

Firewall Evolution - Deep Packet Inspection

Ido Dubrawsky 2003-07-29

Firewalls provide a variety of services to networks in terms of security. They provide for network address translation (NAT), virtual private networks (VPN), and filtering of traffic that does not conform to the network's stated security policy. There are many forms of firewalls from simple packet filters to circuit-level gateways to proxy firewalls. Firewalls are being asked to fill a larger and more varied role in network security these days than several years ago. One of the more recent innovations in firewall technology is the application of deep packet inspection or DPI. Deep Packet Inspection can be seen as the integration of Intrusion Detection (IDS) and Intrusion Prevention (IPS) capabilities with traditional stateful firewall technology. Traditional networks have a defined boundary demarcated by a firewall with an IDS sensor sitting behind it.

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. Also, IDS appliances can be deployed throughout the LAN and monitor traffic *inside* the LAN as opposed to boundary areas between networks. This design is illustrated in Figure 1 below. The IDS monitors traffic that passes through the firewall (as defined in the firewall policy) and inspects packets for malicious activity.

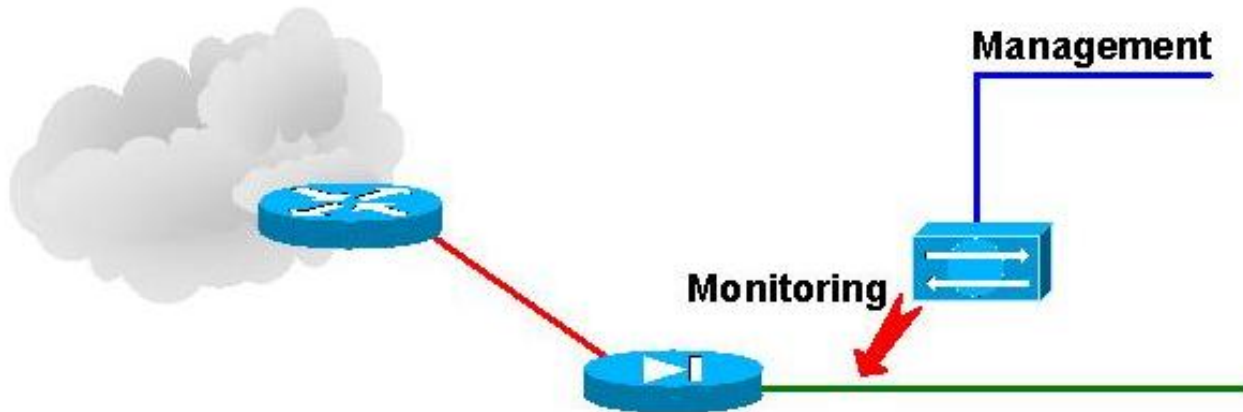


Figure 1 - Traditional Firewall Deployment Design

With Deep Packet Inspection firewalls the IDS collapses into the firewall such that the firewall provides for in-line IDS capabilities. This eliminates an additional piece of network equipment which can fail while increasing the capabilities inherent in the firewall. This article will cover one particular form (and function) of firewalls -- stateful firewalls and how deep packet inspection provides greater functionality to these firewalls than ever before.

Stateful Firewalls -- An Overview

In the early stages of firewalls all traffic had to be explicitly specified whether it was permitted. A good example of a very rudimentary firewall was the original Linux firewall. This firewall (whether manipulated with *ipfwadm* or *ipchains*) required that all traffic traversing the firewall (regardless of direction) be specified. The firewall did not keep track of the various sessions that may exist at any one time in the firewall.

Stateful inspection changed all that. Invented by Check Point Software Technologies in the mid-to-late 1990s stateful inspection quickly became an industry standard. Stateful inspection provides for the analysis of packets at the network layer as well other layers (typically the transport layer in the OSI model but the firewall may look at layers above that as well) in order to assess the overall packet. By combining information from various layers (transport, session, and network) the firewall is better able to understand the protocol it is inspecting. This also provides for the ability to create virtual sessions in order to track connectionless protocols such as UDP-based applications as well as RPC-based applications.

Application proxy firewalls have been around for a long time but have failed to control the emerging threat inherent in data-driven attacks. Additionally, the multitude of applications requiring support as well as the additional latency have dampened demand for application proxy firewalls.

The reality of modern application demands and capabilities require that firewalls with a much more intimate level of knowledge of the application payload. Emerging applications utilizing XML and Simple Object Access Protocol (SOAP) require the firewall to monitor the content within the packets at wire-speed. Additionally, applications which can change their communication ports in order to bypass outbound filtering or those which tunnel within commonly allowed ports (such as 80/TCP) must be monitored as well in order to provide for the maximum amount of security within the network. In order to meet these new demands stateful firewall technology must evolve.

Deep Packet Inspection

Deep Packet Inspection is a term used to describe the capabilities of a firewall or an Intrusion Detection System (IDS) to look within the application payload of a packet or traffic stream and make decisions on the significance of that data based on the *content* of that data. The engine that drives deep packet inspection typically includes a combination of signature-matching technology along with heuristic analysis of the data in order to determine the impact of that communication stream. While the concept of deep packet inspection sounds very nice it is not so simple to achieve in practice. The inspection engine must use a combination of signature-based analysis techniques as well as statistical, or anomaly analysis, techniques. Both of these are borrowed directly from intrusion detection technologies. In order to identify traffic at the speeds necessary to provide sufficient performance newer ASICs will have to be incorporated into existing firewall designs. These ASICs, or Network Processors Units (NPUs), provide for fast discrimination of content within packets while also allowing for data classification. Deep Packet Inspection capable firewalls must not only maintain the state of the underlying network connection but also the state of the application utilizing that communication channel.

For example, consider an SMTP connection between a mail client and a server shown in Figure 1(a) below. The client opens the connection with the typical TCP three-way handshake. The firewall allows the connection because it has the ruleset stating that access to TCP port 25 on the mail server host is permitted. In Figure 1(b)b. the connection has been entered into the state table of the firewall.

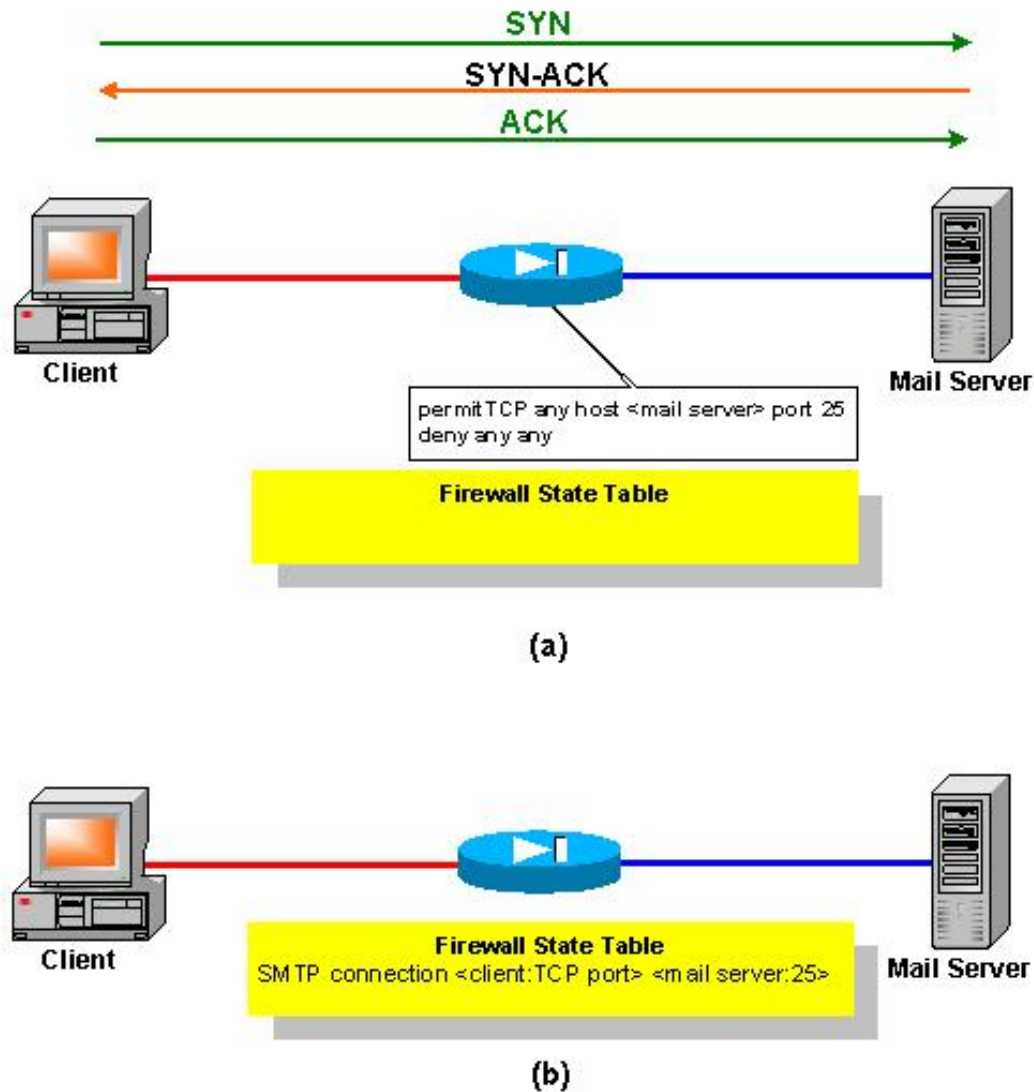


Figure 2 - Stateful Firewall Connection

For most stateful firewalls the establishment of the connection and the monitoring of it for when connection is terminated is sufficient. However, such firewalls do not look further up the protocol stack for events that may be considered "out-of-bounds" in the application. With a firewall that is capable of Deep Packet Inspection the firewall can look at the SMTP protocol and monitor it for any attacks. This is shown in Figure 2 below. In Figure 2(a) the client establishes the SMTP connection by following the RFC defined protocol steps of issuing a HELO, waiting for the response by the mail server. The client may then issue a variety of commands include sending e-mail by specifying the SMTP command **MAIL FROM:** . In Figure 2(b) the client tries to issue a **VERFY** command. The firewall monitoring the communication between the client and the mail server may raise an alarm or respond to the **VERFY** command by disallowing it. The client may also try to exploit the sendmail address token overflow (discussed in the CERT bulletin CA-2003-12) in order to gain shell access to the server. The firewall, because it is capable of Deep Packet Inspection, is able to identify the exploit attempt and deny the connection. Additionally, it may deny the connection from the client altogether.

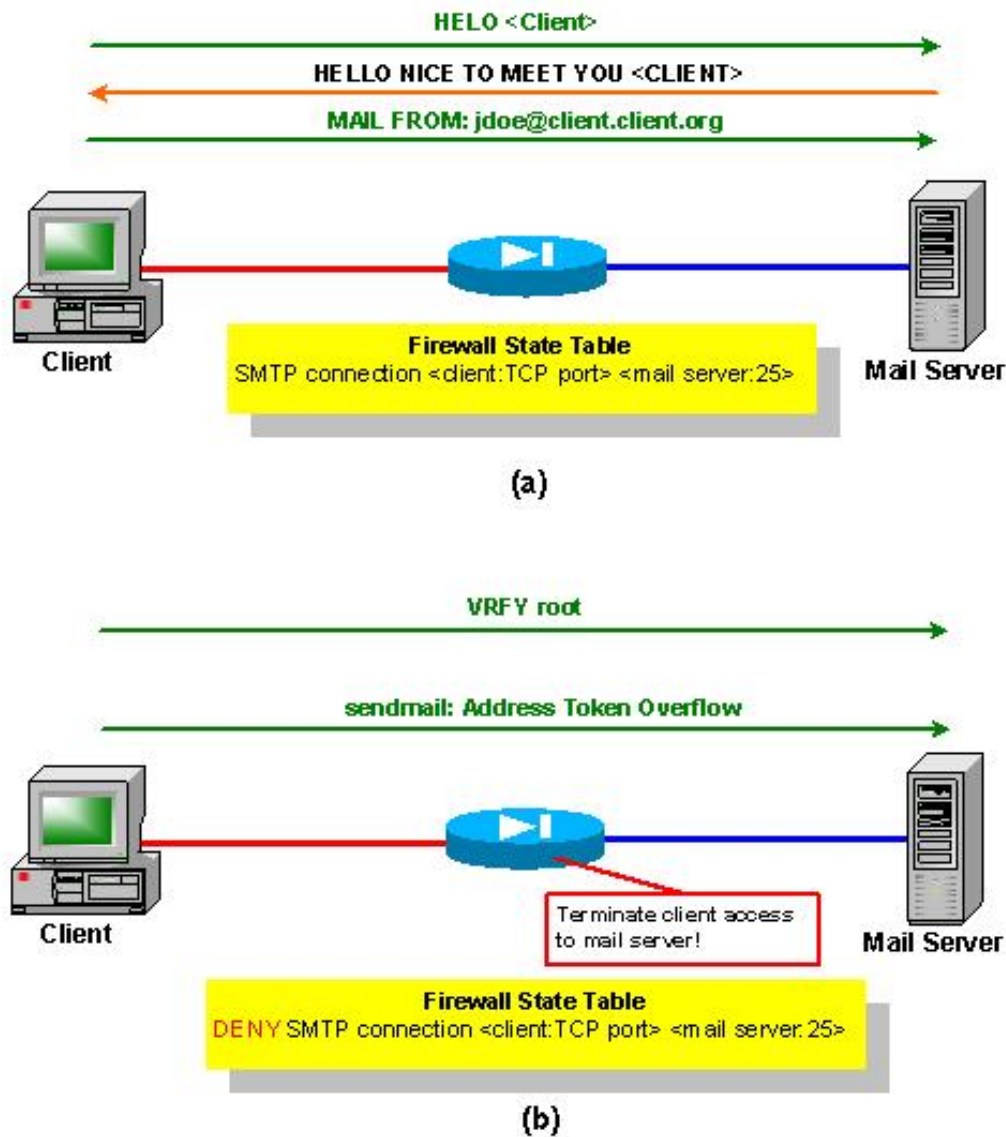


Figure 3 - Deep Packet Inspection Firewall

In order to be successful with Deep Packet Inspection the firewall must provide significant intrusion detection and prevention capabilities. These capabilities include performing anti-virus screening in-line and at wire-speeds. Additionally the firewall must be able to parse, analyze, and, if necessary, filter Extensible Markup Language (XML) traffic, dynamically proxy instant messaging services such as AIM, Yahoo IM, and MSN IM. Additionally the firewall will have to provide for wire-speed Secure Socket Layer (SSL) session inspection and filtering. This will obviously require the capability to decrypt an SSL session and then re-establish it once the packets have been inspected.

The need for this technology and this capability in firewalls stems from such data-driven attacks as *Code Red*, *NIMDA* and the more recent *SQL Slammer* worm. Current IDS technology, while able to detect these attacks, provided very little preventative capabilities against these attacks. Each of these worms infected a significant number of systems within a relatively short period of time. NIMDA's multi-vector infection routes posed serious difficulties for IDS in particular. While IDS provided some relief from each of these attacks, moving the detection and response directly to the firewall through Deep Packet Inspection provides for immediate termination of the attack by cutting the line of communication at a network demarcation point.

Next Generation Firewalls

While current stateful firewall technology provides for tracking the state of a connection, most current firewall products offer limited analysis of the application data. Several firewall vendors, including Check Point, Cisco, Netscreen, Network Associates (who recently acquired Intruvert), and TippingPoint, are moving in the direction of integrating this analysis into the firewall. Cisco's PIX **fixup** commands provide for some Deep Packet Inspection capabilities in the PIX firewall. For example, the command: **fixup protocol http** causes the PIX to perform several functions including:

- URL logging of GET messages
- URL screening through N2H2 or Websense
- Java and ActiveX filtering

For the last two functions above the firewall must also be configured with the **filter** command. These functions represent a small subset of capabilities which must be included in firewalls in order to provide a greater degree of protection to networks. Like traditional IDSs these new capabilities rely on pattern-matching techniques to identify attacks and, also as with traditional IDSs, attackers can exploit weaknesses in the detection methods to avoid raising alarms.

As Deep Packet Inspection technology continues to improve the capability to provide more robust and dynamic protection to the network will only continue to increase. Moving the inspection of the data in packets to the network firewall provides network administrators greater flexibility in defending their systems from malicious traffic and attacks. Such firewalls do not eliminate the need for Intrusion Detection Systems, they merely collapse the IDS that should sit directly behind the firewall into the firewall itself. However, IDSs role within the network as part of an overall defense-in-depth approach remains unchanged.

Author Credit

View [more articles by Ido Dubrawsky](#) on SecurityFocus.

[Privacy Statement](#)

Copyright 2006, SecurityFocus