SECURITY

Why Deep Packet Inspection still matters

Deep Packet Inspection (DPI) is a technology that should offer much more weight than SPI (Stateful Packet Inspection).

By Frank Ohlhorst | October 2, 2014, 6:30 AM PST

Security vendors like to throw around a lot of acronyms when discussing their technologies. However, many of those acronyms have much more weight than others. Take for example DPI (Deep Packet Inspection), a technology that should offer much more weight than SPI (Stateful Packet Inspection), at least when it comes to enterprise security.

However, many firewall and security appliance vendors use SPI performance as there calling card, touting their packet throughput capabilities based upon what is little more than a simplified packet scan. Although SPI performance is very important, especially when it comes to calculating acceptable latency and overall application throughput, SPI comes up short in the security department and can let some devastating threats slip through the cracks to compromise network security. It all comes down to sacrificing security for speed.

To truly understand the performance/security paradigm, one has to take a deep dive into how DPI and SPI differ and why those differences matter.

Stateful Packet Inspection (SPI) works at the network layer of the OSI model and examines some very basic information contained within the packet, such as the packet header, packet footer and also determines if the packet belongs to a valid session. That information is used by a basic firewall to determine if the packet should be allowed to enter the network or be blocked.

Firewalls using SPI also check to see what connections have been established from the inside of the network to the Internet, using that information to determine if there is an open connection related to the packet before allowing the packet to traverse the firewall and into the internal network. If the packet fails to meet any of the basic requirements set forth by the firewall, it will be rejected.

However, SPI is little more than a basic gatekeeper, simply checking header and footer information, as well as the origin and destination of the packet. Simply put, SPI offers no knowledge as to what the packet contains and if that packet is part of a larger transmission of packetized information. Therein lies the problem, if the packet appears to be legitimate as indicated by its basic transportation information, SPI will allow that packet to travel into the network, even if the packet contains malicious code or other damaging data.

Deep Packet Inspection (DPI) looks at not only the header and footer of a packet, but also examines the data part (content) of the packet searching for illegal statements and predefined criteria, allowing a firewall to make a more informed decision on whether or not to allow the packet through based upon its content.

Simply put, DPI delves into the data content of the packet, which allows additional determinations to be made before that packet can travel into the network.

DPI accomplishes that by dissembling incoming packets, examining the payload (data), comparing that data with defined criteria, and then re-assembles the packet for transmission (or rejection). When examining the payload, DPI engines can also employ signature matching, stealth payload detection and numerous other security capabilities.

SPI vs. DPI

It is obvious that DPI offers better protection than SPI, however there are other factors to consider - one being speed. SPI is many times faster than DPI, since it does not have to examine payloads and other data centric elements found in the typical IP packet.

On the other hand, that speed comes at a price - security. While SPI may be able to block hordes of attackers trying to flood a network with bad packets, it does very little for when it comes to malicious code being delivered into the network. SPI leaves that task to other security products, such as anti-virus gateways, intrusion detection systems and security appliances.

Nonetheless, that is an area where DPI starts to shine - although DPI requires much more processing power to accomplish its tasks, it ultimately delivers a methodology that makes sure that not only is the packet formed correctly, but it also does not contain any malicious

code. What's more, appliances using DPI are able to delve into application centric information, allowing different applications to be protected in different ways from threats.

With that in mind, it becomes clear as to why DPI proves to be a better security centric technology than SPI. However, from a security point of view, it may work best to employ both - using SPI at the edge to discard malformed packets and then only allowing the rest to enter the network for more analysis under DPI - a combination that can deliver both speed and security.

More to the eye with DPI

While DPI has garnered a strong foothold in the auspices of security, DPI offers much more than packet data examination. Today, network (and application) performance management tools are coming on to the scene that gather DPI information to create a better understanding of network traffic, unifying application and network performance management into a singular element.

The value offered there comes in the form of improved troubleshooting, where a network manager can see the whole traffic picture (both application and infrastructure related) in a single view to determine what the root cause is for a performance related problem.

Not only does DPI offer advantages with performance management, it also offers additional information that can be used for network trending, network analytics and even forensics.

It all comes down to having the right information at the right time, regardless if it is for security, analytics or network forensics. The time has come for network managers to demand DPI on some level, prices on DPI infused solutions have fallen and the information provided can be of immense value for today's enterprise networks.

About Frank Ohlhorst

Frank J. Ohlhorst is an award-winning technology journalist, author, professional speaker and IT business consultant. He has worked in editorial at CRN, eWeek and Channel Insider, and is the author of Big Data Analytics. His certifications include MC...