/cracks etc, turned up three vulnerabilities.

[2]A DoS vulnerability
BorderManager has a feature called the CS Audit Trail Proxy. This proxy is installed by default and opens a listening port at port 2000 on both the internal and external interfaces. Memory allocation problems will result if a connection is made to port 2000 and the enter key is hit a few times. Eventually the server will lock up and a reboot is needed to get it functioning properly. Novell has issued a patch to correct the problem.
We had this happen on our BorderManager server. The culprit was one of our own in-house applications that used port 2000. Till the server was patched we used the temporary fix of unloading the CSATPRX.NLM.

[3]A User Impersonation Vulnerability
The client trust app that runs on the workstation listens on port 3024 for authentication requests from the BorderManager server when the user is accessing the Internet. BorderManager does not verify the origin of the request allowing an attacker to use port redirection to impersonate a valid authenticated user. Using port forwarding on the attacker's machine, any requests to port 3024 are sent to the authenticated user's machine. When the attacker makes a request, BorderManager queries the attacker's machine. Port forwarding sends the query to the authenticated user's machine. BorderManager then allows the request.

The results being the attacker can get unauthorized content access, and the authorized user's ID is attached to any illicit web activity that is done.

The attacker's machine IP address will be logged instead of the authorized user's IP address.

[4]URL Rule Restriction Bypass Vulnerability
URL based access rules set on subdirectories on an intranet running Novell BorderManager may be bypassed if http encoded characters are used in the URL

request.
E.g.
to access: http://target/subdirectory

type: http://target/subdir%45ctory

Logging
Logging is the weakest part of BorderManager. While there is logging for most of the proxies, access rules and filters, BorderManager does not have a way of tying the data together and giving you a useful statistical report.

[5]Webtrends Firewall Suite is a 3rd party software package that can be used to monitor, manage and create reports on the firewall activity. If you've set any of your logs to do indexed logging Webtrends will not be able to use those logs.

Cyber Patrol
[6]Cyber Patrol is a 3rd party package for doing Internet content filtering. BorderManager ships with a Cyber Patrol nlm. If you use the Cyber Patrol software you get a free 45-day trial subscription. After the trial period you can either renew the subscription or continue using Cyber Patrol with the last lists downloaded.

Novell – "Novell BorderManager Enterprise Edition 3.6 Overview and Planning"
Novell BorderManager 3.6 URL:
http://www.novell.com/documentation/lg/bmee36/docui/index.html (Feb 5, 2001)

Novell – "Novell BorderManager Enterprise Edition 3.6 Installation and Setup"
Novell BorderManager 3.6 URL:
http://www.novell.com/documentation/lg/bmee36/docui/index.html (Feb 5, 2001)

Novell – "Implementing a More Comprehensive Firewall Solution" 4621005 1999 URL:
http://www.novell.com/info/collateral/docs/4621005.01/4621005.html (Feb 7, 2001)

Johnson, Craig - "BorderManager: A Beginner's Guide to Configuring Filter Exceptions"
First Edition October 27, 1999

Novell – "Understanding SSL Proxy Authentication with BorderManager" 10023518
16 Dec 1999 URL:
http://support.novell.com/search/kb_indexf.htm (6 Feb, 2001)

[1] Novell – "Overview of Proxy Services"
Novell BorderManager 3.6 URL:
http://www.novell.com/documentation/lg/bmee36/docui/index.html (Feb 5, 2001)

[2] SecurityFocus – "Novell Border Manager A DoS vulnerability"

Vulnerabilities July 5, 2000
http://www.securityfocus.com/bid/1440 (Feb 7, 2001)

[3] SecurityFocus – "Novell Border Manager Audit Trail Proxy DoS Vulnerability" Vulnerabilities February 4, 2000 URL:
http://www.securityfocus.com/bid/1440 (Feb 7, 2001)

[4] SecurityFocus – "URL Rule Restriction Bypass Vulnerability" Vulnerabilities July 7, 2000 URL:
http://www.securityfocus.com/bid/1440 (Feb 7, 2001)

[5] Webtrends – "**WebTrends Firewall Suite** " 2001 URL:
http://www.webtrends.com/products/firewall/default.htm (6 Feb, 2001)

[6] Lanvision, "Internet Control for BorderManager" URL:
http://www.lanvision.com.au/CyberPatrol/novell.htm (6 Feb, 2001)

Appendix A: Additional Information

Two books "BorderManager: A Beginner's Guide to Configuring Filter Exceptions" and "A Beginner's Guide to BorderManager 3.x" by Craig Johnson can be found at:

http://nscsysop.hypermart.net/index.html

More in-depth information on Novell BorderManager Firewall can be found at:
http://www.novell.com/products/bordermanager

Links to the Novell knowledge base and BorderManager support forums can be found at:
http://support.novell.com