



## County Government Links Sites, Protects Citizens

A Case Study in Network Security

*“The WatchGuard units enable a huge WAN topology for us, including both managed and unmanaged tunnels,” states Jean St-Pierre. “It’s very hard for me to have stability and performance plus security. The only way we can do that at a reasonable cost is with WatchGuard security solutions.”* **Jean St-Pierre, IT Manager**

### BACKGROUND

In eastern Ontario, Canada, the United Counties of Prescott and Russell deliver emergency and social services and handle public works for a largely rural area. Approximately 80,000 residents are distributed across small towns and villages. The government’s IT department connects approximately 40 widespread sites using whatever connections are locally available. The budgets are tight and the staff is small. For more than ten years, the united counties have relied on WatchGuard for terminating and securing their connections, evolving from a handful of sites in the beginning to an extensive, sophisticated and highly secure WAN topology.

## CHALLENGE

The most recent upgrade came with the installation of a fiber line to the data center, providing more capacity to serve new public works sites as well as remote users working from home. Explains Jean St-Pierre, IT Manager for the counties, “I looked at all the tunnels we were adding — every month, we had to create new tunnels. We’ve always used WatchGuard, because the tunneling engine is very strong, very stable, easy to manage and easy to configure. I looked at the specs on the new WatchGuard devices and found that the proxied services, performance, tunneling engine and throughput were exactly what I needed to increase performance at the main site while benefiting from the speed of fiber.”

## WATCHGUARD® SOLUTION

Jean St-Pierre installed a WatchGuard Firebox® X Peak™ 5500e at the main data center, and he immediately saw an “incredible performance increase.” The X5500e serves as the endpoint for over a hundred tunnels, each terminated at the other end by a WatchGuard device. Some are legacy units, while some are newer WatchGuard Firebox X Edge devices including X10e, X20e and X55e appliances in both Ethernet-only and wireless models.

“The WatchGuard units enable a huge WAN topology for us, including both managed and unmanaged tunnels,” states Mr. St-Pierre. “In addition to the sites, we’re also allowing more supervisors and directors to connect from home. We found out that a small Edge appliance was the best and most reliable way to connect them. In the long run, it pays off because you don’t have to maintain it much — it’s very stable.”

## BENEFITS

“Since we are in a rural environment and don’t have big budgets, we need to work around those limitations,” explains Mr. St-Pierre. “It’s very hard for me to have stability and performance plus security. The only way we can do that at a reasonable cost is with WatchGuard security solutions.”

### Proxied Services for Government-Strength Security

“We’re a government agency, and need to be extremely secure because we can be a target for attacks,” declares Jean St-Pierre. So he maintains an extremely vigilant security posture, relying heavily on the WatchGuard appliance’s application-layer proxies. “The proxies offer more security than the other appliances out there, and add an extra layer of security that we need here at the counties. What’s wonderful is that the proxies are available with FTP, SMTP, HTTP, HTTPS, and any type of custom service that you can think of. All the traffic that is coming from the outside world to our DMZ is inspected by those proxied services and the packets are opened and identified.

“We’re very granular, even when it comes to mime types. WatchGuard makes it easy to manage and understand. For example, if a .pdf file comes in with a mime type that’s not compliant with standards, you know why it’s been blocked. If we trust it, we’ll define a new rule and let it in. If we don’t trust it, it will be dropped, and we’ll keep it that way.”

### One Hundred Tunnels, No Issues

“We’re providing services to our citizens, and there’s a lot of information that needs to be secured,” says Mr. St-Pierre. “We’re talking about welfare, childcare services, and public works. We have emergency services as well - we’re supporting 18 ambulances, plus a few cars. They all have Internet in the vehicles, and they’re popping an application every time there’s an emergency situation. If they need to populate a patient chart, it’s tunneling back to the data center.”

Some of the connections are extremely data-intensive. “Every key site that has a server is using a very cool WatchGuard feature called zero-route tunneling to complete a full tunnel to the data center. Our main office in L’Original talks to a Domain Controller Replication Partner at each site that takes care of replicating files. All the security/antivirus is also partnered - the main servers at the data center have replication partners that get the refreshes to deploy the antivirus. And we also have WSUS at the other sites that are keeping the Microsoft patches up to date. So a lot of data is going through.

“The star topology that we’re using is one hundred percent based on WatchGuard tunnels, and they’re very efficient. We’re pushing and pulling data through a hundred tunnels and we’ve never had a single issue,”

### **QoS for Prioritizing the Most-Essential Services**

For Jean St-Pierre, the WatchGuard QoS capability is another key to maintaining a reliable distributed-computing infrastructure. As he says, “We have 62 services coming through the X5500e that are working together at the same time, all the time. I don’t want any of those services killing my tunnel services. So I give less priority to SMTP traffic, because we don’t need that much performance for emails, and less to the other services like FTP, HTTP, and other customized services. I give more juice to the tunnels. We’re also able to prioritize tunnels as needed.”

### **Streamlined Management, Backed by Responsive Support**

Strikingly, only three system administrators handle the entire infrastructure, including the servers at the remote sites. Mr. St-Pierre credits that to the stability of the tunnels and the manageability of the WatchGuard appliances running WatchGuard System Manager. “We have a dedicated server to maintain, configure and update the appliances, maintain the tunnels and to see the cloud — everything that is going on, the alerts, the logging, the reporting. With WatchGuard, we’re able to manage those remote offices as if they were in the main office.”

“The other thing that I’ve appreciated from WatchGuard, is the high level of service, their Gold LiveSecurity support is very good, and very fast. They understand what we’re talking about and recognize that we’re advanced users. When we need their help, they always deliver.”

---

#### **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 has been building award-winning unified threat management (UTM) network security solutions that combine firewall, VPN and security services to protect networks and the businesses they power. We recently launched the next generation: extensible threat management (XTM) solutions featuring reliable, all-in-one security, scaled and priced to meet the unique security needs of every enterprise. Our products are backed by 15000 partners representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including retail, education, and healthcare. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

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. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and Firebox 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. WGCE66642\_100909