Electrical Utility Safeguards Grid from Malicious Threats

British Columbia Transmission Corporation uses security solutions to protect systems and streamline compliance.

EXECUTIVE SUMMARY

BCTC

- **Industry:** Energy
- **Location:** Vancouver
- **Number of Employees:** ~450

BUSINESS CHALLENGE

- Protect critical infrastructure from internal and external threats
- Manage multiple levels of access for different users
- Comply with strict regulatory requirements

NETWORK SOLUTION

- Intrusion Prevention/Detection System (IDS/IPS) and policy management solutions

BUSINESS RESULTS

- No security-related anomalies detected in network since deployment
- Highly reliable security for corporate network to help safeguard critical infrastructure
- Reduced time-consuming manual effort to demonstrate compliance and configure network devices

Business Challenge

British Columbia Transmission Corporation (BCTC), a major North American electric utility, manages the publicly owned transmission system for British Columbia. Responsible for helping ensure the safe transmission of electricity within British Columbia, BCTC's operation is considered "critical infrastructure." As a result, the company must comply with the North American Electric Reliability Corp. (NERC) Critical Infrastructure Protection (CIP) regulatory standards which are intended to maintain the reliability of the bulk electric system.

"We are responsible for ensuring a reliable bulk electric system for both British Columbians as well as those Canadian and American utilities which interconnect with the grid," says Tony Dodge, IT planner and coordinator, BCTC. "That includes protecting against a breach of our IT network that could severely impact BCTC's critical systems."

"We try to keep critical systems separated from our corporate Internet-connected applications to lower our security risk," says Dodge. "But we also recognize that people are getting smarter, and the technology used for malicious attacks is getting less expensive and more widespread. We really have to be on our toes."

Complicating the problem is the fact that BCTC needs different levels of network access for different users, including external consultants who must be given some level of access to perform services on behalf of BCTC.

"We have hard rules in effect to ensure we protect our critical infrastructure from both inside and outside threats," says Dodge. "One key aspect of this is promoting a "need to know" account management strategy to ensure only those who need to access our critical assets for their work related duties are permitted to do so. Making sure all of the devices in our network are configured appropriately for the different levels of access can be challenging."

As BCTC prepared for the 2010 Vancouver Winter Olympic Games, the pressure only grew to help ensure that British Columbia's electricity grid would be reliable and secure.

"We knew the entire world would be watching Vancouver," says Dodge. "If the electricity supply to any game venues was compromised it would have had a major impact on BCTC's reputation. We needed to make sure we could closely monitor any traffic coming through our firewalls to detect and respond to any anomalies."

Network Solution

With so much relying on BCTC's transmission infrastructure, the company has enormous responsibility to keep its network safe from malicious attacks. To accomplish this, BCTC utilizes Cisco® security solutions.

BCTC uses Cisco routers, switches, and firewalls as the foundation of its network infrastructure. However, as a public utility, the company was required to examine all options when undertaking the security overhaul that would help ensure CIP compliance and help prepare for the Olympics. BCTC turned to KOIOS Systems, a Cisco Premier Partner with proven expertise in large enterprise and government security solutions.

> "The Cisco IDS/IPS defenses have definitely enhanced our overall security. Since we deployed the solution, we have not seen a single anomaly penetrate our defenses."
> **—Tony Dodge, IT Planner and Coordinator, Enterprise Security, BCTC**

KOIOS conducted a study of security solutions on the market. At the end of the process, Cisco was the clear choice for BCTC.

"We were able to demonstrate the benefits BCTC would realize by integrating new security capabilities within the existing infrastructure," says Alexander Kotchetkov, managing director, KOIOS Systems. "By implementing new security features in the Cisco devices that were already deployed, we were also able to reduce the cost of the project."

"Our biggest concern is reliability: making sure that the equipment we deploy will coexist with our environment and deliver the results we need," says Dodge. "We didn't want to go with a patchwork design for the new security implementation. It made a lot of sense to use Cisco security modules and appliances."

Intrusion Prevention

To safeguard against malicious attacks, BCTC deployed Cisco Intrusion Detection/Prevention System (IDS/IPS) solutions. Because BCTC already uses Cisco ASA 5500 Series Security Appliances, the company was able to add IPS capabilities by simply installing Cisco Advanced Inspection and Prevention Security Services Modules (AIP-SSM). Now, in addition to providing robust firewall and virtual private network (VPN) services, the Cisco ASA platforms closely monitor all network traffic to identify and lock down abnormal activity.

To protect other segments of the network, BCTC uses standalone IPS appliances, Cisco IPS 4200 Series Sensors. The solutions provide the same sophisticated defenses against malicious threats, as well as the ability to be segmented into multiple "virtual" sensors. That means BCTC can extend strong IPS protection across logically separated corporate and transmission networks, without having to invest in separate hardware.

"BCTC has different security policies and requirements for the different networks, so we needed separate IPS instances, but we wanted to be able to manage them as one system," says Kotchetkov. "The ability to partition the IPS appliances into separate sensors, with each monitoring and analyzing a different network within the same piece of hardware, was a tremendous value."

Policy Management

BCTC also needed tools to help enforce the diverse security policies. At KOIOS' recommendation, the company deployed Cisco Security Manager (CSM). CSM provides a comprehensive tool for managing policies, configuration, and tuning of security devices in the network from a single interface. The tool will also help BCTC demonstrate compliance with CIP regulations.

"Under CIP requirements, we have to track anyone making changes or updates to any of our firewall or IPS configurations," says Dodge. "We have to ensure that they're logged in properly and that we have a history of all changes made. CSM provides an excellent tool for managing all of those policies centrally."

Expert Implementation

BCTC worked with Cisco Premier Partner, KOIOS Systems, through the entire process (from the early planning stages, to the competitive analysis, to the implementation), and the utility was very pleased with every step.

“We’ve had such great experiences with KOIOS,” says Dodge. “They have been a strong partner and they provided highly qualified and professional staff. I can’t say enough good things about them.”

Business Results

Today, BCTC has a stronger and more manageable security environment that provides powerful defenses against malicious threats. The company is a leader in CIP compliance, and supported the Winter Olympic Games, with the eyes of the world on Vancouver, with zero security incidents. The new IPS capabilities in particular have proven highly successful, and give BCTC the confidence of knowing that its network is “on the watch” for any suspicious activity that could affect the critical transmission grid.

“The Cisco IPS defenses have definitely enhanced our overall security,” says Dodge. “Since we deployed the solution, we have not seen a single anomaly get through our defenses.”

The new security solutions are also helping BCTC’s network and security teams operate more efficiently, even as they take on new demands for meeting regulatory requirements and demonstrating compliance.

“Cisco Security Manager allows BCTC to simplify software updates for all of the IPS sensors and modules, and other security devices” says Kotchetkov. “It provides a centralized tool where the utility can run one job, and update everything.”

“Without CSM, we would have to configure each network device with individual user names and accounts to track people making changes,” says Dodge. “It would be a much more manual, labor-intensive process. CSM lets us manage all of our policies from a central interface. It’s a tremendous time-saver.”

Ultimately, BCTC’s Cisco network and security infrastructure provides a much more manageable and effective defense system, and helps safeguard the critical electricity grid on which British Columbia depends.

PRODUCT LIST

Routing and Switching

- Cisco Catalyst® 6500 Series

Security and VPN

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco AIP-SSM Advanced Inspection and Prevention Security Services Module for Cisco ASA 5500 Series
- Cisco IPS 4200 Series Sensor
- Cisco FWSM Firewall Services Module for Cisco Catalyst 6500 Series
- Cisco Security Manager

“There’s a natural synergy when a customer is using Cisco gear,” says Kotchetkov. “We can take advantage of the synergy and vision Cisco has, and the integration between different network layers, components, and management systems, and create a single solution that really works for a customer.”

“When you start bringing in a patchwork infrastructure, you end up having to deal with multiple vendors and multiple levels of support,” says Dodge. “With Cisco, we only have to go to one place to resolve issues. It comes down to easier maintenance, faster problem resolution, and most important, a more reliable environment.”

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C36-609138-01 09/10