Firewall Evolution - Deep Packet Inspection

by Ido Dubrawsky

last updated July 29, 2003

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

One of the primary benefits of the traditional firewall/IDS deployment is that the failure of one component completely unprotected. Also, IDS appliances can be deployed throughout the LAN and monitor traffic *insid* boundary areas between networks. This design is illustrated in Figure 1 below. The IDS monitors traffic tha defined in the firewall policy) and inspects packets for malicious activity.

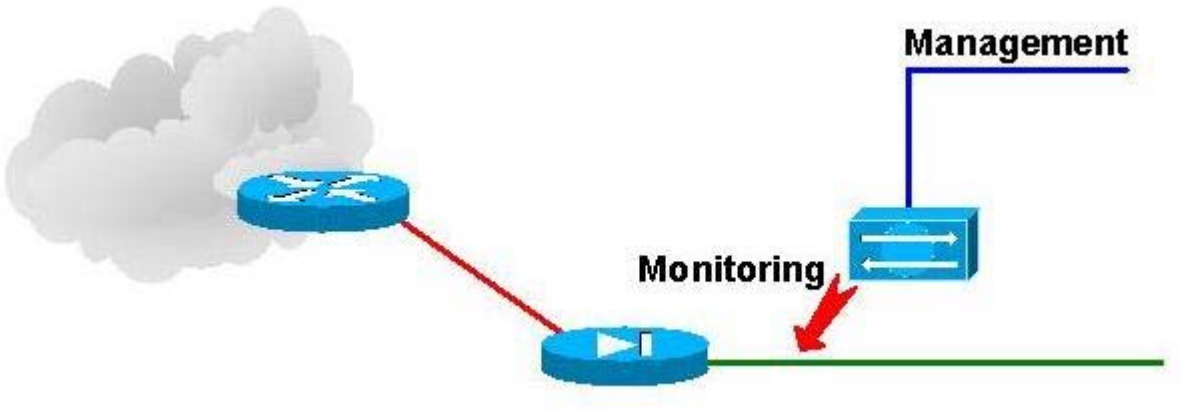

Figure 1 - Traditional Firewall Deployment Design

With Deep Packet Inspection firewalls the IDS collapses into the firewall such that the firewall provides for i eliminates an additional piece of network equipment which can fail while increasing the capabilities inheren cover one particular form (and function) of firewalls -- stateful firewalls and how deep packet inspection pr 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 exa firewall was the original Linux firewall. This firewall (whether manipulated with *ipfwadm* or *ipchains* require firewall (regardless of direction) be specified. The firewall did not keep track of the various sessions that m firewall.

Stateful inspection changed all that. Invented by Check Point Software Technologies in the mid-to-late 199 became an industry standard. Stateful inspection provides for the analysis of packets at the network layer transport layer in the OSI model but the firewall may look at layers above that as well) in order to assess t information from various layers (transport, session, and network) the firewall is better able to understand t also provides for the ability to create virtual sessions in order to track connectionless protocols such as UDI RPC-based applications.

Application proxy firewalls have been around for a long time but have failed to control the emerging threat Additionally, the multitude of applications requiring support as well as the additional latency have dampene

firewalls.

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

Deep Packet Inspection

Deep Packet Inspection is a term used to describe the capabilities of a firewall or an Intrusion Detection Sy application payload of a packet or traffic stream and make decisions on the significance of that data based engine that drives deep packet inspection typically includes a combination of signature-matching technolog the data in order to determine the impact of that communication stream. While the concept of deep packet not so simple to achieve in practice. The inspection engine must use a combination of signature-based anal statistical, or anomaly analysis, techniques. Both of these are borrowed directly from intrusion detection te traffic at the speeds necessary to provide sufficient performance newer ASICs will have to be incorporated These ASICs, or Network Processors Units (NPUs), provide for fast discrimination of content within packets classification. Deep Packet Inspection capable firewalls must not only maintain the state of the underlying n 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. with the typical TCP three-way handshake. The firewall allows the connection because it has the ruleset sta on the mail server host is permitted. In Figure 1(b)b. the connection has been entered into the state table

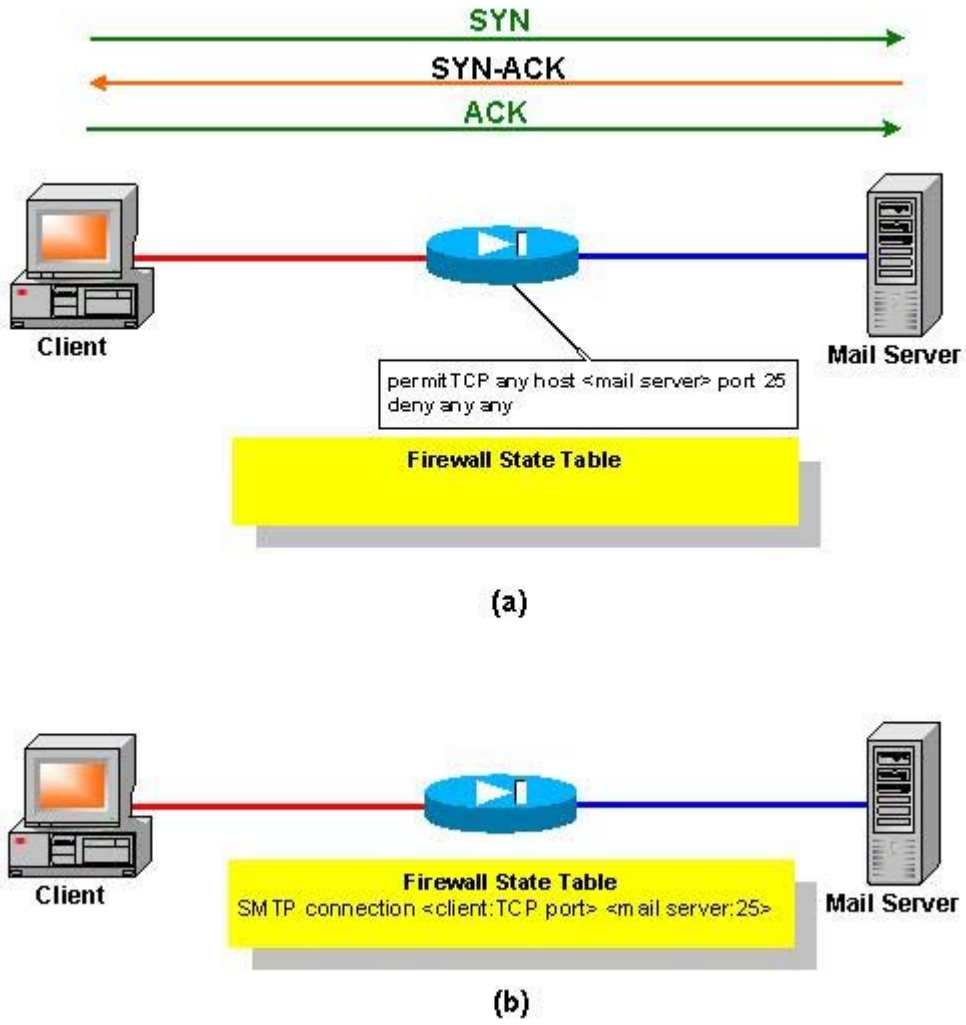

Figure 2 - Stateful Firewall Connection

For most stateful firewalls the establishment of the connection and the monitoring of it for when connectior However, such firewalls do not look further up the protocol stack for events that may be considered "out-of a firewall that is capable of Deep Packet Inspection the firewall can look at the SMTP protocol and monitor i in Figure 2 below. In Figure 2(a) the client establishes the SMTP connection by following the RFC defined pı waiting for the response by the mail server. The client may then issue a variety of commands include sendi SMTP command **MAIL FROM:** . In Figure 2(b) the client tries to issue a **VRFY** command. The firewall moni between the client and the mail server may raise an alarm or respond to the **VRFY** command by disallowin exploit the sendmail address token overflow (discussed in the CERT bulletin CA-2003-12) in order to gain s firewall, because it is capable of Deep Packet Inspection, is able to identify the exploit attempt and deny th may deny the connection from the client altogether.

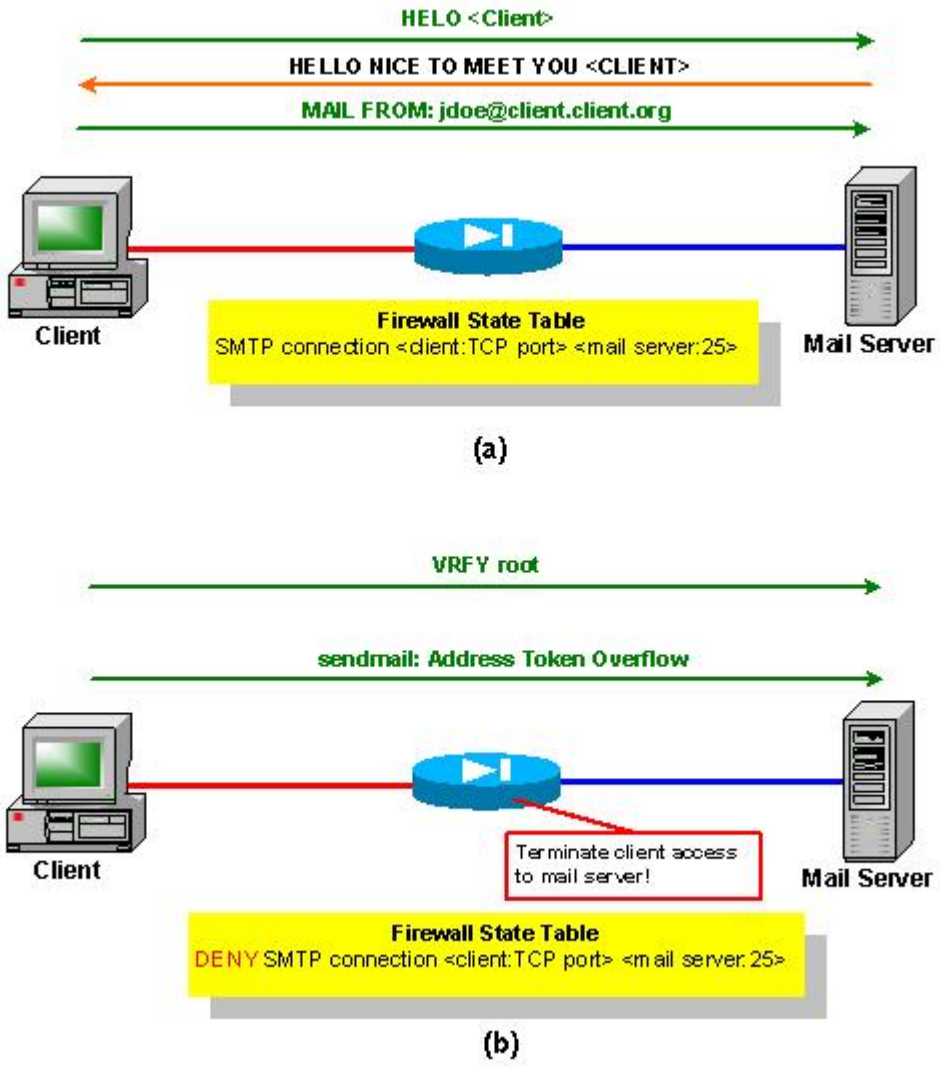

Figure 3 - Deep Packet Inspection Firewall

In order to be successful with Deep Packet Inspection the firewall must provide significant intrusion detecti These capabilities include performing anti-virus screening in-line and at wire-speeds. Additionally the firewa analyze, and, if necessary, filter Extensible Markup Language (XML) traffic, dynamically proxy instant mess Yahoo IM, and MSN IM. Additionally the firewall will have to provide for wire-speed Secure Socket Layer (S filtering. This will obviously require the capability to decrypt an SSL session and then re-establish it once th

The need for this technology and this capability in firewalls stems from such data-driven attacks as *Code R* *SQL Slammer* worm. Current IDS technology, while able to detect these attacks, provided very little prever attacks. Each of these worms infected a significant number of systems within a relatively short period of tir infection routes posed serious difficulties for IDS in particular. While IDS provided some relief from each of detection and response directly to the firewall through Deep Packet Inspection provides for immediate term 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 firew analysis of the application data. Several firewall vendors, including Check Point, Cisco, Netscreen, Network acquired Intruvert), and TippingPoint, are moving in the direction of integrating this analysis into the firewa provide for some Deep Packet Inspection capabilities in the PIX firewall. For example, the command: **fixup** 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 functi capabilities which must be included in firewalls in order to provide a greater degree of protection to networ new capabilities rely on pattern-matching techniques to identify attacks and, also as with traditional IDSs, in the detection methods to avoid raising alarms.

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

Author Credit

View more articles by Ido Dubrawsky on SecurityFocus.