CASE STUDY

Mission Accomplished: Fortinet Dramatically Improves Security for British Columbia City

Located in the forests of British Columbia in northwestern Canada, the city of Mission is an idyllic setting. “We have lakes and a lot of trees,” explains Chris Knowles, Manager of Information and Telecommunications Systems for the city. “Mission is also steeped in tradition and First Nations heritage, and a lot of artists and artisans make their home here.”

It is also a bedroom community located about an hour outside of Vancouver, B.C. “Because of the West Coast Express commuter rail line, people can live in Mission and work in Vancouver,” Knowles says. “We have access to the amenities and shopping of a big city, but housing here has historically been priced a little lower than in communities closer to Vancouver.” For all these reasons, the city is growing rapidly; projections indicate its population will double over the next quarter century.

Being such a quiet, family-friendly community “is a blessing, and a curse to some degree,” Knowles says. “We have around 41,000 residents, and the city aspires to shift the homeowner tax burden, to put more money back in residents pockets by expanding the industrial and commercial tax base. This is essential as it looks to bring new services and amenities online and to attract new residents and businesses to the community. For those reasons, the city of Mission is always diligent about optimizing its use of tax dollars.”

Addressing Security Concerns with Limited Staffing

Knowles, along with Technical Services Supervisor Shaun Greene and three other IT professionals, manage networking, security, telecommunications, and other technology needs across the city’s 17 locations. “We do not have a large enough staff for anyone to dedicate most of their time to security remediation,” Knowles says.

Still, “the ever-evolving threat landscape is very high on our priority list,” he adds. “We are constantly trying to stay abreast of vulnerabilities and zero-day attacks. Staying ahead of the hackers is a challenge that municipalities across the country are struggling with, and it is magnified for a smaller team like ours.”

A couple of years ago, the city was running security solutions from a total of eight different vendors. “Our network had evolved over time into a multi-vendor soup,” Knowles explains. “The city might budget a replacement of firewalls one year and switches the next, replacing solutions one at a time. The products we were using were best of breed, but each had its own logs and its own interface, and many of them were closed and proprietary. The complexity of our infrastructure made it more difficult to achieve some of our security goals.”

In 2020, the city engaged an external firm to perform a security audit. The report indicated that Knowles’s team was doing well in some areas, but that a network redesign could provide better resiliency and streamline security. “We were lacking some next-generation capabilities, and we had difficulty ascertaining what was really going on in the network,” Knowles says. Mission engaged Vancouver-based Wirefire Solutions Inc. to develop a vendor-neutral network design that would simplify management and visibility into security events.

CITY OF Mission ON THE FRASER

“A lot of municipalities are struggling with evolved networks that they have never been able to redo from the ground up. When you can go from the complexity that we formerly had to a full redesign with one provider, why wouldn’t you?”

– Chris Knowles, Manager, Information and Telecommunications Systems, City of Mission, B.C.

Details

Customer: City of Mission

Industry: Government

Headquarters: Mission, British Columbia, Canada

Number of Secure SD-WAN Locations: 13

Business Impact

- Dramatically improved security posture minimizes chances that an attack will be successful
- 15% reduction so far in total cost of ownership (TCO) of security infrastructure
- Minimal staff time required to manage security and networking across 17 city locations

"Once we had the design, we shopped around for a solution that would be a good match," Knowles says. "We focused on three proposals. Fortinet really separated from the pack in terms of the integration among the products and management simplicity. In addition, the transition process would have been very slow with the other vendors. They would have replaced one technology at a time, dragging out the project for multiple years. Fortinet offered to provide wireless and networking all at once. Because of the timeline, cost, and single-pane-of-glass management, we decided to go with Fortinet."

The city of Mission worked with local provider IT Blueprint to deploy FortiGate Next-Generation Firewalls (NGFWs) and FortiSwitch enterprise switches. "We created a new network that ran in parallel with our legacy network," Greene says. "We stood up the firewalls and switches in several locations and started moving end-users over to the new network. Then we gradually worked into Wi-Fi, deploying FortiAP access points and FortiWeb, Fortinet's web application firewall. And we rolled out the FortiClient endpoint solution for VPN connectivity, endpoint vulnerability scanning, and other endpoint protection features."

Security on a Mission

Today, the city of Mission runs a high-availability pair of FortiGate NGFWs at the city's primary data center and disaster recovery locations. These sites connect with one another and four additional key city facilities via private fiber connections. "We use the Secure SD-WAN [software-defined wide-area networking] capabilities built into the FortiGate devices to balance internet connectivity between the two data centers," Greene says. "So, rather than having one firewall just sitting there not being used, we can use both at the same time, which is improving our network performance."

Each of the city's 15 other locations runs a single FortiGate NGFW, and the 11 that do not have fiber connectivity use Fortinet Secure SD-WAN for their WAN connections. The FortiGate NGFWs also provide internal segmentation of each site's local-area network (LAN), helping prevent lateral movement should an attacker successfully breach the city's network perimeter.

"All the traffic trunks back to the FortiGate devices, so they inspect everything in between every VLAN [virtual LAN]," Greene says. Every endpoint runs FortiClient, and "we use some of the ZTNA [zero-trust network access] tagging in FortiClient to dynamically apply firewall policies. FortiClient will determine whether a workstation is up to date with antivirus, or whether it has permission to contact a certain server, then determine which firewall policies apply. That microsegmentation of the network has improved our internal security dramatically."

FortiSwitch devices handle routing within each city location, and FortiAP access points provide wireless networking. FortiAuthenticator facilitates client authentication for both Wi-Fi and wired LAN connections. When an outsider, such as a consultant, needs VPN access to the city's network, FortiToken provides multi-factor authentication (MFA). The FortiGates and FortiWeb filter inbound and outbound internet traffic.

"We never did outbound inspection previously," Greene says. "Now, traffic to sites that are not listed in the Fortinet database runs through a FortiGate analysis of encrypted traffic. That was relatively painless to implement, and it has been really

Products and Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiClient
- FortiWeb
- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- FortiToken

> *"All the products have a familiar look and feel, and they communicate with one another. With FortiAnalyzer, we can follow an issue all the way through the network from a single pane of glass, as opposed to trying to stitch together multiple different products."*
>
> – Shaun Greene, Technical Services Supervisor, City of Mission, B.C.

helpful. The FortiGate NGFWs have not found any issues that we were unaware of, but they are regularly blocking malicious traffic." The city council was also impressed with the anti-scraping capabilities found in FortiWeb. "We are always concerned about bots scraping emails and contact information off our websites and then using that data for malicious purposes. This is a nice feature to protect against that," adds Knowles.

Simplified Day-to-Day Management

The Fortinet solutions have substantially improved the efficacy of the city's security infrastructure. Equally important for this lean team, they have dramatically reduced the complexity of managing security day to day. Because all the solutions are part of the Fortinet Security Fabric, they provide Knowles, Greene, and the team with the simplified management they were looking for.

"All the products have a familiar look and feel, and they communicate with one another," Greene says. "We get centralized logging, with log data pulled from all our different solutions. And with FortiAnalyzer, we can follow an issue all the way through the network from a single pane of glass, as opposed to trying to stitch together multiple different products." FortiAnalyzer also alerts the team when a security incident requires their attention.

> *"The FortiGate devices inspect everything in between every VLAN. We use some of the ZTNA tagging in FortiClient to dynamically apply firewall policies. That microsegmentation of the network has improved our internal security dramatically."*
>
> – Shaun Greene, Technical Services Supervisor, City of Mission, B.C.

Meanwhile, FortiManager simplifies firewall management. "We are using FortiManager to manage the configuration and deployment of our remote firewalls," Greene explains. "That way, we can ensure our firewall policies stay consistent. We can onboard new locations quickly, rather than configuring everything from scratch, and we can push policy changes to all the locations at the same time. A few sites have minor anomalies for specific reasons, but we manage that through FortiManager as well."

All in all, Knowles estimates that the transition to the Fortinet solutions is saving the city of Mission around 15% on total cost of ownership of the security infrastructure. "And that is only going to increase, as we continue to phase out legacy solutions," he says. Next up, the city is planning to replace a legacy phone system with a FortiVoice Secure Unified Communications solution. It is also evaluating Fortinet protection for its operational technology (OT) systems.

"A lot of municipalities are struggling with evolved networks that they have never been able to redo from the ground up," Knowles concludes. "When you can go from the complexity that we formerly had to a full redesign with one provider, why wouldn't you?"

December 6, 2022 10:41 PM

1870165-0-0-EN