

Gourmet distributor boosts security

First Source implemented a cost-effective, next-generation firewall solution for increased network security, constant uptime and ease of collaboration



“Looking at reviews by the systems admin community in terms of the performance and reliability of these devices, everything really pointed me in the direction of SonicWall.”

Kelley Parkes, Director of Technical Operations, First Source

Customer profile



Company	First Source LLC
Industry	Wholesale and retail specialty foods
Country	United States
Employees	500
Website	www.first-source.com

Business need

As First Source grew, it needed an updated security infrastructure to better protect against threats 24x7.

Solution

The gourmet food distributor deployed a Dell next-generation firewall solution to keep the business safe and running smoothly around the clock.

Benefits

- Increased security through content filtering and deep-packet inspection
- Easy collaboration between locations with site-to-site VPN protocols and load balancing
- Zero downtime with a double-loop network configuration for system rollover in case of failure
- Increased efficiency with secure mobile VPN access and separate, secure Wi-Fi access for employees and visitors

Solutions at a glance

- [Network Security](#)
- [Mobile Network Security](#)

Located in Toano, Virginia, just outside of Colonial Williamsburg, 50-year-old First Source LLC is a distributor of fine chocolates and other specialty food items, including Lindt Lindor truffles, Ghirardelli chocolate, extra virgin olive oil, gourmet barbecue sauce and even caviar. The company distributes through a single retail outlet as well as to customers nationwide via online sales and retail partners, so having a secure and high-performing technology infrastructure is critical to the business.

When Kelley Parkes, Director of Technical Operations at First Source, joined the company in 2007, it had been doing business for over a decade with the same Windows NT servers. These servers weren't very secure. In addition, with more and more customers nationwide, First Source needed to improve the speed and quality of its order processing. "We had servers in place that were 12 years old," Parkes says. "I knew we had to harden our infrastructure, or we'd put ourselves in a position where our services would go down."

And he was right. Around 2009, the company was hit by a nondelivery report (NDR) attack on its email server. NDR spam is tricky because it sends email to an address that doesn't actually exist for a particular IP, triggering an automatic error response from the email server and allowing the spammer to use the company's server as a relay for thousands of spam emails. NDR attacks can be challenging to remove and block once they've been detected, because technically they are a legitimate notification. The processing required for this relay caused the First Source email system to grind to a halt. Around the same time of this attack, the Conficker worm infected server operating systems at First Source, creating additional challenges with regard to the company's information systems. After an extensive scan and cleanup, Parkes was determined to keep company data out of harm's way.

He initially implemented a competitor's firewall, but the features were limited and could not scale. After a couple of years and two acquisitions in New York and California, it became obvious that something more robust was required. Parkes sought a solution that could offer content filtering and deep-packet inspection, along with fast processing power to ensure the overall infrastructure continued to run smoothly.

Parkes compared security products in the market from a technical standpoint and also read a lot of customer reviews. "When I looked at the SonicWall appliance's CPU and its ability to process information, it came in with the same stats as other machines out there that cost two or three times more," he says. "And looking at reviews from the systems admin community in terms of the performance and reliability of these devices, everything really pointed me in the direction of SonicWall."

Over a period of 18 months, First Source designed and deployed a company-wide SonicWall next-generation firewall solution — including firewall appliances at each remote location — to act as

Products & Services

Hardware

SonicWall NSA Series

SonicWall SonicPoint Wireless Access Points

"The site-to-site VPN technology is probably the best out there."

Kelley Parkes, Director of Technical Operations, First Source

the gatekeepers for the First Source IT infrastructure. The SonicWall solution has not only boosted the company's security, but having site-to-site VPN access with load balancing and high-speed internet connections has allowed the company to increase efficiency and collaboration too. With the application control feature, the company is able to have network resources focused on productive applications.

Securing business

Having a secure technology infrastructure in place not only protects First Source from outside attacks, but it puts customers at ease because they know their business-critical account information is protected. The SonicWall solution views all of the company's network routing between the internet and the company network as well as its backup and VPN connections.

In addition, Parkes and his team use internal content filtering to ensure employee traffic is not contributing to security issues. SonicWall generates automatic weekly reports detailing the top websites users have been accessing, ongoing bandwidth usage and other details that help them keep track of the system and how it's being used.

"The reports allow us to be proactive instead of reactive when it comes to handling how our network performs," Parkes says.

Site-to-site collaboration

One of the major selling points for First Source was SonicWall's ability to support site-to-site VPN access and load balancing. Prior to the SonicWall installation, all First Source locations operated independently. The company did not have a way to easily share information and collaborate on projects until it connected the various locations using the site-to-site VPN technology provided by the SonicWall appliances. Prior to the upgrade, teams would have to ship external hard drives around to the other sites to share large marketing

projects related to the company's various product catalogs and high-definition graphics files .

"As we continue to improve our business intelligence systems, I've been working with large database table extractions where the information can be in the hundreds of megabytes," Parkes says. "Obviously, you can't easily attach that to an email and send it to someone, but with all of our locations connected to network shares and folders, I can make the information available in one place so everyone can access it from their location. Having that VPN link and load balancing to connect us makes it seem as if we're all in the same building."

Teams can now easily collaborate, saving time and money. "The site-to-site VPN technology is probably the best out there," Parkes says.

Zero downtime

In early 2014, Parkes hired Systems Engineer Dave Rupert. Parkes and Rupert's prior experience with SonicWall appliances allowed them to design a double-loop network configuration for First Source that added security and fault tolerance. If a location using the primary (private fiber optic MPLS) loop of this network fails to connect — because of circuit issues outside of the company's control at any of the company's five locations — that location will automatically roll over to the secondary network loop so that employees and customers always experience continuous availability.

"From a hardware performance standpoint, a software reliability standpoint and a usability standpoint, it's all just easy for us to work with."

Kelley Parkes, Director of Technical Operations, First Source

“One of our routers went down for about four hours recently and no one noticed,” Rupert says. “Kelley and I got the alert that the connection was down, and the firewall immediately recognized the issue and failed over to the loop that was working.”

For a company that handles approximately 20,000 electronic transactions per month resulting in annual business revenues of nearly \$400 million, a lot would be at stake if the entire network went down.

“Our customers know they’re not limited to a 9-to-5 schedule for customer service,” Parkes says. “They can go to our e-commerce website and place orders online any time of day.”

Mobility means efficiency

The SonicWall secure connection app allows employees to connect using Android or Apple devices from anywhere using VPN access with outstanding speeds. “We laugh about it, but over the summer Dave was able to answer user questions and provide support while poolside,” Parkes jokes. “On a more serious note, he is very good at what he does. It only takes him five minutes or so to get on his tablet and change somebody’s password or fix an issue, and we think that puts us a step ahead of most businesses — being able to resolve issues from literally any location.”

Parkes likes the mobile capabilities because it allows him to keep tabs on the network in real time over VPN. “I’m able to see any issues right there on my tablet. It doesn’t matter if I’m in the office or not. I can handle any challenges that come up at any time on any day.”

In addition, First Source uses SonicWall SonicPoint wireless access points in each location allowing effortless access to the network using mobile devices and laptops. Also, the company is able to deliver a guest network that is completely separate from its production network. Visiting customer sales reps and other guests can easily log in and work on-site without treading on the internal company network. This feature provides greater customer service and more flexibility during meetings.

“Since implementation, we have had no issues with the product at all,” Parkes says. “From a hardware performance standpoint, a software reliability standpoint and a usability standpoint, it’s all just easy for us to work with.”

View more case studies at www.sonicwall.com/casestudies