> "It lowers our administration and maintenance of our servers, and saves a considerable amount of time and money."
>
> Randy Paxton, Lead Network Engineer

Blue Cross Blue Shield: High Availability, Best Practices Security, and HIPAA Compliance Using F5 BIG-IP Solutions

Blue Cross Blue Shield of Kansas City (BCBSKC) is the area's largest health benefits provider, serving more than 880,000 members in 32 counties in greater Kansas City, northwest Missouri, and Kansas.

As a prominent local healthcare provider with a strong reputation for quality, BCBSKC recognized the need to ensure high availability and strong security for their website, which typically receives more than 30,000 hits a day.

By using F5® BIG-IP® Local Traffic Manager,™ (LTM) F5 BIG-IP® Application Security Manager™ (ASM—formerly TrafficShield®), and F5 BIG-IP Link Controller,™ BCBSKC dramatically improved page load times, supercharged their application performance, improved their scalability to meet future growth challenges, and effectively locked down their data to meet the rigorous compliance goals mandated by the Health Insurance Portability and Accountability Act (HIPAA).

Business Challenges

BCBSKC had several goals for their heavily trafficked site, which provides key healthcare plan information for providers, brokers, and employers; general health and wellness information; directories; and healthcare coverage information.

First, they needed to improve the performance of the site, based on the simple fact that if a site is slow or difficult to use, phone calls (and blame) are directed to the IT help desk while the site remains unused.

Another goal was to protect personal healthcare information from prying eyes. Obviously important for any business on the web is to maintain data security; for healthcare organizations, HIPAA requires added precautions to ensure the security of their networks and the privacy of patient data.

Overview

Industry

Healthcare/Insurance

Challenges

- Enhance application performance
- Secure applications
- Improve scalability

Solution

- F5 BIG-IP Local Traffic Manager, F5 BIG-IP Application Security Manager, and F5 BIG-IP Link Controller

Benefits

- Lowered server maintenance and administration
- Reduced page load times from 30 seconds to less than a second
- Improved scalability and lower costs
- Met HIPAA security requirements

A third goal for BCBSKC, particularly for the engineers behind the site, was that their investments were protected, and could scale to meet increasing traffic numbers, new applications, and ever-evolving security challenges. Replacing equipment every few years because it was outdated or obsolete—along with the associated expenditures and costs—was simply not an option.

Solution

"F5's BIG-IP Link Controllers were the first products we purchased, mainly to achieve ISP redundancy," said Randy Paxton, Lead Network Engineer for BCBSKC.

This was a smart move because maintaining only one link to the public network represents a single point of failure and a serious network vulnerability. BIG-IP Link Controller monitors the health and availability of each connection, detecting outages to a link or an ISP. In the event of a failure (one ISP goes down, for example), traffic is transparently directed across other available links so BCBSKC users stay connected.

Next, BCBSKC brought in F5 BIG-IP LTM "to balance our DMZ web servers and some application servers internally," stated Paxton, "as well as perform SSL offload."

"Before, SSL traffic was being terminated on the server itself," said Chad O'Neal, Web Technical Engineer. "That led to performance problems, especially as our traffic numbers began to increase."

By offloading the computational-intensive process of SSL termination from their servers to the BIG-IP LTM device, BCBSKC noted a marked performance gain for their SSL-based traffic while lowering server maintenance costs and improving scalability.

"It lowers our administration and maintenance of our servers, and saves a considerable amount of time and money," said Paxton.

There were other benefits of using BIG-IP LTM as well, most notably ensuring that BCBSKC applications were consistently available. This is not as simple as it seems because in order for a device to consistently deliver high availability, it has to first understand the content of applications and make decisions based on complex rules associated with a specific application.

This added intelligence differentiates BIG-IP LTM from other Application Delivery Networking solutions that can recognize the nature of a message but can't understand it—just as an English speaker might recognize a conversation in Spanish or French without understanding the words.

By the same analogy, BIG-IP LTM can understand what is being said, translate between the parties if necessary, and alter the content as needed to provide increased security and deliver functions that would otherwise require a change in the application itself.

Security without compromise was perhaps the primary objective of BCBSKC. Healthcare data in the wrong hands could spell disaster, which is why F5 BIG-IP ASM is an important part of BCBSKC's overall security initiatives.

"It's very important that we maintain a good reputation about this website," said O'Neal. "And the biggest reason we went with [BIG-IP] ASM was to protect our constituents' personal health information. We'd much rather know that somebody is attempting to hack into our site, be notified, and correct the problem—versus somebody's personal health information showing up in the Kansas City Star."

BIG-IP ASM ensures the security of web-based applications which access or could be used to access patient records or other protected health information. This security extends beyond encryption (which ensures privacy from outsiders) and authentication/authorization (which provides user access to a given application).

With the amount of attention surrounding vulnerabilities of web applications today—and the fact that 80% of enterprise hacking attempts happen through the web (source: Gartner)—BIG-IP ASM has become a necessary component in overcoming BCBSKC's everyday and ever-changing security challenges.

Previously, BCBSKC used another type of application firewall that resulted in web pages that often took up to 30 seconds to download. With BIG-IP ASM, they cut that page load time to less than one second—without losing any of the many application security benefits they required.

Finally, the devices needed to support myriad applications today while seamlessly supporting new application deployments tomorrow; application firewalls need to effectively deal with both known and as-of-yet unknown threats without adversely affecting site performance; and hardware/software needs to seamlessly scale while avoiding costly obsolescence expenses.

"We're upgrading to bigger F5 hardware platforms with [BIG-IP ASM], and will continue to use our existing gear in additional capacities or transition them to test boxes," said O'Neal. "We don't have to throw anything away, and we can consolidate our existing systems into the new ones."

And that, according to both Paxton and O'Neal, will "save a lot of money in the long run toward administration duties and future hardware purchases."

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com