Lippis Report 158

Next Generation Network Security for Data Center Protections

by

Nicholas John Lippis III
President, Lippis Consulting

October 2010

Lippis Report 158: Next Generation Network Security for Data Center Protections

One significant trend that has emerged during the current business/economic cycle is that IT projects that reduce cost are winners. This savings trend is as strong as I have experienced in my twenty-five years within the IT industry. In particular, it's propelling data center consolidation, server virtualization and mobile computing projects. As enterprises consolidate data centers and miniaturize them with virtualization, cloud-computing providers are busy offering a new lower cost IT delivery economic model. In short, a new tier of computing has emerged were endpoint devices are mobile and applications are delivered via corporate data centers and cloud computing facilities. This new model of computing that also increases convenience and productivity is lacking in one important area; network security for both mobile endpoints and the ability of data center security appliances to keep up with application demand.

And keeping up with application demand is one of the most challenging tasks IT business leaders are encountering. Not only has information demand skyrocketed during this business cycle but content in the form of web pages has become dynamic, where a single page request opens a multitude of connections pulling content from various sources to satisfy user expectations of real time information access. For example, a single web page request can easily spawn more than fifty network connections over physical and virtual infrastructure placing extraordinary demands on network speed, latency, reliability and security. For the uninitiated, just point your browser to any of these sites—disney.com, cnn.com, nytimes.com, et al—and notice rich content in action. As the page is presented, it serves up video, photos, audio, rich text and more, all of which are pulled from various sources within a data center fabric over virtual and physical infrastructure. The calculus IT leaders are seeking to solve includes massive growth in information demand plus Brownian motion traffic flows, thanks to dynamic content plus densely packed data centers, thanks to virtualization. Even with consolidation and virtualization information/application, demand is forcing the overall data center market size to expand from 108 million sq. ft. in 2009 to a projected 117 million sq. ft. by year end 2010, according to Frost & Sullivan. Part of the solution to IT leaders' calculus problem is found in a data center network fabric that supports millions of connections/session of east-west and north-south traffic flows securely.

To put the mobility trend into perspective, Apple sold over 3.3 million iPads in its first 3 months; the highest uptake of any endpoint device. Google activates 100,000 Android-based phones per day. Cisco recently announced its CIUS android-based table for business use with tight links to its unified communications (UC) and videoconference systems. Every major UC provider will be offering similar devices while traditional computer vendors serve up android-based tablets over the next few quarters. The iPad and Android tablet is a new tier of computing, which are driving users to access applications over mobile and wireless networks in addition to their wired and VPN networks.

And therein lays the rub. In today's modern IT world, applications are being extended over multiple networks, e.g., wired, wireless, mobile and remote, where users shift their application access back and forth between these different network access methods and expect the same or consistent experience. Security is paramount to user experience and IT asset protection. While IT security executives have fortified their defenses of IT assets within corporate boundaries or perimeters, exponentially growing numbers of mobile endpoints being connected into corporate networks and data centers present significant security challenges that are unfortunately outside the control of IT.

The nature of mobile smart phone endpoints is to combine personal and business IT services, thereby creating a unique user experience. Part of that experience includes information access from a plethora of online destinations, such as public WIFI hotspots, SaaS applications, e.g., Salesforce.com, workday.com, netsuite.com, etc, corporate VPN, and a wide range of personal sites for social networking, banking, music, videos, news, communications, etc. Therefore, for every employee equipped with a mobile endpoint, security vulnerabilities and threats are opened unless IT mitigates with network security. Clearly mobile devices are becoming ubiquitous, and there are security solutions available, such as VPN support, data wipe after loss, cloud-based security services, etc. But mobile devices need a security solution that works in real time, meaning it's always-on protection and provides comprehensive coverage.

For example, mobile endpoints, and thus corporate assets, need to be protected from users accessing the corporate network from insecure home WIFI networks and hackers. Internal applications need to be secured against attacks such as SQL injection/data leakage, request forgery/impersonation, cross site scripting/phishing, etc. SaaS access needs to be secure against unauthorized access, exposure from password reuse, layer 7 attacks and more. Also the same level of reporting for mobile users as wired users needs to be supported to assure activity/audit trail, regulatory compliance plus governance and reporting. In short, IT needs the same level of control over mobile endpoints as it does over devices within the corporate perimeter without ruining the mobile experience.

Mobile Endpoint Policy and Enforcement

The most important aspect of real-time mobile security is policy enforcement as it places control of corporate asset and SaaS access back into the hands of IT. Not only does policy and enforcement mitigate threats from being transmitted from mobile endpoints onto corporate networks, it makes them safer devices, too, by providing a means to adhere to corporate policy as corporate devices, even though they are used for business and pleasure. This is important as many mobile devices are purchased by employees, part of the huge consumerization trend that has been building over the last five years. With IT able to administer policy with a means of enforcement, mobile devices can deliver personal and business IT services. Employees may purchase mobile devices but if they require access to corporate IT, then the endpoint has to comply with corporate policy and IT needs a means to enforce such policy. In short, policy and enforcement enables IT to extend the corporate perimeter around mobile devices to creating a virtual perimeter around IT assets.

Consider the following example of policy and enforcement creating a virtual perimeter… A user may be accessing an SaaS application while at his/her desktop. This flow traverses the corporate firewall with associated policy and enforcement. When this user is outside the corporate perimeter, he/she could access the SaaS application directly without corporate policy or enforcement opening vulnerabilities. However, with mobile policy and enforcement, this same user could access the SaaS application with the same policy, enforcement and protections as available when within the corporate perimeter mitigating any vulnerability. Solutions to this usually require the mobile device to first pass through the corporate firewall or a security cloud service where IT controls policy before the user connects to the SaaS application.

New Security Performance Demands

With mobile endpoints under corporate IT policy and enforcement, this huge security vulnerability can now be managed and mitigated. At the same time that mobile devices are becoming ubiquitous, data center security appliances are failing to keep up with the huge demand for information and application access. As more compute power is concentrated into smaller spaces, traffic volume increases exponentially, and security appliances need to adjust accordingly.
Consider how web sites serve up a rich media web page. Every time a user requests a webpage, its server typically needs to request 50 to 100 different objects just to display the one webpage requested. Now consider a data center with thousands of servers and five-thousand connections per second of requests each spawning 50 to 100 server requests. The backend east-to-west traffic flows between servers are one to two orders of magnitude larger than the north-to-south user request flows with the combination of both flows being immense.

New Firewall/IPS Performance Metrics Needed

From a security point of view, not only is firewall throughput an important performance metric, but "connections per second" is becoming more important. A high number of "connections per second" supported assures IT that backend server flows are being screened without delaying user experience. In addition to the number of connections per second, another performance measurement is "maximum connections" supported per second to assure that the number of server-to-server flows to deliver a webpage can be securely delivered. The combination of throughout, connections per second and maximum number of connections can be defined as "true scale performance." Typically a firewall can deliver hundreds of thousands of connections per second, but this is too slow for most demanding data centers by at least a factor of 2 to 3. Typical maximum number of simultaneous connections supported per firewall is around a few million, which is too low by at least a factor of 4 to 6. Also consider a more realistic throughput measurement other than a range of UDP packet sizes, which is common in the industry. Real world throughput performance numbers that represent a mixture of traffic profiles is a better measurement to assure throughout quoted is throughput experienced.
In addition to raw security performance, data center rack space too needs to be carefully managed as IT executives quickly start running out of rack space as they consolidate. Security appliances need to reduce their footprint as many appliances occupy 16 to 24 RU or a half rack of space and more

consuming footprint, energy and cooling resources. Expect security appliances to start delivering on the above performance metrics at up to an 8th of their size or 2 RU high if not smaller.

Threat Protection

To assure this security infrastructure protects IT assets at the rate in which cybercriminals and hackers wish to penetrate it, the industry is serving up cloud-based threat protection. A few suppliers have launched cloud-based security services, which collect anomalistic data throughout the internet and corporate networks via sensors, analyze/correlate the anomalies with reputation scores and when a new exploit's signature is detected, the cloud transmits mitigation code/signature updates to corporate IPSs. The speed in which this process takes place is a competitive differentiation. Those that send updates every five or so minutes have the best chance of mitigating exploits from cybercriminals which tend to change IP address every hour to avoid detection. IT business leaders will know when cloud-based threat protection becomes highly reliable. It's at that point that suppliers will start offering "guaranteed protection" that incorporate penalties to suppliers if protection is penetrated. Policy and enforcement of mobile devices creates a virtual perimeter while true scale performance enables security appliances to keep up with application demand and new traffic flow realities. Smaller security appliance footprint allows IT executives to maximize data center space while minimizing energy and cooling. Cloud-based threat protection keeps the security infrastructure updated in near real time with signatures to mitigate threats throughout the corporate and virtual perimeter. In short, IT business leaders gain control and manage mobile security vulnerabilities while delivering applications to users securely at speed with small footprint consumption. Mobile, data center consolidation and virtualization plus cloud computing are powerful trends rooted in economic efficiency and increased information demand. To maximize the value of these investments, a new security model is needed.