

DOCUMENT\* PRESENTED  
BY WICK HILL

access  
**access**  
management  
**management**  
performance  
performance  
security  
**security**

\* © Wick Hill and the Wick Hill logo are trademarks of Wick Hill Group Plc. Registered in the UK and other countries. Other logo, brand and product names are trademarks of their respective owners. All 3rd party information contained within this document is copyright of the originator. Errors and omissions excluded.



# Countywide Government Network Stays Secure with WatchGuard Solution

## A Case Study in Network Security

March 2008

### **BACKGROUND**

The Goshen County government operates one of the most advanced networks in the state of Wyoming. The county hosts its own Internet server, has its own WAN and a private/public co-op using a VPN to link data and services to the state government and other law enforcement networks. The county also operates a 180-extension VoIP phone system with remote locations over a LAN, as well as WAN and VPN connections. Additionally, the county offers free Wi-Fi service with both a public and a private network.

"We support all government entities in the county," explains Matt Rolf, IT Director for Goshen County. "Every firehouse and police station in the county is on the network. Some of the small town governments in Goshen County use our network as well. We supply them with software, desktops, tech support, email, web hosting, and in some cases Internet access. This is cost-effective for small towns that might have only two employees working in the town hall, who can't afford tech support or their own IT system. Working off our network saves them money and costs us practically nothing. And it makes things productive for all citizens of the county."

### **CHALLENGE**

As the Goshen County government network has grown, so has the need for enhanced security to protect mission-critical services and government information. As a government agency, they are responsible for protecting confidential data according to government compliance standards, including Criminal Justice Information System (CJIS) security policies set forth by the FBI.

Goshen County faced a number of challenges in finding an effective security solution for its network. First, the solution had to be robust and scalable enough to handle the ever-increasing number of VPN connections and Internet-based applications on the network.

In addition, the security solution needed to be cost effective. Goshen County's entire annual budget is \$6.2 million. Its annual IT budget is \$120,000, including salaries. With the high cost of commercial bandwidth, the county cannot afford leased lines and uses residential services for its network.

The low quality of Goshen County's residential-grade Internet providers posed another challenge. Goshen County uses cable, DSL, and wireless providers, and one of these will typically go down every day. The county cannot afford a connection with guaranteed uptime, so the security solution needed to provide redundancy, as well as failover that would not be noticeable to the end user.

A special concern was the county's ability to offer free Wi-Fi services to the general public in its government buildings, while still protecting the county's private network from potential outside attacks from wireless-capable devices.

## **WATCHGUARD® SOLUTION**

After consulting with WatchGuard® Technologies about Goshen County's security needs, Rolf selected and installed a WatchGuard Firebox® X Core™ 750e appliance with a Fireware® Pro advanced appliance software enhancement. The X750e appliance allowed Goshen County to unite its multi-site network environment under a single unified threat management (UTM) solution, in compliance with CJIS regulations.

During the initial consultation, WatchGuard referred Rolf to CDW-G, the division of Computer Discount Warehouse that sells IT products and services for government clients. Rolf purchased the WatchGuard products he needed from CDW-G and did the installation himself. "WatchGuard offered the only security solution that could affordably handle more than two ISPs. CISCO wanted \$25,000 for a similar solution. I also looked at Juniper and SonicWall, but they could not provide the solution we needed." said Rolf. "And it was a relatively painless installation."

"WatchGuard was the only company that had enough confidence in their technology to offer us a free one-month trial," Rolf commented. "They gave us time to test the product and see if it was what we really wanted."

## **BENEFITS**

### **Reliable, Secure Connections for Multi-Site Networking**

The X750e with Fireware Pro can handle up to four ISPs, provides multi-WAN load balancing, and delivers application layer security and remote location encryption for multiple VPN tunnels.

WatchGuard Firebox allows the secure exchange of government information over Goshen County's network, while providing proactive, multiple-layered inspection of network traffic to block cyber attacks. All network traffic on Goshen County's LAN is locked into the internal firewall known as the "Trusted Interface Zone," which allows no traffic except what is specifically designated by Goshen County's security policies. All inbound and outbound traffic on Goshen County's LAN passes through the Firebox's various proxy policies where it is scanned for viruses, spyware, and other malware, and logged.

"A few months ago, we had a Distributed Denial-Of-Service attack," said Rolf. "The attacker sent us a deluge of malformed packets designed to block up the traffic on our network. Receiving 10,000 packets per second overwhelmed our network. The WatchGuard Firebox firewall blocked the attacks, but we still had to process traffic on the network. We used the Firebox System Manager to monitor network traffic to see what was hitting in the interfaces. Using this information, we were able to coordinate with our ISP providers to stop the attack."

### **Effective Security for Public/Private Wi-Fi Access**

The Firebox X includes security options that allow Goshen County to provide regulated Internet access to certain users through the county network, while still protecting confidential government information. For example, Goshen County has free public Wi-Fi access for wireless-capable devices in government buildings. The government also has agreements with organizations and programs that are considered "non-trusted entities" who are not official government agencies but occupy office space in the Goshen County government buildings.

On the Goshen County network, all outbound Internet traffic from public wireless users and non-trusted entities is routed through a special security interface on the WatchGuard firewall known as the "DMZ." With the DMZ option, public Wi-Fi users and non-trusted entities have access to the Internet through Goshen County's ISPs, but are isolated from accessing the county's government network. The DMZ interface includes security options set up by Goshen County to regulate Internet access by these users. For example, all Internet traffic from public Wi-Fi users through the DMZ is limited to an access speed of 256k.

### **Redundancy**

The X750e provides redundancy to Goshen County's DSL, cable, and wireless ISPs using a "round-robin" checking system. The firewall moves traffic between all three ISPs to share bandwidth, and periodically pings each ISP to make sure it is still working. If the pinged ISP returns three failure responses, the firewall determines that the ISP has gone down, and directs traffic to the other two ISPs. When the ISP is restored, the firewall pings it again, and must receive three positive responses before it allows traffic to be routed onto the ISP once more.

By upgrading to Fireware Pro advanced appliance software, which enables policy-based routing, Goshen County can direct traffic to a designated provider based on the traffic's source, destination or protocol. For example, Fireware Pro uses policy-based routing derived from protocol to route all outbound email traffic from Goshen County's network over a specific ISP. If this ISP fails, the Fireware Pro software has a specific failover order that automatically re-routes all outbound email traffic over another ISP. The same principle applies to web-browsing traffic and outbound VoIP on Goshen County's network.

### **Real-Time Bandwidth Utilization Monitoring**

Goshen County came to rely on the Firebox's real-time bandwidth utilization monitoring feature, which allows the county to monitor the use of its networks. "With real-time bandwidth utilization monitoring, we can monitor our ISPs," said Rolf. "If we are not getting as much access as we should, we can contact the provider about it. It makes me feel better to know what's going on in the network."

### **Dependable Products, Exceptional Support**

Rolf has also been impressed with the reliability of the appliances and software from WatchGuard. "We've never had to replace WatchGuard's technology, and it has never failed. We feel comfortable with the WatchGuard support agreement behind it. The WatchGuard LiveSecurity<sup>®</sup> plan is designed specifically for IT professionals like me. It gives me peace of mind to know that WatchGuard is there to help when I need them."

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. Our newest products – the WatchGuard SSL 500 and SSL 1000 – make secure remote access easy and affordable, regardless of the size of your network. 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, Fireware, Core, and LiveSecurity 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. WGCE66518\_032708



# 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



# Protecting a Large Distributed School Network from Without and Within

## A Case Study in Network Security

October 2007

### **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](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. ©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\_111507



# Extending Robust UTM Protection to the Edges of the Network

## A Case Study in Network Security

November 2007

### BACKGROUND

Tollways Management Corporation (TMC) operates and maintains the longest expressway in the Philippines – the North Luzon Expressway (NLEX). Established in 2000, TMC has been managing the NLEX and the Subic-Tipo Road since 2005 in support of the government’s program to spur economic and social development in Northern Luzon. TMC, part of the Lopez Group of Companies, has also formed strategic alliances with the world’s largest toll road operator – Transroute International SA – which has operations in Australia, France, Greece, and other countries.

### CHALLENGE

Even before TMC commenced managing NLEX operations in February 2005, the company recognized the need to upgrade the security and capacity of its existing firewall. With the number of users expected to grow dramatically from 50 to over 200, it was clear the initial firewall could not scale to meet TMC’s changing needs.

According to TMC Information Technology Manager Arthur Ong, the existing firewall presented several problems. “First, the unit’s performance degraded drastically as more and more users simultaneously accessed the Internet. In addition, the cost of additional user licenses for both the firewall and the VPN was significant. And finally, since the existing firewall management system worked through a text-based program, it was difficult to use a non-GUI-based firewall interface,” said Ong.

TMC had several additional requirements it wanted to address by investing in a superior network security solution.

“Because our main office and the branch offices had different ISPs, we needed a security appliance that could seamlessly integrate with the WAN connecting the two branch offices, the mobile VPN linking our headquarters’ executives to our network, and the secure remote access VPN connecting our mobile users and consultants in France,” added Ong.

Most importantly, TMC wanted an appliance that offered unified threat management (UTM) and failover capability with the capacity to secure at least 300 simultaneous users.

## **WATCHGUARD® SOLUTION**

In the first quarter of 2005, TMC requested its long-standing IT solutions provider, Integrated Computer Systems, Inc., to assist in evaluating network security options. After considering a number of solutions – both appliance and software-based – TMC chose WatchGuard as its vendor of choice.

Anthony Jhay Fausto, WatchGuard Product Manager of Integrated Computer Systems, Inc. said, “We chose WatchGuard because its stand-alone security appliances could unify and integrate multiple security features onto a single hardware platform with a single management interface. Their solution can provide automatic integration between TMC’s Firebox® X Core™ and Firebox X Edge units, with wireless access for their executives – which ultimately means more reliability and convenience for those connecting from remote offices to headquarters.”

TMC decided to install WatchGuard Firebox X security appliances including the Firebox X700 for its main office, a Firebox X50 at its 15-user branch office, and a Firebox X15w at its 5-user branch office. Once the decision to deploy WatchGuard was made, the installation was up and running in less than a month.

“WatchGuard offered a higher return on investment compared to the other vendors because its appliances are fully upgradeable to accommodate new features and meet new threats as they emerge. In terms of economics, it made perfect sense to purchase an appliance that offered multiple firewall options and could be upgraded to higher firewall standards at a later date, without needing to replace the entire appliance unit,” said Ong.

## **BENEFITS**

A WatchGuard network security appliance was installed as TMC’s first line of defense against all external Internet traffic, working hand-in-hand with a third-party antivirus enterprise software suite. After passing through the firewall, the Internet traffic is further checked for viruses, spam, and other harmful malware.

Since the organization installed the Firebox X700, X50, and X15w appliances, TMC has upgraded the firmware to Fireware® Pro on the X700 and purchased WebBlocker, spamBlocker, and Gateway AntiVirus/IPS subscriptions.

According to Ong, the benefits of TMC’s new WatchGuard security solution have exceeded the costs of implementing and maintaining the system.

“Since the implementation, we have not experienced any major network threats of any kind,” said Ong. “We have secured remote network access for our mobile users and we only require minimal IT support on the remote network connections. With WatchGuard security appliances, we can now access and run critical business applications such as ERP through our VPN connection. In addition, we can remotely manage our firewall configuration via the Web and VPN,” added Ong.

Ong also commented that the Firebox X700 appliance at the headquarters facility eliminated the need for another layer of security, allowing the unit to double as a router, while providing robust WAN redundancy and failover.

“Since we deployed WatchGuard security appliances, we have enjoyed more than 99% uptime on our VPN, with no WAN connection problems, and zero recorded unauthorized intrusions. As our growth requires additional users and more branch offices, we will definitely consider expanding our WatchGuard security solution to scale with our evolving needs,” concluded Ong.

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. ©2007 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. WGCE66477\_110807