



Simplifying Network Infrastructure and Reducing Costs

A Case Study in WatchGuard Network Security

BACKGROUND

M2R Technology Group, based in West Chester, Ohio, is a computer network engineering company that offers IT planning, management, and support services. By designing systems that are both reliable and efficient, with each component engineered to precisely fit its clients' business needs, M2R helps clients streamline their business operations. M2R's services also include selecting, supplying, and installing the hardware and software required to implement its solutions.

One of M2R's clients is Shared Resource Technology Group (SRTG), located in Cincinnati, Ohio. SRTG is a service organization formed by three Ohio credit unions for the purpose of offering cost-competitive, industry-focused technology solutions. Using a collaborative business model and leveraged technical expertise, SRTG provides its members with core data processing solutions and server and web hosting. It also assists them with network and PC management and disaster recovery.

CHALLENGE

SRTG's WAN, as originally deployed, consisted of a mix of T1 and Ethernet WAN connections in the traditional point-to-point configuration, with Cisco routers at each end. As the organization grew, it added new circuits individually, resulting in a mix of router types and an overall lack of standardization. This lack of standardization made the network difficult to monitor and keep up to date.

In addition, SRTG was finding it difficult – and expensive – to enlarge its network to accommodate expansion, monitor WAN operations, and troubleshoot problems. To stay on top of growth, SRTG had to repeatedly purchase more equipment. And to keep its highly complex network functioning smoothly, it had to outsource engineering support.

To solve these problems, SRTG put out a bid to redesign the core of the network. Their requirements included high bandwidth, high availability, and real-time reporting and troubleshooting. In addition, federal regulations required separation of the traffic from each of the three credit unions the organization supported. SRTG previously met this requirement by using separate equipment for each credit union, but that approach was expensive both in terms of hardware and labor.

After reviewing bids, SRTG selected M2R to do the work, in part because their bid came in much lower than the others. “A key reason we were able to keep our bid so low was the cost-effectiveness of WatchGuard firewalls, which enabled us to reduce hardware costs by over 50%,” said Steve Guest, M2R’s chief operations officer.

WATCHGUARD® SOLUTION

In redesigning SRTG’s network, M2R removed all routers between SRTG’s collocation facility and its main branches and routed all traffic – including a mix of 1000 Mbps LAN, 100 Mbps and 10 Mbps WAN, and 10 Mbps Internet traffic – directly through two WatchGuard Firebox® Peak™ X6000 appliances.

“With the WatchGuard firewalls’ high bandwidth, large number of ports, and ease of management, we were able to get rid of seven routers and meet all of SRTG’s needs, including the separation of traffic from the three credit unions and the reporting specifications, with just two X6000 appliances,” said Guest. “And the only reason we needed the second box was to provide full fault tolerance. All the other products we looked at would have required around 10 times more equipment, or else a very high-end core router that would have cost up to four times what the two WatchGuard firewalls cost.”

Deployment

M2R began installing the new network in early 2006. In the initial phase, two WatchGuard Firebox Peak X6000 firewalls were deployed in a redundant configuration to provide high availability. These firewalls formed the core of the new deployment, replacing seven non-redundant routers. This phase also included redeploying existing third-party VPN routers to the untrusted side of the network so their traffic could be filtered. (Previously, these routers were connected directly to the network backbone, with no ability to filter traffic.)

During this phase, M2R moved SRTG’s three credit unions over to the new system one at a time. “The WatchGuard firewalls are very, very simple to deploy – in large part because of their graphical user interface, which makes setup and configuration really easy,” noted Guest. “We had the X6000s up and running the same day they arrived, and started the switchover that same day. In fact, some of the smaller deployments took us less than an hour to set up.”

The core switchover took M2R about six months because of other network components, including a large number of third-party VPNs. “SRTG had made some small windows available for downtime, but the WatchGuard firewalls made switching over so easy that we didn’t need them. We could complete a switchover in a matter of moments,” said Guest. “The ease of use of the WatchGuard firewalls played a big role in enabling us to manage the switchover with zero downtime.”

Equally important to SRTG, M2R was able to carry out the switchover without needing the additional routers, switching equipment, and phone lines that are typically required for a WAN cutover with no service loss. Although the additional equipment is only needed temporarily, it can double a company’s infrastructure costs during the time that it’s in place. M2R’s solution, however, required no additional equipment. “We just unplugged the lines and plugged them into the new equipment,” said Guest.

Because M2R was able to keep costs so low in designing and installing the new network, SRTG kept the team on the project after the core switchover was complete so they could add more features to the network. This included a centralized offsite backup facility with a large disk farm that provides real-time backups for more than 50 servers. The facility replaced a random collection of tape backup equipment that had been installed on each of the servers, along with the batch tape-backup procedures the organization had previously used. The high bandwidth of the X6000 appliances enables them to handle the backups along with the normal network traffic without any problems.

BENEFITS

A substantial benefit for SRTG was the low cost of M2R's solution – a benefit due in large part to the cost-effectiveness of the firewalls. Not only was the initial price less than many competitive products, their design also enabled M2R to get the job done with far less equipment. For example, because the X6000 has eight ports, M2R was able to meet SRTG's traffic separation requirement with a single appliance, simply by plugging each of the three credit unions it supported into a different port. "The WatchGuard firewalls have doubled the usual number of ports," noted Guest. "I'm unaware of any competing product that has anywhere near that many." Because of the cost effectiveness of the WatchGuard products, the hardware costs in M2R's network design were more than 50% lower than the hardware costs of competing bids.

Interoperability with a wide variety of different equipment was another cost-reducing factor. Because of the broad compatibility, M2R was able to retain SRTG's many legacy VPNs. This saved the company the expensive of replacing them, as well as several weeks of engineering time that would have been required to reconfigure the remote PCs and train end users to use the new software. In the future, if SRTG chooses to use the built-in VPN capabilities of the WatchGuard firewalls, that option is always available to them. And they can, if they wish, choose to switch over one user at a time to minimize the impact of the change. The benefit of using the firewalls' built-in VPN capabilities is that it extends the redundancy of the WatchGuard firewalls to VPN users as well.

The high bandwidth of the WatchGuard products was another advantage, as the credit unions that SRTG supports generate considerable traffic. Each has a main branch plus several sub-branches, as well as multiple ATMs. With the X6000's throughput ability, however, plus the 10Mb Ethernet WAN that M2R installed between the core collocation facility and the three credit unions' main branches, SRTG had plenty of bandwidth to support all traffic.

The X6000's easy-to-use management capabilities helped speed the deployment process. What's more, the centralized management and real-time monitoring capabilities enabled SRTG staff to take system management functions back in house, so all systems, local and remote, could be managed from one central location. "With the entire routing core collapsed into a pair of redundant WatchGuard firewalls—and the firewalls' intuitive graphical user interface—it was easy to train SRTG to maintain the infrastructure in-house, with their existing staff, rather than continuing to outsource this function," said Guest. "That was another source of significant savings."

Monitoring, reporting, and troubleshooting capabilities were also greatly improved. With all traffic coming in over the WAN through the redundant WatchGuard firewalls, network administrators could monitor network traffic in real time and react proactively to potential support issues. "The combination of centralized management and color-coded real-time logging makes it easy to spot potential problems, such as high bandwidth usage," said Guest. "In fact, in many cases, SRTG was able to identify and resolve problems before users were even aware of them."

"Having all the equipment in our own facility – as opposed to in a vendor's facility, as it was previously – in itself makes the network much easier to manage," added Dave Teetz, SRTG's network administrator. "And with the ability to maintain three separate traffic streams and still have all traffic coming in through one firewall, plus the centralized management capabilities, it's even easier." He noted that most of the issues that have come up – such as the need to add a new port for an additional ATM, or to allow users to have browser access to an additional type of content – can be handled in just a few minutes. That's a far cry from the previous situation, where a user would report a problem, the network staff would pass the report on to the external service provider, the external provider would fix the problem, and the resolution would eventually filter back to the network staff.

“With direct access and centralized management, we can provide our users with a much higher level of service,” said Teetz. “We also appreciate the high reliability of the firewalls. We’ve experienced no problems at all with them.”

As for Guest, he’s convinced that WatchGuard firewalls are a network essential. “We’ve been using them for seven or eight years now, and I believe they are absolutely the best product available on the market,” he said. “They have far and away the best pricing; they’re highly reliable, and they’re really easy to manage – which is important both for us, as a VAR [value-added reseller], and for our clients. We go out of our way to recommend WatchGuard products to our clients for all networks we design.”

For more information about WatchGuard security solutions, visit us at www.watchguard.com, or contact your reseller.

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB: www.watchguard.com

U.S. SALES: 1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2007 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Firebox, and Peak are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGPE66465_072409