A New Firewall for the Data Center

Jeff Wilson
Principal Analyst, Security
Infonetics Research

TRADITIONAL FIREWALLS STRUGGLE TO HANDLE TODAY'S DATA CENTER REQUIREMENTS

Data centers have changed significantly since the dot.com boom and bust introduced the concept into the collective consciousness. A decade ago, when the modern network firewall was just reaching maturity, data centers hosted a wide variety of client/server apps, had <100Mbps connections to the Internet, and may have hosted a web site or early web application. Today's data centers all connect to the Internet, many at 40G, 100G, and beyond, and nearly exclusively host web sites or web applications. Instead of several thousand clients each connecting to 1 of 100 different databases, mail servers, ERP, and CRM servers, we now have hundreds of thousands to millions of users attempting to reach the same web site or application.

The near-complete webification of the data center is causing a shift in security requirements. Networking and security professionals looking to properly secure data center infrastructure today are primarily concerned with:

- The rapidly increasing scale of attacks
- Connection performance requirements, including the ability to rapidly ramp up connections
- A small set of protocols mostly focused around the web and web applications

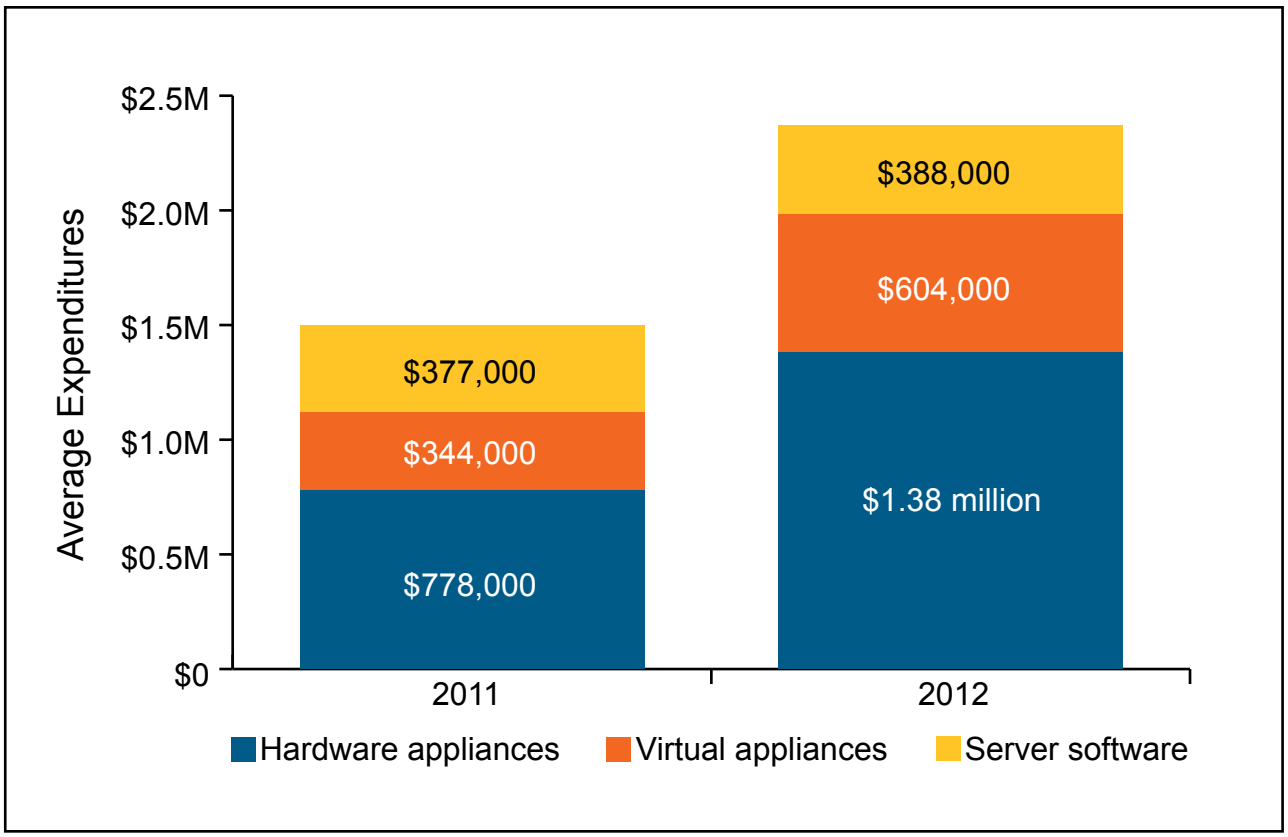
There are 100G DDoS attacks on record, and multiple reports of sustained DDoS attacks at 20G, 30G, and 50G, and it's very possible that a firewall in a large data center environment would need to handle 10s of millions of concurrent connections. While the scale of the problem has increased, the number of protocols that need to be protected in the data center has decreased; the gradual elimination of proprietary enterprise client-server apps has shifted the focus to HTTP/HTTPS, SSL/TLS, FTP, and DNS (while TCP remains important for both client server and web applications).

Traditional firewalls are designed to provide security across a wide range of protocols, but aren't designed specifically to handle the massive volume, variety, and size of threats aimed at this narrow range of protocols. Though all reputable firewalls can adequately secure the enterprise perimeter, they don't necessarily scale up to meet large data center performance requirements, and if they do it may be at a price that's hard to swallow for data center buyers.

INFONETICS RESEARCH

These changes in security requirements are forcing companies to evaluate and purchase new solutions, and spending on security for data centers is skyrocketing. In our March 2012 *Data Center Security Strategies and Vendor Leadership: North American Enterprise Survey*, we talked to security buyers at 101 medium and large companies operating their own data centers, and as shown in the chart below, they're planning to increase their spending for security in the data center 58% between 2011 and 2012, with much of this increase coming from additional spending on new hardware appliances. Key drivers impacting this spending include the need to upgrade the performance of the security infrastructure to match the network infrastructure, to handle the volume of threats, and to deal specifically with new DDoS attacks.

Enterprise Spending on Data Center Security Is Skyrocketing



Source: Infonetics Research, *Data Center Security Strategies and Vendor Leadership: North American Enterprise Survey*, March 2012

If there is a new market for firewalls specifically designed for data centers, with data-center scale and a focus on the protocols and threats affecting the data center, we're in the very early stages of that market. To further understand the impact of data center changes and the evolving threat landscape, we recently had detailed conversations with buyers on the leading edge of data center security: three different types of companies that operate large data centers, all of whom have an immediate need for a new type of security solution for their data centers. We talked about the notion of a consolidated data center security platform that met the three key requirements listed above at a lower cost than deploying traditional firewalls. These discussions, summarized below, provided fascinating insight on data center security requirements and led to some clear conclusions.

© INFONETICS RESEARCH, INC. JUNE 2012

"Based on our conversations with leading-edge buyers, there clearly is a need for new data center infrastructure security solutions."

JEFF WILSON, PRINCIPAL ANALYST FOR SECURITY, INFONETICS RESEARCH

MULTI-FUNCTION DATA CENTER FOR DISTRIBUTED ENTERPRISE

The first company we spoke with is a large distributed enterprise that operates a data center providing on-line services to customers and a large network of agents and partners. They're looking for a firewall solution to provide security specifically for their customer/agent facing web applications, and as such are primarily concerned with security HTTP/HTTPS and FTP, with a need to secure themselves from XSS and CSRF attacks, IP spoofing, DDoS, and reconnaissance attacks. They continue to use traditional enterprise firewalls to protect the borders at their main, branch, and remote offices, but in the data center the focus is 100% on securing their web apps.

All agents in their network were moved to web services several years ago, and the rapid increase in use of their customer-facing web application as well as the increase in the number of services offered to customers has caused a sharp uptick in the traffic volume in and out of the data center. They need a new solution to handle the increased volume of traffic, but are budget constrained and having trouble finding a traditional firewall solution that meets performance, security, and budget requirements.

This buyer's new solution needs boil down to three things: a single platform for a broad range of data-center attacks (from DDoS to application layer attacks), high performance with the ability to scale up in the near future (they're anticipating another sharp uptick in traffic when they roll out mobile and tablet apps), and total cost below the traditional firewall vendors.

SINGLE-SITE WEB HOSTING ENVIRONMENT

The next company we talked with sells software online and maintains data centers for their commerce site. The actual delivery of their software solution happens over a separate CDN infrastructure that they don't maintain, so they are looking for a new security solution just for the customer-facing web site through which they sell their product. They operate multiple data centers and initially they're looking for a 30Gbps-capable DDoS solution. Though that seems simple enough, and there are many dedicated DDoS solutions available, they are not interested in a hosted solution, and can't find a dedicated solution that meets their spending requirements.

They still have traditional network firewalls in front of their PCI infrastructure and at their main sites, and will continue to use them, but need something that will scale in the data center, especially since they're looking to go public soon and are expecting massive increases in attacks once that happens. They're also looking to consolidate infrastructure wherever possible, so they're interested in a DDoS solution that can take over some of the heavy lifting from other security and/or traffic management products in the data center over time. They tested a variety of products from traditional firewall vendors, but meeting their current and future performance requirements was hard for most of the traditional solutions, and the solutions that did perform adequately were prohibitively expensive.

For this buyer, the need today is simple: high performance DDoS at a cost they can swallow; however, their attention was also caught by the idea of a consolidated security platform for the data center that could also handle traffic management tasks and had deep coverage against threats for the protocols they care about (TCP, HTTP/HTTPS).

© INFONETICS RESEARCH, INC. JUNE 2012

INTERNET DATA CENTER HOSTING SAAS APPLICATION

Our final conversation was with a large SaaS vendor. Their exact situation and requirements are different from the first two companies we talked with, in that they literally only care about HTTP/HTTPs (and SSL offload); anything besides HTTP/HTTPs is simply dropped. They have massive data centers around the globe that have to scale from 100K+ concurrent connections to 10s of millions. They use a hosted service for DDoS prevention, but they need deep protection from application layer attacks within HTTP/HTTPS, and they need a platform that can also handle SSL offload and visibility.

Like the other two companies we talked with, they continue to use traditional firewalls in their HQ/branch/remote offices, but unlike the other two, they can envision a future where they won't need those firewalls; they believe in the not-too-distant future every internal and external application their company uses will be web-based. Like the other companies we talked with, they tested firewalls from traditional vendors in their environments, and they found products that met some of their performance requirements, but just barely; the products lacked the depth of security they required for HTTP/HTTPS, or didn't offer SSL offload.

Though they have a laser focus on HTTP/HTTPS, they have some interest moving forward in integrating DDoS prevention for smaller data centers to save on their hosted DDoS prevention service, and they're interested in integrating security services in the data center with traffic management. Cost of the solution isn't a primary driver for this customer; they're willing to spend as needed to solve their scale problem, but the notion of a high performance solution focused on a critical set of protocols and threats at a lower price than a very-high-end traditional network firewall is compelling to them.

BOTTOM LINE: SCALE AND COST DRIVE THE SEARCH FOR A NEW FIREWALL IN THE DATA CENTER

Based on our conversations with these leading-edge buyers, there clearly is a need for new data center infrastructure security solutions. Cost and performance/scale are the intersecting drivers for the three companies we talked with. For the first, traditional solutions meet their scale requirements, but are too costly. The second customer has cost and scale requirements that cannot be met by traditional firewalls, and the third customer isn't cost sensitive, but has not found a product that meets their exact needs at any price. There are other common drivers as well, namely depth of security for the protocols they care about, and the desire to collapse functions and increase the efficiency of their data center operations, particularly security and traffic management.

These three companies are on the leading edge, but as evidenced by the 2012 spending plans detailed earlier and the massive increase in highly publicized threat events aimed at data centers, they won't be the only ones looking at new solutions. Many will evaluate new platforms to solve a narrow range of problems; in these three discussions alone we have a buyer who simply needs a great data center DDoS solution today, and another that drops all traffic that isn't HTTP/HTTPS. Looking to the future, all of them express an interest in expanding the use of a data center firewall beyond their initial need. Given their experience evaluating products from traditional firewall vendors, they're all willing to look at new companies for data center firewalls as long as they have solid data center infrastructure credentials.

There's no sign that the volume of attacks aimed at data centers will ever decrease, nor are there signs that use of the web or web-delivered applications will decrease, so we can only expect the drivers that came up repeatedly in our discussions will push buyers to urgently pursue new solutions and roll them out quickly. ■

© INFONETICS RESEARCH, INC. JUNE 2012