Global Information Assurance Certification Paper

Access Control Lists to Protect a Network from Worm/DoS Attacks

By Dennis Eck CCNA

December 4, 2003
GSEC Practical Assignment
Version 1.4, Option 1

Table of Contents

1. Abstract

Internet worms and Denial of Service (DoS) attacks have had a significant impact on businesses and governments in recent years. The damage caused by these attacks is measured in billions of dollars. Corporate productivity and government functioning are significantly impaired during these attacks.

Network security requires a Defense in Depth solution that is implemented at the client and server level as well as the network level. Solutions at the network level can include stateful firewalls, private virtual LAN's at the switch level, and packet filtering at the router level.

Five major Internet worms are reviewed in this paper: Code Red, Nimda, Slammer, Blaster, and Nachi. The network specific behavior of each virus is discussed along with research demonstrating that DoS attacks have the ability to completely overwhelm a network infrastructure.

The use of access control lists (ACL's) at the router level is a critical network security practice to safeguard a network infrastructure from worm/DoS attacks. ACL's should be implemented at several key points within a network. These locations include the network edges, including the Autonomous System (AS) boundaries and connection to the Internet, WAN links that connect geographically separate sites, and LAN access points to individual systems and end users.

This paper presents a variety of examples of ACL entries that can be used on a daily basis to protect a network from worm/DoS attacks. Examples of ACL entries are presented for general monitoring and blocking of malicious traffic, logging of potentially malicious traffic, blocking infected hosts, filtering out malicious traffic from mission critical systems, and an emergency stop ACL to block a significant worm/DoS attack.

Network administrators are encouraged to keep up to date with known vulnerabilities on the Internet and keep ACL's ready on their routers to implement at a moment's notice to protect their infrastructure.

2. Introduction

Network security has become serious business in the past few years. Internet worms and Denial of Service (DoS) attacks impact almost every user on the Internet, especially businesses and governments. While end users may experience slowness in connections or inaccessibility of certain websites, businesses and governments experience a significantly greater impact.

The financial impact sustained as a result of worm/DoS attacks is alarming. Code Red I and II cleanup costs totaled nearly $2.62 billion. The most expensive virus ever to hit was the Love Bug virus, which rang up $8.75 billion in damages by itself. Computer Economics, a research company that keeps a track of IT costs, published several

estimates on the economic damage caused by major computer viruses. The figure below provides their estimates for years 1995 to 2001. Data for the year 2002 was not available to the public as of this writing.

Analysis by Year Year	Worldwide Economic Impact ($ U.S. Billions)
2001	$13.2
2000	17.1
1999	12.1
1998	6.1
1997	3.3
1996	1.8
1995	0.5

Figure 1. Economic Impact of Malicious Code Attacks[1]

In addition to the financial impact, corporate productivity and a variety of critical government services have been significantly impacted by worms released on the Internet. The following list illustrates some of the documented damage:

- The Pentagon had to take down a number of its web sites
- The White House had to change its IP address
- Bank of America and Canadian Imperial Bank reported that many customers could not withdraw money from ATMs
- Internet congestion prevented consumers from contacting Microsoft over the Internet to download patches
- Millions of South Korean users lost Internet access when Korea Telecom Freetel and SK Telecom service failed
- Networks at the U.S. departments of State, Agriculture, Commerce were disrupted
- Some Associated Press news services and several newspapers were temporarily interrupted
- Trading volume at the Korea Stock Exchange fell to a 13-month low as a result of investors avoiding submission of orders to buy
- Continental Airlines reported widespread computer problems including delays at several major airports
- Operations were disrupted within a number of high-profile companies such as Qwest Communications, AT&T, FedEx, and Intel.

[1] Waite, "Malicious Code Attacks Had $13.2 Billion Economic Impact in 2001."

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.