Strategy, Threat intelligence

Advancing firewalls

SC Staff July 2, 2012

The security mainstay is evolving and becoming entrenched into the enterprise as departmental gateways. Deb Radcliff reports.

Before pummeling the Vatican website with a distributed-denial-of-service (DDoS) attack in February, members of the Anonymous group probed the site to find the best means to drain it of computational resources. Ultimately, they targeted the site's search window with a specially crafted URL that incorporated common search terms to overload the server.
"If you look at where the action was in the Vatican case, a network firewall couldn't have detected or stopped a DDoS like this because these are expected application behaviors a traditional firewall would simply allow," says Rob Rachwald, director of security strategy for Imperva, a Redwood Shores, Calif.-based provider of data security solutions which, according to a company blog posted in February, thwarted the attempted intrusion. "Attacks like these are moving up the stack to the applications, so firewalls must also move up the stack to become application-aware."

Unlike firewalls of 10 years ago, today's "advanced," or "next-generation," firewalls, as they are being called, do a whole lot more than allow or deny traffic based on port and destination – so much so that some suggest the firewall name may be passé.

> **"Firewalls are no longer just firewalls, they're more like multifunction internet communication gateways."**
>
> *– Sasha Puric, senior director of IT for Toronto-based Maple Leaf Sports & Entertainment*

"Firewalls are no longer just firewalls, they're more like multifunction internet communication gateways," says Sasha Puric, senior director of IT for Toronto-based Maple Leaf Sports & Entertainment (MLSE). "These multifunction gateways are part of our infrastructure, enabling

MLSE – with four professional sports teams, five venues and three TV channels – has embraced Facebook, Twitter, gaming platforms and other social media forms to interact directly with its audience. Thus, it can't rely on a traditional firewall that would be unable to distinguish traffic types.

To secure these traffic types, MLSE introduced Dell SonicWALL's Next-Generation Firewalls into its portfolio. This platform recognizes, inspects, allows or denies social media and streaming traffic based on multiple rules, such as location, device, user, application and content.

Types and deployments

“There are many flavors of firewalls today at different layers of the stack and each adds an additional layer of security,” says Roxana Bradescu, director of product management for Oracle Database Security.

For example, web application firewalls (WAFs) are one layer being widely deployed in today's advanced gateways – and for good reason. Of the 9,300 malicious websites detected daily in 2011, 61 percent were good sites that had been compromised, according to Symantec's “Internet Security Threat Report,” published in April.

WAFs can look beyond the application traffic type going from port and destination (which is what traditional firewalls used to monitor). Additionally, WAFs can look deeper into user and traffic behaviors so they can detect attacks that look like normal application traffic, such as DDoS, SQL injections, iFrame and forms-field manipulations, and many more application attack methods that would fly under the radar of traditional firewalls.

A database firewall is another type of application firewall that is often bundled with WAFs, either through a single vendors such as Imperva, or through a database-centric provider such as Oracle.

“Enterprise gateway firewalls must handle the volume, velocity and variety of traffic they inspect…”

– Tony Zirnoon, senior director of global security strategy for VSS Monitoring

blacklists using a finetuned “grammar analysis.”

Not to be forgotten are network firewalls, which will never abandon their posts at the perimeter, says Gabi Reish, head of product management for Check Point Software Technologies, a global internet security company with U.S. headquarters in Redwood City, Calif.

They too are providing deep-packet inspection, virtual private network (VPN), application protection, whitelisting, intrusion detection system (IDS)/intrusion prevention system (IPS) and other capabilities that their predecessors didn't have, he says.

Use it or lose it

Next-generation firewalls can perform DPI, correlation, quarantine, reporting and blocking and other actions with more accuracy and negligible impact on performance, according to analysts and vendors.

However, in a recent survey conducted by Crossbeam, a Boxborough, Mass.-based firewall management vendor, 81 percent of 560 IT professionals who responded didn't turn on the prevention portion of their next-generation firewalls. Also, these users are barely using any of the firewall features due to concerns with workflow interruption.

Thus emerges another management layer supporting today's firewalls: load balancing and bandwidth optimization.

“Enterprise gateway firewalls must handle the volume, velocity and variety of [inbound/outbound] traffic they inspect, while offering a high security service assurance via load balancing, filtering and other network traffic optimization techniques,” says Tony Zirnoon, senior director of global security strategy for VSS Monitoring, an international network intelligence optimization company whose central U.S. office is in San Mateo, Calif.

Network speeds will need to evolve to keep up with complexities, he says. This includes new varieties and forms of traffic to parse, open and inspect (down to each individual packet), as well as more types of wrappers and encryption with which to contend.

according to analysts. As with other emerging technology markets, organizations are being forced between opting for best-of-breed firewalls (supported by external third-party or homegrown management), or standardizing on a single firewall vendor and using that choice to manage its own brand of firewalls.

The New York-based foreign exchange broker Forex Capital Markets (FXCM), with more than $1 billion in assets and hundreds of subnets to support, launched in 2010 and was able to start with a new standardized firewall infrastructure for better management.

"A next-generation firewall can determine a Facebook login and compliance with policy, and even block specific traffic within that application, like Farmville or streaming video."

– Dimitriy Ayrapetov, product line manager network security at SonicWALL

As a new company, it had the luxury of standardizing on the Check Point Software Blade Architecture to protect its global subnets. With this level of standardization, management can be done remotely, with security data feeding 20 regionalized Check Point clusters for firewall infrastructure management.

"The blades provide the level of firewall functionality we need to monitor our small subnet offices without having to multiply solutions in a location where we don't have a full IT staff," says Ryan Leonard, director of production engineering for FXCM. "More important, they can be easily managed remotely. For us, the level of security, ease of administration and audit are the biggest advantages of standardizing."

For privacy reasons, Leonard wouldn't say what blades they employed for the remote offices, but Check Point offers ones for firewall, VPN, mobile access, IPS, application control and identity awareness, data protection, web security and URL filtering, anti-malware and voice over IP (VoIP).

For large organizations with more diverse firewalls to manage, external firewall managers may be required, says Michael Hamelin, chief security architect for Tufin, a global firewall management vendor with U.S. headquarters in Burlington, Mass.

For example, U.K.-based Virgin Media uses Tufin to manage a variety of firewalls in its 20,000-employee organization. It wanted a best-of-breed implementation. "We have a hundred firewalls that manage corporate enterprise connectivity around the world," says Colin Miles,

management operations."

Along with centralized administration, Tufin provides Virgin with the ability to see changes over time, which enables the firewall team to optimize the rule base for best use of assets and overall application performance, he says.

Cloud providers offering security management also need to be able to support a wide variety of firewall brands, versions and types. In this case, third-party managers make the most sense, says Peter Bybee, president and CEO of Security On-Demand, a hybrid (on-premise and cloud-based) security provider based in San Diego.

"There is a lot of complexity in managing firewalls today because firewalls do more things," he says. "This is especially true when managing firewalls in the cloud."

To support its large breadth of firewall brands, Security On-Demand uses AlgoSec firewall management, which provides firewall change visibility into the cloud that his customers – and his team – require, he says.

"Say we have a client with admin privileges making changes to their firewall that we're also responsible for," he says. "AlgoSec gives us that visibility and workflow to make sure any change controls are being followed, and it gives our clients the visibility they need to manage their firewalls themselves."

Architecture

As important as manageability is the security of the underlying operating system on which these firewalls reside, says William Mabon, director of cyber security products at London-based BAE Systems, a global defense, security and aerospace company.

"Every firewall, whether virtual or physical, sits on an operating system," he says. "In highly secure government and financial environments, these operating systems should be stripped down, locked down and have passed third-party security evaluations."

Other considerations when upgrading firewalls, managers and optimizers include whether these firewalls will be able to manage IPv6 traffic, the next-generation internet protocol (IP)

And, as they improve on their application protections, these advanced security gateways also must provide more granular controls within the applications being accessed and manipulated by users.

“A next-generation firewall can determine a Facebook login and compliance with policy, and even block specific traffic within that application, like Farmville or streaming video,” says Dimitriy Ayrapetov, product line manager network security at SonicWALL (which was purchased by Dell in May). “What they can't do is distinguish what specific video stream within that approved application – such as a training video – is allowed without creating new, more granular rules.”

Size matters: Here comes the UTM

Forrester Research and Gartner identify two layers of advanced firewalls used by organizations today:

The unified threat management (UTM) gateway device. Gartner Analyst Lawrence Pingree describes UTMs as firewalls with bolted-in or add-on functionality, such as IDS/IPS, VPN/encryption, web and email security, and application controls. These are often used in small and midsized businesses without all services turned on, say analysts.

The next-generation firewall. Larger enterprises, which have more gateway devices to manage and bandwidth to support advanced features, are turning to what is called “next-generation” enterprise firewalls, says John Kindervag, a research analyst at Forrester. Next-generation firewalls are also multifunctional, more integrated and, vendors say, more accurate at performing intrusion prevention.

Both Pingree and Kindervag agree that the line between UTM and next-generation firewalls is blurring. “Some vendors are calling themselves next-generation firewalls, but are really UTM vendors,” says Pingree. “It really depends on the breadth and depth of coverage and the management features.”

SC Staff

RELATED EVENTS

CYBERCAST
Top 7 Ways to Evaluate a SASE Service
THU JUL 15

CYBERCAST
Delivering the "R" in NDR – How Guided-SaaS NDR Enables Rapid Response
THU JUL 22

CYBERCAST
Your Attack Surface Is Far More Than Just the Tip of the Iceberg
WED JUL 14

EXPLORE

Product reviews | Research | White papers | Webcasts | Podcasts

Copyright © 2021 CyberRisk Alliance, LLC All Rights Reserved This material may not be published, broadcast, rewritten or redistributed in any form without prior authorization.

Your use of this website constitutes acceptance of CyberRisk Alliance Privacy Policy and Terms & Conditions.