



# Integrating Security for Multiple LANs with a Central WAN

## A Case Study in Network Security

November 2007

### **BACKGROUND**

The customer is a large community-based agency responsible for administration of all departments, facilities, and government services within the community. The services are varied and include Education, Finance, and Human Resources departments, public service departments such as the Fire and Police Departments, community service organizations such as the Boys & Girls Club, the Health Clinic and Pharmacy, as well as a casino and shopping center.

### **CHALLENGE**

A solution that would provide security for a dozen separate LANs operated by various departments and facilities, while allowing those networks to integrate seamlessly with the organization's central WAN, was required. The organization needed a solution that would provide secure Internet access for voice, video, and data for all

government services, and would also provide security for hosted web servers for all the separate entities involved.

Executives and upper management needed to access their networks, servers, and desktops while traveling. The VPN connection had to be secure and reliable. Additional security was needed for the medical center and pharmacy to comply with HIPAA requirements.

Finding a solution that would provide security for multiple disparate LANs proved to be an exceptional challenge. The organization had previously contracted with Verizon to provide network security services, but the vendor had been unable to successfully deploy their product, Cisco Pixbox, due to the number of separate LANs involved.

## **WATCHGUARD® SOLUTION**

A privately-held firm that provides network and security consulting services determined the extent of the security required, and recommended a solution employing WatchGuard Firebox X5000 security appliances.

The Firebox X5000 was recommended for its advanced networking features and 2.0 Gbps firewall throughput to support high-speed LAN infrastructure and gigabit WAN connections. Additionally, the inspection of all seven layers of data communication offered by the Application Proxy technology from WatchGuard was ideal for providing true zero day attack prevention to the multiple networks in place.

"[The solution] was a challenge, because of the number of different networks the organization had," explained the president of the security provider. "We had to build a substantial route table to accommodate the diverse network infrastructure. Also, we had to create approximately 70 custom packet filters in order to allow all the different types of data through to the various local area networks. The fact that WatchGuard was flexible enough to be able to route traffic efficiently between all the different networks was a huge advantage."

Because redundancy was a mandatory requirement for the security solution, two WatchGuard Firebox X5000 appliances were installed in High Availability mode. Both firewalls maintain a mirror image of the configuration. If the primary firewall should fail or become unavailable for any reason, the secondary firewall immediately takes over for it as the primary firewall.

Compatibility was another important consideration in creating a successful integrated security solution. As part of the security setup, the WatchGuard Firebox X5000 was deployed in tandem with an RSA Technologies secure authentication server and an Aventail ST-1500 SSL-VPN appliance to great results.

"The fact that WatchGuard meshes with the RSA Secure Authentication server was very critical," said a representative from the security provider. "[They] wanted dual authentication methodologies to provide a means for securely accessing servers and applications on the local area network from any remote location, while at the same time keeping unwanted traffic out of the network. We used the RSA Secure Authentication server in conjunction with their token key fobs, so we actually had three types of authentication being applied to remote access users before they ever got to the LAN. Actually there were four, because the Aventail SSL-VPN appliance played a part in that as well."

## **BENEFITS**

Since the deployment, the customer has found it much easier to manage their security solution. The clear, visually driven interface of WatchGuard System Manager (WSM) with its plain-English log messages has made it easier for the organization to validate security policies and to make changes or adjustments as desired. At the same time, the interactive tools in WSM have enabled them to take instant preventive or diagnostic action directly from the monitoring interface, without the need to open separate configuration screens.

"I've been able to implement all necessary applications with the WatchGuard firewall," commented the organization's network engineer. "We have certain 'access allows' that I've been able to implement with no trouble. Also, we use the SYSLOG to assist us in isolating threats within the network, whether they are inside or outside. We can isolate viruses and examine denial-of-service attacks to help us identify and eliminate problems within our network."

"The Live Security® service has also been helpful in providing maintenance and threat updates. Overall, the WatchGuard Firebox X5000 appliance solution has provided us with a very stable, robust, low-latency firewall."

For more information about WatchGuard security solutions, visit us at [www.watchguard.com](http://www.watchguard.com), or contact your reseller.

---

**ADDRESS:**  
505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

**WEB:**  
[www.watchguard.com](http://www.watchguard.com)

**U.S. SALES:**  
1.800.734.9905

**INTERNATIONAL SALES:**  
+1.206.613.0895

**ABOUT WATCHGUARD**

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](http://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. ©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Firebox, Core, Peak, and Stronger Security, Simply Done 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. WGCE66514\_022908