

“F5 products do everything they promise. They work exactly the way we could have hoped for. If I had to do it all over again, there is no doubt in my mind I would make exactly the same decision.”

Steve Morenzeni
Network Engineer

Lake Forest Hospital Delivers Life Saving Care with F5's BIG-IP Link Controller and FirePass SSL VPN



Industry:

Healthcare

Challenges:

- Functional, flexible, secure network access from any location
- Externalize internal applications
- Complete link redundancy and ISP failover

Solution:

F5's FirePass® Controller
F5's BIG-IP® Link Controller

Benefits:

FirePass

- Comprehensive security for remote application access
- Increased medical care and business efficiency
- Ease of management and functionality
- Support remote employees
- Lower overhead

Benefits (con't):

BIG-IP® Link Controller

- Business/Medical applications always available
- Maintain cash stream from patient accounting applications
- Loss avoidance of one million dollars in revenue

Network Environment:

Applications

- OBLink
- Dictaphone
- Scheduling.com
- Nebo
- Citrix

Architecture

- Cisco Backbone (6513s in core)
- Cisco 3500/4500 switches at edge
- OC-12 Sonnet Ring connecting 6 remote sites
- Single Enterprise Network
- 4 T-1s, 3 connections (two T-1s bonded)

Lake Forest
Hospital

Advanced Caring
Close at HandSM

Overview

Lake Forest Hospital Foundation is among the nation's premier medical care providers. Located on the north shore of Chicago, Lake Forest Hospital offers state-of-the-art people-centered healthcare. To operate efficiently and deliver premium medical treatment, the hospital needed a technological solution that kept their application infrastructure accessible yet secure. Taking advantage of a versatile product suite, Lake Forest Hospital chose F5's BIG-IP Link Controller and FirePass SSL VPN to keep their network applications safe, reliable, and fast.

Challenge

Network Engineers at Lake Forest Hospital have developed a single enterprise network. Key administrative and medical support applications such as Dictaphone and Nebo, as well as every appliance including time clocks, security cameras, x-rays, mammography equipment, and OBLink, a fetal monitoring system, plug into the network system. The hospital also relies heavily on third-party Application Service Providers (ASP) like Scheduling.com for scheduling, and Picture Archive

Communications System (PACS) for archiving.

As innovators, Lake Forest Hospital employees quickly understood the benefits of remote access to their medical and administrative applications. Unfortunately, their previous remote access solution was a hassle because users had an increasingly difficult time tunneling into the network. Therefore, it was important that employees and doctors had functional, reliable access to vital applications from their homes, offices, or while away on business. More importantly, remote access needed to be secure since passing private medical information from remote employee computers to hospital servers could not be compromised. Compliance with government-mandated personal information security policies such as the Healthcare Insurance Portability and Accountability Act (HIPAA) was absolutely crucial.



Lake Forest Hospital also realized Internet connectivity was the key to their continued success. Any Internet Service Provider failure would result in serious business consequences as hundreds of employees would be unable to do their job. Remote network access would cease, and essential business functions such as insurance verification, scheduling, accounting, and PACS would shut down. To address these problems, Lake Forest Hospital scheduled an appointment with F5.

Solution

To ensure remote, secure, and highly available access to their applications, Lake Forest Hospital relies on F5's FirePass. FirePass SSL VPN offers employees a simple, expedient, and secure way to access business applications from any remote location via a standard web browser. With FirePass, there is no need for client-side software installation, saving thousands of dollars in management costs, and enabling a hassle-free connection to the hospital network from any computer at any location.

Other SSL VPN alternatives were evaluated but failed to deliver the ease of management and functionality offered by FirePass. The hospital believes F5's FirePass presents an industry leading SSL VPN solution. **"F5 is where Lake Forest Hospital wants to be and where the industry needs to be"**, commented Morenzoni.

Lake Forest network engineers can easily integrate FirePass with their existing active directory, and create policies granting application access based on user identification and privilege for time-saving user authentication management. Steve Morenzoni, Network Engineer at Lake Forest Hospital, spoke to the functionality of FirePass,

"We are really pleased with the functionality it gives us and the ease of use in terms of supporting our end users. I love the flexibility of it because we're always running into people saying, 'I want to do this', and with FirePass, we rarely have had to tell them we can't."

Approximately half of the hospital's remote users rely on FirePass. The number of FirePass users will increase, as management expects the demand for secure remote access to skyrocket. This anticipated user growth has highlighted the need to make sure the hospital's Internet links are available 24x7.

As a result, Lake Forest Hospital chose F5's BIG-IP Link Controller to deliver continual Internet link connectivity and optimal bandwidth usage. The BIG-IP Link Controller intelligently monitors the availability and performance of multiple WAN connections, ensuring full link redundancy. BIG-IP Link Controller offers an extensive array of link management options. Administrators can predetermine the amount of traffic funneled through multiple links based on a variety of variables, including link connection cost, link performance, and amount of bandwidth available.

For Lake Forest Hospital, the BIG-IP Link Controller was the only viable solution. ***"We had talked a little bit about Border Gateway Protocol (BGP), it was actually our reseller who came to us and said we need [F5] Link Controllers. They informed us on how we could completely avoid the use of BGP,"*** recalled Steve Morenzoni.

The hospital currently relies upon four T-1 lines and three connections for Internet connectivity. Two T-1s are bonded while the other two are independent. The BIG-IP Link Controller successfully load

balances traffic across all these connections to deliver non-stop network availability.

Lake Forest Hospital has also taken advantage of the BIG-IP Link Controller's intelligent traffic routing capabilities. ***"Because the Link Controllers are so smart, they are able to determine that link one gets twice as many packets as links two and three,"*** Morenzoni said. ***"The intelligence built into them is wonderful."***

Benefits

Remote Access

With F5, Lake Forest Hospital has successfully alleviated the pain associated with remote access, difficult VPN installation, client-side management headaches, and WAN outages. Secure remote access from FirePass is a key component to delivering the high quality medical care patients expect. Lake Forest doctors are thrilled with FirePass. At 2am, for example, a doctor can access the company network from home via FirePass. Based on pictures and strips generated from PACS and OBLink, the doctor can easily consult with the nursing staff rather than making the trip back into the hospital to access information.

On a side note, the hospital was having difficulty recruiting transcriptionists. Thanks to FirePass, recruitment efforts have proved fruitful, as employees are now able to work from nearly anywhere, lowering overhead and better utilizing expensive office space. Likewise, building engineers can log into FirePass, bring up the system tool for the building management system, and adjust a variety of factors such as pool and room temperature from virtually anywhere.



Network Security

Network and application security are a must. The Hospital literally cannot afford to have patient medical information compromised. F5's FirePass allows the hospital to maintain its "best practice" security policy, guaranteeing privacy-sensitive applications are delivered in a secure, HIPAA compliant manner.

Extensibility

Considering the future, as bandwidth usage swells, so will the need for a scalable link management solution. Lake Forest Hospital plans on adding two T-3 lines and anticipates a sizeable increase in bandwidth usage. In spite of the hospital's aggressive bandwidth management requirements, the F5 BIG-IP Link Controller will continue to provide a

powerful load balancing solution while guaranteeing redundant, cost effective, and optimized bandwidth usage.

"Everything we've thrown at the F5 Link Controllers, they've been able to handle", said Morenzoni.

Availability

Redundancy provided by the BIG-IP Link Controller keeps the hospital's FirePass users connected to the network, and is the bedrock for non-stop access to ASPs responsible for patient accounting and scheduling. In terms of accounting, **"A network outage would have the potential to lose us hundreds of thousands of dollars a day,"** said Jay Manfred, network engineer at the hospital.

The F5 BIG-IP Link Controller has vastly improved WAN connectivity as well. Morenzoni commented, **"Our [Internet] uptime has gone from very poor to 99.3%"**.

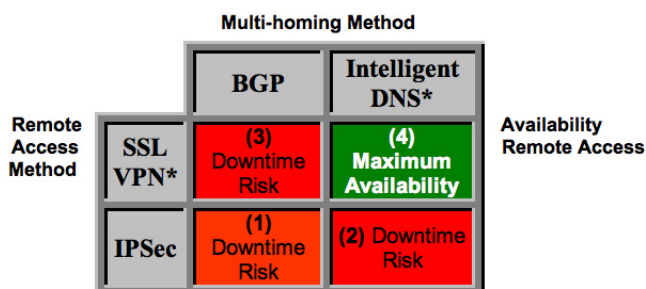
Conclusion

F5's FirePass SSL VPN and BIG-IP Link Controller solutions have played a key role in the success of Lake Forest Hospital. Hospital staff is pleased with the reliability, security, and functionality delivered by the F5 solution, and they couldn't be happier.

"F5 products do everything they promise," said Morenzoni. **"They work exactly the way we could have hoped for. If I had to do it all over again, there is no doubt in my mind I would make exactly the same decision."**

Tech Tip

Availability Quadrant for Reliable Remote Access



Inferior availability for Remote Access:

(1) IPSec and BGP

IPSec clients are traditionally hardwired to a static IP address. Regardless of the multihoming techniques used (BGP or Intelligent DNS) IPSec resiliency and availability is limited by routing paths. IPSec clients can experience up to 30 minutes of downtime when links fail because route propagation delays.

(2) IPSec and Intelligent DNS

Multihoming via intelligent DNS provides near instantaneous failover for hosted web based traffic. However, IPSec clients do not leverage DNS and rely on BGP for routing changes, which limits availability and increases the failover times when ISPs or routing issues exist.

(3) SSL VPN and BGP

SSL VPNs provide built in protection against ISP failures by using the DNS lookup process to select the best path. However, when organizations rely on BGP to multi-home and do not have an intelligent DNS system in place, SSL VPNs are at the mercy of BGP multihoming issues. Once again, a failed ISP or routing issue can translate into more than 30 minutes of downtime.

Maximum Availability for Remote Access:

(4) SSL VPN and Intelligent DNS

Through DNS, Intelligent DNS systems and SSL VPNs work to understand the real time availability and performance of each ISP and path into the network. Deployed together, these solutions provide near instantaneous ISP failover, providing a per connection link selection for remote users, and delivering a high I resiliency for an organization.

*Lake Forest Hospital deploys F5's FirePass SSL VPN and BIG-IP Link Controller (Intelligent DNS) solutions to provide maximum availability for Secure Remote Access.