

# Ryerson University

## Of Gigabits and Bottom Lines: Universities Need to Secure Internet Gateways and Subnets

### Background

The overflow of unwanted network traffic, viruses and other types of malware continues to be an ongoing problem for users of any sort of data services. The bloom in the information age has been a double-edged sword. On the one hand, it is easier than ever before to connect to networks such as the Internet with a variety of devices today, including cellular phones, computers and PDAs. On the other hand, these devices that offer extended connectivity are bringing with them a whole new family of security related challenges. Network administrators are more frequently taking the role of security administrator; and relatedly, having to allocate already limited resources to maintain a vigil against real-time network threats presents a challenge for even the most progressive private sector organization.

This need is multiplied, but paradoxically, the resources are more limited in a university or academic setting. The user base, consisting of students, administrators, university employees and local community users, has very unpredictable usage needs unlike the fairly defined needs of most companies. Students may need to access information Websites for research while employees may have to use that same network to access payroll or human resources.

### Situation

Ryerson University, based in Toronto, Ontario, is Canada's leader in career-focused education, with 80 graduate and undergraduate programs. Ryerson University was moving towards high-bandwidth Internet pipes at the gateway via a gigabit network. At the same time, the University needed to protect its network against increased attacks and unwanted traffic, while securing a growing amount of multi-platform devices that have restricted and unrestricted access to the campus Internet network. A growing number of network security challenges and incidents caused Ryerson University to take a look at its network security needs and requirements.

"Being a member of the Internet community has its privileges and its obligations," said Larry Lemieux, assistant director IT support for Ryerson University. "Just because our security needs are much more widespread than a corporate organization does not give us license to compromise on security practices. In fact, Ryerson University has a more extended reach into our community than many universities, with the largest continuing education program in Canada - a program that relies on secure access to data services such as video conferencing, multicasting, interactive multimedia course-ware and other technologies."

LCM Security, a leading Canadian based supplier of security products and technologies and Fortinet Platinum Partner, assisted Ryerson University with the evaluation and selection of its network security



RYERSON  
UNIVERSITY

*"100,000 virus incidents is a typical volume for us - monthly. Our FortiGate enterprise security appliances have scaled to protect our network from an extremely large volume of incidents, and have greatly reduced the amount of manpower necessary to maintain our network. In addition, by scanning outgoing and incoming traffic at the gateway, our FortiGate systems help us continue to be responsible citizens of the Internet."*

Larry Lemieux  
Assistant Director IT Support  
Ryerson University

Systems:  
FortiGate-3600 systems  
FortiGate-800 systems  
FortiGate-300 systems  
FortiManager system  
FortiGuard AV service  
FortiGuard IPS service

Industry: Education

# Ryerson University

## Of Gigabits and Bottom Lines: Universities Need to Secure Internet Gateways and Subnets

needs. The University needed a fault-tolerant security solution for its gigabit Internet gateway to keep up with today's prevalence of known and unknown malware threats.

Ryerson University's gigabit gateway services the diverse users of its network, some of which present new security challenges and implementations. "Ryerson has a large Distance Education program with students taking courses from around the world by using the Internet and never having to set foot on campus, in addition to the typical needs of a university network," said Lemieux. "Student residences, remote computers, wireless devices-all present unique security issues. The bottom line is that over 50,000 people, including students, employees and alumni, must have access to a vast network of IT services and the reality is that IT security best practices cannot always be applied-or as easily enforced-as in the private sector."

"Fortinet's FortiGate enterprise security appliances were able to be configured in a variety of modes, and seamlessly integrate into existing networks"

Larry Lemieux  
Assistant Director IT Support  
Ryerson University

### Solution

With the help of Lee Pecori, account manager at LCM Security, Ryerson University evaluated security products from other enterprise security vendors including Alteon, Cisco, NetScreen and Nortel, and ultimately chose and deployed Fortinet. "Fortinet was the cost-per feature leader," said Pecori. "In addition, Ryerson had different security needs in different parts of its network, and Fortinet was able to offer a combination of security products, services and support for these needs to comprehensively protect from edge to core, and at gigabit speeds."

To secure its University network, consisting of numerous multi-platform subnets for various departments, Ryerson University deployed an enterprise security platform with Fortinet's flagship ASIC-accelerated enterprise security appliances. FortiGate-3600 large enterprise security appliances are deployed in a cluster at the Internet gateway through which traffic is filtered and scanned for viruses, intrusions and other unwanted network traffic, using integrated firewall, antivirus and intrusion prevention technologies. Antivirus and intrusion prevention signature updates are delivered to the FortiGate systems via Fortinet's FortiGuard Antivirus and FortiGuard Intrusion Prevention Subscription Services.

A variety of FortiGate-800 enterprise security appliances and FortiGate-300 mid enterprise security appliances are deployed throughout the campus to protect different buildings and subnets for various academic and administrative departments. The subnets' security appliances are configured with individual and varied firewall policies and leverage integrated antivirus and intrusion prevention functionality for comprehensive internal network protection. Ryerson University centrally manages its FortiGate security appliances using Fortinet's FortiManager system, a management and monitoring tool that allows enterprises to easily manage large numbers of FortiGate systems.

Additionally, Ryerson University subscribes to three separate Internet Service Providers (ISPs), which are connected to the University's redundant core network switches. In the event of component failure, the network will automatically reroute ISP traffic from the FortiGate-3600 cluster to another FortiGate-3600 system running in firewall mode only. Another FortiGate-3600 system is used for testing of new versions of patches.

"Fortinet's FortiGate enterprise security appliances were able to be configured in a variety of modes, and seamlessly integrate into existing networks," said Lemieux. "Combining security into the network gateway can add overhead resulting in performance issues. Fortinet's ASIC chip alleviates this overhead by providing gigabit speed throughput at the gateway, while still maintaining comprehensive protection in real-time applications."

# Ryerson University

## Of Gigabits and Bottom Lines: Universities Need to Secure Internet Gateways and Subnets

### Success

Over the past year, Ryerson University's cluster of FortiGate-3600 systems at its Internet gateway has filtered out as many as 165,000 viruses in a single month, while the additional FortiGate systems act as a stalwart for its various internal networks. For Ryerson's network, virus incident numbers vary in line with the academic cycle such that the volumes tend to be low during the summer when students are mostly away and higher at the beginning of term when most students come back, and the FortiGate systems scaled seamlessly to provide appropriate protection and support.

"100,000 virus incidents is a typical volume for us-monthly," said Lemieux. "Our FortiGate enterprise security appliances have scaled to protect our network from an extremely large volume of incidents, and have greatly reduced the amount of manpower necessary to maintain our network. In addition, by scanning outgoing and incoming traffic at the gateway, our FortiGate systems help us continue to be responsible citizens of the Internet."

**Learn More at [Fortinet.com](http://Fortinet.com)**

[Fortinet.com/contact](http://Fortinet.com/contact)

Tel: +1-408-235-7700 - Sales: +1-866-868-3678 - Tech Support: +1-866-648-4638

\* 2005 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiGuard, and FortiManager are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. CAS1380510