Global Information Assurance Certification Paper

Limiting the Exposure of a NetWare Server in an IP World

Dana McLaughlin

15 December 2000

Introduction

Prior to Novell's release of NetWare 5, IPX was the default protocol for NetWare file servers. Servers could run pure IP with the load of a NetWare Loadable Module (nlm) called tcpip.nlm. This nlm allowed for routing and client/server applications (such as GroupWise 5.X, DNS, and DHCP) but clients could not authenticate to Novell's Novell Directory Services (NDS). The only IP option that allowed for authentication was Novell's proprietary NetWare/IP.

NetWare 5 and its follow-on, NetWare 5.1, default to pure IP as their primary network protocol. As the agency I work for prepared for its migration to pure IP file servers, I began to look into how we could limit their exposure (harden them) against IP hacks with a $0 budget for purchasing add-on software such as Novell's BorderManager.

This document discusses what I found to answer my primary questions. What does a NetWare 5.1 file server need to communicate with other NetWare servers and with clients? What ports are active by default? How do I disable non-needed ports? Are there any other settings that can be used to reduce vulnerability?

NetWare Communications

NetWare servers and clients use NetWare Core Protocol (NCP) for much of their communication. The active port on a file server for NCP is TCP and UDP ports 524.(1)

Locating services, such as file servers, application servers and gateways, is done via Service Location Protocol (SLP). SLP is also used to provide backward compatibility with IPX applications that relied on Service Advertising Protocol (SAP) broadcasts.(1) Servers listen on TCP and UDP ports 427 for SLP requests. Depending on the server, SLP, and site configuration, NetWare devices will use multicast 224.0.1.35 to find a directory agent, which catalogs all known services. Also depending on configurations clients will use multicast 224.0.1.22 to locate their preferred NDS tree and server as well as other general requests, or they may use DHCP settings.(2)

The most conclusive way we've found to ensure that we know how our clients and servers are locating services is to analyze communications trace files with Novell's Lanalyzer application and then compare the findings to the NDS, client, and server configurations. During these examinations, we've often found servers and / clients from other agencies connected to our systems due to improper configuration by one of us and unfiltered multicast communications.

Active Ports

To determine what IP ports are active on a file server, run the TCP/IP Console utility

(tcpcon.nlm) at the server console. In the utility, select Protocol Information, TCP, and then TCP Connections. The active TCP ports, port state, and connections will be listed. The defaults for my agency's configuration showed ports 389 (LDAP), 427, 524, 636 (SSL for LDAP), 80, and 8008 in either listening or established states.

I expected to see the LDAP (which NDS is compatible with) as well as the SLP and NDS ports active. I wasn't expecting to find ports 80 and 8008 active by default. I connected to one of the servers via my web browser and found that it redirected me to port 8008 which was NetWare Management Portal. This feature allows management via a web browser by connecting via http to the server's tcpip address port 8008. Some very interesting information, such as system statistics and all loaded NLMs and their versions, can be accessed without having to authenticate. Logging in (authenticating) via the Portal allows access to more extensive management options.(3)(4)

The UDP ports active (accessed via Protocol Information, UDP, UDP Listeners) were ntp (port 123), snmp (port 161), and 524.

NetWare 5.1 file servers not yet patched with support pack 1 also had ports 7 (echo), 9 (discard), and 19 (chargen) active by default.

Disabling Unnecessary Ports / Controlling Access to Ports

The TCP/IP Console utility does not have a disable port feature. NetWare Management Portal can be unloaded / disabled (as can other unneeded nlms) by the sysadmin. I've found that the only built in option on a NetWare file server for controlling access to necessary ports is to block access to them via filters.

To activate filters, first load the Internetworking Configuration utility (inetcfg.nlm) at the console, select Protocols, TCP/IP, and set Filter Support to Enabled. Exit the utility, saving and activating changes. To configure filters, load the Filter Configuration utility (filtcfg.nlm) at the console, select Configure TCP/IP Filters, set Packet Forwarding Filters to Enabled.(5)

Finding information on how to configure the filters was not easy. The information was scattered across BorderManager and Novell Internet Access Server (NIAS) documentation and Technical Information Documents (TIDs) with none going into any of the idiosyncrasies of what NetWare 5.1 can do by itself. Through experimentation and opening an incident with Novell, I found that basic filtering does work but some active options don't work. Ignore all logging options, as unfortunately logging requires an application like BorderManager before it will function. Also beware of doing anything with Stateful Filtering.

I was quite successful at implementing basic filtering with the Filter Configuration utility by doing steps similar to the following:

1) On the first menu of the utility (Filter Configuration Available Options), Configure TCP/IP Filters.
2) Select and enter Packet Forwarding Filters, keeping the state Disabled until I actually want the

filters to be in operation.

3) Select whether I want to Deny only what I specifically list or Permit what I specifically list. In this test case I want to permit all NCP packets from a specific network, denying all others, so I will chose the Permit Packets in Filter List option.
4) Select List of Permited Packets and press enter.
5) Press insert to create a new filter, setting the fields as follows: (6)
   Source Interface Type: Interface
   Source Interface: <All Interfaces>
   Destination Interface Type: Interface
   Destination Interface: *the network interface of the server*
   Packet Type: ncp *Note: Protocols not on the list can be added by pressing Ins on the list screen.*
   Src Addr Type: Network
   Src IP Address: *network and submask allowed*
   Dest Addr Type: Any Address
   Logging: Disabled
   Comment: Allowing NCP from *network*
6) Escape and save the filter.
7) As this is the last filter I will make, I escape to the Packet Forwarding Filters menu, and change the Status to Enabled.

Testing filters can be done by sending packets to the server and not getting or getting a response and by analyzing trace files. You can also temporarily set TCPIP Debugging on. The steps to do this are:

1) Initiate console logging by loading conlog.nlm at the server console.
2) At the console, type set tcp ip debug = 1.

This will display header information on all IP packets to or from the server on the console screen and write the information to the server's console.log file.(7) Set the debug back to 0 and unload conlog.nlm to open the log file for review.

General Server Settings

The Console Monitor screen's Server Parameters, Communication section lists configuration settings that can be altered to further lock down access to the server. This section includes options that can defend against TCP Land and SYN Flood Attacks, as well as options such as setting maximum sizes for ping packets, filter packets with ip header options, discard oversize ping packets, etc. Changes to these settings should not be done without careful testing.(8)

References

(1) Plett, Corey. "Migrating to Pure IP with NetWare 5." Novell AppNotes. September 1998. URL: http://developer.novell.com/research/appnotes/1998/septembe/03/index.htm.
(2) Chappell, Laura. "Service Location Protocol." Netware Connection. July 1998. URL: http://www.nwconnection.com/jul.98/slp78/index.html.
(3) Novell. "Using the NetWare Management Portal." URL:

http://www.novell.com/documentation/lg/nw51/docui/index.html#../port_enu/data/a27vgr6.html.
(4) Anderson, Ron. "Novell NetWare 5.1 Is Primed To Ensnare You In Its Web." Network Computing. December 13, 1999. URL: http://www.networkcomputing.com/1025/1025sp1.html.
(5) Novell. Technical Information Document (TID) #10022164 "TCPIP blocking ports (7, 9, 19, etc)." February 11, 2000. URL: http://support.novell.com/cgi-bin/search/search.pl?database_name=kb&type=HTML&docid=%03%21F201153%3a977014763%3a%20%28%2010022164%20%29%20%20%07%01%00&byte_count=7195.
(6) Novell. "How To Run FILTCFG." January 6, 2000. URL: http://www.novell.com/documentation/lg/nias41/docui/index.html#../filtrenu/data/hq768iej.html.
(7) Novell. Technical Information Document (TID) #10013542 "How to use the TCPIP debug SET commands." October 14, 1999. URL: http://support.novell.com/cgi-bin/search/search.pl?database_name=kb&type=HTML&docid=%03%21F182481%3a977021838%3a%20%28%2010013542%20%29%20%20%07%01%00&byte_count=21283.
(8) Novell. Technical Information Document (TID) #10018661 "NetWare TCPIP Performance Troubleshooting and" November 20, 2000. URL: http://support.novell.com/cgi-bin/search/search.pl?database_name=kb&type=HTML&docid=%031F191417%3a977032572%3a%20%28%20%22tcp%20defend%20syn%20attacks%22%20%29%20%20%07%01%00&byte_count=25691.

Last Updated: April 23rd, 2018

Upcoming Training

Mentor Session - AW SEC401	Detroit, MI	May 01, 2018 - May 17, 2018	Mentor
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event
SANS Atlanta 2018	Atlanta, GA	May 29, 2018 - Jun 03, 2018	Live Event
Community SANS Bethesda SEC401	Bethesda, MD	Jun 04, 2018 - Jun 09, 2018	Community SANS
SANS London June 2018	London, United Kingdom	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, CO	Jun 04, 2018 - Jun 09, 2018	Live Event
Community SANS New York SEC401	New York, NY	Jun 04, 2018 - Jun 09, 2018	Community SANS
Community SANS Madison SEC401	Madison, WI	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Crystal City 2018	Arlington, VA	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, Japan	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
Minneapolis 2018 - SEC401: Security Essentials Bootcamp Style	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NC	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, Malaysia	Jul 16, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Bethesda SEC401	Bethesda, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
San Antonio 2018 - SEC401: Security Essentials Bootcamp Style	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, India	Aug 06, 2018 - Aug 11, 2018	Live Event