Are You Prepared For The Future Of Security Threats?

The deep packet inspection software you used in the past is no match for the ever-evolving malicious content that's threatening your customers' networks now.

By Hongwen Zhang, president
and CEO, Wedge Networks

Traditional network filtering technologies are becoming obsolete. As network traffic continues to increase in volume and complexity, malicious content and attacks are evolving at an alarming rate.

In 2011, Microsoft reported that one in every 14 downloads contained malicious content, which could jeopardize operations, reputation and create customer relationship management challenges. According to PwC's 2012 Global State of Information Security Survey, a mere 43% of security experts are confident in their information security strategy. Malicious content and non-compliant data (which have evolved with the proliferation of mobile data usage, social media and cloud computing) can easily breach a weak network security system. Consequently, organizations will suffer from information leakage and possible IT infrastructure damage.

Hongwen Zhang

Dr. Hongwen Zhang is president and CEO of Wedge Networks, a provider of remediation-based deep content inspection for high-performance, network-based Web security.

Standard inspection technologies that secure networks at the packet level, such as packet filtering and deep packet inspection (DPI), are relatively inefficient and unable to provide safe usage of the new Internet. A different approach to network security needs to be taken.

The Limits of Traditional Technologies: Deep Packet Inspection

DPI is currently the most widely used and readily available technology for monitoring and managing network packet data. It operates by matching IP packet sequences against a known set of offending patterns; to be effective, however, it must do so at wire speed. This poses two major limitations:

- At a given time, a DPI chip is able to hold only a limited amount of packets for pattern matching. The amount of IP packets necessary for transmitting an application payload often surpasses the number of packets that a DPI system can inspect at once. As a result, malware embedded in large application payloads will slip onto the network undetected.
- The second major problem posed by real-time DPI is the limited amount of memory available for pattern matching. Since the packet data obtained from a DPI system must be matched against a known malware threat, the amount of unique signatures (against which the system can match) is restricted.

An inept DPI system is unable to properly secure a network. As a result, unsupported application types, as well as nested, zipped or archived files, will easily slip through a DPI network.

Preparing for the Future: Deep Content Inspection

In order to address undetected and emerging threats, a different approach to network data inspection (one that incorporates thorough analysis) must be employed. Deep content inspection (DCI) is an advanced form of network filtering that reassembles, decompresses and/or decodes network traffic packets into their constituting application level objects (often referred to as MIME objects). Functioning as a fully transparent device at a more comprehensive level, DCI does more than simply check the body or header of data packets moving through a network. Instead, DCI examines the entire object and detects any malicious or non-compliant intent.

To understand the intent of data-in-motion, the current generation of DCI performs full content-based inspections in real-time. As a result, DCI gains a much broader inspection scope than would be available by solely matching packet sequences against patterns. In addition, DCI is able to execute a reputation search and behavior analysis on structured or packed data, resulting in an entirely new level of protection. By monitoring content across multiple packets, DCI finds and assesses signatures that cross packet boundaries.

By honing in on the content and intent of data, and moving away from traditional packet inspection, DCI provides a more comprehensive approach to screening for attacks and malicious content. As such, DCI is more to effectively able to secure enterprises, governments and service providers against today's threats. ●