How to Achieve Network Nirvana

Application optimization not only improves network performance for users, it can also enhance security.

Talk about great expectations.
When an organization’s mobile workers connect with the corporate network from anywhere in the field, they expect the same performance as when they’re inside corporate headquarters and tapping directly into a LAN. Never mind that wide area networks come with bandwidth constraints that can result in a host of performance and security challenges.

The answer would be simple if the solution to WAN performance problems was simply one of adding capacity. “Just throwing bandwidth at the problem is not going to solve bottlenecks and other issues,” says Tina Herrera, director of campus marketing for Juniper Networks.

For example, applications for unified communications and collaboration have strict requirements about latency, jitter and traffic prioritization. “So when you’re considering how to support a UCC solution, it’s important to understand if the network you have can handle these stringent requirements,” Herrera says. “If it can’t, IT managers must determine what steps are needed to address any gaps.”

Fortunately, there’s help. Performance enhancements through sophisticated WAN and application optimization technologies, combined with a thorough network assessment, provide a manageable approach to meeting today’s performance requirements. “Optimization tools help enterprises tune applications to create more flexible and programmable networks,” says Lee Doyle, principal analyst at Doyle Research.

Just as important, the best WAN and application optimization technologies also offer essential tools to help IT administrators tackle security more holistically and effectively. For example, network administrators design most WANs with a firewall device at the border. Now, some leading networking manufacturers are adding security features to these edge devices. The capabilities may include URL and content filtering, application identification, and control features associated with next-generation firewalls.

Inside Optimization
Application optimization technology improves the performance of applications that won’t typically benefit from the core tools used in WAN optimization – data compression and deduplication, which speed the transfer of large files.

Instead, application optimization works by condensing communications instructions associated with protocols such as HTTP and Transport Control Protocol. These headers slow transmissions when they send extraneous data over network pipelines.

Application optimization solutions also use data compression and caching algorithms to further streamline transmissions.

While WAN optimization requires a physical or virtual solution at each end of the communication channel, application acceleration can happen asymmetrically, which makes it easier to use for mobile workers and authorized users who don’t log into networks from corporate headquarters or remote offices.

MageMojo
One company that’s benefitting from application optimization for both performance and security is MageMojo, a Pittsburgh e-commerce hosting provider. In 2012, a series of distributed denial-of-service (DDoS) attacks flooded MageMojo’s network, crippling the company’s ability to effectively service its customer base of online-store owners, who rely on that network to complete customer-generated transactions. (See CDW.com/MageMojo.)

The attacks didn’t just degrade performance; they took the network completely offline for a couple of hours, which meant a loss of business and customers. To restore customers’ faith, MageMojo executives wanted a dedicated solution that would mitigate future DDoS attacks.

The solution consisted of the MageMojo staff choosing a combined solution from F5 that offers scalability, performance, redundancy and attack protection, says Eric Hileman, MageMojo’s cofounder. The solution consists of five key pieces:

1. F5 VIPRION:
   This platform let MageMojo IT managers start small with a single blade, then scale quickly and seamlessly by inserting more blades into the chassis. When the company reaches the maximum vertical scaling by filling a chassis with blades, IT administrators can add more chassis and begin scaling horizontally. The VIPRION hardware also offers additional DDoS protection through...
and redundancy,” Hileman says. Appliances, with better performance than their counterparts, allow organizations to better manage the features of dedicated DDoS protection appliances, with better performance than their counterparts, allowing organizations to better manage the features of dedicated DDoS protection

who can analyze existing infrastructures from third-party networking experts how traffic patterns may be changing,

important best practices to keep their managers should also follow some they’re not the entire answer. Network performance and security goals, but helping organizations achieve their for WAN optimization are essential for

assess for Success Together, the five components offer “all the features of dedicated DDoS protection appliances, with better performance and redundancy,” Hileman says.

TOP 5 WAYS WAN OPTIMIZATION BOOSTS SECURITY

1. Acceleration of encrypted protocols, such as HTTPS
2. Strong encryption to protect data during transmission and at rest
3. Decryption of hosted virtual desktop traffic for quality of service (QoS) in interactive communications
4. Cross-session compression, deduplication and caching
5. QoS for encrypted streams, with guaranteed in-order delivery of packets

synchronized (SYN) cookies, a Transmission Control Protocol sequence that offsets a SYN flood and application acceleration using Secure Sockets Layer offloading.

2. F5 BIG-IP Suite's base software: The software can cull and remove data injected by an attacker to ensure that even the heaviest DDoS attack will not overwhelm the network.

3. BIG-IP Local Traffic Manager: The LTM module provides load balancing and Network Address Translation features, which route packets from network to network. It also includes F5’s iRules scripting up to Layer 7, which mitigates many common attacks.

4. BIG-IP Advanced Firewall Manager: The AFM module, certified by ICSA Labs, helps MageMojo meet its PCI DSS requirement to protect payment card data.

5. BIG-IP Application Security Manager: The ASM module helps the company mitigate Layer 7 application-level attacks. MageMojo also relies on F5’s IP Intelligence subscription-based service to block connections from known botnets and other malicious IP addresses.

and identify the root cause of WAN bottlenecks created by cloud computing, virtualization, remote networking and other bandwidth-heavy applications. In addition, IT leaders should arm their network administrators with tools to keep WANs running at top speed. “The network has to be more intelligent than ever in transporting applications and services that are being delivered across the network,” says Doug Roberts, managing director for enterprise products at Fluke Networks.

As a result, he’s seeing a rise in solutions for what he calls application-aware network performance management. Basically, AANPM tools provide a way to measure performance using a wide variety of data, including packet traffic, net-flow information and Windows Management Instrumentation results. By combining multiple data sources, Fluke’s AANPM solution helps network managers gauge performance from application, end-user and IT infrastructure perspectives, Roberts says.

“This comprehensive view breaks down the difference between application response time, data transfer time and network round-trip time, which are the three core components of our end-user response time measurement,” Roberts says. “This enables organizations to isolate problems down to the individual component or service responsible for the degradation and identifies how administrators can achieve the greatest efficiency gains on behalf of end users.”

A number of other network chiefs are also increasing their focus on enhanced data gathering and analytics. “Part of network performance monitoring is understanding application performance,” says Matt Ellis, vice president of service availability and performance management for IBM. “You can’t optimize what you can’t control, and you can’t control areas where you lack visibility.”

Acting on the Metrics But network administrators need more than just the ability to gather performance data about applications accessed by mobile workers or other users. They also require sophisticated analytics to put the information into context and make it actionable. “You may be gathering thousands of metrics, but understanding the inter-relationships can be a challenge,” Ellis says.

To address data complexities, IBM recently introduced IBM SmartCloud Analytics – Predictive Insights, which draws on research associated with IBM Watson to learn the behavior of individual networks, correlate a wide variety of metrics, and uncover anomalous behavior that causes slow application performance and creates unacceptable user experiences.

Other data gathering and analysis solutions include Juniper Junos Space Network Management platform, an automated solution that provides a central management console for visualizing, analyzing and controlling the entire network – both wired and wireless segments.