



Protecting a Large Distributed School Network from Without and Within

A Case Study in Network Security

BACKGROUND

Compute is a solution services company and managed service provider specializing in IT infrastructure, Voice over Internet Protocol (VoIP), wireless broadband, data centers, and procurement. Established in 1983, the company maintains its headquarters in Oshawa, Ontario, and delivers local service in most major centers across North America.

One of Compute's clients is the Durham District School Board in Durham, Ontario. The Durham District serves more than 70,000 students and 8,000 staff members, in an area encompassing some 3,700 square miles, and includes 105 elementary schools and 21 high schools in the regional municipality of Durham. Its main offices are located in Whitby, Ontario.

CHALLENGE

Over the past two years, the Durham District School Board had been upgrading its IT systems by converting its WAN to fiber, and implementing various IP solutions, including a VLAN (virtual LAN), VoIP, and IP-based surveillance cameras. As part of the upgrade, the district also wanted to strengthen its network security.

The Durham District had already experienced malware problems that brought down one school's network, and eventually spread to affect other district facilities. With nearly 80,000 users connected to their network, the Durham District wanted to ensure aggressive steps were taken to prevent future malware attacks and other unauthorized intrusions.

Like other K-12 school districts, the Durham District had to protect their network from external threats, as well as the risk of unauthorized intrusions by users within the network. “Today’s students are often able to manipulate technology in order to exploit weaknesses within a system and gain access to restricted information,” explained Don Conaby, president of Compute. “The Durham District realized that a single outbreak could potentially spread throughout the entire district, giving students access to other schools and potentially the main education center. They needed a security solution that would prevent this.”

The district’s environment was complex. With approximately 15,000 desktops and a need for more than 130 firewall appliances, the WAN was similar in size to that of a large enterprise. In addition, the protection of sensitive student information was vital, and the school district is required to retain that information until a student turns 18. The district also needed to provide sufficient redundancy to ensure uncompromised connectivity, even in the event of equipment failures. What’s more, because the Durham District was in the middle of changing its IP strategy, Compute had to validate that its proposed solution would work with the district’s current IP systems and with the new systems that it would be implementing. The complexities required that Compute spend several months researching possible solutions and pre-qualifying vendors to ensure success.

WATCHGUARD® SOLUTION

In mid-2006, Compute began discussions with WatchGuard Technologies about its Firebox® X family. “We already knew about the company’s strength as a firewall vendor, but we hadn’t realized how extensive their unified threat management (UTM) capabilities were,” said Conaby. “Once we found out that their security solution incorporated anti-virus, anti-spam, anti-spyware, and content filtering capabilities, as well as intrusion detection and prevention, it was no contest – we knew that we’d be moving forward with a WatchGuard-based solution.”

Another key differentiator for Compute between WatchGuard and the other vendors that were evaluated was the real-time monitoring and reporting features, and WatchGuard was the only vendor to provide this. “That was a vital improvement for the Durham District,” notes Conaby. “When you’re monitoring some 70,000 students connecting to the network on around 15,000 computers, you don’t want to find out that you have a problem after the fact – you need to be able to catch it while it’s occurring.”

Compute also liked the scalability throughout the WatchGuard product line. “You can easily upgrade the boxes without having to replace the hardware,” explained Steve Conaby, Compute’s Education Account Manager. “You just purchase a model upgrade license key. Since the Durham District installation was going to involve more than 130 appliances – and its needs could increase in the future – it was an important feature for us to consider.”

Solution Details

Compute’s solution provided WatchGuard Firebox X firewalls at each location, for a total of 134 security appliances. This gave the school district full proxy firewall capabilities at each school and facility, providing protection against intrusions, viruses, worms, and spyware, from both external and internal sources.

Two of the company’s highest-end firewalls – the Firebox X Peak™ 8500e-F – were placed at the school district’s data center in the central office. These appliances are specifically designed for complex networks and data centers, and provide multi-gigabit performance and Ethernet interfaces with fiber interface support. They also provide stateful packet and application-based proxy inspection, branch office and mobile user VPN capabilities, and zero day attack prevention to deliver a much higher level of security than systems that rely solely on signature analysis for protection.

By installing two Fireboxes at the district’s data center, Compute’s implementation provided redundancy in the event of an equipment failure. The fiber ports of the X8500e-F enabled the school district to connect the appliances directly into its fiber-optic WAN, without having to purchase a separate fiber switch.

“Originally, the district was planning to purchase firewalls only for its peripheral sites, as it already had Cisco firewalls in its data center,” said Steve Conaby. “Once they found out how powerful the WatchGuard appliances were, they decided to replace their Cisco firewalls, as well.”

The remainder of the firewalls came from the Firebox X Core™ e-Series line: one X1250e appliance, 13 X750e appliances, and 118 X550e appliances. The Core e-Series are the company’s best-selling security appliances and provide comprehensive unified threat management that is ideal for peripheral locations.

Each of the Core e-Series models were enhanced with Fireware® Pro advanced appliance software, which provides advanced networking features for the traffic-shaping and redundancy capabilities that Durham’s network required.

In addition, the Durham District added a suite of WatchGuard UTM security subscriptions to enhance protection in critical attack areas, including anti-spyware, anti-spam, anti-virus, and web content filtering.

BENEFITS

The number one benefit that the Durham District has experienced from its WatchGuard solution is **increased security, from both external and internal threats**. The district’s three main concerns were intrusion detection and prevention, anti-virus protection, and content filtering – all areas in which WatchGuard UTM solutions excel.

The **web content-filtering** capabilities of the WatchGuard firewalls were critically important, and enabled Durham to eliminate a third-party content-filtering solution that it had previously been using. “It’s a double benefit because not only are we saving money, we now have content filtering that is much more effective than what we were using before,” said Wilson Chan, Manager of Information Systems for the Durham District School Board. “Since installing the WatchGuard solution, we’ve learned that some of our staff has been shopping on the Internet during business hours. Now we’ve blocked those sites, so that can’t happen any more.”

“The content filtering piece is compatible with Active Directory, allowing the Durham Board to create separate policies for teachers and students,” explained Don Conaby. “As a result, they can tighten the web security for students, while allowing teachers the flexibility they need for research and content downloading.”

The solution’s **real-time monitoring** component is another major benefit, as it enables IT administrators to look at each individual school or facility and see what is happening at that very moment. With this information, they are able to troubleshoot problems instantaneously and make certain that they are diagnosing the correct issues. This is a capability the Durham District hadn’t had before.

“Having real-time monitoring is great, because we no longer have to go to a log file after the fact to discover what problems we’ve been experiencing,” said Chan. “We can see what users are trying to do and solve the problem immediately.”

The **strong centralized management** features allow Durham’s IT staff to administer all of its sites from one central location. Because they can create one master configuration file and easily replicate it for all the other appliances and activate it remotely, they can quickly complete a large deployment.

“Before, whenever we needed to download a patch or make some other software change to our firewalls, we’d have to send technicians out to every facility,” said Chan. “We were easily spending more than 250 labor hours a year adjusting the software—not to mention the time the schools lost from having their systems down during the update. Now we can implement software changes quickly and easily, during off hours, with no need for travel. It’s a tremendous time saver.”

The reports provide a wealth of information, including what kinds of services are being used and what types of threats the WatchGuard systems have found and counteracted. Not only do the reports demonstrate the value to the Durham District of their firewall investment, they also enable the district to establish more effective security policies moving forward.

“With the WatchGuard reports, we know exactly where the problems are and can take the necessary steps to counter them,” said Chan. “Looking at each school—and even at each desktop within a school—we can identify which viruses or other malware the WatchGuard firewalls have blocked, see inappropriate web sites students or staff are attempting to access, and recognize any attempts that have been made to hack into our systems. Soon it will be even better: the next WatchGuard software release will allow us to identify these problems down to the individual user level.”

Additionally, the Durham District liked the **flexibility of the WatchGuard UTM offering**. While the district licensed all components of the UTM package – anti-spyware, anti-spam, anti-virus, and content filtering – they still liked having the ability to choose elements individually. “Customers like the way WatchGuard works with them to best meet their individual needs,” comments Don Conaby. “It does not force them into an all-or-nothing situation.”

Strong support was also a major selling point in the eyes of the Durham District. “They knew they’d be making further changes to their network over time, and they wondered if the solution would be able to adapt,” explained Steve Conaby. “From our perspective, the support we get from the manufacturer is critical,” he added. “When we got close to project commencement, WatchGuard supported us to the nth degree, sending out technicians to meet with us and the school district – taking whatever steps were necessary to make sure the solution would work in the district’s environment. They really went above and beyond to help us make the sale. Once Durham saw the extensive support that WatchGuard provided during the presales period, it really increased their comfort level.”

As for the Durham District, they are delighted with the way Compute’s solution and the WatchGuard firewalls are working out for them. “We spent over a year researching and testing different products, and we’re very happy with the WatchGuard firewalls,” said Chan. “Of all the solutions we looked at, WatchGuard is definitely the best fit with our technology and our needs. We highly recommend them to any school district that wants to get a handle on its security problems and prevent unauthorized intrusions, whether from outside or inside the network.”

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

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.

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, Fireware, Core, 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. WGCE66474_072409