

The Perils of Deep Packet Inspection

Dr. Thomas Porter 2005-01-11

Introduction

This paper looks at the evolution of firewall technology towards Deep Packet Inspection, and then discusses some of the security issues with this evolving technology.

Microsoft, Cisco, Checkpoint, Symantec, Nortel, SonicWall, NAI, Juniper/Netscreen, and others, have, in the past eighteen months started manufacturing firewall appliances that implement Deep Packet Inspection (DPI). In general, the DPI engine scrutinizes each packet (including the data payload) as it traverses the firewall, and rejects or allows the packet based upon a ruleset that is implemented by the firewall administrator. The inspection engine implements the ruleset based upon signature-based comparisons, heuristic, statistical, or anomaly-based techniques, or some combination of these.

Deep Packet Inspection promises to enhance firewall capabilities by adding the ability to analyze and filter SOAP and other XML messages, dynamically open and close ports for VoIP application traffic, perform in-line AV and spam screening, dynamically proxy IM traffic, eliminate the bevy of attacks against NetBIOS-based services, traffic-shape or do away with the many flavors of P2P traffic (recently shown to account for ~35% of internet traffic), and perform SSL session inspection.

Deep Packet Inspection essentially collapses Intrusion Detection (IDS) functionality into the firewall appliance so that both a firewall and an in-line IDS are implemented on the same device. Many of these products have recently been shown to be vulnerable to exploitation of software defects in their DPI inspection engines, however. These data suggest that the addition of these enhanced functions to firewalls may, in fact, weaken, rather than strengthen network perimeter security.

Shallow Packet Inspection

Traditionally, firewalls have provided a physical and logical demarcation between the inside and the outside of a network. The first firewalls were basically just gateways between two networks with IP forwarding disabled. Most contemporary firewalls share a common set of characteristics:

1. it is a single point between two or more networks where all traffic must pass (choke

point);

2. it can be configured to allow or deny IP (and other protocol) traffic;
3. it provides a logging function for audit purposes;
4. it provides a NAT function;
5. the operating system is hardened;
6. it often serves as a VPN endpoint; and,
7. it fails closed - that is, if the firewall crashes in some way, no traffic is forwarded between interfaces.

Steven Bellovin classically stated, "Firewalls are barriers between "us" and "them" for arbitrary values of "them.""

One of the first commercial firewalls, The DEC SEAL, was comprised of three systems. One of these, the Gate, or packet-screening device, relied upon the kernel to pass packet headers to a user-space program, screend, which informed the kernel whether or not to forward the packet. Policy was defined in the screend configuration file and this policy was then implemented by the kernel.

IP packet filtering firewalls all share the same basic mechanism: As an IP packet traverses the firewall, the headers are parsed, and the results are compared to a ruleset defined by a system administrator. The ruleset, commonly based upon source and/or destination IP address, source and/or destination port, or a combination of the two, defines what type of traffic is subsequently allowed or denied. Interestingly, some early (and not particularly popular) packet filtering implementations required that the system administrator define specific byte fields with the packet headers, and the specific byte patterns to match against. The point here is that packet filtering (and the code that performs these tasks) based upon parsing of IP headers has been common for many years.

Stateful Inspection Firewall Technology, a term coined by Check Point Software Technologies (Patent #5,606,668), describes a method for the analysis and tracking of sessions based upon source/destination IP address and source/destination ports. A stateful inspection firewall registers connection data and compiles this information in a kernel-based state table. A stateful firewall examines packet headers and, essentially, remembers something about them (generally source/destination IP address/ports). The firewall then uses this information when processing later packets. Interestingly, Lance Spitzner (<http://www.spitzner.net/>) showed that, contrary to what one would expect, sequence numbers, and other header information is not utilized by

Check Point in order to maintain connection state tracking.

Medium Depth Packet Inspection

The DEC SEAL also required a Gatekeeper device, which acted as an application proxy (AP). Application proxies or gateways are a second, common type of firewall mechanism. An AP functions by providing intermediary services for hosts that reside on different networks, while maintaining complete details of the TCP connection state and sequencing. In practice, a client host (running, for example, a web browser application) negotiates a service request with the AP, which acts as a surrogate for the host that provides services (the webserver). Two connections are required for a session to be completed - one between the client and the AP, and one between the AP and the server. No direct connection exists between hosts. Additionally, APs typically possess the ability to do a limited amount of packet filtering based upon rudimentary application-level data parsing. APs are considered by most people to be more secure than packet filtering firewalls, but performance and scalability factors have limited their distribution.

Although current stateful firewall technologies provide for tracking the state of a connection, most provide only limited analysis of the application data. Several firewall vendors, including Check Point, Cisco, Symantec, Netscreen, and NAI have integrated additional application-level data analysis into the firewall. Checkpoint, for example, initially added application proxies for TELNET, FTP, and HTTP to the FW-1 product. Cisco's PIX fixup protocol initially provided for limited application parsing of FTP, HTTP, H.323, RSH, SMTP, and SQLNET. Both vendors have since added support for additional applications.

Deep Packet Inspection

To address the limitations of Packet-Filtering, Application Proxy, and Stateful Inspection, a technology known as Deep Packet Inspection (DPI) was developed. DPI operates at L3-7 of the OSI model. DPI engines parse the entire IP packet, and make forwarding decisions by means of a rule-based logic that is based upon signature or regular expression matching. That is, they compare the data within a packet payload to a database of predefined attack signatures (a string of bytes). Additionally, statistical or historical algorithms may supplement static pattern matching.

Analysis of packet headers can be done economically since the locations of packet header fields

are restricted by protocol standards. However, the payload contents are, for the most part, unconstrained. Therefore, searching through the payload for multiple string patterns within the datastream is a computationally expensive task. The requirement that these searches be performed at wirespeed adds to the cost. Additionally, because the signature database is dynamic, it must be easily updateable. Promising approaches to these problems include a software-based approach (Snort implementing the Boyer-Moore algorithm), and a hardware-based approach (FPGA's running a Bloom filter algorithm).

DPI technology can be effective against buffer overflow attacks, denial of service (DoS) attacks, sophisticated intrusions, and a small percentage of worms that fit within a single packet. However, the complexity and immaturity of these systems have resulted in a number of recent exploits, as will be shown below.

Example Exploits

1. [Snort RPC Preprocessing Vulnerability](#)

Researchers at Internet Security Systems (ISS) discovered a remotely exploitable buffer overflow in the Snort stream4 preprocessor module. When the RPC decoder normalizes fragmented RPC records, it incorrectly checks the lengths of what is being normalized against the current packet size, leading to an overflow condition. The RPC preprocessor is enabled by default. Remote attackers may exploit the buffer overflow condition to run arbitrary code on a Snort sensor with the privileges of the Snort IDS process, which typically runs as the superuser.

2. [Trend Micro InterScan VirusWall Remote Overflow](#)

An implementation flaw in the InterScan VirusWall SMTP gateway allows a remote attacker to execute code with the privileges of the daemon. Due to an implementation fault in VirusWall's handling of a UUencoded file name, it is possible for a remote attacker to specify an arbitrarily long string, overwriting the stack with user defined data, and allowing a remote attacker to execute arbitrary code.

3. [Microsoft ISA Server 2000 H.323 Filter Remote Buffer Overflow Vulnerability](#)

The H.323 filter used by Microsoft ISA Server 2000 is prone to remote buffer overflow vulnerability. The condition presents itself due to insufficient boundary checks performed

by the Microsoft Firewall Service on specially crafted H.323 traffic. Successful exploitation of this vulnerability may allow a remote attacker to execute arbitrary code in the context of Microsoft Firewall Service running on ISA Server 2000. This may lead to complete control of the vulnerable system.

4. [Cisco SIP Fixup Denial of Service \(DoS\)](#)

The Cisco PIX Firewall may reset when receiving fragmented SIP INVITE messages.

5. [Cisco H.323 Vulnerabilities](#)

Multiple Cisco products contain vulnerabilities in the processing of H.323 messages, which are typically used in Voice over Internet Protocol (VoIP) or multimedia applications.

6. [Check Point FireWall-1 H.323 Vulnerabilities](#)

FireWall-1 is affected by the recently reported vulnerabilities in various products' H.323 protocol implementation. The vulnerabilities are caused due to various errors in the processing of H.225 messages over TCP.

Observations

1. Recently, the FBI noted that 98% of organizations use firewalls, but that 56% of them had still experienced unauthorized network access.
2. Companies today are increasingly adopting B2B and B2C applications that rely upon HTTP transport to tunnel through firewalls.
3. P2P file sharing has become "the" latest killer application, and brings with it a number of concerns: files are often quite large and P2P traffic flow is asymmetric, leading to bandwidth problems; and P2P traffic is often tunneled through other protocols, thus circumventing security controls

The bottom line is that in order to exercise sound bandwidth and security controls, organizations and service providers must be able to differentiate traffic types based upon the contents of the application payload.

Conclusion

Deep Packet Inspection is a promising technology in that it may help to solve these problems. DPI engines are situated at network boundaries where bandwidth and security controls are logically implemented. New, programmable ASICs coupled with efficient algorithms can realistically parse the entire contents of each packet at gigabit speeds. Also, combining Firewall and IDS within a single device should simplify device configuration and management. But there are concerns as well.

One of the primary benefits of the traditional firewall/IDS deployment is that the failure of one component does not leave the network completely unprotected. Deploying devices with separate functionality also prevents being locked in to a single vendor. Additionally, IDS appliances can be deployed throughout the LAN and can monitor internal traffic as opposed to boundary areas between networks. When a DPI appliance fails or is misconfigured, will the internal network be exposed?

DPI adds complexity to an already complicated solution - firewalls, IDSs, session border controllers, and honeypots/nets are currently arrayed at network margins in order to defend security boundaries; and all of these require regular monitoring, configuration changes, and log analysis. Will DPI appliances replace these tools or will they add to rack clutter? And, as seen above, DPI appliances can introduce their own native vulnerabilities as a consequence of their mechanisms of action. Time and experience will determine the fate of this new technology.

About the author

[Thomas Porter](#), Ph.D., CISSP, is a security architect with Avaya's Global Managed Services division. He has spent over eleven years in the networking and security industry as a consultant, speaker and developer of security tools; he also holds numerous security certifications. Tom lives in Chapel Hill, North Carolina with his wife. View [more articles by Thomas Porter](#) on SecurityFocus.

[Privacy Statement](#)

Copyright 2006, SecurityFocus