

BUYER CASE STUDY

INTRUST Implements F5 Networks BIG-IP

Lucinda Borovick

IDC OPINION

One of the more visible forces behind the implementation of datacenter Layer 4–7 switch technology is to improve application performance for users. This technology, however, has the potential to provide additional benefits to an organization's IT infrastructure, including security, load balancing, and high availability, and can be the cornerstone to an IT department's business continuity and disaster recovery (DR) strategy. For INTRUST, an innovative bank that had an early entry into Internet banking:

- ☒ Datacenter Layer 4–7 switch technology was initially implemented for security purposes, specifically to help with intrusion detection and to enable encryption truncation functionality.
- ☒ After the initial installation, it leveraged other features, including load balancing to enhance performance and availability between the primary datacenter and a recovery site.

IN THIS BUYER CASE STUDY

This IDC Buyer Case Study describes the implementation of F5's BIG-IP products at INTRUST, an innovative and growing regional bank headquartered in Wichita, Kansas. In 2002, INTRUST evaluated products and technologies that would improve the security of its Web servers. The company implemented datacenter Layer 4–7 switch technology from F5 to support these initiatives at its primary and recovery datacenters.

This document provides a detailed examination of INTRUST's evaluation and implementation of F5's BIG-IP product, as well as the IT, network, and application infrastructure at the bank and the IT department's objectives. Specific benefits from this technology deployment are examined and future initiatives are highlighted. End users can use this information to benchmark whether datacenter Layer 4–7 switch technology is applicable within their environments.

SITUATION OVERVIEW

Organization Overview

INTRUST is a midsize bank headquartered in Wichita, Kansas, serving the region for more than 100 years. The bank is the oldest homegrown Wichita-based bank in continuous existence, originally established in 1876 under the name of the Farmers & Merchants Bank.

The bank has a long history of local business support, focusing on building relationships in the community it serves, delivering innovation, and emphasizing customer service. It is currently one of the leading small business lenders in the country and was one of the first 100 banks in the country to offer Internet banking services via its Web site (www.intrustbank.com). With a focus on making banking convenient and its customers successful, the bank has grown significantly in the past 10 years. From a competitive standpoint, its long-standing competitor was purchased in the mid-1990s by Boatman's Bank, which was quickly acquired by NationsBank, and then again by Bank of America. INTRUST prides itself on its long-standing local presence and history of supporting the community and region. The bank now has more than 45 branches throughout Kansas and Oklahoma and more than 100 ATM locations in these two states. In Wichita, the state's largest city, INTRUST has more banking locations than any other bank.

IT Overview

IDC recently conducted an in-depth interview with Jim Betts, operations officer and senior network analyst for INTRUST. Topics of discussion included a description of INTRUST's overall IT environment, network infrastructure, and application portfolio. Additionally, IDC probed for information regarding the implementation of F5's BIG-IP technology within the bank's primary and recovery IT datacenters. Specific information on this installation included the evaluation and implementation process, the resulting benefits, and future IT initiatives.

Betts' responsibilities include Web infrastructure, including networking and routing; security, including intrusion detection; VoIP; including application deployment; and serving as the backup resource to the system administrator. Betts' tenure spans 10 years at INTRUST during which the IT department has stayed relatively the same size. The IT department at INTRUST consists of 15 dedicated IT personnel, with 3 focused on telephony issues and the rest focused on network and application support. In the past few years, the IT department added a help desk function, and there are now an additional 3 people supporting those functions. The IT department at INTRUST has a relatively flat organizational structure — all IT personnel report to a department manager and/or an assistant manager. Most of the IT team works interchangeably with the servers and their applications, networking equipment, and the virtualized environment.

The IT department at INTRUST supports two major datacenters — a primary datacenter in downtown Wichita and a disaster recovery site (which the bank owns) in one of its branches in North Wichita. The primary datacenter is approximately 4,000 sq ft, with the existing DR facility in a 500 sq ft space. Collectively, these datacenters

house over 70 physical servers, 45TB of storage, networking gear, Web servers, firewall technology, and F5 devices. The bank has implemented virtualization technology representing 80 virtual servers. From an application standpoint, one of the bank's more critical applications is its statement and check imaging application, which is from Metavante (which previously acquired Advanced Financial Solutions). Metavante does not support virtualization, which is why the bank does not have a higher ratio of virtual servers to physical ones.

From a hardware perspective, the bank works almost exclusively with Dell servers (all are 1U, 2U, and 3U rack form factors) and chooses Dell because of superior price and performance. The IT department migrated away from Gateway servers several years ago because of quality issues. Storage is all EMC gear, with a recent upgrade to EMC's latest Symmetrix platform. Networking gear is exclusively from Cisco, with Cisco's 6509 as the core switch. Internally the servers connect to the switch via gigabyte copper Ethernet, with 9MB of throughput at the primary site and 6MB at the second datacenter. Externally, the bank has a gigabyte link between its primary and DR datacenters (two T1 lines). From a disaster recovery perspective, the bank is running synchronous replication (EMC's SRDF) between the two sites.

Challenges and Solution

Approximately five years ago, INTRUST's IT department wanted to improve the bank's security initiatives to more effectively protect the bank's IT resources against unwanted access through its Web servers. IT felt that intrusion detection was not sufficient because this technology does not detect attacks from properly encrypted traffic. The bank sought to ensure that no unwanted access could come through the bank's HTTPS Web servers.

The IT department began to explore encryption truncation, and through research, it determined that F5 was the only company at the time that had a comprehensive solution to meet its security requirements. After an initial evaluation, the company purchased F5's BIG-IP switch and installed it to sit between its firewall and Web servers.

Although the initial installation was predominantly for security purposes, INTRUST's IT department then implemented load balancing functionality on the switch to boost performance. The load balancing was between three types of Web servers — it put Web content (brochureware) on one server, image files on another, and Internet banking on a third server.

The most recent application of F5's technology at INTRUST is to satisfy disaster recovery initiatives. In response to regulatory directives (and since Hurricane Katrina put additional corporate focus on DR), F5's technology has been key to the bank's disaster recovery and business continuity strategies. About 18 months ago, the bank installed another F5 switch at its DR datacenter, ensuring that if a failure was to take place at the primary site, the second switch would pick up the load and redirect traffic to the DR datacenter.

Interestingly, 18 months ago when INTRUST was assessing its DR strategy, it decided to reevaluate competitive offerings in this space to make sure that it was still making the best platform decision. The IT department reviewed Cisco's offerings, but F5 came out on top in terms of lower cost, less complexity, and a more comprehensive solution. Of

particular praise from INTRUST is F5's management console that configures the entire system from a single point. Additionally, iRules, F5's open application programming interface (API) that allows end users to customize their applications to be more "network aware," is being used at INTRUST for business applications and to ultimately enhance security, performance, and availability. Recently, the bank added merchant capture capabilities to streamline the process of scanning, uploading, and processing check images, before sending them to clearing houses. iRules allowed the IT department to use its existing site certificate and seamlessly (and securely) add this capability to its Web servers with no disruption to the site.

Results

INTRUST gave the F5 technology high marks with respect flexibility and to supporting changes in its IT infrastructure either when upgrading or when implementing virtualization within its IT environment. During the consolidation process (when IT personnel were adding memory, expanding disk partitions, consolidating resource pools, or making other infrastructure changes), INTRUST was easily able to make these migration changes without disruption to the security or performance of the environment. Also, when upgrading the F5 device, the IT department was able to port all rules over to the new device with no new API development.

The IT department at INTRUST has analyzed several metrics relative to its datacenter Layer 4–7 technology, and uptime was improved from 97% to over 99.5% availability.

Future Direction

INTRUST is looking into a new disaster recovery facility. INTRUST is growing out of its DR facility — currently housed in cramped quarters in the basement of one of its branches in North Wichita. The IT department is in the process of constructing a new DR facility that will be migrated to in the next several quarters.

The company has no current plans to adopt WAN application delivery functionality. INTRUST is currently satisfied with its application performance over the WAN. The bank has a gigabyte link between sites, and at this time the link is not oversubscribed because performance is not an issue; INTRUST does not want to incur the costs associated with 45+ branch banks, and consequently does not anticipate adding WAN application delivery in the near term.

ESSENTIAL GUIDANCE

Advice for End Users

End users should seek answers to the following questions to help them comprehensively evaluate the security, performance, availability impact, and relative ROI of datacenter Layer 4–7 technology within their environments:

- Which sites/users are experiencing security, availability, or performance issues?
- What applications/servers are at the site(s), and what are the bandwidth and security requirements of these applications?

- ☒ Which locations are affected? What are the WAN connections/speeds at each of these locations?
- ☒ What are the security requirements? Is there a security policy? If not, what constituents should be involved in creating the security policy? If so, what IT policies need to be implemented to ensure adherence to the security policy?
- ☒ What are the latency, congestion, and bandwidth characteristics of the application(s) at each location?
- ☒ What applications/servers require load balancing?
- ☒ Do any applications require additional security features?
- ☒ Who are the key suppliers of datacenter Layer 4–7 technology? And what features and functions do their products support that help IT meet specific business requirements?
- ☒ Does the vendor have experience in the specific vertical industry? Can the vendor provide reference accounts with similar environments?
- ☒ Are there any server and storage virtualization/consolidation projects under way? How does the vendor's technology map into any overall datacenter consolidation/virtualization initiatives?
- ☒ How does the vendor's technology map into any DR/BC initiatives?
- ☒ How does the technology integrate with installed networking products, specifically routers?
- ☒ What expertise does the vendor have for training and maintenance? What is the server administration/maintenance process? How will these products fit within those processes?

LEARN MORE

Related Research

- ☒ *Worldwide Datacenter Network 2007–2011 Forecast* (IDC #213520, August 2008)
- ☒ *Worldwide Enterprise Remote Branch Network 2008–2012 Forecast* (IDC #212831, June 2008)
- ☒ *Worldwide WAN Application Delivery 2008–2012 Forecast* (IDC #212355, May 2008)
- ☒ *Datacenter Networking News from Interop* (IDC #212373, May 2008)
- ☒ *Worldwide Datacenter Layer 4–7 Switch 2008–2012 Forecast* (IDC #211578, April 2008)

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2008 IDC. Reproduction is forbidden unless authorized. All rights reserved.