SearchSecurity

e-guide

E-Guide

NEXT-GEN FIREWALLS: PREVENTING APPLICATION-LAYER ATTACKS

BY JOHN BURKE

TechTarget

SearchSecurity

NEXT-GENERATION FIREWALLS ARE "next generation" for a lot of reasons, one being they are identity aware, highly scalable and application aware. Application awareness presents IT security teams with a new set of opportunities and challenges. This expert E-Guide highlights the benefits of these firewalls and provides tips on how to tackle potential challenges you may encounter.

SearchSecurity

Next-generation firewalls are "next generation" for a lot of reasons, including that they typically are identity aware, highly scalable and "application aware" -- and it's this last point, application awareness, that presents IT security teams with a grand new set of opportunities and challenges.

The concept of application awareness is both clear and somewhat misleading: clear in that, certainly, these devices are aware that a particular traffic stream can be tied back to a specific application, but misleading in that they can do a lot more than detect and identify an application's traffic. They are also able to act on that information: to selectively block or otherwise affect use of applications, or even components of applications, not just specific ports and protocols as with an old-fashioned firewall.

As important, and less obvious, application awareness in this case means they can often detect and defend against attacks aimed at applications; they can even serve as a temporary or a permanent fix to an application-level vulnerability by blocking malicious traffic. This capability is particularly useful with two of the most common application attacks: buffer overflows and SQL injections.

A buffer overflow, of course, happens when the application code where input is gathered does not limit that input properly. By pushing too much data into the input -- say by pasting 256,000 letters into a text field that can't accept

that much input -- an attacker can sometimes gain access to the server's processor and get it to execute whatever code they please. Most often this kind of attack is used to install some kind of back door on a system so the attacker can gain control of it.

A SQL injection attack relies on an application's interface with a back-end database and takes advantage, like a buffer overflow, of poorly filtered or controlled inputs. If a Web page has a form facing the user -- for example, a form for a health plan customer to look up clinics -- they might have a field to enter a ZIP code. The application will take that information and use it to create a SQL query. However, if the input is passed along without being adequately filtered, a malicious user could add arbitrary SQL commands to it and have them passed into the database. For example, by slipping in extra code, they could inject into the SQL stream a command to drop the table of physician information. Even if this data can be recovered, it will seriously disrupt operations to have it deleted this way.

Of course, NGFWs are not a panacea, and they are not without their own challenges. Unlike a signature-based antivirus engine, they are built from the ground up to be aware of how individual users and systems behave, essentially to understand the context of the network packets. This means they lack the

same constant stream of updates that a virus engine needs, but nonetheless they do need to be kept up-to-date so they can "learn" an ever-increasing number of application fingerprints (the characteristics of traffic beyond port and protocol, including potentially the content of specific packets). And, since it does maintain a rule set, it is potentially susceptible to the same kind of rule bloat to which traditional firewalls so often fall prey.

It's also important to note that for those organizations that have developed applications in-house (likely the majority of large enterprises), the firewall will not recognize them or understand how to handle them until they train it in or manually define an application fingerprint, a process that may need to be repeated as applications are upgraded or replaced.

Obviously, for all its value, an NGFW can't protect against every kind of vulnerability or risk. For example, it can limit Facebook users to posting plain text, and really isn't intended to scan such text for protected information such as client names. An NGFW can't even prevent all exploitation of application vulnerabilities, and so should not be seen as an alternative to implementation of a secure software development lifecycle.

However, the ability of next-generation firewalls to identify and block or disrupt attacks like buffer overflows and SQL injections allows them to serve as

SearchSecurity

a first line of defense against such attacks, and also as a detection mechanism, providing developers with feedback on what they have to code against. While NFGWs are not without challenges, their advanced defensive capabilities make them important to evaluate for inclusion in any robust enterprise defense for the enterprise and the datacenter.

JOHN BURKE is principal research analyst with Nemertes Research.

SearchSecurity

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.